FACULTAD DE POSGRADOS

Diseño de una hoja de ruta para la implementación de los planes de continuidad basados en cloud computing de los servicios tecnológicos que soportan los procesos de logística de una empresa ubicada en el Aeropuerto Internacional Mariscal Sucre

AUTOR

Dennis Fernando Reyes Pérez

AÑO

2019

FACULTAD DE POSGRADOS

Diseño de una hoja de ruta para la implementación de los planes de continuidad basados en cloud computing de los servicios tecnológicos que soportan los procesos de logística de una empresa ubicada en el Aeropuerto Internacional Mariscal Sucre

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magister en Gerencia de Sistemas y Tecnología Empresarial.

Profesor Guía

MSc. Carlos Andrés Regalado Moncayo

Autor

Dennis Fernando Reyes Pérez

Año

2019

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido el trabajo, Diseño de una hoja de ruta para la implementación de los planes de continuidad basados en cloud computing de los servicios tecnológicos que soportan los procesos de logística de una empresa ubicada en el Aeropuerto Internacional Mariscal Sucre, a través de reuniones periódicas con el estudiante Dennis Fernando Reyes Pérez, en el semestre 202000, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Carlos Andrés Regalado Moncayo

Magister en Gerencia de Sistemas

CI: 1716459373

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, Diseño de una hoja de ruta para la implementación de los planes de continuidad basados en cloud computing de los servicios tecnológicos que soportan los procesos de logística de una empresa ubicada en el Aeropuerto Internacional Mariscal Sucre, del estudiante Dennis Fernando Reyes Pérez, en el semestre 202000, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Jairo Javier Goyes Mosquera

Magister en Gerencia de Sistemas

CI: 1714191952

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

Dennis Fernando Reyes Pérez

CI: 1718040619

RESUMEN

En la actualidad las organizaciones sean estas grandes o pequeñas, se encuentran preocupadas por mantenerse a flote dentro del mercado tan competitivo en donde desarrollan sus actividades. Esto hace que su intranquilidad por mantener sus procesos operativos ante cualquier eventualidad se acreciente a través del tiempo.

El plan de continuidad de negocio ofrece a cualquier tipo de compañía mantenerse preparada y consciente de las diversas circunstancias por las que el negocio atraviesa. Conocer las principales amenazas que ponen en riesgo las operaciones normales de la empresa y su continuidad en el mercado, hace que estas preocupaciones se conviertan en fortalezas el momento en que se presente algún evento que detenga los procesos críticos de una organización.

El presente documento detalla una guía para la implementación de un plan de continuidad de negocio que se encuentra estructurado en cinco fases. La primera fase, parte del entendimiento del negocio de la Zona de Distribución del Aeropuerto Internacional Mariscal Sucre. Una vez entendido el giro del negocio, se definen los procesos críticos para que la organización proporcione un presupuesto para establecer un plan de contingencia y que dichos procesos se encuentren operativos durante todo el tiempo de vida de la compañía. Con esta información, se detallan los servicios y componentes tecnológicos que soportan y apalancan de forma estratégica dichos procesos de negocio.

La tercera fase hace énfasis en el análisis de riesgos sobre los procesos críticos de la organización, los servicios y componentes tecnológicos. La forma en que los mitiga o transfiere a terceros con el fin de controlar las operaciones en el aeropuerto. Después, se estructura un análisis de impacto de negocio identificando los diferentes tiempos de restauración y de recuperación que la Zona de Distribución está dispuesta a soportar cuando un evento que paralice las actividades core de la organización se materialice. El momento que esto sucede, la empresa se puede ver afectada tanto de forma económica como de

imagen. De la misma manera, pone en riesgos su continuidad dentro del mercado.

En base a la información anterior, nace la cuarta fase del presente estudio. En este apartado se establecen las estrategias de recuperación que la Zona de Distribución debe emplear antes de activar el plan de continuidad de negocio. Adicional, se realiza un análisis de posibles escenarios contrastados con un análisis de riesgos. La principal estrategia de recuperación planteada en este documento es la continuidad de negocio basado en Cloud Computing, para este estudio se hace énfasis en la recuperación de desastres como un servicio DRaaS.

Finalmente, la quinta fase presenta una guía de implementación con el objetivo principal de poner a disposición de la compañía un manual para implantar un plan de continuidad de negocio. Dicho plan estará alineado desde los objetivos estratégicos de la organización, lo que le permitirá mantenerse preparada ante cualquier eventualidad en donde su core de negocio se vea afectada y con ello las operaciones de comercio exterior del país.

ABSTRACT

Nowadays, big or small organizations are worried about staying afloat within the competitive market where they develop their activities. This makes increase over time their restlessness to maintain their operational processes to any eventuality.

The business continuity plan offers to any type of company to be prepared and awared of the various circumstances that the business goes through. Knowing the main threats that put the normal operations of the company at risk and their continuity in the market, makes these concerns become strengths when an event that stops the critical processes of an organization occurs.

This document details a five phases guide for the implementation of a business continuity plan. The first phase starts with the understanding of the business of the Distribution Zone of Mariscal Sucre International Airport. Once the business is understood, the critical processes are defined that the organization is willing to establish a budget to control and kept these processes operative during all the life of the company. With this information, the services and technological components that support and strategically leverage said business processes are detailed.

The third phase emphasizes the analysis of risks on the critical processes of the organization, the services and technological components. The way it mitigates or transfers them to third parties in order to control operations at the airport. Afterwards, a business impact analysis is structured, identifying the different restoration and recovery times that the Distribution Zone is willing to support when an event that paralyzes the core activities of the organization materializes and the company can be affected both economic and in an image, and put its continuity in the market at risk.

Based on the above information, the fourth phase of the present study is born. This section establishes the recovery strategies that the Distribution Zone must use before activating the business continuity plan. Additionally, an analysis is made of possible scenarios contrasted with a risk analysis. The main recovery

strategy proposed in this document is business continuity based on Cloud Computing, for this study, emphasis is placed on disaster recovery as a service DRaaS.

Finally, the fifth phase presents an implementation guide with the main objective of making available to the company a manual for implementing a business continuity plan. Aligned since the strategic Objectives of the organization that allows the company to be prepared before any eventuality where its core business is affected, and with it the foreign trade operations of the country.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

El presente trabajo de titulación tiene como objetivo principal diseñar una guía de implementación orientada a un plan de continuidad de negocio tomando como referencia estándares, normas y modelos. En donde, mediante el apalancamiento tecnológico que brinda el cloud computing establecer una hoja de ruta que pueda ser utilizada por la Zona de Distribución del Aeropuerto Mariscal Sucre para su futura implementación.

El documento trata de integrar varias áreas de conocimiento para fortalecer la veracidad en la obtención de resultados. Se espera que las empresas que manejen procesos logísticos aeroportuarios dispongan de una estructura definida que les permita mantener sus procesos críticos en total funcionamiento ante cualquier eventualidad que afecte el core del negocio de la empresa.

Para el desarrollo de la guía de implementación se ha estructurado el trabajo en siente capítulos. El primer capítulo detalla el nivel de criticidad que tienen los procesos aeroportuarios en el país, define el objetivo general con los respectivos objetivos específicos. El siguiente capítulo define el marco metodológico donde se detallan las herramientas a utilizar para conseguir los objetivos planteados en el presente trabajo de titulación.

El tercer capítulo desarrolla la situación actual de la Zona de Distribución en el Aeropuerto Mariscal Sucre. Este apartado identifica los servicios, componentes y arquitectura tecnológica que dispone la empresa para su correspondiente análisis y definición del plan de recuperación.

La siguiente sección identifica los riesgos en base a los procesos críticos de la empresa y estos a su vez asociados al impacto de los servicios tecnológicos que soportan dichos procesos.

El quinto capítulo presenta el plan de recuperación de los servicios de tecnología sobre los procesos críticos de la Zona de Distribución del Aeropuerto Mariscal Sucre. Las estrategias definidas en este documento se basan principalmente en Cloud Computing.

En el sexto capítulo se define la guía de implementación de los planes de recuperación basados en una hoja de ruta de mejoramiento. Para finalizar el trabajo de titulación se establecen las conclusiones y recomendaciones que deberán ser considerados en un futuro.

1.1 Antecedentes

Actualmente la Zona de Distribución del Aeropuerto Internacional Mariscal Sucre dispone procesos críticos que tras una interrupción puedan afectar con la economía o la imagen de la compañía. Es importante fortalecer las estrategias de continuidad de los servicios de la organización con el fin de contrarrestar eventos como: desastres naturales, cortes de energía por largos periodos de tiempo o daños de componentes en los equipos físicos en data center locales.

Dentro de los procesos aeronáuticos, la empresa gestiona el cien por ciento (100%) de carga que arriba al país y el setenta y cinco por ciento (75%) de toda la mercadería que se exporta, principalmente flores. La organización al disponer de un modelo de negocio en donde sus procesos críticos están soportados por tecnología, es primordial que se desarrolle la iniciativa de continuidad de servicios de tecnología; con esto la organización dispondrá de estrategias de recuperación de los servicios tecnológicos que soportan los procesos críticos del negocio. Es importante desarrollar estas estrategias ya que en un caso extremo, la organización podría verse en la necesidad de parar sus operaciones y en un caso extremo, cerrar la empresa.

Uno de los temas más importantes es que la empresa es el brazo operativo del Servicio nacional de Aduana del Ecuador (SENAE), por lo que, el cierre de las operaciones de la organización conlleva un gran impacto en los procesos de comercio exterior del país. Lo anteriormente mencionado, se traduce en pérdidas millonarias para la empresa y su reputación se verá impactada negativamente.

En el caso de la Zona de Distribución del Aeropuerto Internacional Mariscal Sucre, es fundamental mapear aquellos servicios tecnológicos que soporten los procesos logísticos de la organización, validar los principales stakeholders e identificar las soluciones tecnológicas serán los factores de éxito para respaldar a la organización ante cualquier acontecimiento, inclusive de su prestigio y reputación.

Es importante mencionar que cloud computing ya no es una tendencia, por lo contrario, esta tecnología es una opción atractiva para fortalecer las diferentes iniciativas de las organizaciones. Esto se debe a que hoy en día la computación en la nube se ha convertido una tendencia global que apalanca de forma óptima la gestión de servicios de TI.

1.2 Justificación

En la actualidad, las organizaciones se encuentran en un punto de inflexión en la correcta gestión de sus activos tecnológicos. La era de la digitalización, obliga a todas las compañías concienciar una gestión adecuada a uno de sus principales activos que es la información. En esta era, en la que se dispone varios dispositivos interconectados transfiriendo información cada segundo, es importante que cada empresa considere este activo tan valioso.

La empresa se ha visto en la necesidad de analizar los procesos core de negocio que puedan afectar las operaciones de logística en el Aeropuerto Internacional Mariscal Sucre. En este escenario, la organización ha definido al proceso de logística como unos de los procesos críticos que requieren ser mapeados a detalle para la definición de las actividades, servicio y componentes a ser tomados en cuenta para su correcta gestión.

En su preocupación, la compañía ha realizado un levantamiento de definición de eventos y la identificación de posibles riesgos para el proceso logística, y al tener todas sus actividades en cascada, se llegó a la conclusión de definir un esquema

que permita levantar los servicios de TI en el menor tiempo posible con la finalidad de soportar los procesos críticos de la organización. Según el análisis realizado, del total de ingresos que mantiene la empresa, en el 2017 el manejo de carga tuvo una ponderación del cuarenta y dos por ciento (42%), y de lo que va del año 2018 con corte al mes de mayo el proceso de logística en el Aeropuerto Internacional Mariscal Sucre corresponde en un cuarenta por ciento (40%).

Es decir, la afectación económica que sufriría la empresa cuando este proceso de negocio se vea afectado es de gran escala. Adicional, la consecuencia que tendría el Aeropuerto al no disponer del brazo operativo y gestión documental sería importante al ser considerada la empresa como unos los principales facilitadores del comercio exterior del país.

De acuerdo a la información anterior el proceso logístico de la empresa debe ser considerado y gestionado tecnológicamente de acuerdo a las mejores prácticas. Se debe analizar y definir esquemas de disponibilidad y tiempos de recuperación aceptables para que los servicios y componentes tecnológicos soporten de la mejor manera a las estrategias de la organización. En base a la criticidad del proceso contar con un plan de recuperación es de suma importancia para lo cual se considerará la inclusión de estrategias de recuperación basadas en Cloud Computing.

1.3 Objetivos

1.3.1 Objetivos Generales

Proponer una hoja de ruta para la implementación de los planes de recuperación de los servicios tecnológicos que soporte el proceso logístico de distribución basado en estándares y buenas prácticas.

1.3.2 Objetivos Específicos

- Identificar y analizar los diferentes marcos de referencia y buenas prácticas que guíen en el diseño de estrategias de recuperación y planes de continuidad.

- Definir los servicios y componentes tecnológicos que soportan las actividades del proceso de logística en la organización.

- Determinar los riesgos y el impacto asociado de los servicios tecnológicos que soportan el proceso logístico de la organización.

- Elaborar el plan de recuperación de los servicios de tecnología priorizando sus estrategias hacia Cloud Computing.

- Elaborar la guía de implementación de los planes de recuperación en base a una hora de ruta de mejoramiento.

1.4 Metodología Investigativa

Para el desarrollo de este trabajo de titulación se utilizará como base la metodología de investigación explicativa que se utiliza con el fin de analizar las causas y consecuencias de una situación puntal que permitirá identificar los factores que intervienen en la estructuración de un plan de recuperación de servicios tecnológicos.

2. MARCO TEÓRICO

2.1 Marcos de referencia de continuidad

Hoy en día, las organizaciones de todos los tamaños deben prepararse técnicamente y establecer políticas que le permitan protegerse ante cualquier eventualidad sea esto causado por un fenómeno natural o negligencia humana. La capacidad que tiene una empresa de recuperarse antes estos posibles eventos está directamente asociada a su grado de madurez que disponga en su planificación de la continuidad de negocio antes que este ocurra. (St-Germain René, 2014)

2.1.1 Modelo americano ISO/IEC 22301

El modelo americano ISO 22301, es un estándar internacional cuyo objetivo principal es ayudar a las organizaciones a implementar un plan de continuidad de negocio. Su contribución es ofrecer una protección y una ayuda para recuperarse de desastres naturales que afecten los procesos de negocio de la empresa. (BSI Group, 2016)

Los requisitos para la implementación de la ISO 22301 son aplicables a todas las organizaciones cualquier sea esta su naturaleza. Es decir, es independiente del tipo, tamaño y su alcance; depende de los procesos de cada empresa y la complejidad de sus estrategias. (St-Germain René, 2014)

Entre los principales beneficio ofrece:

- Ayuda a proteger al negocio
- Genera confianza al negocio
- Aumenta la ventaja competitiva

- Gestiona el riesgo empresarial

La norma ISO 22301 se basa bajo el principio operativo Plan-Do-Check-Act (PDCA).

- **Plan:** Establecer la política de continuidad del negocio, objetivos y procedimientos que mejoren la continuidad de operación. La política debe alinearse con las políticas y objetivos estratégicos de la organización.

- **Do:** Implementar y operar la política de continuidad del negocio.

- **Check:** Realizar un monitoreo del correcto funcionamiento de la política de continuidad del negocio. Generar reportes gerenciales para su respectiva revisión y determinar las posibles soluciones de remediación y mejoramiento.

- **Act:** Mantener y mejorar el Sistema de Gestión de Continuidad de Negocios. (BSI Group, 2014)

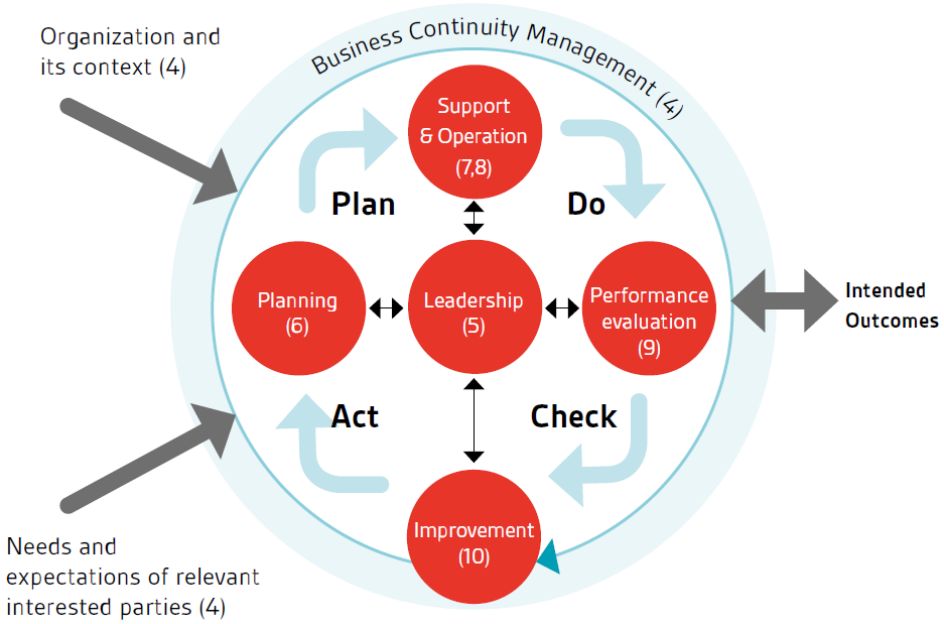

Figura 1. Business Continuity PDCA.
Tomado de BSI Group, 2016

El principio es aplicado a los procesos del Sistema de Gestión de Negocio con el objetivo principal de obtener mayor eficiencia y un mayor empoderamiento de la alta gerencia. (BSI Group, 2016)

2.1.2 Cláusulas claves del ISO/IEC 22301:2012

Contexto de la organización

Es necesario identificar los problemas internos y externos que son de importancia para la empresa. El fin principal es generar un vínculo entre la política de continuidad del negocio con los objetivos estratégicos empresariales, inclusive con la gestión de riesgos. (BSI Group, 2016)

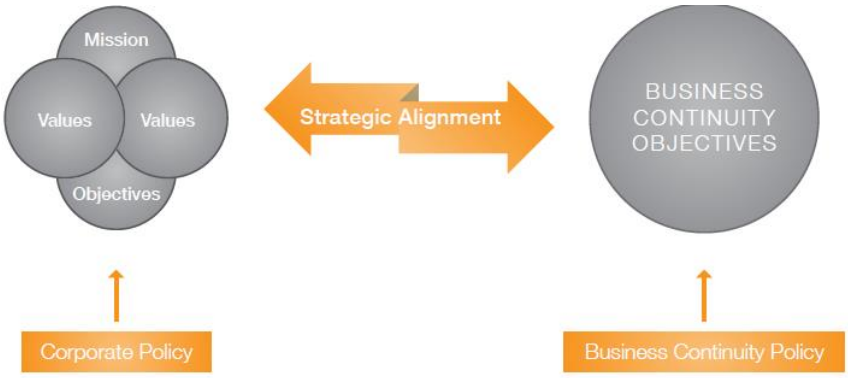

Figura 2. Alineación estratégica ISO 22301.
Tomado de ISO 22301 Societal Security Business Continuity Management Systems, 2012

Liderazgo

La implementación de un sistema de gestión de continuidad de negocio demanda de forma irrevocable el continuo compromiso por parte de la alta gerencia. Mediante este liderazgo y compromiso se asegura disponer personal comprometido e involucrado. Así mismo, la alta gerencia será el principal responsable de alinear el sistema de gestión con los objetivos estratégicos de la empresa, ofrecer una dirección hacia la mejora continua y asignar los diferentes roles, responsabilidades y autoridades en el sistema. (St-Germain René, 2014)

Planificación

La etapa más importante y crítica es la planificación. En esta sección se construyen los objetivos y dirección que tomará el sistema de gestión de continuidad de negocio (BCMS). Los objetivos del BCMS son:

- Identificar los riesgos y cumplir con las necesidades de la organización.
- Considerar el nivel mínimo de productos y servicios para que la organización pueda cumplir con sus objetivos estratégicos.
- Medibles y que puedan ser monitoreados. (St-Germain René, 2014)

Soporte

La gestión diaria de un sistema de gestión de continuidad de negocio se centra básicamente en el uso eficaz de los recursos disponibles de manera correcta. Esto incluye: personal capacitado, competente, servicios de apoyo, la comunicación y sensibilización se la debe gestionar a través de información certera documentada. Finalmente en el punto de la comunicación se debe especificar procedimientos para la comunicación tanto interna como externa, se considerará el contenido y formato. (St-Germain René, 2014)

Operación

St-Germain René en el 2014 menciona que la cláusula de la operación se la ejecuta después de haber definido y planificado el BCMS. Se deberán considerar los siguientes puntos:

Análisis de impacto del negocio (BIA)

El Business Impact Analysis (BIA), permite a la organización mapear los procesos críticos que soportan a sus productos o servicios. De la misma manera, considera los recursos que son necesarios para que dichos procesos puedan operar a un nivel aceptable. (St-Germain René, 2014)

Evaluación de riesgos

El segundo aspecto es la identificación y evaluación de los riesgos. Para la implementación de este requisito la ISO 22301 hace referencia a la norma ISO 31000. El principal objetivo es implementar y documentar un proceso que permita identificar, analizar y evaluar de forma sistemática los diferentes eventos a los cuales las organizaciones se enfrentan y que pueden ser perjudiciales en el caso de que no se logren controlar. (St-Germain René, 2014)

Figura 3. Análisis de riesgos ISO 3100.
Tomado de ISO 22301 Societal Security Business Continuity Management Systems, 2012

Estrategia de continuidad de negocio

En los puntos anteriores se han recabado los requerimientos de la organización a través del BIA. Adicional, se han identificado y evaluado los riesgos a los cuales la empresa deberá enfrentar. Toda esta información permitirá a las organizaciones disponer de un modelo de protección de los procesos críticos para desarrollar estrategias para recuperarse de cualquier evento catastrófico

basadas en la tolerancia del riesgo que la empresa pueda soportar y dentro de los objetivos de tiempo de recuperación. (St-Germain René, 2014)

Procedimientos de continuidad de negocio

Para garantizar la continuidad de negocio la organización debe documentar los procedimientos de las actividades, la gestión de un incidente que haya detenido las operaciones normales de la compañía y, finalmente documentar las acciones correctivas que fueron puestas en acción. Los procedimientos deben cumplir los siguientes aspectos:

- Protocolo de comunicación interno y externo.
- Pasos claros y detallados a seguir durante un incidente.
- Presentar flexibilidad para responder ante situaciones imprevistas.
- Centrarse en los procesos críticos de la organización.
- Establecer las estrategias de mitigación efectivas para minimizar las consecuencias. (St-Germain René, 2014)

Ejercicio y pruebas

Los procesos de ejercicios y pruebas sirven para contrastar que las estrategias establecidas en los procedimientos de continuidad de negocio brindan resultados de respuesta y tiempo de recuperación óptimos de acuerdo a los niveles de aceptación que se haya acordado con la alta gerencia. (BSI Group, 2014)

Las pruebas deberán ejecutarse regularmente, este tiempo se deberá definir con la alta gerencia de acuerdo a las necesidades de la organización. El objetivo principal es garantizar que los procedimientos de BCMS se encuentren alineados con los objetivos estratégicos de la empresa. (BSI Group, 2014)

Evaluación de desempeño

La norma ISO 22301 requiere de un constante monitoreo, las verificaciones periódicas permitirán adquirir madurez en los procesos y mejorar su funcionamiento como un todo. Se deberá evaluar:

- Cumplimiento de la política de continuidad del negocio.
- Alineamiento del BCMS con los objetivos estratégicos. (BSI Group, 2014)

Mejora Continua

Es el proceso en el cual una organización puede mejorar continuamente la efectividad del sistema implementado, indicadores, acciones preventivas y correctivas. El fin último es brindar mayores beneficios de seguridad a la empresa y sus stakeholders a través de una mejora constante de su estrategia de continuidad de negocio. (BSI Group, 2014)

2.2 Gestión de continuidad

2.2.1 Definición del Business Continuity Management

En base al Business Continuity Institute (BCI), a continuación se define a Business Continuity Management (BCM) como “un proceso de gestión integral que identifica las amenazas potenciales de una organización. De la misma manera, proporciona un marco de referencia para creación de fortalezas y capacidad para una respuesta efectiva que proteja los interés de sus principales interesados”. (Greenhill Alison, 2017)

El ciclo de vida de un BCM comprende:

- Comprender la organización.
- Definir la estrategia del BCM.
- Desarrollar e implantar una respuesta del BCM.
- Probar, mantener y revisar. (Greenhill Alison, 2017)

Figura 4. Ciclo de vida del BCM.
Tomado de Business Continuity Management Policy Statement and Strategy, 2018

2.2.2 Importancia del BCM

El Business Continuity Management es de vital importancia para proteger los procesos comerciales de las organizaciones cuando se enfrentan a interrupciones causadas por terceros o de forma natural. El BCM proporciona una sólida continuidad comercial administrando eficientemente el impacto a

través de respuestas proactivas y planificación la recuperación en el menor tiempo operacional posible. (Velker Arthur, 2018)

2.2.3 Business Continuity Planning

La gestión de la continuidad del negocio requiere en primera instancia la clara identificación sobre lo que es un stakeholder. Un stakeholder serán todas las personas que son afectadas directa o indirectamente sea de forma positiva o negativa. En este contexto los, clientes, inversores, empleados, proveedores, y la comunidad serán considerados como stakeholder. (Quevedo Jesús, 2012)

La planificación de la continuidad del negocio es un proceso en donde las organizaciones preocupadas por los activos tangibles e intangibles establecen las capacidades necesarias para proteger dichos activos y reanudar con los procesos críticos una vez que un desastre se haya materializado. (Quevedo Jesús, 2012)

Los aspectos claves para el proceso de planificación son:

- Entender el negocio.
- Evaluar los riesgos.
- Preparar el plan de continuidad de negocio.
- Probar el plan.

