



FACULTAD DE POSGRADOS

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE DISASTER RECOVERY AS A  
SERVICE (DRaaS) BASADO EN EL MODELO DE CLOUD COMPUTING  
EN LA COOPERATIVA "ALIANZA DEL VALLE".

Trabajo de Titulación presentado en conformidad con los requisitos establecidos  
para optar por el título de Magister en Gerencia de Sistemas y Tecnologías  
de la Información

Profesora Guía  
Mgt. Katalina del Rocío Koronel Hoyos

Autora  
Andrea Erika Cadena Marten

Año  
2017

## **DECLARACIÓN DEL PROFESOR GUÍA**

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

---

Mgt. Katalina del Rocío Coronel Hoyos

Magister en Gerencia de Sistemas y Tecnologías de Información.

C.I. 1711000016

## **DECLARACIÓN DEL PROFESOR CORRECTOR**

Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan el Trabajo de Titulación.

---

Luis Patricio Moreno Buitrón

Magister en Gerencia de Sistemas y Tecnologías de Información.

CI. 1705511051

## **DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE**

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

---

Andrea Erika Cadena Marten

CI. 0401438213

## **AGRADECIMIENTOS**

Agradezco a mi esposo por todo el apoyo y amor que me brinda cada día.

A padres y amigos, por acompañarme a cumplir mis metas y mis objetivos que han sido reflejados en la presente tesis.

A mi hermano, que es el motivo por el que vivo mi vida plena y feliz.

A mi hijo, porque me acompañó desde mi vientre durante todo este camino, y ahora es mi fortaleza.

A mis profesores, pero por sobre todo a mi tutora ya que fue un constante apoyo en el desarrollo de la presente.

## **DEDICATORIA**

Con la culminación de esta etapa de mi vida, dedico este trabajo a mi hijo, por ser el pedazo de cielo que ilumina mi vida, impulsándome a ser mejor como persona, mamá y profesional.

A mi esposo, por ser mi mejor amigo y ayudarme a alcanzar este objetivo.

A mis padres, por ser mis pilares, siempre brindándome su apoyo incondicional.

A mi angelito del cielo, mi hermano, por cuidarme SIEMPRE.

## RESUMEN

La información institucional de las empresas, se ha convertido en un activo fijo realmente invaluable y dado que es el activo más importante, no es de extrañar que se la debe proteger en caso de que se produzca un imprevisto que pueda provocar una interrupción en la continuidad del negocio, como la interrupción de su servicio, ya sea que se trate de errores humanos o de otros factores externos y se vea afectada la imagen institucional y por su puesto la rentabilidad de la misma.

El presente estudio de factibilidad se ha desarrollado debido a la importancia de contar con un manejo estratégico de la información, como la Recuperación ante Desastres como Servicio (DRaaS), la cual es una solución de réplica y recuperación ante desastres basada en la tecnología de Computación en la Nube, que permite albergar una copia de los sistemas operativos y las aplicaciones en un sitio alternativo a modo de plataforma de contingencia en caso de desastre o indisponibilidad de la plataforma principal.

En el primer capítulo se detalla los objetivos, alcance, justificación, y el planteamiento del problema que se desarrolla en la presente tesis.

El segundo capítulo resume el fundamento teórico del uso de DRaaS como mecanismo de recuperación antes desastres tecnológicos en la Cooperativa de Ahorro y Crédito "Alianza del Valle".

En el tercer capítulo se efectúa un diagnóstico sobre la situación actual de la cooperativa frente a la implementación de Recuperación ante Desastres como Servicio(DRaaS).

En el cuarto capítulo se desarrolla el estudio de factibilidad para la implementación de la recuperación ante desastres como servicio, frente a la implementación del fortalecimiento del sitio alternativo actual.

El quinto capítulo detalla un resumen ejecutivo del estudio de factibilidad donde se presenta los resultados del análisis, más las recomendaciones y la propuesta para la implementación de la recuperación ante desastres como servicio.

Y finalmente en el sexto capítulo, se presenta un compendio de las conclusiones obtenidas a partir de desarrollo del presente trabajo, y se expone las recomendaciones del caso.

## **ABSTRACT**

The institutional information of companies has become an really invaluable fixed asset and since it is the most important asset, it is not surprising that it must be protected in the event of an unforeseen event that may lead to an interruption in continuity of the business, such as the interruption of its service, whether it is due to human errors or to other external factors and the institutional image is affected and, of course, the profitability of it.

The present study has been developed due to the importance of having a strategic management of information, such as Disaster Recovery as a Service (DRaaS), which is a replication and disaster recovery solution based on computer technology in the Cloud, that allows to host a copy of the operating systems and the applications in an alternate site as a platform of contingency in case of disaster or unavailability of the main platform.

The first chapter details the objectives, scope, justification, and approach of the problem that is developed in the present thesis.

The second chapter summarizes the theoretical basis of the use of DRaaS as a mechanism of recovery before technological disasters in the Cooperative of Savings and Credit "Alianza del Valle"

In the third chapter, a diagnosis is made on the current situation of the cooperative in relation to the implementation of Disaster Recovery as a Service (DRaaS).

In the fourth chapter the feasibility study for the implementation of the disaster recovery as a service is developed, as opposed to the implementation of the strengthening of the current alternate site.

The fifth chapter contains an executive summary of the feasibility study where the results of the analysis are presented, plus the recommendations and the proposal for the implementation of disaster recovery as a service.

Finally, in the sixth chapter, a compendium of the conclusions obtained from the development of the present work, and the recommendations of the case are presented.

# ÍNDICE

1. CAPÍTULO I. ANTECEDENTES.....	1
1.1 Introducción .....	1
1.2 Objetivos.....	2
1.2.1 Objetivo General.....	2
1.2.2 Objetivos Específicos.....	2
1.3 Planteamiento del Problema.....	3
1.4 Alcance .....	3
1.5 Justificación .....	4
1.6 Empresa .....	5
1.6.1 Servicios de la institución.....	5
1.6.2 Orgánico estructural del departamento informática y tecnología.....	6
1.6.3 Funciones Críticas del Departamento de Sistemas.....	7
2. CAPÍTULO II. MARCO TEÓRICO APLICADO.....	8
2.1 Introducción .....	8
2.2 Virtualización .....	9
2.2.1 Tipos de Virtualización .....	10
2.2.1.1 Virtualización de servidores.....	10
2.2.1.2 Virtualización de Almacenamiento.....	12
2.2.1.3 Virtualización de Servicios.....	12
2.2.2 Ventajas de la Virtualización. ....	13
2.2.3 Desventajas de la Virtualización.....	13
2.3 Computación en la Nube.....	14

2.3.1 Características.....	14
2.3.2 Tipos de Nube.....	15
2.3.2.1 Modelo de Despliegue de Computación en la Nube.....	16
2.3.2.2 Modelos de Servicio de Computación en la Nube.....	22
2.4 Seguridad de Datos en la Nube.....	26
2.5 Plan de Recuperación ante desastres(DRP).....	28
2.5.1 Tipos de Contingencia.....	29
2.5.2 DRP tradicionales Vs DRP en la nube.....	30
2.6 Disaster Recovery As A Service (DRaaS).....	30
2.6.1 Tipos de DRaaS.....	32
<b>3. CAPÍTULO III. SITUACIÓN ACTUAL DE “ALIANZA DEL VALLE” FRENTE A LA IMPLEMENTACIÓN DE DISASTER RECOVERY AS A SERVICE (DRAAS).....</b>	<b>33</b>
3.1 Introducción.....	33
3.2 Conocimiento de los Procesos Críticos.....	34
3.3 Revisión de los requerimientos de la empresa para su funcionamiento.....	39
3.3.1 Disponibilidad de recursos y servicios.....	39
3.3.2 Infraestructura.....	40
3.3.2.1 Inventario de Servidores.....	41
3.3.3 Escalabilidad.....	43
3.3.4 Sitio Alterno.....	43
3.4 Situación actual de su DRP.....	44

3.4.1	Objetivo del Plan de Contingencia de Alianza del Valle.....	44
3.4.2	Análisis de los riesgos y problemas de continuidad.....	45
3.4.3	Identificación de Riesgos.....	47
3.4.3.1	Identificación de componentes de cada recurso que deben ser restaurados completamente bajo posibles contingencias.....	48
3.4.3.2	Tiempo máximo permitido para la recuperación.....	49
3.5	Aplicaciones de alta criticidad. ....	51
3.5.1	Priorización de las aplicaciones.....	54
3.5.2	Aplicaciones implementadas en el sitio alternativo.....	55
3.6	Capacidad de Procesos de la Continuidad de Negocio .....	57
3.7	Amenazas a considerar para la migración. ....	60
4.	<b>CAPÍTULO IV. ANÁLISIS DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE RECUPERACIÓN ANTE DESASTRES EN LA NUBE.....</b>	<b>66</b>
4.1	Introducción.....	66
4.2	Problemas a Solucionar con DRaaS.....	67
4.3	Análisis de los proveedores de DRaaS.....	67
4.3.1	Requisitos para la contratación.....	70
4.3.2	Comparativa entre Proveedores.....	73
4.4	Estudio de Factibilidad .....	74
4.4.1	Estudio de Factibilidad Técnica.....	75
4.4.2	Estudio de Factibilidad Operativa.....	78
4.4.3	Estudio de los aspectos económicos.....	80
4.4.3.1	Solución IN HOUSE.....	81

4.4.3.2 Solución en la Nube.....	84
4.4.3.3 Viabilidad Económica.....	85
4.4.4 Estudio de los aspectos Legales.....	87
4.4.4.1 Obligaciones contractuales.....	90
<b>5. CAPÍTULO V. RESULTADOS DEL ANÁLISIS.....</b>	<b>93</b>
5.1 Introducción .....	93
5.2 Resultados .....	93
5.2.1 Aspectos Técnicos.....	93
5.2.2 Aspectos Operativos.....	95
5.2.3 Aspectos Económicos.....	95
5.2.4 Aspectos Legales.....	96
5.3 Recomendaciones para la Implementación .....	96
5.3.1 Solución Propuesta.....	100
5.3.2 Mapa de Ruta para implementación.....	102
5.3.2.1 Programación Estimada.....	102
5.3.2.2 Actividades del Proyecto.....	103
5.3.2.3 Fase 1: Rediseño.....	104
5.3.2.4 Fase 2: Planeamiento.....	104
5.3.2.5 Fase 3: Kickoff (Patada Inicial).....	105
5.3.2.6 Fase 4: Transferencia del conocimiento.....	106
5.3.2.7 Fase 5: Evaluación.....	106
5.3.2.8 Fase 6: Diseño.....	106
5.3.2.9 Fase 7: Despliegue.....	107
5.3.2.10 Fase 8: Validación.....	107
5.3.2.11 Fase 9: Conclusión.....	107

6. CONCLUSIONES Y RECOMENDACIONES .....	108
6.1 Conclusiones.....	108
6.2 Recomendaciones.....	109
REFERENCIAS .....	111
ANEXOS .....	118

## ÍNDICE DE FIGURAS

Figura 1. Orgánico estructural del departamento informática y tecnología .....	6
Figura 2. Tipos de Virtualización .....	10
Figura 3. Virtualización de Servidores .....	11
Figura 4. Virtualización de almacenamiento .....	12
Figura 5. Tipos de Nube .....	16
Figura 6. Nube Pública .....	17
Figura 7. Nube Privada .....	19
Figura 8. Nube Comunitaria .....	20
Figura 9. Nube Hibrida .....	22
Figura 10. PaaS vs SaaS vs IaaS .....	26
Figura 11. Plan de Recuperación ante Desastres .....	29
Figura 12. Esquema de Red Lan .....	40
Figura 13. Red Wan .....	41
Figura 14. Amenazas para la seguridad .....	45
Figura 15. Gartner - Proveedores de DRaaS .....	68
Figura 16. Servicio Microsoft DRaaS .....	69
Figura 17. Servicios IBM DRaaS .....	69
Figura 18. Servicios VMWare DRaaS .....	69
Figura 19. Recomendación de arquitectura .....	101
Figura 20. Actividades del Proyecto .....	103
Figura 21. Diagrama de Gantt del Proyecto .....	104

## ÍNDICE DE TABLAS

Tabla 1. Servicios de la institución .....	5
Tabla 2. Sucursales de la institución .....	7
Tabla 3. DRP Local Vs Nube.....	30
Tabla 4. Procesos Críticos de la institución.....	34
Tabla 5. Enlace de Datos .....	39
Tabla 6. Inventario Servidores.....	41
Tabla 7. Problemas y Consecuencias Depto. IT .....	46
Tabla 8. Riesgos Identificados .....	47
Tabla 9. Acciones Finales para riesgos encontrados .....	48
Tabla 10. Tiempo máximo de interrupción .....	49
Tabla 11. Riesgos de Alta criticidad de Alianza del Valle .....	50
Tabla 12. Aplicaciones categorizadas por su criticidad .....	51
Tabla 13. Priorización de aplicaciones .....	54
Tabla 14. Referencia priorización de aplicaciones .....	55
Tabla 15. Aplicaciones en sitio alternativo .....	55
Tabla 16. Metas, Prácticas clave y productos de trabajo de los procesos .....	57
Tabla 17. Ratio de la ISO/IEC 15504 .....	59
Tabla 18. Amenazas de migración a la nube .....	60
Tabla 19. Mitigación de posibles riesgos.....	62
Tabla 20. Importancia Parámetros Evaluación de Proveedores.....	73
Tabla 21. Comparativa de Proveedores.....	74
Tabla 22. Solución In House vs Nube .....	75
Tabla 23. Solución In House vs Solución en la Nube .....	76

Tabla 24. Encuesta aceptación del proyecto.....	78
Tabla 25. Encuesta solución In House vs Nube .....	79
Tabla 26. Compra e instalación COBIS.....	81
Tabla 27. Costo compra e instalación aplicaciones críticas .....	81
Tabla 28. Costo operación de servidores.....	82
Tabla 29. Costo contratación operador técnico .....	82
Tabla 30. Costo contratación Analista de Base de Datos .....	82
Tabla 31. Costo implementación Sitio Alterno.....	83
Tabla 32. Flujo de efectivo sitio alternativo .....	83
Tabla 33. Costo implementación DRaaS .....	84
Tabla 34. Costos contratación nuevo personal DRaaS.....	84
Tabla 35. Flujo de Efectivo - Costos DRaaS .....	85
Tabla 36. Valor Actual (VA).....	86
Tabla 37. VAN In House.....	86
Tabla 38. VAN DRaaS .....	86
Tabla 39. Tasa interna de Retorno (TIR).....	87
Tabla 40. Capacidades Requeridas .....	94
Tabla 41. Procesos Críticos y No críticos de Alianza del Valle .....	120
Tabla 42. Evaluación de Procesos – Encuesta .....	126
Tabla 43. Procesos Cobit 5 .....	131

# CAPÍTULO I

## ANTECEDENTES

### 1.1 Introducción

La información institucional de las empresas, se ha convertido en un activo fijo real invaluable y dado que es el activo más importante, no es de extrañar que se la debe proteger en caso de que se produzca un imprevisto que pueda provocar una interrupción en la continuidad del negocio, como la interrupción de su servicio, ya sea que se trate de errores humanos o de otros factores externos y se vea afectada la imagen institucional y por su puesto la rentabilidad de la misma (Esparza, 2016).

Sabemos que, la importancia de contar con un manejo estratégico de la información, hoy en día, implica la necesidad de estar preparados ante situaciones críticas que supongan paradas inesperadas en nuestras empresas, teniendo un plan B para una rápida recuperación desde el mismo punto en que se produjo la parada (Esparza, 2016).

La Recuperación ante Desastres como Servicio (DRaaS), es una solución de réplica y recuperación ante desastres basada en la tecnología de Computación en la Nube, que permite albergar una copia de los sistemas operativos y las aplicaciones en un sitio alternativo a modo de plataforma de contingencia en caso de desastre o indisponibilidad de la plataforma principal (NTT Communications, 2016).

Entre los principales beneficios se destaca la capacidad de proteger los sistemas y aplicaciones de carácter crítico para la empresa, evitando la pérdida e indisponibilidad de información, y así los costos que conllevaría una posible afectación de la continuidad de negocio, además la escalabilidad a la hora de incrementar las características de la plataforma actual, de acuerdo a lo que se requiera resguardar (Greenhouse, 2016).

Según (Gartner, 2014), antes de adoptar DRaaS, los líderes de TI deben entender su valor y limitaciones. Sin un análisis detallado, las organizaciones son propensas a tomar decisiones equivocadas y pueden entrar en contratos inapropiados.

Ahora tomando en cuenta que este nuevo aliado es la solución más factible para la recuperación de desastres tecnológicos, ¿Debería dar el salto a la Nube, la Cooperativa de Ahorro y Crédito “Alianza del Valle”?

La Cooperativa “Alianza del Valle”, es una Institución financiera que se conformó hace 46 años con la finalidad de satisfacer las necesidades económicas y sociales de los sectores productivos que no tienen acceso al sistema financiero tradicional. “Alianza del Valle”, busca como objetivo principal proyectar una imagen de confiabilidad a través de servicios financieros ágiles y oportunos (Alianza del Valle, 2016).

## **1.2 Objetivos**

### **1.2.1 Objetivo General**

Realizar el estudio de factibilidad para la implementación de *Recovery As A Service* (DRaaS) basado en el modelo de Computación en la Nube en la Cooperativa “Alianza del Valle”

### **1.2.2 Objetivos Específicos**

- Fundamentar teóricamente el uso de DRaaS como mecanismo de recuperación antes desastres tecnológicos en la Cooperativa de Ahorro y Crédito “Alianza del Valle”
- Efectuar un diagnóstico sobre la situación actual de “Alianza del Valle” frente a la implementación de *Disaster Recovery As A Service* (DRaaS).
- Realizar un estudio de factibilidad para implementar en “Alianza del Valle” *Disaster Recovery As A Service* (DRaaS) basado en el modelo de *Cloud Computing*.

- Proponer recomendaciones que le permita implementar *Disaster Recovery As A Service* (DRaaS) basado en el modelo de Computación en la Nube en “Alianza del Valle”.

### **1.3 Planteamiento del Problema**

La cooperativa de Ahorro y Crédito “Alianza del Valle”, no se encuentra realmente preparada para una recuperación ante desastres de su plataforma tecnológica, debido a que no cuenta con redundancia para asegurar que sus clientes tengan una alta disponibilidad de los servicios bancarios.

### **1.4 Alcance**

El alcance del presente tema de tesis, es realizar un estudio de factibilidad para la implementación de Recuperación ante Desastres como Servicio (DRaaS), para su sistema core COBIS.

#### Sistema Bancario COBIS

COBIS es un Sistema Bancario que maneja los siguientes módulos, fundamentales para el funcionamiento de la cooperativa:

- MÓDULO CUENTAS DE AHORROS
- MÓDULO DE CARTERA
- MÓDULO CONTABILIDAD
  - Manejo de Empresas
  - Manejo de la Estructura Organizacional
  - Periodos Contables
  - Plan de Cuentas
  - Manejo de Monedas
  - Uso de Comprobantes Contables
  - Saldos Contables
  - Reexpresión Monetaria
  - Interfaces Contables
  - Control Presupuestario
- MÓDULO DE CRÉDITO

- MÓDULO DE FIRMAS
- VALORES EN GARANTÍA
- CLIENTES
  - El CIF (*Central Information File*)
  - Información para Mercadeo
  - Información de Saldos de Clientes
- MÓDULO DEPÓSITOS A PLAZO FIJO

### **1.5 Justificación**

En la actualidad, la función interrumpida de las aplicaciones informáticas o las pérdidas de datos, causan graves perjuicios económicos. Las cooperativas no pueden dejar de entregar sus servicios en ningún momento, ya sea por un periodo de tiempo corto o largo por la criticidad de sus operaciones (Mercuriana, 2016).

Cada vez hay más conciencia sobre la importancia de mantener la continuidad del negocio, la productividad y la satisfacción de las expectativas de sus socios durante interrupciones y desastres operaciones (Mercuriana, 2016).

Los servicios de Computación en la Nube pueden ser de gran ayuda para las cooperativas, ya que generan confianza al realizar respaldo de aplicaciones y datos, pero, más allá de ello, pueden ser muy valiosos para apoyar los planes de recuperación ante desastres (Barahona, 2016).

Actualmente, “Alianza del Valle” requiere una solución tecnológica acorde a las tendencias actuales que le permita estar preparada para responder de forma efectiva, ante cualquier interrupción del servicio o pérdida de la información, considerando la criticidad de la administración de la misma y buscando disminuir la posibilidad de ocurrencia de un incidente de gran impacto para la organización.

Por lo tanto, se eligió este tema de tesis ya que DRaaS (recuperación ante desastres como servicio) se está convirtiendo rápidamente en una excelente alternativa para soportar las necesidades de las organizaciones, como alternativa de solución para la continuidad del negocio (Mercuriana, 2016).

## 1.6 Empresa

Cooperativa Alianza del Valle, es una Institución financiera que se conformó hace 46 años con el fin de colaborar con el progreso y bienestar de la comunidad, brindando seguridad y confianza, siempre enfocada hacia la satisfacción de sus socios, ya que gracias estos, ha logrado convertirse en una institución financiera sólida (Cadena & Barros , 2011).

Alianza del Valle se ha convertido en “Su Cooperativa Amiga”, dado que es una entidad solidaria que trabaja por la comunidad ofreciendo sobre todo seguridad y confianza a sus socios y empleados (Alianza del Valle, 2016).

### **Misión:**

“Satisfacer las necesidades y expectativas de nuestros socios, ofreciéndoles productos y servicios financieros innovadores, de calidad y con valor agregado, contando con una estructura administrativa/financiera sólida y con personal y directivos con visión social” (Alianza del Valle, 2016).

### **Visión:**

“En el año 2018, Alianza del Valle, se mantendrá dentro de las cinco primeras Cooperativas del Segmento 1, evaluados en términos de productividad y desempeño; ofertando sus productos y servicios financieros dentro de la Provincia de Pichincha” (Alianza del Valle, 2016).

### 1.6.1 Servicios de la institución

La Cooperativa “Alianza del Valle”, cuenta con los siguientes productos y servicios:

Tabla 1. Servicios de la institución

#### **Servicios:**

- \* Seguro Amigo
- \* Tarjeta de Débito
- \* Pago de Bono de Desarrollo Humano
- \* Sistema de Remesas CREER Ecuador

- \* Impuesto Predial
- \* Sistema de Envíos Western Union
- \* Transferencias Interbancarias
- \* Bono de Desarrollo Humano
- \* Ventanillas Extendidas
- \* Acreditaciones a Instituciones
- \* Acreditaciones IESS
- \* Impuestos Municipales
- \* Matriculación Vehicular

#### Productos:

- \* Productos de Ahorro
- \* Cuenta Efectiva
- \* Cuenta Sueña
- \* Cuenta Joven
- \* Cuenta Metahorro

#### Productos de Crédito:

- \* Seguro de desgravamen
- \* Bajas tasas de interés
- \* Cero comisiones
- \* CrediConsumo
- \* MicroCrédito
- \* CrediVivienda

#### Inversiones:

- \* Plazo Fijo Alianza

Adaptado de (Alianza del Valle, 2016)

### 1.6.2 Orgánico estructural del departamento informática y tecnología

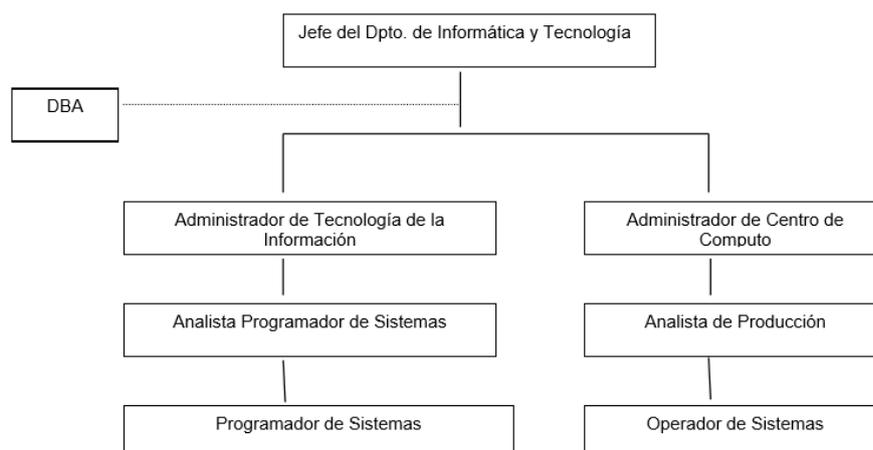


Figura 1. Orgánico estructural del departamento informática y tecnología

Tomado de (Alianza del Valle, 2016)

### 1.6.3 Funciones Críticas del Departamento de Sistemas

El Departamento de Informática y Tecnología, administra un software financiero contable de información llamado (COBIS) que permite a los usuarios gestionar de mejor manera su trabajo, a través de los siguientes módulos:

- a. Ahorros – Cajas - Socios Nuevos
- b. Inversiones - Plazo Fijo
- c. Crédito - Cartera
- d. Cobranzas
- e. Contabilidad (sólo Matriz)
- f. Clientes
- g. Firmas
- h. Seguridades

Además, el Departamento de Informática y Tecnología administra y desarrolla otras herramientas informáticas.

Todo esto respaldado por el soporte técnico que brinda a todas las dependencias de la Cooperativa; las agencias a las que se proveen servicios y herramientas informáticas son:

Tabla 2. Sucursales de la institución

Sucursales	Dirección
1 Matriz	Valle de los Chillos
2 El Inca	Los Nogales NE-47-161 y Av. El Inca
3 Chillogallo	Mariscal Sucre S30-125 y Morán Valverde
4 La Colón	Av. Colón e9-52 y 6 de diciembre
5 Guamaní	Av. Maldonado 4165 y Yanayacu
6 Machachi	Av. Colón y Av. Colombia s/n
7 Sanlgolquí	Av. General Enríquez 3032 y Río Chinchipe
8 Amaguaña	Gonzáles Suárez Parque Central
9 Conocoto	García Moreno 564 y Ponce Enríquez
10 Tumbaco	Av. Oswaldo Guayasamín E19 y Gaspar de Carvajal
11 Bicentenario	Av. la Prensa N53 - 153 y Gonzalo Gallo

## CAPÍTULO II

### MARCO TEÓRICO APLICADO

#### 2.1 Introducción

La Computación en la Nube, con frecuencia llamada *Cloud* o Nube, busca transformar todos los datos y aplicaciones en servicios online, es decir, ofrece la posibilidad de tener toda nuestra información subida en la nube, convirtiéndose en un recurso escalable que permite de forma rápida y sencilla a las organizaciones cubrir sus necesidades de tratamiento de la información (IBM, 2016) .

En un entorno de Computación en la Nube, la administración de la información es de forma virtual ya que, el cliente al contratar los servicios de la nube, accede mediante Internet a soluciones de correo electrónico, aplicaciones, bases de datos de acuerdo a sus necesidades, y a un click de distancia.

Tomando en cuenta que la Nube es una solución innovadora y que se apalanca mediante las tecnologías de vanguardia, no era de esperarse que también se la utilice para optimizar el plan de recuperación ante desastres. En este sentido la Recuperación ante desastres como Servicio (DRaaS), representa un gran paso respecto al *backup* tradicional. Se trata de usar el poder de la Nube para tener allí a todo el entorno informático crítico, virtualizado y en estado latente, a la espera de ser puesto en marcha si fuera necesario (German Bacca & Innovation Consultant, 2013).

