Metodología para determinación de los tiempos objetivos de recuperación RTO de los activos de información críticos en una estrategia de continuidad de negocio BCP en el sector de servicios en Colombia.

Sergio Andrés Durán Vásquez

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2022

Metodología para determinación de los tiempos objetivos de recuperación RTO de los activos de información críticos en una estrategia de continuidad de negocio BCP en el sector de servicios en Colombia.

Sergio Andrés Durán Vásquez

Tesis o trabajo de investigación presentado como requisito parcial para optar al título de:

Magister en Seguridad informática

Director:

Msc, Andrés Alberto Gómez Acosta

Codirector:

PhD, Juliver de Jesús Gil Herrera

Instituto Tecnológico Metropolitano

Facultad de ingeniería

Ciudad, Colombia

2022

“Nunca se pierde el esfuerzo que ponemos para lograr algo hermoso”.

Hellen Keller

Agradecimientos

Quiero agradecer a Dios, a mis padres y mis hermanos, especialmente a mi hermano Javier Mauricio Durán Vásquez por el apoyo y acompañamiento en el correcto desarrollo de esta tesis, mi novia Johana Galeano y mi hijo Miguel Ángel Durán Galeano, ya que han sido un pilar importante de apoyo y motivación para realizar todas mis metas y proyectos. Dedico este trabajo y cada uno de mis esfuerzos a ellos. Agradezco a mis amigos por el acompañamiento y apoyo incondicional en todos los procesos de aprendizaje y celebración de cada logro.

Resumen

En la actualidad, el sector de servicios está expuesto a diversos riesgos en sus sistemas de información, para lo cual, en muchos casos no se está preparado, lo que ocasiona que este sector sea vulnerable ante a las diversas amenazas que tiene el medio digital. Este proyecto propone una metodología basada en estándares internaciones, que busca facilitar la optimización de los tiempos objetivos de recuperación, con el fin de conservar la disponibilidad de los activos de información. Lo anterior, se realiza una investigación que se estructura por capítulos, primero se aborda el contexto de la tesis, seguido por el estado del arte que permite tener un panorama general de los términos utilizados, luego la caracterización de los activos de información y del sector servicios. Se realiza el análisis de estándares internacionales y metodologías existentes, cuyas bases fundamentaron la metodología propuesta en función de la disponibilidad de los servicios que se generan a partir de los activos de información. Definida la metodología se procede a construir una herramienta informática orientada a la web que permite conocer los tiempos de recuperación, además de recomendaciones de buenas prácticas para el sector.

Palabras clave: Activos de información, Ataques informáticos, BCP, DRP, RPO, RTO, SGSI en Colombia, Vulnerabilidades tecnológicas.

Abstract

Nowadays, companies from the service sector are exposed to different kinds of security information risks and in most of the cases they are not even prepared to face them. This situation causes this sector to be vulnerable to diverse threats that arise in the digital environment everyday. This project proposes a methodology based on international standards, which seeks to facilitate the identification of recovery time objectives (RTO) for each information asset, in order to preserve its availability as much as possible for the business to continue. Firstly, this thesis presents the whole business continuity and risks context, secondly we take a look at the state of art that allows us to have an overview of the terminology that is used, afterwards we present a set of features that can characterize information assets according to its criticality in the service sector, and then an analysis of international standards and existing methodologies is conducted so then it is proposed a methodology for information assets with availability requirements. Once the methodology was defined, we proceeded to build a web tool that allows us to calculate recovery time objectives (RTO), as well as recommendations of good practices for the sector.

Keywords: Information assets, IT attacks, BCP, DRP, RPO, RTO, ISMS in Colombia, Technological vulnerabilities.

Contenido

Pág.

Resumen **5**

Lista de figuras **10**

Lista de tablas **12**

Estructura general de la tesis **13**

1. Introducción **15**
1.1 Objetivos 19
1.1.1 Objetivo General 19
1.1.2 Objetivos Especificos 20

2. Marco Teorico y Estado del Arte **21**
2.1 Marco teorico 21
2.1.1 Sector Servicios en Colombia 22
2.1.2 Información 22
2.1.3 Sistemas de Información 23
2.1.4 Riesgos Informáticos 23
2.1.5 Ataques Informáticos 23
2.1.6 Activos de Información 24
2.1.7 Servidor Aplicaciones 25
2.1.8 Servidor Bases de Datos 26
2.1.9 Servidor de Correo Electrónico 26
2.1.10 Cortafuegos(Firewall) 27
2.1.11 Equipos de Cómputo 27
2.1.12 Telefonía IP / Dispositivos Móviles 27
2.1.13 Planta Telefónica 27
2.1.14 Switches 28
2.1.15 Enrutador (Router) 28
2.1.16 Repetidores (Access Point) 28
2.1.17 Cámaras de Seguridad 28
2.1.18 Seguridad Informática 28
2.1.19 Punto Objetivo de Recuperación (RPO) 29
2.1.20 Tiempo Objetivo de Recuperación (RTO) 29
2.1.21 Tiempo de Recuperación Actual o Real (RTA) 29
2.1.22 Planificación de Continuidad del Negocio (BCP) 30
2.1.23 Disponibilidad de datos 30
2.1.24 Ciclo de gestión PHVA 30
2.2 Estado del arte 30

3. Metodología del desarrollo de la investigación y Resultados **30**

3.1 Clasificación de empresas del sector servicios en Colombia 32
3.2 Sector Servicios 33
3.2.1 Procesos del sector servicios 35
3.3 Niveles de Criticidad 36
3.3.1 Impacto Financiero 38
3.3.2 Impacto Operacional 38
3.3.3 Impacto Legal 39
3.3.4 Impacto Reputacional 39

4. Evaluación y clasificación de métricas adecuadas en la identificación de los puntos objetivos para el cálculo de tiempos de recuperación sobre cada activo, identificando el patrón de criticidad 40
4.1 Descripción de métricas para activos de información 40
4.2 Clasificación de Impactos sobre activos de información 42
4.3 Resultados del análisis. 42
4.4 Definición de Metodologías y normas existentes para el análisis RTO 48
4.4.1 Gestión de riesgos 49
4.4.1.1 ISO 22301 49
4.4.1.2 DAFP versión 4 49
4.4.1.3 Nist 800-30 Rev.1 - Guía de gestión de riesgos para sistemas de tecnología de la información 49
4.4.1.4 OCTAVE 50
4.4.1.5 MAGERIT 50
4.4.1.6 ISO 27005:2018 51
4.4.1.7 ISO 31000 51
4.5 Análisis de controles de seguridad de la información para la continuidad de negocio .. 52
4.6 Análisis de metodologías 52
4.6.1 Metodología para el diseño de un plan de recuperación ante desastres o DRP 52
4.6.2 Metodología de análisis y gestión de riesgos de los sistemas de información 53
4.6.3 Metodología para la gestión de la Continuidad de Negocio 54
4.6.4 Metodología del análisis de impacto del negocio 55

5. Validación de metodologías sobre caso de estudio en Empresa de servicios del Valle de Aburra 56
5.1 Descripción del negocio 56
5.2 Diagnóstico Inicial 56
5.3 Implementación de las metodologías 57
5.4 Conclusiones y aplicabilidad de las metodologías 58

6. Metodología para determinación de los tiempos objetivos de recuperación RTO de los activos de información críticos en una estrategia de continuidad de negocio BCP en el sector de servicios en Colombia 60
6.1 Técnica definida para la investigación 60
6.2 Análisis de normas y metodologías de continuidad de negocio 60

6.2.1 Resumen y conclusiones de análisis de metodologías 61
6.3 Propuesta de metodología para determinación de los tiempos objetivos de recuperación RTO de los activos de información críticos en una estrategia de continuidad de negocio BCP en el sector de servicios en Colombia 62
6.3.1 Desarrollo 62
6.3.2 Guía y desarrollo de la metodología propuesta 65
6.3.2.1 Fase Planear: Diagnostico Organizacional 66
6.3.2.2 Fase Hacer 67
6.3.2.3 Fase Verificar 68
6.3.2.4 Fase Actuar 68
6.3 Análisis de la metodología propuesta en caso de estudio (Empresa Valle de Aburra) ... 69

7. Construir una herramienta informática, de acuerdo con la metodología diseñada, que proponga recomendaciones, alertas y planes de acción sobre el activo crítico, permitiendo dar continuidad al negocio y adoptando buenas prácticas en Seguridad Informática para la disponibilidad del servicio 80
7.1 Componentes Hardware 81
7.2 Componentes Software 81
7.3 Desarrollo Herramienta Informática 81
7.4 Diseño Herramienta 82

8. Conclusiones y recomendaciones 92
8.1. Conclusiones 92
8.2. Recomendaciones 95

9. Bibliografía 98

Lista de figuras

Pág.

Figura 0-1: Estructura general de la tesis……2

Figura 1-1: Causas de activación del BCM (Business Continuity Management) en porcentaje. [60]…… 17

Figura 1-2: Causas de activación del BCM (Business Continuity Management) según IBM. [60]……18

Figura 1-3: Aceleración de crecimiento tecnológico ante la crisis del COVID 19 según IBM. [63]……19

Figura 3-1: Crecimiento del Sector de Servicio [26]……37

Figura 3-2: Actividades Económicas del Sector Servicios [27] ……38

Figura 3-3: Procesos genéricos dentro del sector servicios. [28] ……39

Figura 4-1: Clasificación de métricas según aplicabilidad a los activos de información. Construcción Propia……44

Figura 4-4: Nivel de criticidad de activos de información críticos según el impacto en la organización……49

Figura 4-5: Metodología para un plan de recuperación ante desastres o DRP. (Metodología 1) [55]……56

Figura 4-6: MAGERIT (Metodología de análisis y gestión de riesgos de los sistemas de información.) (Metodología 2) [56] ……57

Figura 4-7: Metodología para la gestión de la Continuidad de Negocio. [57]……57

Figura 4-8: Metodología del Análisis de Impacto del Negocio [29]……58

Figura 4-9: Evaluación comparativa de metodologías para la adquisición de consideraciones clave para la definición de un RTO.]……58

Figura 4-10: Comparativo de normas internacionales …. …. …. ……58

Figura 6-1: Ciclo PHVA[59]……66

Figura 6-2: Metodología propuesta para la determinación de los tiempos objetivos de recuperación RTO. Construcción Propia……71

Figura 7-1: Etapas clave del proceso de construcción de la herramienta informática……81

Figura 7-2: Arquitectura de la herramienta informática.....82
Figura 7-3: Fases del proceso de construcción de la herramienta informática. Construcción Propia.....83
Figura 7-4: Pregunta tipo de activo critico de información que tiene la organización. Construcción Propia.....84
Figura 7-5: Pregunta tipo de servicio que presta la organización al comercio. Construcción Propia.....84
Figura 7-6: Pregunta la cual planeta un porcentaje si el activo no está disponible y los servicios presentan ausencia operativa. Construcción Propia.....85
Figura 7-7: Pregunta de la cantidad de tiempo tolerable en que puede estar indisponible el activo. Construcción Propia.....86
Figura 7-8: Pregunta cantidad de información en Gigabytes que contiene el activo de información. Construcción Propia.....86
Figura 7-9: Pregunta sobre donde se almacenan los diversos Backups del activo de información. Construcción Propia.....87
Figura 7-10: Pregunta sobre el promedio de tiempo en que se le notifica al cliente la ausencia o indisponibilidad del servicio que presta un activo de información. Construcción Propia.....88
Figura 7-11: Pregunta sobre la frecuencia en que se realizan las copias de seguridad de la información contenida sobre el activo. Construcción Propia.....88
Figura 7-12: Pregunta sobre el ancho de banda que tiene el internet donde se realizaría el proceso de restauración. Construcción Propia.....89
Figura 7-13: Pregunta sobre el ancho de banda que tiene el internet donde se realizaría el proceso de restauración. Construcción Propia.....90
Figura 7-14: Pregunta basada en el conocedor del activo de información, luego de tener los Backups o copias de seguridad cuanto puede tardar en restablecerse o restaurar dicha información y así dando disponibilidad al servicio. Construcción Propia.....90
Figura 7-15: Resultados del cuestionario en tiempo, permitiendo tener un dato aproximado de cuando puede ser el RTO al momento de una indisponibilidad de los activos críticos. Construcción Propia.....91

Lista de tablas

Pág.

Tabla 2-1: Vida útil Activos de Información. [30] Construcción Propia.....24

Tabla 2-2: Análisis de trabajos relacionados. Construcción Propia.....30

Tabla 3-1: Ley 590 del 2000. Marco de acción para la pequeña y mediana empresa. [25].....36

Tabla 3-2: Valor de criticidad del activo de información en disponibilidad. [29] 40

Tabla 3-3: Criterios de clasificación de los pilares en la gestión de la información.[29].....40

Tabla 3-4: Niveles Clasificación. [49].....41

Tabla 4-1: Definición de métricas aplicables activos de información. Construcción Propia.....42

Tabla 4-2: Evaluación de métricas con respecto a los activos de información. Construcción Propia.....43

Tabla 4-3: Métrica Impactos Financieros [42] 45

Tabla 4-4: Métrica Impactos Operacional. [42].....46

Tabla 4-5: Métrica Impactos Legales o Íntegros [42] 46

Tabla 4-6: Métrica Impactos Reputacionales [42] 47

Tabla 4-7: Clasificación de activos según nivel de criticidad con respecto al impacto. Construcción propia.....48

Tabla 4-8: Rangos de tiempo en recuperación de la disponibilidad de los activos. (RTO) [42].....49

Tabla 5-1: Algunas características del sector servicios. Construcción Propia.....60

Tabla 5 2: Aplicabilidad y validación de las metodologías sobre las características del sector servicios en función del caso de estudio.....62

Tabla 6-1: Ciclo PHVA (Fase Planear) Metodología Propuesta... Construcción Propia.....74

Tabla 6 2: Ciclo PHVA (Fase Hacer) Metodología Propuesta...Construcción Propia.....75

Tabla 6 3: Ciclo PHVA (Fase Verificar) Metodología Propuesta...Construcción Propia.....77

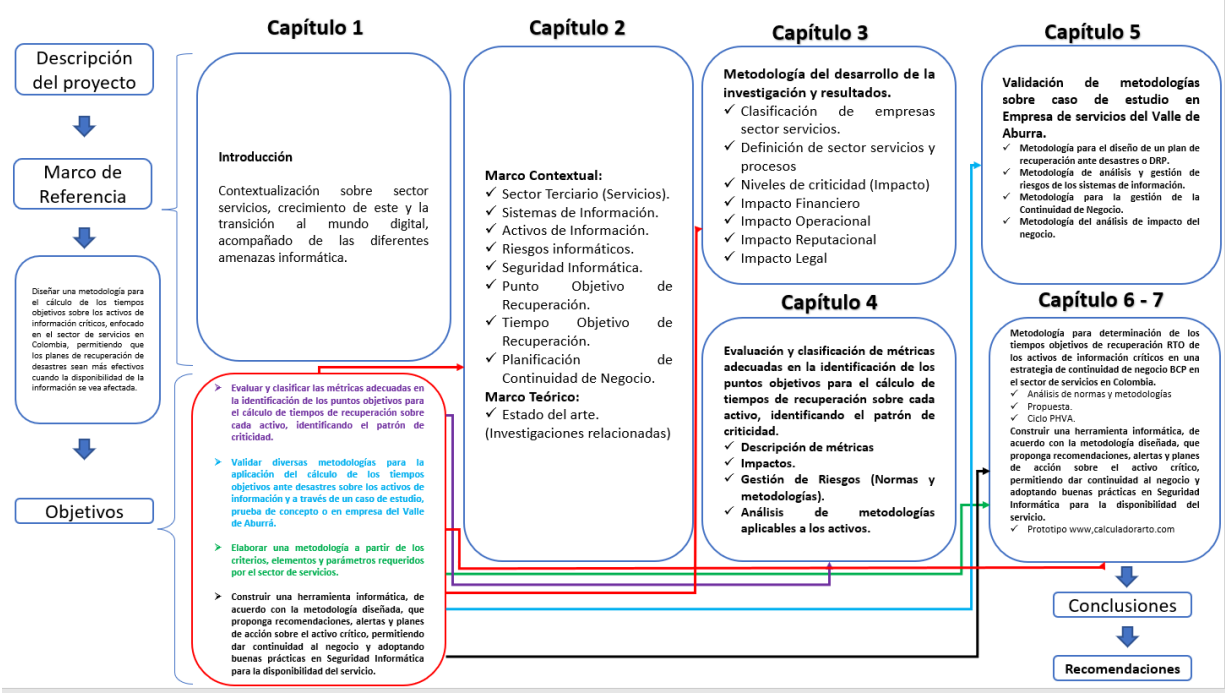
Tabla 6 4: Ciclo PHVA (Fase Actuar) Metodología Propuesta....Construcción Propia.....78

Estructura general de la tesis

La presente figura resume el proceso de esta tesis de maestría descrita en 7 capítulos.

Figura 0-1:

Estructura general de la tesis.



Autor: Construcción Propia.

Esta tesis está ordenada de forma que en el capítulo 1 se desarrolla una introducción y contextualización del tema a tratar y se incluye información de valor para una mejor interpretación de lo relacionado con la continuidad de negocio. Continúa con el capítulo 2 que presenta un marco teórico sobre las características más relevantes del sector terciario de la economía, conceptos de riesgos, punto objetivo de recuperación y presenta un estado del arte sobre investigaciones relacionadas en Colombia y el mundo.

En el capítulo 3 se presenta la metodología de investigación y la forma en que se obtienen los diferentes resultados de esta tesis.

Seguidamente se aborda el capítulo 4 que contiene el proceso de identificación, evaluación y clasificación de métricas para cada activo de información, esto con el fin de identificar los puntos objetivos de recuperación y así identificar un patrón de criticidad.

Luego de identificar todas las características del sector servicios y los activos de información, se construye el capítulo 5 donde se validan las metodologías existentes relacionadas al cálculo de un RTO, haciendo una evaluación de cumplimiento de las características del sector con respecto a la aplicabilidad de la metodología, para tomar características relevantes que permiten construir una nueva metodología optimizada.

Teniendo en cuenta estas etapas, en el capítulo 6 se procede a analizar normas internacionales y metodologías de continuidad de negocio existentes con el fin de construir una metodología optimizada para el cálculo del tiempo objetivo de recuperación dirigida al sector servicios de Colombia, teniendo en cuenta un ciclo PHVA para incorporar la mejora continua en la metodología.

Finalmente, en el capítulo 7 se presenta un análisis y explicación de la herramienta construida en función de la metodología propuesta para ser utilizada por el personal de TI en el sector, luego se presentan conclusiones y recomendaciones de valor para tener en cuenta en el cálculo de los tiempos objetivos de recuperación. De esta forma, se integran todos los resultados y se consigue el cumplimiento del objetivo general al respecto de una metodología para la recuperación de los activos de información del sector servicios cuando la disponibilidad de los activos de información se vea afectada.

1. Introducción

En América latina durante los últimos años la cifra de ciudadanos conectados a Internet ha presentado un incremento considerable, pues representa alrededor del 10% de usuarios de Internet en el mundo (495 millones) el número de usuarios de internet en el mundo ha alcanzado (4.950 millones) [1], y además cuenta con una de las tasas de crecimiento más altas. Lo que hace que las grandes, medianas y pequeñas empresas tengan sus diferentes sistemas de información alojados en la web como en local (Infraestructura propia), para el control y la gestión de sus datos.

Dicho crecimiento genera también un incremento en la exposición a ciberataques, afectando así los sistemas de información de organizaciones de diferentes sectores y tamaños. Colombia hace parte de las cinco economías más grandes de América Latina, donde cada vez que crecen, se tornan más tecnológicamente inteligentes. Un informe publicado por Symantec, un proveedor de productos y soluciones de seguridad alega que el coste de los delitos cibernéticos ha alcanzado 464 millones de dólares en Colombia. [61]

Esto no es de sorprender al ser una de las economías más grandes de América latina ocupando el quinto lugar en el top de economías latinoamericanas [2], además también son las más vulnerables a los ataques cibernéticos. En Colombia las pequeñas, medianas y grandes empresas utilizan sus sistemas de información algunos desarrollados a la medida, otros son software licenciados o software libre genéricos para la gestión y control de la información; lo que hace que estos sistemas de información donde se almacenan grandes volúmenes de datos sean de vital importancia para las organizaciones.

En la actualidad, con la evolución de las nuevas tecnologías de la información los diversos sectores de la sociedad están constituidos por múltiples activos de información además de sistemas de información, los cuales son de gran importancia para la gestión y control de la información. Esto hace que se tenga dependencia a estos equipos, activos o sistemas de información, pero en la actualidad y en nuestra realidad no se está preparado para una suspensión o desastre dentro de

los sistemas o activos de información debido al desconocimiento del RTO (Recovery Time Objective - Punto Objetivo de Recuperación) dentro de la organización.
Sin embargo, a esta evolución tecnológica se suma la existencia de amenazas tecnológicas, sociales o naturales, las cuales pueden ser explotadas por los ciberdelincuentes, teniendo como principal objetivo, atacar la infraestructura tecnológica y sistemas de información, ocasionando suspensión o fallas en los servicios, todo esto con el fin de generar dinero, hacer daño o afectar la reputación. Dichos ataques se realizan buscando vulnerabilidades de las tecnologías y los activos de información, así aprovechan para causar el mayor daño posible.

En los últimos años, algunas entidades a lo largo del territorio nacional han concedido una importancia creciente a la implementación de planes, procedimientos y estructuras que garanticen la continuidad de sus productos y servicios críticos del negocio ante incidentes de diversas categorías y diferentes niveles de impacto. Estos factores, junto con una legislación cada vez más exigente, (Circulares de la Superintendencia Financiera y el Marco de Referencia de Arquitectura de TI, entre otros) en lo relacionado a la confiabilidad y seguridad en la prestación de estos productos y servicios, hacen necesario en la actualidad que se cuente con una GCN (Gestión de la Continuidad de Negocio), con el objetivo de lograr una sociedad cada vez más comprometida con la protección del talento humano, de la disponibilidad de los procesos del negocio, de la información según la ISO 27001:2013 [3] y del conocimiento, de la tecnología, al igual, que con el incremento de la productividad, la agilidad, la efectividad y la eficiencia.[60]

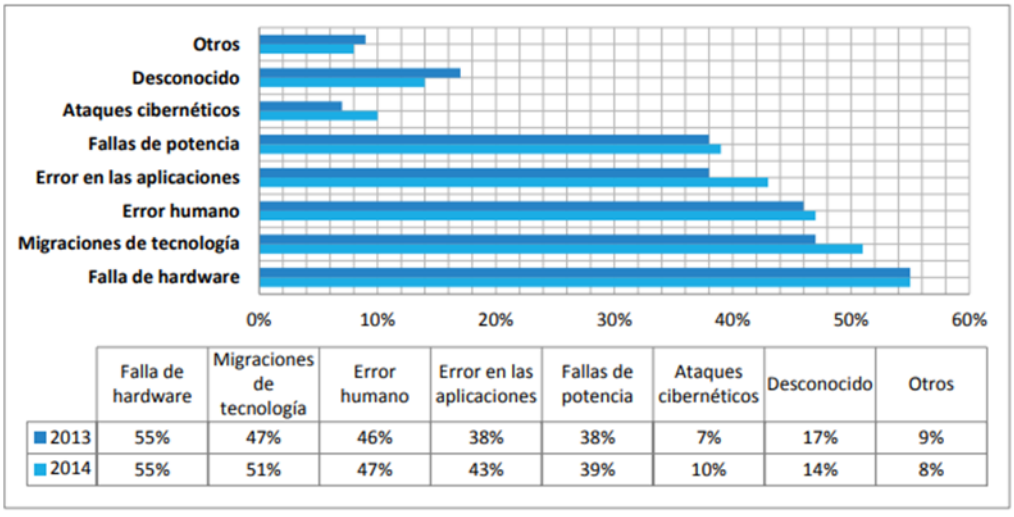
En un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, pero las consecuencias derivadas de sucesos como el terrorismo, la inestabilidad política, las pandemias, la pérdida de empleados claves y el ciberterrorismo, han mostrado la necesidad de incorporar nuevas amenazas en la GCN (Gestión de la Continuidad del Negocio) con el fin de permitir la continuidad de las operaciones ante un escenario cada vez más dinámico en lo relacionado con el tipo de riesgos al que se está expuesto.[60]

Esto es de gran importancia para las organizaciones ya que deben contar con una metodología para la definición de los RTO (Tiempo Objetivo de Recuperación) pues muchas veces es un asunto de

percepción y no está fundamentado en un procedimiento sistemático que realmente le permita al negocio un entendimiento de cuánto tiempo puede soportar inactividad los diferentes activos críticos antes de sufrir consecuencias financieras, reputacional y en general la estabilidad del negocio. De acuerdo con la firma Continuity Software de los Estados Unidos, las fallas a nivel de hardware en los diferentes dispositivos que conforman los sistemas de información, por dos años consecutivos, ha permanecido en el primer lugar de acuerdo con el 55% de los encuestados, le siguen migraciones de tecnología con el 51%; en el 2014, el error humano alcanzó un 47% y las fallas a nivel de las aplicaciones un 43%. Para más información, en la (Figura 1-1), se presentan los resultados completos de la encuesta tanto para el año 2013 como para el año 2014. [60]

Figura 1-1:

Causas de activación del BCM (Business Continuity Management) en porcentaje.