2.2.4 Metodología para la Gestión de Continuidad del Negocio

La metodología para la gestión de la continuidad del negocio considera las siguientes etapas:

- Identificar los procesos, productos o servicio, proveedores y grupos de interés.
- Análisis de impacto en el negocio.
- Evaluación de riesgo.
- Estrategia de continuidad del negocio y plan de contingencia.
- Ejecución del plan de continuidad.
- Plan de evaluación y mejora continua. (Ferrer Rodrigo, 2015)

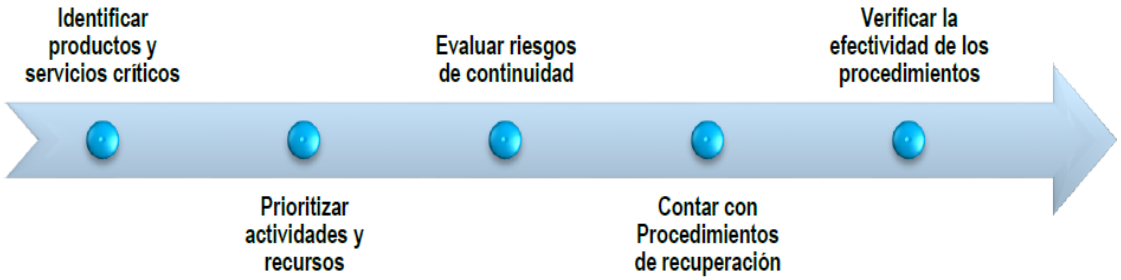

Figura 5. Actividades claves BCM.
Tomado de Metodología para la Gestión de la Continuidad del Negocio, 2015

La ilustración anterior muestra como primer paso identificar los servicios y procesos críticos de la organización. Esta actividad es de suma importancia ya que a través de este levantamiento de información la empresa estará en capacidad de mapear y a su vez proteger sus procesos críticos con la finalidad de garantizar la prestación de sus servicios y entrega de productos. La primera actividad y como eje principal se derivan las siguientes actividades que le permiten a la organización diseñar estrategias eficientes de recuperación. A su vez, le facilita controlar el impacto a consecuencia de que una disrupción se materialice. (Ferrer Rodrigo, 2015)

La planificación de la continuidad empresarial es el proceso a través del cual las organizaciones establecen las capacidades necesarias para proteger sus activos

y continuar con los procesos comerciales clave después de un desastre. El desarrollo de capacidades del BCM requiere lo siguiente: (Ferrer Rodrigo, 2015)

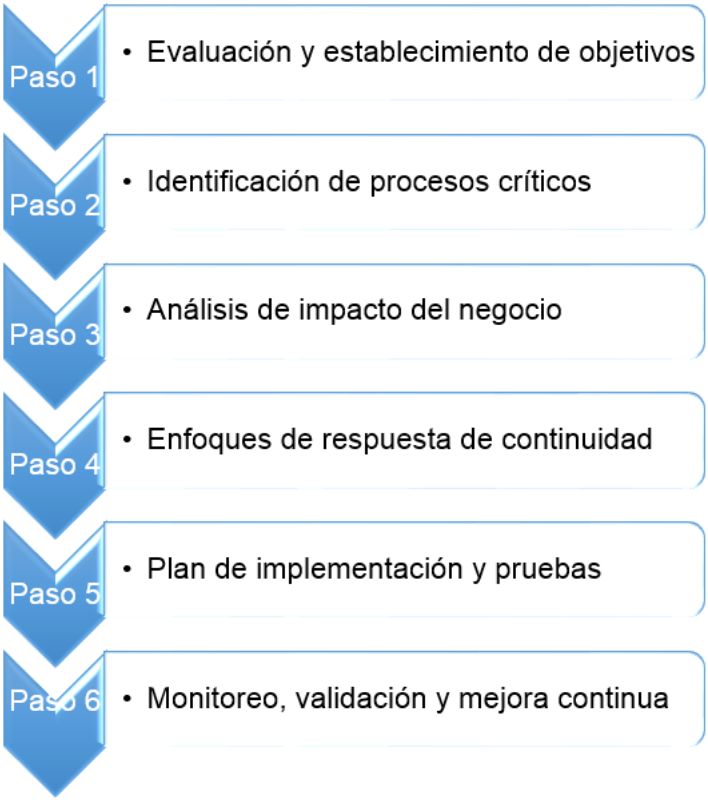

Figura 6. Pasos para desarrollar las capacidades del BCM.
Adaptado de Business Continuity Management – Key Strategies and Processes, 2019

Evaluación y ajuste de objetivos

En la primera fase de la metodología es importante la correcta definición del alcance del proyecto. Para esto es necesario mapear las necesidades y capacidades de negociación de la organización. Adicional, es de vital consideración las partes interesadas que son afectadas de forma positiva o negativa dentro de los procesos empresariales. (Ferrer Rodrigo, 2015)

Identificación de procesos críticos

En este paso es necesario identificar y revisar el plan estratégico de la organización. Una vez verificado, se identifica los procesos comerciales críticos de la empresa, identificar los objetivos estratégicos que son llevados a cabo por aquellos procesos anteriormente identificados, los responsables de dichos procesos y finalmente establecer las medidas y métricas claves con la finalidad de cuantificar o cualificar el rendimiento del éxito del proceso. (CGMA, 2016)

Análisis de impacto del negocio

En la tercera fase se identifica el impacto de los procesos empresariales críticos cuando estos se materializan en un desastre. Es necesario considerar:

- Reputación.
- Relaciones con proveedores.
- Relaciones con clientes.
- Relaciones con inversionistas.
- Recursos humanos.
- Posiciones financieras. (CGMA, 2016)

En el BIA existen dos puntos críticos que deben ser definidos. El primero en donde se debe evaluar el impacto en el tiempo en el que la organización detiene sus actividades de negocio y finalmente especificar los tiempos de recuperación.

El RTO es el tiempo objetivo de recuperación y el RPO es el punto objetivo de recuperación. Éste último determina la máxima información que una

organización está dispuesta a perder desde que ocurre algún evento que pare las operaciones de la empresa. (CGMA, 2016)

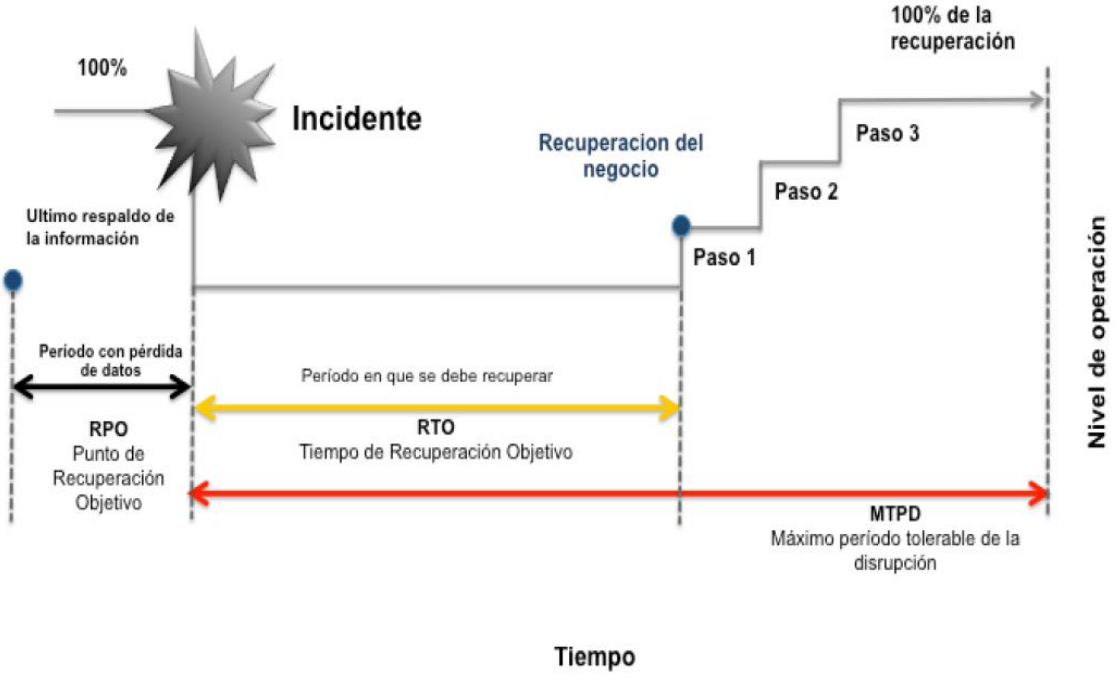

Figura 7. RTO y RPO.
Tomado de Metodología para la Continuidad del Negocio, 2016

Enfoques de respuesta a la continuidad

Las organizaciones pueden reducir de forma proactiva los impactos de un desastre cuando este se materializa. El principal objetivo del BCM es acelerar el retorno de la organización a las operaciones normales con procesos efectivos de administración de crisis. (CGMA, 2016)

En este punto es necesario identificar y mantener un proceso que permita una evaluación sistemática de los riesgos buscando de forma ágil evaluar los riesgos asociados a incidentes disruptivos a los cuales la organización se entrena. (CGMA, 2016)

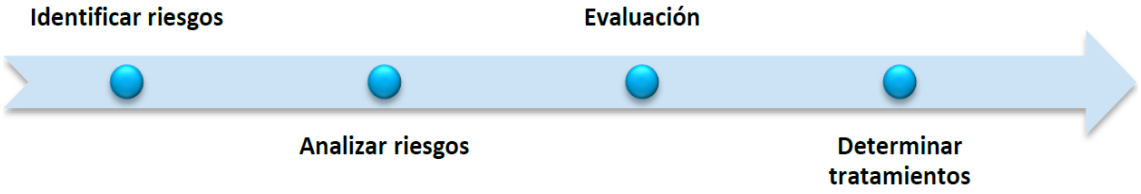

Figura 8. Gestión de riesgos.
Tomado de Metodología para la Continuidad del Negocio, 2015

Así mismo, la estructura de respuesta ante una catástrofe tiene como objetivo principal la toma de decisiones estratégicas que el personal deberá considerar para la recuperación de los procesos críticos de la institución. (Ferrer Rodrigo, 2015)

Entre funciones más importantes se tiene:

- Tomar la decisión de activar o no el plan de continuidad.
- Comunicar a los empleados y stakeholder.
- Definir un presupuesto para gastos que genere la crisis.
- Tomar decisiones ante situaciones no planificadas

Plan de ejecución y pruebas

La sexta fase considera realizar un plan de pruebas para la ejecución del BCM en tiempo real. Esta simulación servirá para determinar si el personal seleccionado para cumplir las tareas asignadas está correctamente capacitadas y son competentes para dichas actividades. Adicional, en el plan de pruebas se podrá identificar las brechas, inconsistencias y áreas problemáticas antes un desastre natural. (CGMA, 2016)

Monitoreo, validación y mejora

Se debe establecer un procedimiento para evaluar la efectividad del BCM. En base a los resultados obtenidos mediante el plan de ejecución y pruebas, se realizarán las correcciones y mejores respectivas a los procedimientos y estrategias planteadas en las fases iniciales. La organización deberá mejorar continuamente la eficacia de su plan de contingencia que soporten sus objetivos estratégicos. (Ferrer Rodrigo, 2015)

2.3 Gestión de servicios

2.3.1 ITIL®v3

De sus siglas en inglés Information Technology Infrastructure Library (ITIL®v3) es un conjunto de publicaciones que recoge las mejores prácticas para la correcta administración de los servicios de TI. ITIL proporciona guías para la gestión de seguridad de información, perspectiva del negocio, gestión de niveles de servicio, gestión de activos y gestión de aplicaciones que ayudan a las empresas a crear estrategias básicas para la gestión del servicio de TI. (Universidad Tec de Monterrey, 2012)

Los siguientes son los cuatro principios que ITIL propone como pilares fundamentales:

- **Procesos:** Gestión de servicios de TI rompiendo los silos empresariales.
- **Calidad:** Se basa en procesos con mejoramiento continuo.
- **Cliente:** Beneficiario directo de la mejora de los procesos o servicios.
- **Independencia:** Disponer de buenas prácticas independiente de métodos y proveedores.

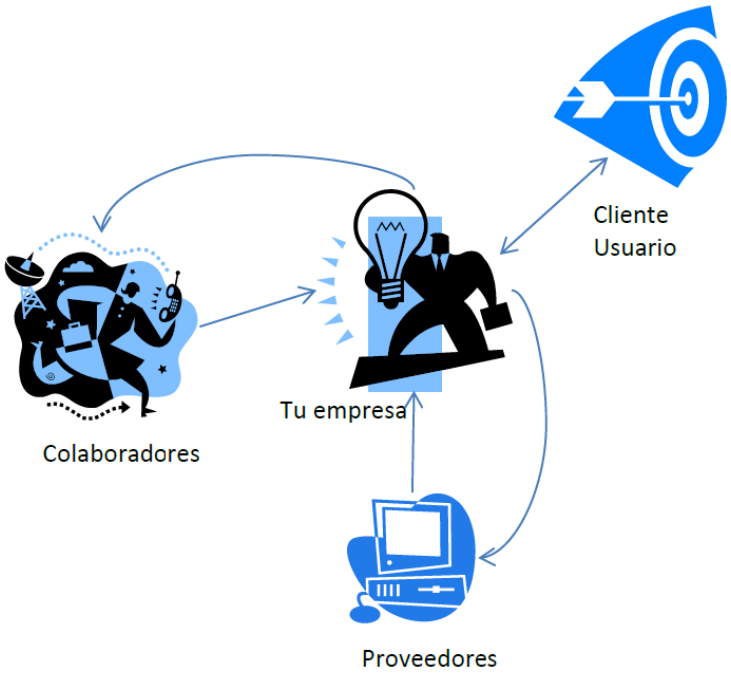

Figura 9. Generación de valor ITIL.
Tomado de Manual ITIL v3, 2015

El principal objetivo de ITIL es proporcionar una orientación de buenas prácticas para la correcta gestión de los servicios de TI. Esto se logra a través de la integración de TI con los objetivos estratégicos de la empresa, para ello es necesario crear un marco para la gestión de:

- Personal.
- Procesos transversales.
- Tecnología / Productos.
- Relaciones socio – proveedores.

Finalmente, ITIL permite facilidad en la gestión de la calidad de los servicios de información, mejorar la eficiencia, reduce los riesgos y aumenta la rentabilidad de la organización. (Hollman Ellis, 2013)

2.3.2 Ciclo de vida del servicio de ITIL®v3

La última versión ITIL v3, tuvo su salida en el año 2007 donde se tuvo la necesidad de agrupar conjuntos estructurados de procesos íntimamente relaciones. A través de este proceso se asociaron los principales elemento de TI en 5 volúmenes los cuales son:

- ITIL v3 Estrategia de Servicio.
- ITIL v3 Diseño de Servicio.
- ITIL v3 Operación de Servicio.
- ITIL v3 Mejoramiento Continuo de Servicio.
- ITIL v3 Transición del servicio. (Ríos Sergio, 2015)

Los cinco libros conforman el ciclo de vida de ITIL.

Figura 10. Ciclo de vida ITIL.
Tomado de Manual ITIL v3, 2015

Estrategia de Servicios

En la fase de estrategia de servicio se planifican las acciones que permitirán a la organización desarrollar una estrategia para los servicios de tecnología de información alineadas con una estrategia organizacional. (Ríos Sergio, 2015)

La estrategia de servicio consta de:

- Gestión estratégica para los servicios de TI.
- Gestión del portafolio de servicios.
- Gestión financiera de los servicios de TI.
- Gestión de demanda.
- Gestión de relaciones del negocio.

Figura 11. Procesos de la estrategia del servicio.
Tomado de El mapa General de ITIL v.3 – Conceptos clave, s.f

Diseño del servicio

El propósito principal es diseñar servicios que apalanquen a los objetivos estratégicos empresariales mediante un correcto diseño de arquitecturas, procesos, políticas y documentación. Se enfoca en la gestión del niveles de servicio con la finalidad de garantizar la calidad de entrega del servicio, disponer de una estrategia de costos y buscar la satisfacción cliente – proveedor. (Universidad Tec de Monterrey, 2012)

El servicio de diseño consta de:

- Coordinación del diseño.
- Gestión de los niveles de servicio.
- Gestión del catálogo de servicio.
- Gestión de la disponibilidad.
- Gestión de seguridad de la información.
- Gestión de proveedores.
- Gestión de la capacidad de servicios.
- Gestión de la continuidad de los servicios de TI.

Transición del servicio

En este punto se definen los cambios que se producirán a los servicios del diario vivir de las empresas. Facilita una guía para implementar y desarrollar capacidades para la transición de servicios asegurando que los servicios sean estos nuevos, modificados o retirados cumplan con los las necesidades y objetivos de la empresa. (Universidad Tec de Monterrey, 2012)

Al desarrollar estas capacidades es factible para las organizaciones aumentar la confianza en relación a la entrega de servicio sin que otros sean afectados. A su vez, asegura que los nuevos servicios o modificaciones sean más rentables y con facilidad de mantenimiento a través del tiempo. (Universidad Tec de Monterrey, 2012)

El servicio de transición consta de:

- Gestión del cambio.
- Gestión de configuración y activos de servicio.
- Gestión de versiones y despliegue.
- Planificación y soporte de la transición.
- Gestión del conocimiento.
- Validación y pruebas del servicio.
- Gestión de liberación e implementación

Figura 12. Procesos de transición del servicio.
Tomado de El mapa General de ITIL v.3 – Conceptos clave, s.f

Operación del servicio

El propósito es definir y aplicar procedimientos para gestión de entrega del servicio de TI. Para esto se define un nivel de servicio de la organización que van de la mano con los requisitos y necesidades de los clientes. Estos niveles de servicio son conocidos como acuerdos de niveles de servicio o de sus siglas en inglés Service Level Agreement (SLA). (Ríos Sergio, 2015)

El objetivo del servicio de operación es asegurar la entrega de los servicio de TI dentro de los plazos y calidad definidos previamente por el cliente. Con el cumplimiento de esto se logra una mayor confianza por parte de TI y satisfacción del cliente por la recepción de servicio. Finalmente, minimiza el impacto que tiene el negocio debido a las interrupciones dentro de sus actividades diarias. (Universidad Tec de Monterrey, 2012)

El servicio de operación consta de:

- Gestión de eventos.
- Gestión de incidentes.
- Gestión de peticiones.
- Gestión de problemas.
- Gestión de accesos.

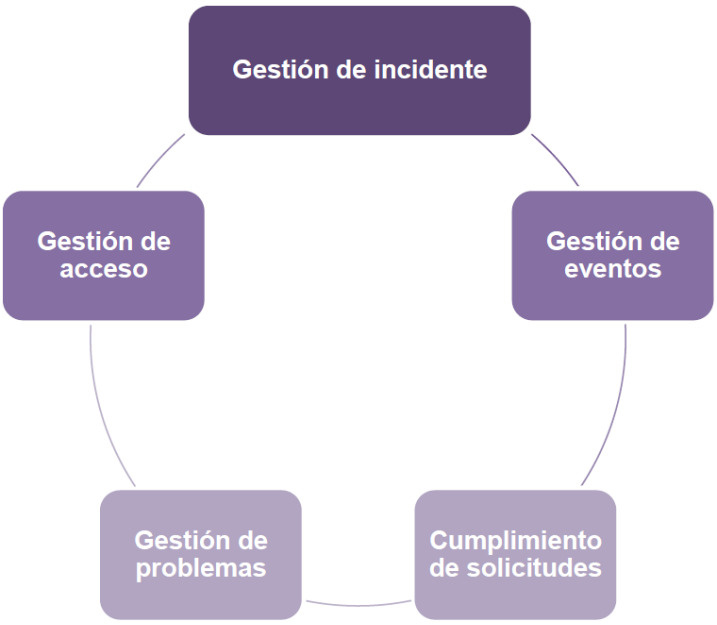

Figura 13. Procesos de operación del servicio.
Tomado de El mapa General de ITIL v.3 – Conceptos clave, s.f

Mejora continua del servicio

El proceso de mejora continua del servicio tiene como propósito medir el desempeño del proveedor de servicios TI. Además, es el responsable de identificar y realizar mejoras a los procesos, infraestructura y servicios de TI. (Universidad Tec de Monterrey, 2012)

La siguiente ilustración muestra los 7 pasos de la mejora continua en la cual se centra el proceso de mejora continua del servicio.

Figura 14. Mejora continua.
Adaptado de Conceptos básicos para la certificación en ITIL®v3, 2019

- **Definir lo que se debería medir.-** En la fase de estrategia se deben definir claramente las métricas a evaluar.
- **Definir lo que se puede medir.-** Determinar nuevos requisitos de nivel de servicio.
- **Recopilar datos.-** En el proceso de servicio de operación se recopilan los datos de acuerdo a los objetivos planteados.
- **Procesar los datos.-** Se procesan los datos de acuerdo los niveles de servicio pres establecidos.
- **Analizar los datos.-** La da se convierte en información.
- **Presentación y uso de la información.-** Las mejoras se presentan los interesados del negocio.

- **Acciones correctivas.-** Son utilizadas para mejorar y optimizar los servicios de TI.

2.3.3 Gestión de Continuidad del Servicio de TI

De sus siglas en inglés, IT Service Continuity Management (ITSCM) es un proceso que integra políticas y procesos que facilitan a las organizaciones actuar de forma eficiente antes una disrupción que cause interrupciones en sus procesos comerciales. El ITSCM es una parte del ciclo de vida de servicios de ITIL v3 cuyo objetivo principal es que las empresas puedan gestionar eficientemente el riesgo, aseguren sus procesos críticos y que puedan perdurar en tiempo después de un incidente considerable. (Rivas Génesis, 2018)

El ITSCM es responsable de:

- Gestión de riesgos.
- Definición de responsabilidades.
- Enfoque de TI.
- Selección de opciones en función de las necesidades de la empresa.