El DRaaS sigue la filosofía con la que nació la nube: aportar eficiencia a los procesos de negocio, apalancarlos en su camino en la era digital con la flexibilidad del pago por uso y la escalabilidad como modelo de negocio.

El avance de la tecnología ha proporcionado una mejor forma de uso de los recursos informáticos, y cada vez se ha adoptado mucho más la estructura de

computación en la nube en las empresas, con la finalidad de ahorrar recursos económicos e invertir estos recursos en mejorar el negocio de la empresa.

## **2.2 Virtualización**

La virtualización se refiere a la creación de un recurso virtual tal como un servidor, de escritorio, sistema operativo, archivos, almacenamiento o de red.

El objetivo principal de la virtualización es la gestión de cargas de trabajo, transformando radicalmente la informática tradicional para que sea más escalable. La virtualización ha sido parte de la infraestructura de TI desde hace años, y hoy en día se puede implementar prácticamente en cualquier escenario, incluyendo virtualización a nivel de sistema, a nivel de hardware y virtualización de servidores.

La forma más común de la virtualización es la virtualización a nivel de sistema operativo. Con la virtualización a nivel de sistema, es posible ejecutar múltiples sistemas operativos en una sola unidad de hardware. La tecnología de virtualización consiste en separar el hardware físico y el software mediante la emulación de hardware mediante software. Cuando un sistema operativo diferente está funcionando encima del sistema operativo primario por medio de la virtualización, se conoce como una máquina virtual.

Una máquina virtual no es más que un archivo de datos en un equipo físico que se puede mover y copiar a otro ordenador, al igual que un archivo de datos normal. Los ordenadores en el entorno virtual utilizan dos tipos de estructuras de archivos: uno que define el hardware y el otro la unidad de disco duro.

La virtualización se puede clasificar en diferentes tipos: de escritorio, servidores, archivos, almacenamiento y redes. Cada capa de virtualización tiene su propio conjunto de ventajas y complejidades. Esta tecnología ofrece muchos beneficios, la utilización total de los recursos, ahorro de costes operativos y de ahorro de energía. Sin embargo, la implementación de la tecnología de virtualización requiere una cuidadosa planificación y expertos técnicos cualificados (Sara Angeles, 2014).

## 2.2.1 Tipos de Virtualización

A continuación, se detalla los principales tipos de virtualización:

- Virtualización de servidores
- Virtualización de almacenamiento
- Virtualización de red
- Virtualización de servicio



Figura 2. Tipos de Virtualización

Tomado de (Venkata & Malcom, 2011)

### 2.2.1.1 Virtualización de servidores

La virtualización de servidores es una técnica que implica particionar un servidor físico en varios servidores virtuales pequeños, con la ayuda de software de virtualización. En la virtualización de servidores, cada servidor virtual se ejecuta varias instancias del sistema operativo al mismo tiempo.

La virtualización de servidores intenta aumentar la utilización de recursos mediante la partición de servidores físicos en múltiples servidores virtuales, cada uno ejecutando su propio sistema operativo y sus propias aplicaciones. La

virtualización de servidores hace que cada servidor virtual actúe como un servidor físico, multiplicando la capacidad de cada máquina física.

El concepto de virtualización de servidores se aplica ampliamente en la infraestructura de TI como una manera de reducir los costos mediante el aumento de la utilización de los recursos existentes. La virtualización de servidores es a menudo una buena solución para pequeñas aplicaciones de mediana escala. Esta tecnología es utilizada para proporcionar servicios rentables de alojamiento web (Microsoft, 2016).

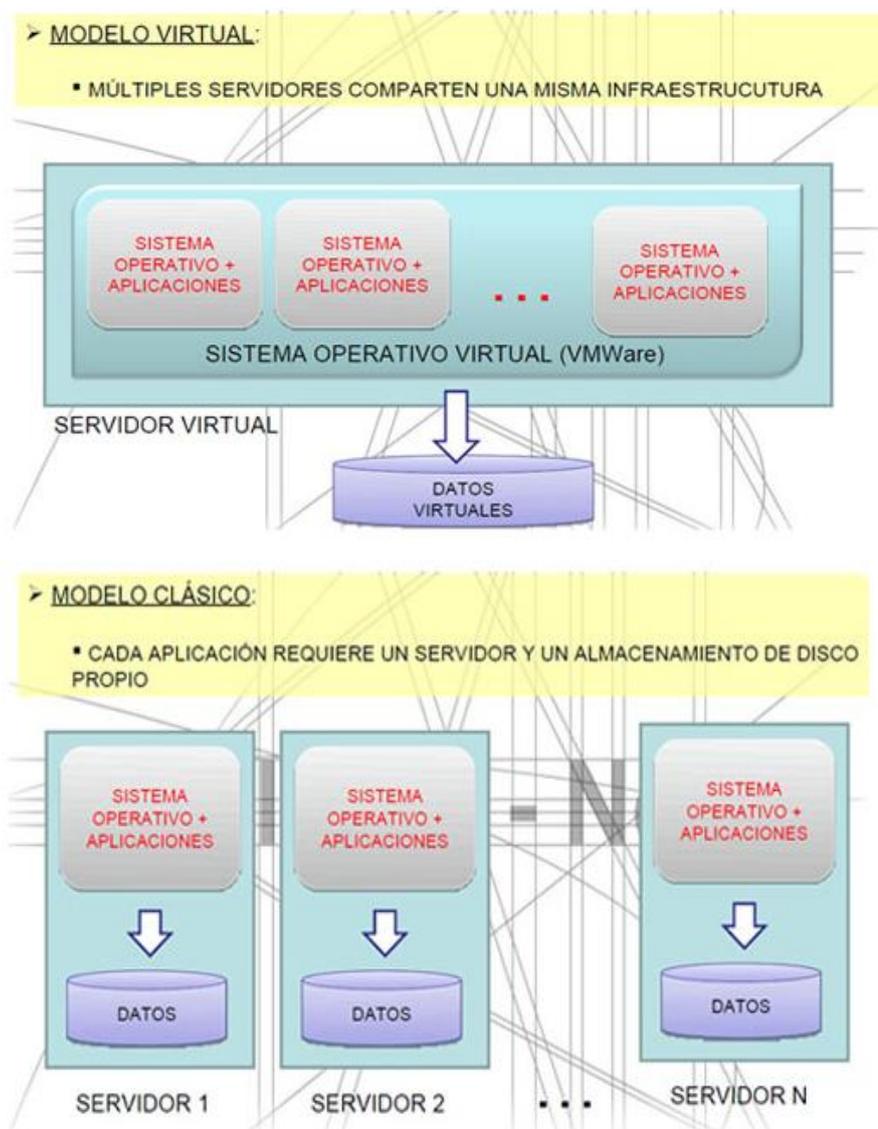


Figura 3. Virtualización de Servidores

Tomado de (Girsanet, 2016)

### 2.2.1.2 Virtualización de Almacenamiento

La virtualización de almacenamiento es el proceso de agrupar el almacenamiento físico de múltiples dispositivos en red para que se vea como un solo dispositivo de almacenamiento.

Este tipo de virtualización es usada a menudo en tareas de almacenamiento, replicación, respaldo y recuperación de datos de forma más fácil y rápida.

Este proceso de virtualización, consiste en independizarse de la locación física de los datos, es decir el sistema de virtualización presenta al usuario un espacio lógico para el almacenamiento de datos (Grupo trevenque, 2016).

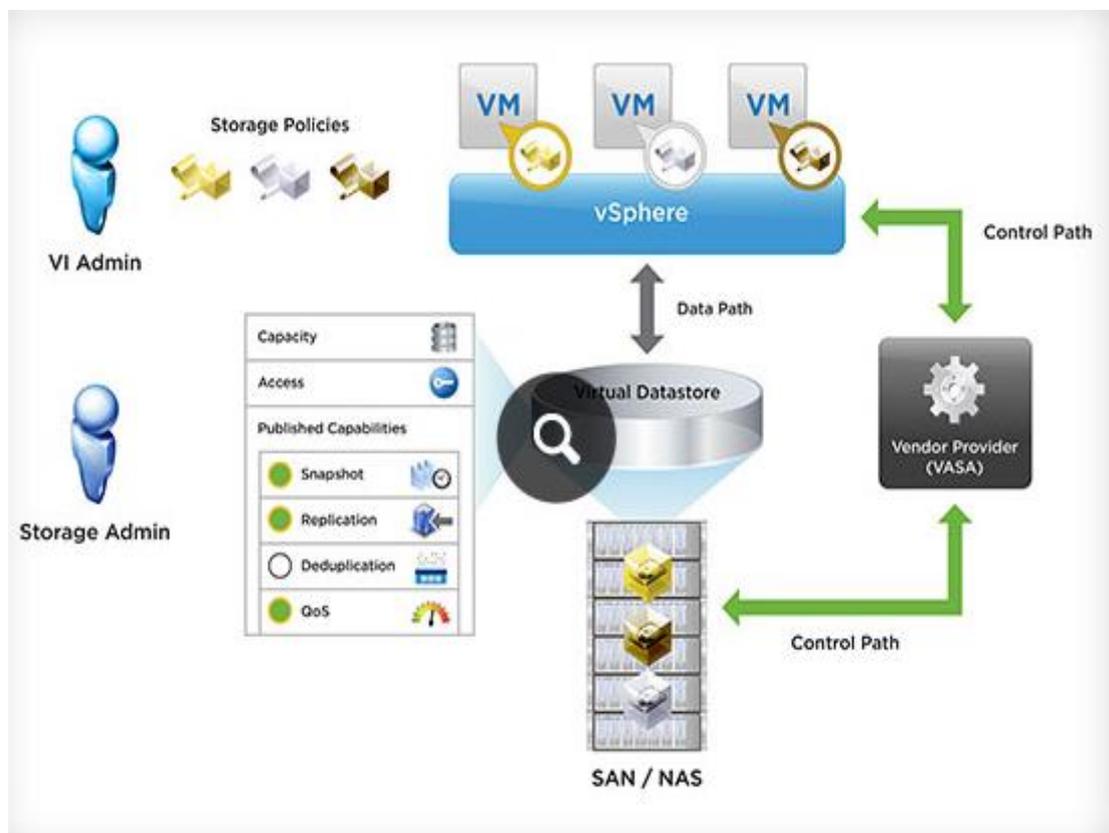


Figura 4. Virtualización de almacenamiento

Fuente: (vmware, 2016)

### 2.2.1.3 Virtualización de Servicios

La virtualización de servicios es la capacidad de crear una simulación de las aplicaciones que se encuentran en producción, en un ambiente virtualizado

permitiendo llevar a cabo distintos procesos en un único servidor, unificando recursos de cómputo, comunicación y almacenamiento.

Este tipo de virtualización también se refiere a servicios, tales como un Firewall para obtener una seguridad adicional o el servicio de balanceadores de carga para obtener un rendimiento y una fiabilidad adicional.

### **2.2.2 Ventajas de la Virtualización.**

- Gestión centralizada de recursos virtualizados.
- Facilita las soluciones de restauración y mejora la protección de los datos.
- Uso eficiente de los recursos del Hardware.
- Reduce drásticamente los costos de mantenimiento.
- Balanceo dinámico de los recursos entre las máquinas virtuales.
- Consumo óptimo de los recursos.
- Portabilidad de las máquinas virtuales entre los servidores físicos.
- Eficiente entre máquinas virtuales, sin la pérdida de servicio.
- Menor costo dado que se aprovecha mejor el hardware.
- Gran capacidad para la clonación y *backup* de los sistemas.
- Ahorro en el consumo de energía.
- Agrupa de toda la capacidad de procesamiento, memoria, red y almacenamiento disponible, mejorando la gestión de los mismos.

### **2.2.3 Desventajas de la Virtualización**

- Requerimiento de hardware muy específico.
- Posibles problemas de compatibilidad con los dispositivos Hardware virtualizados.
- Redistribución de los servicios para balancear la carga de trabajo.
- Si se realiza virtualización local es necesario la renovación y actualización de servidores antiguos ya que se requiere mayor cantidad de recursos como memoria RAM, procesador y disco duro.
- Vacíos legales respecto al uso de licencias virtuales.
- Baja disponibilidad: De perfiles técnicos especializados.

- Posible complejidad de los sistemas.
- Aparición de nuevos retos en el testeo.

## **2.3 Computación en la Nube**

Según Gartner (2016) , la computación en la nube es un tipo de computación, donde las capacidades de IT, son entregadas como servicio mediante la internet, de manera flexible y escalable, esto se refiere al conjunto de programas y servicios que se encuentran alojados en un servidor en Red, donde se puede acceder desde cualquier equipo que cuente con conexión a Internet.

NIST, define a la Computación en la Nube de la siguiente manera:

“La Computación en la Nube es un modelo para habilitar acceso conveniente por demanda a un conjunto compartido de recursos computacionales configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios. Este modelo de nube promueve la disponibilidad y está compuesto por cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue” (Peter Mell & Timothy Grance, 2011).

La “Nube” o *Cloud* ha revolucionado la manera en como trabajaban todos los sectores de negocio, es ahora considerado como un componente indispensable para el éxito de las empresas ya que ha llegado a ser una ventaja competitiva, al facilitar el acceso de aplicaciones, almacenamiento y demás servicios, convirtiéndose en un aliado de negocio.

Se prevé que la Computación en la Nube va a cambiar el futuro de la tecnología ya que ha pasado de ser una tecnología que se adoptó inicialmente para ahorrar costos y aumentar la eficiencia de las operaciones a ser una pieza fundamental en el diseño de las estrategias y los modelos de negocio de las organizaciones.

### **2.3.1 Características**

A continuación, se describirá las características primordiales:

- Auto-servicio por demanda: servicios informáticos tales como el correo electrónico, aplicaciones, servidor de red o servicios en general pueden ser proporcionados sin requerir interacción con el proveedor de servicios.
- Amplio acceso desde la red: Las aplicaciones que se encuentran alojadas en la Nube se encuentran disponibles para los usuarios, pudiendo acceder a ellas mediante equipos que cuenten con conexión a internet.
- Conjunto de recursos: El proveedor del servicio cuenta con una única aplicación que está disponible para todos los usuarios que la requieran, estableciendo permisos de acceso y distinciones para cada usuario. A estas aplicaciones se las conoce como multiusuario, es decir, miles de usuarios usan la misma herramienta a la vez.
- Rápida elasticidad: Las aplicaciones que se encuentran alojadas en la Nube son totalmente elásticas en cuanto a su adaptabilidad, es decir si el día de mañana se requiere mayores características, se puede acceder a ellas con un click o comunicándose con el proveedor.
- Servicio medido: Los recursos alojados en la Nube pueden ser monitoreados, controlados y optimizados de manera automática, proporcionando transparencia por el servicio utilizado, tanto para el proveedor como para el consumidor.

### **2.3.2 Tipos de Nube**

Según NIST (2012) la Computación en la Nube se divide en:

Modelo de Despliegue encontramos:

- Nube Pública
- Nube Privada
- Nube Comunitaria

Modelo de Servicio encontramos:

- Infraestructura como Servicio (IaaS).
- Plataforma como Servicio (PaaS).
- Software como Servicio (SaaS).



Figura 5. Tipos de Nube

Tomado de (Peter Mell & Timothy Grance, 2011)

### 2.3.2.1 Modelo de Despliegue de Computación en la Nube

#### Nube Pública

La nube Pública o *Cloud* Público, es un modelo estándar donde la infraestructura de la nube está disponible para cualquier usuario en Internet, donde el usuario hace uso de software o hardware con todas las ventajas del modelo de consumo de la Nube (Forma libre, pago por uso, aprovisionamiento ágil, elasticidad, etc.), ya que los servicios que ofrece el proveedor, se encuentran en servidores externos al usuario u organización.

El usuario puede automatizar el despliegue de máquinas pre-configuradas o integrar estos servicios rápidamente con aplicaciones propias, gracias a la virtualización y a los procesos de automatización del servicio que dicho proveedor tiene implementados.

#### **Ventajas**

- Capacidad de procesamiento y almacenamiento sin instalar máquinas localmente
- No tiene una inversión inicial o gasto de mantenimiento.
- Responsabilidad de carga operacional y la seguridad de los datos única del proveedor.
- El riesgo por la adopción de una nueva tecnología es bastante bajo.

- Retorno de la inversión mucho más rápido.

### Inconvenientes

- Dependencia de los servicios en línea (a través de Internet).
- Puede resultar difícil integrar estos servicios con otros sistemas propietarios.
- El usuario o cliente no conoce la ubicación física de sus datos, ya que estos dependen del funcionamiento y arquitectura adoptada por el proveedor de servicios de la Nube.

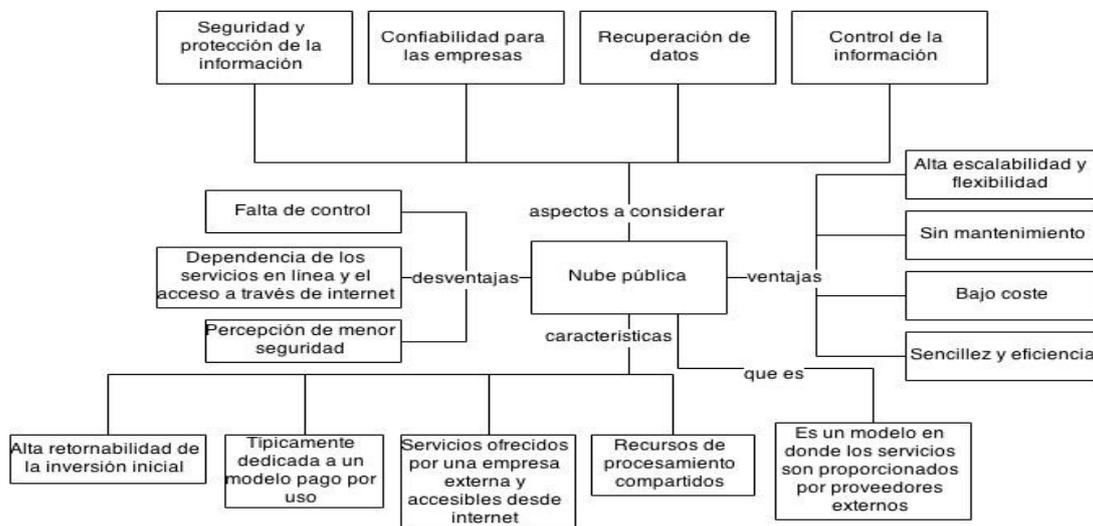


Figura 6. Nube Pública

Tomado de (Duarte, 2015)

### Nube Privada

La nube privada es aquella en que las empresas disponen de un entorno en la Nube exclusivo para ellas, utilizando tecnologías como la virtualización, tiene acceso a los recursos de la nube.

Estas nubes podrían compararse con un centro de datos normal de cualquier empresa, ya que emulan la computación en la nube con redes o centro de datos propietarios. Mediante la virtualización podemos añadir a las características del

centro de datos los beneficios de la Nube, tales como la agilidad en la provisión o cierto nivel de elasticidad.

### **Ventajas**

- Sensación de mayor seguridad de los datos ya que se encuentran alojados en la nube dentro de la misma ubicación geográfica de la empresa.
- Proporcionan un control óptimo de la gestión de la información, la seguridad de los datos y de la calidad de los servicios ya que suelen tener un diseño específico para cada usuario.

### **Inconvenientes**

- Es más complicado realizar una ampliación de algún servicio, ya que esto conllevaría a adquirir nuevos sistemas antes de garantizar un adecuado funcionamiento
- Fuertes inversiones tanto iniciales en la adquisición del equipamiento como posteriores para su gestión. Además de contar con las licencias respectivas del software desplegados en ellas.

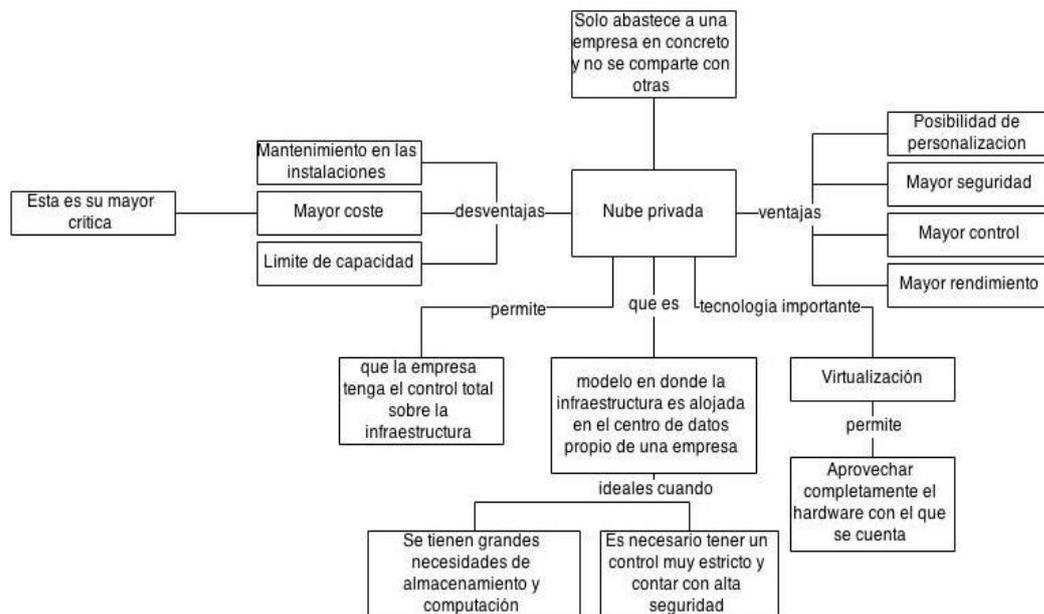


Figura 7. Nube Privada

Tomado de (Duarte, 2015)

### **Nube Comunitaria**

En el modelo de nube comunitaria, la infraestructura de la nube es compartida por varias organizaciones, logrando apoyar a una comunidad u organización específica que comparte las mismas preocupaciones (misión, seguridad, requisitos, consideraciones de normativa legal, etc). En este tipo de nube puede ser gestionada por las mismas organizaciones o encargada a una tercera organización independiente y que solo se dedique a gestionar la nube, esto se puede lograr a través de tecnología estándar o propietaria que facilite la portabilidad de los datos y aplicaciones alojadas en la nube comunitaria.

#### **Ventajas**

- Costos compartidos,
- Infraestructura compartida
- Responsabilidad compartida

## Inconvenientes

- Posibles conflictos entre las organizaciones involucradas

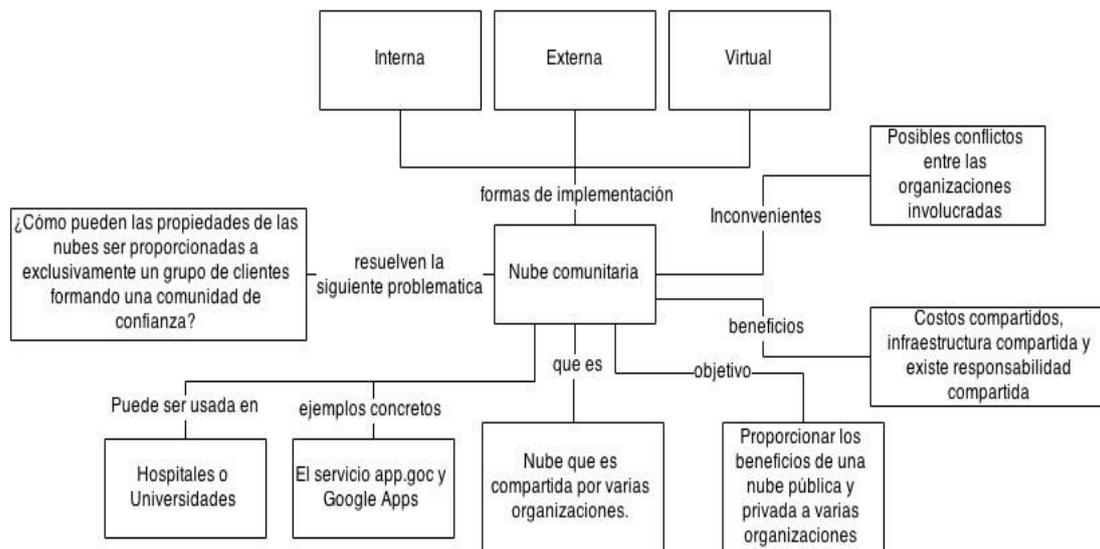


Figura 8. Nube Comunitaria

Tomado de (Duarte, 2015)

## Nube Híbrida

El NIST (2012), define a la nube híbrida como una composición de dos o más nubes (privados, comunitarios o públicos) que mantienen su propia identidad, pero son unidas entre sí por una tecnología propietaria o estándar para permitir la portabilidad de datos y aplicaciones desde cualquier punto. Este tipo de nube surge a partir de la necesidad de los clientes que cuentan con infraestructura propia, pero buscan aprovechar las ventajas de los servicios de un proveedor externo.

A continuación, se detalla las diferentes maneras de implementar el modelo de Nube híbrida:

- Colaboración entre varios prestadores de servicios de Computación en la Nube para proveer servicios integrados combinando la Nube pública y privada.

- Servicios integrados proveídos por un único proveedor de servicios en la Nube.
- Empresas que cuentan con Nubes privadas propias y que a su vez contraten un servicio de Nube pública y los integren posteriormente en sus infraestructuras.

### **Ventajas**

- Escalabilidad; dado que las Nubes privadas ofrecen una limitada escalabilidad dependiendo su configuración, interna o externa, los servicios de Nube públicas ofrecen una escalabilidad mucho más flexible, es por esto que si las organizaciones trasladan las funciones y servicios que requieran a la Nube pública reducirán la demanda ejercida sobre la infraestructura de su Nube privada.
- Eficiencia en Costos; Las Nubes híbridas permiten a las organizaciones beneficiarse de la gestión centralizada de la Nube pública, significando mayor ahorro, y a su vez mantener la seguridad de sus operaciones más críticas en la nube privada.
- Seguridad; La Nube Híbrida mediante el componente de Nube privada aporta con la seguridad necesaria para las actividades más críticas de la organización, aunque se debe tener el mismo cuidado que con una nube pública.
- Flexibilidad/elasticidad; Gracias a las facilidades de la nube pública, las organizaciones pueden acceder a una mayor capacidad cuando agoten la capacidad de su nube privada, lo cual les permitiría continuar operando sin ningún inconveniente.

### **Inconvenientes**

- Dependencia de las capacidades tecnológicas y financieras de los proveedores de servicios en la nube.
- La información de la empresa debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos representan un punto de inseguridad.

- Dependencia de los proveedores debido a la centralización de las aplicaciones y el almacenamiento de los datos.