	Falla de hardware	Migraciones de tecnología	Error humano	Error en las aplicaciones	Fallas de potencia	Ataques cibernéticos	Desconocido	Otros
2013	55%	47%	46%	38%	38%	7%	17%	9%
2014	55%	51%	47%	43%	39%	10%	14%	8%

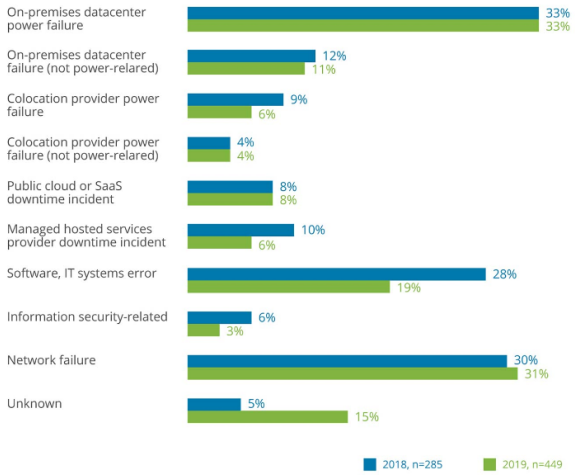
Autor: Rodrigo Ferrer V. [60]

Nota: Según el autor Rodrigo Ferrer V la figura anterior hace referencia a los porcentajes de ocurrencia de las diferentes amenazas por año, se logra observar que año tras año hay un crecimiento de estas. La antigüedad del documento es importante por la proyección que se evidencia en función del crecimiento año tras año [60]

Luego de analizar la situación que se presentó en la (Figura 1-1), se evidencio el crecimiento sobre la tendencia de crecimiento tecnológico y las diferentes fallas que se presentan sobre los activos tecnológicos. Teniendo presente la anterior investigación, se logra visualizar que históricamente que la tecnología ha crecido y adicionalmente en paralelo las fallas, amenazas y vulnerabilidad también van creciendo en paralelo, ya que todas las organizaciones tecnifican sus procesos. A continuación, se presenta en la (Figura 1-2) una actualización de la información y se logra identificar que algunas características aumenten y otras disminuyen en el paso del tiempo, ya que la tecnología constantemente mitiga y resuelve algunas situaciones que presentan los activos. [63]

Figura 1-2:

Causas de activación del BCM (Business Continuity Management) según IBM.



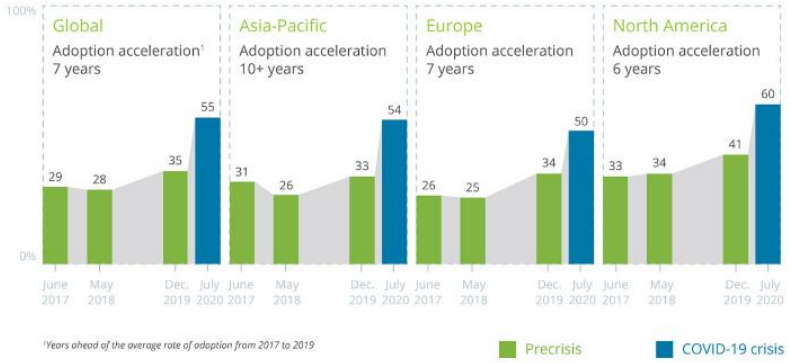
Autor: Infopulse. [63]

Luego de la identificación de las diferentes fallas y situaciones que se presentan sobre los activos de información, se logra visualizar en la (Figura 1-3) el crecimiento exponencial de la tecnología ante la aparición del COVID 19 en el mundo, esto genero un crecimiento tecnológico y con este crecimiento también aumentan las diferentes fallas sobre los activos.

Esto nos hace entender que la tecnología va en crecimiento y las organizaciones deben generar planes de continuidad de negocio y plantear estrategias de restauración o recuperación ante la ausencia de disponibilidad de los activos. Así mitigando los impactos sobre la organización. [63]

Figura 1-3:

Aceleración de crecimiento tecnológico ante la crisis del COVID 19 según IBM.



Autor: Infopulse. [63]

Para el cumplimiento del proyecto se desarrollaron los siguientes objetivos:

1.1. Objetivos

1.1.1. Objetivo General:

Diseñar una metodología para el cálculo de los tiempos objetivos sobre los activos de información críticos, enfocado en el sector de servicios en Colombia, permitiendo que los planes de recuperación de desastres sean más efectivos cuando la disponibilidad de la información se vea afectada.

1.1.2. Objetivos Específicos:

- Evaluar y clasificar las métricas adecuadas en la identificación de los puntos objetivos para el cálculo de tiempos de recuperación sobre cada activo, identificando el patrón de criticidad.
- Validar diversas metodologías para la aplicación del cálculo de los tiempos objetivos ante desastres sobre los activos de información y a través de un caso de estudio, prueba de concepto o en empresa del Valle de Aburrá.
- Elaborar una metodología a partir de los criterios, elementos y parámetros requeridos por el sector de servicios.
- Construir una herramienta informática, de acuerdo con la metodología diseñada, que proponga recomendaciones, alertas y planes de acción sobre el activo crítico, permitiendo dar continuidad al negocio y adoptando buenas prácticas en Seguridad Informática para la disponibilidad del servicio.

2. Marco Teórico y Estado del Arte

A continuación, se presenta el marco teórico y el estado del arte de este trabajo. En la primera parte se abordarán las temáticas más relevantes que aportan a la fundamentación del tema de investigación, en la segunda parte se analizaran diferentes trabajos relacionados, propuestos por investigadores y desarrollado en tópicos similares con el fin de identificar los elementos claves para la determinación y el cálculo de los tiempos objetivos de recuperación sobre los activos de información.

2.2. Marco teórico

Búsqueda de información. Se realizó una indagación a través de diversos motores de búsqueda y bases de datos utilizando métodos activos, los cuales permitieron identificar proyectos y artículos los cuales tuvieran referencia a las palabras clave, RTO (Tiempo Objetivo de Recuperación), RPO (Punto Objetivo de Recuperación), Activos de información, BCP (Planificación de la Continuidad de Negocio).

Encontrando diversas investigaciones en la recuperación de desastres y continuidad de negocio. Con el fin de identificar los riesgos ante un desastre sobre los activos de información críticos dentro de una organización y poder así a través de esta investigación desarrollar una metodología que permita el cálculo de los tiempos objetivos de recuperación y así lograr tener claridad de los tiempos en que se logra la disponibilidad de los activos información y así permitir la continuidad del negocio.

Éste es el soporte conceptual de todo el proyecto de grado, no es un glosario, es una identificación y claridad de los diferentes componentes usados en el desarrollo del proyecto y que permiten dar a conocer (explicar) el proceso recomendado a realizar para la determinación de los tiempos objetivos de recuperación dentro de una estrategia de continuidad de negocio.

2.2.1. Sector Servicios en Colombia.

De acuerdo con el Departamento Administrativo Nacional del Estadísticas de Colombia (DANE), el sector terciario aloja más del 80% de la fuerza laboral del país.

El sector servicios o sector terciario es el sector económico que engloba las actividades de comercio, servicios y transporte, el sector terciario no se encarga de producir sino de ofrecer y distribuir productos. Generar servicios que se ofrecen para satisfacer las necesidades de cualquier población en el mundo. [4]

El sector terciario incluye todas aquellas actividades que se relacionan con la provisión de bienes y servicios a un consumidor. Entre estas se destacan el comercio, las telecomunicaciones, el transporte, la medicina, la salud pública, la educación, el turismo, la administración y las finanzas. [5]

2.2.2. Información.

Es un conjunto de datos con un significado, es decir, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones [6].

2.2.3. Sistemas de Información.

Es un conjunto de datos que interactúan entre sí con un fin común. Ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.

Son importantes porque radican en la eficiencia en la correlación de una gran cantidad de datos ingresados a través de procesos diseñados para cada área con el objetivo de producir información válida para la posterior toma de decisiones.

Son destacados por su diseño, facilidad de uso, flexibilidad, mantenimiento automático de los registros, apoyo en toma de decisiones críticas y mantener el anonimato en informaciones irrelevantes. [7]

2.2.4. Riesgos Informáticos.

Es el conjunto de vulnerabilidades que se representan como una debilidad o fallo de un sistema de información que pone en riesgo la seguridad de la información, su integridad, confidencialidad y disponibilidad, permitiendo que un atacante pueda comprometer o generar daños en la información, por lo que es necesario controlarlas, evitarlas o eliminarlas lo más pronto posible dentro de los riesgos evidenciados. [8]

2.2.5. Ataques Informáticos.

Los ataques son aquellos actos en los cuales se cometen daños, agravios o perjuicios dirigidos a los sistemas computacionales que se encuentran dentro de una red a nivel mundial, o los datos e información que están almacenados en una base de datos. Al enfocarse en los sistemas de información estos buscan la manera de anular el servicio de forma temporal o permanente, implantando algún tipo de virus o dispositivo que captura o secuestra información. [9]

2.2.6. Activos de información.

La norma ISO 27001:2013, define los activos de información como toda organización posee información importante que desea proteger frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta fundamental para la organización es lo que se denomina (Activo) [3].

Y hace referencia de la gran importancia de la integridad, disponibilidad y confidencialidad de los activos de información. Donde se garantice la correcta gestión y control de la información que se maneja en una organización.

Se realiza investigación de los activos de información más comunes con respecto a los procesos y se realiza la descripción de la función de cada uno dentro de la organización y/o empresa en las diversas actividades económicas del sector servicios.

En la organización es importante conocer cuál es la vida útil de cada activo, para ello se procede una investigación sobre la vida útil de los activos de información críticos que nos brinda la información de cuánto tiempo se espera que el activo funcione correctamente, los activos son susceptibles a sufrir desgaste y su valor o costo se amortiza en la medida en que se va desgastando.

Según el artículo 137 del estatuto tributario señala que los activos de computación, redes de procesamiento de datos, equipos de comunicación tienen una tasa de depreciación anual de 20% y una vida útil equivalente a 5 años. [30]

En la (Tabla 2-1) se investiga de acuerdo con el estatuto tributario la vida útil de cada uno de los activos que se utilizan con frecuencia en el sector servicios, esto nos permiten tener otra variable de importancia, para conocer el activo y tener un diagnóstico inicial, que permita tomar acciones correctivas y preventivas con el fin de que se logre conservar la disponibilidad de los servicios.

Tabla 2-1:

Vida útil Activos de Información. [30]

Activos de Información Tecnológicos comunes del Sector Servicios	Vida Útil
Servidor de Aplicaciones	5 Años
Servidor de Bases de Datos	5 Años
Servidor de Correo	5 Años
Firewall	5 Años
Equipos de Computo	5 Años
Teléfonos IP / Dispositivos Móviles	5 Años
Planta Telefónica	5 Años
Switches	5 Años
Routers	5 Años
Repetidores	5 Años
Cámaras de Seguridad	5 Años

Autor: Construcción Propia.

Nota: Se realiza un análisis de la vida útil según el artículo 137 del estatuto tributario para cada tipo de activo.

A continuación, se describe la funcionalidad de cada activo dentro de la organización y se plantea un supuesto para tener mejor claridad de su nivel de criticidad y funcionalidad en la organización y/o empresa.

2.2.7. Servidor Aplicaciones.

En informática, se denomina servidor de aplicaciones a un servidor en una red de computadores que ejecuta ciertas aplicaciones.

Usualmente se trata de un dispositivo de software que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones gestiona información que es consultada, insertada, modificada o eliminada por computadoras cliente. [31]

Supongamos que en el servidor de aplicaciones presta un servicio por medio de un software el cual gestiona la facturación y la cartera de una empresa, esta información es de gran valor por ser datos sensibles y monetarios que permiten manejar las finanzas de la compañía.

2.2.8. Servidor Bases de Datos.

Un servidor de base de datos es un tipo de software de servidor que permite la organización de la información mediante el uso de tablas, índices y registros.

Su propósito es servir consultas a clientes remotos o locales que solicitan información o realización modificaciones a los registros y tablas que existen dentro de las bases de datos del sistema. [32]

Supongamos una base de datos con las siguientes tablas: facturas, notas crédito, pagos, etc. En ellas se tiene organizada y separada la información para la gestión de cada proceso dentro de la organización.

2.2.9. Servidor de Correo Electrónico.

El servicio de correo electrónico es uno de los métodos de comunicación más usados del mundo. Lo usamos en nuestras computadoras de escritorio, notebooks, móviles, tablets e incluso desde nuestros relojes inteligentes.

Está encargado de enviar y recibir mensajes de correo electrónico entre hosts, usuarios o servidores. Entre sus funciones se incluye el procesado de los mensajes, filtrado, almacenamiento, envió, recepción y reenvío de correos. [33]

Supongamos que en la organización tenemos un servidor de correo propio con el dominio @ejemplo.com en el cual tenemos múltiples nombres de correo donde se envíe y reciben correos con documentos importantes y una comunicación sobre la gestión de los procesos dentro de la organización, esto nos indica que se maneja información confidencial y sensible que debe ser manejada correctamente, ya que por medio de este servicio pueden llegar virus y/o amenazas informáticas.

2.2.10. Cortafuegos (Firewall).

Los firewall o cortafuegos en su traducción son programas de software o dispositivos de hardware que filtran y examinan la información que viaja a través de tu conexión a Internet. Representan la primera defensa porque pueden evitar que un programa malicioso o un atacante obtengan acceso a tu red y a tu información antes de que se produzca cualquier posible daño. [34]

2.2.11. Equipos de Cómputo.

Es un sistema informático de componentes electrónicos que en conjunto proporcionan datos de salida procesados mediante ecuaciones matemáticas. Los componentes son el hardware y se encargan de procesar todas las instrucciones del software. [35]

2.2.12. Telefonía IP / Dispositivos Móviles.

Es un término utilizado para describir las tecnologías que usan el protocolo IP para el intercambio de voz, fax, y otras formas de información, tradicionalmente transportada sobre la Red Telefónica Pública Conmutada (PSTN). La llamada viaja en forma de paquetes, sobre una red de área local (LAN) o Internet. [36]

2.2.13. Planta Telefónica.

Las Plantas Telefónicas, también conocidas como Centrales, son equipos de comunicaciones que permiten interconectar diferentes grupos de teléfonos, también conocidos como Extensiones, dentro de su oficina, casa o empresa. Su función más importante consiste en permitir la comunicación entre diferentes oficinas o secciones dentro de un mismo edificio, permitiendo mejorar la interacción entre los empleados, ganando tiempo y eficiencia. [37]

2.2.14. Switches.

Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet. [38]

2.2.15. Enrutador (Router).

Es un dispositivo que ofrece una conexión Wifi, que normalmente está conectado a un módem y que envía información de Internet a tus dispositivos personales, como ordenadores, teléfonos o tablets. Los dispositivos que están conectados a Internet en tu casa conforman tu red de área local (LAN). [39]

2.2.16. Repetidores (Access Point).

También llamado amplificador o adaptador Wifi, es uno de los dispositivos que puedes encontrar para ampliar la cobertura de tu red doméstica. [40]

2.2.17. Cámaras de Seguridad.

Son las que se encargan de grabar todo lo que puede ocurrir en una casa o negocio. Contar con este tipo de cámara te puede proporcionar sensación de seguridad y protección. [41]

Se califica para cada activo según el impacto para determinar los activos en un orden de relevancia según su criticidad.

2.2.18. Seguridad Informática.

Proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. [10]

En la mayor parte de los casos, la seguridad de las Tecnologías de la Información queda garantizada por unos sistemas de encriptado y protección altamente fiables. No obstante, estos sistemas no son 100% infalibles, y en alguna ocasión se puede producir una invasión de malware, o bien una caída fortuita del servidor o del soporte digital. Cuando se produce la pérdida temporal de los datos, es cuando entra en escena el DR Recuperación de Desastres y los tiempos RTO (Tiempo Objetivo de Recuperación) y RPO (Punto Objetivo de Recuperación). [11]

2.2.19. Punto Objetivo de Recuperación (RPO)

El punto en el tiempo a partir del cual se deben restaurar los datos para reanudar las transacciones de procesamiento.

El RTO indica la rapidez con la que necesita recuperarse de un tiempo de inactividad, mientras el RPO define la frecuencia con la que se necesitan hacer copias de seguridad. [12]

2.2.20. Tiempo Objetivo de Recuperación (RTO)

El período de tiempo permitido para la recuperación, es decir, el tiempo que puede transcurrir entre el desastre y la activación de sitio secundario.

Es el tiempo que un negocio necesita para recuperar sus sistemas después de inactividad producida por un incidente (desastre), es decir, la cantidad de datos que se pierden y se tienen que volver a ingresar durante el tiempo de inactividad de la red. [12]

2.2.21. Tiempo de Recuperación Actual o Real (RTA)

RTA se refiere al período de tiempo real transcurrido para completar la recuperación de datos y hacer que la copia de almacenamiento esté disponible para el acceso a la aplicación. Mientras que RTO es el valor estimado establecido como objetivo, RTA es el tiempo real medido contra él. [65]

2.2.22. Planificación de Continuidad del Negocio (BCP)

Se utiliza un modelo para determinar el tiempo de inactividad esperado debido a un desastre impacto, así como el hardware normal y fallas de software. Existen diversos tipos de desastres, como lo son naturales, tecnológicos y provocados por el hombre. eventos que interrumpen el funcionamiento normal de la economía y sociedad a gran escala. [13]

2.2.23. Disponibilidad de datos.

Un proceso del sistema garantiza pérdida mínima de datos (ΔL). Requiere todo activo / sitios en espera / paralelos en una corporación para tener copia de datos críticos. Esto se puede lograr replicando los datos del sitio primario o del sitio secundario. El original de los datos aún puede reproducirse dentro de tiempo aceptable requerido para cumplir con el MTPD (Periodo Máximo Tolerable de Interrupción) comercial. [14]

2.2.24. Ciclo de gestión PHVA.

El ciclo PHVA (Planificar-Hacer-Verificar-Actuar) es una estrategia interactiva de resolución de problemas para mejorar procesos e implementar cambios. El ciclo PHVA es un método de mejoras continuas. No es un proceso que se ejecuta una sola vez, sino un espiral continuo que busca mejorar los procesos e interacciones. [58]

2.3. Estado del arte.

En la (Tabla 2-2) se construye una investigación sobre los diferentes proyectos relacionados al RTO, esto con el fin de tomar las diferentes variables que potencien esta tesis e identificando los vacíos en cada uno de estos proyectos, así permitiendo realizar una construcción solida de una metodología que permita calcular los tiempos de recuperación sobre los activos.

Tabla 2-2:

Análisis de trabajos relacionados.

Trabajo Relacionado	Contribucion	Vacios	Proyecto Propuesto
Disaster Recovery and Business continuity for Database Services in Multi-Cloud(Recuperación ante desastres y continuidad empresarial para Servicios de base de datos en multiples nubes)	Recuperación de desastres y continuidad de negocio en múltiples nubes sobre las bases de datos.	Determinación de criticidad y alternativas para realiza la recuperación y metodologías para practicar la recuperación de una manera practica y ágil.	Lograr calcular el tiempo objetivo de recuperación ante un desastre en activos críticos, evaluando el escenario de la organización permitiendo que a través de una metodología puedan tomarse medidas correctivas que le brinden a la organización tiempos objetivos.
Disaster Recovery and Business Continuity Plan (Plan de recuperación ante desastres y continuidad del negocio)	Pasos para realizar una recuperación de desastres, dar disponibilidad a los sistemas de información de las organizaciones y poder así tener continuidad de negocio en las organizaciones.	Determinación de criticidad y cálculo del tiempo objetivo de recuperación para tener un tiempo claro de recuperación y ser más eficiente la continuidad del negocio.	Aplicación que permite el calculo del tiempo objetivo sobre la recuperación de los activos de información ante un desastre.
Evaluating Disaster Recovery Plans Using the cloud (Evaluación de planes de recuperación ante desastres utilizando la nube.)	Planes de recuperación ante desastres en diversos escenarios.	Cálculo del tiempo de recuperación de los activos críticos de información para poder aplicar planes óptimos de recuperación.	Aplicación de planes prácticos a través de una metodología que permite tener claridad de la determinación de los tiempos objetivos de recuperación sobre los activos críticos y así llevar acabo una recuperación objetiva.

Autor: Construcción propia.

A continuación, se presentan diferentes investigaciones y trabajos existentes en el medio a nivel mundial, que permitieron obtener información relevante para la construcción de esta tesis sobre recuperación de desastres, continuidad de negocio, etc. Así permitiendo conocer características y funcionalidades actuales para construir una metodología optimizada que permita al personal de TI ser más eficientes en la recuperación al momento de una ausencia de disponibilidad de los activos de información.

Se encontró un estudio recuperación ante desastres y continuidad comercial para servicios de bases de datos en múltiples nubes, por lo tanto, existe la necesidad de desarrollar un marco de Recuperación ante Desastres (DR) práctico basado en múltiples nubes con el objetivo de minimizar costo de respaldo con respecto al Tiempo de Recuperación Objetivo (RTO) y Punto Objetivo de Recuperación (RPO) para reducir el riesgo de pérdida de datos.

El marco intenta mantener la disponibilidad de datos, logrando datos con alta fiabilidad, bajo costo de respaldo y recuperación corta y asegurar continuidad para los negocios antes, durante y después

del incidente de desastre Este documento tiene como objetivo proponer un marco de múltiples nubes que mantenga una alta disponibilidad de datos antes, durante y después del desastre. Además, asegura la continuidad de los servicios de la base de datos durante y después del desastre. [15]

También se identificó un estudio análisis de RTO y RPO de un servicio almacenado en Servicio Web de Amazon (AWS) y Google Cloud Motor (GCE), hoy la disponibilidad de la aplicación está más allá todo. No se puede acceder a la aplicación ni siquiera en un minuto convertirse en un problema importante para el negocio y amenazar la reputación de la empresa especialmente que necesitan disponibilidad 24/7 de solicitud. Empresas que tienen físico tradicional los entornos generalmente deben duplicar su infraestructura para garantizar la disponibilidad de capacidad disponible en caso de desastre. [16]

Además, un estudio de evaluación de planes de recuperación ante desastres usando la nube, toda organización requiere un Plan de Continuidad Comercial (BCP) o Plan de Recuperación ante Desastres (DRP) que se encuentra dentro de limitaciones de costos mientras se logra el objetivo de recuperación requisitos en términos del Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO). Las organizaciones deben identificar los eventos probables que pueden causar desastres y evaluar su impacto. Necesitan establecer los objetivos claramente, evaluar planes de recuperación ante desastres factibles para elegir el DRP que lo haría ser óptimo.