Plan de continuidad del negocio

Es una planificación que se centra principalmente en los procesos del negocio en lugar de la infraestructura de TI. Alinea procesos con servicios de TI. (Hollman Ellis, 2013)

Tiempo objetivo de recuperación

Es el tiempo en el que una empresa puede soportar sus procesos de negocio sin el apoyo de TI antes de que sus finanzas o su imagen puedan verse afectados de forma negativa. (Hollman Ellis, 2013)

Punto objetivo de recuperación

Es la cantidad de datos que una empresa se puede permitir perder ante una situación de crisis en los procesos de negocio. (Hollman Ellis, 2013)

Salida máxima tolerable

Es la cantidad de tiempo máxima que la empresa puede sobrevivir sin el proceso empresarial sea este de forma manual o utilizando servicios de TI. (Hollman Ellis, 2013)

2.3.4 Ciclo de vida del ITSCM

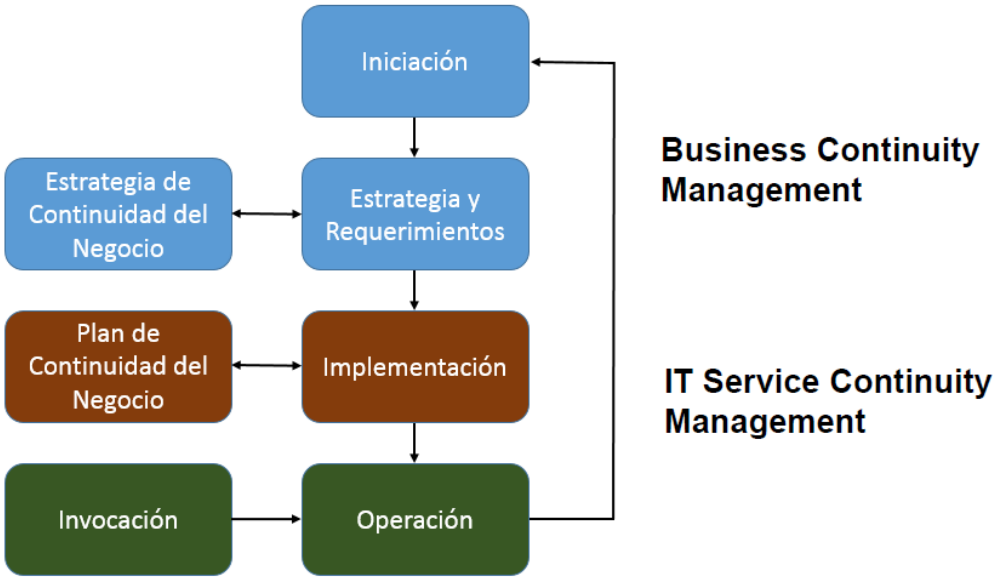

Figura 15. Ciclo de vida ITSCM.
Adaptado de ITSCM (IT Service Continuity Management) Overview: ITIL®'s IT Disaster Recovery and Business Continuity Management, 2019

Iniciación

En esta fase se configura la política y alcance. Se establece el BIA, controles, asignación de recursos. Finalmente se define la estructura de gestión de proyectos para dar inicio a la implementación dando un enfoque organizacional. (Hollman Ellis, 2013)

Estrategia y requerimientos

En la fase de estrategia y requerimientos se realizar un análisis de impacto de negocio, se determina y prioriza los procesos críticos del negocio. Esta priorización se logra definiendo el RTO y RPO. (Hollman Ellis, 2013)

Implementación

Una vez definida y aprobada la estrategia por la alta gerencia, se da paso al establecimiento de los planes del ITSCM en donde se asegura que la recuperación de los servicios de TI se encuentre definidos a detalle y completamente documentados. (Hollman Ellis, 2013)

El contenido de un plan de TI consta de:

- Planificación preliminar
    - Propósito.
    - Alcance.
    - Asunciones.
    - Responsabilidades.
    - Eventos Críticos.

    - Estrategias.

- Acciones preparatorias
    - Personas.
    - Datos.
    - Software / Hardware.
    - Documentación.
    - Suministros.

- Plan de acción
    - Respuesta.
    - Recuperación.
    - Restauración.

Operaciones en marcha

En la fase final se realizan los siguientes aspectos:

- Educación y formación.
- Conocer las implicaciones de ITSCM.
- Revisión periódica de los procesos comerciales de la organización.
- Gestión del cambio. (Hollman Ellis, 2013)

2.4 Gobierno de TI

En la actualidad la tecnología abarca más presencia en las organizaciones tanto públicas como privadas. El paradigma que se refiere a las tecnologías como un gasto innecesario por la carencia de valor para las empresas, debe finalizar. Es necesario comprender el empoderamiento que hoy en día tiene la tecnología sobre los procesos de negocio de forma transversal y alineada con los objetivos estratégicos empresariales. Esto se logra en primera instancia con un eficaz gobierno de TI.

El gobierno corporativo de la tecnología de la información, es aplicable a organizaciones de todos los tamaños, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro. Esta norma proporciona un marco para la gobernanza efectiva de TI para ayudar a aquellos en el más alto nivel de organizaciones a comprender y cumplir sus obligaciones legales, reglamentarias y éticas con respecto al uso de TI de sus organizaciones. (ISO / IEC 38500, 2008)

La norma ISO/IEC 38500:2008 Corporate governance of information technology (ISO/IEC, 2008) define el gobierno de las TI como “el sistema por el que se dirige y controla la utilización actual y futura de la tecnología de la información”.

El gobierno de las TI se centra en el uso de la tecnología para satisfacer los objetivos de la organización fijados por la dirección. Por ello, el gobierno corporativo incluye aspectos del gobierno de las TI, ya que, sin una gestión eficaz de las TI, los encargados de las responsabilidades corporativas no podrían desempeñarse de forma efectiva. (Hamidovic Haris, 2011)

2.4.1 Marcos de control

Hoy en día y con el avance exponencial de las tecnologías existen diferentes metodologías orientadas al control de las organizaciones, cada una con un nivel de detalle de comprensión en distintos ámbitos.

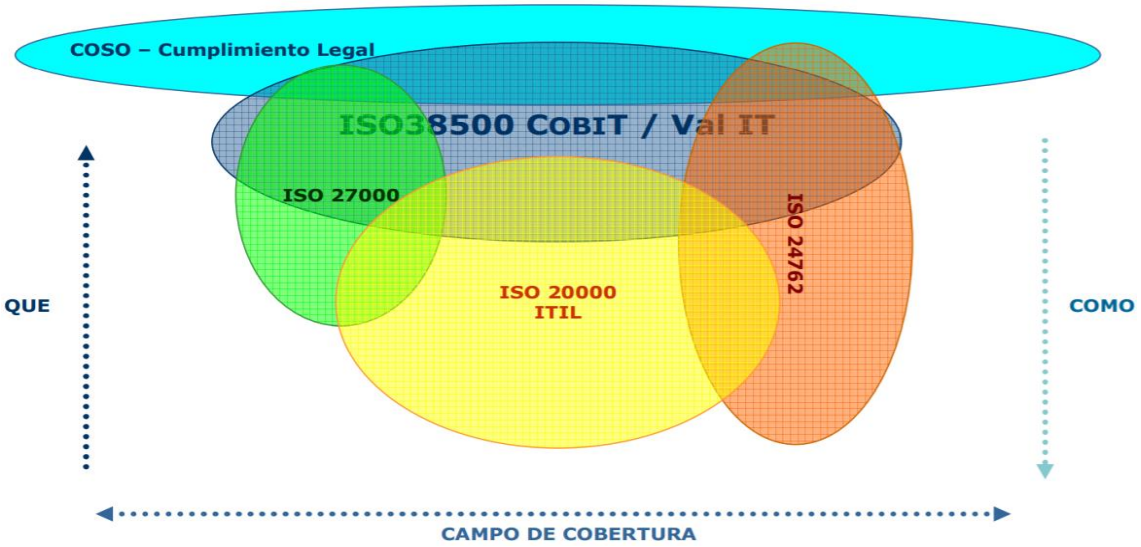

Figura 16. Marcos de control.
Tomado de ISO 38500, s.f

2.4.2 COBIT 5

Para el desarrollo de la tesis, se llevará a cabo un análisis del marco de referencia COBIT en su última versión. COBIT significa “Control Objectives for Information and Related Technology” y es un conjunto de mejores prácticas para el manejo de información. Fue creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992.

El IT Governance Institute (ITGI) establece, que fundamentalmente el Gobierno de TI se encarga de:

1. Entregar valor de TI al negocio y,

2. Mitigar los riesgos de TI

Las empresas existen para crear valor para sus partes interesadas. En consecuencia, cualquier empresa—comercial o no — tendrá la creación de valor como objetivo de gobierno. La creación de valor significa obtener beneficios a un coste óptimo de recursos mientras se optimiza el riesgo. (COBIT® 5: Procesos Catalizadores, 2012)

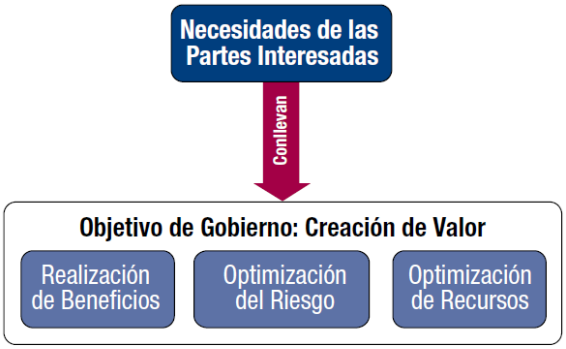

Figura 17. Objetivo de gobierno: Creación de Valor.
Tomado de COBIT® 5 – ISACA, 2012

Los principios y habilitadores de COBIT 5 son genéricos, los cuales permiten a cualquier tipo de empresa sea esta pública o privada implementar un marco tanto para el gobierno así como también para la gestión. Su principal objetivo es hallar una convergencia entre la estrategia de TI y la estrategia empresarial. Los principios son:

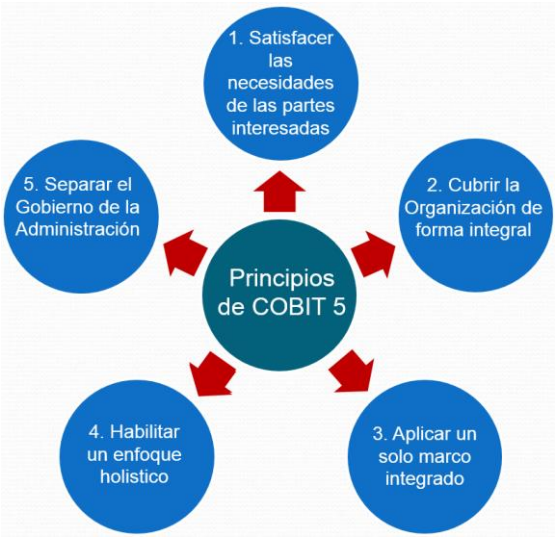

Figura 18. Principios de COBIT 5.
Tomado de COBIT® 5 – ISACA, 2012

COBIT 5 incluye un modelo de referencia de procesos que define a detalle procesos de gobierno y de gestión. Esto proporciona un marco para medir y supervisar el desempeño de TI, comunicar con proveedores de servicios e integrar las mejores prácticas de gestión. (COBIT® 5: Procesos Catalizadores, 2012)

La siguiente figura expone un conjunto de 37 procesos de gobierno y gestión dentro de COBIT 5.

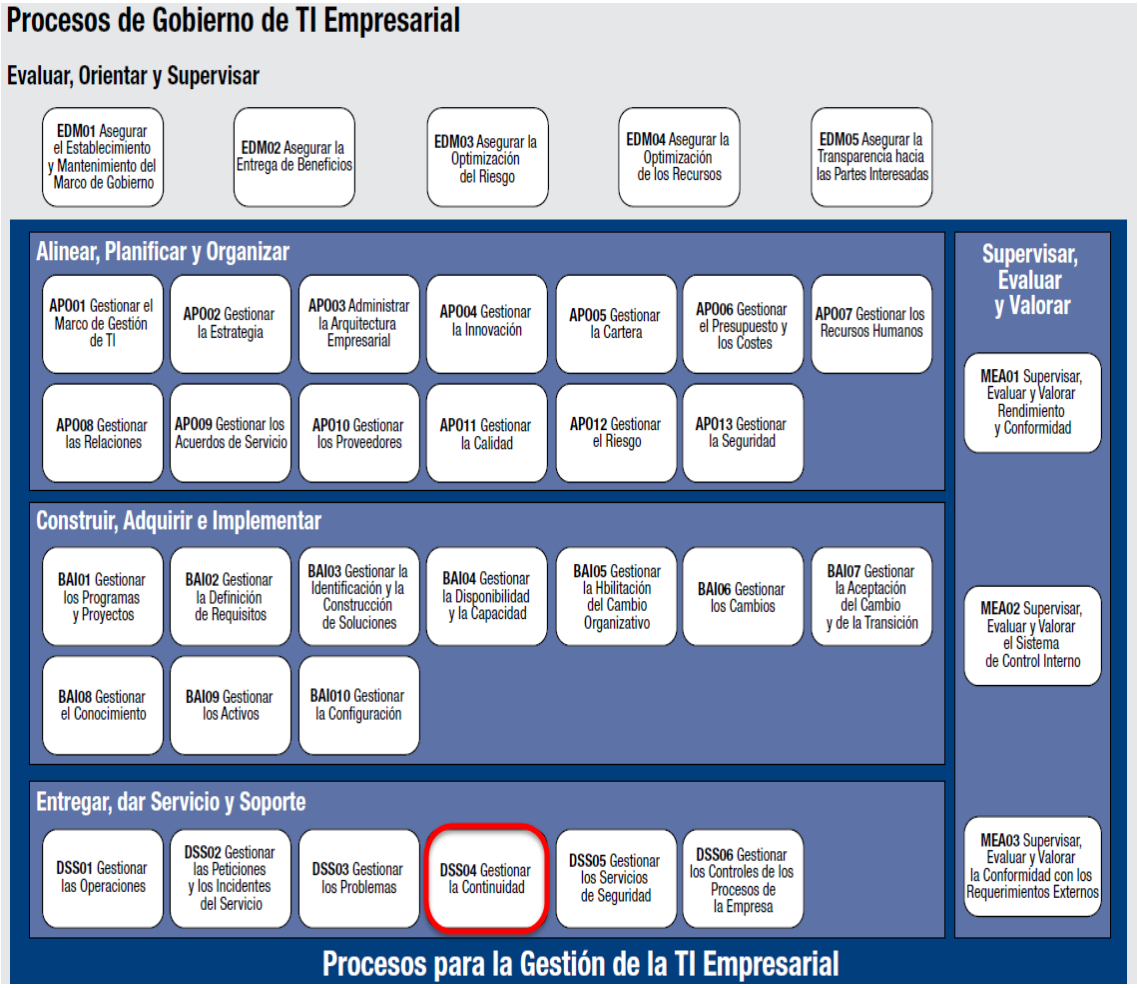

Figura 19. Procesos de Gobierno de TI Empresarial.
Tomado de COBIT® 5 – ISACA, 2012

2.4.3 Proceso DSS04, Gestionar la Continuidad

Para el desarrollo de la tesis se ha considerado el proceso DSS04, Gestionar la Continuidad, se encuentra en el área de Gestión dentro del dominio Entrega, Servicio y Soporte (DSS). Este proceso permite establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa. (COBIT® 5: Procesos Catalizadores, 2012)

COBIT 5 indica que el proceso para gestionar la continuidad apoya directamente la obtención tanto de métricas de TI, así como también alcanzar objetivos y métricas del proceso. Entre las metas de TI dispone:

- Riesgos de negocio relacionados con las TI gestionados.
- Entrega de servicios TI de acuerdo a los requisitos del negocio.
- Disponibilidad de información útil y relevante para la toma de decisiones.

Finalmente, los objetivos del proceso que apoya son:

- La información crítica para el negocio está disponible para el negocio en línea con los niveles de servicio mínimos requeridos.
- Los servicios críticos tienen suficiente resiliencia.
- Las pruebas de continuidad del servicio han verificado la efectividad del plan.
- Un plan de continuidad actualizado refleja los requisitos de negocio actuales.

- Las partes interesadas internas y externas han sido formadas en el plan de continuidad.

El proceso DSS04 se encuentra divido en ocho prácticas clave de gobierno que a continuación se detalla:

- **DSS04.01:** Definir la política de continuidad del negocio, objetivos y alcance.
- **DSS04.02:** Mantener una estrategia de continuidad.
- **DSS04.03:** Desarrollar e implementar una respuesta a la continuidad del negocio.
- **DSS04.04:** Ejercitar, probar y revisar el plan de continuidad.
- **DSS04.05:** Revisar, mantener y mejorar el plan de continuidad.
- **DSS04.06:** Proporcionar formación en el plan de continuidad.
- **DSS04.07:** Gestionar acuerdos de respaldo.
- **DSS04.08:** Ejecutar revisiones post-reanudación.

Es importante definir los roles y niveles de responsabilidad para cada una de las prácticas clave de gobierno. En este contexto, se presenta la matriz RACI en donde subproceso puede recaer sobre un rol empresarial sea este de TI o de cualquier unidad del negocio. (COBIT® 5: Procesos Catalizadores, 2012)

Los niveles de responsabilidad son los siguientes:

- **R:** Es la persona responsable de ejecutar las diferentes actividades y tareas.

- **A:** Es la persona que rinde cuentas a la alta dirección del éxito o fracaso de las actividades y tareas.

- **C:** Es la persona que es consultado para la ejecución de actividades y tareas.

- **I:** Es la persona que recibe la información (entregables).

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.				A	C	R					C					C	C	R			R	C	R		R	
DSS04.02 Mantener una estrategia de continuidad.				A	C	R					I					C	C	R	R	C	R				R	
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.					I	R									I	C	C	R	C	C	R				A	
DSS04.04 Ejercitar, probar y revisar el plan de continuidad.					I	R									I		R	R		C	R				A	
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.				A	I	R					I							R		C	R				R	
DSS04.06 Proporcionar formación en el plan de continuidad.					I	R												R		R	R	R			A	
DSS04.07 Gestionar acuerdos derespaldo.																				C	A				R	
DSS04.08 Ejecutar revisiones post-reanudación.					C	R					I							R	C	C	R	R			A	

Figura 20. Matriz RACI.
Tomado de COBIT® 5 – ISACA, 2012

2.5 Cloud Computing

Actualmente las preocupaciones de los CIOs han aumentado en los últimos años por el volumen del ecosistema de aplicaciones y por los datos generados. Una de las tecnologías que actúa a favor del desarrollo del negocio, es la computación en la nube. (Becerra José, 2018)

En la publicación especial de NIST 800-145 menciona: “La computación en la nube es modelo para permitir acceso a la red ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y lanzar rápidamente con un esfuerzo de administración mínimo o interacción de proveedor de servicios.” (Simmon Eric, 2018)

2.5.1 Características del Cloud Computing

De acuerdo a la evaluación de servicios de computación en la nube basados en el NIST SP 800-145, esta tecnología dispone las siguientes características definidas a continuación.

Autoservicio bajo demanda

Esta característica permite al consumidor proporcionar capacidades al centro de cómputo de manera unilateral. Según sea necesario facilita, incrementar o disminuir capacidades informáticas sin necesidad de una interacción humano con cada proveedor de servicio. En principal beneficio es el acceso según necesite a las capacidades informáticas. (Simmon Eric, 2018)

Acceso a la red amplia

Mediante un acceso amplio a la red, las capacidades se encuentran disponibles en cualquier momento. Los servicios se pueden consumir a través de cualquier cliente sea este: teléfonos móviles, tabletas, computadoras portátiles y estaciones de trabajo. El beneficio que ofrece esta característica es que se puede acceder desde cualquier lugar y en cualquier momento a los recursos informáticos desde cualquier dispositivo dentro de las restricciones de seguridad y políticas de la red. (Simmon Eric, 2018)

Agrupación de recursos

Los recursos informáticos del proveedor son agrupados utilizando un modelo de múltiples inquilinos para servir a múltiples consumidores. Dichos recursos sean estos físicos o virtuales, son asignados y reasignados dinámicamente de acuerdo con la demanda del consumidor. (Simmon Eric, 2018)

El modelo de múltiples inquilinos genera un sentido de independencia en el sentido de que el cliente no tiene control ni conocimiento sobre la ubicación exacta de los recursos proporcionados. Entre los recursos incluyen: almacenamiento, procesamiento, memoria y ancho de banda de red. El objetivo principal es la reducción de costos al momento de compartir recursos. (Simmon Eric, 2018)

Elasticidad rápida

Las capacidades pueden ser aprovisionadas y liberadas elásticamente, en algunos casos de forma automática. Es decir, para el consumidor las capacidades disponibles para el aprovisionamiento a menudo suelen ser ilimitadas. Así mismo, éstas pueden asignarse o reasignarse en cualquier cantidad y cualquier momento. El principal beneficio que ofrece es la habilidad para aumentar y reducir la capacidad informática, y los costos de forma dinámica de acuerdo a las necesidades del consumidor. (Simmon Eric, 2018)

Servicio medido

Los sistemas en la nube controlan y optimizan automáticamente el uso de los recursos en red. Esta funcionalidad se consigue al aprovechar la capacidad de medición en algún nivel de abstracción apropiado para el tipo de servicio. Las mediciones automáticas se pueden ejecutar por ejemplo: al almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas. (Simmon Eric, 2018)

El uso de recursos puede ser monitoreado, controlado e informado, proporcionando transparencia tanto para el proveedor como para el consumidor del servicio utilizado. (Simmon Eric, 2018)

2.5.2 Modelos de servicios en la nube

Existen varios modelos y estrategias de implementación en la nube. Conforme avanzan las tendencias tecnológicas e incrementa la popularidad del cloud computing, es importante considerar y diferenciar cada modelo con el objetivo de determinar los niveles de control, flexibilidad y administración conforme las necesidades del consumidor. (Amazon Web Services Inc., 2018)

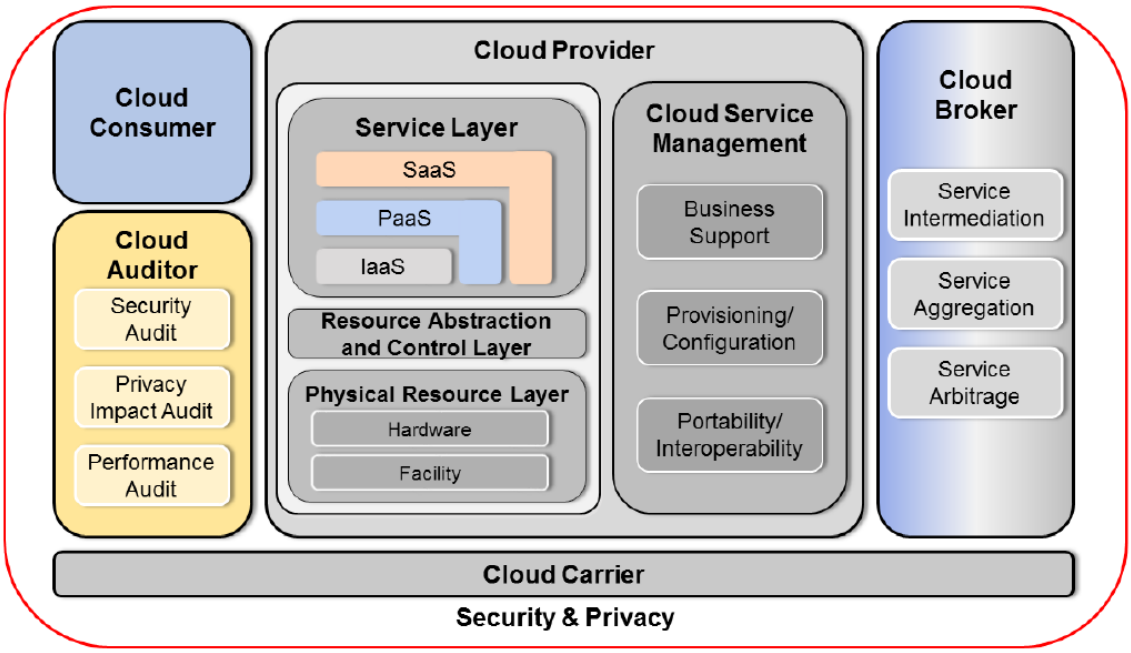

Figura 21. Arquitectura de Cloud Computing.
Tomado de NIST SP 800-145, s.f

La anterior ilustración muestra una referencia de la arquitectura de la computación en la nube. La capa de servicios muestra los tres modelos principales de cloud computing como son: Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS) y Software como servicio (SaaS).