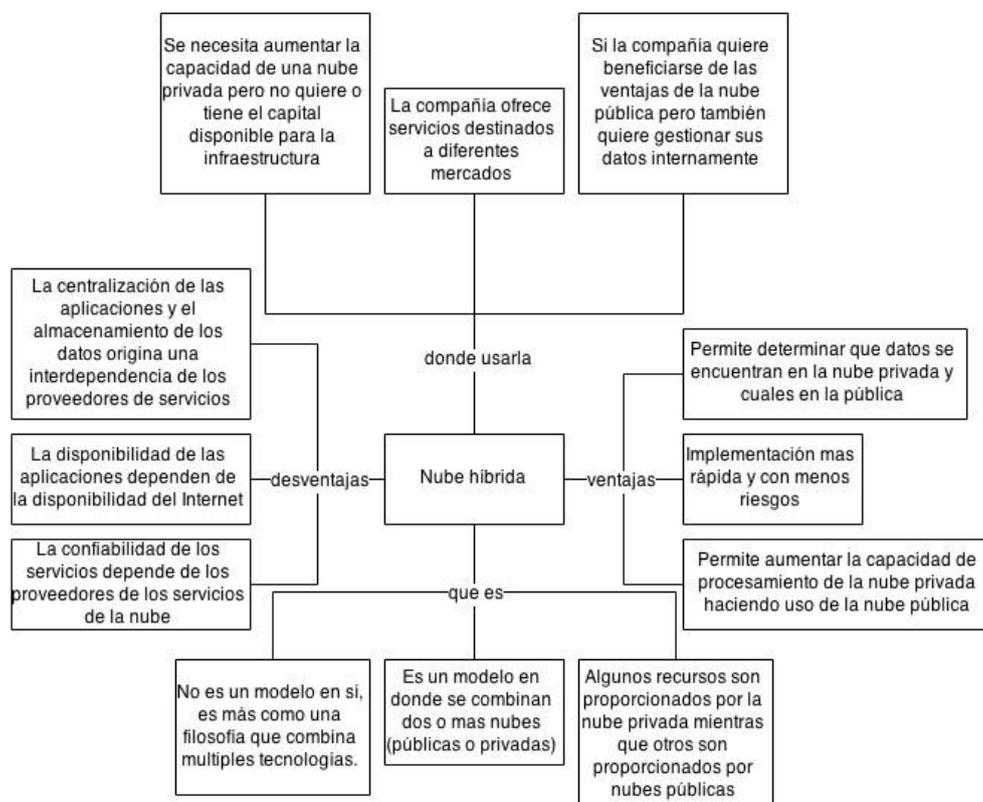


Figura 9. Nube Híbrida

Tomado de (Duarte, 2015)

### 2.3.2.2 Modelos de Servicio de Computación en la Nube

#### Infraestructura como servicio (IaaS)

En el modelo IaaS el cliente renta infraestructura informática como servicio, es decir los clientes no usan sus propios equipos físicos, sino que usan los recursos virtualizados que le proporciona el proveedor de servicios de Computación en la Nube, en este caso el cliente no gestiona dichas infraestructuras (servidores, SAN, routers, switches, etc.), pero es responsable de la instalación, mantenimiento, y ejecución de sus propias aplicaciones, teniendo el control sobre los sistemas operativos, política de almacenamiento, aplicaciones desplegadas y posiblemente un control limitado sobre componentes de red, de

forma que el costo de la infraestructura depende de los recursos consumidos (Interoute, 2016).

### **Tipos de IaaS**

- "*Cloud Hosting*" o alojamiento en nube, es un servicio de hosting que permite escalabilidad y crecimiento del servicio de alojamiento contratado por el cliente; además, el cliente tiene acceso remoto al servicio contratado, a través de Internet, mediante un navegador web.
- "*Datacenter As a service*" o centro de datos como servicio. En este modelo tecnológico un proveedor ofrece una solución completa de centro de datos de manera virtual.

Las ventajas que nos brinda IaaS:

- Los recursos son virtualizados, entregando mayor eficiencia ya que se garantiza que se utilice la máxima capacidad de su infraestructura física.
- Rápida escalabilidad ya que los recursos de cómputo adicionales se pueden asignar rápidamente para satisfacer las exigencias del negocio.
- Menores costos gracias al modelo de "pago en función del uso".
- Las herramientas de evaluación permiten a los administradores de TI detectar las áreas dónde se pueden reducir los costos.
- Mayor utilización de las inversiones en TI
- Mejor seguridad y protección de los recursos de información

### **Plataforma como servicio (PaaS)**

En este modelo, el proveedor del servicio entrega al cliente una solución en la que se le permite albergar sus aplicaciones utilizando el sistema operativo provisto por el proveedor, de acuerdo a las necesidades del cliente. En el modelo PaaS el proveedor ofrece el uso de su plataforma tecnológica por lo que el usuario tiene control únicamente sobre sus aplicaciones y no sobre dicha plataforma (Gartner, 2012).

Uno de los tipos de PaaS es "*Storage As a Service*" o almacenamiento como servicio, este se basa en alquiler de espacio de almacenamiento en la infraestructura del proveedor del servicio. Gracias a este modelo el cliente no sobredimensiona inicialmente las capacidades de almacenamiento de acuerdo a sus necesidades futuras, si no que expande el tamaño de almacenamiento contratado según como vayan aumentando sus necesidades (Devicro, 2016).

Entre las facilidades que nos brinda PaaS son:

- Tiene la capacidad de soportar el uso simultaneo de una aplicación por varios usuarios.
- Control total de las aplicaciones albergadas en la nube, así como también el entorno de las configuraciones de las mismas.
- No necesitan invertir en infraestructura física.
- Facilidad de uso.
- Los clientes cuentan con la flexibilidad de crear plataformas adaptadas perfectamente a sus necesidades específicas.
- Este modelo cuenta con diversos mecanismos de seguridad como protección de los datos almacenados y copias de seguridad.

### **Software como servicio (SaaS)**

En el modelo SaaS, el cliente accede remotamente desde cualquier lugar mediante conexión a internet a aplicativos entregados por el proveedor del servicio, el proveedor es el encargado de mantener la operatividad, dar mantenimiento y realizar las actualizaciones de las mismas de acuerdo a las necesidades del cliente.

Este modelo se lo conoce también como "software a demanda", en él los usuarios se suscriben generalmente por periodos mensuales, en lugar de comprarlo. Las aplicaciones corren en servidores de propiedad de los proveedores del servicio, y se accede a ellas mediante navegadores Web; el cliente no necesita instalar nada adicional en los equipos locales para acceder a las aplicaciones contratadas.

El cliente no conoce la plataforma tecnológica donde corre la aplicación contratada, únicamente debe tener en claro el límite de usuarios permitidos de acuerdo a lo contratado (Gartner, 2012).

Uno de los tipos más utilizados de SaaS es el "*desktop as a service*", esta solución se basa en entregar un escritorio al cual se accede de manera remota desde cualquier terminal, otro tipo es el servicio de correo electrónico o el servicio de almacenamiento como Dropbox.

Los beneficios que nos da SaaS son:

- Precio; SaaS evita los costos iniciales de compra e instalación, así como los costos actuales asociados con el mantenimiento y las actualizaciones, además sólo se paga por lo que se necesita sin tener a un exceso de provisión de servicios o hardware.
- Tiempo; Se puede acceder a aplicaciones SaaS, con tan solo tener un navegador conectado a Internet.
- Además, hay ahorro de tiempo al no tener que llevar a cabo cualquier mantenimiento o actualizaciones de las aplicaciones o de su hardware subyacente, ya que el proveedor de SaaS hace todo.
- Escalabilidad; SaaS ofrece gran flexibilidad. El aumento por ejemplo del número de usuarios del servicio se puede hacer fácilmente y sin previo aviso.
- Compatibilidad entre dispositivos, SaaS permite acceder a las aplicaciones alojadas en la nube mediante cualquier dispositivo que cuente con conexión a internet.
- Accesible desde cualquier lugar con conexión a internet, sin las limitaciones de instalaciones de equipos específicos.

## IaaS vs PaaS vs SaaS

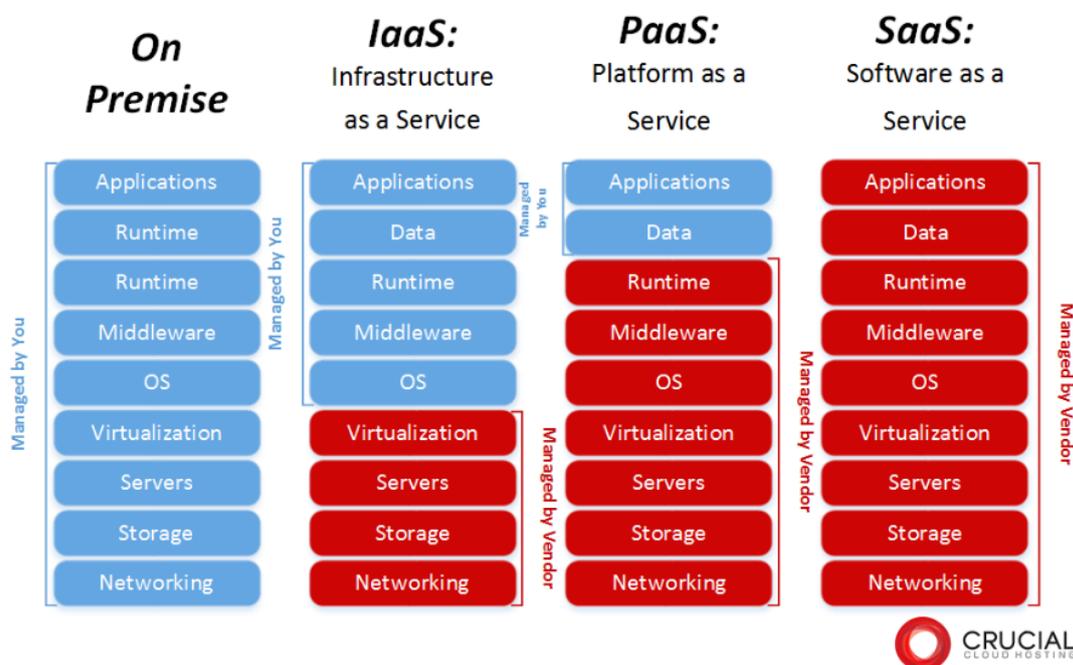


Figura 10. PaaS vs SaaS vs IaaS

Tomado de (Weller, 2013)

### 2.4 Seguridad de Datos en la Nube

En los últimos años muchas empresas han migrado a la Nube para utilizar sus servicios debido al ahorro que representa, ya sea por la modalidad de pago por uso o al no tener que comprar infraestructura de Data Center, etc. Aunque la Nube no es un servicio nuevo, las compañías y los departamentos IT, aún tienen sus reservas cuando consideran su adopción, ya que es necesario tener en cuenta que al migrar se está poniendo la seguridad e integridad de los datos en manos de terceras personas, y es por esto que la seguridad debe ser un elemento fundamental si se piensa en migrar.

Las principales preguntas que se hacen las empresas respecto al uso de los servicios de Computación en la Nube es, ¿Cómo asegurar sus activos de información en estos entornos externos? O ¿Quién es responsable de mantener la seguridad y cuál es la responsabilidad de cada una de las partes involucradas?, ya que los usuarios no conocen la localización remota en donde

se encuentran almacenados sus datos, ni los mecanismos empleados como seguridad para proteger los mismos; es decir el usuario no conoce si la información que se encuentra en la nube está siendo cifrada, o si “alguien” no autorizado está haciendo uso de ella.

Según una investigación realizada por *Unisys Corporation* (2014), revela que, a pesar de la preocupación continua por la seguridad, los CIO y otros líderes de TI, están migrando en un porcentaje en aumento, su información a la Nube y están haciendo uso de la nube privada y de software como servicio (SaaS).

Al adquirir un servicio en la nube, el proveedor de los servicios se encarga de garantizar la seguridad física en sus centros de datos, así como de mantener las máquinas actualizadas, con el ahorro de costes que esto conlleva (BBVA Innovation Center, 2015).

Sin embargo, hay tres claves que se debe tener en cuenta si se quiere migrar a la Nube:

- **Segmentación de entornos:**  
Los entornos para hacer las aplicaciones están separados, es decir los datos reales por un lado y los datos de prueba por otro evitando la mezcla de los mismos. A través de la segmentación se genera una seguridad más estricta en los entornos de servicio final al cliente.
- **Segregación de responsabilidades:**  
Los proveedores de nube se encargan de la seguridad física. Son los responsables de impedir que personas no autorizadas entren en las instalaciones, así como de mantener sus equipos actualizados tanto a nivel hardware como software, ellos deben estar preparados para hacerle frente toda amenaza existente en la internet.  
Por ello, el proveedor debe aplicar estrictas normas de seguridad en sus procesos.  
El usuario por su parte, se encarga de la seguridad de las aplicaciones migradas y de sus datos, como por ejemplo debe ser responsable con el manejo de contraseñas y configuraciones.

- Disponibilidad:  
Al ser un entorno distribuido en múltiples centros de datos, los sistemas de nube son muy resistentes a fallos de todo tipo.

## **2.5 Plan de Recuperación ante desastres(DRP)**

Un desastre es un evento que afecta a la continuidad de los servicios y funciones normales de una empresa, es por esto que los planes de recuperación ante desastres son de vital importancia, ya que lo único que puede salvar a una empresa, ante la amenaza de un desastre o después de que ha ocurrido es la forma de prevenirlos.

Un plan de recuperación ante desastres (DRP) es un conjunto de procesos que se encuentran documentados con la finalidad de proteger la plataforma tecnológica de una empresa y de recuperarla en caso de un desastre, ya que la pérdida de datos o peor aún la interrupción de la continuidad del negocio puede llegar a tener un impacto económico grave y perjudicial para la empresa, ya que podría ocasionar la pérdida de clientes por la desconfianza que esto conlleva o peor aún el cierre de las operaciones por un tiempo indefinido.

Cada empresa es muy diferente, ya sea por el tipo de negociación, objetivos institucionales, por sus procesos o por el nivel de seguridad que esta requiera, es por esto que los planes de recuperación ante desastres deben de ser adaptados según los requerimientos de cada institución.

### **Beneficios de implementar un DRP**

- La capacidad de proteger los sistemas críticos para la empresa.
- Reducción de pérdidas tras un incidente.
- Proporciona sentido de seguridad.
- Minimizar el riesgo de retrasos tras un incidente.
- Garantizar la fiabilidad de los sistemas de reserva.
- Minimizar la toma de decisiones en caso de desastre.
- La reducción de las posibles responsabilidades legales.

- Ayuda a la identificación de la relación que tiene entre los activos, recursos humanos y los recursos financieros que intervienen en los servicios críticos.

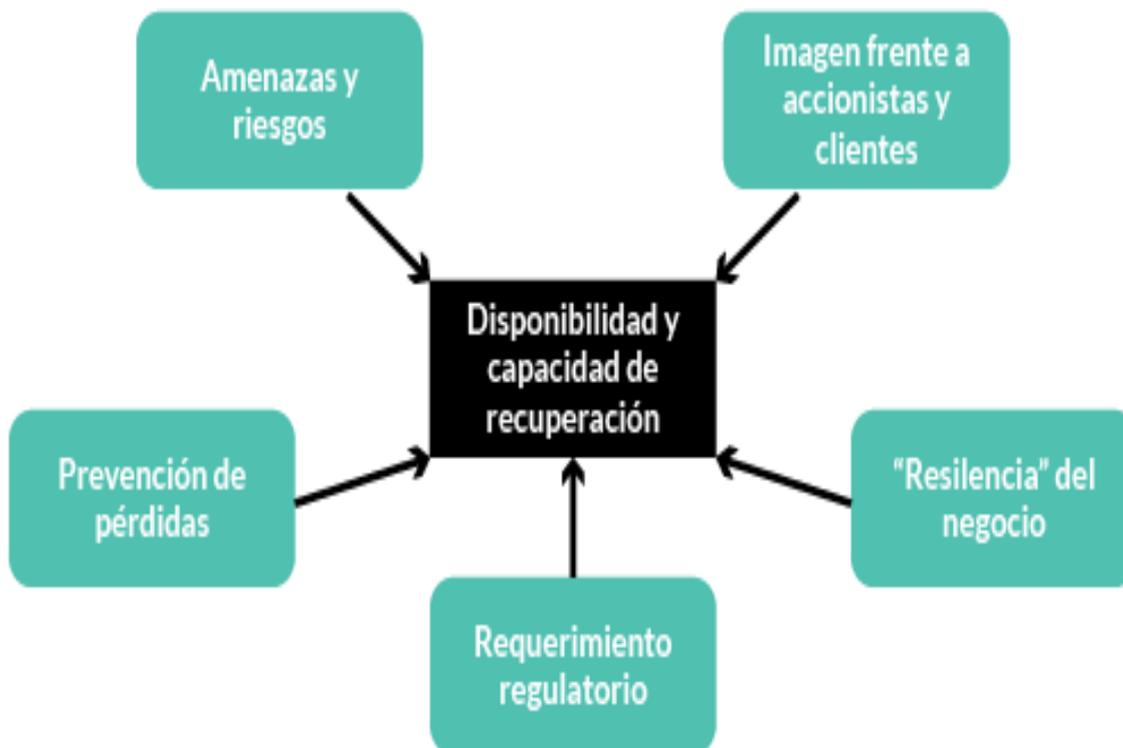


Figura 11. Plan de Recuperación ante Desastres

Fuente: (ECloud, 2015)

### 2.5.1 Tipos de Contingencia

Existen diferentes tipos de contingencia de acuerdo a los daños sufridos:

- No Crítica: recuperación menor a 24 horas y solo afecta a las operaciones diarias no críticas.
- Crítica: afecta directamente a la imagen institucional, frenando las operaciones y servicios. Este incidente no es recuperable a corto plazo y puede deberse por fallas humanas o por algún tipo de desastre natural. Esto puede impedirse median normas preventivas.

Los tipos de contingencias serán aplicados en la presente tesis para identificar las aplicaciones de alta criticidad.

### 2.5.2 DRP tradicionales Vs DRP en la nube

A continuación, se mostrará una comparación entre los métodos tradicionales y los de la computación en la nube, para recuperación ante desastres:

Tabla 3. DRP Local Vs Nube

<b>DRP Local</b>	<b>DRP Nube</b>
Tiempo de recuperación de varias horas	Recuperación imperceptible para el cliente
Respaldos en su mayoría incrementales una vez al día	Respaldos diferenciales en minutos
RPO (Objetivo de punto de recuperación) y RTO (Objetivo de tiempo de recuperación), desconocido e inestable.	RPO y RTO, mejoran considerablemente, ya que se tiene una protección continua de los datos y se ejecuta un respaldo del servidor virtual de manera inmediata sin necesidad de restauración.
Contempla el uso de Software especializado para efectuar los respaldos, contemplando desafíos de respaldos mal efectuados, además de costos de servidores para almacenar los mismos.	Facilidad de administración con unos cuantos clics, respaldos completos y sin costos iniciales por compra de servidores.
Posibles fallas en la verificación de los datos respaldados	Verificación de respaldos de manera automática.

### 2.6 Disaster Recovery As A Service (DRaaS)

La interrupción de los servicios TI puede llegar a ser catastrófico, si es que la continuidad de negocio se ve afectada, ya que esto puede ocasionar graves perjuicios económicos, es por esto que en los últimos tiempos se ha vuelto necesario que las empresas estén preparadas para enfrentar los desastres como pueden ser cortes de energía, fallas a nivel de hardware, incendios, terremotos, inundaciones, etc. Uno de los principales desafíos que tienen hoy en día las empresas es contar con un plan de recuperación ante desastres que se adapte a sus necesidades, logrando tiempos rápidos de recuperación y cumpliendo con las normativas vigentes (Bacca, 2013).

Disaster Recovery As A Service (DRaaS) es un componente que no debe faltar en un DRP (Plan de Recuperación de Desastres), ya que permite que las empresas dispongan de una réplica exacta de sus sistemas y aplicaciones en un Data Center remoto alojado en una nube privada o pública. Este Data Center remoto actuará como plataforma tecnológica de contingencia en caso de ocasionarse un paro en los servicios de la empresa, ya que permite tener una réplica exacta de la misma, convirtiéndose en un nuevo concepto de recuperación ante desastres.

DRaaS ofrece una serie de ventajas que vuelven atractiva a esta solución, como, por ejemplo, reducir costos ya que a la hora de implementar un plan de recuperación convencional se tendría que duplicar el Centro de Datos ocasionando mayor gasto.

DRaaS lleva el concepto de recuperación más allá, ya que no solo es recuperar datos críticos sino recuperar la continuidad del negocio en el menor tiempo posible; DRaaS es una estrategia que incluye poder de cómputo en la nube, seguridad, almacenamiento y servicios de conectividad (Revista MyM, 2015).

#### **Beneficios del DRaaS:**

- **Automatización:** gestión automatizada de los planes de recuperación, lo que disminuye el RTO.
- **Flexibilidad:** crecimiento flexible de acuerdo a las necesidades del negocio, de manera fácil, y automática.
- **Reducción de costes:** DRaaS ofrece el modelo de pago por uso, solo es necesario estimar de manera adecuada los requerimientos.
- **Rápida recuperación:** RTO mínimos.
- **Backup seguro:** DRaaS ofrece opciones de réplica que encriptan la información, impidiendo que terceras personas puedan acceder a la misma.
- **Reducción de infraestructura:** ahorro en servidores, medios de almacenamiento, y espacio de backup.

- **Movilidad:** administración y mantenimiento de manera remota, accediendo desde cualquier dispositivo que cuente con conexión a internet.

En conclusión, con DRaaS, es posible conseguir los objetivos del Plan de Recuperación ante Desastres a un bajo costo, ya que permite eliminar la pérdida de datos gracias a la replicación en tiempo real, y así reducir el tiempo de inactividad de las aplicaciones críticas de la empresa.

### 2.6.1 Tipos de DRaaS

- Entorno de producción y backup en la Nube:  
Esta opción se refiere a tener los dos entornos de producción y de backup en la Nube y así aprovechar todos los beneficios que entrega la Computación en la Nube, como la opción de “Pago por Uso”, o la eliminando de las instalaciones de infraestructura locales, que conllevan mantenimiento y gasto operativo.
- Entorno de Backup en la Nube:  
En esta opción el entorno primario que es un entorno tradicional se encuentra de manera local y, únicamente se realiza copias de seguridad en un entorno de Nube.
- Réplica de Máquinas Virtuales en la Nube:  
La replicación de máquinas virtuales a la Nube, ya sea de máquina a máquina en la nube o de máquina local a máquina en la nube, es de manera automática e inmediata, prácticamente sólo se debe restaurar una copia de la máquina virtual, esto es la mejor opción cuando se requiere de RTO agresivos.

## CAPÍTULO III

### SITUACIÓN ACTUAL DE “ALIANZA DEL VALLE” FRENTE A LA IMPLEMENTACIÓN DE *DISASTER RECOVERY AS A SERVICE* (DRAAS)

#### 3.1 Introducción

En cualquier momento los Sistemas de Información de la institución pueden quedar afectados de manera total o parcialmente a consecuencia de un siniestro fortuito. Si las operaciones más importantes de la Cooperativa de Ahorro y Crédito “Alianza del Valle”, se suspendieran repentinamente, como consecuencia de ello nacen preguntas ¿Cómo se afectaría el negocio?, ¿Cómo quedaría afectada la imagen institucional?, ¿Cuánto tiempo aguantaría la Cooperativa, sin acceder a la información crucial para el negocio?, ¿En cuánto tiempo estarían disponibles las aplicaciones que proporcionan esa información en volver a estar disponibles? Todas estas interrogantes hacen pensar en estar preparados para riesgos de impacto.

En el presente capítulo, se presenta la primera parte adaptada de la estrategia para la migración a la nube, recomendado por *CloudTweaks* (2011), donde se detalla:

- Diagnostico Preliminar
  - Procesos críticos,
  - Requerimientos para el funcionamiento actual,
  - Plan de recuperación.
- Evaluación de Negocios y de las Aplicaciones
  - Aplicaciones de Alta criticidad,
  - Capacidad de Procesos de la Continuidad de Negocio.
- Conocimiento de los Riesgos
  - Amenazas a considerar para la migración.

### 3.2 Conocimiento de los Procesos Críticos

A continuación, se detallarán los procesos y subprocesos críticos de la cooperativa “Alianza del Valle”, que han sido categorizados de acuerdo a rentabilidad, continuidad del negocio, satisfacción socio/cliente y objetivos institucionales dándoles una categorización de 1-Bajo, 2-Medio Bajo, 3- Medio, 4- Medio Alto, 5-Alto.

La siguiente tabla es un resumen de los procesos críticos del Inventario de procesos de la Cooperativa como se puede apreciar en el (Anexo 2): Inventario de Procesos Críticos y no Críticos.