El documento examina las compensaciones involucradas y presenta pautas para elegir entre la recuperación ante opciones de desastres. La planificación óptima de recuperación ante desastres

debe tomar en consideración los parámetros clave, incluido el costo inicial, el costo de las transferencias de datos y el costo del almacenamiento de datos. Las necesidades de datos de la organización y sus objetivos de recuperación ante desastres necesitan ser considerados para evaluar el riesgo, los tipos de desastre (natural o causado por el hombre) necesitan ser identificados. La probabilidad de que ocurra un desastre debe evaluarse junto con los costos de las fallas correspondientes. [17]

Seguidamente se evidencio un estudio para la evaluación de mecanismos de replicación de bases de datos para la recuperación ante desastres en entornos de nube, las bases de datos relacionales son la base de datos más popular. Sistema en todo el mundo. La ocurrencia de fallas en estos sistemas puede producir graves consecuencias para el negocio, como pérdida de datos, insatisfacción del cliente y posterior pérdida de ingresos. En consecuencia, muchas organizaciones han adoptado la Recuperación ante Desastres. (DR) como un intento de evitar la pérdida de datos y garantizar la continuidad del negocio. La replicación de datos para bases de datos es una de las soluciones DR más utilizada para garantizar la seguridad de los datos y disponibilidad. [18]

Según el estudio descripción general de la copia de seguridad de datos y desastres Recuperación en la nube, hoy en día, en cada organización se desarrollan grandes volúmenes de datos en formato electrónico que requiere la seguridad servicios de almacenaje. Copia de seguridad de datos y recuperación ante desastres. Los problemas de continuidad se encuentran volviendo fundamentales en las redes desde La importancia y el valor social de los datos digitales es continuamente creciente. [19]

Toda organización requiere una Continuidad Comercial Plan (BCP) o Plan de Recuperación ante Desastres (DRP) y copia de seguridad de datos que cae dentro de las limitaciones de costos mientras se alcanza el objetivo requisitos de recuperación en términos del Tiempo Objetivo de Recuperación (RTO) y Punto Objetivo de Recuperación (RPO). [19]

Según el estudio uso de la virtualización para preparar su centro de datos para la "Garantía de negocio en tiempo real continuidad", al crear una aplicación para distribuir la utilización de recursos perfil a través de varios sistemas de gestión, y utilizando un combinación de virtualización de servidor, red y almacenamiento tecnologías, objetivos RTO y RPO específicos de la aplicación (Definido en función de los perfiles de carga de trabajo y las prioridades comerciales) se cumplen en una tecnología agnóstica y multi proveedor ambiente. [20]

Además, existen una estrategia de optimización para la recuperación de desastres, Estas precisiones, disponibilidad, seguridad y la actualización de los registros financieros es crucial para la banca servicios de negocios. La importancia del servicio 24x365 horas disponibilidad con datos precisos y seguros es la resolución para negocios ventajas competitivas. Elegir la TI Correcta Planificación de Contingencias (ITCP) para Recuperación de Desastres (DR) asegura la continuidad del negocio y optimiza la banca inversión. Esta investigación investiga el imperativo. [21]

Requisitos fundamentales de cada unidad de negocio bancario y aborda el mapeo de la importancia crítica del negocio para DR preparación mediante la evaluación del Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO) para garantizar el negocio continuidad bajo un Período Máximo de Interrupción Tolerable (MTPD) El modelo de estrategia DR propone optimización estrategia para elegir el patrón correcto de recuperación ante desastres solución para cada requerimiento de unidad de negocio. [21]

El modelo empírico de planificación de contingencia de TI para la selección de las estrategias de recuperación de desastres en la industria bancaria actual, 24x365 horas de servicio, la disponibilidad es de suma importancia para ganar competitividad. La Planificación adecuada de Contingencias de TI (ITCP) para la Recuperación de Desastres (DR) asegura la continuidad del negocio y optimiza inversión. Esta investigación investiga los requisitos fundamentales de cada unidad de negocio bancario para mapear la criticidad del negocio para la continuidad a la preparación ante un desastre. [22]

El proceso evalúa la recuperación del Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO) para asegurar la continuidad del negocio dentro de un Período Máximo Tolerable de Interrupción (MTPD). El modelo ITCP sirve como soporte de decisiones estándares y justificación para elegir la más apropiada solución de recuperación ante desastres para diferentes unidades de negocio requisitos. [22]

Luego de analizar documentación en la red se identifica una herramienta de cálculo RTO y RPO creada y publicada en la página web de QBR (your data, our business) que calcula el costo de inactividad según el tiempo de inoperancia de la organización. Esta herramienta se basa en los procesos de recuperación y los costos de tiempo de inactividad a nivel organizacional, con el fin de tener una visión general del costo con respecto al tiempo de inactividad.

Sin embargo, esta calculadora no demuestra con claridad el tiempo de recuperación de cada activo crítico particular u organizacional, esto le hace falta para lograr tener claridad sobre la recuperación y lograr la restauración óptima para dar la disponibilidad a los servicios. [23]

Adicionalmente, se identifica una calculadora que evalúa el tiempo de recuperación y objetivos de punto de recuperación publicada por Alpha & Omega Computer & Network Services, Inc. Dicha calculadora está separada por objetivos de recuperación, proceso de recuperación y almacenamiento de datos, costos de tiempo de inactividad y recuperación.

Aunque al realizar análisis de esta calculadora no permite tener la claridad la recuperación sobre los activos críticos y evaluar los niveles de criticidad de estos, para lograr una disponibilidad, debería permitir separar por activo, evaluando su nivel de criticidad y determinar el RTO sobre los activos para lograr tomar correcciones sobre estos y minimizar los tiempos de recuperación. [24]

Las cuales sirven como referencias para la elaboración de este proyecto con el fin de identificar según el activo crítico el tiempo de recuperación teniendo en cuenta diversas variables lo cual permitiría tener un tiempo objetivo de recuperación sobre los activos del sector servicios.

3. Metodología y Resultados

A continuación, se presenta la metodología con la cual se realizaron los objetivos y de manera inmediata la presentación de los resultados de cada una de las fases definidas.

Se desarrolló de la metodología se presenta en 3 etapas.

Métodos de la Investigación:

Etapa 1: Búsqueda de información. Se realizó una exhaustiva indagación a través de diversos motores de búsqueda utilizando métodos activos, los cuales permitieron identificar patrones importantes acerca las diferentes metodologías y aspectos importantes en el RTO para la continuidad de negocio y la remediación de incidentes de seguridad sobre los activos críticos de información, a su vez identificando cualidades y características del sector servicios que permitieron tener un panorama mucho más claro de todo lo que puede repercutir a la hora de buscar disponibilidad de un activo informático, a su vez se investigó sobre desarrollo de software, entre ellos se logró identificar y aclarar conceptos para la construcción de una herramienta informática.

El tipo de búsqueda utilizado fue secuencial, ya que se recurre al uso del buscador introduciendo las palabras claves, permitiendo entonces extraer todo lo relevante en cuanto al tema del desarrollo de un software dirigido a la web, su implementación en la gestión y control para así brindar conectividad y conseguir una correcta manipulación de los equipos y agilidad en el análisis. La búsqueda se clasificó de la siguiente manera: normas de continuidad de negocio, RTO, RPO, incidentes de seguridad, sector servicios, metodologías de riesgo, desarrollo ágil, software, hardware, redes, características del sector servicios, desarrollo software, PHP, bases datos, Metodología Scrum, Metodologías de Desarrollo, métricas de sistemas de información o activos informáticos, velocidad de internet, restauración, características RTO, parámetros RTO, Calculo de tiempo, Seguridad Informática, versionamiento , Sistemas de información, AWS, Sophos, Linux, dependencias del sector y todas aquellas características del sector servicios.

Etapa 2: Constitución del análisis. Una vez terminada la búsqueda de información y de realizar la respectiva clasificación necesaria para los fines de este estudio, se tomó todo lo relevante al tema

de investigación y se estructuró el análisis, pero que aportan detalles importantes acerca las características y métricas a aplicar sobre los activos de información, todos estos detalles son de vital importancia para el análisis y cálculo de los tiempos objetivos de recuperación en un desastre.

La literatura encontrada en los diferentes sitios web, revistas indexadas, libros, textos, imágenes y demás, principalmente en sitios de libre acceso en la Web, se encontró mucha información que contribuyó a nutrir el análisis y la implementación de la metodología y generación de una herramienta informática orientada al sector servicios, luego se identifican los parámetros en seguridad informática, tipos de servidores, tipos de servicios, características del servicio, esta permitió identificar las diversas cualidades que debe tener la metodología y construir una eficiente para la determinación de los tiempos objetivos en recuperación que permita al sector servicios la mejora continua en la identificación de los tiempos y así estas tener disponibilidad sobre los activos informáticos.

Etapa 3: Conclusiones del análisis. Luego de estructurar el análisis y temas relacionados con este trabajo se procede a inferir sobre los resultados obtenidos, se construyó una herramienta informática básico para lograr comprender las múltiples variables que se deben tener en cuenta al momento de realizar un RTO sobre un activo de información critico en el sector servicios, para brindar a una empresa más eficiencia y control de la información manteniendo la disponibilidad de los activos de información y tener planes de recuperación de desastre sobre los activos de información.

Para la correcta identificación de las múltiples características que debe tener una metodología que permita determinar los tiempos objetivos y un sistema de información a la web. Se procede inicialmente a investigar las metodologías y normas actuales que permiten la continuidad de negocio.

Las metodologías de continuidad de negocio son decisivas en el éxito o fracaso del negocio, ya que cada una de ellas debe aplicar a la organización y al sector debido a sus características al nivel de disponibilidad que requiere este sector en la prestación de sus servicios.

La elección de una metodología inadecuada o su mala ejecución puede conducir a que el proyecto no llegue al fin o no funciones correctamente.

3.2. Clasificación de empresas del sector servicios en Colombia

Según la ley 590 de 2000 en Colombia, las empresas se clasifican en microempresas, pymes, compuestas por pequeñas y medianas empresas, y grandes empresas; esta clasificación se define según el número de trabajadores que tenga la organización y el total de activos valorados por el Salario Mínimo Mensual Legal Vigente (SMMLV). [25]

En la (Tabla 3-1) nos permite conocer como están clasificadas los diferentes tamaños de empresas y cuáles son sus características, esta información es de gran importancia para esta investigación ya que nos da un parámetro importante para conocer la cantidad de trabajadores, activos de información y posibles dependencias con el fin de entender cómo funciona u opera dicha organización.

Tabla 3-1:

Ley 590 del 2000. Marco de acción para la pequeña y mediana empresa. [25]

Clasificación	Número de trabajadores	Valoración de activos Totales SMMLV
Microempresa	Menores a 10	Inferior a quinientos uno (501) SMMLV.
Pyme (Pequeña Empresa)	Entre 11 y 50	Entre quinientos uno (501) y menos de cinco mil (5.001) SMMLV.
Pyme (Mediana Empresa)	Entre 51 y 200	Entre cinco mil uno (5.001) y quince mil (15.000) SMMLV.
Grandes Empresas	Mayor a 200	Mayor o igual a quinientos un mil (15.001) SMMLV.

Autor: Ley 590 del 2000. Marco de acción para la pequeña y mediana empresa. [25]

Nota. Se investiga las diferentes características de empresas con el fin de entender cómo se clasifican las empresas en Colombia.

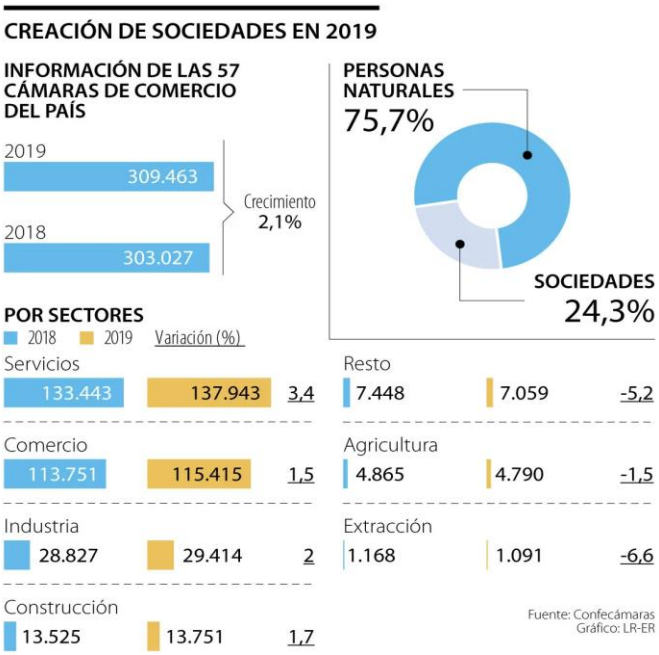
3.3. Sector Servicios

Comprendiendo el significado del sector de servicios o terciario se entiende como el conjunto de actividades económicas que dan servicio a la sociedad.

En la (Figura 3-1) se aprecian los diferentes sectores que tiene Colombia y el crecimiento exponencial que tiene cada uno de estos. Se logra visualizar que el sector servicios es el más alto y el de mayor crecimiento año tras año, identificando así que es el sector económico con más empresas en Colombia.

Figura 3-1:

Crecimiento del Sector de Servicio [26].



Autor: Confecámaras

Nota: Se identifica el crecimiento y proporción de empresas en Colombia en los diversos sectores económicos, permitiendo conocer la cantidad de empresas del sector servicios que crece cada día más, significando un gran volumen de empleados y activos de información orientados a la prestación de sus servicios.

Siendo el sector de servicios el más abundante en Colombia, se realiza un análisis de las diversas actividades económicas en el sector con el fin de identificar los activos de información tecnológicos más comunes para la ejecución de los servicios.

En la (Figura 3-2) logra mostrar el personal ocupado según las diversas actividades económicas y cuáles tienen mayor tendencia de crecimiento, para lo cual nos da un parámetro importante de entender cuáles son los servicios con más abundancia en Colombia. Se logra identificar que el sector servicios tiene el 80% de la fuerza laboral del país, 4,3 millones prestan servicios personales y/o sociales y aportan 15% a la economía del país. Siendo de gran valor para esta investigación realizar un aporte significativo a los sistemas de información de dicho sector.

Figura 3-2:

Actividades Económicas del Sector Servicios [27].

Fuente: DANE, EMS.
* Incluye personal permanente, personal temporal contratado directamente y personal temporal contratado a través de agencias.

Autor: DANE, EMS.

Nota. Se identifican las actividades económicas del sector servicios o terciario, esto nos indica y muestra la cantidad de personal ocupado en estas diversas actividades lo que demuestra cuales son las actividades con mayor cantidad de servicios en Colombia.

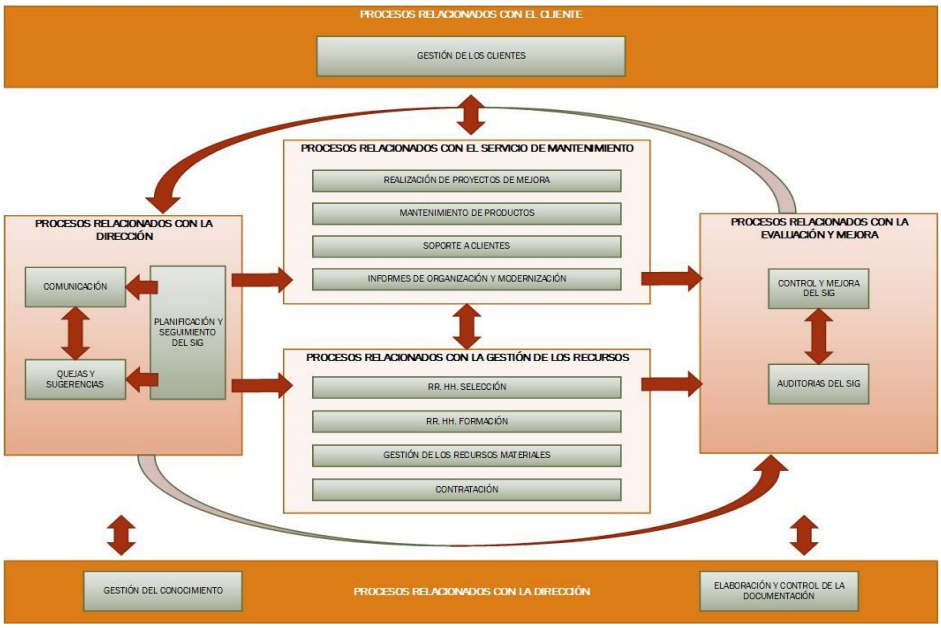
Luego de identificar las diversas actividades económicas, partiendo del supuesto en que se seleccionan al azar las siguientes tres actividades, ya que en sus procesos tienen similitudes para la prestación de los servicios.

3.3.1. Procesos del sector servicios.

En la (Figura 3-3) podemos visualizar un modelo de mapa de procesos que aplica al sector servicios, mostrándonos el flujo de trabajo y de dependencias de cada proceso que realiza dicho sector, aportando a la tesis una claridad de cómo están formadas las organizaciones prestadoras de servicios. Esta información es de gran valor ya que se debe conocer que activos de información que contiene cada proceso, que tan críticos son, así logrando determinar la recuperación de estos.

Figura 3-3:

Procesos genéricos dentro del sector servicios. [28].



Autor: Christina Aguado, Profesora de Cela Open Institute. [28]

Nota: Se identifica los procesos básicos y relaciones entre los procesos los cuales tiene una organización en el sector de servicios o terciario. Es de gran importancia conocer como están compuestos los procesos y subprocesos, las dependencias y actividades que realiza una organización prestadora de servicios, permitiendo así entender el diagrama de flujo y las operaciones habituales de las diversas empresas prestadoras de servicio.

3.4. Niveles de Criticidad

Con el fin de identificar el nivel de criticidad de cada activo de información del sector servicios se realiza un análisis con respecto a los impactos financieros, operacionales, legales y reputacionales otorgándoles a cada impacto un nivel de importancia igual para caso práctico. [29]

En la (Tabla 3-2) se caracterizan los niveles de criticidad con el fin de tener un parámetro para los activos críticos y tomar decisiones razonables ante la ausencia de disponibilidad de dicho activo o en su defecto un desastre, este valor tiene un aporte valioso a la tesis ya que permite tener una variable que permite categorizar los activos del sector de servicios.

Tabla 3-2:

Valor de criticidad del activo de información en disponibilidad. [29].

Valor de Criticidad		
#	Valor	Descripción
1	Bajo	Reemplazable
2	Medio	Ausencia Parcial de Disponibilidad
3	Alto	Ausencia Total de Disponibilidad

Autor: MINTIC.[29]

Nota. Se caracteriza nivel de criticidad en caso de que un activo de información falle o su funcionalidad altere la disponibilidad ante un desastre.

Teniendo presente los tres pilares en la gestión de la información se incluye la siguiente tabla para tener los niveles de criticidad con respecto a la información según el pilar.

En la (Tabla 3-3) se plasma la importancia sobre los activos de información que resalta que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que dentro de las buenas prácticas esta la gestión de los riesgos. Dichos criterios son un parámetro que aporta con gran valor a esta tesis ya que permite tener una visión de como calificar los activos de información en nivel de criticidad y así tener claro cuáles serían los procedimientos para seguir en la recuperación de estos.[29]

Tabla 3-3:

Criterios de clasificación de los pilares en la gestión de la información.[29]

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACION PUBLICA RESERVADA	ALTA	ALTA
INFORMACION PUBLICA CLASIFICADA	MEDIA	MEDIA
INFORMACION PUBLICA	BAJA	BAJA
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Autor: MINTIC**.** [29]

En la (Tabla 3-4) y teniendo presente la (Tabla 3-3) nos permite conocer cuáles son los niveles de clasificación sobre los criterios para tener en cuenta en la gestión de los activos de información y así poder visualizar como clasificarlos para proceder a una recuperación o restauración de estos de forma oportuna. [29]

Tabla 3-4:

Niveles Clasificación. [29]

ALTA	Activos de información en los cuales la clasificación de la información en los (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Autor: MINTIC**.** [29]

Luego de tener en cuenta los diferentes niveles de criticidad existentes sobre las diferentes afectaciones que pueden surgir sobre un activo de información en la organización prestadora de servicios, se debe tener en cuenta los diversos impactos que puede tener la organización al verse comprometido uno de los activos en cuanto a confidencialidad, integridad y disponibilidad de los diferentes activos. A continuación, se presentan las definición y descripción de los impactos.

3.4.1. Impacto Financiero

Se define como la magnitud del impacto económico y/o monetario que afecta a la organización. [1]

3.4.2. Impacto Operacional

Se define impacto operacional a la disminución o suspensión de actividades que se ejecutan en cada proceso de la organización para su correcto funcionamiento. [1]

3.4.3. Impacto Legal

Se define como las acciones jurídicas o judiciales a las que se expone la empresa ante una falla, filtración o indisponibilidad de la información, además de procesos disciplinarios, multas, quejas o reclamos que afecten la imagen de la organización. [1]

3.4.4. Impacto Reputacional

Se define como pérdida o merma en la reputación o imagen de la organización, que afecta de forma negativa la percepción que el entorno social tiene sobre la misma. Puede producir una pérdida directa o indirecta del valor de la compañía. [1]

4. Evaluación y clasificación de métricas adecuadas en la identificación de los puntos objetivos para el cálculo de tiempos de recuperación sobre cada activo, identificando el patrón de criticidad.

Para los activos de información se evalúan y clasifican diferentes métricas adecuadas para lograr identificar cuáles aplican y cuáles no aplican, así obtener los criterios a evaluar y tener presentes para la determinación del cálculo de los tiempos objetivos de recuperación.

4.2. Descripción de métricas para activos de información.

Las métricas en los activos de información se utilizan para impulsar mejoras y analizar comportamiento.

La importancia de estas permite conocer los estados y características de funcionamiento de los activos de información. Los beneficios de las métricas son muchos, pero se intenta en no caer en el error de tener métricas vanidosas. Métricas que se ven bien, que son bonitas y llamativas, pero no aporta nada a la organización en cuanto a una recuperación objetiva ante un desastre.

Teniendo presente lo anterior es importante tener unas métricas estandarizadas que son basadas a nivel internacional, por empresas fabricantes, herramientas digitales, software y demás que permiten monitorear e identificar información de valor de un activo informático. Estas hacen referencia a modelos de medición que se han realizado a nivel mundial.

Las métricas definidas a continuación buscan medir el activo de información el cual contiene los servicios que deben estar disponibles, estas métricas se describen las existentes que son tomadas del medio, que son utilizadas para conocer el estado actual del activo, estas muestran un valor cuantificable de las diferentes características que tiene un activo informático.

Así pues, se puede tener en cuenta todos estos datos para implementar estrategias y objetivos para mejorar dichos valores. Las métricas presentadas en (Tabla 4-1) son identificadas por que hacen parte del proceso clave de identificación sobre los tiempos de recuperación del activo informático que la organización requiere o necesita para cubrir sus procesos operacionales para la prestación de los diferentes servicios. Estas diferentes características deben ser medidas, ya que son determinantes al momento de ejecutar una recuperación del activo de información.

En la (Tabla 4-1) se presenta la lista de métricas aplicables a los activos de información con sus respectivas unidades de medida. Ver más en el (Anexo A).

Tabla 4-1:

Definición de métricas aplicables activos de información.