Infraestructura como servicio (IaaS)

De las siglas Infraestructure as a Service (IaaS), proporciona la capacidad de administración y control del aprovisionamiento en referencia al procesamiento, almacenamiento, redes y otros recursos que incluyen sistemas operativos y aplicaciones. (Simmon Eric, 2018)

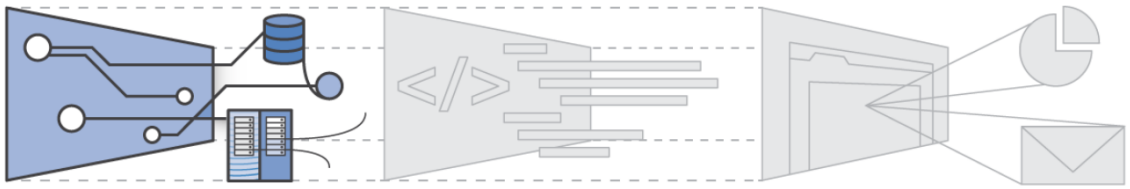

Figura 22. Infraestructura como servicio (IaaS).
Tomado de Amazon Web Services Inc., 2018

Plataforma como servicio (PaaS)

De las siglas Platform as a Service (PaaS), elimina la necesidad de administrar la infraestructura subyacente. Esto contribuye a incrementar la eficacia al despreocuparse del aprovisionamiento de recursos, planificación de la capacidad y mantenimiento de software. (Amazon Web Services Inc., 2018)

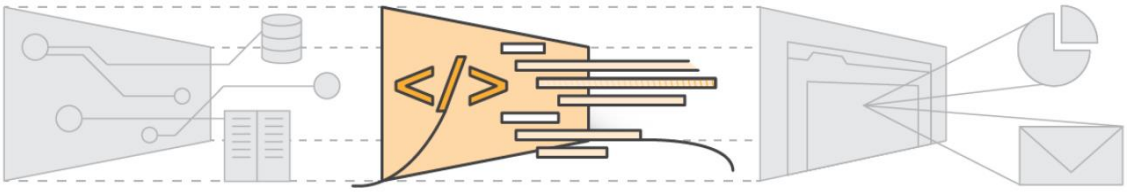

Figura 23. Plataforma como servicio (IaaS).
Tomado de Amazon Web Services Inc., 2018

Software como servicio (SaaS)

De las siglas Software as a Service (SaaS), permite utilizar aplicaciones que se ejecutan en una infraestructura en la nube. El acceso a este tipo de aplicaciones se puede realizar desde varios dispositivos cliente mediante una interfaz ligera

como por ejemplo un navegador web. En este modelo el consumidor solo se preocupa por utilizar el software en específico y el proveedor en proporciona un producto completo que lo ejecuta y administra. (Simmon Eric, 2018)

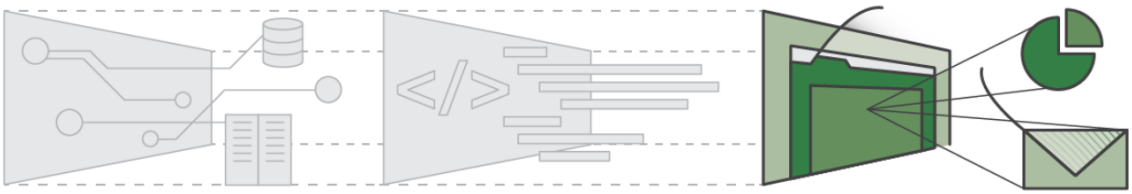

Figura 24. Software como servicio (SaaS).
Tomado de Amazon Web Services Inc., 2018

2.5.3 Recuperación de desastres como servicios (DRaaS)

Como medida de seguridad a considerar, la recuperación de desastres como servicio (DRaaS) es un componente que forma parte de un Plan de Recuperación de Desastres (DRP). SU objetivo principal implica el mantenimiento de datos empresariales almacenados de manera estratégica en la nube. (Colom José, 2015)

Plan de recuperación de desastres (DRP)

De las siglas Disaster Recovery Plan (DRP), es una planificación que realizan las organizaciones con la finalidad de prepararse ante posibles desastres, sean estos naturales o no naturales. El objetivo principal es identificar los componentes informáticas (hardware y software) para definir estrategias y las actividades que se deben seguir para restablecer los servicios de TI en el menor tiempo posible. (Casillas Mireya, 2018)

De acuerdo a un análisis estadístico realizado en agosto del 2018, las empresas pymes muestran un alto índice de que sus operaciones cierren sus negocios para siempre por no contar con un plan de recuperación de desastres. El estudio demuestra un porcentaje entre el 40% y 60% de pequeñas empresas que

pierden disponibilidad hacia sus sistemas de información y de almacenamiento. (Casillas Mireya, 2018)

Normalmente las empresas que cuentan con un DRP, muestran índices demasiado alentadores lo que hace que su tiempo de recuperación sea corto a costos muy bajos. (Allen Chris, 2018)

Parámetros

En este contexto, las empresas disponer un plan sólido que haya sido probado y que pueda ser aplicado sin problema alguno. Existen dos parámetros se suma importancia en el plan de recuperación de desastres. En primero es el Objetivo del Punto de Recuperación (RPO) y finalmente, el Objetivo del Tiempo de Recuperación (RTO). (Puricica Cristian, 2018)

Objetivo del Punto de Recuperación (RPO)

El RPO describe el momento en el que toda la información de la empresa debe ser restaurada para reanudar sus respectivas actividades en total plenitud. Un concepto más amigable, es considerado el tiempo entre la última copia de seguridad y el momento en que la organización tuvo cualquier evento que detuvo sus operaciones normales. (Colom José, 2015)

Objetivo del Tiempo de Recuperación (RTO)

El RTO es el tiempo en el cual un conjunto de procesos empresariales deben ser restituidos después de que un evento catastrófico ha ocurrido. (Puricica Cristian, 2018)

Ambos conceptos parecen similares, pero en su contexto ofrecen una utilidad y propósito totalmente diferentes. El objetivo de todo plan de recuperación de

desastres es conseguir que tanto el punto de recuperación como el tiempo de recuperación sean cercanos a cero como sea posible. Sin embargo, desde el punto de vista financiero el costo por conseguir estos parámetros en cero son excesivamente costosos. (Puricica Cristian, 2018)

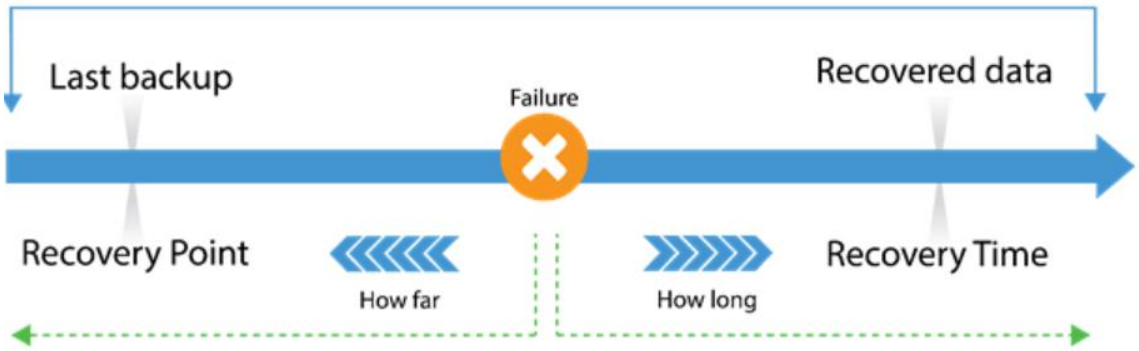

Figura 25. RPO y RTO.
Tomado de Veeam, 2018

3. PROCESOS, SERVICIO Y COMPONENTES

En este apartado se describe la situación actual de la Zona de Distribución del Aeropuerto Mariscal Sucre. Se identifica los procesos principales de la empresa así como también los servicios e infraestructura tecnológica que son base de la efectiva operación de los procesos de negocio.

3.1 Información de la organización

La Zona de Distribución nace en el año 2013 bajo la necesidad de contar con un área en donde se puedan desarrollar actividades de comercio exterior de forma segura dentro del Aeropuerto Mariscar Sucre en Quito. Para efectivizar esta iniciativa, Quiport decide concesionar el manejo de carga que llega al Ecuador a un tercero. Después de obtener un préstamo con un fondo inversión en EE.UU, el mismo advierte la importancia de este proyecto para el desarrollo económico del país y decide apoyar.

En un lapso de dos años, la inversión realizada se completó y aquí nace la Zona de distribución del Aeropuerto Mariscal Sucre. En la actualidad, el fondo de inversión Darby es el dueño del 100% de la Zona de Distribución convirtiéndose en el mejor Centro Logístico de Latinoamérica en la actualidad.

3.1.1 Misión

Proporcionar servicios aeroportuarios y logísticos de carga que faciliten todas las actividades de comercio exterior, con el recurso humano comprometido, infraestructura y tecnología de punta, basados en procesos seguros para lograr soluciones globales.

3.1.2 Visión

En Alcanzar un fortalecimiento corporativo a través de la especialización de nuestros procesos que permanecen en un lapso de dos años la integración de la cadena logística y así atender las necesidades del cliente final.

3.1.3 Valores corporativos

Los valores fundamentales de la organización son los siguientes:

- **Compromiso:** Es la perseverancia para cumplir con lo encomendado pese a las limitaciones y los obstáculos del día a día.

- **Servicio Colaborativo:** Buscar satisfacer a los stakeholders siendo empáticos a sus necesidades, ofreciendo disponibilidad de inmediata y brindar ayuda en todo momento en busca de un mismo fin.
- **Transparencia:** Ser sinceros, asumir las consecuencias de cada una de las acciones. Evitar las mentiras sin doble discurso y actuar en todo momento con honestidad y ética.

- **Seguridad:** Mostrar seguridad en cada acción, seguir los procesos establecidos con certeza y confianza de las habilidades personales para ejecutar las acciones encomendadas por la empresa.

- **Creatividad:** Mostrar proactividad para anticiparse a los hechos, innovar y buscar soluciones en busca de la mejora continua.

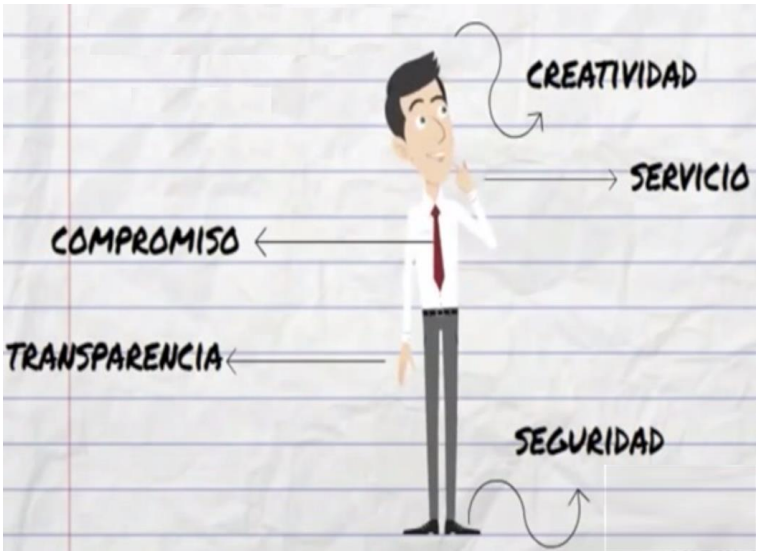

Figura 26. Valores organizacionales.

3.1.4 Propuesta de valor

Servir sin límites.

3.1.5 Estructura organizacional

La compañía dispone si estructura organizacional basada en procesos. La misma pone énfasis en la búsqueda continua hacia la excelencia y mejora continua.

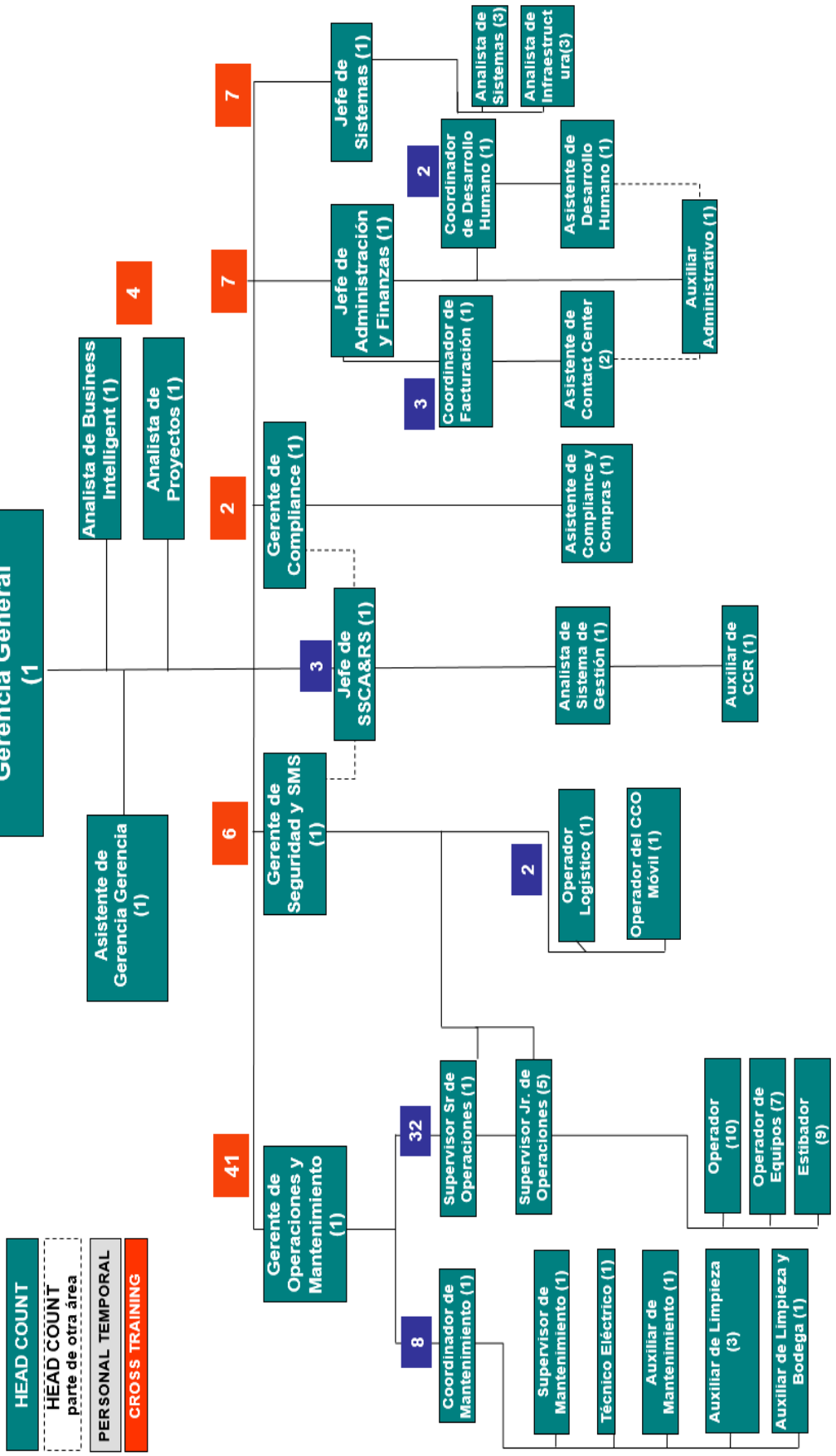

Figura 27. Estructura organizacional.

3.2 Proceso de logística aeroportuario

La cadena de valor de la organización se centra específicamente en el cumplimiento de las necesidades de sus stakeholders. Para ello, sus procesos macro inician desde las necesidades y requerimientos de las partes interesadas.

En la estrategia, la empresa cuenta con un sistema integrado de gestión donde abarcan las siguientes certificaciones:

- ISO
- ISAGO
- BASC
- SSO
- Calidad
- Ambiente

Lo anteriormente descrito se basa en una política empresarial fuertemente estructurada, una planeación estratégica alineada con el cumplimiento normativo legal que permita una evaluación del desempeño efectiva.

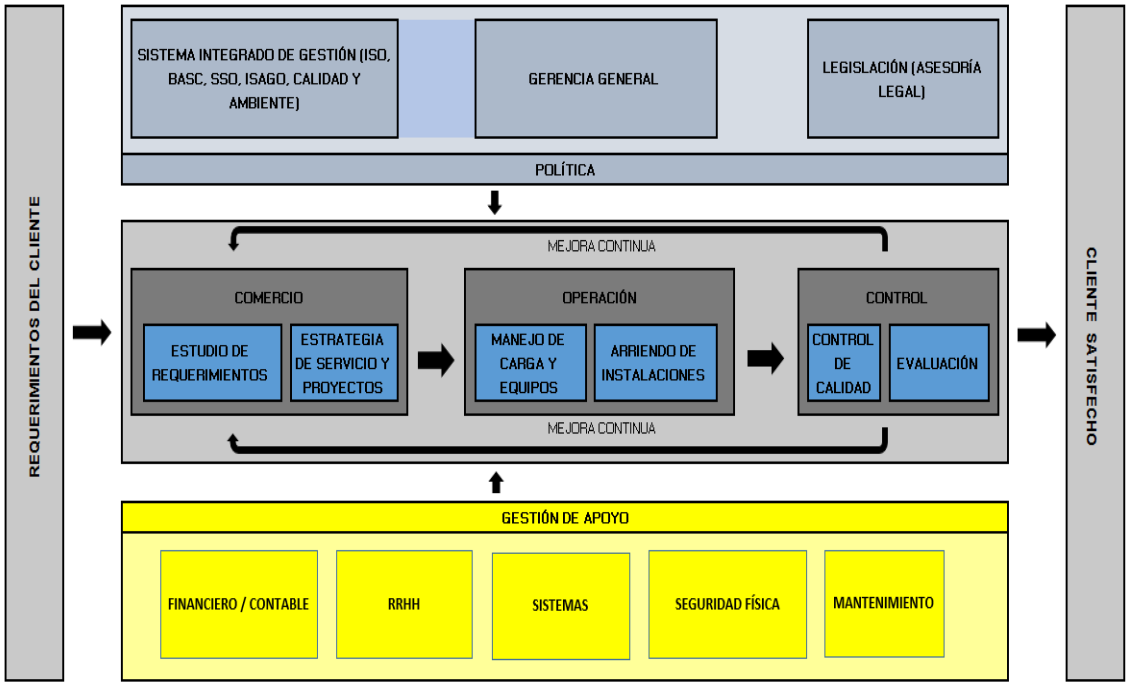

Figura 28. Mapa de procesos Zona de Distribución.

La matriz de proceso de la zona de distribución inicia desde los requerimientos de los stakeholders. Los procesos estratégicos se encuentran claramente establecidos bajo la política organizacional.

Entre los procesos que agregan valor a la organización constan el comercio, la operación y el control de calidad. El proceso en el que se centrará el desarrollo de este estudio será el proceso operativo de la empresa el cual es considerado por la alta dirección el de mayor impacto dentro del giro del negocio.

Los procesos establecidos en la Zona de Distribución del Aeropuerto Mariscal Sucre disponen un enfoque de servicio al cliente que descienden desde la ideología de la alta gerencia. Así mismo, consideran un pilar importante en sus procesos la mejora y el aprendizaje continuo con el objetivo principal de servir sin límites a todos sus stakeholders.

Para finalizar, la empresa ha identificado los procesos que soportan su giro de negocio. Mediante su correcta gestión, los siguientes procesos apoyan de manera transversal a todos los procesos clave. Los procesos de soporte son:

- Financiero / Contable.
- Desarrollo Humano.
- Seguridad Física.
- Mantenimiento.
- Seguridad.

Mediante una correcta orquestación, armonía de los procesos y con personal plenamente comprometido con la visión de la organización; el producto final que ofrece la Zona de Distribución es una satisfacción de todos los stakeholders

partiendo desde los accionistas, clientes hasta conseguir un bienestar común de todos sus empleados.

3.3 Proceso de Operaciones

Uno de los procesos agregadores de valor en la Zona de Distribución es el proceso de Operaciones.

A continuación se presenta el detalle del proceso de operaciones.

Tabla 1.
Mapa de procesos de operaciones

Macro proceso:	Operaciones
Proceso:	Operaciones
Responsable de proceso:	Gerencia de Operaciones
Participantes:	Personal de planta
Objetivo estratégico:	**Sostenibilidad financiera:** Lograr un desempeño financiero que satisfaga las expectativas de los accionistas.
	Salud integral de los trabajadores: Lograr un lugar de trabajo saludable y motivador basado en valores y principios de conducta claramente definidos.
	Operaciones seguras y eficientes: Operar con seguridad cumpliendo con las normas, regulaciones y procedimientos vinculados a la naturaleza del negocio. Mantener un enfoque de mejoramiento continuo y respetuoso con el medio ambiente.
	Servicio Colaborativo: Satisfacer las expectativas de los stakeholders

Objetivo del proceso:	Gestionar las operaciones de carga de importaciones.

3.3.1 Mapa de Proceso de Operaciones

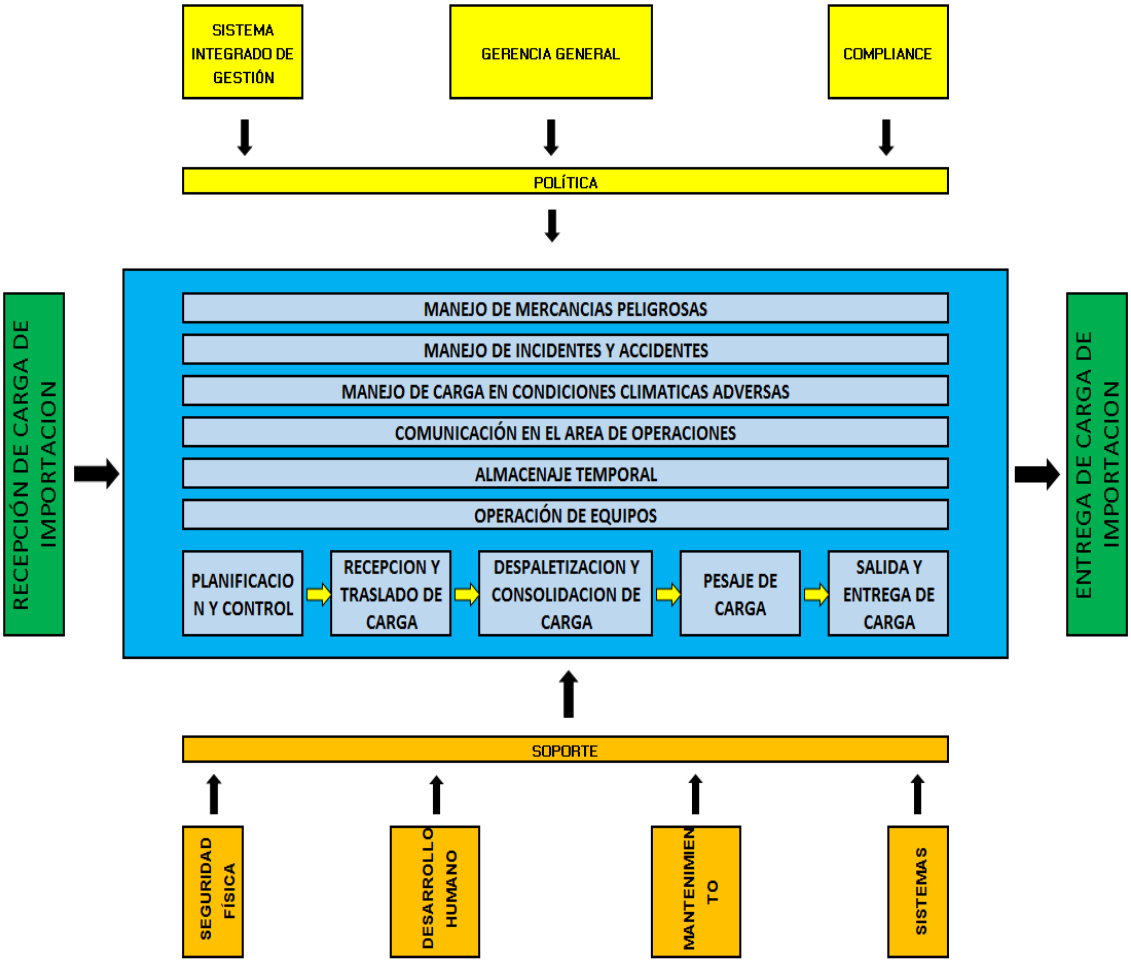

Figura 29. Mapa de procesos de Operaciones.

Planificación y Control

El proceso de planificación y control responde a una de las actividades más importantes en el proceso de operaciones. En este proceso se organizan los vuelos que arribarán al Ecuador sean estos cargueros o pasajeros de acuerdo a un itinerario y convenios pre establecidos con las diferentes líneas aéreas.

Mediante el análisis de esta información se planifica tanto personal como los equipos motorizados que se utilizarán en la operación para atender en los tiempos establecidos en los acuerdos con cliente (SLA).

Recepción y traslado de carga

La recepción de las mercancías se realiza en el Aeropuerto Internacional Mariscal Sucre. La Zona de Distribución dispone un lugar específico en donde recibe toda la carga para su traslado hacia las instalaciones de bodegaje de tránsito.

Para realizar un efectivo proceso de recepción y traslado de la carga que arriba al país, la empresa dispone de una vía exclusiva en el interior del aeropuerto para evitar posibles contaminaciones de la mercancía. El proceso de traslado lo realizan en equipos propios de la empresa que cuentan con un sistema de video vigilancia móvil para brindar trazabilidad a las mercancías.

Despaletización y consolidación de carga

Una vez las mercancías se encuentren en la zona de distribución, se procede con el proceso de despaletizaje de la carga. En este punto los operadores de carga proceden a desarmar los pallets de avión para continuar al proceso de consolidación de carga.

El proceso de consolidación de carga consiste en preparar pallets de madera que contengan el mismo número de guía master si es carga directa o consolidar las mercancías por el mismo número de guía hija en el caso de pertenecer a una carga consolidada.