Tabla 4. Procesos Críticos de la institución

TIPO DE PROCESO	MACRO-PROCESO	PROCESO		SUBPROCESO		CRÍTICO / NO CRÍTICO	PROCEDIMIENTO	
		CÓDIGO	NOMBRE	CÓDIGO	NOMBRE		CÓDIGO	NOMBRE
ESTRATÉGICOS	GIN - Gestión Institucional	GIN-02	Prevención y Control de Lavado de Activos	GIN-02-01	Prevención y Control de Lavado de Activos	Crítico	GIN-02-01-01	Revisión de Transacciones de cada Cliente/Cuenta de Ahorros (Semanal)
							GIN-02-01-02	Revisión de Transacciones de cada Cliente/Concesión de Créditos (Semanal)
							GIN-02-01-03	Revisión de Transacciones por cada Cliente de Depósitos a Plazo Fijo (Mensual)
							GIN-02-01-04	Monitoreo de Transacciones de Ahorros, Crédito e Inversiones (Mensual)
							GIN-02-01-05	Revisión Aperturas de Cuentas de Ahorros

--

--	--

--	--

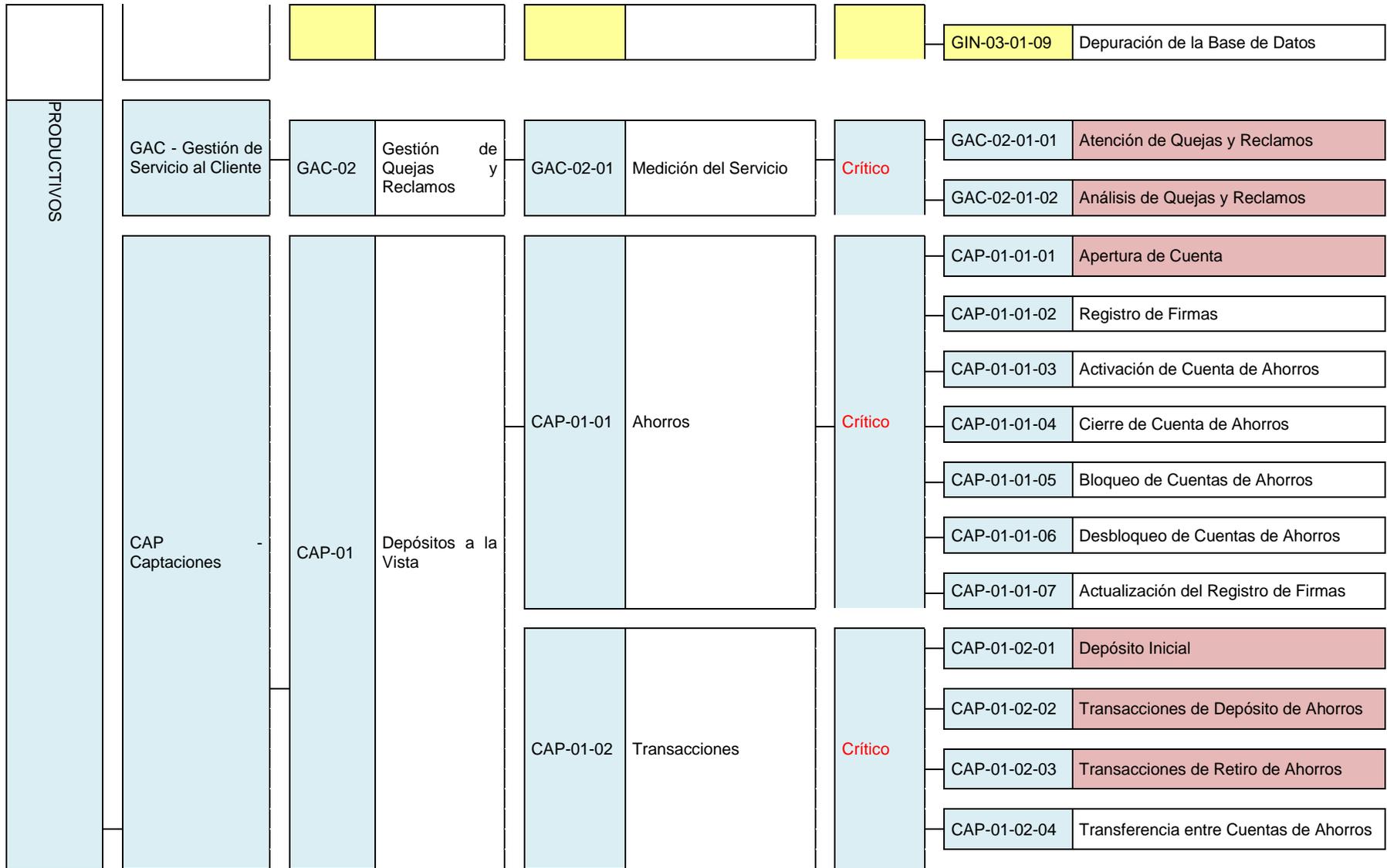
GIN-03	Administración de Accesos al Sistema Cobis
--------	--

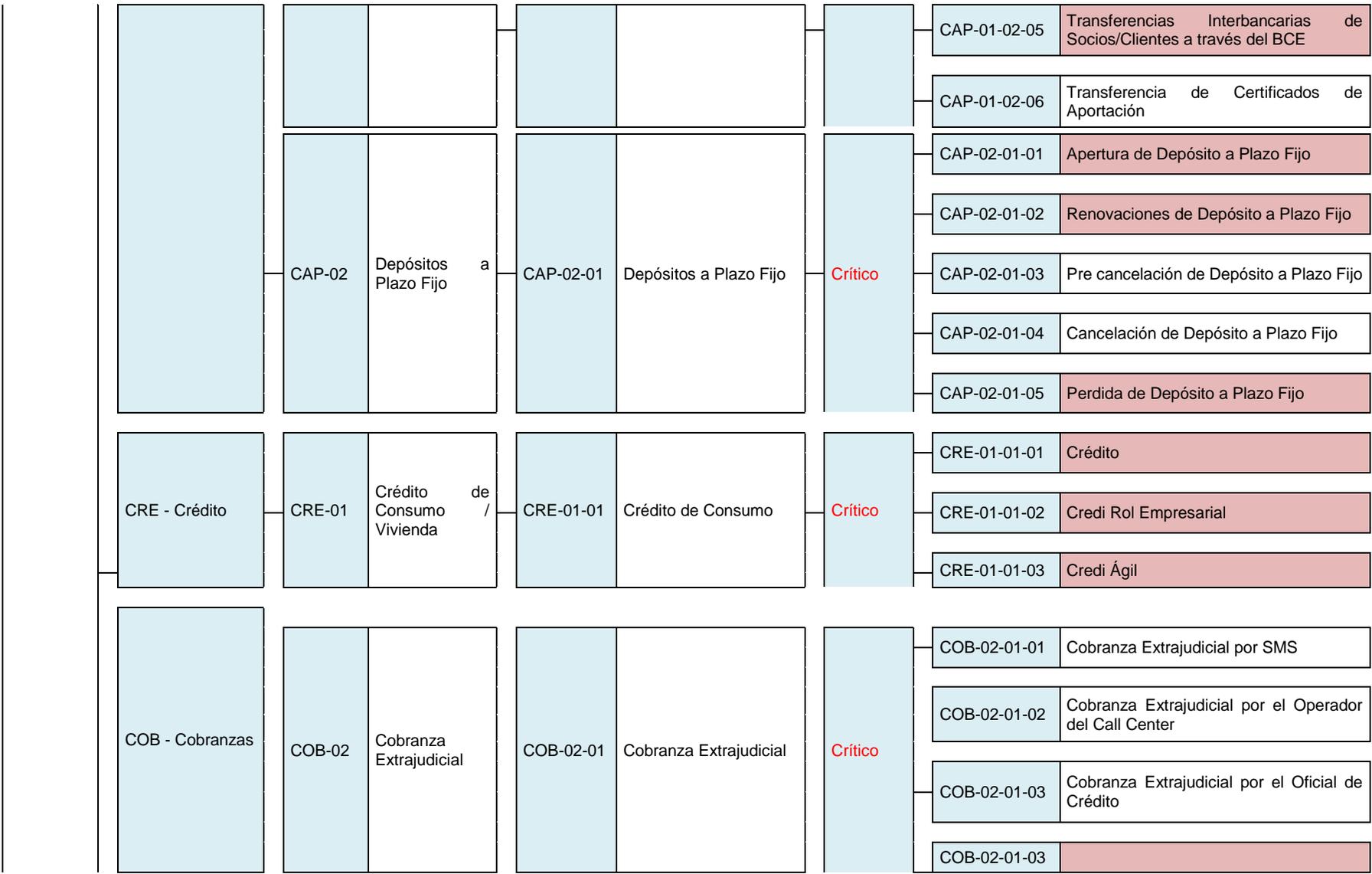
GIN-03-01	Administración de Accesos al Sistema Cobis y Programas Aplicativos
-----------	--

--

Crítico
---------

GIN-02-01-06	Monitoreo de Transacciones no Sujetas a Reporte
GIN-02-01-07	Capacitación sobre la Prevención de Lavado de Activos
GIN-02-01-08	Capacitación al Personal Nuevo sobre la Prevención del Lavado de Activos
GIN-02-01-09	Monitoreo de Transacciones Wester Union
GIN-02-01-10	Validación de la Base de Información Reservada
GIN-03-01-01	Acceso a Nuevos Usuarios
GIN-03-01-02	Actualización de Accesos por Transferencia de Empleados o Cambio de Cargos
GIN-03-01-03	Accesos Temporales
GIN-03-01-04	Bloqueos Temporales
GIN-03-01-05	Desbloqueo de Acceso al Sistema
GIN-03-01-06	Activación de Usuario
GIN-03-01-07	Eliminación de Accesos
GIN-03-01-08	Creación de Roles







### 3.3 Revisión de los requerimientos de la empresa para su funcionamiento

Se detallará a continuación los aspectos concernientes al departamento de tecnología e infraestructura tecnológica de la cooperativa para determinar los requerimientos necesarios para su correcto funcionamiento, además se tomará en cuenta las necesidades existentes en el departamento de tecnología.

#### 3.3.1 Disponibilidad de recursos y servicios.

- Gestión de red LAN

La gestión de la infraestructura de la red LAN la realiza el departamento de tecnología de la cooperativa, quien ha definido que la red LAN debe mantenerse operativa 24 horas durante los 7 días de la semana, con monitoreo en sitio de 7:30 am a 5:00 pm, y monitoreo remoto mediante VPN.

- Internet

Los proveedores de internet son, New Access que asegura 99.96% de disponibilidad con un ancho de banda de 5MB 1:1, como enlace secundario (Backup) y Telconet con 10 MB 1:1, con disponibilidad de 99.98% como enlace primario, para la matriz y sitio alterno.

- Datos

Tabla 5. Enlace de Datos

ENLACE DE DATOS		
AGENCIAS	PROVEEDORES	
	TELCONET	NEW ACCES
Inca	5 Mbps	2 Mbps
Chillogallo	2 Mbps	2 Mbps
Sangolquí	2 Mbps	2 Mbps
Amaguaña	2 Mbps	2 Mbps
Machachi	2 Mbps	2 Mbps
Conocoto	2 Mbps	2 Mbps
Guamaní	2 Mbps	2 Mbps
Colón	4 Mbps	2 Mbps
Tumbaco	2 Mbps	2 Mbps
Bicentenario	2 Mbps	2 Mbps

### 3.3.2 Infraestructura.

La infraestructura de red de la cooperativa se encuentra ubicada en un centro de datos, ubicado en un espacio central de las oficinas, en matriz, en este centro de datos se encuentran los equipos de conectividad, así como también los servidores de la cooperativa.

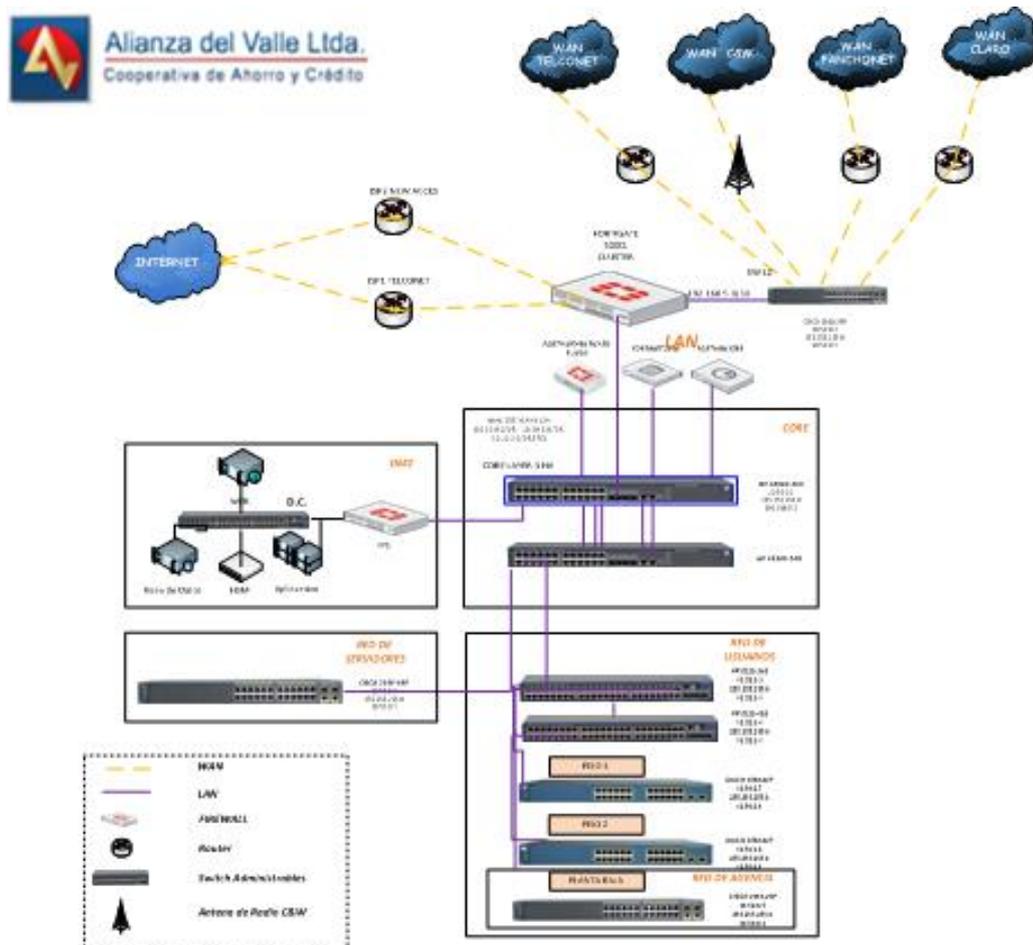


Figura 12. Esquema de Red Lan

Tomado de (Alianza del Valle, 2015)

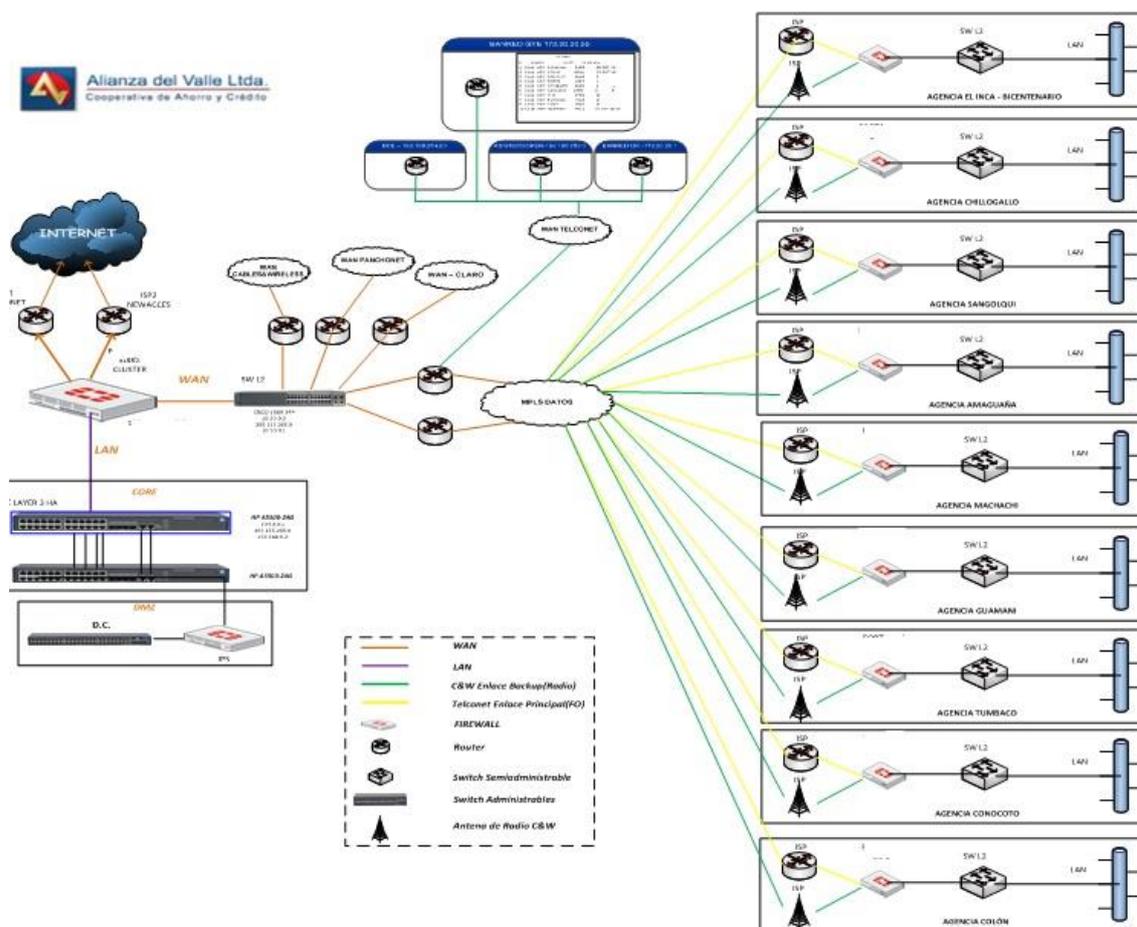


Figura 13. Red Wan

Tomado de (Alianza del Valle, 2015)

### 3.3.2.1 Inventario de Servidores:

Tabla 6. Inventario Servidores

TIPO	MARCA	DETALLE/NOMBRE	LOCACIÓN
Servidor Central	Fujitsu sparck M3000	Producción	Matriz
Servidor Central	Sun M4000	STAND BY(Réplica)	Inca
Servidor Central	Sun fire v240	Replicación	Matriz
Servidor Central	Sun fire v490	Desarrollo	Matriz
Storage	EMC Vnx 5000	Producción	Matriz
Servidor de aplicación	Hp bl460c gen 8	Virtual (red lan, cajeros automáticos, sitios web)	Matriz

Se detallará a continuación las especificaciones técnicas del servidor principal y secundario donde corre el Core de la cooperativa COBIS, además de su servidor de almacenamiento.

#### Servidor Principal - Sistema Core

- Marca Fujitsu sparck-enterprise M300/rack
- Memoria de RAM 32768 MB
- 7 Procesadores de 2.750 MHZ
- 2 Discos de 300 GB, Raid 1(40% utilizado)
- Versión del sistema Solaris 10
- Software instalado Cobis v.3.3(32 bits)
- Base de Datos Sybase 15.03

#### Servidor Secundario (Stand By) - Sistema Core

- Marca Spark Enterprise
- Memoria de RAM 16384 MB
- 4 Procesadores de 2.150 MHZ
- 2 Discos de 147 GB, Raid 1(70% utilizado)
- Versión del sistema Solaris 10
- Software instalado Cobis v.3.3 (32 bits)
- Base de Datos Sybase 15.03

#### Servidor de Almacenamiento – Sistema Core

- Marca STORAGE EMC VNX 5000
- 3 Discos de 1Tb, Raid 5 (70% utilizado)
- Memoria RAM 16 Gb

A continuación, se detallará las especificaciones técnicas del servidor blade para virtualización.

- Marca Hp
- Modelo BL460c Gen 8

- Dos procesadores Intel Xeon E5-2640 v2 de 2.0GHz/8-core, 20 MB cache
- 64 GB de memoria RAM tipo PC3- 12800R
- Dos puertos de red HP Flex Fabric 10 Gb
- Mezzanine card con 4 puertos Gigabit
- Software de virtualización VMWARE VSphere ver 5.5
- Almacenamiento SAN de 12 TB de capacidad en RAW

### **3.3.3 Escalabilidad**

El modelo de negocio tecnológico de la cooperativa de ahorro y crédito “Alianza del Valle”, está directamente relacionado con el número de transacciones que se realizan, ya sea por depósitos, créditos o retiros. Si existe el crecimiento en el número de socios, y en el número de transacciones, la cooperativa necesita nuevos recursos computacionales, así como también la seguridad de la administración de los datos que estos generan.

El almacenamiento de los datos del sistema core se encuentra en un 70% utilizado, y se ha estimado un crecimiento de un 20% anual en el volumen de información.

Por lo antes mencionado, se proyecta que la flexibilidad que ofrece la tecnología de la Computación en la Nube, puede ser de gran utilidad para el crecimiento de Alianza del Valle.

### **3.3.4 Sitio Alternativo**

El sitio alternativo se instauró por seguridad y disponibilidad de la información de los socios/clientes en caso de alguna eventualidad, y así pueda seguir operando la Cooperativa con sus principales operaciones como depósitos, retiros, pagos de préstamos, plazos fijos y desembolso de préstamos.

Por cumplimiento de la resolución de riesgo operativo de la Superintendencia de Economía Popular y Solidaria, las instituciones controladas deben implementar planes de contingencia y continuidad, a fin de garantizar su capacidad de operar

en forma continua y minimizar las pérdidas en caso de interrupción severa del negocio (SEPS, 2014).

Actualmente el sitio alternativo se encuentra en la agencia el Inca, donde funciona únicamente para depósito por ventanilla, por el momento, no se puede realizar retiros de dinero por asistencia personalizada, ya que se encuentra implementado reconocimiento por huella para realizar retiros, y este debe ser desactivado para que funcione.

Las transacciones por cajero o por página web están igualmente deshabilitadas, ya que el servidor donde se encuentra instalado el Core Cobis, no cuenta con las capacidades necesarias para instalar todas las aplicaciones críticas que se detallará en el siguiente punto, es por esto que se busca implementar DRaaS, para poder solventar estas fallas en la capacidad de la cooperativa para recuperar sus servicios principales ante una eventualidad, que pudiera perjudicar la atención del cliente viéndose afectada la imagen de la cooperativa.

Este proceso no es imperceptible para el personal de IT, y menos para el cliente/socio, ya que se deben seguir varios procedimientos, tanto técnicos como operativos, asignados a personal especializado, que está normado en un instructivo de procedimientos. Para esto se necesita personal externo e interno.

### **3.4 Situación actual de su DRP**

Es necesario conocer la capacidad con la que cuenta la organización para restablecer su infraestructura tecnológica y de esta manera asegurar la continuidad del negocio, en caso de que ocurran graves incidentes. Es por esto que se han tomado los puntos más relevantes del plan de recuperación ante desastres de la Cooperativa “Alianza del Valle”, para ayudar en el diagnóstico inicial para el estudio de factibilidad propuesto.

#### **3.4.1 Objetivo del Plan de Contingencia de Alianza del Valle**

Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.

### 3.4.2 Análisis de los riesgos y problemas de continuidad

Dentro del plan de recuperación ante desastres es importante obtener una valoración del riesgo, y para esto es necesario entender los riesgos implicados en el funcionamiento de las operaciones de la institución y por sobre todo el tiempo máximo de caída que puede tolerar cada una de ellas.

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas, y las amenazas más comunes se dan como se indica en la siguiente figura.



Figura 14. Amenazas para la seguridad

Tomado de (Alianza del Valle, 2015)

A continuación, se detallan los principales problemas y las consecuencias que se plantea el departamento de IT de la Cooperativa de Ahorro y Crédito “Alianza del Valle” al surgir un incidente fortuito dentro de su plan de recuperación ante desastres.

Tabla 7. Problemas y Consecuencias Depto. IT

	Problemas	Consecuencias
<b>Procesos</b>	<ul style="list-style-type: none"> <li>• Cuáles procesos fueron afectados y cuáles son las consecuencias.</li> <li>• Donde más se ejecutan los procesos de negocio.</li> <li>• ¿Cuál será la reacción de los clientes y del público?</li> </ul>	<ul style="list-style-type: none"> <li>• Los procesos que pueden continuar dependerán de las decisiones de los empleados, con acceso incompleto a los sistemas, datos, clientes y falta de control.</li> <li>• Los procesos de negocio de la otra ubicación se suspenden.</li> <li>• Los productos y servicios no pueden ser posicionados sin aplicaciones.</li> </ul>
<b>Tecnología</b>	<ul style="list-style-type: none"> <li>• ¿Qué datos se perderán?</li> <li>• ¿Cuánto tiempo tomará esto?</li> <li>• Los empleados/ clientes tienen acceso a los datos?</li> <li>• ¿Cómo re-estableceremos el servicio de conectividad de datos al sitio alternativo?</li> <li>• ¿Cómo nos reconectaremos a los procesos de negocio?</li> </ul>	<ul style="list-style-type: none"> <li>• La cantidad de datos perdidos no se pueden determinar.</li> <li>• La infraestructura tecnológica no está disponible para esta ubicación incluyendo aplicaciones únicas y críticas.</li> <li>• La interrupción brusca resulta en pérdida o corrupción de datos y transacciones incompletas.</li> <li>• La conectividad y las redes no están disponibles</li> </ul>

Tomado de (Alianza del Valle, 2015)

### 3.4.3 Identificación de Riesgos

Los riesgos a continuación detallados, han sido tomados del plan de recuperación ante desastres de la Cooperativa de Ahorro y Crédito “Alianza del Valle”, basados en los estándares internacionales ISO 31000 e ISO 27005.

Tabla 8. Riesgos Identificados

No.	Riesgo	Impacto
R-01	Daño del motor de base de datos Sybase	A+
R-02	Corrupción de las bases de datos de usuario	A+
R-03	Daño total del servidor central	A+
R-04	Daño parcial del servidor central	A+
R-05	Daño del sistema de almacenamiento externo	A+
R-06	Interrupción en las comunicaciones	A+
R-07	Fuego en la sala de servidores	A+
R-08	Daños en segmentos de Red Local	M
R-09	Incendios	A+
R-10	Terremotos	A+
R-11	Daños de Backups de Datos y Aplicaciones	A
R-12	Siniestros Naturales	A
R-13	Dependencia del Proveedor	A
R-14	Errores no permitidos por usuarios internos	M

A=Alto M=Mediano B=Bajo Muy Alto=A+

Tomado de (Alianza del Valle, 2015)

La identificación de los riesgos y la valoración del impacto de los mismos fueron analizados por el comité de tecnología, previa elaboración del plan de recuperación ante desastres de la Cooperativa.

### 3.4.3.1 Identificación de componentes de cada recurso que deben ser restaurados completamente bajo posibles contingencias.

Tabla 9. Acciones Finales para riesgos encontrados

No.	Recurso	Componentes	Acciones
R-01	SERVIDORES	Sistema Operativo	Reinstalación
		Base de Datos	Reinstalación
		Software de Back-End	Reinstalación
		Discos Duros	Cambio
		Tarjeta de Red	Cambio
R-02	ESTACIONES	Sistema Operativo	Reinstalación
		Software de Front-End	Reinstalación
		Discos Duro	Cambio
		Tarjeta de Red	Cambio
		MODEM	Cambio
R-03	BACK-END	Base de Datos	Reinstalación
		Módulo Administrativo	Reinstalación
		Módulo de Oferta	Reinstalación
		Módulo de Demanda	Reinstalación
		Módulo de Reporto	Reinstalación
		Módulo de Cajeros	Reinstalación
		Impresión Remota	Reinstalación
		Módulo de Mensajería	Reinstalación
R-04	FRONT-END	Módulo de Consultas	Reinstalación
		Módulo Administrativo	Reinstalación
		Módulo de Oferta	Reinstalación
		Módulo de Demanda	Reinstalación
		Módulo de Reporto	Reinstalación
		Módulo de Cajeros	Reinstalación
		Impresión Remota	Reinstalación
		Módulo de Mensajería	Reinstalación
R-05	RED LAN	Módulo de Consultas	Reinstalación
		Cables	Instalación
		Conectores	Instalación
		Puntos de Red	Instalación

R-06	RED WAN	Canales de	Soporte
		Comunicación	Soporte
R-07	EQUIPO DE COMUNICACIONES	Ruteadores Centrales	Reinstalación
		Ruteadores Remotos	Reinstalación
		Access Server	Soporte
		Módems Remotos	Cambio
R-08	EQUIPOS DE RED	Switches	Soporte
		Hubs	Cambio
		Tarjetas de Red	Cambio
R-09	EQUIPOS DE SEGURIDAD	Router/Firewall	Cambio
		Firewall	Cambio
R-10	ENERGÍA ELÉCTRICA	Energía Pública	Notificación
		Generador de Energía	Soporte
		UPS	Soporte

Tomado de (Alianza del Valle, 2015)

Las acciones finales detalladas en la tabla anterior, son planteadas por el departamento de IT en su plan de recuperación ante desastres

### 3.4.3.2 Tiempo máximo permitido para la recuperación.

Tabla 10. Tiempo máximo de interrupción

No.	Recursos	Frecuencia de Uso	Tiempo máximo de interrupción
R-01	SERVIDORES	Cada día	4 horas
R-02	ESTACIONES	Cada día	1 hora
R-03	BACK-END	Cada día	10 minutos
R-04	FRONT-END	Cada día	10 minutos
R-05	RED LAN	Cada día	1 hora
R-06	RED WAN	Cada día	2 horas
R-07	EQUIPO DE COMUNICACIONES	Cada día	2 horas
R-09	EQUIPOS DE SEGURIDAD	Cada día	0
R-10	ENERGÍA ELÉCTRICA	Cada Día	10 minutos

Adaptado de (Alianza del Valle, 2015)

En base al cuadro anterior y a los riesgos identificados en la tabla 8, el departamento de IT de la Cooperativa de Ahorro y Crédito “Alianza del Valle”, ha determinado la probabilidad de ocurrencia de los riesgos con alta criticidad, que son los siguientes:

Tabla 11. Riesgos de Alta criticidad de Alianza del Valle

CONTINGENCIA	PERSONAS	TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)	PUNTO OBJETIVO DE RECUPERACIÓN (RPO)	PROCESO AFECTADO	TECNOLOGÍA	PROBABILIDAD DE OCURRENCIA
<b>DAÑO DEL MOTOR DE BASE DE DATOS SYBASE</b>	Técnicos Coop. De BDD, y empresa Uniplex, Personal Admin	2 Días	24 horas	Estratégicos , Gestión institucional, Adm. Información, Contable, no atención de operaciones.	Bases de Usuario y del sistema	<b>Baja:</b> 1 vez cada 10 años
<b>CORRUPCIÓN DE LAS BASES DE DATOS DE USUARIO</b>	Técnicos Coop. De BDD, y empresa SINETCOM , Personal Admin	1 Día	24 horas	Estratégicos , Gestión institucional, Adm. Información, Contable, no atención de operaciones.	Bases de Usuario.	<b>Media:</b> 2 veces en 10 años
<b>Daño total del servidor central</b>	Técnicos Coop. De BDD, y empresa SINETCOM , Personal Admin	2 Días	30 días, o tras su última actualización	Estratégicos , Gestión institucional, Adm. Información, Contable, no atención de operaciones.	Servidor de BDD, físicamente	<b>Baja:</b> 1 vez cada 10 años
<b>Daño parcial del servidor central</b>	Técnicos Coop., y empresa SINETCOM .	4 Horas	31 días, o tras su última actualización	Estratégicos , Gestión institucional, Adm. Información, Contable, no atención de operaciones.	Aislamiento del elemento dañado, reemplazarlo con otro.	<b>Baja:</b> 1 vez cada 10 años
<b>Daño del sistema de almacenamiento o externo</b>	Técnicos Coop., empresa SINETCOM , y UNIPLEX.	3 Horas	12 horas	Estratégicos , Gestión institucional, Adm. Información, Contable, no atención de operaciones.	Bases de Usuario y del sistema	<b>Media:</b> 2 veces en 10 años
<b>Interrupción en las comunicaciones</b>	Técnicos Coop., empresa Telconet, y empresa cable & Wireless	10 minutos	no aplica	Estratégicos , Gestión institucional, Adm. Información, Contable, no atención de operaciones.	Aplicación de sistema alternativo de comunicaciones	<b>Media:</b> 2 veces en 10 años

<b>Fuego en la sala de servidores</b>	Técnicos Coop. De BDD, empresa Uniplex, SINETCOM, Telconet y Personal Admin	3 Días	se toma la información anterior	Estratégicos, Gestión institucional, Adm. Información, Contable, no atención de operaciones.	Pérdida total del hardware, conexión al sitio alterno	<b>Baja:</b> 1 vez cada 10 años
---------------------------------------	---	--------	---------------------------------	--	---	---------------------------------

Tomado de (Alianza del Valle, 2015)

### 3.5 Aplicaciones de alta criticidad.

Es importante dimensionar lo que la organización desea de la migración a la nube. Por ende, es importante identificar cuales servicios o aplicaciones son candidatos a migrar según su criticidad. Por esta razón, se propone la siguiente categorización de las aplicaciones de la cooperativa.