Metricas	
Nombre	**Unidades de Medida**
Capacidad de almacenamiento y uso	Gigabytes - Megabytes - Kilobytes
Capacidad de rendimiento y uso	Velocidad Procesador (GHz (gigahertz)) - Ram (megabytes) - Porcentajes uso
Calcular la capacidad y el uso	Megabytes - Uso - Promedio mes almacenamiento
Copia de seguridad	Dias - Peso (Gigabytes - Megabytes) - Horas-minutos-segundos
Punto de recuperacion y realidad del tiempo de recuperacion	Dias - horas - Minutos
Adquisicion activo/ servicios / atencion	Costo - Horas - Semana - Mes - Año - Cantidad - Megabytes
Comportamiento / Vinculos / Conexiones / Trafico / Dependencias	Peticiones - Conexiones - Trafico - Volumen de datos promedio - Usuarios
Producto / Activo	Ram(Gigabytes, Megabytes) - Procesador(Porcentaje de uso) - Disco duro(Gigabytes,Megabytes) - Configuraciones(Topes) - Cantidad Activos
Costos Mensuales	Pesos Colombianos-Dias- Dolares-Ingenieros
Registros Digitales	Filas -tablas - peso(megabytes)
Recursos Humanos / Usuarios / Visitantes	ngenieros - Numero Usuarios - Actualizaciones
Riesgos / Fallas / Amenazas / Errores	Ataques - Riesgos - Vulnerabilidades - Fallas - Dia - Tiempo de inactividad
Financiero	Costos Mes - dia - tiempo

Autor: Construcción Propia.

Nota: Se investigo en las diferentes plataformas las unidades de medida que se aplican a los diversos activos, las cuales son de valor para esta tesis ya que permite evaluar e identificar características del activo y conocer el servicio que presta; esto con el fin de lograr tener unos datos claros del funcionamiento de este. Estas características son importantes medirlas ya que hacen parte de los activos informáticos y hace referencia al nivel de información o las características necesarias que se deben medir para la correcta funcionalidad de un activo de información.

4.3. Resultados del análisis de las métricas para los activos críticos de información.

En la (Tabla 4-2) se presenta un consolidado de las diferentes métricas que se lograron identificar en el transcurso de la investigación, las cuales fueron parámetros importantes para evaluar los activos de información de acuerdo con la integridad, disponibilidad, autenticidad, utilidad y funcionalidad.

Se logra realizar una evaluación y clasificación de las métricas con respecto al activo de información, así, permitiendo obtener información de valor para esta tesis, ya que nos permite entender qué características se miden sobre los activos y que se debe tener en cuenta al momento de evaluar e identificar la criticidad de un activo de información.

Tabla 4-2:

Evaluación de métricas con respecto a los activos de información.

	Metricas											
Activos	Capacidad de almacenamiento	Capacidad de rendimiento	Copias de Seguridad y Respaldo	Tiempo disponibilidad	Tiempo de tolerancia	Vinculos y Dependencias	Riesgos / Criticidad	Seguridad	Financiero	Operacional	Legal	Reputacional
Servidor Aplicaciones	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA
Servidor Bases de Datos	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA
Servidor Correo	APLICA	APLICA	APLICA	APLICA	APLICA	NO APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA
Firewall	NO APLICA	APLICA	APLICA	APLICA	APLICA	NO APLICA	APLICA	APLICA	APLICA	NO APLICA	APLICA	NO APLICA
Equipos de Computo	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	NO APLICA
Telefonos Ip / Dispositovos Moviles	APLICA	APLICA	APLICA	APLICA	APLICA	NO APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA
Planta Telefonica	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA	APLICA
Switches	NO APLICA	APLICA	NO APLICA	APLICA	APLICA	NO APLICA	NO APLICA	APLICA	APLICA	NO APLICA	NO APLICA	NO APLICA
Routers	NO APLICA	APLICA	NO APLICA	APLICA	APLICA	NO APLICA	APLICA	APLICA	APLICA	NO APLICA	NO APLICA	NO APLICA
Repetidores (Access Point)	NO APLICA	APLICA	NO APLICA	APLICA	APLICA	NO APLICA	APLICA	APLICA	APLICA	NO APLICA	NO APLICA	NO APLICA
Camaras de Seguridad	NO APLICA	NO APLICA	NO APLICA	APLICA	NO APLICA	NO APLICA	APLICA	APLICA	APLICA	NO APLICA	APLICA	NO APLICA

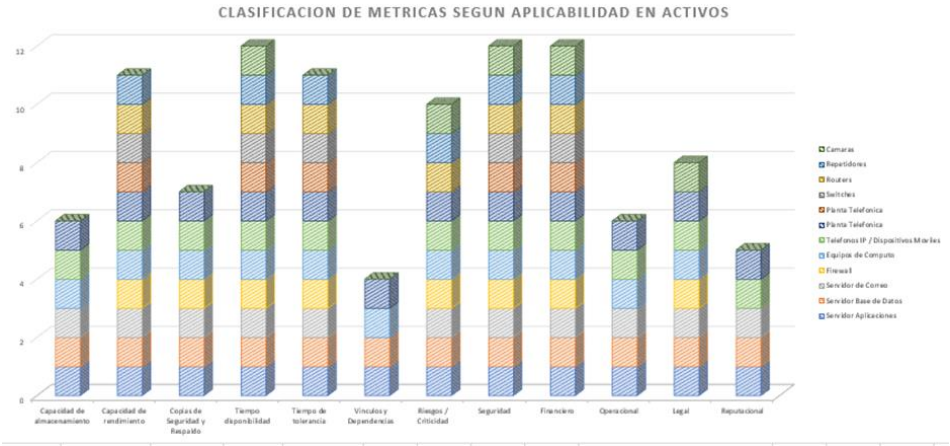
Autor: Construcción Propia.

Nota: Se evalúa que métricas aplican según el activo de información, de esta manera se identifican las características comunes para cada activo lo que permitirán medirlo. Asi se obtiene la tendencia de métricas estándares para los diferentes activos de información. Esto permite tener los diferentes modelos de medición que brindaran datos relevantes y claves para determinar los tiempos de recuperación o restauración de dicha característica, que es importante para el correcto funcionamiento del servicio que presta el activo.

En la (Tabla 4-1) se presenta la clasificación de las métricas anteriormente evaluadas según la aplicabilidad sobre los activos de información (Tabla 4-2). Dicha clasificación nos permite visualizar cuales son las métricas más utilizadas.

Figura 4-1:

Clasificación de métricas según aplicabilidad a los activos de información.



Autor: Construcción Propia.

Nota: En la imagen anterior se pueden visualizar la aplicabilidad de las diversas métricas sobre los activos de información, permitiendo observar obtener una clasificación de estas y así tener una visión de cuáles son las métricas más adecuadas para determinar la medición de los tiempos de recuperación.

Al identificar las diversas métricas se permite observar un patrón de criticidad, este patrón va de acuerdo con la aplicabilidad de las métricas y las que son más aplicadas, ya que miden múltiples características de valor sobre los activos, esto dando pie a la identificación de variables importantes para el cálculo de los tiempos objetivos de recuperación de los activos en función de la disponibilidad de este.

Luego de identificar las métricas más utilizadas, permite tener un panorama de cuáles son las métricas de mayor valor al momento de analizar un activo de información, esto permite encontrar un patrón de criticidad ya que podemos identificar diferentes características de medición de los activos, de acuerdo con dichas métricas, además obteniendo información que permite identificar vulnerabilidad y riesgos de los activos en una organización. A continuación, se presenta una clasificación de las métricas de impacto asociadas a los activos y como se puede evaluar un activo dentro de estas métricas. Dichas métricas son de mucho valor ya que permiten identificar el nivel de criticidad y la afectación que puede presentar la organización al momento de una indisponibilidad.

4.4. Clasificación de Impactos sobre activos de información.

El impacto refiere a las consecuencias que tienen la materialización de las diferentes amenazas que tiene un activo de información. Entre los impactos se identifican (Legal, Reputacional, Operacional y Financiero).

Luego de identificar los diferentes impactos que afectan al sector servicios al momento de presentar una falla, una ausencia de disponibilidad o un desastre en los sistemas de información disponibles para la prestación de los servicios de la organización. Se presentan las siguientes tablas con su respectiva clasificación según la criticidad del impacto.

En la (Tabla 4-3) define los impactos financieros traducidos a las pérdidas económicas al momento de presentarse una indisponibilidad de los servicios prestados por un activo de información.

Tabla 4-3:

Impactos Financieros. [42]

Impactos Financieros		
Descripción	Magnitud del Impacto Económico (Millones $)	Magnitud del Impacto Económico (Millones $)
	Límite Inferior (Mayor o igual que)	Límite Superior (Menor o igual que)
Insignificante	$ 0	$ 700.000.000
Menor	$ 700.000.001	$ 1.400.000.000
Moderado	$ 1.400.000.001	$ 2.100.000.000
Mayor	$ 2.100.000.001	$ 2.800.000.000
Catastrófico	$ 2.800.000.001	

Autor: Supersociedades.

Nota: Se clasifican rangos de nivel de impacto financiero para así conocer la magnitud del impacto económico sobre la organización.

En la (Tabla 4-4) representa una clasificación que permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio. Los impactos se agrupan en tres categorías: Especificaciones técnicas y nuevas pruebas, no disponibilidad y respuesta de planta.

Tabla 4-4:

Impactos Operacional. [42]

Impactos Operacional	
Descripción	**Impacto Operacional**
Insignificante	Afecta menos del 10% de las actividades normales del proceso.
Menor	Afecta entre el 10% y el 30% de las actividades normales del proceso.
Moderado	Afecta entre el 30% y el 50% de las actividades normales del proceso.
Mayor	Afecta entre el 50% y el 80% de las actividades normales del proceso.
Catastrófico	Afecta más del 80% de las actividades normales del proceso.

Autor: Supersociedades.

Nota: Se clasifican rangos de niveles de impacto operacional, lo que indicara los porcentajes de afectación sobre las actividades normales de los procesos que realiza la compañía.

En la (Tabla 4-5) define los impactos legales que se representan en una violación de la seguridad podría dar como resultado multas por incumplimiento de las regulaciones sobre el uso de datos del cliente.

Tabla 4-5:

Impactos Legales o Íntegros. [42]

Impactos Legal	
Descripción	**Impacto Legal o Integro**
Insignificante	Conlleva a multas por organismos de control o una accion constitucional menor del 10%.
Menor	Conlleva a multas por organismos de control o una accion constitucional de 10% al del 25%.
Moderado	Conlleva a multas por organismos de control o una accion constitucional menor del 35%.
Mayor	Conlleva a multas por organismos de control o una accion constitucional menor del 45%.
Catastrófico	Conlleva a multas por organismos de control o una accion constitucional menor del 60%.

Autor: Supersociedades.

Nota: Se clasifican rangos de niveles de impactos legales o íntegros, identificando posibles multas por los organismos de control o acción constitucional.

En la (Tabla 4-6) define los impactos reputacionales al momento que se provoca una pérdida potencial de capital financiero, capital social y / o participación de mercado debido a daños relacionados con la reputación de una empresa.

Tabla 4-6:

Impactos Reputacionales. [42]

Impactos Reputacional	
scripción	Impacto Reputacional a nivel de proceso
Insignificante	No afecta la imagen de la Entidad o Mala imagen dentro de la Entidad
Menor	Deterioro de la imagen que una persona o grupo externo tiene de la Entidad.
Moderado	Mala Imagen en el sector (Ministerio)
Mayor	Mala imagen a nivel de organismos del estado
Catastrófico	Mala imagen a nivel nacional e internacional.

Autor: Supersociedades.

Nota: Se clasifican rangos de impacto reputacional identificando así los niveles de impacto sobre la imagen de la organización.

Clasificación los niveles de criticidad para la evaluación de los impactos sobre los activos y así determinar cuáles son los activos de información con mayor criticidad dentro de la organización. Según la (Tabla 3-2). Esta Tabla describe 3 niveles de criticidad (Bajo, Medio, Alto).

A continuación, en la (Tabla 4-7) se realiza una clasificación de los activos de información según la criticidad y su impacto al momento de perder la disponibilidad de los servicios que presta cada activo, se establecen 4 tipos de impacto que decreta supersociedades. Este ejercicio es de gran valor para la tesis ya que permite identificar los activos más críticos y con mayor impacto a la organización.

Tabla 4-7:

Clasificación de activos según nivel de criticidad con respecto al impacto. En esta tabla se realiza una calificación con la (Tabla 3-2) de cada activo de información con respecto al impacto que tenga, como se afecta la organización. Finalmente se suman los valores de cada impacto, así obteniendo como resultado valores que permiten identificar cuales activos presentan mayor impacto y así logrando identificar un parámetro de criticidad.

	Nivel de criticidad			
Activos	Impacto Financiero	Impacto Operacional	Impacto Legal	Impacto Reputacional
Servidor Aplicaciones	3	3	3	3
Servidor Bases de Datos	3	3	3	3
Servidor Correo	1	2	2	2
Firewall	1	2	2	1
Equipos de Computo	1	1	1	1
Telefonos Ip / Dispositovos Moviles	1	1	1	1
Planta Telefonica	1	1	1	1
Switches	1	1	1	1
Routers	1	1	1	1
Repetidores (Access Point)	1	1	1	1
Camaras de Seguridad	1	1	1	1

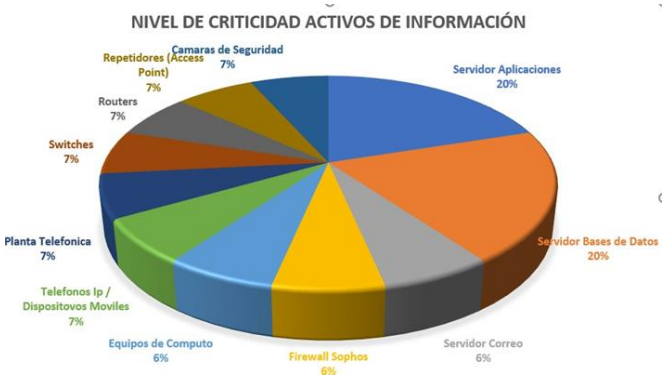
Autor: Construcción Propia.

Nota: Se califica el nivel de criticidad de cada activo de información del sector servicios con el fin de determinar que activo puede ser más crítico. Según la (Tabla 3-2).

En la (Figura 4-4) permite visualizar de acuerdo a la información obtenida en la (Tabla 4-7) los activos con mayor criticidad al momento de una perdida de disponibilidad, esta figura nos da un parámetro importante para la tesis ya que se logra identificar los activos más críticos en el sector servicios, así lograr establecer unos criterios para el cálculo del tiempo objetivo de recuperación de estos, así logrando que conserven la disponibilidad de los servicios que presta cada uno de los activos.

Figura 4-4:

Nivel de criticidad de activos de información críticos según el impacto en la organización.



Autor: Construcción Propia.

Nota: Se grafica los diferentes niveles de criticidad con respecto a la calificación de criticidad de los activos.

Teniendo en cuenta el RTO (Tiempo de recuperación objetivo) se definen los siguientes rangos donde se tiene en cuenta el impacto de la indisponibilidad o falla del activo de información no afecte a la organización.

Al ubicarse en un rango permite tener un equilibrio y tener diferentes estrategias para la recuperación. En caso de que el rango sea menor las pérdidas serán menores y en caso de ubicarse en el rango catastrófico las pérdidas serán muy altas y críticas, si se encuentra dentro de este rango se recomienda implementar mejoras y buscar estar entre el menor rango.

En la (Tabla 4-8) describe los rangos representados en horas y días, al presentar indisponibilidad de los servicios y estos se clasifican en criticidad.

Tabla 4-8:

Rangos de tiempo en recuperación de la disponibilidad de los activos. (RTO) [42]

Clasificación	Tiempo en el cual deben ser recuperados los datos	Descripción
0	Entre 0 y 8 Horas	Menor
1	Entre 8 y 24 Horas	Manejable
2	Entre 24 y 48 Horas	Menor
3	Entre 2 y 5 Días	Moderado
4	Entre 5 y 10 Días	Mayor
5	Superior a 10 Días	Catastrófico

Autor: Supersociedades**.**

Nota: Se identifican los rangos de calificación según el tiempo de la recuperación de la disponibilidad del activo de información, teniendo un nivel de criticidad de 0 a 5, siendo 0 el nivel menor y 5 el nivel mayor de criticidad.

Teniendo presente que el RTO mide la cantidad de tiempo de inactividad "tolerado" según el plan BCDR (Business Continuity and Disaster Recovery Plan). El impacto sobre la organización es representado sobre la disponibilidad de los activos de información que están operantes en cada proceso del sector servicios.

Para el RTO se consideran las siguientes variables para el cálculo del tiempo objetivo teniendo presente las características del sector servicios, teniendo como referencia los métodos de cálculo según unas calculadoras existentes publicadas en las páginas web de QBR y Alpha & Omega Computer & Network services, Inc [24]

Que se necesita para restaurar los servicios, datos o activos, desde que comienza un incidente cuánto tiempo de inactividad puede permitirse e identificar el escenario de pérdida de datos o disponibilidad.

De acuerdo con las métricas evaluadas y los impactos asociados a los activos de información se clasifican las siguientes métricas las cuales se tendrán en cuenta al momento de calcular el tiempo objetivo de recuperación ya que tienen mayor aplicabilidad dentro de los activos analizados y estas permiten tener un panorama general sobre las características y la criticidad del activo de información en la organización.

A continuación, se describen las características más relevantes según las métricas analizadas en la (Tabla 4-1) para los activos de información del sector servicios:

- Costo del tiempo de inactividad.
- Costo de inactividad por activo.
- Evaluar el valor de cada servicio (activo).
- Tiempo de tolerancia a la pérdida.
- Tiempo máximo de inactividad tolerable.
- Tiempo de copias de seguridad o cambio de dispositivo. (Según Aplique)
- Almacenamiento.
- Dependencias.

- Ubicación de datos o activo (Local - Nube).
- Impactos (Legal, Reputacional, Operacional y Financiero).

Dichas características mencionadas anteriormente, se determinaron dada la frecuencia sobre la clasificación de las métricas, que permitió identificar estas de forma particular que dan una referencia para el análisis y evaluación de estas características para determinar la criticidad del activo además de tener en cuenta los impactos que puede generar la indisponibilidad de este.

4.5. Definición de Metodologías y normas existentes para el análisis RTO.

El comité nacional para el conocimiento del riesgo SNGRD en Colombia en su terminología sobre gestión del riesgo de desastres y fenómenos amenazantes define el riesgo [43] como la probabilidad que ocurra un desastre o daño de forma negativa. Así, un riesgo está compuesto por dos factores, el primero son las vulnerabilidades o una ausencia de control (Físico o Lógico), la segunda son las amenazas. Por separado no representan un peligro, pero si se juntan se convierten en un riesgo [44] y (Ley 1523 de 2012).

4.5.1. Gestión de riesgos.

Como indica la organización internacional de normalización ISO en su norma ISO 31000:2018 gestión de riesgos es el proceso de preparación en el cual se planifica, y se organiza los recursos humanos, tecnológicos y materiales de la organización, para el desarrollo de las actividades de la gestión de riesgos [45] (Identificación, Análisis, Evaluación y Tratamiento del riesgos) [46], con el objetivo de prevenir desastres, reducir al mínimo los riesgos e incertidumbres a los que están expuestos las organizaciones.

La gestión de riesgos es de gran valor para esta tesis ya que va orientada a la disponibilidad cuando se determinan los diferentes impactos que pueden afectar la prestación de los servicios a un activo de información.

4.5.1.1. ISO 22301.

Es una norma internacional de gestión de continuidad de negocio. Esta ha sido creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras

normas. Identifica los fundamentos de un Sistema de Gestión de la Continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio. [52]

Proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de la organización. Se usa para asegurar a las partes interesadas clave que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente. [52]

4.5.1.2. DAFP versión 4.

El Departamento Administrativo de la Función Pública de la República de Colombia (DAFP) define y actualiza la guía para la administración de gestión del riesgo, la cual se encuentra en su versión 4 [47] y a través del Decreto 1537 de 2001 [48]. Esta es determinada como una metodología de gestión del riesgo organizacional para las entidades públicas las cuales deben contar con una política de gestión de riesgos apuntando a los riesgos de corrupción y seguridad digital.

4.5.1.3. Nist 800-30 Rev.1 - Guía de gestión de riesgos para sistemas de tecnología de la información.

Esta es una guía [49] para realizar evaluaciones de riesgos de los sistemas de información y organizaciones federales de los Estados Unidos. De acuerdo con esta guía, las evaluaciones de riesgos, realizadas en los tres niveles en la jerarquía de gestión de riesgos, son parte de un proceso general de gestión de riesgos, que proporciona a los líderes / ejecutivos seniors la información necesaria para determinar los cursos de acción adecuados en respuesta a los riesgos identificados. Esta guía brinda información sobre la selección de controles de seguridad rentables, los cuales pueden ser usados para mitigar el riesgo, para una mejor protección de la información de misión crítica y los sistemas de TI que procesan, almacenan y transportan esta información [49].

4.5.1.4. OCTAVE.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), es una metodología desarrollada por la empresa Computer Emergency Response Team (CERT) desde el (2001) [2], que corresponde a un método de planificación y consultoría estratégica en seguridad de la información basada en riesgo, la cual realiza una verificación y validación a los riesgos que afectan a la seguridad de la información, incluyendo los aspectos organizaciones y técnicos.

Para cualquier iniciativa de mejora frente a la seguridad de la información, se requiere un análisis previo que permita ver de forma transversal a la organización y los riesgos potenciales, con esto se obtiene una base para entender e implementar dichas mejoras. A diferencia de metodologías tradicionales, Octave se enfoca en los riesgos tecnológicos y temas tácticos pasando por la estrategia y práctica organizacional, dando peso a la gobernabilidad de las TIC en las organizaciones.

4.5.1.5. MAGERIT.

Magerit es una metodología de análisis y gestión de riesgos de los sistemas de información [51], la entidad responsable de las actualizaciones y publicaciones es el Ministerio de Hacienda y Administraciones Públicas de España, secretaria de estado y administraciones públicas, la cual es emplea el método de gestión de riesgo dentro de un marco de trabajo para que las unidades de gobierno realicen dictámenes teniendo en cuenta los riesgos derivados de las tecnologías de información.

Los objetivos que persigue esta metodología se enfocan en sensibilizar a los responsables de la información con la existencia de los riesgos y que es imperativo gestionarlos, presentar un método sistemático para analizar los riesgos resultantes del uso de la TIC y ayuda a describir y planificar el tratamiento para mantener el riesgo controlado.

El Ministerio de Hacienda y Administraciones Públicas de España, secretaría de estado y administraciones públicas indica que la versión de Magerit v3 liberada en octubre de 2012, los derechos de uso de la metodología son de uso libre y no requiere autorización previa. [51] [3]

4.5.1.6. ISO 27005:2018.

Proporciona directrices para la gestión de riesgos de seguridad de la información, elaborada y actualizada por la organización internacional de normalización ISO dicha publicación en julio de 2018. Es compatible con los conceptos generales especificados en ISO / IEC 27001 [53] y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.[52]

El conocimiento de los conceptos, modelos, procesos y terminologías descritos en ISO / IEC 27001 e ISO/IEC 27002 [54] es importante para una comprensión completa de ISO/IEC 27005:2018. Es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que pretenden gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

4.5.1.7. ISO 31000.

Es una técnica de gestión del riesgo - directrices, proporciona principios, marco y un proceso para gestionar el riesgo, dada por la organización internacional de normalización ISO [45]

La cual puede ser aplicada por cualquier organización, independientemente de su tamaño, actividad o sector. El uso de ISO 31000 puede ayudar a las organizaciones a aumentar la probabilidad de lograr objetivos, mejorar la identificación de oportunidades y amenazas, y asignar y utilizar de manera efectiva recursos para el tratamiento de riesgos.