Pesaje de carga

En el proceso de pesaje de carga, la empresa cuenta con un sistema propio denominado Datapass.

El objetivo de este aplicativo es brindar facilidades y automatizar el proceso de pesaje de carga con el objetivo principal de brindar transparencia y eficiencia a al desarrollo del comercio exterior en el proceso de importaciones del país.

En el detalle del proceso de pesaje de carga, el usuario registra el número de manifiesto, el número de guía de master y el número de guía hija para iniciar con el registro de información al sistema. En esta instancia, el sistema automáticamente registra el pesaje de la carga, el usuario registra la cantidad de paquetes recibidos y las novedades con la que dicha mercadería llegó al país.

Después de un proceso de transmisión automático de documentos electrónicos de la carga que está arribando al país hacia el sistema del Servicio Nacional de Aduanas del Ecuador (SENAE), se espera autorización por parte del Senae para entregar la carga a las distintas bodegas para el proceso de nacionalización y entrega hacia el importador.

Salida y entrega de carga

Una vez se dispone la autorización del Servicio Nacional de Aduanas, la zona de distribución procede con el despacho de las mercaderías a las diferentes bodegas con las que previamente el importador decidió importarla hacia el Ecuador.

Este proceso es también automatizado por el mismo sistema desarrollado internamente por la zona de distribución. De la misma manera, dispone de un proceso interno automático para el envío de documentos electrónicos hacia el sistema del Senae para su respectivo despacho.

3.3.2 Mapa de riesgos del Proceso de Operaciones

Basado en el levantamiento de los procesos del departamento de operaciones y del giro de negocio de la Zona de Distribución, se han levantado los principales riesgos que amenazan con la correcta ejecución de dichos procesos y por ende con la continuidad del negocio.

La probabilidad se califica con el siguiente rango:

- Extremadamente probable (1).
- Improbable (2).
- Remoto (3).
- Ocasional (4).
- Frecuente (5)

Así mismo la consecuencia se cualifica de la siguiente manera:

- Catastrófico (A).
- Peligroso (B).
- Mayor (C).
- Menor (D).
- Insignificante (E)

A continuación se detalla el levantamiento de riesgos del proceso de operaciones:

Tabla 2.
Mapa de riesgos de operaciones

CONTROL DE SALIDA NO CONFORME (ANÁLISIS DE FACTORES DE RIESGO DE SALIDA NO CONFORME)					
AMENAZAS	**Controles existentes**	**Probabilidad**	**Consecuencia**	**Nivel de riesgo**	**Acción**
No existe suficiente personal	Existe Planificación de horarios de trabajo de acuerdo a la demanda	3 Remoto	C Mayor	Riesgo Tolerable	No aplica
Suspensión del aplicativo Datapass	Existe un Programa de Mantenimiento IT	4 Ocasional	B Peligroso		**Plan de contingencia:** Proceso manual, uso de sistema Servicio Nacional de Aduana.
La maquinaria está fuera de funcionamiento	Existe un Plan Anual de Mantenimiento	4 Ocasional	B Peligroso		**Plan de contingencia** equipos de backup
Condiciones climáticas adversas		3 Remoto	B Peligroso	Riesgo Tolerable	

No existe personal a cargo de la planificación de las operaciones diarias	Responsabilidad asignada al Gerente de Operaciones en la Descripción de Cargos.	3 Remoto	C Mayor	Riesgo Tolerable	No aplica
El personal cuenta con el suficiente conocimiento para el desempeño de sus actividades	Existe un Programa de Capacitación normado y un procedimiento de inducción.	3 Remoto	C Mayor	Riesgo Tolerable	No aplica
Suspensión de vías internas del aeropuerto por operativos varios.	E-mail de notificación del Concesionario	3 Remoto	C Mayor	Riesgo Tolerable	No aplica
Accidentes en la vía	Existe un Programa de Capacitación normado y un procedimiento de inducción.	3 Remoto	C Mayor	Riesgo Tolerable	No aplica

EVALUACION DEL RIESGO DEL PROCESO

CONSECUENCIA

PROBABILIDAD de ocurrencia	A Catastrófico	B Peligroso	C Mayor	D Menor	E Insignificante
5 Frecuente	5A	5B	5C	5D	5E
4 Ocasional	4A	4B	4C	4D	4E
3 Remoto	3A	3B	3C	3D	3E
2 Improbable	2A	2B	2C	2D	2E
1 Extremadamente improbable	1A	1B	1C	1D	1E

FRECUENCIA		GRAVEDAD	
Frecuente	La situación que afecta la salida del proceso es probable que ocurra muchas veces.	Catastrófico	El proceso se DETIENE, NO hay salidas que ponen en RIESGO EL NEGOCIO. Imagen de la compañía comprometida. Seguridad en riesgo. REQUIERE PLAN DE ACCION
Ocasional	La situación que afecta la salida del proceso es probable que ocurra algunas veces.	Peligroso	El proceso se DETIENE, NO hay salidas pero NO SE AFECTA EL NEGOCIO. Márgenes de seguridad se reducen. REQUIERE PLAN DE ACCION
Remoto	La situación que afecta la salida del proceso es IMPROBABLE, pero posible que ocurra.	Mayor	El proceso PUEDE CONTINUAR pero hay AFECTACIONES SIGNIFICATIVAS a las salidas del proceso. Márgenes de seguridad se reducen. REQUIERE ACCIONES DE MEJORA.
Improbable	La situación que afecta la salida del proceso es MUY IMPROBABLE que ocurra algunas veces.	Menor	El proceso PUEDE CONTINUAR porque las salidas del proceso tienen AFECTACIONES MENORES. Puede causar daños superficiales.
Ocasional	La situación que afecta la salida es INCONCEBIBLE que ocurra.	Insignificante	El proceso PUEDE CONTINUAR y las afectaciones a las salidas del proceso son IMPERCEPTIBLES.

Criterios sugeridos	Índice de evaluación del riesgo	Criterios sugeridos
Región no tolerable	5A, 5B, 5C, 4A, 4B, 3A	Inaceptable bajo las circunstancias existentes
Región tolerable	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Aceptable en base a mitigación del riesgo.Puede requerir una decisión de la dirección.
Región aceptable	3E, 2D, 2E, 1A, 1B ,1C, 1D, 1E	Aceptable

Requiere plan de acción o de contingencia.

No requiere plan de acción. Comprobación periódica en auditoría.

No requiere acción específica

Figura 30. Evaluación de riesgos del proceso de Operaciones.

La matriz de riesgos del proceso de operaciones muestra una gran preocupación en referencia al sistema que automatiza este proceso y declara toda la mercadería de que arriba al país. Si bien es cierto, cuentan con el sistema del Servicio de Aduana del Ecuador. La empresa pierde varias funcionalidades automáticas que presta su aplicativo.

De acuerdo al análisis realizado, el riesgo de que el sistema tenga alguna falencia ha sido cuantificado bajo una probabilidad ocasional (4) y cualificado con una consecuencia (B) peligrosa en relación a los objetivos y giro del negocio de la organización.

3.4 Servicios tecnológicos

A continuación se ha realizado un levantamiento de los servicios tecnológicos que cuenta la organización.

Tabla 3.
Servicio tecnológico sistema Datapass

SISTEMA DATAPASS	
IDE:	Backend: Python 2.7, Frontend: Django 1.5
Base de datos:	Postgres
Alojamiento:	Ubuntu 14.0
Arquitectura:	Web
Objetivo:	Sistema para manejo del proceso de operaciones

Tabla 4.
Servicio tecnológico sistema Latinium

SISTEMA LATINIUM	
IDE:	Visual Studio
Base de datos:	Microsoft SQL 2016
Alojamiento:	Windows Server 2016
Arquitectura:	Web
Objetivo:	Sistema Financiero - Contable

Tabla 5.
Servicio tecnológico sistema PMI

SISTEMA PMI	
IDE:	Visual Studio
Base de datos:	Microsoft SQL 2016
Alojamiento:	Windows Server 2016
Arquitectura:	Web
Objetivo:	Programa de Mantenimiento Integral y Compras

Tabla 6.
Servicio tecnológico sistema Parqueadero

SISTEMA PARQUEADERO	
IDE:	Visual Studio
Base de datos:	Microsoft SQL 2016
Alojamiento:	Windows Server 2016
Arquitectura:	Web
Objetivo:	SQL 2016

Tabla 7.
Servicio tecnológico sistema Compras y Presupuesto

SISTEMA COMPRAS Y PRESUPUESTO	
IDE:	Visual Studio
Base de datos:	Microsoft SQL 2016
Alojamiento:	Windows Server 2016
Arquitectura:	Web
Objetivo:	Programa para la gestión de Compras y presupuesto

Tabla 8.
Servicio tecnológico sistema Reloj Biométrico

SISTEMA RELOJ BIOMÉTRICO	
IDE:	Visual Studio
Base de datos:	Microsoft SQL 2016
Alojamiento:	Windows Server 2016
Arquitectura:	Cliente - Servidor
Objetivo:	Sistema para manejo de ingreso y salida de personal

Tabla 9.
Servicio tecnológico sistema Sitrad

SISTEMA SITRAD	
IDE:	Visual Studio
Base de datos:	Microsoft SQL 2016
Alojamiento:	Windows Server 2016
Arquitectura:	Cliente - Servidor
Objetivo:	Sistema para evaluar datos de temperatura en cuartos fríos

Tabla 10.
Servicio tecnológico sistema PME

SISTEMA PME	
IDE:	Visual Studio
Base de datos:	Microsoft SQL 2016
Alojamiento:	Windows Server 2016
Arquitectura:	Web
Objetivo:	Sistema para evaluar consumo de energía en el Centro Logístico

Tabla 11.
Servicio tecnológico sistema Control de Accesos

SISTEMA CONTROL DE ACCESOS	
Aplicativo:	Winpak 4.0
Base de datos:	Microsoft SQL 2016
Alojamiento:	Windows Server 2016
Arquitectura:	Web
Marca:	Honeywell
Objetivo:	Sistema para administrar las puertas del Centro Logístico

Tabla 12.
Servicio tecnológico sistema Incendios

SISTEMA DETECCIÓN TEMPRANA DE INCENDIOS	
Marca:	Edwards
Objetivo:	Sistema para detección temprana de incendios

3.5 Infraestructura física

La zona de distribución para soportar los diferentes servicios que proporciona a sus stakeholders cuenta con la siguiente infraestructura física.

Tabla 13.
Infraestructura física sistema Datapass

SISTEMA DATAPASS	
Servidor:	APLICACIONES005
Marca:	HP
Modelo:	ProLiant-ML350e-Gen8
Procesador:	Intel Xeon E5-2407
Memoria:	32GB

Tabla 14.
Infraestructura física sistema Latinium7

SISTEMA LATINIUM	
Servidor:	APLICACIONES001
Marca:	DELL
Modelo:	PowerEdge R530
Procesador:	Intel Xeon E5-2620
Memoria:	32GB

Tabla 15.
Infraestructura física sistema PMI

SISTEMA PMI	
Servidor:	APLICACIONES003
Marca:	HP
Modelo:	ProLiant ML310e Gen8 v2
Procesador:	Intel Xeon E3-1240
Memoria:	16GB

Tabla 16.
Infraestructura física sistema Parqueadero

SISTEMA PARQUEADERO	
Servidor:	APLICACIONES001
Marca:	DELL
Modelo:	PowerEdge R530
Procesador:	Intel Xeon E5-2620
Memoria:	32GB

Tabla 17.
Infraestructura física sistema Compras y Presupuesto

SISTEMA COMPRAS Y PRESUPUESTO	
Servidor:	APLICACIONES003
Marca:	HP
Modelo:	ProLiant ML310e Gen8 v2
Procesador:	Intel Xeon E3-1240
Memoria:	16GB

Tabla 18.
Infraestructura física sistema Reloj Biométrico

SISTEMA RELOJ BIOMÉTRICO	
Servidor:	APLICACIONES001
Marca:	DELL
Modelo:	PowerEdge R530
Procesador:	Intel Xeon E5-2620
Memoria:	32GB

Tabla 19.
Infraestructura física sistema Sitrad

SISTEMA SITRAD	
Servidor:	APLICACIONES002
Marca:	DELL
Modelo:	PowerEdge R530
Procesador:	Intel Xeon E5-2620
Memoria:	32GB

Tabla 20.
Infraestructura física sistema PME

SISTEMA PME	
Servidor:	APLICACIONES002
Marca:	DELL
Modelo:	PowerEdge R530
Procesador:	Intel Xeon E5-2620
Memoria:	32GB

Tabla 21.
Infraestructura física sistema Control de Accesos

SISTEMA CONTROL DE ACCESOS	
Servidor:	APLICACIONES004
Marca:	DELL
Modelo:	PowerEdge R440
Procesador:	Intel Xeon Bronze 3106
Memoria:	32GB

Tabla 22.
Infraestructura física sistema Incendios

SISTEMA DETECCIÓN TEMPRANA DE INCENDIOS	
Servidor:	APLICACIONES004
Marca:	DELL
Modelo:	PowerEdge R440
Procesador:	Intel Xeon Bronze 3106
Memoria:	32GB

Finalmente, la organización cuenta como proveedor de servicio de internet a la empresa Telefónica. Dispone de 20 megas de ancho de banda, distribuido estratégicamente de acuerdo al consumo y al servicio que ofrece a todos sus clientes. Un dato importante es que en el aeropuerto Mariscal Sucre el proveedor de última milla para los servicio de internet es la Corporación Nacional de Telecomunicaciones. Es decir, para que el ISP de la Zona de Distribución llegue con su servicio a sus instalaciones, el mismo deberá utilizar una arquitectura mixta entre su infraestructura y la infraestructura de CNT.

3.6 Base de datos de la gestión de la configuración

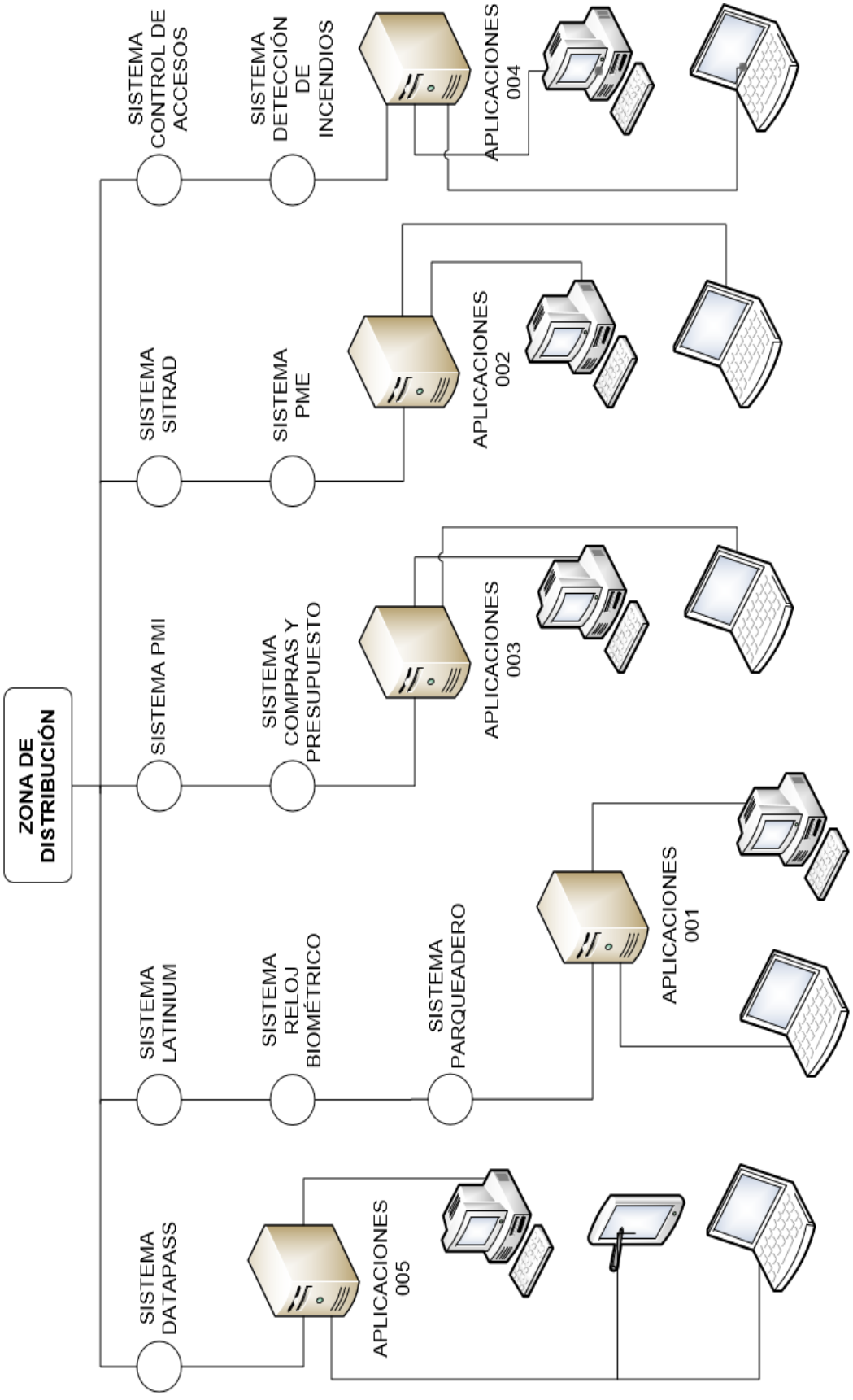

Figura 31. Base de datos de gestión de la configuración.

El presente documento se centrará en realizar un plan de continuidad de negocio que soporte al proceso operativo de la Zona de Distribución del Aeropuerto Mariscal Sucre. En este contexto, y de acuerdo al análisis realizado en la organización; este estudio se enfocará únicamente a los servicios tecnológicos que apalanquen a las operaciones de la empresa.

Figura 32. CMDB operaciones.

4. IMPACTOS Y RIESGOS COMO SERVICIOS

En este capítulo se realiza el análisis del impacto del negocio (BIA), en donde se identifican las amenazas sobre los activos y procesos, así mismo se determina el impacto de cada una de las amenazas que dispone la empresa.

Finalmente, se realiza una evaluación de riesgos teniendo como entregable un mapa de riesgos que permite identificar y priorizar aquellos procesos o activos que pueden ocasionar daños considerables cuando este sea materialice en el tiempo.

4.1 Identificación de impactos del negocio

Como se había señalado en capítulos anteriores, este estudio se centra en la recuperación de los servicios que soportan al proceso core del negocio de la Zona de Distribución del Aeropuerto Mariscal Sucre. La empresa dispone como proceso central teniendo un porcentaje del 75% en referencia a los ingresos netos de la organización al proceso operativo.

En este contexto, se ha realizado una entrevista directa con el dueño del proceso utilizando una herramienta para el levantamiento de los impactos del negocio (BIA). El método utilizado consiste en definir claramente las actividades, procesos y procedimientos con el objetivo de identificar los impactos que se pueden considerar críticos para la organización y que afectan con el giro del negocio. A continuación el formato utilizado:

Tabla 23.

Análisis de Impacto (BIA)

ANÁLISIS DE IMPACTO DE NEGOCIO - CUESTIONARIO	
ORGANIZACIÓN:	
ÁREA / DEPARTAMENTO DE NEGOCIO:	
NOMBRE DEL DIRECTOR DEL ÁREA / DEPARTAMENTO:	
DESCRIPCIÓN DEL OBJETIVO DEL ÁREA / DEPARTAMENTO:	
NOMBRE DE LA PERSONA ENTREVISTADA:	**CARGO:**

LISTA DE PROCESOS DEL ÁREA / DEPARTAMENTO

Nº	**PROCESO**
1	
2	
3	
4	
5	
6	

ÁREA/DEPARTAMENTO DE NEGOCIO:	**PROCESO DE NEGOCIO Nº:**		
DESCRIPCIÓN:			
PERSONA ENTREVISTADA:	**CARGO:**		
SISTEMA QUE LO SOPORTA	**ADMINISTRADOR DEL SISTEMA:**		
ACTIVIDADES	**PRIORIDAD DE RECUPERACIÓN**		
	ALTA	**MEDIA**	**BAJA**
DESCRIPCIÓN DEL SISTEMA: **(Incluir arquitectura, diagramas de sistemas, etc)**			
		RECURSO	

1. IDENTIFICAR PUNTOS DE CONTACTO FUNDAMENTALES DEL SISTEMA	**ROL CRÍTICO**	
INTERNOS: (Identificar personas o departamentos de la organización que dependen o apoyan al sistema)		
EXTERNOS: (Identificar personas o departamentos fuera de la organización)		
2. IDENTIFICAR EL TIEMPO DE RECUPERACIÓN OBJETIVO: (Identificar el período máximo aceptable de indisponibilidad del recurso)		
RECURSO	**TIEMPO ADMISIBLE DE INTERRUPCIÓN**	
3. IDENTIFICAR EL PUNTO DE RECUPERACIÓN OBJETIVO: (Punto de recuperación de la información requerida para continuar con el proceso después de la interrupción)		
RECURSO	**PUNTO DE RECUPERACIÓN OBJETIVO**	
4. PRIORIZAR LA RECUPERACIÓN DE RECURSOS: (Indicar la prioridad asociada a la recuperación de un recurso específico, considerando el impacto de interrupciones y tiempos de interrupción permisibles)		
ACTIVIDADES	**PRIORIDAD DE RECUPERACIÓN**	
	ALTA	**MEDIA**	**BAJA**

Elaborado por:	**Autorizado por:**		**Aprobado por:**	**Fecha Elab:**	
			Fecha Rev:		

4.1.1 Identificación de funciones y procesos

A continuación se presenta el detalle de la entrevista con la Gerencia de operaciones para el levantamiento de información.

Tabla 24.
Análisis de impacto (BIA) Operaciones

ANÁLISIS DE IMPACTO DE NEGOCIO - CUESTIONARIO	
ORGANIZACIÓN: Zona de Distribución Aeropuerto Mariscal Sucre.	
ÁREA / DEPARTAMENTO DE NEGOCIO: Operaciones	
NOMBRE DEL DIRECTOR DEL ÁREA / DEPARTAMENTO: Gerencia Operaciones	
DESCRIPCIÓN DEL OBJETIVO DEL ÁREA / DEPARTAMENTO: Gestionar las operaciones del 100% de carga que arriba al Ecuador cumplimento estándares y SLA en concordancia con los stakeholder.	
NOMBRE DE LA PERSONA ENTREVISTADA: Gerente de Operaciones	**CARGO:** Gerente de Operaciones
LISTA DE PROCESOS DEL ÁREA / DEPARTAMENTO	

Nº	**PROCESO**
1	Planificación y Control
2	Recepción y traslado de carga
3	Despaletización de carga
4	Consolidación de carga
5	Pesaje de carga
6	Salida y entrega de carga

4.1.2 Identificación de procesos críticos

Considerando los procesos operativos de la organización se evalúa el nivel de impacto en el caso de una interrupción. Para ello se realiza un análisis con el fin de identificar el nivel negativo de una suspensión al proceso core de la empresa.

A continuación se presenta el esquema de valoración del impacto con los niveles: A, B o C.

- **Nivel A:** Es una operación crítica para la organización. Al no contar con ésta, la función del negocio no puede realizarse.

- **Nivel B:** La función no es crítica, pero sin ésta el negocio no podría operar con normalidad

- **Nivel C:** La operación no es una parte integral del negocio.

En este contexto, con el levantamiento realizado con la gerencia de operaciones; se definió los procesos críticos del área core del negocio de la Zona de Distribución. A continuación se presenta el análisis realizado con los niveles de criticidad para determinar los procesos de mayor preocupación para el negocio.

Tabla 25.
Identificación de procesos críticos

Proceso (Servicio)	Nivel	Tolerancia a Fallos (Horas)	Descripción
Planificación y Control	A	1	
Recepción y Traslado de carga	B	1	
Despaletización de carga	B	2	
Consolidación de carga	B	2	
Pesaje de carga	A	1	Uso aplicativo Datapass
Salida y entrega de carga	A	1	Uso aplicativo Datapass

La Zona de Distribución tiene una latente preocupación principalmente en los procesos de Pesaje de carga y Salida y entrega de carga. Su preocupación se fundamenta ya que hace cinco años estos procesos eran totalmente manuales.

Con la implementación del sistema Datapass, éste aplicativo se ha convertido en una de las herramientas primordiales para el proceso operativo de la organización.