La categorización de las aplicaciones se realizó en conjunto con el departamento de Sistemas y Gerencia General, mediante un mapeo entre el inventario de aplicaciones de la cooperativa y los procesos críticos de la institución.

Tabla 12. Aplicaciones categorizadas por su criticidad

MACRO PROCESO	ACTIVO	TIPO	DESCRIPCIÓN	CRITICIDAD
<b>Desarrollo Área de TI</b>				
GFI- Gestión Financiera	Administración RecaudaFácil	Web Form	Permite administrar y parametrizar la aplicación RecaudaFácil	Media
GFI- Gestión Financiera	Conocimiento socio/cliente	Web Form	Permite Gestionar la Información del Socio/Cliente.	Alta
GIT - Gestión de Informática y Tecnología	Help Usuarios.	Web Form	Permite Gestionar las credenciales de los usuarios para las aplicaciones satélites	Media
GIT - Gestión de Informática y Tecnología	Sisvoz	Windows Form	Permite realizar llamadas automáticas por Gestión de cobranzas	Alta
GFI- Gestión Financiera	Navidad	Windows Form	Permite Controlar la entrega de navidad.	Baja
GFI- Gestión Financiera	Datos Focus financiero	Web Form	Extrae información para indicadores financieros.	Media
GFI- Gestión Financiera	RecaudaFácil	Windows Form	Gestiona el Cobro de pensiones y otros conceptos, para Instituciones Educativas y Asociaciones	Alta
GRI - Gestión de Riesgos	Riesgos de mercado y liquidez	Windows Form	Gestiona la información para los reportes de	Alta

			Riesgos de mercado y liquidez	
GAD - Gestión Administrativa	Suministros	Windows Form	Permite Controlar el inventario de suministros de oficina y limpieza	Media
GAD - Gestión Administrativa	Votación	Windows Form	Permite gestionar el proceso de votaciones para delegados al Consejo de Administración de la Coop	Baja
GAC - Gestión de Servicio al Cliente	Rifa promoción	Windows Form	Sorteo de rifa.	Baja
GIT - Gestión de Informática y Tecnología	Gestión Página Transaccional	Web Form	Permite Gestionar las credenciales de los usuarios, permisos y roles, para la página web transaccional.	Crítica
CRE - Crédito	Interfaz credireporte.	Servicio Web	Gestiona el análisis crediticio de los clientes evaluados por el scoring.	Alta
GFI- Gestión Financiera	Inversiones pasivas	Web Form	Gestiona la información de inversiones pasivas.	Alta
GIN - Gestión Institucional	Lavado de Activos	Web Form	Control de lavado de activos mediante el sistema Cobis	Crítica
GIT - Gestión de Informática y Tecnología	Servicio para Cajeros automáticos	Servicio Web	Gestiona la transaccionalidad de Cajeros entre la coop. y banred.	Crítica
GFI- Gestión Financiera	Sismma	Web Form	Permite dar seguimiento a la Gestión de cobranzas.	Crítica
GIT - Gestión de Informática y Tecnología	SMS	Servicio Web	Permite interactuar con las diferentes aplicaciones en el envío de SMS a través de la empresa MSPLUS	Crítica
GIT - Gestión de Informática y Tecnología	Software de Mensajería	Web Form	Permite administrar, parametrizar los SMS, Controla el envío de SMS Masivos por Gestión de cobranzas, transacciones por cajero automático, transacciones por página web como transferencias y pagos de servicios.	Crítica
GRH - Gestión de Recursos Humanos	Talento Humano	Web Form	Permite administrar y parametrizar la aplicación de Recursos humanos.	Media
GFI- Gestión Financiera	Página web Transaccional	Web Form	Permite verificar los saldos de todos los servicios financieros, Transferencias Internas y	Crítica

			Externas, Pago de Servicios	
GIT - Gestión de Informática y Tecnología	Página web Transaccional	Web service	servicios web de la página transaccional.	Crítica
<b>SOFTWARE DE TERCEROS</b>				
GFI- Gestión Financiera	Cardcontroller	Switch Transaccional	Gestiona la administración de las tarjetas de débito.	Crítica
GFI- Gestión Financiera	Cardcontroller	base de datos	Gestiona la administración de las tarjetas de débito.	Crítica
GIT - Gestión de Informática y Tecnología	Correo Electrónico		Lotus	Alta
GFI- Gestión Financiera	Pago directo/Bono	Switch Transaccional	Gestiona la transaccionalidad entre la Coop y Banred	Alta
GFI- Gestión Financiera	Servicios de Banred	RichClient	Servicios de bono, cajeros automáticos, ventanilla compartida y transferencia.	Crítica
GIT - Gestión de Informática y Tecnología	Aplicación WAP transaccional	Wap	consultas, transferencias de dinero a través del teléfono.	Alta
GAD - Gestión Administrativa	Planificación estratégica	Web Form	Software para control del plan estratégico.	Media
GIN - Gestión Institucional	Bussinesintelligence	Web Form	Reporte de información gerencial y para análisis.	Crítica
GIN - Gestión Institucional	COBIS	Windows Form	Core bancario, sistemas principales para la transaccionalidad de sus socios/clientes.	Crítica
GFI- Gestión Financiera	WorkFlow	Web Form	Workflow de créditos y ahorros.	Crítica
GFI- Gestión Financiera	Activos Fijos	Web Form	activos fijos	Baja
GAD - Gestión Administrativa	Reloj Biométrico	Windows Form	Almacenamiento del timbre de entrada y salida de los empleados	Media
GIT - Gestión de Informática y Tecnología	Servidor de huella	Aplicación	servidor de huella principal	Crítica
GIT - Gestión de Informática y Tecnología	Servidor de huella	Aplicación	servidor de huella secundario	Crítica
GIT - Gestión de Informática y Tecnología	Monitoreo de base Sybase	Aplicación	monitoreo de base de datos	Media
GIT - Gestión de Informática y Tecnología	Página web informativa	Web Form	Página web informativa	Crítica

GFI- Gestión Financiera	Facilito	Switch Transaccional	Server para pago de impuestos	Media
-------------------------	----------	----------------------	-------------------------------	-------

Adaptado de (Alianza del Valle, 2015)

### 3.5.1 Priorización de las aplicaciones.

En la tabla 13 se detalla las aplicaciones críticas de la cooperativa que han sido categorizados por su prioridad de acuerdo a la clasificación anterior. La escala utilizada para determinar la prioridad de cada aplicación se encuentra descrita en la tabla 14.

Tabla 13. Priorización de aplicaciones

ACTIVO	DESCRIPCIÓN	Críticidad	TIPO	PRIORIDAD
Desarrollo Área de TI				
Gestión Página Transaccional	Permite Gestionar las credenciales de los usuarios, permisos y roles, para la página web transaccional.	Crítica	Virtual	2
Lavado de Activos	Control de lavado de activos mediante el sistema Cobis	Crítica	Virtual	1
Servicio para Cajeros automáticos	Gestiona la transaccionalidad de Cajeros entre la coop. y banred.	Crítica	Virtual	2
Sismma	Permite dar seguimiento a la Gestión de cobranzas.	Crítica	Virtual	2
SMS	Permite interactuar con las diferentes aplicaciones en el envío de SMS a través de la empresa MSPLUS	Crítica	Virtual	3
Software de Mensajería	Permite administrar, parametrizar los SMS, Controla el envío de SMS Masivos por Gestión de cobranzas, transacciones por cajero automático, transacciones por página web como transferencias y pagos de servicios.	Crítica	Virtual	3
Mensajería masiva	envío automático de SMS	Crítica	Virtual	3
Página web Transaccional	Permite verificar los saldos de todos los servicios financieros, Transferencias Internas y Externas, Pago de Servicios	Crítica	Virtual	2
<b>SOFTWARE DE TERCEROS</b>				
Cardcontroller	Gestiona la administración de las tarjetas de débito.	Crítica	Virtual	2
Servicios de Banred	Servicios de bono, cajeros automáticos, ventanilla compartida y transferencia.	Crítica	Físico	2

Bussinesintelligence	Reporte de información gerencial y para análisis.	Crítica	Virtual	3
COBIS	Core bancario, sistemas principales para la transaccionalidad de sus socios/clientes.	Crítica	Físico	1
WorkFlow	Workflow de créditos y ahorros.	Crítica	Virtual	3
Servidor de huella	servidor de huella principal	Crítica	Virtual	2
Servidor de huella	servidor de huella secundario	Crítica	Virtual	2

Tabla 14. Referencia priorización de aplicaciones

PRIORIDAD	DEFINICIÓN
1	Impacto directo con la continuidad del negocio ya que afecta al Core del negocio.
2	Aplicaciones que van de la mano, con el Core de negocio.
3	Aplicaciones críticas, pero sin su funcionamiento no afecta directamente al funcionamiento de la cooperativa

### 3.5.2 Aplicaciones implementadas en el sitio alternativo.

El siguiente cuadro, explica brevemente qué aplicaciones han sido implementadas en el sitio alternativo, y cuáles necesitan ser implementadas por su alto grado de criticidad.

Tabla 15. Aplicaciones en sitio alternativo

ACTIVO	Criticidad	PRIORIDAD	SITIO ALTERNO
Desarrollo Área de TI			
Gestión Página Transaccional	Crítica	2	No implementada
Lavado de Activos	Crítica	1	No implementada
Servicio para Cajeros automáticos	Crítica	2	No implementada
Sismma	Crítica	2	No implementada

SMS	Crítica	3	No implementada
Software de Mensajería	Crítica	3	No implementada
Mensajería masiva	Crítica	3	No implementada
Página web Transaccional	Crítica	2	No implementada
<b>SOFTWARE DE TERCEROS</b>			
Cardcontroller	Crítica	2	No implementada
Servicios de Banred	Crítica	2	No implementada
Bussinesintelligence	Crítica	3	No implementada
COBIS	Crítica	1	Implementada
WorkFlow	Crítica	3	No implementada
Servidor de huella	Crítica	2	No implementada
Página web informativa	Crítica	3	No implementada

### 3.6 Capacidad de Procesos de la Continuidad de Negocio

El medir la capacidad de los procesos de continuidad de negocio, es una herramienta que se utilizó para conocer el estado en que se encuentra la cooperativa en términos de nivel de preparación para afrontar y recuperar sus operaciones críticas.

A continuación, en la Tabla 16 se presenta la evaluación de nivel 1 de la capacidad de los procesos de continuidad de negocio, como objetivo planteado por la Cooperativa “Alianza del Valle”; esta fue evaluada en conjunto con el departamento de Sistemas, Riesgos y Gerencia General; la evaluación completa se puede visualizar en (Anexo 3: Evaluación de Procesos).

Tabla 16. Metas, Prácticas clave y productos de trabajo de los procesos

Metas del proceso	Rating de evaluación de metas del proceso	Prácticas clave	Descripción de las Actividades	Rating de evaluación de prácticas clave	Productos (salidas)	Rating de evaluación de productos
<b>Dominio: DSS04 Entregar Servicio y Soporte</b>						
<b>Gestionar la continuidad</b>	<b>62</b>			<b>79,75</b>		<b>80,375</b>
1. La información crítica para el negocio está disponible para el negocio en línea con los niveles de servicio mínimos requeridos.	20	DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance.	Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.	70	- Política y objetivos de continuidad de negocio - Escenarios de incidentes que causan una interrupción - Valoraciones de las capacidades actuales y lagunas de continuidad	70
2. Los servicios críticos tienen suficiente resiliencia.	60	DSS04.02 Mantener una estrategia de continuidad.	Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa	85	- Análisis de impacto en el negocio - Requerimientos de continuidad - Opciones estratégicas aprobadas	90

3. Las pruebas de continuidad del servicio han verificado la efectividad del plan.	75	DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas	80	- Acciones y comunicaciones de respuesta a incidentes - Plan de Continuidad de Negocio (BCP)	85
4. Un plan de continuidad actualizado refleja los requisitos de negocio actuales.	75	DSS04.04 Ejercitar, probar y revisar el plan de continuidad.	Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.	75	- Pruebas de objetivos - Pruebas de ejercicios - Pruebas de resultados y recomendaciones	75
5. Las partes interesadas internas y externas han sido formadas en el plan de continuidad.	80	DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.	75	- Resultados de las revisiones de los planes - Cambios recomendados a los planes	75
		DSS04.06 Proporcionar formación en el plan de continuidad.	Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.	75	- Requerimientos de formación - Resultados de la supervisión de habilidades y competencias	75
		DSS04.07 Gestionar acuerdos de respaldo.	Mantener la disponibilidad de la información crítica del negocio.	98	Probar los resultados de las copias de seguridad de los datos	98

		DSS04.08 Ejecutar revisiones post reanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.	80	- Informe de revisión postreanudación - Cambios aprobados a los planes	75
--	--	--	--	----	---	----

Adaptado de (Coronel Katalina, 2016)

Para evaluar la tabla anterior se utilizó las escalas y ratios de la ISO/IEC 15504 para asignar un ratio para el grado en el que cada objetivo es alcanzado. Esta escala consiste en las siguientes ratios:

Tabla 17. Ratio de la ISO/IEC 15504

N (No Alcanzado)	P (Parcialmente Alcanzado)	L (Ampliamente Alcanzado)	F (Completamente Alcanzado)
0 - 15	16 – 50	51 - 85	86 - 100

Como se puede apreciar de los resultados obtenidos, es notorio que la cooperativa logra cumplir sus metas de continuidad de negocio en un ratio de (51 – 85), aunque posee algunas debilidades, que deberán ser solventadas, para la migración a la nube.

### 3.7 Amenazas a considerar para la migración.

Para identificar y valorar las amenazas se realizó la siguiente encuesta en conjunto con el Departamento de Sistemas, Auditoría Interna y Gerencia General, donde se valoró las posibles amenazas que pueden generar riesgos en la adopción de DRaaS basado en el modelo de Nube en una escala de importancia e impacto.

Las amenazas fueron tomadas de INTECO-CERT (2011), quienes los han recopilado de diferentes fuentes como Gartner, NIST y CSA.

Tabla 18. Amenazas de migración a la nube

ID	Tipo	Amenazas	BAJO	MEDIO	ALTO	MUY ALTO
R1	Organizacional	Pérdida de control y de gobernabilidad sobre los recursos (control físico y de gestión).				X
R2	Organizacional	Pérdida de experiencia en TI, es decir falta de experiencia local y pérdida de conocimiento al largo plazo.		X		
R3	Organizacional	Reducción de la productividad del personal de apoyo durante la migración (menor satisfacción en el trabajo) e incertidumbre laboral.			X	
R4	Organizacional	La gestión de un sistema en la nube puede tomar un esfuerzo de gestión adicional, gestión de la relación con los proveedores de DRaaS.			X	
R5	Organizacional	Pérdida de reputación del negocio debido a actividades malintencionadas de terceros (spam, escaneo de puertos, congestión de servidores)				X
R6	Organizacional	Cambios en los servicios del proveedor de <i>Cloud</i> (terminación de un servicio).			X	
R7	Organizacional	Incremento de dependencia de terceros lo que podría ocasionar deterioro en el cuidado al cliente y la calidad del servicio.				X
R8	Organizacional	Incertidumbre con las nuevas tecnologías y una falta de recursos de soporte para resolver problemas técnicos.		X		
R9	Organizacional	El proveedor de DRaaS está fuera de la organización.		X		
R10	Organizacional	Resistencia al cambio debido a cambio en las políticas de la organización y en el trabajo de las personas.		X		
<b>TOTAL</b>			<b>0</b>	<b>3</b>	<b>4</b>	<b>3</b>
R11	Legal	Incumplimiento con las regulaciones de manejo de datos personales				X
R12	Legal	Incumplimiento con regulaciones de confidencialidad de datos. Acceso no autorizado a los datos por el proveedor de <i>Cloud</i> .				X
R13	Legal	Incremento del riesgo que los derechos de propiedad intelectual sean violados.			X	
R14	Legal	Obsoletas protecciones contractuales que no aplican al modelo <i>Cloud</i> .				X
R15	Legal	Datos privados almacenados en <i>Cloud</i> pueden ser accedidos por gobiernos extranjeros debido a las				X
<b>TOTAL</b>			<b>0</b>	<b>0</b>	<b>1</b>	<b>4</b>

R16	Seguridad	Ataques de denegación de servicio. Conduce a la falta de disponibilidad de recursos.				X
R17	Seguridad	Los datos privados podrían ser accedidos por otros clientes o proveedores de <i>Cloud</i> . Varias vulnerabilidades de seguridad pueden ser utilizadas para extraer información de máquinas virtuales.				X
R18	Seguridad	Insegura e inefectiva eliminación de datos al escalar el uso de los recursos o cuando se cambia de proveedor.				X
R19	Seguridad	Las vulnerabilidades de los navegadores son más significativas.			X	
<b>TOTAL</b>			<b>0</b>	<b>0</b>	<b>1</b>	<b>4</b>
R20	Técnico	Una interrupción del servicio de back-up, causa una indisponibilidad de los servicios o pérdida de datos.				X
R21	Técnico	Bloqueo de datos.				X
R22	Técnico	Rendimiento no esperado de acuerdo a los ANS (Acuerdo de nivel de servicios).			X	
R23	Técnico	La falta de recursos podría inhabilitar al proveedor para atender las demandas de recursos actuales o futuras.			X	
R24	Técnico	Problemas de interoperabilidad entre Nubes debido a incompatibilidades entre las plataformas de los proveedores de <i>Cloud</i> .			X	
R25	Técnico	Los proveedores de modelos de <i>Cloud</i> mantienen los defectos con mejoras tecnológicas		X		
R26	Técnico	Los costos de cambiar de un proveedor de DRaaS a otro puede ser bastante alto. Esto también podría tomar un largo tiempo dependiendo del volumen de datos involucrados y se complica debido a las incompatibilidades entre las plataformas del proveedor.		X		
R27	Técnico	Inhabilidad para reducir costos debido a la irrealización en la reducción del número de personal de soporte.			X	
R28	Técnico	Fuentes no controlables de transferencia de datos por retrasos o cuellos de botella. Las diferencias de banda ancha en los precios y servicios son importantes para las empresas multinacionales.				X
R29	Técnico	Los datos privados que han sido expuestos debido a cambios en la responsabilidad de los usuarios quienes tienen una falta de conciencia acerca de dónde colocar los diferentes tipos de datos.				X
R30	Técnico	Errores entre el manejo de procedimientos de incidentes existentes y los procedimientos del proveedor de DRaaS. Falta de información o no acceso a la información de las vulnerabilidades de almacenamiento <i>Cloud</i> o incidentes de datos reportados. Conduce a respuestas limitadas desde una organización en caso de incidentes.			X	
<b>TOTAL</b>			<b>0</b>	<b>2</b>	<b>5</b>	<b>4</b>

Adaptado de (INTECO-CERT, 2011)

Estos posibles riesgos pueden ser mitigados mediante procesos de control de COBIT 5, como se plantea en la tabla 19; de esta manera, se identificará los procesos de la cooperativa que se deberán optimizar, es decir, encontrarse maduros para poder mitigar estos posibles riesgos.

De igual manera esto permitirá a Alianza del Valle tomar la decisión de asumir el riesgo cuando el proceso no está maduro, y optimizarlo en paralelo a la

implementación, o no implementar la solución hasta que estén mitigados todos los posibles riesgos.

Tabla 19. Mitigación de posibles riesgos

ID	Tipo	AMENAZAS	PROCESOS COBIT 5
R1	Organizacional	Perdida de control y de gobernabilidad sobre los recursos (control físico y de gestión).	EDM01, APO01, APO02, APO07
R2	Organizacional	Perdida de experiencia en TI, es decir falta de experiencia local y pérdida de conocimiento al largo plazo.	APO07, BAI07, BAI08
R3	Organizacional	Reducción de la productividad del personal de apoyo durante la migración (menor satisfacción en el trabajo) e incertidumbre laboral.	APO07, BAI08
R4	Organizacional	La gestión de un sistema en la nube puede tomar un esfuerzo de gestión adicional, gestión de la relación con los proveedores de DRaaS.	APO08, APO10, DSS06
R5	Organizacional	Perdida de reputación del negocio debido a actividades malintencionadas de terceros (spam, escaneo de puertos, congestión de servidores)	APO12, APO13, DSS05
R6	Organizacional	Cambios en los servicios del proveedor de Cloud (terminación de un servicio).	EDM01, EDM02, DSS01, DSS04, DSS06
R7	Organizacional	Incremento de dependencia de terceros lo que podría ocasionar deterioro en el cuidado al cliente y la calidad del servicio.	APO10, APO11, DSS01
R8	Organizacional	Incertidumbre con las nuevas tecnologías y una falta de recursos de soporte para resolver problemas técnicos.	APO09, APO10, BAI05, BAI06
R9	Organizacional	El proveedor de DRaaS está fuera de la organización.	APO02, APO03, APO09
R10	Organizacional	Resistencia al cambio debido a cambio en las políticas de la organización y en el trabajo de las personas.	APO07, BAI05
R11	Legal	Incumplimiento con las regulaciones de manejo de datos personales	DSS01, DSS06
R12	Legal	Incumplimiento con regulaciones de confidencialidad de datos. Acceso no autorizado a los datos por el proveedor de Cloud.	EDM03, APO02

R13	Legal	Incremento del riesgo que los derechos de propiedad intelectual sean violados.	APO01, DSS05, APO07
R14	Legal	Obsoletas protecciones contractuales que no aplican al modelo Cloud.	APO09, APO10, MEA03
R15	Legal	Datos privados almacenados en Cloud pueden ser accedidos por gobiernos extranjeros debido a las diferentes jurisdicciones.	APO09, APO10, MEA03
R16	Seguridad	Ataques de denegación de servicio. Conduce a la falta de disponibilidad de recursos.	APO01, DSS05
R17	Seguridad	Los datos privados podrían ser accedidos por otros clientes o proveedores de Cloud. Varias vulnerabilidades de seguridad pueden ser utilizadas para extraer información de máquinas virtuales.	APO01, DSS05, APO07
R18	Seguridad	Insegura e inefectiva eliminación de datos al escalar el uso de los recursos o cuando se cambia de proveedor.	BAI02, DSS05
R19	Seguridad	Las vulnerabilidades de los navegadores son más significativas.	APO01, DSS05
R20	Técnico	Una interrupción del servicio de back-up, causa una indisponibilidad de los servicios o pérdida de datos.	APO03, BAI03, BAI04
R21	Técnico	Bloqueo de datos.	BAI04, DSS03
R22	Técnico	Rendimiento no esperado de acuerdo a los ANS (Acuerdo de nivel de servicios).	APO03, BAI03, BAI04
R23	Técnico	La falta de recursos podría inhabilitar al proveedor para atender las demandas de recursos actuales o futuras.	APO03, BAI03, BAI04
R24	Técnico	Problemas de interoperabilidad entre Nubes debido a incompatibilidades entre las plataformas de los proveedores de Cloud.	BAI07
R25	Técnico	Los proveedores de modelos de Cloud mantienen los defectos con mejoras tecnológicas	APO10, BAI03
R26	Técnico	Los costos de cambiar de un proveedor de DRaaS a otro puede ser bastante alto. Esto también podría tomar un largo tiempo dependiendo del volumen de datos involucrados y se complica debido a las incompatibilidades entre las plataformas del proveedor.	APO10, BAI03

R27	Técnico	Inhabilidad para reducir costos debido a la irrealización en la reducción del número de personal de soporte.	APO02, APO03, BAI03, APO13
R28	Técnico	Fuentes no controlables de transferencia de datos por retrasos o cuellos de botella. Las diferencias de banda ancha en los precios y servicios son importantes.	APO03, BAI03, BAI04
R29	Técnico	Los datos privados que han sido expuestos debido a cambios en la responsabilidad de los usuarios quienes tienen una falta de conciencia acerca de dónde colocar los diferentes tipos de datos.	APO01, BAI02
R30	Técnico	Errores entre el manejo de procedimientos de incidentes existentes y los procedimientos del proveedor de DRaaS. Falta de información o no acceso a la información de las vulnerabilidades de almacenamiento Cloud o incidentes de datos reportados. Conduce a respuestas limitadas desde una organización en caso de incidentes.	BAI03, APO09, APO10

Adaptado de (ICESI, 2015)

Para la realización de la presente tabla se ha efectuado una comparación de las amenazas detalladas en la Tabla 18, con la descripción de cada una de las fichas de los procesos de COBIT 5, determinando así, que la implementación de dichos procesos mitigará la ocurrencia de las amenazas, ya que se fortalecerá los controles internos.

El detalle de procesos utilizados se puede visualizar en el (Anexo 4: Procesos COBIT 5)

El conocimiento de la situación actual de Alianza del Valle frente a la migración a la nube, es el primer paso, para realizar un análisis de factibilidad para migrar a un modelo de servicio de recuperación ante desastres en la nube, ya que nos ha permitido apreciar qué componentes intervienen en su plataforma tecnológica actual, cuáles son sus aplicaciones críticas, y cuáles son las posibles amenazas a afrontar, y por lo tanto, apreciar si con la solución propuesta se puede llegar a optimizar el uso de los recursos.

Para este estudio se intentó obtener la mayor cantidad de detalles de tal forma que la solución propuesta pueda satisfacer los requerimientos actuales para el funcionamiento de Alianza del Valle. Es recomendable que se realice un estudio más detallado, para identificar de forma oportuna las brechas y debilidades que deben ser cubiertas en el proyecto.