Sin embargo, ISO 31000 no se puede utilizar con fines de certificación, pero proporciona una guía para los programas de auditoría internos o externos. Las organizaciones que lo utilizan pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido internacionalmente, proporcionando principios sólidos para la gestión eficaz y el gobierno corporativo.[45].

4.6. Análisis de metodologías relacionadas al cálculo de un RTO en activos de información.

Se realiza investigación de los diversas normas internacionales y metodologías que contienen diversos controles de seguridad de la información para protección de los activos de información. Tomando características, modelos, bases y todas aquellas herramientas que son de valor para el sector servicios. [4]

4.7. Análisis de metodologías.

Dentro del análisis de las metodologías se lograron identificar 4 metodologías interesantes que permitieron construir una nueva metodología que permite tener como prioridad la disponibilidad de los servicios dentro de una organización. Dentro del análisis de las diversas metodologías se encontraron múltiples orientadas a la recuperación de desastres o DRP (Disaster Recovery Plan), gestión de riesgos e impacto del negocio.

Se logra entender e identificar que el impacto sobre los activos de información va directamente asociado a la disponibilidad de estos, además que la gestión de riesgos de la información va orientada a la disponibilidad cuando se determinan los diferentes impactos que pueden afectar la prestación de los servicios a un activo de información. [62]

4.7.1. Metodología para el diseño de un plan de recuperación ante desastres o DRP.

La metodología está orientada para los sistemas de información críticos de TI en un plan de recuperación ante desastres o DRP. [55]

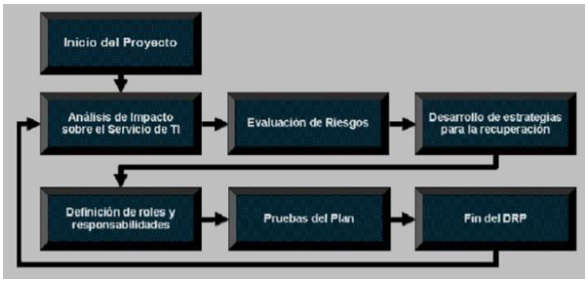
1. Inicio del proyecto Plan de Recuperación ante desastres.
2. Análisis de impacto sobre el negocio (BIA).
3. Análisis de riesgo.
4. Desarrollo estrategias de recuperación para el DRP.
5. Roles y responsabilidades.

6. Pruebas del DRP.

En la (Figura 4-5) define una metodología recomendada para el desarrollo de un plan de recuperación ante desastres o DRP para los sistemas de información críticos TI. Está basada en las recomendaciones del NIST, DRII y el BCI. Esta metodología tiene un valor importante para la construcción de la metodología propuesta en esta tesis ya que permite tomar características de valor para la construcción de una metodología optima en la recuperación de la disponibilidad de los activos de información.

Figura 4-5:

Metodología para un plan de recuperación ante desastres o DRP. (Metodología 1) [55]



Autor: Rodrigo Ferrer [55]**.**

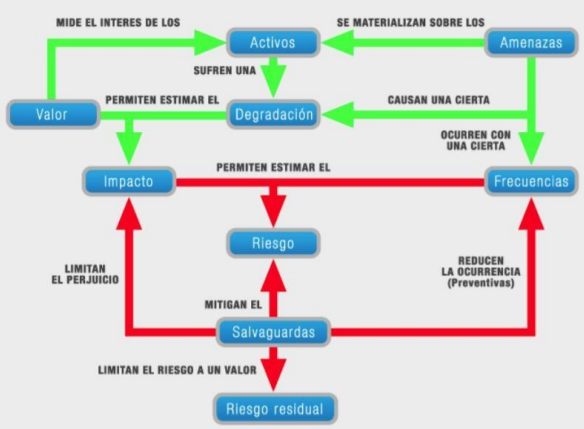
4.7.2. Metodología de análisis y gestión de riesgos de los sistemas de información.

Metodología que puedan identificar los procesos claves de la organización y se puedan tener presentes tres aspectos para el análisis de los riesgos: La criticidad de los recursos de información relacionados con los procesos críticos del negocio, El período de recuperación crítico antes de incurrir en pérdidas significativas y finalmente el Sistema de clasificación de riesgos.

En la (Figura 4-6) representa una metodología que permite identificar los procesos claves de la organización y presenta tres aspectos para el análisis de los riesgos. La criticidad de los recursos de información relacionados con los procesos críticos del negocio, El periodo de recuperación critico antes de incurrir en pérdidas significativas y finalmente el sistema de clasificación de riesgos. Esta metodología nos permite tomar características importantes para la construcción de la nueva metodología, ya que nos permite tener un panorama de los análisis que se realizan sobre los activos y así mitigar los riesgos aplicando correcciones oportunas y estrategias que permitan conservar la disponibilidad.

Figura 4-6:

MAGERIT (Metodología de análisis y gestión de riesgos de los sistemas de información.) (Metodología 2) [56]



Autor: Yisel Adriana Romero Romero [56]

4.7.3. Metodología para la gestión de la Continuidad de Negocio.

En la (Figura 4-7) define una metodología que propone un proceso que comprende la respuesta ante incidentes. Estableciendo procesos para la continuidad de negocio.

Figura 4-7:

Metodología para la gestión de la Continuidad de Negocio. [57]

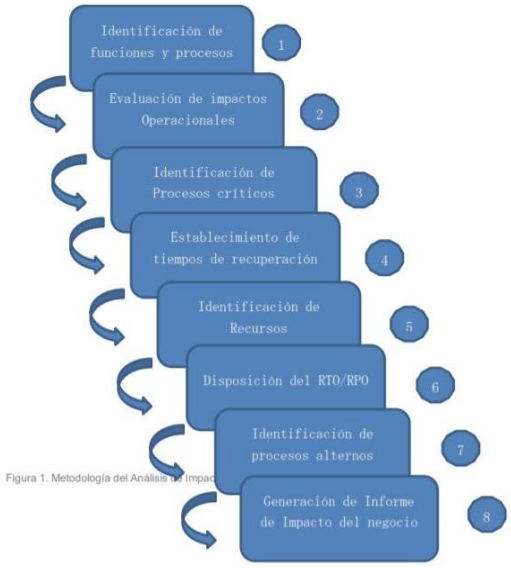
Autor: Rodrigo Ferrer V [57]

4.7.4. Metodología del análisis de impacto del negocio.

En la (Figura 4-8) define una serie de pasos interactivos con el objeto de identificar claramente los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre. Esta metodología es de gran valor para la construcción de la metodología ya que brinda parámetros relevantes al momento de identificar, clasificar y evaluar los activos.

Figura 4-8:

Metodología del Análisis de Impacto del Negocio [29]



Autor: MINTIC [29]

Teniendo presente el caso de estudio que va en función de las organizaciones del sector servicios puedan tener estrategias y procesos para lograr mantener la disponibilidad sobre los activos de información con los respectivos servicios que prestan estos para la operación de las diversas actividades que presta la organización.

Para ello se analiza cada una de las metodologías (Tabla 4-9) con el fin de tomar las consideraciones clave para el sector y así lograr elaborar una metodología eficiente que permita calcular un tiempo de recuperación optimo.

Tabla 4-9:

Evaluación comparativa de metodologías para la adquisición de consideraciones clave para la definición de un RTO.

METODOLOGIAS			
Metodología	**Características**	**Actividades**	**Consideraciones clave para el RTO**
Metodología para el diseño de un plan de recuperación ante desastres o DRP.	* Plan de recuperación ante desastres. * Análisis de riesgo. * Estrategias de recuperación. * Definición de roles. * Responsabilidades.	*Validar el objetivo de continuidad del proyecto. *Acordar el compromiso con las directivas. *Conformar el equipo del DRP. *Refinar el alcance del proyecto. *Identificar sitios físicos. *Identificar sistemas de información. *Evaluar la criticidad de los sistemas de información. *Determinar el RTO, RPO y MTD de cada sistema. *Identificar amenazas sobre los sistemas. *Identificar vulnerabilidades de los sistemas. *Cálculo de la probabilidad de ocurrencia de un evento.	*Análisis de riesgo *Estrategia de recuperación. *Alcance del proyecto. *Identificación de Activos. *Evaluar criticidad.
Metodología de análisis y gestión de riesgos de los sistemas de información.	*Análisis de Impacto sobre el negocio. *Impactos Operacionales. *Impactos Financieros. *Impactos Talento Humano. *Impactos Legales. *Impactos Reputacionales. *Gestión de Riesgos.	*Análisis de Activos. *Estimación de Valor. *Análisis de dependencias. *Análisis de criticidad. *Análisis de vulnerabilidades. *Análisis de Amenazas. *Análisis de Impactos. *Análisis de Riesgos. *Análisis de Frecuencias. *Estrategias de Continuidad de Negocio. *Respuesta a emergencias y operaciones.	*Análisis de Impactos. *Gestión de riesgos. *Análisis de activos. *Análisis de dependencias. *Análisis de Frecuencias. *Estrategias de Continuidad
Metodología para la gestión de la Continuidad de Negocio.	*Política de continuidad. *Compromiso de la alta gerencia. *Contexto de la organización. *Análisis de impacto al negocio. *Gestión de riesgos. *Estrategias de continuidad. *Estructura de respuesta a incidentes. *Revisión, mantenimiento y mejoras. *Planes de contingencia. *Planes de recuperación de desastres. *Plan de respuesta a ciberincidentes. *Planes de evacuación por edificio. *Plan de comunicación de crisis.	*Evaluar el impacto potencial de un incidente disruptivo. *Identificar las actividades que soportan la prestación de los productos y servicios. *Evaluar el impacto en el tiempo de no realizar las actividades propias del negocio. *Especificar los tiempos de recuperación. *Identificar dependencias y recursos.	*Contexto de la organización. *Estructura de respuesta. *Revisión, mantenimiento y mejoras. *Planeas de respuesta y recuperación. *Especificar los tiempos de recuperación. *Identificar las actividades que soportan la prestación del servicio. *Identificar dependencias y recursos.
Metodología del análisis de impacto del negocio.	*Identificación de funciones y procesos. *Evaluación de impactos Operacionales. *Identificación de procesos críticos. *Establecimiento de tiempos de recuperación. *Identificación de recursos. *Disposición del RTO/RPO. *Identificación de procesos alternos. *Generación de informe de Impacto del negocio.	*Listado de roles y procesos. *Identificación de elementos operacionales. *Identificación de activos. *Identificación de amenazas. *Identificación de vulnerabilidades. *Identificación de Tolerancia a fallas. *Análisis de criticidad. *Análisis de prioridades. *Análisis de procedimientos alternos. *Análisis de riesgos Tecnológicos, Humanos, Naturales. *Análisis de escenarios de amenazas. *Planes y estrategias de continuidad del negocio.	*Identificación de funciones y procesos. *Identificación de procesos críticos. *Identificación de procesos alternos. *Identificación de Tolerancia a fallas. *Análisis de procedimientos alternos. *Análisis de riesgos Tecnológicos, humanos y naturales.

Autor: Construcción Propia.

Nota: La anterior tabla sintetiza cada una de las metodologías extrayendo las características que benefician o aportan al proyecto como son los elementos clave para un cálculo más preciso del tiempo de recuperación sobre un activo de información.

Además, se realiza un análisis de las diversas normas internacionales (Tabla 4-10) que permitirán tomar todas aquellas características y ventajas clave que aportar significativamente a una metodología funcional y eficiente.

Tabla 4-10:

Comparativo de normas internacionales.

NORMAS			
Norma	**Características**	**Ventaja**	**Consideraciónes Clave**
ISO 22301	*Planes de gestión de continuidad de negocio. *Mejora la imagen de la organizacion. *Mejora en la revision y control de empleados. *Mejora en el registro de debilidades e incidentes. *Mejora en la gestión de la empresa en general.	*Identificar y gestionar las amenazas actuales y futuras para su empresa. *Tener la capacidad de resister a incidentes. *Enfoque proactivo para minimizar el impacto de los incidentes.. *Minimizar el tiempo de interrupción. *Adquirir una mayor flexibilidad ante la interrupción.	*Minimizar el tiempo de interrupción. *Enfoque proactivo para minimizar el impacto. *Identificar y gestionar amenazas. *Planes de continuidad de negocio.
DAFP Versión 4	*Politica de administración de riesgos. *Identificación del riesgo. *Valoración del riesgo. *Lineamientos sobre los riesgos relacionado con posibles actos de corrupción. *Lineamientos riesgos de seguridad de la información.	*Politica de riesgos. *Identificación de puntos de riesgo, areas de impacto, areas de factores de riesgo, clasificación del riesgo. *Analisis, evaluación, estrategias, herramientas, monitoreo y revision de riesgos. *Identificación de los activos, indentificación, valores de riesgo y controles asociados a la seguridad de la información.	*Politica de riesgos. *Identificación de puntos de riesgo, areas de impacto, areas de factores de riesgo, clasificación del riesgo. *Analisis, evaluación, estrategias, herramientas, monitoreo y revision de riesgos. *Identificación de los activos, indentificación, valores de riesgo y controles asociados a la seguridad de la información.¨ *Identificación, valoración y lineamientos asociados a los riesgos.
NIST 800-30 Rev.1	*Sugerencias, recomendaciones y operaciones a implementación de gestion de riesgos. *Fundamentos de seguridad de la información.	*Herramienta de mitigación y valoración en riesgos. *Bajo costo de implementación. *Mejora a la administración, informes sobre el análisis por riesgos identificados.	*Bajo costo de implementación. *Mejora a la administración, informes sobre el análisis por riesgos identificados. *Sugerencias, recomendaciones y operaciones a implementación de gestion de riesgos. *Fundamentos de seguridad de la información.
OCTAVE	*Subdivide los activos en sistemas y personas. *Evalúa cada riesgo de seguridad y establece plan de mitigación.	*Procesos de analisis, observación y gestión sobre los riesgos. *Involucra a los trabajadores de la organización. *Involucra los procesos,departamentos, recursos, activos, amenazas y salvaguardas.	*Involucra los procesos,departamentos, recursos, activos, amenazas y salvaguardas. *Subdivide los activos en sistemas y personas. *Evalúa cada riesgo de seguridad y establece plan de mitigación.
MAGERIT	*Define alcance *Analisis de riesgos. *Implementación de controles. *Activos, vulnerabilidades, impactos, riesgos y salvaguardas. *Controles a los elementos. *Planificacion del proyecto de riesgos. *Gestión de riesgos.	*Metodo sistematizado para analizar los riesgos. *Ayuda a identificar y planificar medidas necesarias para reducir los riesgos. *Brinda herramientas que ayuda a facilitar en analisis de riesgos. *Seguimiento y Mejora continua. *Analisis de activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas.	*Analisis de riesgos. *Implementación de controles. *Activos, vulnerabilidades, impactos, riesgos y salvaguardas. *Controles a los elementos. *Planificacion del proyecto de riesgos. *Gestión de riesgos. *Seguimiento y Mejora continua. *Analisis de activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas.
ISO 27005:2018	*Contexto de la organización. *Compromiso de la alta direccion.(Liderazgo y Sistema de gestión de la información). *En apoyo de los recursos. *Comunicación y consulta de los riesgos para la seguridad de la información. *Criterios de evalución del riesgo. *Criterios de impacto. *Criterios de aceptación del riesgo. *Evaluacion del riesgo.	*Tecnicas de seguridad y gestion de la seguridad de la información. *Gestion de riesgos. *Planificacipon, liderazgo, soporte, operación, evaluación y mejora. *Plan de comunicación interno y externo. *Contextualizacion de la organización. *Valoración de los riesgos. *Tratamiento de riesgos.	*Criterios de evalución del riesgo. *Criterios de impacto. *Criterios de aceptación del riesgo. *Evaluacion del riesgo. *Valoración de los riesgos. *Tratamiento de riesgos. *Tecnicas de seguridad y gestion de la seguridad de la información. *Gestion de riesgos. *Planificacipon, liderazgo, soporte, operación, evaluación y mejora.
ISO 31000	*Contexto de la organización. *Liderazgo y compromiso. *Asignación de recursos. *Comunicación y consulta. *Definición de los criterios del riesgo. *Definición del alcance. *Asignación de roles, autoridades, responsabilidades y obligaciónes. *Evaluación del riesgo. *Tratamiento del riesgo. *Mejora continua.	*Mejorar su eficiencia operativa. *Tener una mejor gobernabilidad interna de la organización. *Aumentar la confianza de partes externas. *Mejorar su rendimiento y la sostenibilidad. *Acentuar su calidad. *Reducir los costes. *La disminución o desapariçon de incidentes inesperados. *Mejora la calidad de la información. *Mejora la gestión organizacional. *Mejora los indicadores de seguridad y salud en el trabajo. *Minimiza el impacto negativo de los incidentes y accidentes. *Gestion de riesgos proactiva.	*Evaluación del riesgo. *Tratamiento del riesgo. *Mejora continua. *Mejora los indicadores de seguridad y salud en el trabajo. *Minimiza el impacto negativo de los incidentes y accidentes. *Gestion de riesgos proactiva.

Autor: Construcción Propia.

Nota: En anterior tabla se interrelacionan cada una de las normas con el fin de identificar las características y adoptar todas aquellas ventajas que son consideraciones clave para el RTO.

Luego de analizar cada una de las características, actividades y ventajas tanto de las metodologías y normas internacionales que existentes para el RTO, se logra obtener múltiples consideraciones clave para lograr que el sector servicios tenga disponibilidad sobre los activos de información que utiliza para la prestación de sus servicios. La aplicación del conjunto de estas consideraciones es de gran valor para la elaboración de una nueva metodología más eficiente.

Esto permite cumplir la necesidad del caso de estudio de lograr que los activos de información estén disponibles, además de que el sector tenga una herramienta útil y un proceso de mejora continua para el calculo de los tiempos objetivos de recuperación sobre sus activos, así buscando hacer los procesos mas seguros, permitiendo así realizar estrategias y planes de mejora sobre los activos de información.

5. Validación de metodologías sobre caso de estudio en Empresa de servicios del Valle de Aburra.

En esta etapa se procede a validar la aplicabilidad de las diversas metodologías al sector servicios y en concreto al caso de estudio, identificando las características que aplican en función de cada una de las etapas de las metodologías, así tomando las características de valor, esto con el fin de determinar múltiples características que permitan construir una metodología eficiente y útil para el sector servicios.

5.2. Descripción del negocio.

Por seguridad no se mencionará el nombre de la compañía en la cual se realiza el análisis de las diversas metodologías. Para ser prácticos le daremos en nombre de Ejemplo S.A.S.

Ejemplo S.A.S es una compañía ubicada en la ciudad de Medellín – Colombia con una trayectoria de 21 años en sector de servicios, prestando sus servicios a clientes (Grande, Mediana, y Pequeña empresa de cualquier Sector Económico), su misión es proporcionar soluciones en la entrega de mercancías en diferentes ciudades.

5.3. Diagnóstico Inicial.

Antes de implementar las diversas metodologías investigadas para la identificación de los tiempos objetivos para la recuperación de los activos críticos, se realiza un diagnóstico inicial del estado de implementación desde 3 criterios. El primero identificar los procesos que tiene la compañía, Segundo identificando los activos de la organización y tercero identificando los procesos que se tienen sobre estos activos.

Se identifican algunas de las siguientes variables en la (Tabla 5-1) según las características de la organización de caso de estudio para la prestación de sus servicios y características propias del funcionamiento.

Tabla 5-1:

Algunas características del sector servicios.

Caracteristicas Sector Servicios
Jornada Operacional Laboral Ejemplo: 12 / 18 / 24 Horas
Empleados / Vidas / Cerebros
Costo Activos
Activos Nube / Local
Sedes
Aspectos Ambientales
Sector de prestacion de Servicios / Conexiones con clientes
Confianza - reputacion

Autor: Construcción Propia.

Nota: Al analizar el sector servicios, se observan algunas características importantes para el funcionamiento de la organización, esto es relevante ya que permite identificar como presta la organización los diferentes servicios al medio y que infraestructura debe tener.

5.4. Implementación de las metodologías.

Se realiza inicialmente una reunión con el gerente de la compañía y con los ingenieros a cargo del área de sistemas, con el fin de contextualizarlos acerca del interés de analizar diversas metodologías para identificar si aplican sobre su operación y lograr obtener las características necesarias para resaltar los principales aspectos los cuales permitirán construir una metodología

universal para la identificación de los tiempos objetivos de recuperación sobre los activos de información críticos.

Se indagó y se revisaron cada una de las características de cada metodología con el fin de verificar su aplicación e identificar las necesidades que pudiesen presentar el propósito de identificar los activos críticos, su impacto en el sector y los tiempos óptimos y objetivos que debe tener el activo para la conservación y la continuidad del negocio.

Luego de identificar los procesos y características de cada metodología se procede a aplicar en conjunto con el área de sistemas cada una de estas, se realiza un análisis de la organización y de sector servicios, identificando las fases más relevantes de cada metodología y las debilidades con el propósito de construir una metodología eficiente y aplicada a la continuidad de negocio orientada al sector servicios y al cálculo de los tiempos objetivos de recuperación que deben tener los activos críticos de la organización.

5.5. Conclusiones y aplicabilidad de las metodologías.

Al realizar un análisis de cada una de las metodologías investigas, sus características y flujo de cada uno de ellas aplicadas al sector servicios y teniendo como premisa el funcionamiento, las necesidades, cualidades y particularidades del sector se realizó la siguiente tabla que permite identificar la aplicabilidad y tomar de cada una de las metodologías aquellas características que permiten construir una metodología orientada al sector con el fin de lograr determinar los tiempos de recuperación sobre los activos críticos y así brindar una alternativa eficiente para la continuidad de negocio.

En la (Tabla 5-2) presenta las diferentes metodologías con respecto a las diferentes características que tiene el sector servicios con el fin de determinar si dicha variable es aplicable en las metodologías. Y así evaluar las diferentes características, etapas y fases que tiene cada metodología y tomar las cualidades y herramientas que contine cada una estas para así construir una metodología optimizada y eficiente que aplique al sector servicios y permita tener procesos solidos sobre sus activos de información.

Para validar las metodologías, se realizó un análisis de acuerdo con el sector servicios, en los parámetros de funcionamiento y en base los activos que utilizan en estas organizaciones. Se procedió a realizar una tabla de validación de las metodologías con respecto a las características de la organización caso de estudio del sector servicios. Así visualizando, obteniendo una tendencia de las características que aplican y así tomar todas aquellas características de utilidad para el sector y así generar una metodología eficiente.

Tabla 5-2:

Aplicabilidad y validación de las metodologías sobre las características del sector servicios en función del caso de estudio.

- **Metodología 1:** Metodología para un plan de recuperación ante desastres o DRP. (Metodología 1) [55] (Figura 3-5).
- **Metodología 2:** MAGERIT (Metodología de análisis y gestión de riesgos de los sistemas de información.) (Metodología 2) [56] (Figura 3-6).
- **Metodología 3:** Metodología para la gestión de la Continuidad de Negocio. [57] (Figura 3-7).
- **Metodología 4:** Metodología del Análisis de Impacto del Negocio [29] (Figura 3-8).

	Metodologia 1	Metodologia 2	Metodologia 3	Metodologia 4
Variables				
Jornada Laboral 12/24	APLICA	N/A	N/A	N/A
# Empleados / Vidas / Cerebros	APLICA	APLICA	APLICA	APLICA
Costo Activos	APLICA	APLICA	N/A	N/A
Activo Nube/Local	APLICA	APLICA	APLICA	APLICA
# Sedes / Aspectos ambientales	APLICA	APLICA	APLICA	APLICA
Sector Servicios / Conexión con los clientes	APLICA	APLICA	APLICA	APLICA
Confianza, reputacion	APLICA	APLICA	APLICA	APLICA

Autor: Construcción Propia.