4.1.3 Establecimiento de tiempos de recuperación

De acuerdo a los procesos establecidos como principales preocupaciones del core del negocio, se procede a identificar el tiempo máximo de inactividad. Este tiempo permite reconocer hasta qué punto la organización es capaz de tolerar inactividad de sus procesos críticos antes de un colapso y sus procesos de negocio e imagen se vean afectados. Así mismo, se constituirá un nivel de priorización para la recuperación de los procesos o servicios.

Tabla 26.
Prioridades de recuperación

Proceso Crítico (Servicio)	MTD (en días)	Prioridad de recuperación
Planificación y Control	1 día	3
Pesaje de carga	1 día	3
Salida y entrega de carga	1 día	3

Nota: Prioridad de recuperación: 1: Bajo, 2: Medio, 3: Alto

4.1.4 Identificación de recursos

Dentro del establecimiento de los procesos críticos para la Zona de Distribución, todos ellos son soportados por recursos tecnológicos. La identificación de los recursos críticos de los Sistemas de Tecnología y de Información permite considerar acciones y decisiones para medir el impacto y mapear los servicios que sostienen los procesos de la organización.

La siguiente tabla muestra la identificación de recursos críticos de Sistemas de Información y Tecnología.

Tabla 27.
Identificación de recursos críticos de TI

Servicio Crítico	Identificación de recursos críticos de Sistemas de TI
Sistema Datapass	Sistema para manejo del proceso de operaciones. Servicio Web. Servicio de aplicaciones. Servicio de almacenamiento. Servicio de base de datos.
Servicio Internet	Enlace principal de fibra óptica. Servicio de firewall. Gestión router.
Equipos Cliente	Terminal balanza. Terminal aplicativo Datapass.
Servidores	Servidor de aplicaciones sistema Datapass. Servidor de Base de Datos. Servidor de almacenamiento edocs.
Equipos Móviles	Terminal aplicativo Datapass.
Centro de Datos	Monitoreo y control de operaciones de los servidores. Sistemas de almacenamiento y backup. Aire acondicionado. Energía Eléctrica. Energía Asegurada.
Servicio WiFi	Control de usuarios locales. Control de usuarios invitados. Límite de conexiones.
Firewall	Control de servicio DHCP. Control de reglas y asignación de entrada / salida de puertos de puertos. Reglas NAT. Direccionamiento IP Público.
Talento Humano	Falta de personal capacitado. Error de configuración de aplicaciones y aplicación de políticas de seguridad de la información.
Sistema Facturación	Interfaces con el sistema Financiero.

4.1.5 Disposición de los RTO/RPO (Recovery Time Objective / Recovery Point Objective)

A continuación se define el RTO de sus siglas en inglés Recovery Time objetive. El tiempo de recuperación objetivo consiste en el tiempo que tomará el equipo de la Zona de Distribución en recuperar los recursos alterados a los activos o servicios de tecnología e información.

Adicional, se establece el WRT de sus siglas en ingles Recovery Point Objective cuya especificación indica el tiempo que es requerido para completar con las actividades con el principal objetivo de volver a la normalidad y la organización continúe con sus procesos core.

En la siguiente tabla se detallan los tiempos tanto el RTO y RPO de los procesos y servicios críticos de la Zona de Distribución del Aeropuerto Mariscal Sucre.

Tabla 28.
RTO y WRT por cada servicio crítico

Servicio Crítico	Identificación de recursos críticos de Sistemas de TI	Tiempo de Recuperación Objetivo - RTO	Tiempo de Recuperación de Trabajo - WRT
Sistema Datapass	Sistema para manejo del proceso de operaciones. Servicio Web. Servicio de aplicaciones. Servicio de almacenamiento. Servicio de base de datos.	1 día	1 día
Servicio Internet	Enlace principal de fibra óptica. Servicio de firewall. Gestión router.	0.5 día	0.5 día
Equipos Cliente	Terminal balanza. Terminal aplicativo Datapass.	0.5 día	0.5 día

Servidores	Servidor de aplicaciones sistema Datapass. Servidor de Base de Datos. Servidor de almacenamiento edocs.	1 día	1 día
Equipos Móviles	Terminal aplicativo Datapass.	0.5 día	0.5 día
Centro de Datos	Monitoreo y control de operaciones de los servidores. Sistemas de almacenamiento y backup. Aire acondicionado. Energía Eléctrica. Energía Asegurada.	4 día	4 día
Servicio WiFi	Control de usuarios locales. Control de usuarios invitados. Límite de conexiones.	0.5 día	0.5 día
Firewall	Control de servicio DHCP. Control de reglas y asignación de entrada / salida de puertos de puertos. Reglas NAT. Direccionamiento IP Público.	0.5 día	0.5 día
Talento Humano	Personal capacitado.	1 día	1 día
Sistema Facturación	Interfaces con el sistema Financiero.	1 día	1 día

4.2 Levantamiento de riesgos

Es imprescindible mantenerse preparados ante una posible ocurrencia de un evento que ponga en riesgo la correcta operación de la Zona de Distribución del Aeropuerto Mariscal Sucre. Es por eso que es importante definir los riesgos, los diferentes escenarios de amenazas y los planes para contrarrestar o mitigar la ocurrencia o impacto en la operación de la empresa.

4.2.1 Identificación y clasificación de riesgos

La siguiente tabla muestra los potenciales riesgos en los servicios de tecnología de información de la Zona de Distribución. Los servicios críticos identificados anteriormente han sido agrupados en procesos con la finalidad de abarcar en su totalidad a todos los componentes y servicio de tecnología de la compañía.

Tabla 29.
Identificación de riesgos

IDENTIFICACIÓN DEL RIESGO				
#	**Servicio**	**SECTOR**	**AMENAZA GENÉRICA**	**CATEGORÍA**
1	Sistema Datapass	Data Center	Funcionamiento inadecuado de aplicaciones	Desarrollo de aplicaciones
		Data Center	Afectación de la disponibilidad del respaldo de la información	Hardware distribuido
		Data Center	Funcionamiento inadecuado del almacenamiento	Hardware distribuido
2	Servicio de Internet	Data Center	Ausencia servicios del canal de internet de última milla	Red Datos, Internet y Seguridad
		Data Center	Problemas en firewall	Red Datos, Internet y Seguridad
		Data Center	Ausencia de integridad de la información	Red Datos, Internet y Seguridad

3	Equipos Cliente	Todas las áreas	Presencia de virus en equipos y servidores	Red Datos, Internet y Seguridad
4	Servidores	Data Center	Indisponibilidad del servidor o equipos de computo	Hardware distribuido
		Data Center	Problema con los servidores	Hardware distribuido
		Data Center	Afectación de la disponibilidad del respaldo de la información	Aplicaciones infraestructura distribuida
		Data Center	Problema capa de base de datos	Aplicaciones infraestructura distribuida
		Data Center	Afectación de la integridad de los datos	Aplicaciones infraestructura distribuida
5	Equipos Móviles	Todas las áreas	Presencia de virus en equipos y terminales móviles	Red Datos, Internet y Seguridad
6	Centro de Datos	Data Center	Interrupción completa en la continuidad del negocio (Daño en Data Center)	Red Datos, Internet y Seguridad
		Data Center	Interrupción completa en la continuidad del negocio	Red eléctrica
7	Servicio Wi-Fi	Data Center	Ausencia servicios del canal de internet de última milla	Red Datos, Internet y Seguridad

		Data Center	Problemas en firewall	Red Datos, Internet y Seguridad
		Data Center	Falla del equipo	Red Datos, Internet y Seguridad
8	Firewall	Data Center	Falla del equipo	Red Datos, Internet y Seguridad
9	Talento Humano	Humano	Sin personal capacitado.	Humano
10	Sistema Facturación	Data Center	Funcionamiento inadecuado de aplicaciones	Desarrollo de aplicaciones

Tabla 30.
Identificación de amenazas

IDENTIFICAIÓN ESPECÍFICA DE LA AMENAZA							
#	PROCESO	SECTOR	AMENAZA GENÉRICA	CATEGORÍA	COMPONENTE ESPECÍFICO DE LA AMENAZA		CONSECUENCIA DE LA AMENAZA
					COMPONENTE	FACTOR	
1	Sistema Datapass	Data Center	Funcionamiento inadecuado de aplicaciones	Desarrollo de aplicaciones	Bloqueos a nivel de log de aplicaciones	Técnico	Mal funcionamiento del software, retraso en los procesos asociados a la aplicación
			Afectación de la disponibilidad del respaldo de la información	Hardware distribuido	Falla respaldo de información	Técnico	Pérdida de información
			Funcionamiento inadecuado del almacenamiento	Hardware distribuido	Saturación de capacidad de almacenamiento	Técnico	Pérdida de información

2	Servicio de Internet	Data Center	Ausencia servicios del canal de internet de última milla	Red Datos, Internet y Seguridad	Internet	Técnico	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla
			Problemas en firewall	Red Datos, Internet y Seguridad	Internet	Técnico	Falla general de los servicios de red, sin políticas de seguridad
			Ausencia de integridad de la información	Red Datos, Internet y Seguridad	Ataques informáticos frente a la seguridad de la información.	Técnico	Pérdida, robo o mala utilización de información.
3	Equipos Cliente	Todas las áreas	Presencia de virus en equipos y servidores	Red Datos, Internet y Seguridad	Flash memory	Humano	Pérdida de información
					Internet	Humano	Pérdida de información

4	Servidores	Data Center	Indisponibilidad del servidor o equipos de computo	Hardware distribuido	Obsolescencia Tecnológica	Técnico	Pérdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos
			Problema con los servidores	Hardware distribuido	Problema de hardware con los servidores	Técnico	Indisponibilidad de los servicios de TI
			Afectación de la disponibilidad del respaldo de la información	Aplicaciones infraestructura distribuida	Falla tareas programadas	Técnico	Pérdida de información
			Problema capa de base de datos	Aplicaciones infraestructura distribuida	Problemas en los motores de bases de datos	Técnico	Pérdida de información, indisponibilidad de servicios de TI
			Afectación de la integridad de los datos	Aplicaciones infraestructura distribuida	Niveles de seguridad de la información inadecuada	Técnico	Posibles ataques a la integridad de los datos

5	Equipos Móviles	Todas las áreas	Presencia de virus en equipos y servidores	Red Datos, Internet y Seguridad	Problemas de conectividad	Técnico	Pérdida de información, indisponibilidad de servicios de TI
6	Centro de Datos	Data Center	Interrupción completa en la continuidad del negocio (Daño en Data Center)	Red Datos, Internet y Seguridad	Eventos catastróficos: inundaciones, incendios, terremotos.	Técnico	Interrupción completa de los servicios tecnológicos
			Interrupción completa en la continuidad del negocio	Red eléctrica	Fallas en fluido eléctrico normal	Técnico	Interrupción completa de los servicios tecnológicos
			Interrupción completa en la continuidad del negocio	Red eléctrica	Fallas en fluido eléctrico regulada	Técnico	Interrupción completa de los servicios tecnológicos
7	Firewall	Data Center	Falla del equipo	Red Datos, Internet y Seguridad	Ataques informáticos	Técnico	Pérdida, robo o uso no permitido de información confidencial.

8	Servicio Wi-Fi	Data Center	Ausencia servicios del canal de internet de última milla	Red Datos, Internet y Seguridad	Internet	Humano	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla
			Problemas en firewall	Red Datos, Internet y Seguridad	Mala configuración de servicios	Humano	Indisponibilidad de los servicios de TI
9	Talento Humano	Humano	Falta de personal	Humano	Sin el número de personal suficiente y competente.	Humano	Error de configuración en aplicaciones y políticas de seguridad.
10	Sistema Facturación	Data Center	Funcionamiento inadecuado de aplicaciones	Desarrollo de aplicaciones	Bloqueos a nivel de log de aplicaciones	Técnico	Funcionamiento incorrecto del software, retraso en los procesos asociados a la aplicación

Tabla 31.
Valoración del riesgo

VALORACIÓN DEL RIESGO										
#	SERVICIO	SECTOR	AMENAZA GENÉRICA	CATEGORÍA	COMPONENTE ESPECÍFICO DE LA AMENAZA		CONSECUENCIA DE LA AMENAZA	DEFENSA EXISTENTE	PROB	IMPACTO
					COMP	FACTOR				
1	Sistema Datapass	Data Center	Funcionamiento inadecuado de aplicaciones Desarrollo de aplicaciones	Desarrollo de aplicaciones	Bloqueos a nivel de log de aplicaciones	Técnico	Mal funcionamiento del software, retraso en los procesos asociados a la aplicación	Realizar monitoreo diario del espacio en disco para evitar que el tamaño de los logs desborde el espacio	BAJO	MEDIO

			Afectación de la disponibilidad del respaldo de la informació	Hardware distribuido	Falla respaldo de información	Técnico	Pérdida de información	Copias de seguridad, Revisión y respaldo semanal a disco externo	BAJO	ALTO
			Funcionamiento inadecuado del almacenamiento	Hardware distribuido	Saturación de capacidad de almacenamiento	Técnico	Pérdida de información	Realizar los correspondientes Backus para liberar espacio. Tareas programadas y monitoreadas	BAJO	ALTO
2	Servicio de Internet	Data Center	Ausencia servicios del canal de internet de última milla	Red Datos, Internet y Seguridad	Internet	Técnico	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla	Modem USB con plan de internet ilimitado, Enlace de respaldo	BAJO	MEDIO

			Problemas en firewall	Red Datos, Internet y Seguridad	Internet	Técnico	Falla general de los servicios de red, sin políticas de seguridad	Backup de configuración de firewall, reposición nuevo equipo	BAJO	MEDIO
			Ausencia de integridad de la información	Red Datos, Internet y Seguridad	Ataques informáticos frente a la seguridad de la información.	Técnico	Pérdida, robo o mala utilización de la información.	Monitoreo preventivo para determinar anormalidades mediante firewall	BAJO	ALTO
3	Equipos Cliente	Todas las áreas	Presencia de virus en equipos y servidores	Red Datos, Internet y Seguridad	Flash memory	Humano	Pérdida de información	Antivirus, firewall	BAJO	MEDIO
					Internet	Humano	Pérdida de información	Antivirus, firewall	BAJO	MEDIO

4	Servidores	Data Center	Indisponibilidad del servidor o equipos de computo	Hardware distribuido	Obsolescencia Tecnológica	Técnico	Pérdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos	Plan de actualización de equipos	MEDIO	MEDIO
			Problema con los servidores	Hardware distribuido	Problema de hardware con los servidores	Técnico	Indisponibilidad de los servicios de TI	Plan de actualización de equipos	MEDIO	MEDIO
			Afectación de la disponibilidad del respaldo de la información	Aplicaciones infraestructura distribuida	Falla tareas programadas	Técnico	Pérdida de información	Copias de seguridad, Revisión y respaldo diario a disco externo	BAJO	ALTO

			Problema capa de base de datos	Aplicaciones infraestructura distribuida	Problemas en los motores de bases de datos	Técnico	Pérdida de información, indisponibilidad de servicios de TI	Copias de seguridad, servidores alternos	BAJO	ALTO
			Afectación de la integridad de los datos	Aplicaciones infraestructura distribuida	Niveles de seguridad de la información inadecuada	Técnico	Posibles ataques a la integridad de los datos	Manejo de perfiles, grupos y acceso a aplicaciones	BAJO	MEDIO
5	Equipos Móviles	Todas las áreas	Presencia de virus en equipos y servidores	Red Datos, Internet y Seguridad	Problemas de conectividad	Técnico	Pérdida de información, indisponibilidad de servicios de TI	Plan de actualización de equipos	BAJO	MEDIO

6	Centro de Datos	Data Center	Interrupción completa en la continuidad del negocio (Daño en Data Center)	Red Datos, Internet y Seguridad	Eventos catastróficos: inundaciones, incendios, terremotos.	Técnico	Interrupción completa de los servicios tecnológicos	Backup de bases de datos de todos los sistemas.	BAJO	ALTO
			Interrupción completa en la continuidad del negocio	Red eléctrica	Fallas en fluido eléctrico normal	Técnico	Interrupción completa de los servicios tecnológicos	Sistemas de alimentación ininterrumpida	BAJO	ALTO
			Interrupción completa en la continuidad del negocio	Red eléctrica	Fallas en fluido eléctrico regulada	Técnico	Interrupción completa de los servicios tecnológicos	Generadores de energía	BAJO	ALTO
7	Firewall	Data Center	Falla del equipo	Red Datos, Internet y Seguridad	Ataques informáticos.	Técnico	Pérdida, robo o uso no permitido de información confidencial.	Backup de configuración de firewall, reposición nuevo equipo	BAJO	MEDIO

8	Servicio Wi-Fi	Data Center	Ausencia servicios del canal de internet de última milla	Red Datos, Internet y Seguridad	Internet	Técnico	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla	Modem USB con plan de internet ilimitado, Enlace de respaldo	BAJO	MEDIO
			Problemas en firewall	Red Datos, Internet y Seguridad	Mala configuración de servicios	Técnico	Indisponibilidad de los servicios de TI	Backup de configuración de firewall, reposición nuevo equipo	BAJO	MEDIO
9	Talento Humano	Todas las áreas	Falta de personal	Humano	Sin el número de personal suficient	Humano	Error de configuración en aplicaciones y políticas de seguridad.	Backup de personal, capacitaciones continuas	BAJO	MEDIO
10	Sistema Facturación	Data Center	Funcionamiento inadecuado de aplicaciones	Desarrollo de aplicaciones	Bloqueos a nivel de log de aplicaciones	Técnico	Funcionamiento incorrecto del software, retraso en los procesos asociados a la aplicación	Realizar monitoreo diario del espacio en disco para evitar que el tamaño de los logs desborde el espacio	BAJO	MEDIO

4.2.4 Clasificación del riesgo

La siguiente tabla muestra la clasificación del riesgo ponderando la probabilidad y el impacto en los siguientes niveles:

- 1: Nivel bajo.
- 2: Nivel medio.
- 3: Nivel alto.

Tabla 32.
Análisis del riesgo

CÓDIGO	PROCESO	AMENAZA GENÉRICA	PROB	IMPACTO	EXPOSICIÓN
R9	Servidores	Problema con los servidores	2	3	6
R12	Centro de Datos	Interrupción completa en la continuidad del negocio	2	3	6
R4	Servicio de Internet	Ausencia servicios del canal de internet de última milla	2	3	6
R5	Servicio de Internet	Problemas en firewall	2	2	4
R4	Servicio Wi-Fi	Ausencia servicios del canal de internet de última milla	2	2	4
R5	Servicio Wi-Fi	Problemas en firewall	2	2	4

R13	Firewall	Falla del equipo tecnológico	2	2	4
R1	Sistema Datapass	Funcionamiento inadecuado de aplicaciones	1	3	3
R2	Sistema Datapass	Afectación de la disponibilidad del respaldo de la información	1	3	3
R3	Sistema Datapass	Funcionamiento inadecuado del almacenamiento	1	3	3
R6	Servicio de Internet	Ausencia de integridad de la información	1	3	3
R8	Servidores	Indisponibilidad del servidor o equipos de computo	1	3	3
R2	Servidores	Afectación de la disponibilidad del respaldo de la información	1	3	3
R10	Servidores	Problema capa de base de datos	1	3	3
R6	Servidores	Ausencia de integridad de la información	1	3	3
R14	Talento Humano	Falta de personal	1	3	3
R1	Sistema Facturación	Funcionamiento inadecuado de aplicaciones	1	3	3
R7	Equipos Cliente	Presencia de virus en equipos y servidores	1	2	2
R11	Equipos Móviles	Presencia de virus en equipos y servidores	1	2	2

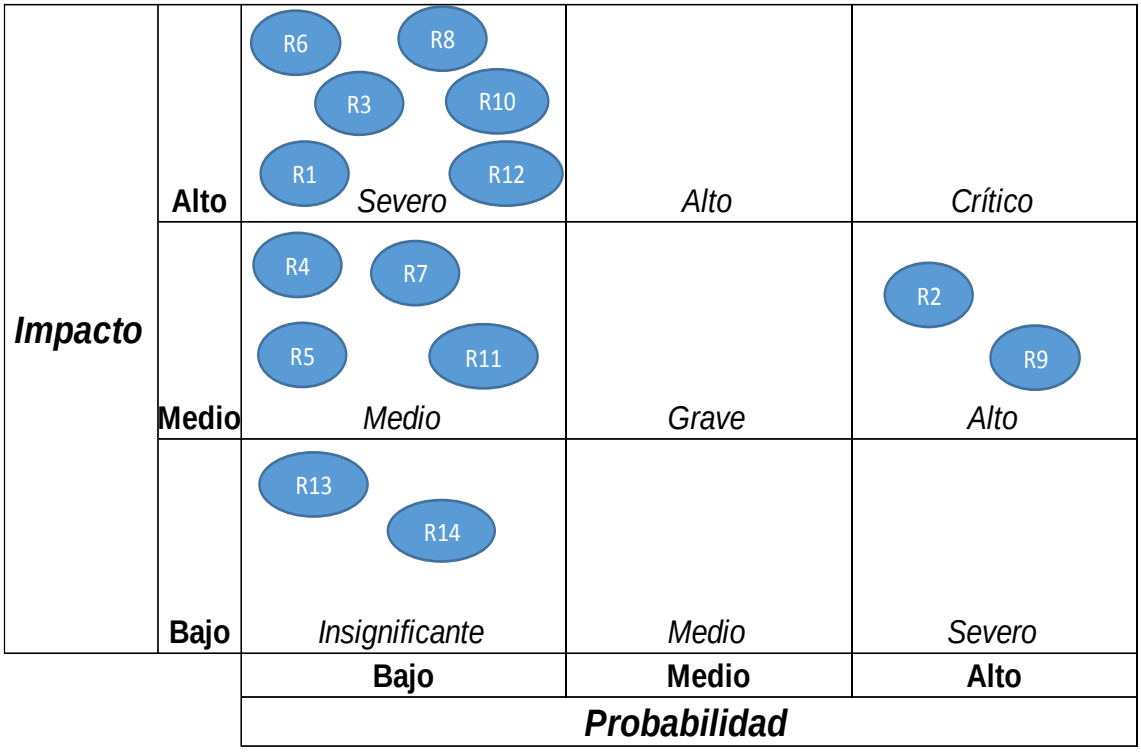

Figura 33. Clasificación del riesgo.

Tabla 33.
Clasificación del riesgo

TIPO DE RIESGO	RIESGOS
Riesgo Insignificante	R13, R14
Riesgo Medio	R4, R5, R7, R11
Riesgo Severo	R1, R3, R6, R8, R10, R12
Riesgo Grave	----------
Riesgo Alto	R2, R9

5. ESTRATEGIAS DE RECUPERACIÓN

El quinto capítulo presenta una identificación de los riesgos a la que toda organización podría estar expuesta, evaluando su impacto y probabilidad de ocurrencia. Adicional, describe la planificación e implementación de estrategias de continuidad para los procesos o actividades críticas de la Zona de Distribución del Aeropuerto Mariscar Sucre.

5.1 Análisis de escenarios y evaluación de riesgos

Para la definición de la continuidad de negocio se consideran en este apartado cuatro escenarios para definir las estrategias de recuperación. Con el objetivo de abarcar el mayor número de escenarios, se ha definido en cuatro grupos ya que las consecuencias de materialización de cualquier amenaza, desembocarán en los siguientes escenarios.

- Imposibilidad de acceso a instalaciones.
- Falta de personal.
- Fallo de la tecnología.
- Fallo de un proveedor clave.

Figura 34. Análisis de escenarios.

5.1.1 Análisis de escenarios

Imposibilidad de acceso a las instalaciones

Este escenario hace referencia cuando no se dispone acceso a las oficinas principales de la Zona de Distribución del Aeropuerto Mariscal Sucre. Así mismo, se puede considerar una obligación de abandono de las instalaciones principales.

Consideraciones:

- Las personas no disponen lugar para el normal desempeño de los procesos críticos de la Zona de Distribución.
- La infraestructura básica de la organización no se ha visto afectada.
- Se encuentran habilitados los servicios de internet y demás servicios soportados por tecnología.

La principal estrategia para resolver el primer escenario es el traslado del personal a un sitio alterno para que se puedan efectivizar los procesos críticos de la empresa.

Falta de personal

El escenario de falta de personal hace referencia cuando uno o varias personas por cualquier situación o circunstancia extrema se ven obligadas a ausentarse de su lugar de trabajo o trabajar de forma aislada. En este caso, la organización se ve afectada al no disponer de personal suficiente para ejecutar los procesos críticos.

Consideraciones:

- Tras el análisis de la situación, de ser el caso, se deberá cumplir con estándares de sanidad y asistencia controlada al lugar de trabajo.
- Se dispone de acceso a las instalaciones para realizar los procesos de negocio de forma normal.
- Se encuentran habilitados los servicios de internet y demás servicios soportados por tecnología.