## CAPÍTULO IV

### ANÁLISIS DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE RECUPERACIÓN ANTE DESASTRES EN LA NUBE

#### 4.1 Introducción

En este capítulo se desarrollará el análisis de factibilidad para la implementación de Recuperación ante Desastres como Servicio (DRaaS) basado en el modelo de Computación en la Nube en la Cooperativa “Alianza del Valle”. La decisión de su implementación depende únicamente de los directivos de la cooperativa, quienes deberán evaluar las recomendaciones propuestas en la presente tesis.

El estudio de factibilidad es un instrumento que sirve para orientar la toma de decisiones en la evaluación de un proyecto, optimizando el uso de los recursos de la empresa, midiendo las posibilidades de éxito o fracaso para una adecuada evaluación. Apoyándose en él, se tomará la decisión de proceder o no con su implementación, y de acuerdo a esto una futura inversión que contribuya al desarrollo a mediano y largo plazo de una empresa.

El análisis de factibilidad es parte del proyecto de inversiones, en donde “Podemos definir un proyecto de inversión como: conjunto de acciones que son necesarias para llevar a cabo una inversión la cual se realiza con un objetivo previamente establecido, limitado por parámetros, temporales, tecnológicos, políticos, institucionales, ambientales y económicos” (Miranda, 2016).

Como primer punto se presenta la segunda parte adaptada de la estrategia para la migración a la nube, recomendado por *CloudTweaks* (2011), donde se realizará un estudio de proveedores. Como segundo punto, se analizará la factibilidad técnica, factibilidad operativa, aspectos económicos y los aspectos legales para considerar si esta implementación es viable. Para el efecto, se debe obtener resultados positivos en todos los estudios propuestos, cada uno de los cuales tiene igual importancia. El análisis de factibilidad debe proveer ventajas

considerables en los aspectos organizacionales, técnicos, económico-financiero, legales, y si los resultados son favorables se considera que la propuesta es factible de realizarla.

Se ha recolectado información no sensible para el funcionamiento de la empresa, la misma que fue proporcionada por parte de los directivos de la cooperativa. No obstante, esta información se considera de carácter confidencial, y la Cooperativa de Ahorro y Crédito “Alianza del Valle” se reserva los derechos de no publicar información que se considere perjudicial para el desenvolvimiento de su negocio.

#### **4.2 Problemas a Solucionar con DRaaS**

La Cooperativa “Alianza del Valle”, ha visto la necesidad de optimizar los recursos tecnológicos y adecuar los servicios que dispone dándoles mayor flexibilidad.

Como se menciona en el capítulo anterior, la cooperativa busca implementar un sitio alternativo para complementar su plan de recuperación ante desastres, donde se encuentre instalado el Core Cobis, ya que, actualmente el sitio alternativo que poseen, no cuenta con la capacidad necesaria para que funcionen todas las aplicaciones de alta criticidad, y es por esto que, si llegara a suscitarse un evento fortuito, no se podría poner en funcionamiento todos los procesos de negocio. Además, es necesario optimizar el almacenamiento de los datos, porque en un ambiente de constante cambio, el crecimiento de la información se vuelve impredecible y los servidores pueden llegar a tener poca capacidad de almacenamiento para cubrir un futuro crecimiento en los próximos cinco años.

#### **4.3 Análisis de los proveedores de DRaaS.**

Para el presente análisis se utilizó como referencia el cuadrante mágico de Gartner para la recuperación de desastres como servicio actualizado junio 2016, donde se detalla a los principales proveedores de DRaaS.



Figura 15. Gartner - Proveedores de DRaaS

Tomado de (Gartner, 2016)

Por petición de la Gerencia General, se procedió a evaluar a los proveedores IBM, Microsoft y VMWare, por la confianza que se tiene con la marca, además, porque cuentan con partners dentro del Ecuador, lo que facilita las consideraciones contractuales.

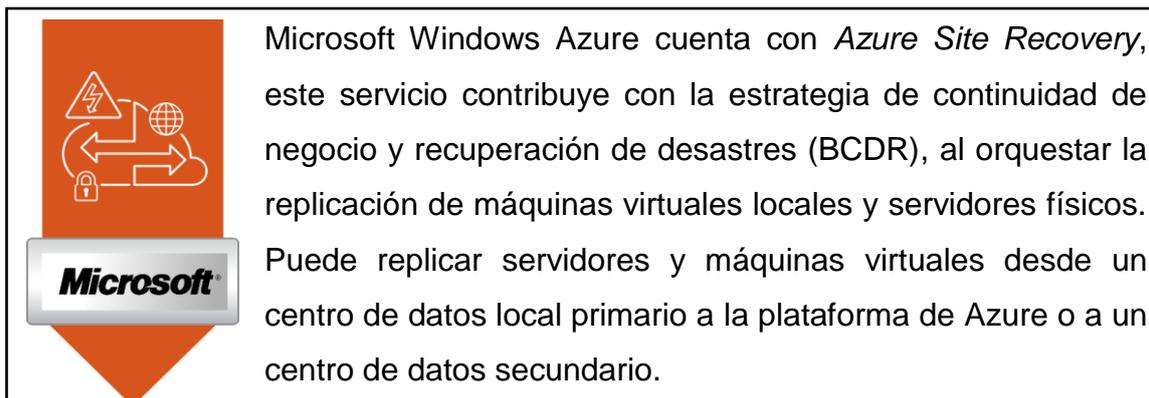


Figura 16. Servicio Microsoft DRaaS

Adaptado de (Microsoft, 2016)

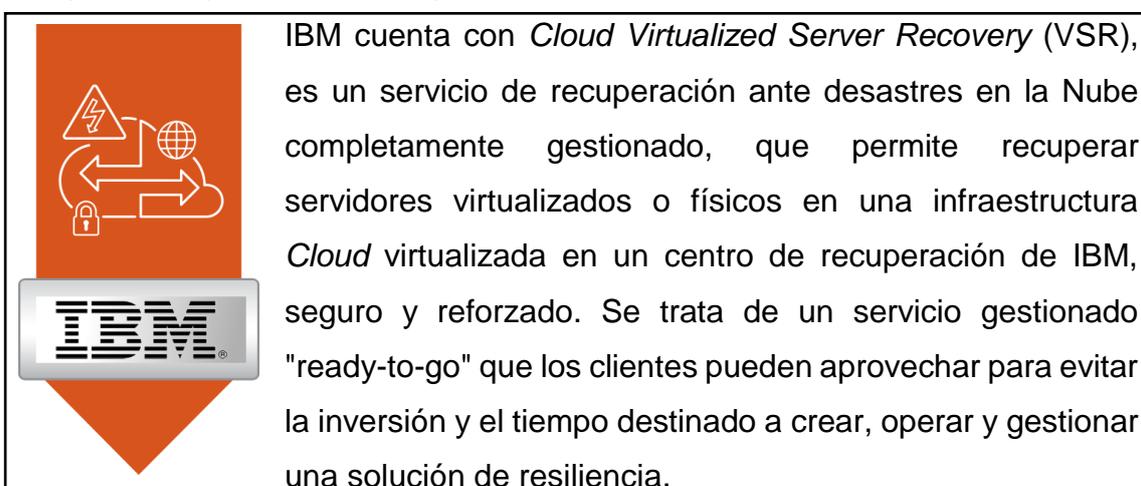


Figura 17. Servicios IBM DRaaS

Adaptado de (IBM, 2016)

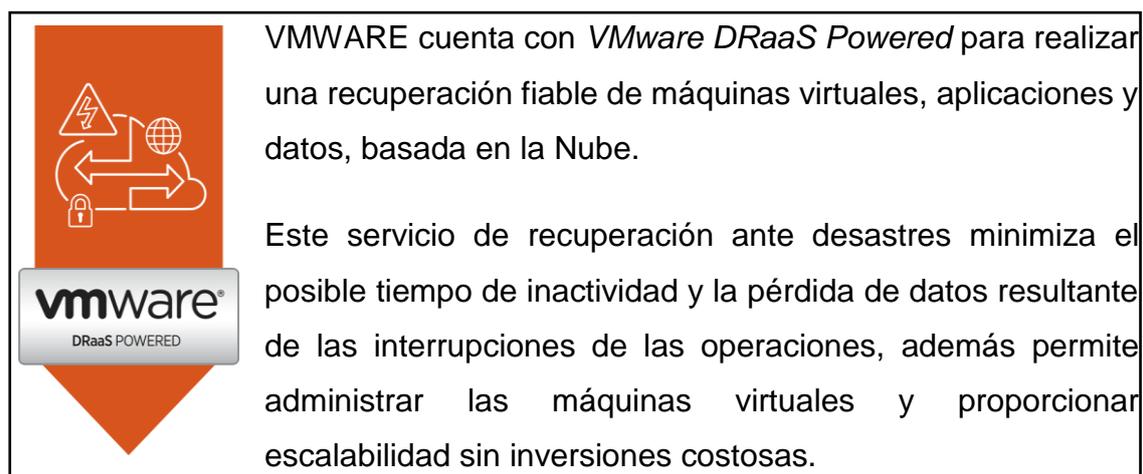


Figura 18. Servicios VMWare DRaaS

Adaptado de (VMWare, 2016)

#### **4.3.1 Requisitos para la contratación.**

Los requerimientos para la contratación de los proveedores se detallaron basándose en las mejores prácticas en materia de contratación de Servicios de Computación en la Nube de ENISA (2014), y en las normas generales de la Superintendencia de Economía Popular y Solidaria del Ecuador (2014).

##### Continuidad del Servicio:

La Cooperativa está comprometida a entregar sus servicios los 365 días del año, las 24 horas del día, ya que según la Superintendencia de Economía Popular y Solidaria, “las instituciones controladas deben contar con la tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté DISPONIBLE para una apropiada toma de decisiones”.

En consecuencia, la cooperativa debe poner especial atención a la continuidad permanente del servicio en la Nube puesto que, en caso contrario, se podría ver impedida de cumplir dicho compromiso hacia sus socios/clientes; en este sentido, los proveedores de servicios deben tener la capacidad organizativa y técnica que pueda asegurar la continuidad del servicio con una alta disponibilidad 24/7.

##### Confidencialidad de la información:

Los datos subidos a la Nube, deben tener un estricto grado de confidencialidad de la información y datos, rigiéndose a la normativa de la Superintendencia de Economía Popular y Solidaria de contratación de servicios. Esto tiene particular importancia no solo en el caso de los datos personales y datos sensibles, sino también con información secreta o reservada. Se exige, a los proveedores del servicio, cláusulas de confidencialidad acerca de los datos almacenados, prohibiendo que dicha información sea puesta en conocimiento de terceros no autorizados.

### Borrado de Datos:

Se debe tomar especial atención al tema del borrado de información, ya que en el caso de que no se desee continuar con el proveedor del servicio DRaaS, se requiere que se mencione en el convenio de confidencialidad, que el proveedor esté dispuesto a migrar la información a un nuevo proveedor y que se entregue las garantías necesarias para que exista un borrado completo de información, considerando los respaldos que este proveedor posea.

### Seguridad de la información:

Para verificar la seguridad de la información, se solicitó que al menos cuenten con estas cuatro perspectivas:

- El prestador del servicio en la Nube, debe tener e implementar las medidas técnicas y organizativas adecuadas para que la información que es almacenada en la nube no se pierda, dañe o corrompa.

Se solicitará que el prestador del servicio cuente con alguna certificación que asegure que éste cumple con normas de seguridad de la información, para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados. Por solicitud de la SEPS, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya.

- Los datos que se almacenan en las instalaciones del prestador del servicio no serán accedidos/utilizados por terceras personas.
- Los datos que almacena el prestador del servicio no serán accedidos/utilizados por éste para fines distintos a los que establece el contrato.
- La comunicación de datos, entre el prestador de servicios y el cliente, debe ser de forma segura.

Se requiere que las comunicaciones y el acceso remoto que se da entre el prestador del servicio y la cooperativa tenga la seguridad suficiente como para evitar que sean interceptadas por terceros. Es necesario que el proveedor brinde canales de comunicación seguros mediante la

utilización de técnicas de encriptación acorde con los estándares internacionales vigentes, por normativa de la SEPS.

#### Propiedad Intelectual:

La SEPS solicita que se cuente con derechos de propiedad intelectual del conocimiento, productos, datos e información, cuando aplique, es decir únicamente la Cooperativa "Alianza del Valle", será titular de los derechos de propiedad intelectual sobre la documentación y bases de datos que se sube al servicio de Nube.

#### Auditoría:

Por la sensibilidad de los datos que maneja la cooperativa, requiere que, como contratante del servicio, esté en condiciones de auditar las políticas, procesos, sistemas y servicios del prestador del servicio en la Nube.

#### Facilidad de Uso:

La cooperativa requiere una solución racionalizada y de fácil manejo, para disminuir las cargas de trabajo futuras en gestión de IT, por lo que se requiere que los proveedores brinden una solución amigable para el usuario.

#### Flexibilidad:

La cooperativa "Alianza del Valle", requiere una solución flexible que pueda satisfacer todas sus necesidades de administración de datos, ya que prevé tener un crecimiento mayor en los próximos 5 años.

#### Calidad de Soporte:

Se requiere que el proveedor entregue un soporte inmediato a los requerimientos o problemas que se presenten, por lo que deberán cumplir con los más altos estándares y tiempos de respuesta.

### Costo

Para la implementación de una solución que ayude a cumplir con los objetivos del plan de continuidad de negocio, se tiene un presupuesto de \$100.000 dólares americanos; las propuestas no pueden exceder este valor.

#### **4.3.2 Comparativa entre Proveedores**

Una vez descrito los parámetros de evaluación, es necesario priorizarlos por importancia. Este factor ayudará en la elaboración de la tabla final de calificaciones de cada proveedor, donde el factor de importancia es de 1 a 3; siendo 3 el valor asignado al parámetro de mayor importancia.

Se procedió a elaborar la Tabla 20, luego de conversar con el personal del departamento de Sistemas, Financiero, y Gerencia General.

Tabla 20. Importancia Parámetros Evaluación de Proveedores

Parámetros	Importancia
Continuidad del Servicio	3
Confidencialidad de la información	3
Borrado de Información	3
Seguridad de la información	3
Propiedad Intelectual	2
Auditoría	2
Facilidad de Uso	2
Flexibilidad	2
Calidad de Soporte	3
Costo	2

Para valorar a los proveedores se asignó una calificación, aplicando el rango de 0 al 3, siendo 0 = no cumple, 1 = cumple levemente, 2 = en proceso de mejora, 3 = cumple a totalidad, como se muestra en la Tabla 21.

Para la valoración se analizó información entregada por los proveedores y la obtenida de la página web informativa de cada uno de ellos.

Tabla 21. Comparativa de Proveedores

Parámetros	Windows Azure			IBM			VMWARE				
	Imp	Cal	Total	Imp	Cal	Total	Imp	Cal	Total		
Continuidad del Servicio	3	3	9	3	3	9	3	3	9		
Confidencialidad de la información	3	3	9	3	3	9	3	3	9		
Borrado de la Información	3	2	6	3	3	9	3	2	6		
Seguridad de la información	3	3	9	3	3	9	3	3	9		
Propiedad Intelectual	2	2	4	2	3	6	2	3	6		
Auditoría	2	3	6	2	2	4	2	2	4		
Facilidad de Uso	2	2	4	2	2	4	2	3	6		
Flexibilidad	2	3	6	2	2	4	2	2	4		
Calidad de Soporte	3	2	6	3	3	9	3	2	6		
Costo	2	2	4	2	3	6	2	3	5		
Total			<b>96</b>	Total			<b>104</b>	Total			<b>97</b>

Nota: Imp - Factor Importancia, Cal-Calificación.

Tanto Microsoft, IBM y VMWare cumplen con los requerimientos necesarios para convertirse en un proveedor potencial para la implementación del servicio, siendo IBM el que alcanza la mayor puntuación.

Es por esto que se tomará en cuenta a los tres proveedores, para realizar el análisis de factibilidad.

#### 4.4 Estudio de Factibilidad

A continuación, se presentará los estudios de factibilidad técnica, operativa, económica y legal para la implementación de DRaaS en la Cooperativa de Ahorro y Crédito Alianza del Valle, en la que se realizará un análisis comparativo entre la tecnología en la Nube con los proveedores IBM y Microsoft, así como

también tecnología propietaria (*in house*) como mejora para su sitio alterno actual.

Para el siguiente estudio se tomará los requerimientos para el funcionamiento de todas las aplicaciones críticas de la cooperativa detalladas en el capítulo anterior.

#### 4.4.1 Estudio de Factibilidad Técnica

En este punto se analiza los aspectos técnicos del proyecto, detallados en el capítulo III, donde se realizó el estudio de los requerimien/s mínimos para el funcionamiento de la cooperativa, tomando en cuenta los aspectos de:

- Disponibilidad de recursos y servicios
- Infraestructura
- Escalabilidad
- Sitio Alterno

En la Tabla 22 se realiza un comparativo entre soluciones *In House* y soluciones en la nube, tomando en cuenta las estimaciones de requerimientos mínimos para el funcionamiento del Core Financiero COBIS.

Tabla 22. Solución In House vs Nube

SERVIDOR PRODUCCIÓN	SOLUCIONES <i>IN HOUSE</i>	SOLUCIONES EN LA NUBE		
	SITIO ALTERNO	MICROSOFT	IBM	VMWARE
Memoria RAM	32 GB	Pago por uso	Pago por uso	Pago por uso
Cantidad de Procesadores	7	Pago por uso	Pago por uso	Pago por uso
Capacidad de Procesadores	2.750 MHZ	Pago por uso	Pago por uso	Pago por uso
Cantidad de Discos	2	Pago por uso	Pago por uso	Pago por uso
Capacidad de Discos	300 GB	Pago por uso	Pago por uso	Pago por uso
Crecimiento anual en disco	5%	Crecimiento flexible	Crecimiento flexible	Crecimiento flexible
Aplicativo instalado	COBIS v.3.3(32 bits)	No aplica	No aplica	No aplica

Licenciamiento COBIS	Reutilización de licencia	No aplica	No aplica	No aplica
Aplicativo 2 instalado	base de datos SYBASE	No aplica	No aplica	No aplica
Licenciamiento Sybase	Reutilización de Licenciamiento	No aplica	No aplica	No aplica
Gestión de la red lan, internet y datos	Capacidad actual suficiente	Capacidad actual suficiente	Capacidad actual suficiente	Capacidad actual suficiente
Sistema operativo instalado	Solaris 10	No soportado	No soportado	Soportado

Los proveedores de servicio DRaaS ofrecen un pool de recursos donde se paga por lo que se usa, es por esto que no se requiere estimar el aumento de capacidades de hardware para un tiempo determinado, de esta manera no solo se evitan fuertes inversiones iniciales de hardware, si no también tener que repotenciar los equipos en base a los requerimientos de la cooperativa como en el caso de fortalecer el sitio alterno. Cabe indicar que por políticas internas y de control, es necesario reemplazar los equipos cada 5 años de funcionamiento.

Cobis es un sistema Core que corre únicamente bajo la plataforma de Solaris y AIX, actualmente el Core Cobis se encuentra instalado sobre el sistema operativo Solaris 10, esto ocasiona que VMware sea el único proveedor que soporte dicho sistema operativo.

En la siguiente Tabla, se realiza un comparativo entre soluciones *In House* y soluciones en la nube, tomando en cuenta los requerimientos mínimos para el funcionamiento de las aplicaciones de alta criticidad detalladas en el capítulo III.

Tabla 23. Solución In House vs Solución en la Nube

SERVIDOR DE APLICACIONES	SOLUCIONES IN HOUSE	SOLUCIONES EN LA NUBE		
	SITIO ALTERNO	MICROSOFT	IBM	VMWARE
Memoria RAM	64 GB	Pago por uso	Pago por uso	Pago por uso

Cantidad de Procesadores	2	Pago por uso	Pago por uso	Pago por uso
Procesador	Intel Xeon E5-2640 v2 2.0 MHZ	Pago por uso	Pago por uso	Pago por uso
Cantidad de Discos	4	Pago por uso	Pago por uso	Pago por uso
Capacidad de Discos	3 TB	Pago por uso	Pago por uso	Pago por uso
Crecimiento anual en disco	10%	Crecimiento flexible	Crecimiento flexible	Crecimiento flexible
Cantidad de sistemas virtualizados	20	Pago por uso	Pago por uso	Pago por uso
Cantidad de Aplicaciones críticas	16	No aplica	No aplica	No aplica
Gestión de la red lan, internet y datos	Capacidad actual suficiente	Capacidad actual suficiente	Capacidad actual suficiente	Capacidad actual suficiente
Sistema de virtualización	VMWARE VSphere ver 5.5	Hyper-V	IBM PowerVM	VMware VSphere

Al igual que en el análisis anterior, con las soluciones en la nube, no se requiere estimar capacidades de hardware para un tiempo determinado, a diferencia de la solución *in house*, donde se debe realizar inversiones iniciales para fortalecer el sitio alterno actual.

Al ser aplicativos instalados en el sistema de virtualización VMWare VSphere es factible la migración a la plataforma Microsoft, IBM y VMWare, es por esto que se selecciona VMWare porque trabaja bajo la misma tecnología que el servidor de aplicaciones local.

#### 4.4.2 Estudio de Factibilidad Operativa

El presente estudio permite conocer a “Alianza del Valle”, la posibilidad de poner en marcha el servicio de DRaaS, aprovechando los beneficios que este ofrece, por otra parte, la correcta implementación y funcionamiento depende de la capacidad de los miembros del departamento de IT y de las áreas involucradas, razón por la cual se necesita garantizar el pleno entendimiento, consentimiento y capacidad de los antes mencionados.

A continuación, se presenta una encuesta realizada en conjunto con el área de IT y Gerencia General, donde se pretende conocer el estado de aceptación del proyecto.

Tabla 24. Encuesta aceptación del proyecto

PREGUNTA	SOLUCIÓN ACTUAL
¿Cuenta con un sitio alternativo de recuperación?	SI
¿Se cuenta con el apoyo suficiente para la implementación de la solución por parte de la directiva?	SI
¿Se cuenta con el apoyo por parte de los usuarios para implementar la solución?	SI
¿Los usuarios se encuentran conformes con la solución actual con la que cuenta la cooperativa para su recuperación ante desastres?	NO
¿Los usuarios han participado en la planeación y desarrollo del proyecto?	SI
¿Se podrá hacer uso del personal actualmente contratado para desarrollo del proyecto?	SI
¿La cooperativa cuenta actualmente con personal capacitado para la implementación y mantenimiento de la solución?	SI
¿La cooperativa está clara de los beneficios que brindará la solución propuesta?	SI
¿Usted como persona encargada de manejar los procesos de recuperación actuales, cree que la solución propuesta le es de gran ayuda?	SI
¿Se cuenta con el aval para hacer uso de la infraestructura física y equipos existentes?	SI

Como se puede visualizar en el cuadro anterior, se cuenta con el aval del Consejo de Administración para hacer uso de la infraestructura física y equipos existentes, además se dispone de los recursos humanos para la implementación de la solución, adicionalmente el personal de la Cooperativa “Alianza del Valle”, tiene muy en claro los beneficios que la solución propone.

Igualmente es necesario valorar la solución In House contra la solución en la Nube como se presenta en la siguiente encuesta, que se realizó en colaboración con la Jefatura de IT, y el asesor de venta VMWare.

Tabla 25. Encuesta solución In House vs Nube

PREGUNTA	SOLUCIÓN IN HOUSE	SOLUCIÓN EN LA NUBE
¿Cuántos mantenimientos preventivos al servidor de producción y aplicaciones se requieren al año?	Mantenimiento a nivel de hardware 2 veces al año de manera semestral, el mantenimiento a nivel de software de manera trimestral.	No se requiere mantenimiento por parte del cliente.
¿Cuánto tiempo les toma recuperar el servicio cuando se dañan los servidores principales?	Actualmente toma aproximadamente 30 minutos el recuperar parcialmente los servicios	Los planes de DR tradicionales exigen gestiones manuales. Esto no sucede con el DRaaS, lo que disminuye el RTO (recovery time objective)
¿Cuenta con una solución de respaldo?	La base de datos se replica con el software propietario de Sybase, mientras que Cobis se respalda de manera manual mediante envío de archivos.	En caso de requerir la base de datos se realiza una replicación incremental de manera constante, o a su vez una replicación de la imagen de la máquina virtual.
¿Cuenta con alguna herramienta de monitoreo de la salud de sus servidores?	Se cuenta con el software de monitoreo WhatsUp Gold	VMWare cuenta con una familia de soluciones y productos integrados, DRaaS <i>Powered</i> que brinda el monitoreo continuo de las máquinas virtuales instaladas.

¿La cooperativa cuenta con alguna herramienta que analice el desempeño y predicción de la necesidad de recursos para los servidores actuales??	No	VMWare cuenta con una familia de soluciones y productos integrados, DRaaS <i>Powered</i> que brinda análisis de desempeño y predicción de necesidad de recursos autoajustables.
¿Se requiere la contratación de personal capacitado para administrar la solución planteada?	Si, en el caso de que se implemente correctamente el sitio alternativo, ya que se requiere que se monitoree y se dé soporte de manera más personalizada. Se requiere contratar un analista de infraestructura y base de datos.	Si, ya que, aunque todo es automático y el hipervisor de administración es muy fácil de utilizar, es necesario que alguien esté en constante monitoreo y control de la solución. Se requiere contratar un administrador de soluciones

Como se demuestra en la encuesta realizada, la solución de DRaaS brinda factibilidad operativa, ya que facilitará el monitoreo, administración y respuesta de los servidores virtualizados, que se instalarán como recuperación ante desastres evitando tiempos de inactividad que pueden incurrir en costos.

#### 4.4.3 Estudio de los aspectos económicos

Este estudio económico – financiero servirá para determinar el costo que implicaría el implementar, administrar y mantener la solución IN HOUSE en el sitio alternativo, y los costos de implementación y mantenimiento del servicio DRaaS, tomando en consideración que ambos proyectos son mutuamente excluyentes.

Para realizar el presente estudio, es necesario analizar las soluciones de manera independiente, y luego realizar una comparación entre los resultados obtenidos.

Los indicadores económicos que se utilizaron para el presente estudio es VAN (Valor Actual Neto) y TIR (Tasa interna de retorno).

#### 4.4.3.1 Solución IN HOUSE

Para la solución In House se ha tomado en cuenta los requerimientos mínimos para el funcionamiento de las aplicaciones críticas de la cooperativa detalladas en el capítulo III.

A continuación, se presentan los costos aproximados para implementar lo necesario para el funcionamiento del sitio alterno.