Dicha validación de aplicabilidad de cada una de las metodologías se analiza según el flujo de operación del sector servicios, ya que para el sector servicios es de gran importancia la disponibilidad de los servicios de información, dado esto se analiza cada metodología y se verifica su aplicabilidad sobre las diferentes variables que tiene el sector, este análisis se realiza identificando todas las características de cada metodología, permitiendo tomar características clave que permitirán construir una nueva metodología que permita al sector servicios aplicar métodos y procesos que permitan minimizar los tiempos de recuperación y tener claridad sobre los procesos a realizar ante una indisponibilidad.

6. Metodología para determinación de los tiempos objetivos de recuperación RTO de los activos de información críticos en una estrategia de continuidad de negocio BCP en el sector de servicios en Colombia.

Teniendo en cuenta que la propuesta de una metodología orientada al RTO de los activos críticos de información, se considera el estado actual de las metodologías utilizadas en función de la estrategia de continuidad de negocio, para brindar disponibilidad a los activos de información.

Antes de plantear la metodología propuesta, se realizó un estudio de las diversas normas y metodologías de seguridad de la información y gestión de riesgos, las cuales brindan múltiples características importantes para la metodología que se presenta al final de este capítulo.

Luego de identificar las diversas características del sector servicios o sector terciario y las diferentes características, criterios, elementos, parámetros y secuencias de las metodologías analizadas y teniendo presentes las diferentes normas internacionales se procede lo siguiente:

6.1. Técnica definida para la investigación.

Se define como técnica de investigación mixta ya que durante la investigación se realiza la recolección, análisis de datos, comportamientos del medio, investigaciones sociales y del mercado. Además de técnicas documentales, experimentales y de campo. Para el caso de estudio se realizan búsquedas documentales, estudio correlacional y estudio causal - comparativo.

Durante el proceso de investigación se evidencian múltiples características tanto para la organización objeto del caso de estudio como del sector en general, teniendo presente la empresa del caso de estudio validada y analizada en el capítulo 5. Todo con el fin de conocer mas sobre el sector servicios, sus características, necesidades, compromisos, obligaciones, niveles de servicio, etc. Para el correcto funcionamiento de las operaciones para la prestación de sus servicios. Teniendo como prioridad la disponibilidad de los servicios que prestan los activos de información.

En la fase de apropiación, se comienza a investigar como por medio de herramientas tecnológicas y por cultura general de las organizaciones se pueda innovar. Además, la aplicación de diversos controles, la aplicación del conocimiento adquirido a nivel laboral, de enseñanza y de conocimiento general. Para así lograr que las diferentes organizaciones tengan diferentes planes, procesos y estrategias de mejora continua sobre los activos de información con la intención de mantener la disponibilidad de sus servicios.

6.2. Análisis de normas y metodologías de continuidad de negocio.

Al realizar el análisis de las diversas normas y metodologías que corresponden a nivel de la organización como son el contexto del sector de servicios, tener disponibilidad y mejora continua para la planificación y conocimiento sobre los procesos de RTO sobre los activos.

Finalmente, al analizar las diferentes metodologías y visualizar que todas coinciden con en el análisis e impacto del negocio, todo con el fin de brindar disponibilidad a los activos, adicionalmente se evidencia que es necesario la mejora continua para optimizar los tiempos de recuperación sobre los activos, ya que los activos constantemente están en renovación, con incrementos exponenciales a nivel de información y de dependencias.

Además, las diferentes normas planteadas se enfocan en la disponibilidad, integridad y confidencialidad de los servicios informáticos. Dando como parámetro fundamental para el sector servicios la disponibilidad de los activos y por medio del flujo de análisis e identificación de las

características de los activos de información y así construir un proceso de recuperación efectivo planteando estrategias óptimas para un RTO efectivo sobre los diferentes activos.

6.2.1. Resumen y conclusiones de análisis de metodologías.

- Considerando los múltiples procesos de las metodologías, las cuatro se enfocan en la seguridad de la información como en la disponibilidad de los servicios que prestan los activos de información, que brinda a la organización productividad y sostenibilidad en la prestación de sus servicios.

- Al analizar a las metodologías y visualizando las diferentes cualidades que tiene cada una de ellas y tomando de cada una de estas las características indispensables y necesarias para la continuidad del negocio en el sector servicios y brindando la posibilidad de las diferentes organizaciones de planificar y visualizar alternativas para la restauración de sus activos.

- La aplicabilidad de las diversas metodologías brinda constante análisis de impacto del negocio y continuidad de negocio para lograr una gestión de riesgos en los activos, esto brindando información de valor para que se identifiquen cualidades objetivas que permitan tener parámetros y variables consideradas en tiempo. Así identificando los diversos tiempos al momento de realizar una restauración de un activo de información y sus dependencias o configuraciones.

- Al validar las diversas metodologías en el caso de estudio al proceder a implementarla, se encuentran múltiples vacíos que no aplican para el sector, es importante que al momento de aplicar una metodología en la organización verificar si cada una de sus fases cumple al momento de implementarla en la organización, esto es de gran valor para el éxito de los resultados que se esperan al momento de implementar una metodología.

- Se evidencia la gran cantidad de variables que se tienen para el análisis de la recuperación de un activo de información, esto limitando un cálculo exacto, además de la ausencia de procesos para determinar este tiempo de una manera práctica. La investigación se limita dado los criterios y variables que se deben tener en cuenta para el cálculo del tiempo de recuperación de un activo de información, para ello se toma como referencia los impactos del activo según su inoponibilidad, dejando abierta esta investigación para la continuidad del análisis. Dado esto se construyó una metodología en función al PHVA, permitiendo que esta tenga una mejora continua, que permita optimizar los cálculos de recuperación de un activo de información.

6.3. Elaboración de metodología para determinación de los tiempos objetivos de recuperación RTO de los activos de información críticos en una estrategia de continuidad de negocio BCP en el sector de servicios en Colombia.

Una vez analizadas las metodologías y normas internacionales, las metodologías y los controles existentes para proteger los activos de información, se elabora una metodología para la determinación de los tiempos objetivos de recuperación del sector servicios de Colombia.

La (Figura 6-2) ilustra la metodología desarrollada, la cual se basa en el ciclo de Deming PHVA, el planear (P) se encuentra en las fases de contexto, alcance y el corazón para la determinación de la importancia de los activos, el hacer (H) se encuentra en el gestionar, evaluar y calificar los activos de información críticos dentro de la organización, además se incluye la fase de verificación y estrategia para la reducción del tiempo de recuperación y la mejora continua (A). Como lo describe la (Figura 6-1).

6.3.1. Desarrollo.

Esta metodología propone en base a las fases de PHVA, realizar un análisis de la organización en general, identificando los activos críticos de información, evaluándolos y calificándolos con el fin de lograr tener un contexto claro de su utilidad dentro de la organización, dando así una visión de cuánto puede tardarse la recuperación de este activo en caso de un desastre y permita dar continuidad al negocio, nos permite tener una mejora continua.

En la (Figura 6-1) permite conocer el flujo de la herramienta conocida como Ciclo PHVA para la mejora continua. Según lo investigado en las diversas normas internacionales, se toma esta herramienta por su comprobada eficacia. Esta herramienta se encuentra vigente y en la actualidad este sistema o método de gestión de calidad permite tener mejora continua, progresiva y constante en la aplicación de esta en las organizaciones. Conocido por el ciclo sin fin. [63]

Esta herramienta es utilizada y aplicada a la construcción de la metodología, ya que permite aplicar sus características con el fin de que la metodología propuesta sea optima y que permite a la organización mantener un ciclo de mejora continua, ya que este se reinicia una y otra vez de manera periódica. Adicionalmente sirve como fuente de aprendizaje para que en cada una de las etapas se pueda mejorar y aprender de los errores. Así buscando constantemente la optimización de las acciones por medio del análisis de los resultados encontrados en cada una de sus fases. [63]

Figura 6-1:

Ciclo PHVA.

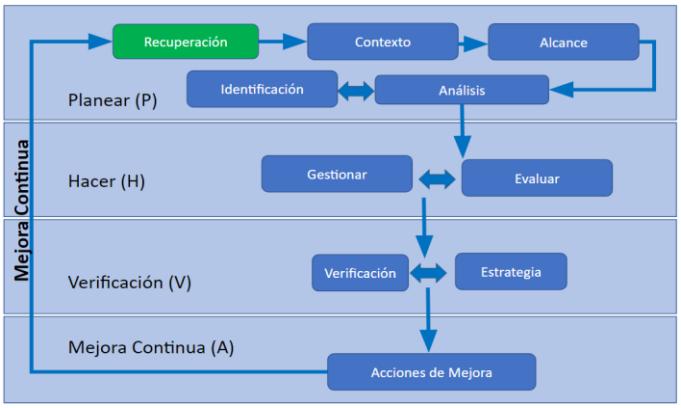
Autor: SafetYA [59].

Nota: De acuerdo con la anterior (Figura 6-1) se realiza la aplicación de las diversas fases a la siguiente metodología permitiendo separar procesos de valor en flujo de esta. Así brindando valor, optimización, eficiencia y resultados concretos para el mejoramiento de los tiempos de recuperación para el mantener los servicios disponibles en el sector el mayor tiempo posible.

A continuación, en (Figura 6-2) se presenta el flujo de la metodología propuesta, definida según la (Figura 6-1) basada en las 4 fases del ciclo y en cada fase se realizan múltiples etapas que permiten a una organización lograr realizar un cálculo objetivo de recuperación de los activos que utiliza para la prestación de múltiples servicios. Esta metodología propone el uso y la aplicabilidad de la guía propuesta alineada al modelo de fases PHVA.

Figura 6-2:

Metodología elaborada para la determinación de los tiempos objetivos de recuperación RTO.



Autor: Construcción Propia.

Nota: Se construye una metodología que a través de un flujo continuo permite que se realice una reducción del tiempo de recuperación de los activos de información para permitir la continuidad

de negocio y permitiendo a la organización realizar un mejoramiento continuo y optimización de los procesos de recuperación, así manteniendo la disponibilidad de los servicios y conociendo claramente las diversas características de sus activos.

- **Fase I - Diagnóstico Inicial:** Busca establecer las características del servicio y el estado de los activos de la organización, conociendo las políticas, controles y procedimientos con respecto a la gestión de los activos de información.

- **Fase II – Definición del contexto y alcance:** El contexto hace referencia a la identificación de los aspectos internos y externos que tiene organización prestadora de servicios, como se encuentra conformada esta, adicionalmente entender como están distribuidos sus procesos y dependencias. El alcance describe hacia donde se orienta en análisis de la organización, puede ser toda la organización, alguna parte de la organización, dependencia, un proceso que presta un servicio en particular o un sistema de información. Esta fase se ubica en la planeación (P) del modelo PHVA (Figura 6-1) y en la metodología propuesta (Figura 6-2).

- **Fase III: Análisis e Identificación:** El análisis y la identificación es la etapa que permite conocer los diferentes activos que tiene la organización, entender su funcionamiento, características y especificaciones. Las cuales permitirán tener claridad al momento de identificar su criticidad y así identificar los tiempos de recuperación que al momento de esta etapa se encuentran. Esta fase se ubica en la planeación (P) del modelo PHVA (Figura 6-1) y en la metodología propuesta (Figura 6-2).

- **Fase IV: Evaluar y gestionar:** Hace referencia a conocer, clasificar, evaluar los procesos que realiza un activo de información, conocer los niveles de criticidad e impactos que podrían tener los activos en ausencia a la disponibilidad del servicio. Esta fase buscar reconocer todas aquellas características, procesos, dependencias, cualidades de estos. Esta Fase se ubica en el hacer (H) del modelo PHVA (Figura 6-1) y en la metodología propuesta (Figura 6-2).

- **Fase V: Estrategia y Verificación:** De acuerdo con los resultados obtenidos en la caracterización de la organización e identificación de los activos de información, así conociendo

cual es el estado actual de la organización y procesos a realizar ante una ausencia de disponibilidad. Así construyendo estrategias de mejora, mitigación, optimización de pro de conservar y mantener la disponibilidad del servicio. Esta fase se ubica en (V) del modelo PHVA (Figura 6-1) y en la metodología propuesta (Figura 6-2).

- **Fase VI: Acciones de Mejora:** Se realiza un análisis de la información obtenida durante el proceso de identificación de las características de la organización y las características de los activos de información orientados al servicio que deben tener disponibilidad. Se elabora una lista de características con las que cuenta la organización en la actualidad. Se ubica en el Actuar (A) del modelo PHVA (Figura 6-1) y en la metodología propuesta (Figura 6-2). Esto con El fin de buscar realizar mejoras o estrategias que permitan minimizar los tiempos de recuperación en función de la disponibilidad de los activos de información de la organización.

- **Fase VII: Mejora Continua:** Es la fase final de la metodología, según sea verificado el estado actual de los activos de información y la determinación de los tiempos objetivos de recuperación en función de las características identificadas en la tesis, se debe continuar en investigación, planificación, estrategias, correcciones para minimizar los tiempos de recuperación y así permitir mantener la disponibilidad de los activos de información.

6.3.2. Guía y desarrollo de la metodología propuesta.

Al tener presente el ciclo PHVA para mejora continua en el desarrollo de las actividades, esta metodología está dirigida a los lideres de proceso y profesionales en sistemas de información o afines. Con ello se busca que estos, continúen con la investigación constante de estrategias que propongan mejoras en la gestión de los activos de información con el fin de brindar disponibilidad a los diversos activos que prestan servicios en la organización, conociendo claramente los procesos internos y la recuperación objetiva y eficiente.

Para la determinación de los tiempos y puntos objetivos sobre los activos según la metodología propuesta, es necesario realizar los siguientes pasos:

6.3.2.1. Fase Planear: Diagnostico Organizacional.

En la (Tabla 6-1) se visualizan los procesos iniciales (Fase Planear), en esta fase se logra tener un contexto general tanto de la organización como de los servicios y activos que utiliza la organización a sus diferentes labores. En esta fase se establece una meta, se separan los diferentes parámetros de seguridad y se identifican los diferentes activos según su relevancia. Esta fase permite tener un panorama general de la organización

Tabla 6-1:

Ciclo PHVA (Fase Planear) Metodología Propuesta.

PLANEAR	
1. (Contexto) Identifique características, servicios, cualidades, modo de operación y generalidades de la organización.	
2. (Alcance) Determinar los activos de informacion y priorizarlos según la disponibilidad.	
3. (Análisis)	
	3.1. Construya o actualice su inventario de activos de información que son utilizados y gestionados en los procesos de la organización.
	3.2. Identifique y clasifique vida util del activo. (Tenga en cuenta si al activo lo han actualizado, esto puede extender la vida util de este) Tenga en cuenta la **(Tabla 2-1)**
	3.3. Clasifique por criticidad los activos documentados en el numeral (3.1) de acuerdo con la **(Tabla 3-4)** teniendo en cuenta la **(Tabla 3-3)**.
	4.4. Seleccione métricas posibles que pueda medir sobre el activo para determinar la criticidad de este.
Confidencialidad	
	3.4. Clasifique los activos de información de acuerdo a la confidencialidad. (Si la información es restringida, privada o publica). **(Tabla 3-3)**
Integridad	
	3.5. Clasifique los activos de información de acuerdo a la Integridad. Debe tener en cuenta la disposición exacta y completa que debe tener la información. (Clasifique en Alta, Media, Baja). **(Tabla 3-4)**
Disponibilidad	
	3.6. Clasifique los activos de información de acuerdo a la disponibilidad. Hace referencia a que la información siempre debe estar accesible y útil para ser consultada. (Clasifique en Alta, Media, Baja). **(Tabla 3-2)**
(Identificación) Identifique el activo informático y realizar el reconocimiento de sus características, especificaciones, utilidad, tareas, descripción detallada.	
	4.1. Categorice el activo ya que es ideal para identificar procesos o dependencias.
	4.5 Describa características del activo (Cantidad de Información), identifique backups (Tiempos entre backups, tipo, forma, ubicación de las copias, proveedor y cantidad de copias),
	3.7. Identique la criticidad del activo en función de la disponibilidad ya que es esencial para la continuidad del negocio tomando en cuenta el numeral (3-2).
	3.8. Determine un tiempo en el cual se debe restaurar la disponibilidad del activo seleccionado y establezcalo como una base de referencia.
(Salida)	
	Inventario de activos actualizado y categorizado en criticidad según la disponibilidad.

Autor: Construcción Propia.

6.3.2.2. Fase Hacer.

En la (Tabla 6-2) representa la Fase Hacer, esta es la fase que representa el corazón de la metodología, en esta fase se pretende describir las características y pasos para el cálculo del RTO, para ello es importante realizar la identificación de características, especificaciones, dependencias, conexiones e información en general del activo, se evalúan los diferentes impactos que puede tener el activo para así determinar su nivel de impacto.

Esta fase brinda un diagnóstico general sobre el activo, permitiendo a la organización conocer el estado de este y calcular un tiempo de recuperación, además de conocer los impactos que puede tener este ante la indisponibilidad.

Tabla 6-2:

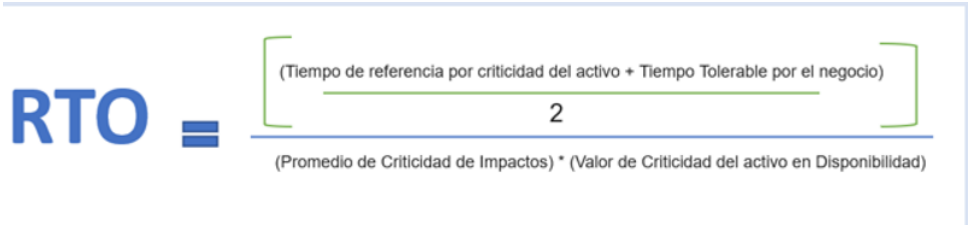
Ciclo PHVA (Fase Hacer) Metodología Propuesta

HACER	
4. (Gestionar)	
	4.3. Gestione y organice un diagrama donde se tenga en cuenta la cantidad de procesos organizacionales o sistemas de información tienen dependencia con la disponibilidad del activo identificado.
(Evaluar)	
	4.6. Identifique el tiempo en que puede la organización operar ante la ausencia del servicio que presta el activo de información. De acuerdo a la **(Tabla 4-4)** sobre el impacto operacional.
	4.7. Evalue los impactos financieros, es importante identificar las afectaciones financieras ante la indisponibilidad del activo. Utilice **(Tabla 4-3)**
	4.8. Evalue los impactos legales, es importante identificar las afectaciones legales ante la indisponibilidad del activo, lo que puede generar multas afectando financieramente la organizacion. Utilice **(Tabla 4-5)**
	4.9. Evalue los impactos reputacionales, es importante identificar las afectaciones en la imagen de la organización ante la indisponibilidad del activo. Utilice **(Tabla 4-6)**
	4.10. Evalue según la **(Tabla 4-8)** cuantas son las horas de indisponibilidad del activo que podría asumir como lo es una perdida o reproceso sin generar impactos financieros u operacionales a la organización, teniendo como presente los niveles de impactos identificados en los numerales 4.6, 4.7, 4.8 y 4.9.
	4.11. Evalue y determine cuanto tiempo le tomaria a la organización notificar a los usuarios y/o clientes sobre la indisponibilidad del activo.
	4.12. Evalue, analice, determine y pruebe cuanto tiempo aproximado puede tardar la restauracion de una copia de seguridad o Backup este accesible y funcional. Este tiempo corresponde al RTA (Tiempo de restauracion actual o real).
(Salida)	
	Teniendo en cuenta los numerales anteriores realice la siguiente formula para calcular un RTO. $RTO = \frac{\left[\frac{\text{(Tiempo de referencia por criticidad del activo + Tiempo Tolerable por el negocio)}}{2}\right]}{\text{(Promedio de Criticidad de Impactos) * (Valor de Criticidad del activo en Disponibilidad)}}$

Autor: Construcción Propia.

Nota: Los tiempos deben darse en una misma unidad de tiempo (Minutos, Horas, Días)

Según la fase anterior, se propone una formula en función de la evaluación de los numerales contenidos en esta fase para el cálculo del tiempo objetivo de recuperación de un activo de información, esta se describe de la siguiente manera.



La fórmula anterior consta de 4 variables las cuales se describen a continuación, dichas variables fueron determinadas con el fin de obtener un tiempo según la criticidad del activo en función de los impactos que tiene este ante una indisponibilidad.

- Tiempo de referencia por criticidad del activo (**Tabla 4-8**): Es un tiempo de recuperación de referencia que se obtiene de acuerdo con el promedio de criticidad del impacto del activo y se fija como el valor medio del rango que le corresponda de la tabla 4-8.
- Tiempo tolerable por el negocio: Es un tiempo que el negocio está dispuesto a tolerar.
- Promedio de criticidad de impactos (**Tabla 4-3, 4-4, 4-5 y 4-6**): Es un promedio que se calcula numéricamente proveniente de los impactos financiero, reputacional, operacional, legal. Catastrófico (5), Mayor (4), Moderado (3), Menor (2), Insignificante (1)
- Valor de criticidad del activo en Disponibilidad (**Tabla 3-2**): Corresponde a la criticidad del activo con respecto a su disponibilidad Alto (3), Medio (2), Bajo (1).

Dichas variables dan como resultado un valor en tiempo, el cual corresponde a un tiempo objetivo de recuperación del activo de información. La cual debe ser tenida en cuenta en el mejoramiento continuo de cada una de las fases de la metodología propuesta.

6.3.2.3. Fase Verificar.

En la (Tabla 6-3) se presta la fase Verificar, esta fase consiste en realizar dos procesos de valor, Verificar que establece la revisión y confirmación de los resultados obtenidos, realizar pruebas e identificar todas aquellas variables del activo, teniendo una visión completa de este. Adicionalmente establece estrategias para la recuperación y mitigación de impactos sobre el negocio ante la indisponibilidad del activo, esto en función de la continuidad de negocio.

Tabla 6-3:

Ciclo PHVA (Fase Verificar) Metodología Propuesta.

VERIFICAR	
5. (Verificar)	
	5.1. Verifique y revise las condiciones actuales del activo.
	5.2. Verifique los resultados obtenidos en las fases PLANEAR y HACER. Y convierta los valores en horas y minutos los tiempos obtenidos.
	5.3. Realice verificacion, pruebas y diagnosticos sobre la informacion del activo y verifique integridad o veracidad de las copias de seguridad.
	5.4. Realice un análisis de los riesgos, valore los riesgos que puede tener el activo.
(Estrategia)	
	5.5. Plantee una estrategia para la recuperacion del activo.
	5.6. Establezca procesos de mejora y auditoria sobre los activos de informacion según su criticidad.
	5.7. Establezca prioridades, limitaciones, tolerancia, controles para la mitigacion de impactos y minizar la criticidad del activo.
(Salida)	
	Validacion de resultados obtenidos y planes para la recuperacion de la indisponibilidad del activo.

Autor: Construcción propia.

6.3.2.4. Fase Actuar.

En la (Tabla 6-4) se presenta la fase actuar, la última fase de la metodología propuesta que tiene una conexión directa con la fase planear, que está conectada por la mejora continua. Esta Fase representa en momento donde se toman acciones para minimizar tiempos, documentar procesos, realizar cambios, identificar múltiples variables de los activos y planear o establecer estrategias en función de la mejora.

Tabla 6-4:

Ciclo PHVA (Fase Actuar) Metodología Propuesta.