Las estrategias a considerar son las siguientes:

- Brindar las facilidades de teletrabajo. Esta estrategia conlleva a disponer altos estándares de seguridad de la información.
- Reemplazo de forma temporal del personal ausente que maneje procesos críticos de la organización.
- Así mismo se podría reemplazar a las personas en procesos críticos mediante un contrato por servicios específicos.

Falla de tecnología

Son considerados fallos tecnológicos, problemas existentes en el centro de cómputo, servidores, aplicaciones de negocio, servicio de internet, base de datos, equipos de telecomunicación y fallo eléctrico.

Consideraciones:

- Se dispone de acceso total a las oficinas principales de la organización.
- Se debe utilizar medios alternos para continuar con los procesos críticos o utilizar o poner en marcha los procesos alternos.

La principal estrategia en este escenario es contar con equipos de tecnología redundante, energía asegurada y generadores de energía. Finalmente contar con un centro alterno que permita continuar con los procesos de negocio catalogados como críticos en capítulos anteriores.

Falla de proveedor clave

Gran cantidad de incidentes que sufren las empresas son causados por los proveedores. En este estudio, para la Zona de Distribución es de vital importancia el servicio de internet.

Consideraciones:

- Se dispone de acceso a las instalaciones para realizar los procesos de negocio de forma normal.
- Se dispone acceso a las aplicaciones de negocio.

La estrategia es disponer procedimientos para las calificaciones de proveedores y principalmente disponer proveedores de backup para servicios considerados críticos para la organización.

5.1.2 Análisis de riesgos

La siguiente tabla define los riesgos presentes en los escenarios principales de la Zona de Distribución del Aeropuerto Mariscal Sucre. Así mismo, se alinea los procesos críticos, componentes y servicios tecnológicos.

La siguiente tabla muestra el alineamiento existente entre los procesos definidos como críticos por la Zona de Distribución del Aeropuerto Mariscal Sucre, los servicios y componentes tecnológicos que soportan dichos procesos y el nivel de complejidad para la implementación del DRaaS como estrategia principal de recuperación definido por la alta gerencia de le organización.

Los niveles de prioridad, alineación y complejidad se ha considerado un rango de 1 al 3. En donde:

- 1: Nivel bajo.
- 2: Nivel medio.
- 3: Nivel alto.

Tabla 34.
Escenarios de riesgos

ESTRATEGIAS DE RECUPERACIÓN							
#	PROCESO	COMPONENTE O SERVICIO TENOLÓGICO	PRIORIDAD	TIPO DE SERVICIO	RIESGO	DRaaS	
						ALINEACIÓN	COMPLEJIDAD
1	Planificación y Control	Servicio de Internet	3	Rutina	R4, R5, R11	3	1
		Equipos Cliente	3	Rutina	R4, R5, R7, R11, R12	3	1
		Servicio Wi-Fi	3	Rutina	R4, R5, R11	3	1
		Firewall	1	Rutina	R4, R5, R11, R12	2	1
		Talento Humano	3	Rutina	R6, R13	2	2
2	Pesaje de carga	Sistema Datapass	3	Rutina	R1, R6, R11, R12	3	3
		Servicio de Internet	3	Rutina	R1, R4, R5, R6, R11, R12	3	3

		Equipos Cliente	3	Rutina	R1, R4, R11, R12	3	1
		Servidores	3	Rutina	R1, R2, R3, R6, R7, R8, R9, R10, R11, R12	3	3
		Equipos Móviles	1	Rutina	R1, R4, R11, R12	1	1
		Centro de Datos	3	Rutina	R1, R2, R3, R6, R7, R8, R9, R10, R11, R12	3	3
		Servicio Wi-Fi	3	Rutina	R1, R4, R5, R6, R1, R12	3	2
		Talento Humano	3	Rutina	R6, R11, R13	2	2
		Firewall	2	Rutina	R1, R4, R5, R6, R11, R12	2	2
3	Salida y Entrega de carga	Sistema Datapass	3	Rutina	R1, R6, R11, R12	3	3
		Servicio de Internet	3	Rutina	R1, R4, R5, R6, R11, R12	3	3
		Equipos Cliente	3	Rutina	R1, R4, R11, R12	3	1
		Servidores	3	Rutina	R1, R2, R3, R6, R7, R8, R9, R10, R11, R12	3	3
		Equipos Móviles	1	Rutina	R1, R4, R11, R12	1	1
		Centro de Datos	3	Rutina	R1, R2, R3, R6, R7, R8, R9, R10, R11, R12	3	3
		Servicio Wi-Fi	3	Rutina	R1, R4, R5, R6, R1, R12	3	2
		Sistema de	2	Rutina	R1	2	2
		Talento Humano	3	Rutina	R6, R11, R13	2	2
		Firewall	2	Rutina	R1, R4, R5, R6, R11, R12	2	2

5.2 Estrategias de recuperación

Este estudio se centra principalmente para solventar el escenario de fallo de los servicios tecnológicos. En este contexto, a continuación se presenta diferentes estrategias que la Zona de Distribución del Aeropuerto Mariscal Sucre puede optar con el fin de disponer un centro alterno basado en cloud computing. Una correcta decisión le permite apalancarse mediante la tecnología para sostener el core de negocio de la organización para sobrevivir en el tiempo ante cualquier catástrofe.

La siguiente tabla muestra las diferentes estrategias de recuperación de la tecnología.

Tabla 35.
Estrategia de recuperación tecnológica

Estrategia de recuperación tecnológica	Descripción
Sitio alterno espejo o duplicado (Mirrored Site)	Centro alterno equipado y operando igual al principal. Se replica en tiempo real. Dispone personal de operación propio.
Sitio alterno equipado (Hot Site)	Centro alterno con equipos necesario para operar en contingencia. No dispone personal y se lo utiliza para replicar datos, obtener respaldos o para procesos menores de la organización.
Sitio alterno - semiequipado (Warm Site)	Centro con cierto tipo de equipamiento, no podría entrar en funcionamiento con lo que cuenta. No dispone servidores principales.
Sitio alterno sin equipamiento (Cold Site)	Espacio físico vacío que dispone únicamente electricidad, no dispone equipamiento de TI.
Sitio alterno contratado con proveedor	Centro alterno que se acuerda con el proveedor las características de operación del mismo.

Adaptado de Banco Capital, s.f

De acuerdo a las mejores prácticas, los tiempos de respuesta según la estrategia de recuperación tecnológica es la siguiente:

Tabla 36.
Tiempo estimado de recuperación tecnológica

Estrategia de recuperación tecnológica	**Tiempo de recuperación estimada**
Sitio alterno espejo o duplicado (Mirrored Site)	Cinco minutos en condiciones favorables. Una hora máxima.
Sitio alterno equipado (Hot Site)	16 horas en condiciones favorables. 48 horas máximo.
Sitio alterno - semiequipado (Warm Site)	Una semana en condiciones favorables. 4 semanas máximo.
Sitio alterno sin equipamiento (Cold Site)	Un mes en condiciones favorables. 3 meses máximo.
Sitio alterno contratado con proveedor	De pocos minutos a varios días. Dependen los términos del contrato.

Adaptado de Banco Capital, s.f

Los procesos críticos de la Zona de Distribución del Aeropuerto Mariscal Sucre definidos en el apartado cuarto de este estudio se presentan a continuación con la mejor estrategia de recuperación de tecnología. Es importante considerar el menor tiempo de afectación para que la organización no se vea afectada en imagen o peor aún temas de índoles financieros.

Tabla 37.
Propuesta de estrategia a procesos críticos

Proceso	Nivel	Responsable	Tolerancia a Fallos (Horas)	Estrategia requerida
Planificación y Control	A	Gerencia de operaciones	1	Sitio alterno espejo o duplicado (Mirrored Site)
Pesaje de carga	A	Gerencia de operaciones	1	Sitio alterno espejo o duplicado (Mirrored Site)
Salida y entrega de carga	A	Gerencia de operaciones	1	Sitio alterno espejo o duplicado (Mirrored Site)

5.2.1 Recursos del plan de continuidad

De acuerdo al levantamiento de los procesos críticos de la Zona de Distribución del Aeropuerto Mariscal Sucre y con el total apoyo de la alta gerencia, se ha definido como estrategia de recuperación la instauración de un centro alterno en la nube. Para ello se ha divido esta definición en dos áreas que corresponde a los recursos que necesitará el sitio alterno y finalmente, los recursos del cliente.

5.2.1.1 Sitio alterno

La Zona de Distribución del Aeropuerto Mariscal Sucre se ve en la necesidad de asegurar sus procesos críticos descritos en capítulos anteriores. Es por ello que la empresa ha definido como principal estrategia de recuperación la implementación de un sitio alterno basado en cloud computing que le permita disponer los servicios tecnológicos que apalanquen sus procesos de negocio de forma flexible optimizando recursos con el objetivo principal de resguardar la imagen y operación de la organización.

Para ello, la Zona de Distribución pretende instaurar un sitio alterno en donde se encuentre implementado y completamente funcional el sistema Datapass, aplicación que soporta el proceso operativo de la empresa.

5.2.1.2 Análisis de proveedores DRaaS

A continuación se presenta el análisis realizado de las características principales que el proveedor deberá cumplir para poder ofrecer el servicio de Data Recovery as a Service donde exista una convergencia entre la tecnología y las necesidades puntuales de la Zona de Distribución. Esta alineación permitirá a la organización reducir la incertidumbre y disponer los principales procesos de negocio en un sitio alterno en la nube.

La siguiente tabla muestra los diferentes criterios que la organización ha considerado de valor para la implementación de la recuperación de desastres como un servicio. Para ello, se ha definido un rango del 1 al 3, en donde 1 es importancia baja y el número 3 es importancia alta.

Tabla 38.
Parámetro evaluación de proveedores

CRITERIO	IMPORTANCIA
Personalización	3
Facilidad de uso	3
RTO y requisitos de RPO	3
Soporte para arquitectura de baja complejidad	2
Soporte para arquitectura de complejidad media	2
Soporte para arquitectura de alta complejidad.	2
Creación de Runbook de recuperación orquestada	2
Recuperación Flexible	3
Soporte de integración	3
Seguridad y Cumplimiento	3
Recuperación de autoservicio	3
Soporte globalizado	2
Habilitación bimodal y de nubes.	2

Flexibilidad de precios	3
Facilidad de integración y despliegue	3
Calidad de Soporte Técnico	3

Adaptado de Proveedores DRaaS Gartner, 2018.

5.2.1.3 Recursos del centro alterno

Personal

Es necesario personal especializado para la administración, mantenimiento y entrega del servicio:

- Administrador Sistema Datapass.
- Administrador servicio DRaaS.
- Personal de telecomunicaciones y tecnología de la información.
- Personal de seguridad de la información
- Gestor de base de datos.

Tecnología

- Sistema Datapass.
    - Servidor de aplicaciones.
    - Servidor de base de datos.
    - Comunicaciones.
    - Redes y seguridad.

Información

- Política de procedimiento del plan de continuidad de negocio de la Zona de Distribución.
- Procedimientos del sistema Datapass de sus diferentes módulos.
- Manual de operación del sistema Datapass.
- Manual de configuración.

Finanzas

Se deberá definir un flujo de caja para cubrir con los gastos operativos y de mantenimiento de DRaaS:

- Hardware para cumplir con el funcionamiento del sistema Datapass.
- Implementación de la solución.
- Servicio de operación del aplicativo.
- Servicio de telecomunicación.
- Gestión base de datos y réplicas de la información

5.2.1.4 Recursos del cliente

Personal

Es necesario personal especializado y capacitado para la efectiva ejecución de los siguientes procesos de negocio.

Tabla 39.
Recurso personal del cliente

Proceso (Servicio)	Responsable	Personal
Planificación y Control	Gerencia de operaciones	- Experto en logística. - Supervisor de operaciones. - Coordinador de aerolíneas.
Pesaje de carga	Gerencia de operaciones	- Estibadores de carga. - Operadores de Datapass.
Salida y entrega de carga	Gerencia de operaciones	- Estibadores de carga. - Operadores de Datapass.

Instalaciones

- Del lado del cliente, es necesario un área específica, delimitada y segura para el despaletizaje y paletizaje de la carga que arriba al Ecuador. Esto asegurará que los procesos operativos de la empresa se realicen de forma adecuada y controlada.

- Se requiere estaciones de trabajo para los operadores del sistema Datapass.

Tecnología

- Es indispensable disponer de tabletas con acceso a datos móviles para la interconexión con el sistema Datapass.

Información

- Procedimientos del proceso de carga de importación.

- Reportes operativos.
- Documentación de la operación.

Finanzas

Se deberá definir un flujo de caja para cubrir con los gatos operativos y de persona ante la presencia de una situación de emergencia. Como por ejemplo:

- Personal
- Alimentación
- Servicios y herramientas para la operación

Suministros

- Servicio de agua, luz, alimentación
- Comunicación con centro alterno

5.2.1.5 Estrategias de recuperación alternas

Para la Zona de Distribución es de vital importancia por la concesión del servicio de handling de carga continuar con las actividades para procesar y dar una efectiva atención a la mercadería que arriba al Ecuador. Por este motivo, la organización ha definido actividades y procedimientos alternos para cumplir con los temas legales.

La principal preocupación de empresa son los procesos que recaen en automatizaciones o que dependen en su totalidad de sistemas informáticos. En este contexto, se han definido procesos alternos para los procesos que utilizan

el aplicativo Datapass. A continuación detalle del proceso alterno que será considerado en primera instancia antes de dar inicio al plan de continuidad de negocio.

Pesaje de carga

En el proceso de la recepción y pesaje de carga, la Zona de Distribución dispone de un proceso en donde se define a detalle los pasos a seguir y cómo activar el proceso alterno en el caso de que las circunstancias lo ameriten.

Previo a activar el proceso alterno de pesaje de carga, existe personal responsable de revisar y autorizar la ejecución de un proceso manual. La empresa ha establecido el siguiente formato para el registro del manifiesto o vuelo que será procesado, el número de guía master, número de guía hija, el número de paquetes recibidos, peso recibido, el depósito al que se asignará la mercadería y finalmente, un campo para detallas las novedades con la que la mercadería ha arribado al Ecuador.

RECEPCIÓN DE CARGA								
Número de manifiesto:								
Ítem	# Guía madre	# Guía hija	Bultos manifestado	Peso manifestado	# Bultos recibidos	Peso recibido	Depósito Temporal	Novedades
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

Figura 35. Registro proceso alterno pesaje de carga.

Es importante indicar que el proceso de transmisión y declaración de la mercadería hacia el sistema del Servicio Nacional de Aduana se realizará previa a la restauración del aplicativo Datapass. Por otro lado, si la situación así lo amerita se realizarán las transmisiones por el sistema Ecuapass.

Salida y entrega de carga

Para el proceso de entrega de la mercancía se dispone el siguiente registro para especificar el número de manifiesto que se está despachando, el número de guía madre, número de guía hija, número de bultos a ser entregados, cantidad de peso entregado, depósito temporal al que se entrega la mercadería y finalmente un campo para indicar cualquier tipo de novedades sobre una carga en específico.

SALIDA DE CARGA						
			Número de manifiesto:			
Ítem	**# Guía madre**	**# Guía hija**	**# Bultos**	**Peso entregado**	**Depósito Temporal**	**Novedades**
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Autorización Zona de Distribución	Autorización Depósito Temporal	Autorización Servicio Nacional Aduana

Figura 36. Registro proceso alterno salida y entrega de carga.

Tabla 40.
Análisis de escenarios por riesgos

ESCENARIOS	RIESGOS
Proveedores alternos	R4, R6, R5, R11
Estrategia manual pesaje de carga	R1, R3
Estrategia manual salida de carga	R1, R3
Personal Backup	R14
Activación sitio Alterno	R1, R2, R3, R6, R7, R8, R9, R10,R13, R12
Equipos redundantes	R1, R2, R3, R6, R7, R9, R10, R13

5.3 Pruebas y mecanismos de verificación

Los diferentes planes de estrategias de recuperación planteados en este estudio basado en la nube necesitan ponerse a prueba para validar su correcto funcionamiento y corrección de posibles aspectos no considerados en el plan con la finalidad principal de disponer un plan de continuidad completamente funcional.

5.3.1 Plan de pruebas

El plan de continuidad de la Zona de Distribución debe ser efectivo para actuar ante cualquier emergencia de forma efectiva en el tiempo definido en anteriores capítulos de acuerdo a los requerimientos de la empresa. Es por ello la necesidad de disponer un plan de pruebas que permita poner en práctica y verificar el nivel ejecución de las áreas, validar los conocimientos y experiencia de los empleados.

A continuación se presenta un plan de prueba sugeridas para verificación del plan de continuidad del negocio.

Tabla 41.
Plan de pruebas

Tipo de ejercicio	Objetivo	Periodicidad	Revisión post-ejercicio
Revisión de escenarios	Validar la realidad actual de la Zona de Distribución para identificar nuevos escenarios y validar que los planteados van acorde al plan de continuidad	6 meses	Observaciones, recomendaciones y actualizaciones de escenarios y plan de continuidad del negocio
Revisión de estrategias de continuidad	Revisar a profundidad las estrategias de continuidad definidas y analizar el nivel de eficiencia en la recuperación.	6 meses	Observaciones, recomendaciones y actualizaciones de las estrategias de recuperación.
Pruebas de funcionamiento del sitio alterno	Validar el funcionamiento del sitio alterno mediante la definición de un escenario que se acerque a la realidad para validad el nivel de ejecución y recuperación	1 cada dos años	De ser el caso re direccionar las estrategias de recuperación y tiempo de recuperación.
Pruebas de equipos tecnológicos	Verificar el correcto funcionamiento de los equipos tecnológicos del sitio alterno así como también los equipos previstos para los terminales del cliente	6 meses	Actualización de equipos y revisión de nuevas tendencias tecnológicas de recuperación.

Adaptado de APEC, 2016

5.3.2 Mecanismos de verificación

A continuación se presenta el detalle de la validación técnica definida por la gerencia general de la Zona de Distribución para cerciorar que el sitio alterno establecido en la nube cumpla con las necesidades y apoye con los procesos críticos de la organización.

5.3.2.1 Validación Técnica del Centro Alterno

Listado de validación técnica del Centro Alterno para la Zona de Distribución del Aeropuerto Mariscal Sucre:

- Comprobación de servicio de comunicaciones con el Centro Alterno.
- Comprobación de operatividad del sistema Datapass en su totalidad.
- Comprobación de transmisiones de documentos electrónicos hacia sistema del Servicio Nacional de Aduanas del Ecuador.
- Revisión y validación de redundancia de energía eléctrica.
- Revisión de réplicas y respaldo de bases de datos.
- Disponibilidad de reportes.
- Validación de usuarios, perfiles y acceso al sistema Datapass.

5.3.2.2 Validación Técnica del cliente

Listado de validación técnica del cliente para la Zona de Distribución del Aeropuerto Mariscal Sucre:

- Comprobación de servicio de comunicaciones con el cliente.

- Comprobación de operatividad del sistema Datapass en su totalidad.
- Comprobación de transmisiones de documentos electrónicos hacia sistema del Servicio Nacional de Aduanas del Ecuador.
- Disponibilidad de reportes.
- Validación de usuarios, perfiles y acceso al sistema Datapass.

5.4 Auditorías internas

Se plantea un grupo de auditorías internas definidas en conjunto con la alta gerencia de la Zona de Distribución. Esto permitirá analizar de forma periódica el nivel de madurez del sistema de gestión de continuidad del negocio y así mismo permitirá un mejoramiento continuo.

Los responsables de las auditorías están definidos por la alta gerencia de la siguiente manera:

- **Sistema de gestión de continuidad del negocio:** Gerencia de Operaciones y su respaldo el Jefe de Sistemas.
- **Tecnología:** Jefe de Sistemas.
- **Operaciones:** Gerencia de Operaciones y su respaldo el Gerente de Seguridad.
- **Validación de funcionamiento:** Líder de Operaciones.

De acuerdo a las necesidades de la empresa se define que las auditorías internas se llevarán a cabo dos veces al año, cuya principal finalidad es identificar los diferentes elementos a mejorar y las detectar las posibles amenazas para posterior a esto definir un plan de acción para controlarlos.

Auditoría Sistemas Datapass

Tabla 42.
Auditoría Sistema Datapass

AUDITORÍA SISTEMA DATAPASS	
Objetivo	Validar el correcto funcionamiento del sistema Datapass y su inter comunicación con el sistema del Servicio Nacional de Aduana. Esto permitirá a la Zona de Distribución mantener un nivel alto de disponibilidad y fiabilidad del servicio.
Periodicidad	Semestral

Auditoría Seguridad de la Información

Tabla 43.
Auditoría de Seguridad de la Información

AUDITORÍA SEGURIDAD DE LA INFORMACIÓN	
Objetivo	Validar los niveles y controles de seguridad disponibles. El objetivo principal es identificar las posibles brechas de seguridad en referencia a la seguridad de la información y definir un plan de acción para solventar y controlar la integridad de la empresa.
Periodicidad	Semestral

Auditoría Sistema de Continuidad de Negocio

Tabla 44.
Auditoría de Sistema de Continuidad de Negocio

AUDITORÍA SISTEMA CONTINUIDAD DE NEGOCIO	
Objetivo	Verificar el correcto funcionamiento del Sistema de Gestión de Continuidad del negocio, estrategias, indicadores y plan de continuidad. El objetivo principal es mantener al sistema dinámico validando todos sus componentes.
Periodicidad	Semestral

5.5 Mejora continua

Lo anteriormente descrito permite a la Zona de Distribución disponer un plan de continuidad del negocio vivo que dispone un mejoramiento continuo y que continúa aprendiendo con el transcurrir del tiempo. Esto beneficia a la organización en tiempo, dinero e imagen en el caso de algún caso de emergencia.

6. GUÍA DE IMPLEMENTACIÓN

El sexto apartado define una hoja de ruta para la implementación de un plan de recuperación de desastres. La sección será dividida en seis fases en donde se detallan los pasos a seguir para una correcta gestión de continuidad del negocio.

6.1 Hoja de ruta de implementación

Se ha planteado la siguiente hora de ruta con el objetivo de tener fases para implementar un plan de continuidad de negocio. Es importante destacar que, la siguiente hoja de ruta tiene como base principal el mejoramiento continuo.

A continuación se detallas las fases de la guía de implementación:

1. **Diseño del plan y política de Continuidad del Negocio.-** Establece las necesidades y requerimientos previos para el diseño e implementación de un Plan de Continuidad de Negocio. (Deloitte, 2015)

2. **Procesos y análisis de riesgos.-** Es de vital importancia conocer el giro del negocio, los procesos agregadores de valor, de soporte y los estratégicos de la organización. Esto ayudará a definir claramente los procesos que la empresa agregará dentro de su estrategia para ofrecer continuidad a dichos procesos. (Deloitte, 2015)

3. **Medidas de prevención.-** En esta fase se plantean las diferentes medidas preventivas de seguridad que la organización dispone para que sus procesos definidos en la anterior fase no se vean interrumpidas ante cualquier eventualidad. Este proceso se realiza sin activar el Plan de Continuidad de Negocio. (Deloitte, 2015)
4. **Estrategias de recuperación.-** Se define con claridad los procesos de negocio a restaurar considerando impacto y prioridad de acuerdo a las necesidades de operación de la empresa. (Deloitte, 2015)

5. **Implementación del plan de continuidad de negocio.-** Son los pasos a seguir para implantar el Plan de Continuidad de Negocio. El mismo debe alinearse de forma estratégica con las estrategias de recuperación definidas en la fase anterior. (Deloitte, 2015)

6. **Mantenimiento y mejora continua.-** Esta fase permite definir parámetros de medición, pruebas de funcionamiento, auditorías y un plan de acción dinámico que permite al Plan de Continuidad de Negocio disponer una mejora y aprendizaje continuo en el tiempo. (Deloitte, 2015)

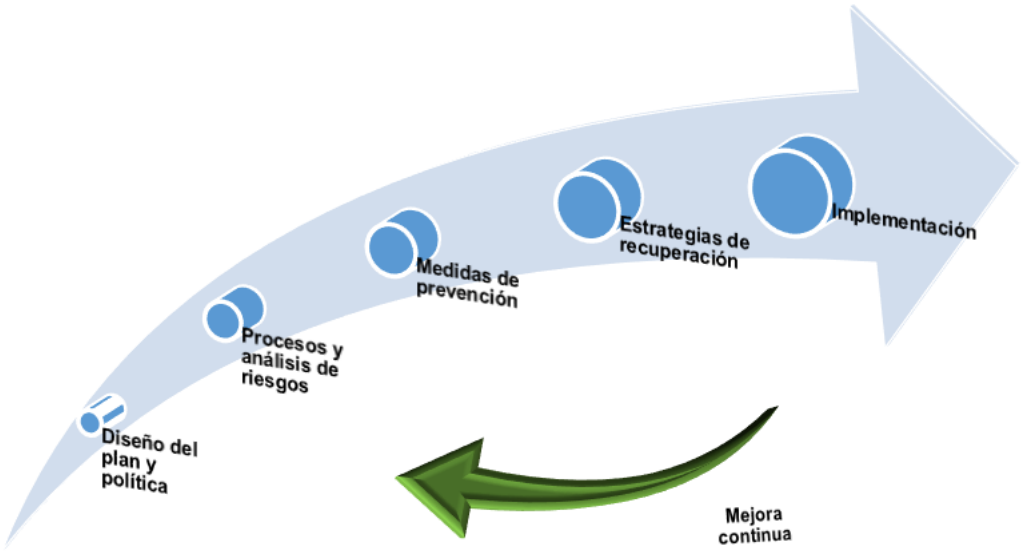

Figura 37. Hoja de ruta de continuo mejoramiento.