##### Costo servidor producción COBIS

Tabla 26. Compra e instalación COBIS

CONCEPTOS	COSTO ANUAL
Adquisición servidor Fujitsu spark-enterprise M300, Ram:32 GB, Disco Duro: 2 discos de 500 GB	51.000
Reutilización licencia Solaris	0
Instalación y configuración Core COBIS	3.000
Reutilización licencia Core COBIS	0
Instalación y configuración base de datos SYBASE	2.500
Reutilización licencia base de datos SYBASE	0
<b>TOTAL</b>	<b>\$56.500,00</b>

##### Costo servidor de Aplicaciones

Tabla 27. Costo compra e instalación aplicaciones críticas

CONCEPTOS	COSTO ANUAL
Adquisición servidor HP Modelo BL460c Gen 8, RAM: 64 GB, Disco Duro: 12 TB, Procesador: Intel Xeon ES-2640 v2	75.000
Licencia VMWARE Standard	9.734
Instalación y configuración de máquinas virtuales y aplicaciones	2.800
<b>TOTAL</b>	<b>\$87.534,00</b>

Costo operación servidores

Tabla 28. Costo operación de servidores

CONCEPTOS	COSTO AÑO1	AÑO2	AÑO3	AÑO4	AÑO5	TOTAL
Mantenimiento servidores físico	16.000	16.000	16.000	16.000	16.000	80.000
Mantenimiento servidores lógico	11.380	11.380	11.380	11.380	11.380	56.900
Costos de operación	5.600	5.600	5.600	5.600	5.600	28.000
<b>TOTAL</b>	<b>\$32.980,00</b>	<b>\$32.980,00</b>	<b>\$32.980,00</b>	<b>\$32.980,00</b>	<b>\$32.980,00</b>	<b>\$164.900,00</b>

Costo contratación Analista de Infraestructura

Tabla 29. Costo contratación operador técnico

CONCEPTOS	AÑO1	AÑO2	AÑO3	AÑO4	AÑO5	TOTAL
SALARIO BÁSICO	1.200	1.200	1.200	1.200	1.200	
SALARIO ANUAL	14.400	14.400	14.400	14.400	14.400	72.000
DECIMO TERCERO	1200	1200	1200	1200	1200	6.000
DECIMO CUARTO	366	366	366	366	366	1.830
IESS	1.750	1.750	1.750	1.750	1.750	8.748
FONDOS DE RESERVA	0	1200	1200	1200	1200	4.800
VACACIONES	600	600	600	600	600	3.000
<b>TOTAL ANUAL</b>	<b>\$18.315,60</b>	<b>\$19.515,60</b>	<b>\$19.515,60</b>	<b>\$19.515,60</b>	<b>\$19.515,60</b>	<b>\$96.378,00</b>

Costo contratación Analista de Base de Datos

Tabla 30. Costo contratación Analista de Base de Datos

CONCEPTOS	AÑO1	AÑO2	AÑO3	AÑO4	AÑO5	TOTAL
SALARIO BÁSICO	1.300	1.300	1.300	1.300	1.300	
SALARIO ANUAL	15.600	15.600	15.600	15.600	15.600	78.000
DECIMO TERCERO	1200	1200	1200	1200	1200	6.000
DECIMO CUARTO	366	366	366	366	366	1.830
IESS	1.895	1.895	1.895	1.895	1.895	9.477
FONDOS DE RESERVA	0	1200	1200	1200	1200	4.800
VACACIONES	650	650	650	650	650	3.250
<b>TOTAL ANUAL</b>	<b>\$19.711,40</b>	<b>\$20.911,40</b>	<b>\$20.911,40</b>	<b>\$20.911,40</b>	<b>\$20.911,40</b>	<b>\$103.357,00</b>

Los valores estimados, son definidos en el manual de recursos humanos como políticas salariales.

Por lo tanto, la inversión necesaria para implementar el sitio alternativo al final de cinco años es:

Tabla 31. Costo implementación Sitio Alternativo

CONCEPTOS	TOTAL
Costo servidor de producción COBIS	\$56.500,00
Costo servidor de Aplicaciones	\$87.534,00
Costo operación servidores	\$170.900,00
Contratación analista de infraestructura	\$96.378,00
Contratación analista de base de datos	\$103.357,00
<b>TOTAL</b>	<b>\$514.669,00</b>

#### Flujo de efectivo sitio alternativo

Se ha proyectado los costos de implementación para cinco años.

Tabla 32. Flujo de efectivo sitio alternativo

CONCEPTOS	AÑO0	AÑO1	AÑO2	AÑO3	AÑO4	AÑO5
Instalación servidor COBIS	\$56.500,00	0	0	0	0	0
Instalación servidor Aplicaciones	\$87.534,00	0	0	0	0	0
Mantenimiento equipos, costo de operación y enlaces de comunicaciones	0	\$38.980,00	\$32.980,00	\$32.980,00	\$32.980,00	\$32.980,00
Contratación personal 1	0	\$18.315,60	\$19.515,60	\$19.515,60	\$19.515,60	\$19.515,60
Contratación personal 2	0	\$19.711,40	\$20.911,40	\$20.911,40	\$20.911,40	\$20.911,40
<b>TOTAL</b>	<b>\$144.034,00</b>	<b>\$77.007,00</b>	<b>\$73.407,00</b>	<b>\$73.407,00</b>	<b>\$73.407,00</b>	<b>\$73.407,00</b>

#### 4.4.3.2 Solución en la Nube

Para la solución de recuperación ante desastres en la Nube, se ha tomado en cuenta los requerimientos mínimos para el funcionamiento de las aplicaciones críticas de la cooperativa detalladas en el capítulo III.

A continuación, se presentan los costos aproximados para implementar lo necesario para el funcionamiento del sitio alternativo.

#### Costo implementación DRaaS

Tabla 33. Costo implementación DRaaS

CONCEPTOS	COSTO ANUAL
Costo servicio DRaaS	62.400
Costo de implementación	10.000
Costo enlace de Datos	6.000
Eventualidades	5.000
<b>TOTAL</b>	<b>\$78.400,00</b>

#### Costo contratación nuevo personal - Administrador de Soluciones

Tabla 34. Costos contratación nuevo personal DRaaS

CONCEPTOS	AÑO1	AÑO2	AÑO3	AÑO4	AÑO5	TOTAL
SALARIO BÁSICO	1.200	1.200	1.200	1.200	1.200	
SALARIO ANUAL	14.400	14.400	14.400	14.400	14.400	72.000
DECIMO TERCERO	1200	1200	1200	1200	1200	6.000
DECIMO CUARTO	366	366	366	366	366	1.830
IESS	1.750	1.750	1.750	1.750	1.750	8.748
FONDOS DE RESERVA	0	1200	1200	1200	1200	4.800
VACACIONES	600	600	600	600	600	3.000
<b>TOTAL ANUAL</b>	<b>18315,6</b>	<b>19515,6</b>	<b>19515,6</b>	<b>19515,6</b>	<b>19515,6</b>	<b>96378</b>

Los gastos por concepto de contratación de personal son considerados de acuerdo a todos los beneficios de ley establecidos por el ministerio de Relaciones Laborales del Ecuador y Aportaciones al IESS.

Esta persona estará encargada de la administración y monitoreo de la solución.

### Flujo de efectivo – Costos

Para el presente análisis se ha realizado una proyección de los costos para la solución en la nube por un tiempo de 5 años.

Tabla 35. Flujo de Efectivo - Costos DRaaS

CONCEPTOS	AÑO0	AÑO1	AÑO2	AÑO3	AÑO4	AÑO5
Costo servicio DRaaS		62400	62400	62400	62400	62400
Costo de implementación	10.000	0	0	0	0	0
Costo enlace de Datos		6000	6000	6000	6000	6000
Costo contratación de personal		18315,60	20065,07	20101,07	20296,22	20101,07
Eventualidades		5000	5000	5000	5000	5000
<b>TOTAL</b>	<b>10000</b>	<b>91715,6</b>	<b>92915,6</b>	<b>92915,6</b>	<b>92915,6</b>	<b>92915,6</b>

#### **4.4.3.3 Viabilidad Económica**

Para el presente análisis se entenderá que ambos proyectos, solución IN House y solución de recuperación ante desastres en la nube (DRaaS), son mutuamente excluyentes.

A continuación, se determinará el Valor presente de los flujos de costos, de ambos proyectos para un periodo de 5 años, a fin de que sean comparables.

La tasa de descuento utilizada para el cálculo de los flujos de costos, es la equivalente al costo de oportunidad del dinero en la cooperativa, la misma que es el 14.2%, de rendimiento en la cartera de crédito.

Es importante indicar que el beneficio de implementar esta solución, a más del cumplimiento normativo, es el de mitigar el riesgo operativo de la institución ante un eventual cierre de operaciones, producto de un incidente catastrófico que podría degenerar en un alto riesgo reputacional y una corrida de fondos. Para fines de este análisis se ha estimado en conjunto con el departamento de Riesgos de la institución, que la pérdida esperada ante el riesgo de un evento fortuito que genere una caída de las aplicaciones fundamentales para el funcionamiento de la cooperativa, es de \$1,000,000 de dólares americanos.

### Valor Actual (VA)

El valor actual sirve para traer a valor presente (día de hoy), los flujos futuros.

Tabla 36. Valor Actual (VA)

	Valor Actual
<b>Solución IN House</b>	\$397.991,88
<b>Solución DRaaS</b>	\$326.408,66

### Valor Actual Neto (VAN)

El valor actual neto se determina restando el valor inicial de la inversión del valor actual, y este valor determina la viabilidad económica – financiera del proyecto, es decir si el valor actual neto es positivo, el proyecto es viable.

- Solución IN HOUSE

Tabla 37. VAN In House

	AÑO0	AÑO1	AÑO2	AÑO3	AÑO4	AÑO5
INGRESOS	\$0	\$1.000.000	\$1.000.000	\$1.000.000	\$1.000.000	\$1.000.000
EGRESOS	\$144.034	\$77.007	\$73.407	\$73.407	\$73.407	\$73.407
FLUJO NETO DE EFECTIVO	-\$144.034	\$922.993	\$926.593	\$926.593	\$926.593	\$926.593
VALOR PRESENTE	-\$144.034	\$808.225	\$710.488	\$622.144	\$544.784	\$477.044

VAN: \$ 3.018.651,22

- Solución DRaaS

Tabla 38. VAN DRaaS

	AÑO0	AÑO1	AÑO2	AÑO3	AÑO4	AÑO5
INGRESOS	\$0	\$1.000.000	\$1.000.000	\$1.000.000	\$1.000.000	\$1.000.000
EGRESOS	\$10.000	\$91.716	\$92.916	\$92.916	\$92.916	\$92.916
FLUJO NETO DE EFECTIVO	-\$10.000	\$908.284	\$907.084	\$907.084	\$907.084	\$907.084

VALOR PRESENTE	-\$10.000	\$795.345	\$695.529	\$609.045	\$533.314	\$467.000
----------------	-----------	-----------	-----------	-----------	-----------	-----------

VAN: \$3.090.234,4

Como se puede apreciar en el presente análisis, el VAN de los 2 proyectos es positivo, es decir ambos son viables, aunque la inversión sobre la solución de DRaaS es más Económica.

Es importante indicar que, por normas internas de la cooperativa, luego de 5 años de operatividad de los equipos deben ser cambiados, es decir se deberá volver a realizar dicha inversión inicial.

#### Tasa Interna de Retorno (TIR)

La TIR se utilizó como indicador de la rentabilidad para el presente proyecto, es decir a mayor TIR, mayor rentabilidad del mismo.

Tabla 39. Tasa interna de Retorno (TIR)

	TIR
<b>Solución IN House</b>	641%
<b>Solución DRaaS</b>	9083%

Como se puede visualizar, la tasa de rendimiento de la inversión es mayor al 100%, esto se da, debido a que la inversión para la solución IN HOUSE, como DRaaS, es de \$397.991,88 y \$326.408,7 respectivamente sobre un ingreso de \$1.000.000, lo que a breves rasgos demuestra rentabilidad.

Es decir, frente a una inversión relativamente pequeña, el beneficio económico esperado es inmensamente elevado, por lo que se concluye que existe factibilidad económica para implementar este proyecto.

#### **4.4.4 Estudio de los aspectos Legales**

Las instituciones deben entender los términos legales dentro de los contratos de servicios que definen las relaciones jurídicas entre los clientes y los proveedores

de tecnologías en la nube. Es de gran importancia conocer la responsabilidad de cada uno de los involucrados como lo es el proveedor y el cliente.

Los aspectos legales en la adopción de DRaaS bajo la tecnología en la nube es de gran importancia para el estudio de factibilidad de este proyecto, puesto que el proveedor de servicios en la nube provee acceso a los recursos informáticos y conserva la información del cliente en virtud del servicio contratado. El Cliente debe cancelar por el servicio contratado y definido en un contrato.

Alianza del Valle al ser una cooperativa de ahorro y crédito se encuentra normada por la SEPS, y esta no cuenta con ningún reglamento que impida tener los datos críticos de las entidades financieras en la "Nube", además en el Ecuador en general no existen normativas específicas que rijan los servicios en la Nube, ya que la nube no es un servicio de telecomunicaciones regulado, por lo cual se debe establecer una relación Jurídica de tipo Civil entre el Cliente y el Proveedor de Servicios, y dicha relación debe ser mediante la suscripción de un Contrato Privado.

Para este caso se hará referencia a los siguientes artículos de la "Ley de Comercio Electrónico, Firmas y Mensajes de Datos", (Congreso Nacional, 2016).

## Capítulo II

De la contratación electrónica y telemática.

"Art. 45 – Validez de los contratos electrónicos. - Los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos" (Congreso Nacional, 2016).

"Art. 46 - Perfeccionamiento y aceptación de los contratos electrónicos. - El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.

La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

Art. 47.- Jurisdicción. - En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario” (Congreso Nacional, 2016).

### Capítulo III

#### De los derechos de los usuarios o consumidores de servicios electrónicos

“Art. 49.- Consentimiento para el uso de medios electrónicos. - De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

- a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,
- b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:
  1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;
  2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;
  3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,
  4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los

registros electrónicos y el costo de esta copia, en caso de existir” (Congreso Nacional, 2016).

Además se tomará la referencia del artículo 92 sección quinta de la Constitución Política de la República del Ecuador, “habeas data”, donde se establece “Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéricos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, que consten en entidades públicas o privadas, en soporte material o electrónico.”

#### **4.4.4.1 Obligaciones contractuales**

Al realizar el contrato se debe tener en cuenta que existen tres sujetos, INTERESADO, que es la persona a la que se refieren los datos en cuestión, RESPONSABLE, el sujeto que recoge y procesa dichos datos y toma decisiones sobre el uso de los mismos y el ENCARGADO DEL TRATAMIENTO, que es quien realiza el tratamiento de los datos por cuenta del responsable.

Es decir “Alianza del Valle”, será el Responsable de los datos de carácter personal y el prestador del servicio DRaaS será Encargado del Tratamiento. Aunque se tenga claro esto, es necesario que exista un contrato que regule detalladamente las obligaciones y los límites en el tratamiento de los datos entre ambos, además de establecer todas las condiciones de la prestación del servicio de DRaaS.

A continuación, se enlistarán los puntos que deben tomarse en cuenta para la elaboración del contrato:

- El modelo de servicio contratado,
- El precio de servicio,
- El deber del proveedor enlistadas en el presente capítulo,
- La responsabilidad del proveedor sobre la información entregada por el cliente,
- Periodo de tiempo en el cual se prestará el servicio,

- Qué hacer con la información entregada al culminar la relación,
- Las penalidades por incumplimiento de contrato.

Al igual por normativa de la (SEPS, 2014), se requiere que se cumplan los siguientes puntos para una adecuada contratación de servicios:

- “Niveles mínimos de calidad del servicio,
  - Garantías técnicas y financieras, tales como:
    - Buen uso del anticipo,
    - Fiel cumplimiento del contrato, funcionamiento y disponibilidad del servicio,
  - Multas y penalizaciones por incumplimiento,
  - Personal suficiente y calificado para brindar el servicio,
  - Transferencia del conocimiento y entrega de documentación,
  - Confidencialidad de la información y datos,
  - Derechos de propiedad intelectual,
  - Definición del equipo contraparte y administrador del contrato,
  - Definición detallada de los productos y servicios a ser entregados,
  - Cumplimiento de las políticas de la entidad contratante,
  - Facilidades para la revisión y seguimiento del servicio prestado,
  - Metodologías para administrar los riesgos derivados de la contratación, particularmente de aquellos servicios identificados como críticos,
  - Políticas, procesos y procedimientos para un adecuado control y monitoreo de los servicios contratados, que incluyan como mínimo lo siguiente:
    - Evaluación y gestión del cumplimiento de los niveles mínimos de servicio,
    - Monitoreo de los riesgos inherentes, particularmente del riesgo operacional y legal, para lo cual deberán mantener una matriz de riesgos y evidencias de su gestión,
  - Contar con proveedores alternos de los servicios críticos
- Notificar a la SB de la contratación de proveedores del exterior, si se trata de procesos productivos y/o servicios críticos, así como la supervisión por

parte de la autoridad supervisora del país en el cual se brindará dicho servicio” (SEPS, 2014).

Del análisis normativo anterior, se desprende que existe viabilidad legal para la implementación del proyecto, considerando para ello los aspectos mencionados en las diferentes bases legales indicadas.

Sobre los diferentes aspectos evaluados durante el estudio de factibilidad, es necesario entregar un resumen ejecutivo y las recomendaciones para la implementación a la jefatura de IT, para su análisis y valoración, lo que será desarrollado en el capítulo V.

## **CAPÍTULO V**

### **RESULTADOS DEL ANÁLISIS**

#### **5.1 Introducción**

En el presente capítulo, se presenta un resumen ejecutivo de los resultados obtenidos del estudio de factibilidad técnica, operativa, económica – financiera, y legal del capítulo precedente, además de las recomendaciones para la implementación de la solución DRaaS, en el caso de encontrarse factible.

Alianza del Valle ha mostrado la apertura para entregar la mayor cantidad de información no sensible, sin embargo, dicha información se considera de carácter confidencial, es por esto que se reserva los derechos de autor sobre los datos provistos para la elaboración de los capítulos IV y V.

Dicho resumen será entregado a la Jefatura de IT para su análisis y valoración.

#### **5.2 Resultados**

Después de concluir con el análisis de factibilidad se ha obtenido los siguientes resultados.

##### **5.2.1 Aspectos Técnicos**

Para el análisis de los aspectos técnicos se consideró el crecimiento de los volúmenes de información impredecibles que tiene la Cooperativa Alianza del Valle para los próximos 5 años, con un 20 % anual para la solución In House y la solución en la nube, además se tomó en cuenta, que actualmente el almacenamiento de la data del sistema Core se encuentra en un 70% utilizado. Es por esto que para la solución In House se debió considerar la compra de un servidor nuevo de producción que soporte los requerimientos actuales, además la compra de un servidor de aplicaciones para que exista una replicación total de servicios.

Cabe recalcar que luego de los próximos 5 años se deberá volver a realizar una evaluación de capacidades para el incremento de las mismas si fuese el caso, lo que conllevaría a realizar nuevamente una inversión.

En el caso de la solución en la Nube es prácticamente transparente, ya que, si se requiere mayores capacidades, solo se solicitaría un crecimiento de los requerimientos del servicio contratado, por medio del hipervisor, recordando que la solución de DRaaS, ofrece el servicio de pago por uso.

Las características de capacidad del servicio solicitado, se determinaron mediante la sumatoria de las características del servidor de producción más el servidor de almacenamiento, al igual que el servidor de aplicaciones más el servidor de almacenamiento, como muestra en la Tabla 40.

Tabla 40. Capacidades Requeridas

NOMBRE	#vCPUs	MEMORIA (GB)	FORMATO (THIN, THICK, RAW)	CAPACIDAD HDD (INDIVIDUAL) GB	SISTEMA OPERATIVO INSTALADO	APLICACIONES INSTALADAS
MV1	2	32	RAW	500	Solaris 10	COBIS
MV2	2	32	RAW	4000	Solaris 11	Sybase 15.03
MV3	2	8	thin	105	Win Server 2008 R2 Standard	Gestión Página Transaccional
MV4	2	4	thin	470	Win2008 R2	Lavado de Activos
MV5	2	8	thin	340	Win2012 R2	Servicio para Cajeros automáticos, Autorizador
MV6	2	4	thin	120	Win Server 2003 Standard Edition SP2	SMS, Software de Mensajería, Mensajería masiva, Sismma
MV7	2	4	thin	96	Win Server 2008 R2 Standard SP1	Página web Transaccional
MV8	2	8	thin	209	Win2012 R2	Cardcontroller, Servicios Banred, Base de datos
MV9	2	4	thin	935	Win2008 R2	Servicios de Banred, Bono, Pago Directo, Cobis servidor Local NT
MV10	2	16	thin	417	Win Server 2012 R2 Standard	Bussinesintelligence/ bussines Objects
MV11	2	16	thin	500	Win Server 2012 R2 Standard	Bussinesintelligence/base de datos Oracle (servidor Físico)
MV12	2	16	thin	356	Win Server 2008 R2 Standard SP1	WorkFlow, aplicación
MV13	2	10	thin	736	Win Server 2008 R2 Standard	Workflow, para envío de correo

MV14	2	16	thin	266	Win Server 2012 R2 Standard	Servidor de huella
MV15	2	4	thin	44	Win Server 2008 R2 Standard SP1	Página web informativa

La empresa VMWare cuenta con la capacidad de soportar todos los requerimientos solicitados por la SEPS y Alianza del valle, además cuenta con la factibilidad de entregar el servicio solicitado, ya que soporta el sistema Solaris y puede implementar la arquitectura actual para el funcionamiento del Core Cobis.

### 5.2.2 Aspectos Operativos

Luego de realizar el estudio de factibilidad se encuentra que, para la implementación de este proyecto de innovación tecnológica, se cuenta con el aval del directorio (Consejo de Administración) para hacer uso de la infraestructura física y equipos existentes; además se dispone de los recursos humanos para la implementación de la solución, para lo cual el personal de la cooperativa “Alianza del Valle”, tiene muy en claro los beneficios que la solución propone.

Luego de realizar el comparativo entre la solución de fortalecimiento del sitio alterno actual (solución In House) y la propuesta de solución de recuperación ante desastres en la nube (DRaaS), se encontró que el proyecto es factible operativamente, ya que facilitará el monitoreo, administración y respuesta de los servidores virtualizados que se instalarán en la nube como recuperación ante desastres, evitando tiempos de inactividad que puedan derivar en costos imprevistos.

### 5.2.3 Aspectos Económicos

Los indicadores económicos – financieros para evaluación de proyectos nos ayudan a identificar si un proyecto resulta conveniente de implementar, es por esto que se analizó de manera independientemente el VAN y el TIR, para determinar la viabilidad y el rendimiento de estos proyectos, que en este caso son mutuamente excluyentes.

Luego del presente análisis se puede concluir que el proyecto de implementación del sitio alterno en la nube es el más económico ya que en la solución IN HOUSE, conlleva a una fuerte inversión inicial, además que se deben renovar equipos cada 5 años por normas institucionales y eso representaría volver a realizar dicha inversión. La solución DRaaS además resultó con una alta viabilidad económica, ya que los valores obtenidos del VAN y la TIR así lo demuestran.

#### **5.2.4 Aspectos Legales**

Al realizar el estudio de factibilidad, se encontró que existe una limitante para el análisis, al no contar con leyes, artículos o reglamentos referidos a la computación en la nube en la legislación ecuatoriana.

Es por esto que, para los aspectos legales, se considera de manera primordial realizar un acuerdo de nivel de servicio o SLA, donde deberá constar todas las pautas mencionadas en el capítulo IV, como los requisitos para la contratación del servicio y las obligaciones contractuales, además se debe tomar en cuenta las leyes vigentes en el Ecuador, igualmente citadas en el capítulo precedente, esto garantiza que los servicios se entreguen según lo acordado en el nivel de calidad.

Al suscribir un acuerdo de nivel de servicio, se podrán llegar a obtener los mayores beneficios siempre y cuando se tenga muy en claro las obligaciones mínimas de calidad, disponibilidad y continuidad del servicio, además de las penalidades que se derivan por incumplimiento del Acuerdo de Nivel de Servicio.

Se recomienda utilizar la referencia de contrato de servicios en la nube (*Cloud services*) de Oracle, que se puede visualizar en la referencia (Oracle, 2016).

### **5.3 Recomendaciones para la Implementación**

Alianza del Valle necesita estar preparado para lo inesperado con soluciones flexibles de recuperación ante desastres que se ajusten a sus necesidades y que sean seguras y de fácil administración; VMWare ha simplificado el proceso de la recuperación ante desastres, gracias a la virtualización de los recursos de TI, donde viaja la información de manera encriptada mediante algoritmos

patentados, a través de su nube pública, en esta solución son los discos virtuales los que se replican, impidiendo que la información sea expuesta, esto permite una mayor protección para todas las aplicaciones críticas.

Dado que se ha demostrado la viabilidad de la implementación de la recuperación ante desastres como servicio luego de realizar el estudio de factibilidad, es necesario presentar algunas recomendaciones que ayuden a la implementación de dicha solución según (Mark Broghammer, 2016), director de soluciones de ingeniería en iLand, líder de DRaaS según Gartner.

### Salto progresivo a la nube.

Para afrontar la migración a la nube de las aplicaciones críticas de la empresa es necesario hacerlo de manera progresiva, y con el asesoramiento de profesionales, migrar a la nube no es algo de todo o nada, se debe realizar una planificación en la que se migre primero las aplicaciones de prioridad 3 es decir de alta criticidad, pero sin su funcionamiento no afecta directamente a la continuidad de negocio, y con esto realizar una primera aproximación con una solución de prueba, que permita evidenciar su correcto funcionamiento y comprobar la facilidad de gestión y eficiencia de los recursos, para poder seguir con el resto de aplicaciones.

### Pruebas de carga

Uno realmente no tiene la seguridad de cómo va a funcionar una aplicación en la nube, es por esto que es necesario realizar pruebas de carga o las pruebas de rendimiento, así se puede probar una aplicación o aplicaciones con el número REAL de usuarios y transacciones.

### Monitoreo Proactivo

La gestión proactiva del rendimiento de la solución es de gran importancia para conocer sobre los problemas potenciales que puedan suscitarse, además se debe realizar pruebas de contexto cada cierto tiempo para verificar que la solución funcione y no esperar al momento del suceso de la falla.

## Gestión del Cambio

El paso a servicios en la nube, implica no solo migrar datos e infraestructura, sino una transformación en la vida operativa diaria de los usuarios y administradores, implica además un nuevo modelo de gestión y utilización de los sistemas informáticos, que afectarían a las personas, procesos y procedimientos de la cooperativa, es por esto que es importante, que para el uso de los servicios en la nube exista una adecuada gestión del cambio, para que esta implementación no sea difícil de asumir.

Durante la implementación, es necesario realizar un adecuado proceso de sensibilización, explicando las ventajas y las implicaciones para disminuir la ansiedad de las personas, además se requiere involucrar a los líderes de la organización, para que sean los facilitadores del cambio manteniendo una comunicación constante y clara.

## Plan de Recuperación ante desastres

Cabe recalcar que el DRaaS, es un servicio que ayudará al cumplimiento de los objetivos del plan de recuperación ante desastres, para esto, el plan debe estar correctamente elaborado y probado para que pueda garantizar la supervivencia de la cooperativa, además puede que requiera de modificaciones pese a su buen funcionamiento. Esto puede ocurrir cuando se producen cambios importantes en la propia organización, los cuales terminan afectando al RTO y RPO de la misma.

Dentro de este es importante que este muy claro los siguientes puntos:

- Inventario

Para partir en la elaboración del diseño de un Plan de Recuperación ante Desastres, se requiere realizar un inventario completo de todos los activos digitales de la cooperativa. De esa manera, serás capaz de valorar adecuadamente la complejidad y los riesgos presentes en el entorno IT. Se debe identificar detalladamente el hardware y software que intervienen en los procesos de la organización.

- Evaluar los riesgos

Luego del levantamiento del inventario, es conveniente determinar todas las amenazas internas o externas que pueden afectar a los equipos y sistemas, siendo este un proceso muy delicado ya que se debe calcular la probabilidad de que dichos sucesos tengan lugar y el impacto que éstos tendrían sobre el negocio.

- Criticidad de las aplicaciones

Es muy importante clasificar los sistemas de información según su criticidad, ya que es necesario conocer que tan críticos son para la continuidad de la actividad de la cooperativa.

- Objetivos de recuperación

Para esto es importante determinar el tiempo para la pérdida aceptable de datos o acceso a éstos (RPO, *Recovery Point Objectives*), es decir los puntos de restauración que se generan al realizar cada backup, esto está definido de acuerdo al criterio de criticidad de cada aplicación, por ejemplo, las aplicaciones más críticas deberán tener un RPO menor y las aplicaciones menos críticas un RPO mayor.