ACTUAR	
6. (Acciones de Mejora)	
	6.1. Establezca procedimientos y planeaes para incorportar las lecciones aprendidas, la documentacion de estas y la generacion de controles sobre cada proceso.
	6.2. Evalue las condiciones y los servicios de conexión que tiene en la organización. Identifique proveedor de servicios de internet y sus características como (Velocidades de subida y descarga),(Estabilidad), identifique si tiene restricciones. Es importante evaluar las condiciones en caso de un desastre para proceder con la restauración del activo.
	6.3. Teniendo en cuenta las velocidades de (Subida y Descarga) y teniendo en cuenta la informacion contenida en el activo. Realice el Calculo de cuanto tardaria descargar esa cantidad de informacion y cuanto tardia subirla. Teniendo en cuenta la siguiente formula: 1byte = 8bit, 8/8 = 1 megabytes por segundo. Así pues, en un minuto (60 segundos) el usuario puede descargar 1*60 = 60 megabytes.
	6.4. Establezca un procedimiento para la aplicación de controles y estrategias que permitan reducir los tiempos de recuperacion objetivos previamente cálculado.
7.(Mejora Continua)	
	7.1. Establezca procesos de mejora continua y validaciones con un tiempo de frecuencia o periodicidad, con el fin de minimizar los tiempos de recuperacion, niveles de criticidad e impactos a la organización ante la ausencia o indisponibilidad del activo de informacion seleccionado.
(Salida)	
	Retroalimentacion, aprendizaje y experiencia según resultados obtenidos para recorrer una y otra vez cada fase con el fin de una mejora continua, en busca de minimizar los tiempos para la recuperación del activo de información.

Autor: Construcción propia.

6.4. Análisis de la metodología propuesta en caso de estudio (Empresa Valle de Aburra).

Se realizo la implementación de la metodología sobre el caso de estudio obteniendo diversos resultados que permiten tener claridad sobre los activos críticos de la información y se permite tener un panorama al momento de la recuperación y restauración de dichos activos, generando así conciencia en la organización lo que permite tener mejoras continuas sobre cada proceso y estar preparados de cómo proceder al momento de una situación catastrófica o un desastre que no permita tener disponibilidad sobre los activos críticos de las organizaciones prestadoras de servicios.

Se logra evidenciar las cualidades y características tomadas por las metodologías investigada y en la elaboración de esta nueva metodología, que nos permite tener un flujo de análisis y evaluación detallado de las características de cada activo y así permitiendo tener una visión de como poder proceder a la recuperación del activo, ya que este es parte importante de la organización en la prestación de sus servicios. También permitiendo el análisis, verificación y pruebas continuas para el mejoramiento continuo de los activos de información y los procesos para la implementación RTO. Así teniendo alertas y proyecciones en la remediación de incidentes sobre los activos.

Al recorrer la metodología permite generar incógnitas para la corrección y aplicación de estrategias para tener control y planificar sobre los activos de información. Así dando paso al análisis en la construcción de una herramienta informática orientada a la web para el uso de las diversas organizaciones, así permitiendo el análisis y la evaluación de los tiempos objetivos de recuperación sobre los activos de la empresa, teniendo como premisa la mejora continua en la disminución de los tiempos al momento de una restauración del servicio prestado por un activo informático.

7. Herramienta informática, de acuerdo con la metodología diseñada.

Las Herramientas informáticas, son programas, aplicaciones o simplemente instrucciones usadas para efectuar otras tareas de modo más sencillo. En un sentido amplio del término, podemos decir que una herramienta es cualquier programa o instrucción que facilita una tarea, pero también podríamos hablar del hardware o accesorios como herramientas. [65]

De acuerdo con la definición anterior se construyo el siguiente diagrama para tener referencia de las características, funcionalidad y resultado final que debe arrojar la herramienta informática a construir. Esta herramienta esta construida con los siguientes componentes:

7.1. Componentes Hardware.

La herramienta fue desarrollada y probada en un computador Lenovo, computadora del 2019. La computadora tiene un procesador de 2.50Ghz Intel Core I5, memoria RAM de 8 GB y sistema operativo Windows 10 pro. Todos los componentes de software descritos a continuación se descargaron y ejecutaron manualmente en este hardware.

7.2. Componentes Software.

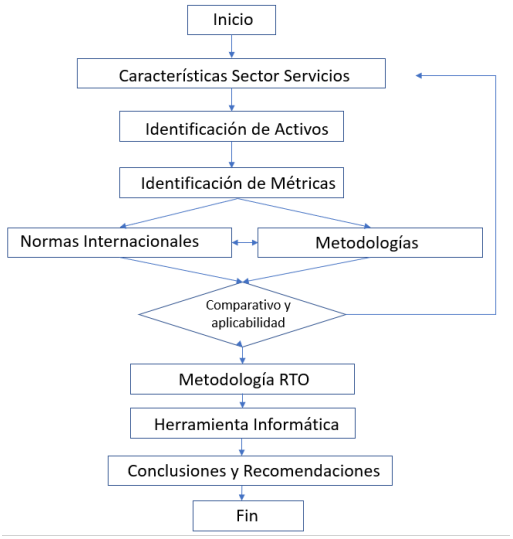
Esta sección describe los componentes de software utilizados para el desarrollo y prueba de la herramienta. Los componentes asociados a la construcción de la herramienta son Linux CentOS, Cpanel, Sublime Text, Google Chrome, Windows 10. Se utilizo HTML y JavaScript para la elaboración de la herramienta. HTML a nivel grafico y JavaScript a nivel funcional.

7.3. Desarrollo Herramienta Informática.

Durante el proceso de análisis del sector servicios con todas sus variables y al lograr identificar las características necesarias para la recuperación de los activos de información a través de las métricas que se usan a nivel mundial en los activos informáticos. Para dicho proceso de análisis se considero el siguiente diagrama de flujo en la (Figura 7-1) donde se describen cada una de las etapas que se debieron realizara para la construcción de las preguntas cable que son las variables que permitirán calcular el tiempo de recuperación de un activo de información.

Figura 7-1:

Etapas clave del proceso de construcción de la herramienta informática.



Autor: Construcción Propia.

Nota: La figura anterior describe en un diagrama de flujo las etapas claves para lograr la construcción y funcionalidad de la herramienta con el fin de determinar el tiempo objetivo de recuperación de los activos de información del sector de servicios, dichas etapas son cruciales para determinar las diferentes características que debe tener cada activo y en función de estas lograr identificar variables que permitan calcular un tiempo de recuperación.

Durante cada fase se presentaron diversas incertidumbres que fueron cubiertas al comparar cada metodología según la aplicabilidad del sector y en función de estas lograr elaborar una metodología que permita calcular el tiempo objetivo de recuperación.

A continuación, se presenta el diseño de la herramienta informática la cual cuenta con una calculadora de RTO. Dicha herramienta puede ser visualizada a través del dominio www.calculadorarto.com.

La herramienta fue construida en base al ciclo PHVA sobre la metodología propuesta, la guía recomendada y se plantean un formulario con una serie de preguntas que permitirán realizar un cálculo y brindar al usuario un valor aproximado en tiempo para la compresión de la situación actual de la organización y así tomar medidas que permitan la remediación.

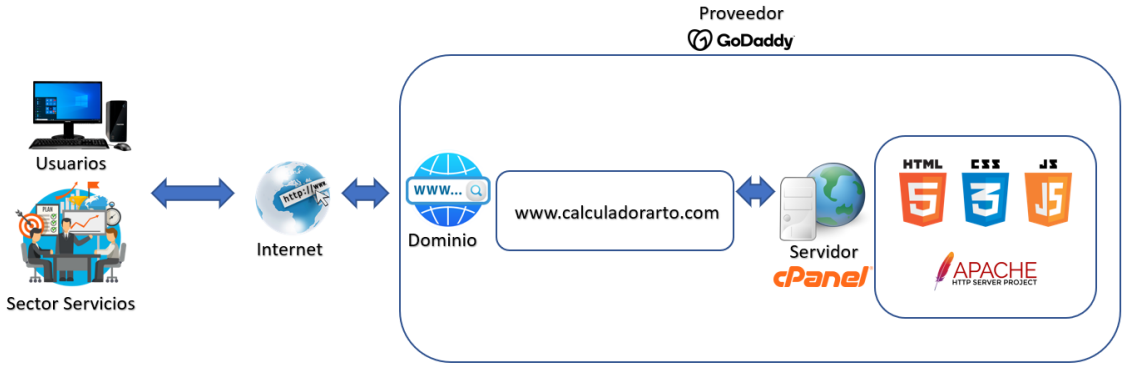
Las preguntas formuladas permiten obtener variables que se traducen a tiempo y así se logra obtener un tiempo de recuperación de un activo informático seleccionado.

Teniendo así planes para el RTO de la organización y buscar que se conserve la disponibilidad de todos aquellos activos críticos de información. Se plantea una pregunta inicial para identificar el activo al cual se hará el análisis, se segmenta en 4 opciones de servidores como activos críticos comunes en el sector servicios.

7.4. Diseño Herramienta.

Figura 7-2:

Arquitectura de la herramienta informática orientada a la web.



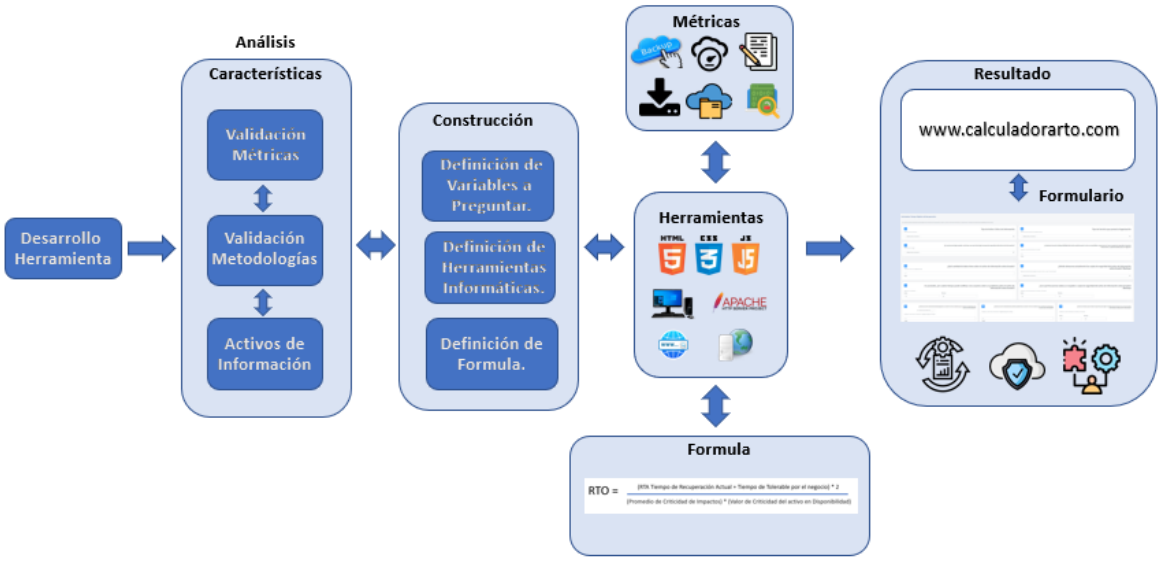
Autor: Construcción Propia.

Nota: La anterior figura ilustra el camino que se debe seguir para llegar a un resultado satisfactorio dentro del proceso de construcción y sus diferentes etapas para lograr la funcionalidad de la herramienta. La anterior arquitectura no contine base de datos ya que su funcionalidad esta diseñada para ser visualizado en tiempo real sin ningún almacenamiento de información. Se recomienda continuar con la investigación para implementar el almacenamiento de la información y de esta manera lograr trazabilidad de los registros que permitirán identificar sucesos en el tiempo y las mejoras continuas de los tiempos identificados.

A continuación, se presenta el flujo del formulario con su descripción aplicado al caso de estudio, empresa del sector servicios del valle de aburra, ya que se diseña la herramienta informática con el fin de brindar un visión, recomendaciones y alertas dentro del conocimiento interno de las organizaciones para visualizar y estar preparados ante alguna situación que se pueda presentar sobre los activos críticos que impidan la funcionalidad y disponibilidad de estos.

Figura 7-3:

Fases del proceso de construcción de la herramienta informática.



Autor: Construcción Propia.

Nota: La figura anterior representa los hitos representativos como eventos diferenciadores en la construcción del proyecto que identifica el RTO.

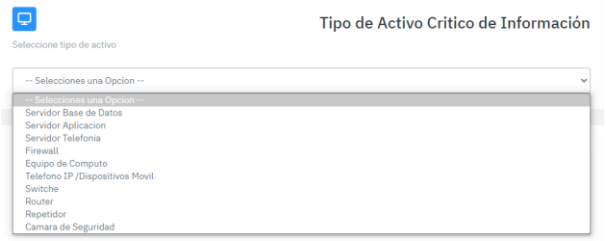
Teniendo en cuenta lo anterior, se procede a definir cada una de las preguntas clave en base a las métricas identificadas para los activos de información para lograr obtener las variables que permitirán realizar el calculo del tiempo objetivo de recuperación.

Se plantea una pregunta inicial para identificar el activo al cual se hará el análisis, se segmenta en 4 opciones de servidores como activos críticos comunes en el sector servicios.

En la (Figura 7-4) muestra un campo de texto seleccionable, el cual es una de las variables que contiene el tipo de activo a analizar. Esto permite tener un contexto sobre las características del activo.

Figura 7-4:

Pregunta tipo de activo critico de información que tiene la organización.



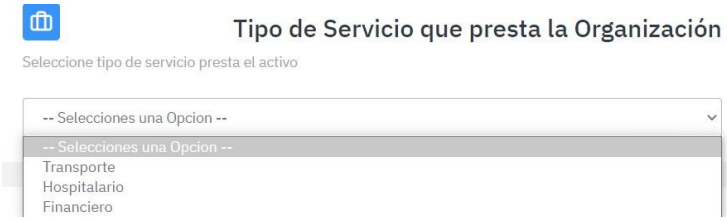
Autor: Construcción propia.

Se plantea una segunda pregunta la cual consiste en el tipo de servicio que presta la organización a la que pertenece el activo crítico. Se segmenta en 3 opciones que pertenecen al sector terciario (Servicios).

En la (Figura 7-5) se muestra un campo seleccionable que permite conocer el sector que se está analizando y al cual el activo este asociado en la prestación de sus servicios. Este campo permite entrar en contexto sobre el tipo de servicio que presta la organización, además de la criticidad e impactos ante una indisponibilidad de los activos.

Figura 7-5:

Pregunta tipo de servicio que presta la organización al comercio.



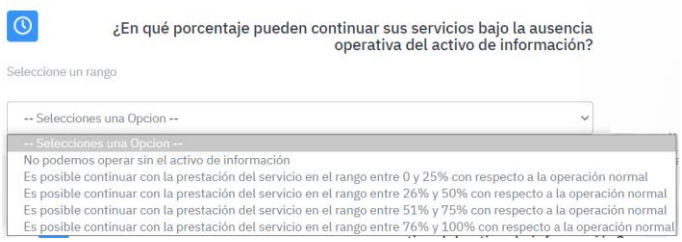
Autor: Construcción propia.

Se plantea pregunta sobre el porcentaje de continuidad sobre los servicios bajo la ausencia con el fin de tener un criterio de cómo puede operar la organización ante la indisponibilidad del servicio que presta el activo, de esta manera lograr tener una variable que permita determinar la prestación de servicio y tener un tiempo aproximado de recuperación teniendo como presente el funcionamiento de la empresa puede minimizar los tiempos RTO.

En la (Figura 7-6) muestra un campo seleccionable sobre la continuidad de servicios ante la indisponibilidad del activo de información, esta pregunta se plantea con el fin de conocer la criticidad durante la ausencia operativa del activo a analizar y conociendo en que porcentaje se ubica la organización ante una situación de indisponibilidad. Así logrando tener esa variable de valor, buscando minimizar el impacto y esto en función de reducir los tiempos de recuperación.

Figura 7-6:

Pregunta la cual planeta un porcentaje si el activo no está disponible y los servicios presentan ausencia operativa.



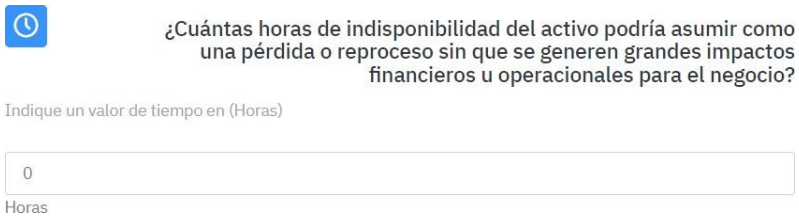
Autor: Construcción propia.

Se plantea pregunta para determinar la cantidad de horas que la organización puede soportar con la indisponibilidad de los servicios proporcionados por los activos, esta pregunta se genera con el fin de conocer los diversos impactos que se pueden generar luego de un tiempo que la organización no puede operar con los sistemas o activos, esto permite que el RTO sea más flexible y se logre unas horas de tolerancia ante la recuperación.

En la (Figura 7-7) muestra un campo numérico el cual se basa en número de (horas) las cuales van en función de conocer el impacto ante la ausencia del activo. Estas horas determinan cuanto tiempo puede tolerar la organización ante la indisponibilidad y realizar los diferentes reprocesos, reconstrucción de información o asumir la perdida de información. Así logrando tener una variable de tiempo que permitirá aportar a la determinación del tiempo actual en que se puede restablecer o recuperar el activo.

Figura 7-7:

Pregunta de la cantidad de tiempo tolerable en que puede estar indisponible el activo.



Autor: Construcción propia.

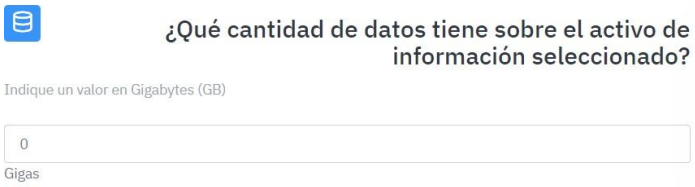
Se plantea pregunta de valor, la cual considera la cantidad de información en gigabytes que contiene el activo de información critico dentro de la organización, con el fin de determinar cuánto puede tardar descargarse y subirse al nuevo activo dicha cantidad de información para restablecer su funcionalidad y la prestación del servicio de forma correcta.

En la (Figura 7-8) muestra un campo numérico se basa en número o cantidad de (Gigas). Este dato es de suma importancia ya que permite conocer cuál es la cantidad de almacenamiento que en la actualidad ocupan los datos sobre el activo de información.

Esta información es de valor ya que permite tener una claridad sobre el volumen de información que se debe restablecer ante un desastre o una indisponibilidad en función de la recuperación del activo, este dato también es de mucha importancia porque nos permite tener en cuenta la criticidad de este activo. Con este valor numérico permite tener una base para calcular el tiempo aproximado de restauración y restauración de esta información.

Figura 7-8:

Pregunta cantidad de información en Gigabytes que contiene el activo de información.



Autor: Construcción propia.

Se plantea pregunta de gran importancia para determina la ubicación donde se encuentran almacenadas las copias de seguridad o backups, dicha pregunta permite tener una visión sobre los

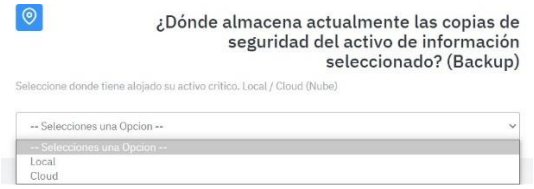
tiempos para tomar la información y tenerla disponible para una restauración en un nuevo activo, considerando la ubicación de la información se logra determinar unos tiempos que harán del RTO un dato para tener en cuenta, ya que implica considerar las variables para restaurar.

En la (Figura 7-9) muestra un campo seleccionable el cual permite conocer donde se encuentran almacenadas las copias de seguridad del activo a analizar. Esta información es de suma importancia ya que nos permite tener en cuenta la integridad, la seguridad, la ubicación, la disponibilidad, entre múltiples variables.

Esto con el fin que al momento de realizar una restauración de la copia de seguridad se debe tener en cuenta los tiempos en que se logra obtener por completo este (Backup) y así proceder a la restauración de este. Una variable más para lograr el cálculo del tiempo de recuperación.

Figura 7-9:

Pregunta sobre donde se almacenan los diversos Backups del activo de información.



Autor: Construcción propia.

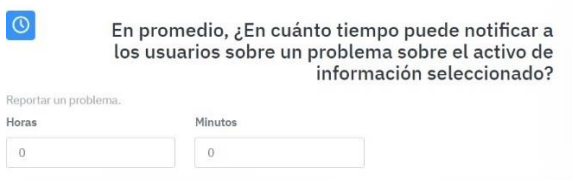
Se plantea pregunta sobre el tiempo en que la organización notifica a sus clientes en general la indisponibilidad de los servicios, lo que se implica un tiempo de socialización de la situación.

En la (Figura 7-10) muestra dos campos numéricos, los cuales están separados para una variable de horas y otra de minutos. Este valor es otra variable de importancia para tener en cuenta un tiempo de recuperación.

Esta pregunta se fundamente en el proceso de notificar a los usuarios que utilizan servicios proporcionados por el activo de información la indisponibilidad de este. Esta es una variable importante, dado que se incurre en un proceso que se basa en tiempo para mitigar el impacto a la organización por la ausencia del servicio.

Figura 7-10:

Pregunta sobre el promedio de tiempo en que se le notifica al cliente la ausencia o indisponibilidad del servicio que presta un activo de información.



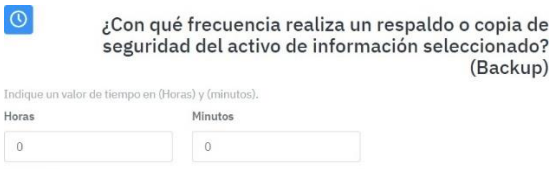
Autor: Construcción propia.

Se plantea pregunta sobre el tiempo en el que se genera cada copia de seguridad y con qué frecuencia, esto es de gran importancia ya que permite tener claro cada cuanto tiempo se realiza el guardado como respaldo de la información contenida en el activo, esto identificando el tiempo entre copia y copia.

En la (Figura 7-11) muestra dos campos numéricos que representan (horas) y (minutos), este valor es de mucha importancia para una recuperación ya que se debe tener en cuenta la frecuencia en que se realizan las copias de seguridad. Dando un parámetro de valor para identificar cada cuanto tiempo se guarda la copia de información y así tener un rango de tiempo para un posible punto de partida desde el momento en que se generó dicha copia.

Figura 7-11:

Pregunta sobre la frecuencia en que se realizan las copias de seguridad de la información contenida sobre el activo.



Autor: Construcción propia.

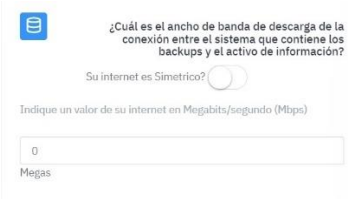
Se plantea pregunta de valor la cual se considera de gran importancia para la adquisición u obtención de las copias de seguridad para así disponer de esta información para proceder con la restauración del backup en un nuevo activo de información. Al conocer este dato de velocidad en la descarga se considera un cálculo para determinar el tiempo para descargar la copia de seguridad.

Realizando una conversión de Gigabytes a bit y a su vez transformando bits a segundos. Porque 1byte = 8bit, 8/8 = 1 megabytes por segundo. Así pues, en un minuto (60 segundos) el usuario puede descargar 1*60 = 60 megabytes.

En la (Figura 7-12) muestra un campo numérico el cual se basa en (megas), este valor permite conocer la velocidad representada en Megabits por segundo (Mbps) que se tiene en la ubicación actual donde podría realizarse un proceso de recuperación del activo de información analizado, este valor permite conocer en cuanto tiempo puedo obtener información, ubicada en un lugar externo.

Figura 7-12:

Pregunta sobre el ancho de banda que tiene el internet donde se realizaría el proceso de restauración.



Autor: Construcción propia.