6.2 Fase I: Diseño del plan y política de Continuidad del Negocio.

El principal objetivo de la fase del diseño del plan y política de continuidad de negocio es en primera instancia, obtener el auspicio de uno de los principales stakeholder de la organización. Contar con el patrocinamiento de la gerencia general de la organización será vital para empezar con el plan de continuidad de negocio. (Deloitte, 2015)

Finalmente, con el aval correcto es necesario disponer de flujo de dinero o las inversiones que sean correspondientes para implementar un plan de continuidad que soporten los procesos principales de la organización.

A continuación se detalla las actividades principales para dar cumplimiento al diseño y la política del plan de continuidad del negocio.

6.2.1 Designar responsable de Continuidad de Negocio

Una de las tareas fundamentales en la fase del diseño y la política es la designación del responsable de la elaboración, supervisión, difusión e implementación del plan de continuidad de negocio. (Deloitte, 2015)

Lo ideal es que la empresa independientemente de su tamaño cuente con los recursos financieros necesarios para definir el equipo que se encargará del plan de continuidad. Este equipo será el responsable de hacer efectivo el plan desde el establecimiento del alcance hasta el mejoramiento continuo del proceso de contingencia de la organización. (Deloitte, 2015)

Finalmente, cabe mencionar que el equipo de trabajo del plan de continuidad de negocio no será necesariamente personal técnico o perteneciente al departamento de Sistemas y Tecnología. Es recomendable que el equipo sea constituido por ejecutivos expertos en los procesos que la compañía haya definido como procesos clave dentro del core de la empresa. En este contexto, el equipo podrá construir, mantener, soportar y dar un mejoramiento continuo sobre las actividades, procedimientos y procesos de los cuales tienen la experiencia suficiente. (Deloitte, 2015)

6.2.2 Elaborar política de Continuidad de Negocio

Una vez definido el responsable, el equipo y el alcance, se procede a documentar la política del plan de continuidad de negocio.

A continuación se presenta un formato de apoyo para la construcción de la política para cualquier organización.

Audiencia

A quién o quieres irá dirigida la presenta política

Introducción

Breve resumen sobre lo que es y el objetivo principal de la política de continuidad de negocio.

Definiciones

Palabras clave a utilizar en el documento con su respectivo significado o enunciado.

Objetivo

Definición del objetivo principal de la implementación de la política.

Roles y responsabilidad

Definición de los cargos dentro de la organización que cumplirán con ciertas actividades dentro del plan de continuidad de negocio.

Desarrollo

Elaboración detallada de la política de continuidad de negocio.

Violaciones a la política

Definición de las consecuencias de no dar cumplimiento a la política.

6.2.3 Planificación del proyecto

El plan de Continuidad de negocio debe ser visto como un proyecto, por lo que es recomendable que el responsable del plan de continuidad posea conocimientos sobre gestión de proyectos. El fin principal es que cumpla con la triple restricción de cumplimiento tanto para la gerencia general, como para con los accionistas en tiempo costo y alcance; sin perder el enfoque de la calidad del plan de continuidad de negocio. (Deloitte, 2015)

6.3 Fase II: Procesos y Análisis de riesgos.

La segunda fase de la guía de implementación tiene por objetivos los siguientes aspectos:

- Conocer a la empresa desde su visión, misión, valores y los principales objetivos y productos o servicios que ofrece a sus clientes.
- Identificar los procesos de toda la organización.
- Definir los procesos o actividades clave de la empresa.
- Identificar los posibles riesgos sobre los procesos críticos del negocio.
- Identificar el impacto ante una posible amenaza materializada en el tiempo. (Deloitte, 2015)

6.3.1 Análisis de procesos de negocio

En este apartado se identifica los procesos de la organización. Es importante identificar los responsables de cada actividad y de qué manera son sus interrelaciones entre sí. Así mismo, se deberá considerar los proveedores que brindan soporte a procesos clave dentro de la empresa.
El primer punto a considerar en esta actividad es tener claro el giro del negocio, esto será vital para identificar los procesos de la organización. Es necesario mapear los procesos estratégicos, de soporte y los procesos agregadores de valor de la empresa. Esta información nos permitirá identificar de forma ágil los procesos que son considerados críticos para la compañía.

Más adelante servirá para definir a través la definición de los procesos que son considerados importantes dentro del giro de la empresa, las prioridades de

recuperación cuando se presente una falla tecnológica o un evento catastrófico en donde la institución se vea afectada en sus actividades diarias.

6.3.2 Análisis de Impacto

Una vez se cuente con los procesos críticos dentro del giro de negocio de la organización, es necesario identificar y medir el impacto que la empresa tendrá debido a alguna interrupción cualquiera sea el tipo.

En este contexto, la empresa debe definir el tiempo máximo permitido de interrupción de sus siglas en inglés MTD. Esta medida permite establecer el tiempo máximo que la compañía puede dejar de operar sin tener pérdidas económicas o de imagen. (Deloitte, 2015)

A continuación se presenta un ejemplo para obtener el tiempo máximo permitido en un proceso de negocio de una empresa.

Figura 38. MTD proceso de nómina.
Tomado de Guía práctica para Pymes: cómo implantar un plan de negocio, 2015

El establecimiento del tiempo máximo de interrupción dependerá de las necesidades de cada empresa. En este estudio se realizaron reuniones con cada responsable de los procesos críticos definidos previamente. En estas reuniones, se identificaron las principales actividades de cada proceso. Así mismo, los componentes y servicios tecnológicos que soportan dichos procedimientos.

Con esta información como principales insumos, se realiza una revisión y validación de los diferentes tiempos de recuperación. El objetivo principal es identificar el tiempo máximo de recuperación de acuerdo a las operaciones de la empresa.

6.3.3 Identificar prioridades de recuperación

Una vez se disponga el mapeo total de la organización, su razón de ser, sus objetivos y procesos, se identifican los procesos críticos de negocio. Dichos procesos son todas las actividades que si en un periodo de tiempo no se las ejecuta la compañía pierde dinero y con ello reputación y clientes. (Deloitte, 2015)

Para cada proceso crítico de la organización es necesario identificar los recursos que ayudan o soportan la correcta ejecución de estas actividades. Se entiende como recursos los siguientes ítems:

- Talento humano.
- Infraestructura.
- Tecnología. (Deloitte, 2015)

La siguiente figura muestra a través de una validación de los recursos críticos de un proceso en específico. La clasificación de prioridad de recuperación es cualificada entre los siguientes criterios: Prioridad baja, cuyos recursos no tienen mayor afección en caso de presentar problemas; prioridad media, cuyos recursos son de consideración y finalmente prioridad alta, en donde se centrará la mayor atención a dichos recursos y procesos para considerar en el plan de continuidad de negocio.

A continuación ejercicio de priorización de actividades críticas de la empresa.

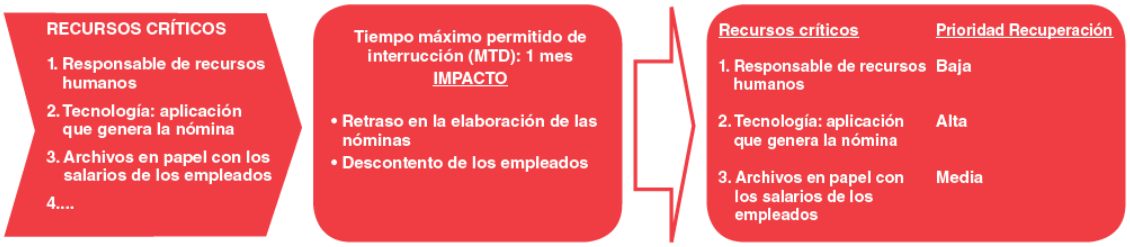

Figura 39. Priorización de recuperación.
Tomado de Guía práctica para Pymes: cómo implantar un plan de negocio, 2015

La herramienta que abarcará toda esa información se denomina BIA o Análisis de Impacto de Negocio. Cabe destacar que existen otros parámetros para la medición del tiempo en referencia a recuperación del negocio. El primero es el RTO que es el tiempo de recuperación objetivo y el RPO que indica el punto de recuperación objetivo. (Deloitte, 2015)

6.3.4 Análisis de riesgos

La siguiente actividad tiene como finalidad principal identificar las diferentes amenazas que los procesos tienen al mantenerse dentro de una normal operación. Así mismo, se identifican las vulnerabilidades de los servicios y componentes tecnológicos que soportan dichos procesos críticos de la organización. Es necesario cualificar o cuantificar para valorar el impacto cuando una amenaza se materialice. (Deloitte, 2015)

Finalmente se realiza una clasificación de amenazas o vulnerabilidades detectadas para disponer de información que sirva para la toma de decisiones de acuerdo a distintos parámetros de evaluación y control de los riesgos.

A continuación se muestra un ejemplo de valoración de la probabilidad por el impacto.

Impacto	**Alto**	*Severo*	*Alto*	*Crítico*
	Medio	*Medio*	*Grave*	*Alto*
	Bajo	*Insignificante*	*Medio*	*Severo*
		Bajo	**Medio**	**Alto**
		Probabilidad		

Figura 40. Clasificación de riesgos.

6.4 Fase III: Medidas de prevención.

La tercera fase consiste en establecer las diferentes actividades y medidas de seguridad que eviten que un riesgo se materialice. El objetivo principal es que si la empresa se ve afectada por algún evento que no se controló en su debido momento, el plan de contingencia no sea activado de forma inmediata. En su lugar, la empresa debe disponer de varias medidas de prevención. (Deloitte, 2015)

6.4.1 Medidas de seguridad

Para la definición de las medidas de seguridad, se toma como base el análisis de impacto de negocio. Esta actividad busca implementar procedimientos y controles de seguridad que pueden apoyar con los siguientes puntos:

- Reducir la probabilidad de materialización de un riesgo.
- Reducir el tiempo de interrupción de un proceso crítico de la organización.
- Reduzcan el impacto hacia la organización cuando un riesgo se materialice en un proceso core de la compañía.
- Aumenten la eficiencia de los procesos al implementar controles y medidas de seguridad. (Deloitte, 2015)

6.5 Fase IV: Estrategias de recuperación.

La cuarta fase nace con el establecimiento del análisis de impacto de negocio y en el análisis de riesgos en base a los procesos críticos que la organización ha definido anteriormente.

Las estrategias de recuperación deben alinearse a las necesidades puntuales de la compañía. El objetivo principal es determinar las estrategias que la empresa debe optar para evitar pérdidas cuantiosas de dinero que afecten a su integridad y la confianza de los clientes.

6.5.1 Alternativas de recuperación

La estrategia de recuperación que establezca la organización debe ajustarse a las necesidades y requerimientos puntuales que así lo exige su giro de negocio.

Para ello debe considerar los siguientes aspectos:

- Los beneficios de cada estrategia de recuperación.
- Flexibilidad de adaptarse al cambio.
- Tiempo máximo permitido de interrupción.
- Tiempo de recuperación permitido.
- La cantidad de información máxima que está la dispuesta la empresa a asumir. (Deloitte, 2015)

Es importante mencionar que el costo de la estrategia de recuperación fluctuará alrededor de los tiempos de recuperación que requiera la organización. Es decir, a menor tiempo de recuperación que necesita la empresa; mayor será el impacto en costo.

En este estudio, la alta gerencia de la Zona de distribución del Aeropuerto Mariscal Sucre ha seleccionado una sola estrategia de recuperación. La alta gerencia apuesta por disponer un sitio alterno basado en la nube que le permita establecer los componentes y servicios tecnológicos que soportan al proceso core de la organización que en este caso son las operaciones del Aeropuerto en Quito.

6.6 Fase V: Implementación del plan de Continuidad de Negocio.

La quinta fase de esta guía es la implementación del plan de continuidad de negocio. Tras realizar el análisis pertinente de la empresa y disponer de un plan a detalle, el siguiente paso es ponerlo en operación dentro de la organización.

Esta fase buscar conseguir dos objetivos específicos. El primero es asegurar la continuidad de las actividades críticas de la compañía, en donde se debe salvaguardar que el plan de continuidad dispone de los recursos necesarios sean

estos humanos o equipos estén disponibles desde la activación del plan hasta volver a la operación normal de los procesos de la empresa. (Deloitte, 2015)

El segundo y último objetivo de esta quinta fase es gestionar la respuesta de incidentes, que hace referencia a disponer eventos de alertas ante situaciones o actividades fuera de lo normal que puedan afectar a los procesos críticos de la organización y que la empresa sea vea en la situación de poder enfrentarlos. (Deloitte, 2015)

6.6.1 Procedimientos de actuación

La implementación del procedimiento de actuación será desarrollada por el responsable del plan de continuidad. El objetivo es disponer un instrumento detallado en donde indica con claridad el momento en que es necesario activar el plan de continuidad de negocio. Esto ayuda a disminuir la incertidumbre de los responsables de ejecución del plan, los tiempo de respuesta para poner en práctica el plan y principalmente reduce la preocupación de los clientes por verse afectado los procesos críticos de la organización. (Deloitte, 2015)

Dicho procedimiento considerará los siguientes aspectos:

- Situaciones específicas para activar la operación del plan de continuidad de la empresa.
- Detalle de los procesos y actividades críticas que deberán ser recuperados.
- Detalle de los tiempos de recuperación de dichos procesos críticos.
- Responsable de cada actividad dentro del plan de continuidad.
- Detalle de proveedores clave, cadena de llamadas, entre otros. (Deloitte, 2015)

6.7 Fase VI: Mantenimiento y Mejora Continua.

Así mismo, se debe promocionar en todos los empleados una cultura sobre procesos continuos bajo una mejora continua.

6.7.1 Socialización del plan

La primera actividad en esta fase es conocer el grupo al que va a llegar la información de que la Zona de Distribución cuenta con un plan de continuidad de negocio. De acuerdo al análisis de stakeholders que realice la empresa se definirán estrategias para llegar a los clientes seleccionados o a todos los clientes.

Los medios de difusión de información serían los siguientes:

- Correo electrónico.
- Publicidad en internet.
- Redes sociales.
- Contenido en la intranet.
- Publicidad en página web institucional. (Deloitte, 2015)

La Zona de Distribución deberá considerar en su presupuesto paquetes formativos y de capacitación continua para el responsable y todo el equipo que está a cargo de la continuidad del negocio.

6.7.2 Pruebas

Una vez que el plan de continuidad de negocio se ha desarrollado, implementado y los empleados están conscientes de su importancia se recomienda disponer de un plan de ejecución de pruebas que permita:

- Validar el correcto funcionamiento del plan de continuidad de negocio.
- Validar que el equipo y responsable del plan dispongan el nivel de experiencia adecuado. Adicional, poseen las capacitaciones suficientes para estar frente a un programa de tal impacto como es la continuidad del negocio.
- Identificar los tiempos de respuesta de la ejecución de cada actividad dentro del plan. (Deloitte, 2015)

La siguiente ilustración describen los tipos de pruebas que se pueden aplicar de acuerdo a las necesidades de la empresa.

Tipos de pruebas del Plan de Continuidad de Negocio

(-) COMPLEJIDAD (+)

Tipo de prueba	Descripción
Test de consistencia	El plan de continuidad de negocio es distribuido a los departamentos y/o áreas funcionales implicadas para su revisión/actualización.
Test de validez	Representantes de cada departamento y/o área funcional implicada se reúnen para revisar y discutir el plan.
Test de simulación (simulacro)	Escenario ficticio de recuperación para verificar que el Plan de Continuidad contiene la información necesaria y suficiente.
Test actividades críticas	Recuperación real de una actividad crítica bajo un entorno controlado y sin poner en peligro la operativa usual/original.
Test completo	Interrupción real de las operaciones y recuperación de las mismas a través de los procedimientos del Plan de Continuidad.

Figura 41. Tipos de pruebas del plan de continuidad.
Tomado de Guía práctica para Pymes: cómo implantar un plan de negocio, 2015

6.7.3 Mejora continua

Disponer un proceso de pruebas bien estructurado brinda la oportunidad de que el plan entre en una etapa de mejora continua. Cabe destacar que si a nivel estratégico la organización se plantea una nueva meta, todos estos cambios deberán ser considerados dentro del plan de continuidad de negocio.

7. CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones.

Basarse en varias metodologías y marcos de referencia dio como resultado un modelo más robusto. Esta estrategia utilizada en este estudio ha facilitado disponer de una guía de implementación en donde existe un alineamiento desde los objetivos hasta los servicios y componentes tecnológicos disponibles por la organización.

Al momento de realizar el entendimiento de la empresa a través de entrevistas con los dueños de cada proceso, se obtuvo como resultado que la empresa cuenta con documentación a detalle de todas actividades del giro del negocio e indicadores de cada área. Así mismo, el departamento de tecnología dispone un mapa con todos los servicios y componentes que soportan los procesos de la organización. Un punto a consideración es que la mayoría de los procesos del negocio son apalancados por sistemas que automatizan y hacen más eficientes las actividades diarios de la compañía. Se determinó que del total de procesos, un 80% se encuentra automatizado.

Se pudo evaluar que Gerencia General tiene serias preocupaciones en referencia a la continuidad de los procesos críticos de la Zona de Distribución. De la misma manera, no existe un entendimiento técnico sobre los planes de contingencia ni de su implementación.

Los análisis de riesgos realizados tanto a los procesos, servicios y componentes tecnológicos; dio como resultado una visión global de las vulnerabilidades que presenta la empresa. Esto dio lugar a que dichas debilidades puedan ser evaluadas y gestionadas de forma integral con el fin principal de minimizar su impacto y mejorar la disponibilidad de los servicios que ofrece la Zona de Distribución.

Un aspecto clave que resultó de este estudio, fue el análisis de impacto de negocio. Este análisis permitió conocer a la organización a profundidad. Es así que, mediante esta herramienta se tuvo como resultado un acercamiento real de los tiempos de recuperación para la que organización no se vea afectada en de forma económica o en imagen que pueda llevarle a perder la concesión dentro del Aeropuerto Internacional Mariscal Sucre.

Las estrategias de recuperación son realmente importantes y tras haber obtenido un análisis de impacto a detalle se pudo definir diferentes estrategias que se encuentran focalizadas hacia los objetivos de la empresa y principalmente con los intereses de la alta gerencia y sus inversionistas. Es importante mencionar que, en este punto del estudio se tuvo como resultado un alineamiento estratégico de los procesos, riesgos, escenarios de riesgos y los diferentes servicios y componentes tecnológicos.

La implementación de un sitio de contingencia basado en la nube es un proyecto que tiene su grado de complejidad. Este proyecto involucra varias aristas a considerar como son: concientización de la importancia de los procesos y responsabilidades de cada grupo de trabajo del plan de contingencia, comunicación con el centro alterno, entre otros. Para esto se necesita apoyo directo de la alta gerencia lo que permitirá conseguir que el proyecto salga a flote, dure a través de los años y disponga un mejoramiento continuo.

7.2 Recomendaciones.

Como se había mencionado anteriormente, el análisis de impacto de negocio es un hito importante dentro del plan de continuidad de negocio. En este contexto, es de suma importancia validar los tiempos que la Zona de Distribución puede trabajar sin el apalancamiento de los servicios tecnológicos sobre sus procesos críticos. Estos tiempos serán considerados más adelante para plantear estrategias de recuperación que sea eficiente y alineada con las necesidades planteadas en este análisis.

Se recomienda que el plan de continuidad de negocio de la Zona de Distribución debe ser difundido a todo nivel. Esto permitirá que los empleados y principalmente los responsables del plan conozcan las actividades que se deben ejecutar y en el tiempo debido. Adicional, se recomienda hacer publicidad del plan de continuidad de negocio a los principales stakeholder externos que disponga la organización.

Las pruebas dentro del plan de continuidad de negocio tienen su razón de ser. Es por ello que se recomienda se plantee pruebas estrictas que validen el correcto funcionamiento del plan. Esto permitirá disponer un entrenamiento de las actividades a realizar y por sobre todo, disponer de información la cual podrá ser utilizada en instancias futuras para una mejora continua de los procesos de contingencia. A su vez, se recomienda que a través del plan de pruebas se valide la operatividad y disponibilidad del centro alterno con sus prestaciones al 100% en el caso de su activación.

REFERENCIAS

Allen Chris, 2018. Estadísticas de recuperación ante desastres de 2018 que impactarán a los propietarios de negocios. Recuperado el 01 de abril de: https://phoenixnap.com/blog/disaster-recovery-statistics

Amazon Web Services Inc., 2018. Tipos de cloud computing. Recuperado el 06 de marzo de 2019 de: https://aws.amazon.com/es/types-of-cloud-computing/

Ballester José, 201. Gobierno Corporativo TIC

Becerra José, 2018. Las 12 preocupaciones importantes de TI a resolverlas. Recuperado el 15 de enero de 2019 de: http://cio.com.mx/las-12-preocupaciones-importantes-las-ti-resolverlas/

BSI Group, 2014. Measurement matters. The role of metrics in ISO 22301.

Carey Scot, 2018. Tendencias de nube pública para 2018. Recuperado el 06 de marzo de 2019 de https://www.computerworld.es/tecnologia/tendencias-de-nube-publica-para-208

Casillas Mireya, 2018. ¿Qué es un DRP? Recuperado el 18 de marzo de 2019 de https://inbest.solutions/que-es-un-drp/

CGMA, 2016. Business Continuity Management – Key Strategies and Processes.

Deloitte, 2015. Guía práctica para Pymes: cómo implementar un Plan de Continuidad de Negocio.

Ferrer Rodrigo, 2015. Metodología para la Gestión de la Continuidad del Negocio.

Greenhill Alison, 2017. Business Continuity Management Policy Statement and Strategy 2018

Hamidovic Haris, 2011. Fundamentos del Gobierno de TI basados en ISO/IEC 38500

Hollman Ellis, 2013. ITSCM (IT Service Continuity Management) Overview: ITIL®'s IT Disaster Recovery and Business Continuity Management

INONI, 2017. Measuring BCM

Isaca, 2012. COBIT 5 Procesos Catalizadores. EEUU: Isaca.

Isaca, 2012. COBIT 5 Un Mar de Negocio para el Gobierno y la Gestión de las TI de la Empresa. EEUU: Isaca.

ISO 22301, 2015. Societal Security - Business Continuity Management Systems - Requirements.

ISO, 2012. International Standard ISO 22301 Societal Security. Business Continuity Management Systems – Requirements, Primera Edición. Recuperado el 10 de diciembre de 2018 de www.iso.org

Krell Eric, 2006. Business Continuity Management

Puricica Cristian, 2018. Desmitificando los Objetivos de Recuperación. Recuperado el 01 de abril de 2019 de https://www.veeam.com/blog/es-lat/rto-rpo-definitions-values-common-practice.html

Quevedo Jesús, 2012. Revisión de modelos de gestión de continuidad del negocio

Ríos Sergio, 2015. Manual ITIL v3

Rivas Génesis, 2018. ITSCM: ¿Qué tan importante es la Gestión de Continuidad para tu empresa?

Simmon Eric, 2018. Evaluation of Cloud Computing Services Based on NIST SP 800-145

St-Germain René, 2014. ISO 22301 Societal Security Business Continuity Management Systems.

Tecnologías con Clase Mundial, 2016. El mapa General de ITIL v.3 – Conceptos clave

Universidad Tec de Monterrey, 2012. Conceptos básicos para la certificación en ITIL®v3

Velker Arthur, 2018. Los mejores consejos para la gestión de la continuidad del negocio. Recuperado el 05 de abril de 2019 de https://irishtechnews.ie/top-tips-for-business-continuity-management-in-2018/