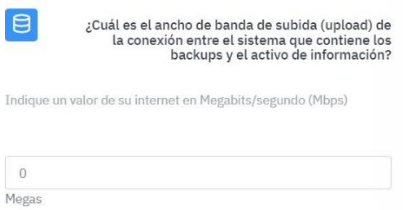
Se plantea propuesta de valor para en caso de que el activo este localizado en la nube o sea un servicio externo se pueda subir o importar la copia de seguridad, esta velocidad de subida es de gran importancia ya que se busca determinar cuánto tarda esta cantidad de información en estar disponible para la restauración de la información.

Calculando y haciendo la conversión de información en Gigabytes a bits y luego conversión de bits a segundos. Así logrando determinar un tiempo aproximado para dicho proceso.

En la (Figura 7-13) muestra un campo numérico representado en (megas), este valor permite conocer la velocidad representada en Megabits por segundo (Mbps) que se tiene en la ubicación actual donde podría realizarse un proceso de recuperación del activo de información analizado, este valor permite conocer en cuanto tiempo se puede transferir información al activo a restaurar.

Figura 7-13:

Pregunta sobre el ancho de banda que tiene el internet donde se realizaría el proceso de restauración.



Autor: Construcción propia.

Se plantea pregunta de relevancia ya que, al momento de conocer toda la información contenida, las dependencias, configuraciones y múltiples características del activo, poder tener un criterio y un dato aproximado de cuánto puede tardar la recuperación y la habilitación en disponibilidad del activo, este tiempo es de gran importancia tenerlo en cuenta ya que nos permite tener más claro cuál sería nuestro RTO y así tener claros los tiempos de ejecución de las diversas actividades que se deben realizar para habilitar el servicio que ofrece el activo.

En la (Figura 7-14) muestra dos campos numéricos (Horas) y (minutos). Este tiempo es de importancia ya que se debe tener un conocimiento de cuánto puede tardar restablecer el servicio luego de tener la copia de seguridad ubicado y disponible para ser utilizado en función de restablecer la información. Esta variable permite tener un tiempo adicional para tener en cuenta al momento de calcular el tiempo de recuperación del activo.

Figura 7-14:

Pregunta basada en el conocedor del activo de información, luego de tener los Backups o copias de seguridad cuanto puede tardar en restablecerse o restaurar dicha información y así dando disponibilidad al servicio.

Autor: Construcción propia.

Se plantean unos resultados los cuales se discriminan para lograr tener una mayor claridad sobre los tiempos de recuperación y los procesos que se deben tener en cuenta para lograr una restauración objetiva y permitir tener una visión cada día más clara sobre el RTO de cada activo critico dentro de la organización.

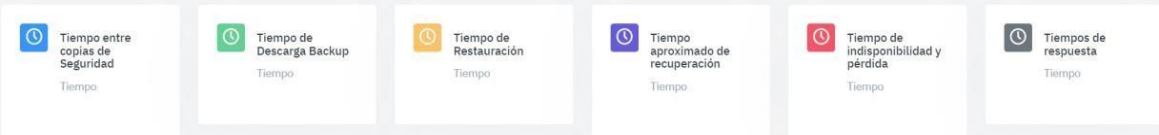
En la (Figura 7-15) muestra los diversos resultados calculados con respecto a la información obtenida en las preguntas anteriores. Y teniendo en cuenta la formula descrita por la metodología propuesta. Estos valores se representan en Tiempo (Horas, minutos y segundos). Estos resultados nos permiten conocer el estado actual de recuperación y los tiempos que me implican en dicho proceso.

Luego de realizar el cálculo la aplicación categoriza y arroja una alerta teniendo en cuenta el rango de criticidad, dicho resultado permitirá conocer el estado actual de recuperación del activo de información, así tomando las diferentes medidas, controles, planes de acción y estrategias para la optimización y minimizar los tiempos de recuperación de este.

Dando pie a la mejora y la búsqueda continuas de reducir estos tiempos y optimizar los procesos internos de la organización en pro de mantener la disponibilidad de los servicios y contar con estrategias para la atención de los activos de información.

Figura 7-15:

Resultados del cuestionario en tiempo, permitiendo tener un dato aproximado de cuando puede ser el RTO al momento de una indisponibilidad de los activos críticos.



Autor: Construcción propia.

Luego de que la herramienta realiza los cálculos, esta presenta recomendaciones y planes de acción para la mejora continua, en busca de minimizar los tiempos de recuperación, permitiendo que la disponibilidad del activo sea la prioridad dentro de la organización y en función de minimizar los impactos ante una indisponibilidad de uno de los activos de información. Se recomienda acceder al dominio www.calculadorarto.com y realizar sus respectivos análisis, dicha herramienta publicada se encuentra en constante actualización, para mejorar la experiencia de usuario y optimización de los cálculos para brindarle información de valor a las organizaciones.

8. Conclusiones y recomendaciones

8.1. Conclusiones

En este trabajo se presentó una propuesta de metodología para la determinación de los tiempos objetivos de recuperación RTO de los activos de información críticos en una estrategia de continuidad de negocio del sector servicios de Colombia.

La metodología propuesta se centra en la disponibilidad de los activos críticos del sector servicios, pero involucra aspectos del contexto de la organización, la implementación de controles, la verificación y la mejora continua para la optimización de los tiempos objetivos de recuperación. Es de gran valor aprender de los errores y tomar medidas de corrección que permitan hacer más eficientes las estrategias que se implementen día a día para la reducción de los tiempos de recuperación. Al pasar por cada una de las normas internacionales y metodologías más usadas en la gestión de riesgos sobre los activos de información, se logró construir una metodología con componentes de nivel estratégico, operacional y táctico permitiendo minimizar impactos y optimización de los activos en función de la disponibilidad.

En el objetivo “Evaluar y clasificar las métricas adecuadas en la identificación de los puntos objetivos para el cálculo de tiempos de recuperación sobre cada activo, identificando el patrón de criticidad.” Se logra identificar que los activos de información son componentes de gran importancia dentro de la organización y se miden de acuerdo con múltiples características, además son componentes críticos y que ante una indisponibilidad se pueden generar impactos importantes a la organización.

Se concluye que los activos prestan múltiples variables y al momento de tenerlas en cuenta pueden no dar un tiempo exacto en un panorama de recuperación dado a los factores externos y de

conocimiento dentro de la organización para la restauración de la disponibilidad de estos ante una situación crítica. Siendo esta una limitante para la investigación, ya que se deben determinar variables solidas que permitan calcular tiempos más exactos, en función del sector, tipo de activo, dependencias, cantidad de almacenamiento, etc. Se recomienda continuar con la caracterización de los activos y generar estrategias optimas a nivel tecnológico para reducir los tiempos de recuperación.

En el objetivo "Validar diversas metodologías para la aplicación del cálculo de los tiempos objetivos ante desastres sobre los activos de información y a través de un caso de estudio, prueba de concepto o en empresa del Valle de Aburrá." Se logran identificar múltiples características que se orientan a la continuidad del negocio y la mejora continua.

En el objetivo "Elaborar una metodología a partir de los criterios, elementos y parámetros requeridos por el sector de servicios", se identificaron metodologías existentes de gran valor que permitieron tener características claves en la búsqueda de la disponibilidad y la construcción de una metodología optimiza en la recuperación de los activos de información críticos, evitando impactos mayores a la organización.

En el objetivo "Construir una herramienta informática, de acuerdo con la metodología diseñada, que proponga recomendaciones, alertas y planes de acción sobre el activo crítico, permitiendo dar continuidad al negocio y adoptando buenas prácticas en Seguridad Informática para la disponibilidad del servicio", se logró identificar múltiples características y técnicas para el cálculo de los tiempos de recuperación de los activos de información, así logrando obtener resultados de valor en el análisis de estos.

- Al realizar el análisis de las diferentes características del RTO y todo aquello que interviene en tiempo al momento de restablecer y dar disponibilidad a los servicios de una organización, se logran identificar múltiples variables que son importantes tenerlas en cuenta al momento de ejecutar una recuperación. Como lo es la velocidad de la red, cantidad de información a restaurar,

con esta información se logró determinar un tiempo aproximado de descarga y subida para la restauración del servicio.

- El conocimiento de la metodología permite tener claridad sobre los parámetros del sector servicios que presta la organización y cómo funciona u operada esta, así buscando la mejora continua sobre los activos de información y teniendo claridad sobre su funcionamiento, dependencias, características y configuraciones que se deben tener en cuenta en un RTO. Haciendo que la metodología cobre un gran valor sobre los procesos que se deben tener en cuenta a la hora de determinar los tiempos de recuperación.
- Al conocer las diferentes características del sector servicios, se logra identificar la necesidad y la dependencia de mantener la disponibilidad de los activos, motivando a generar alternativas para conocer e identificar las diversas cualidades que tiene un activo. Permitiendo así identificar o aproximar una recuperación de dicho activo.
- Al tener un flujo metodológico como el propuesto se logra tener un flujo acorde al crecimiento organizacional y permitir la mejora continua sobre los sistemas informáticos, preparando a la organización y buscando realizar los procesos de manera más eficiente con el fin de permanecer con disponibilidad los servicios que presta esta.
- A través de esta investigación y diferentes análisis del RTO, se proporciona una posible solución para la determinación lo de los tiempos objetivos al momento de un desastre o indisponibilidad, a través de la herramienta informática disponible en el dominio www.calculadorarto.com que permite conocer los diferentes tiempos, alertas y características de impacto, planteando recomendaciones y generando una consciencia a la organización al momento de conocer los diferentes escenarios a los que se puede estar expuesto.

8.2. Recomendaciones

Se presentan una herramienta informática la cual se permitirá modificar, anexar y plantear nuevas preguntas que ayuden al sector servicios a tomar correctivos y tener claridad sobre los diferentes activos críticos de información.

- Realizar periódicamente las características de los activos críticos y evaluar el RTO por medio de la calculadora, para así realizar mejorar continuas y establecer lineamientos de seguridad para evitar que los tiempos de recuperación sean altos, realizando mejoras continuas y pruebas sobre cada activo.
- Dadas las múltiples variables que tienen los activos de información se identificó que son demasiado extensas dichas características y/o variables que se deben tener en cuenta para determinar un tiempo de recuperación, dicho esto se presentó una limitación que impidió lograr encontrar un valor exacto, se recomienda continuar con esta investigación con el fin de consolidar variables solidas que permitan obtener valores más acertados.
- Plantear y definir diferentes escenarios de recuperación con el fin de establecer parámetros y características de los activos críticos, así tener una claridad de cómo proceder con un RTO de manera eficiente.
- Realizar continuas mejoras y análisis de las fórmulas de cálculo de las fórmulas aplicadas al cálculo de los tiempos, con el fin de tener múltiples variables que permitan que el cálculo se ajuste cada vez más a un tiempo que permita conocer claramente cuál es el tiempo de recuperación de la disponibilidad del activo de información.
- Implementar controles a todos los activos de información que tiene la organización. Brindando optimización a los procesos que se realizan en cada una de las etapas de la metodología así aprendiendo y tomando esos aprendizajes para la mejora continua.
- Mejorar el software propuesto a todo nivel, en características funcionales Back-End, en experiencia de usuario y facilidad de uso (Front-End) y en seguridad del sitio web (servidor). Con el fin de optimizar y hacer más eficiente el análisis, además generalizar el uso en todo tipo de dispositivos digitales.
- Proyectar a expandir la metodología propuesta y el crecimiento del software para abarcar todo tipo de activos de información y sectores productivos. Así logrando que se genere conciencia

y permitir a las diferentes organizaciones la restauración y disponibilidad de los servicios informáticos prestados por los activos de información.

Las empresas para tener esta metodología en su ambiente corporativo deben considerar diversas estrategias como lo es la documentación de los procesos, para la permanencia de los datos, procesos realizados, estrategias utilizadas con el fin de tener información base para el continuo aprendizaje optimización y gestión de los activos de información dentro de la organización.

Una recomendación adicional es que se continue con la investigación y generación de estrategias para la mejora de los tiempos, gestión de los activos, procesos y métodos para la optimización de los tiempos de recuperación y brindar al sector servicios diversos planes de acción para ser aplicados dentro de la organización en búsqueda de conservar y mantener la disponibilidad de los servicios.

A. Anexo: Métricas para Activos de información del sector servicios.

Se anexa análisis de las diferentes métricas para los activos de información de las organizaciones del sector servicios.

9. Bibliografía

[1] MINTIC, 2015. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf. [Último acceso: 2021].

[2] E. J. E. Carmona, «OCTAVE, metodolog´ıa para el an´alisis de riesgos de TI,,» 2013.

[3] P. administracion electronica, «PAe - MAGERIT v.3 : Metodolog´ıa de An´alisis y Gesti´on,» 2019.

[4] C. A. G. Durango, «Metodolog´ıa integradora para simplificar la implementaci´on de los,» Medellin, 2019.

[5] S. Galeano, «Marketing 4 Ecommerce,» 27 Enero 2022. [En línea]. Available: https://marketing4ecommerce.net/usuarios-de-internet-mundo/. [Último acceso: 14 Noviembre 2021].

[6] M. Pasquali, «Statista,» 10 Diciembre 2021. [En línea]. Available: https://es.statista.com/grafico/26372/paises-latinoamericanos-con-el-mayor-pib-a-traves-del-tiempo/. [Último acceso: 8 Enero 2021].

[7] ISOTools, «ISOTools,» 2021. [En línea]. Available: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/).. [Último acceso: 7 Noviembre 2021].

[8] A. L. F. Militares, «Agencia Logistica Fuerzas Militares,» 6 Marzo 2020. [En línea]. Available: https://community.secop.gov.co/Public/Archive/RetrieveFile/Index?DocumentId=44967771. [Último acceso: 20 Octumbre 2021].

[9] I. Thompson, «Promonegocios.net,» Octubre 2008. [En línea]. Available: https://www.promonegocios.net/mercadotecnia/definicion-informacion.html. [Último acceso: Septiembre 2021].

[10] A. C. Flores, «lifeder,» 15 Enero 2018. [En línea]. Available: https://www.lifeder.com/sector-terciario-colombia/. [Último acceso: Agosto 2021].

[11] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n. [Último acceso: Octubre 2021].

[12] «Cloud Seguro,» [En línea]. Available: https://www.cloudseguro.co/analisdevulnerabilidades/. [Último acceso: Agosto 2021].

[13] N. Frett, «Auditool,» 9 Junio 2015. [En línea]. Available: https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque. [Último acceso: Septiembre 2021].

[14] U. I. d. Valencia, 21 Marzo 2018. [En línea]. Available: https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme. [Último acceso: Agosto 2021].

[15] «apser,» 04 Junio 2019. [En línea]. Available: https://apser.es/rto-y-rpo-importancia-disaster-recovery/. [Último acceso: Octubre 2021].

[16] «Aurit,» 2021. [En línea]. Available: https://aurit.es/drp-sap/#:~:text=Recovery%20Time%20Objective%20(RTO)%20es,de%20inactividad%20de%20la%20red.. [Último acceso: Octubre 2021].

[17] «welivesecurity,» 04 Octubre 2014. [En línea]. Available: https://www.welivesecurity.com/la-es/2014/10/14/plan-de-recuperacion-ante-desastres/. [Último acceso: Agosto 2021].

[18] pendiente. [En línea].

[19] Y. P. Baginda, A. Affandi y I. Pratomo, «IEEE xplore,» 2018. [En línea]. Available: https://ieeexplore.ieee.org/document/8534758. [Último acceso: 2020].

[20] M. M. Al–shammari y A. A. Alwan, «IEEE xplore,» 2018. [En línea]. Available: https://ieeexplore.ieee.org/document/8442005/. [Último acceso: 2020].

[21] O. H. Alhazmi y Y. K. Malaiya, «IEEE xplore,» 2013. [En línea]. Available: https://ieeexplore.ieee.org/document/6517700. [Último acceso: 2020].

[22] J. Mendonça, W. Medeiros, E. Andrade, R. Maciel, P. Maciel y R. Lima, «IEEE xplore,» 2019. [En línea]. Available: https://ieeexplore.ieee.org/document/8914069. [Último acceso: 2020].

[23] S. Suguna y A. Suhasini, «IEEE xplore,» 2015. [En línea]. Available: https://ieeexplore.ieee.org/document/7033804. [Último acceso: 2020].

[24] R. Mikkilineni y G. Kankanhalli, «IEEE xplore,» 2010. [En línea]. Available: https://ieeexplore.ieee.org/document/5541978. [Último acceso: 2020].

[25] M. Wiboonrat y K. Kosavisutte, «IEEE Xplore,» 2008. [En línea]. Available: https://ieeexplore.ieee.org/document/4654446. [Último acceso: 2021].

[26] M. Wiboonrat y K. Kosavisutte, «IEEE Xplore,» 2009. [En línea]. Available: https://www.tandfonline.com/doi/abs/10.1080/17509653.2009.10671079. [Último acceso: 2021].

[27] QBR, 2020. [En línea]. Available: https://www.quick-backup-recovery.com/rtc/. [Último acceso: 2021].

[28] «Alpha & Omega Computer & Network Services, Inc,» 2021. [En línea]. Available: https://www.aobiz.com/rto-calculator/. [Último acceso: 2021].

[29] L. L. B. Elejalde, «La Republica,» Enero 2020. [En línea]. Available: https://www.larepublica.co/empresas/creacion-de-empresas-de-servicios-la-que-mas-crecio-durante-2019-2954666. [Último acceso: 2021].

[30] «Semana,» Abril 2018. [En línea]. Available: https://www.semana.com/economia/articulo/encuesta-mensual-de-servicios-en-colombia-en-enero-de-2018/256948/. [Último acceso: 2021].

[31] C. Aguado, «IMF,» [En línea]. Available: https://blogs.imf-formacion.com/blog/mba/mapas-de-procesos-empresas-servicios/. [Último acceso: 2021].

[32] Gerencie.com, «Gerencie.com,» Agosto 2019. [En línea]. Available: https://www.gerencie.com/vida-util-de-los-activos-fijos.html. [Último acceso: 2021].

[33] «Wikipedia,» Marzo 2020. [En línea]. Available: https://es.wikipedia.org/wiki/Servidor_de_aplicaciones. [Último acceso: 2021].

[34] E. Borges, «Blog Infra networking,» Marzo 2019. [En línea]. Available: https://blog.infranetworking.com/servidor-base-de-datos/. [Último acceso: 2021].

[35] Á. D. León, «Blog Infra networking,» Marzo 2019. [En línea]. Available: https://blog.infranetworking.com/servidor-de-correo/. [Último acceso: 2021].

[36] ignacio_crespo, «Platzi,» 2021. [En línea]. Available: https://platzi.com/tutoriales/1098-ingenieria/7779-que-es-un-firewall-simplificado/?utm_source=google&utm_medium=cpc&utm_campaign=12915366154&utm_adgroup=&utm_content=&gclid=Cj0KCQiAmeKQBhDvARIsAHJ7mF5jwGGGUdIfczVSuVIYgz2_oDU_wLTsS0Al8I-tzcg2RYFeV_VCMgUaA. [Último acceso: 2021].

[37] I. Bravo, «Reparando,» 2017. [En línea]. Available: https://reparando.com.mx/que-es-un-equipo-de-computo-y-sus-caracteristicas/#:~:text=Una%20explicaci%C3%B3n%20m%C3%A1s%20certera%20de,todas%20las%20instrucciones%20del%20software. [Último acceso: 2021].

[38] «3CX,» [En línea]. Available: https://www.3cx.es/voip-sip/telefonia-ip/. [Último acceso: 2021].

[39] T. &. Citófonos, «Teléfonos & Citófonos,» [En línea]. Available: https://telycit.net/content/17-plantas-telefonicas. [Último acceso: 2021].

[40] «Trabajo Social,» [En línea]. Available: https://www.trabajosocial.unlp.edu.ar/uploads/docs/switch__routers_y_acces_point__conceptos_generales.pdf. [Último acceso: 2021].

[41] «Google,» [En línea]. Available: https://support.google.com/googlenest/answer/6274087?hl=es#:~:text=Un%20router%20es%20un%20dispositivo,de%20%C3%A1rea%20local%20(LAN).. [Último acceso: 2021].

[42] Y. FERNÁNDEZ, «Xataka,» Marzo 2021. [En línea]. Available: https://www.xataka.com/basics/repetidor-wifi-que-como-funciona. [Último acceso: Octubre 2021].

[43] M. G. ACACIO, «Acacio,» Febrero 2019. [En línea]. Available: https://www.acacioseguridad.com/camaras-de-vigilancia/#:~:text=Las%20c%C3%A1maras%20de%20vigilancia%20son,una%20soluci%C3%B3n%20para%20mantenerse%20protegido. [Último acceso: 2021].

[44] S. d. Sociedades, «Super Sociedades,» 2018. [En línea]. Available: https://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Infraestructura%20Tecnologica/Formatos/GINT-F-005%20ANALISIS_IMPACTO.xls. [Último acceso: 2021].

[45] Y. A. R. Romero, «Universidad de La Salle,» 2014. [En línea]. Available: https://ciencia.lasalle.edu.co/maest_ingenieria/10/. [Último acceso: 2021].

[46] R. F. V, «cintel,» 2015. [En línea]. Available: https://cintel.co/wp-content/uploads/2013/05/Metodolog%C3%ADa-para-la-Gesti%C3%B3n-de-la-Continuidad-del-Negocio.pdf. [Último acceso: 2021].

[47] R. Ferrer. [En línea]. Available: https://docplayer.es/2300181-Metodologia-para-el-diseno-de-un-plan-de-recuperacion-ante-desastres-o-drp.html. [Último acceso: 2021].

[48] P. E. C. Martinez, «Metodolog´ıa de seguridad de la informaci´on para la gesti´on del,» 2016.

[49] UNGRD, «TERMINOLOG´IA SOBRE GESTION DEL RIESGO DE DESASTRES Y ´,» 2017.

[50] I. O. f. Standardization, «“ISO 31000 Gesti´on de riesgos.».

[51] INCIBE, «INCIBE,» 2019.

[52] G. P. N. Alberto, «Guıa para la administracion del riesgo y el diseno,» 2018.

[53] Direccion del Departamento Administrativo de la Funcion Publica, «DAFP - Decreto 1537 de 2001 - Gestor Normativo Funci´on P´ublica,,» 2001.

[54] A. G. a. A. F. G. Stoneburner, «Risk management guide for information technology systems,» 2002.

[55] Organizacion Internacional para la Estandarizacion, «ISO / IEC 27005: 2018 - Tecnologıa de la informacion - Tecnicas de seguridad - Gestion de riesgos de seguridad de la,» 2018.

[56] PriteshGupta.com, «ISO27000.es - El portal de ISO 27001 en espanol. Gestion de Seguridad de la Informacion,» 2018.

[57] PriteshGupta.com, «El portal de ISO 27002 en Espanol,» 2019.

[58] J. Martins, «Asana,» 2022. [En línea]. Available: https://asana.com/es/resources/pdca-cycle. [Último acceso: 2022].

[59] [En línea].

[60] SafetYA, 2019. [En línea]. Available: https://safetya.co/phva-procedimiento-logico-y-por-etapas/. [Último acceso: 2021].

[61] R. F. V, 2015. [En línea]. Available: https://cintel.co/wp-content/uploads/2013/05/Metodolog%C3%ADa-para-la-Gesti%C3%B3n-de-la-Continuidad-del-Negocio.pdf. [Último acceso: 2021].

[62] K. Lavinder, 2016. [En línea]. Available: https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-28_Issue-4/2016_4_05_lavinder_s.pdf. [Último acceso: 2021].

[63] G. Solutions, 2020. [En línea]. Available: https://www.globalsuitesolutions.com/what-is-bia-what-is-its-importance-in-business-continuity/. [Último acceso: 2021].

[64] Infopulse, 2022. [En línea]. Available: https://www.infopulse.com/blog/best-practices-business-continuity. [Último acceso: 2022].

[65] «EcuRed,» 2022. [En línea]. Available: https://www.ecured.cu/Herramientas_inform%C3%A1ticas.