Además, se debe determinar el tiempo que se dispone para la ejecución de restauración de los servicios del negocio una vez que se ha declarado un desastre (RTO, *Recovery Time Objectives*), es decir el tiempo máximo que puede tomar levantar las aplicaciones críticas para el funcionamiento de la organización.

- Asignación de Roles y Responsabilidades

Se debe conocer claramente los roles involucrados y las responsabilidades que cada uno de ellos asume, al momento de levantarse una alerta de recuperación.

### 5.3.1 Solución Propuesta

Dentro de la arquitectura propuesta es necesario detallar los principales componentes que intervienen en la solución de DRaaS por parte de la empresa VMWare y son:

*VCloud Air Disaster Recovery* está basado en *vSphere Replication* que es el sistema de replicación de información y *vCloud Air* que es la nube de VMWare, *vSphere Replication* proporciona capacidades de replicación asíncronas y robustas en la capa del hipervisor, esto permite que las máquinas virtuales se configuren y se administren fácilmente (vmware, 2016).

*VCloud Air* es una plataforma escalable, de fácil crecimiento según los requerimientos ya sea creación de nuevas máquinas virtuales o mayor capacidad de almacenamiento u otras características. Es una nube segura y multi-tenant siendo capaz de apoyar a los casos de recuperación ante desastres, replicación, conmutación por error o *failover* y *failback* (vmware, 2016).

A continuación, se presenta la gráfica de la arquitectura propuesta:

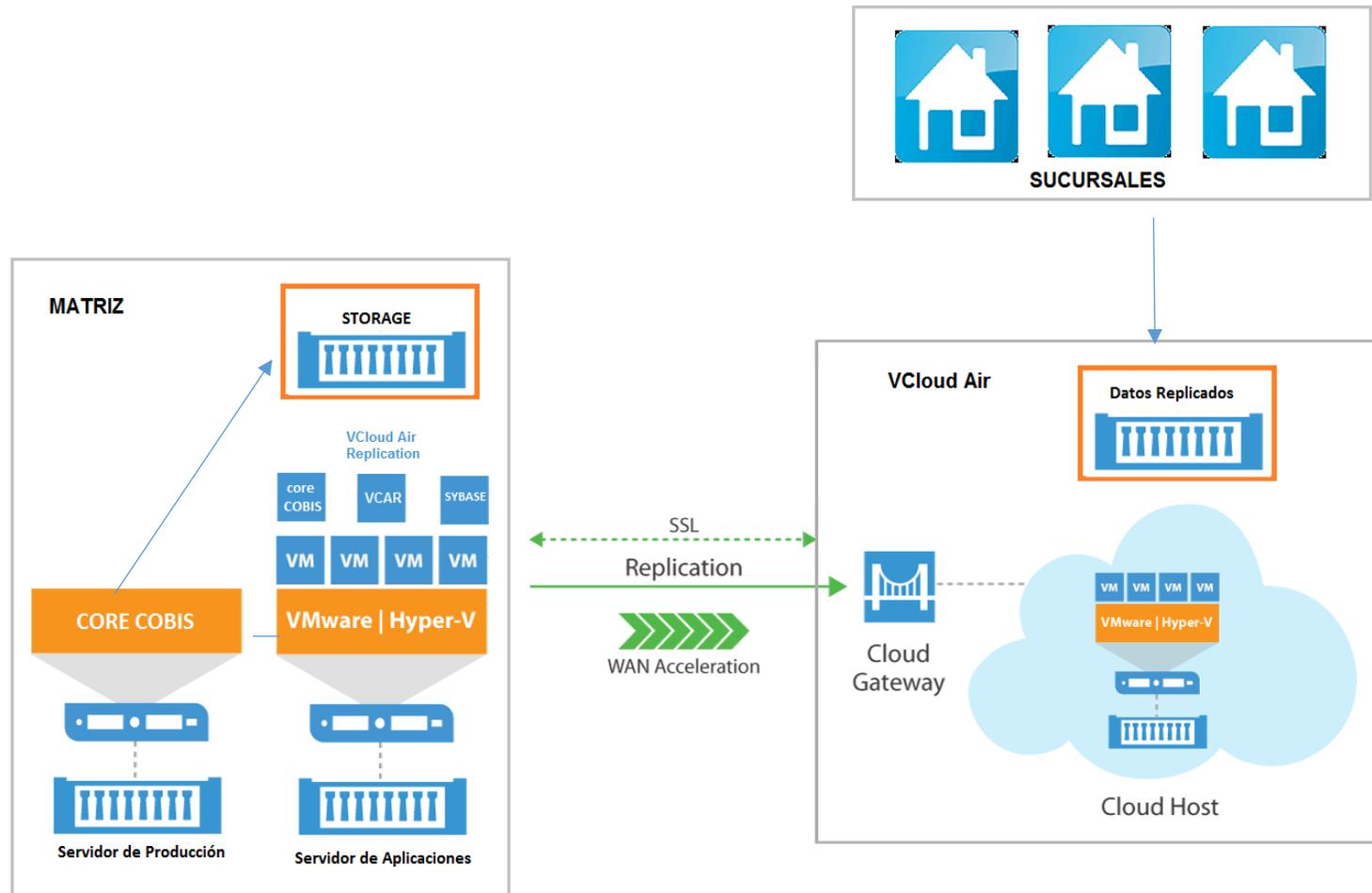


Figura 19. Recomendación de arquitectura

Dentro de la solución es necesario realizar los siguientes cambios por parte del departamento de IT de la cooperativa:

- Separar la base de datos SYBASE del servidor de producción a su propia máquina virtual para generar la replicación a *VCloud Air*.
- Crear una máquina virtual que cuente con el sistema operativo Solaris donde se encuentre instalado el core financiero COBIS, esta máquina se encontrará en estado de shutdown, y no se la replicará a menos que exista una actualización del código fuente y este será un proceso manual a cargo del personal de IT.
- Se sugiere esto, ya que, para que exista la replicación a *VCloud Air*, es necesario que toda la plataforma tecnológica de Alianza del Valle este virtualizada, y si se migra el core financiero COBIS a una máquina virtual puede verse afectado el performance del mismo.

Es decir, se contará con 2 equipos donde esté instalado el sistema core COBIS, uno de ellos es el servidor de producción actual y el segundo será una máquina virtualizada que solo se replicará cuando exista actualizaciones del sistema COBIS.

### **5.3.2 Mapa de Ruta para implementación**

Es importante contar con procedimientos de migración, según el ARTÍCULO 4 de las normas establecidas por la SEPS, donde explica que es necesario tener procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio, es por eso que se sugiere el siguiente mapa de ruta.

Esta sección define las horas previstas, actividades del proyecto y los resultados.

#### **5.3.2.1 Programación Estimada**

La empresa proveedora del servicio estima que la duración de este Proyecto no excederá las diez (10) semanas. Los servicios profesionales de la empresa contratada se realizarán de acuerdo a un calendario acordado por ambas partes. Típicamente, los servicios profesionales de implementación se llevan a cabo durante los días y horas normales laborables (lunes a viernes y los no festivos).

Además, se considerará el tiempo de migración de las aplicaciones físicas actuales a las virtuales, que no excederá los (5) días laborables, para este proceso también se podrá contar con la ayuda del proveedor del servicio.

### 5.3.2.2 Actividades del Proyecto

Las actividades para este Proyecto están organizadas en fases como se presenta en las siguientes ilustraciones.

Modo de	Nombre de tarea	Duración	Comienzo	Fin
	Rediseño - Adecuación	12 mss	mié 01/02/17	mar 02/01/18
	Planeamiento	5 días	mié 01/02/17	mar 07/02/17
	Kikoff	5 días	mié 08/02/17	mar 14/02/17
	Transferencia del conocimiento	53 días	mié 15/02/17	vie 28/04/17
	Evaluación	16 días	lun 20/02/17	lun 13/03/17
	Diseño	9 días	mar 14/03/17	vie 24/03/17
	Despliegue	11 días	lun 27/03/17	lun 10/04/17
	Validación	9 días	mar 11/04/17	vie 21/04/17
	Conclusión	5 días	lun 24/04/17	vie 28/04/17

Figura 20. Actividades del Proyecto

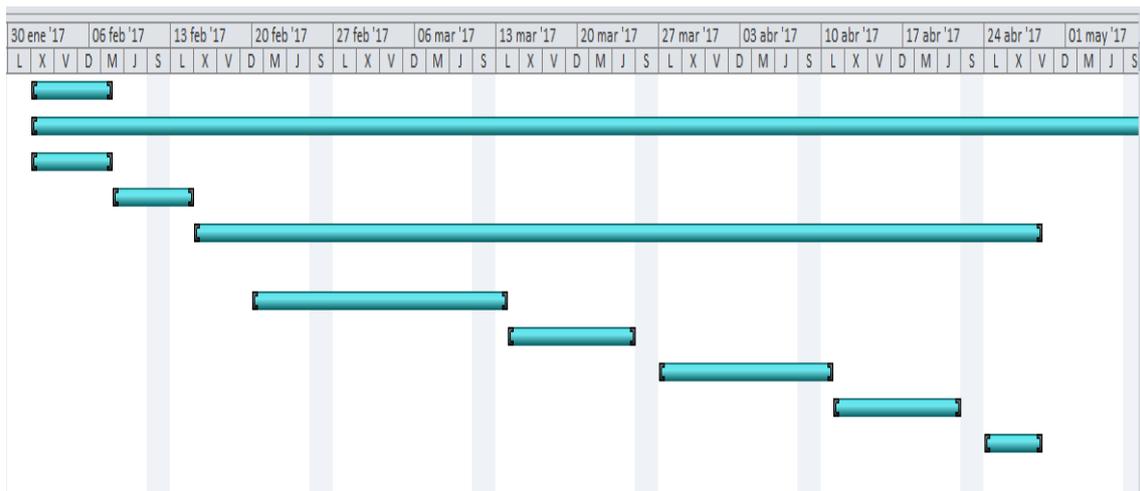


Figura 21. Diagrama de Gantt del Proyecto

### 5.3.2.3 Fase 1: Rediseño

En esta fase es importante realizar una medición de la capacidad de los procesos actuales de Alianza del Valle, ya que se requiere comprender el estado de los Procesos que Gestionan sus Sistemas de TI, con la finalidad de establecer el nivel de administración y control adecuado que debe proporcionar a sus Sistemas en esta implementación, y si deben ser rediseñados o mantenidos.

Además, es necesario conocer las posibles amenazas a considerarse para la migración de la plataforma, y cómo mitigarlas (Barreiro, 2016).

Es importante aclarar que puede utilizarse como referencia, los análisis realizados anteriormente, y que la adecuación de dichos procesos deberá llevarse a cabo en forma paralela a la implementación de DRaaS, como un plan para mitigar riesgos.

### 5.3.2.4 Fase 2: Planeamiento

Dentro de la planeación se deberán incluir los siguientes temas:

- Enfoque del Proyecto y objetivos,
- Plazo del Proyecto,
- Programación y logística,

- Identificar los principales miembros del equipo del Proyecto por parte de Alianza del Valle para trabajar con el equipo del proveedor del servicio.
- Identificar y acordar las fechas de finalización del proyecto.
- Generar un documento de *Checklist* de las actividades a ejecutarse. Esto incluye identificación de requerimientos de *hardware*, *software*, *networking*, y seguridad que se proporcionará por parte de Alianza del Valle para completar con éxito el diseño e implementación.
- Análisis del estado actual de la infraestructura física y virtual para registrar los datos de capacidad existente antes del inicio del proyecto.
- Disponibilidad de instalaciones apropiadas, incluyendo salas de reuniones, lugares de trabajo, pizarras, proyectores, las necesidades especiales de acceso, cualquier otra información pertinente necesaria antes de las reuniones previstas con la empresa proveedora del servicio.
- Requisitos previos y otra preparación necesaria antes del inicio del proyecto.

Para esta fase es importante contar con todos los instaladores de software, VMware vSphere, vSphere Replication, Solaris, Sybase y licencias en uso renovadas o adquiridas para el presente proyecto (Barreiro, 2016).

#### **5.3.2.5 Fase 3: *Kickoff* (Patada Inicial)**

Es necesario realizar una reunión inicial para establecer expectativas sobre el propósito del compromiso entre el proveedor y Alianza del Valle, los plazos, la cantidad de tiempo y esfuerzo que se requiere de los participantes, y las actividades previstas y entregables (Barreiro, 2016).

Los objetivos de la reunión son:

- Presentación del equipo que se encargará de la implementación por parte del proveedor del servicio, los roles y responsabilidades.
- Discusión de los objetivos del Proyecto y el propósito de la participación.
- Establecimiento de un plan de comunicación en el transcurso de la evaluación.
- Explicación de los entregables de compromiso previstos.

#### **5.3.2.6 Fase 4: Transferencia del conocimiento**

Es importante realizar una transferencia de conocimiento sobre el panorama de la solución, para introducir a los involucrados con el vocabulario y los conocimientos necesarios para discutir y tomar decisiones en todo el proceso de diseño.

La transferencia de conocimientos cubre fundamentos, nuevas funciones de vSphere, vSphere Replication, DRaaS, y la capa de gestión con un enfoque en escala de recursos, red, almacenamiento y dominios de seguridad. Además, se llevará a cabo durante todo el proceso para conocer los avances de la solución.

La asistencia de los principales representantes de la administración de servidores, red, almacenamiento y equipos de seguridad se considera obligatoria.

#### **5.3.2.7 Fase 5: Evaluación**

El proveedor de servicio deberá llevar a cabo una revisión de requerimientos, objetivos, requisitos empresariales y tecnológicos de Alianza del Valle, se deberá reunir los objetivos, políticas y restricciones que deben ser considerados en el diseño de la solución en la nube.

La fase de evaluación proporciona datos clave para el proceso de diseño sobre el actual entorno físico y virtual de Alianza del Valle y su utilización de recursos. A partir de este análisis, se verifica la utilización total de los servidores que se quiere migrar a la nube, capturar las variaciones cíclicas en la utilización de los recursos y así poder indicar un estimado de capacidades. Después de la recolección de los datos y el análisis de los resultados se culminará la fase de evaluación (Barreiro, 2016).

#### **5.3.2.8 Fase 6: Diseño**

En esta fase se evaluará el diseño de la solución propuesta por parte del proveedor de servicio, se podrá utilizar como referencia la arquitectura detallada anteriormente.

### **5.3.2.9 Fase 7: Despliegue**

Después de que el diseño de arquitectura está completo, se deberá identificar y acordar los puntos de pruebas y los resultados que definen un despliegue de una solución DRaaS exitosa.

Esta fase incluye lo siguiente:

- Alianza del Valle es responsable de las actividades de preparación de su infraestructura, ya detalladas con anterioridad, mientras que la empresa proveedora de servicios proporcionará asesoramiento técnico y seguimiento de los progresos.
- Construir y configurar el ambiente de replicación vsphere *Replication* de acuerdo a los documentos de diseño.
- Proporcionar adecuadas sesiones de transferencia de conocimiento técnicas y operativas.

### **5.3.2.10 Fase 8: Validación**

Durante esta fase, se realizará una validación del ambiente de replicación y la solución DRaaS. Esto incluye la ejecución de los casos de prueba acordados, previo a la entrega final de la solución.

### **5.3.2.11 Fase 9: Conclusión**

En esta fase se recibirán varios entregables por parte del proveedor del servicio de DRaaS, como por ejemplo un checklist de los requerimientos para la solución solventados, el diseño de Arquitectura, documento de configuración de la solución y los procedimientos de instalación, y un checklist de validación.

Esta recomendación de Mapa de ruta se realizó basándose en el mapa de ruta propuesto por la empresa proveedora del servicio.

## CAPÍTULO VI

### CONCLUSIONES Y RECOMENDACIONES

#### 6.1 Conclusiones

La computación en la nube se ha convertido en tendencia tecnológica en los últimos años, consolidándose como una nueva forma de prestación de servicios de negocio y tecnología; dado esto y que las empresas son cada vez más conscientes de que deben estar preparadas ante posibles desastres que afecten la continuidad de negocio, aparece la recuperación ante desastres como servicio en la nube, convirtiéndose en un componente primordial de un plan de recuperación ante desastres, que ofrece una protección total de datos y servicios a un menor costo.

Para una correcta migración a la nube y la utilización adecuada de sus servicios, en este caso DRaaS, se requiere de un profundo análisis de la situación actual de la Cooperativa, sus procesos críticos, los requerimientos para su funcionamiento actual, como se encuentra desarrollado el plan de recuperación ante desastres, las aplicaciones críticas, y conocer hacia donde se quiere llegar con este nuevo modelo, pero por sobre todo conocer cuáles son las amenazas que están dispuestos a asumir como Alianza del Valle para la implementación de este servicio.

Para el análisis de la situación actual, se cuenta con la guía para preparar los recursos de una empresa para la migración a la nube de *CloudTweaks*, reconocida autoridad en temas de computación en la nube, y COBIT 5, marco de gestión y de negocio global para el gobierno y la gestión de TI de la empresa, con los cuales se determinó la situación actual de Alianza del Valle, frente a la implementación de DRaaS.

Entre las diferentes opciones evaluadas, la selección de VMWare como proveedor del servicio de DRaaS para la implementación del sitio alterno, se

basó en el cumplimiento de varios aspectos, principalmente en Continuidad del Servicio, Confidencialidad de la información, Borrado de Información, Seguridad de la información, Propiedad Intelectual, Auditoría, Facilidad de Uso, Flexibilidad, Calidad de Soporte y Costo, además de ser el único proveedor que permite la implementación del Core COBIS en un ambiente virtualizado que soporte el sistema operativo donde corre únicamente este sistema financiero.

El uso de la solución en la NUBE de la empresa VMWare es factible técnicamente, ya que soporta el sistema operativo Solaris, y evita la estimación de recursos luego de un tiempo dado; es factible operativamente ya que facilitará el monitoreo, administración y respuesta de los servidores virtualizados al presentarse un incidente; es factible legalmente ya que actualmente no existen normativas que impidan la migración de datos a la nube de las entidades financieras y a través del contrato y los niveles de servicio acordados se cumplirá con los requisitos legales requeridos para administrar los servicios prestados por terceros; y por último, es factible económicamente ya que no se requiere de una fuerte inversión inicial en comparación con la solución IN HOUSE.

## **6.2 Recomendaciones**

Se recomienda que las cooperativas de ahorro y crédito en general, y en particular la Cooperativa “Alianza del Valle”, consideren la aplicación de un plan de recuperación de desastres como un servicio en la nube, que permitirá aprovechar las tendencias tecnológicas existentes para optimizar el uso de sus recursos y garantizar la continuidad del negocio a un menor costo.

Previo a la implementación de un plan de recuperación de desastres como servicio en la nube (DRaaS), se recomienda realizar un análisis detallado de la situación actual de la Cooperativa, que permita identificar de forma oportuna las brechas y debilidades que deben ser cubiertas en el proyecto, con lo cual se afianza una adecuada gestión de los riesgos y el éxito en la gestión del cambio.

Al ser de vital importancia para el proyecto el análisis de la situación actual de la institución, se recomienda utilizar marcos de trabajo y metodologías probadas, tales como la guía para preparar los recursos de una empresa para la migración

a la nube de *CloudTweaks*, y COBIT 5, con los cuales se gestionará la tecnología de una forma holística e integral, a la vez que se fomenta el buen gobierno corporativo de TI.

Del análisis de factibilidad realizado, se desprende que la mejor opción es la selección de VMWare como proveedor del servicio de DRaaS, en cuya contratación se recomienda considerar como imprescindible la existencia de cláusulas o normas que estipulen cuáles son las responsabilidades por parte del cliente y por parte del proveedor de servicio, que reafirmen con contundencia que el propietario de los datos es su titular y no la empresa o entidad que los trata, así como considerar los niveles de servicios que se requiere que cumpla el proveedor para garantizar el cumplimiento regulatorio así como la gestión del riesgo operativo y legal, lo cual beneficiaría a la Cooperativa de ahorro y crédito “Alianza del Valle”, no solo para el cumplimiento de los objetivos de su plan de recuperación ante desastres sino también generando un menor costo en el mismo.

Dado que se encontró factible el análisis para la implementación de recuperación ante desastres como servicio (DRaaS), es importante considerar la aplicación de algunas recomendaciones que ayuden a la puesta en marcha de esta solución, como lo son: salto progresivo a la nube, pruebas de carga, monitoreo proactivo y gestión del cambio, que ayudarán al éxito de la propuesta.

Por último, es importante que para la implementación de DRaaS, se cuente con la aprobación y compromiso del Consejo de Administración de la Cooperativa, con lo cual se garantizará la provisión del presupuesto y recursos requeridos para el proyecto así como la demostración de que es posible reducir los costos y mitigar los riesgos tecnológicos cuando se hace un uso óptimo de las nuevas tecnologías, de forma controlada y administrada, tal como se ha comprobado con el presente análisis de factibilidad.

## REFERENCIAS

- AdderGlobal, 2016. *Porque la informacion es el activo más importante de tu empresa backup online*. Recuperado el 07 de julio de 2016, de <https://www.adderglobal.com/porque-la-informacion-es-el-activo-mas-importante-de-tu-empresa-backup-online/>
- Alianza del Valle, 2016. *Alianza del Valle*. Recuperado el 06 de agosto de 2016, de <http://www.alianzadelvalle.fin.ec/>
- Aspectos Profesionales, 2012. *DRaaS*. Recuperado el 06 de julio de 2016, de <http://www.aspectosprofesionales.info/2012/11/draas-la-recuperacion-de-desastres-como.html>
- Bacca G., 2013. *Disaster Recovery como Servicio (DRaaS)*. Recuperado el 10 de agosto de 2016, de <http://www.germanbacca.com/disaster-recovery-como-servicio-draas/>
- Barahona J., 2016. *Recuperación de desastres en la nube*. Recuperado el 12 de julio del 2016, de <http://www.acis.org.co/portal/content/la-recuperaci%C3%B3n-de-desastres-en-la-nube-%C2%BFuna-necesidad-o-un-mito>
- BBVA Innovation Center, 2015. *Las tres claves de los sistemas de seguridad en la nube*. Recuperado el 13 de agosto del 2016, de <http://www.centrodeinnovacionbbva.com/noticias/las-tres-claves-de-los-sistemas-de-seguridad-en-la-nube>
- Broghammer M., 2016. *Recomendaciones para migrar a la nube*. Recupeado el 4 de julio, de <http://www.iland.com/services/cloud-disaster-recovery/>
- Cadena A., & Barros G., 2011. *Academia*. Recuperado el 13 de julio del 2016, de [https://www.academia.edu/12588532/CAP%C3%8DTULO\\_III\\_Estudio\\_d](https://www.academia.edu/12588532/CAP%C3%8DTULO_III_Estudio_d)

el\_modelo\_COBIT\_en\_la\_Cooperativa\_de\_Ahorro\_y\_Cr%C3%A9dito\_Al  
ianza\_del\_Valle\_

CloudTweaks, 2011. *El desarrollo de una estrategia de migración a la nube*. Recuperado el 16 de agosto de 2016, de <http://cloudtweaks.com/2011/06/to-the-cloud-developing-cloud-migration-strategy/>

Colom J., 2012. *DRaaS*. Recuperado el 3 de agosto de 2016, de <http://www.aspectosprofesionales.info/2012/11/draas-la-recuperacion-de-desastres-como.html>

Congreso Nacional, 2016. *LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS*. Recuperado el 18 de septiembre de 2016, de [http://www.redipd.org/legislacion/common/legislacion/ecuador/ecuador\\_ley\\_2002-67\\_17042002\\_comelectronico.pdf](http://www.redipd.org/legislacion/common/legislacion/ecuador/ecuador_ley_2002-67_17042002_comelectronico.pdf)

Coronel K., 2016. *Taller Cobit*. Recuperado el 4 de diciembre de 2016, de <http://www2.udla.edu.ec/>

Corporation A. U., 2014. *CIOs Are Moving More Organizational Information into the Cloud Even as Security Concerns Persist*. Recuperado el 11 de agosto del 2016, de <http://www.unisys.com.mx/news/News%20Release/CIOs-Are-Moving-More-Organizational-Information-into-the-Cloud-Even-as-Security-Concerns-Persist-Unisys-Research-Reveals>

Devicrow, 2016. *IaaS, PaaS, SaaS*. Recuperado el 5 de noviembre de 2016, de <http://www.devicrow.es/iaas-paas-saas/147-saas>

Doña J., & García J., 2014. *Virtualización de servicio*. Recuperado el 2 de noviembre de 2016, de <https://es.scribd.com/document/37592124/Virtualizacion-Servidores>

- Duarte L., 2015. *Computación en la Nube*. Recuperado el 3 de noviembre de 2016, de <https://sites.google.com/site/nubeduarteluis/unidad-iii-modelos-para-computacion-en-la-nube-para-los-servicios/3-1-nube-publica>
- ECloud, 2015. *Recuperación ante desastres en el Cloud*. Recuperado el 3 de agosto de 2016, de <http://evaluandocloud.com/recuperacion-ante-desastres-en-el-Cloud/>
- ENISA, 2014. *Buenas prácticas en materia de contratación de servicios de computación en la nube*. Recuperado el 2 de agosto de 2016, de [http://www.guiadigital.gob.cl/sites/default/files/2014\\_02\\_28\\_GuiaCloud\\_v1.0.pdf](http://www.guiadigital.gob.cl/sites/default/files/2014_02_28_GuiaCloud_v1.0.pdf)
- FASTCLOUD, 2016. *Evaluación de la computación en la Nube*. Recuperado el 15 de noviembre de 2016, de <http://www.fastcloud.org/Evolution.php>
- Gartner, 2012. *platform as a service paas*. Recuperado el 14 de noviembre de 2016, de <http://www.gartner.com/it-glossary/platform-as-a-service-paas/>
- Gartner, 2012. *Software as a service saas*. Recuperado el 14 de noviembre de 2016, de <http://www.gartner.com/it-glossary/software-as-a-service-saas/>
- Gartner, 2016. *Cloud Computing*. Recuperado el 14 de noviembre de 2016, de <http://www.gartner.com/it-glossary/cloud-computing/>
- Gartner, 2016. *Cuadrante Mágico para la recuperación de desastres como servicio*. Recuperado el 14 de diciembre de 2016, de <https://www.gartner.com/doc/reprints%3Fct%3D160617%26id%3D1-39NNEX2%26st%3Dsb&prev=search>
- Gartner, 2014. *Disaster Recovery*. Recuperado el 11 de agosto de 2016, de <https://www.gartner.com/doc/2877120/use-avoid-disaster-recovery-service>

- Bacca G., & Innovation Consultant, 2013. *Recuperación de desastres como servicio*. Recuperado el 11 de julio de 2016, de <http://www.germanbacca.com/disaster-recovery-como-servicio-draas/>
- Girsanet, 2016. *Virtualización de servidores*. Recuperado el 7 de agosto de 2016, de [http://www.girsanet.com/productos\\_servicios/virtualizacion-de-servidores/](http://www.girsanet.com/productos_servicios/virtualizacion-de-servidores/)
- Greenhouse, 2016. *Draas*. Recuperado el 11 de noviembre de 2016, de <https://www.swgreenhouse.com/double-take/entornos/draas>
- Grupo trevenque, 2016. *Virtualización de almacenamiento*. Recuperado el 2 de noviembre de 2016, de <http://sistemas.trevenque.es/soluciones/virtualizacion-almacenamiento/>
- HP, 2011. *Recovery Remote*. Recuperado el 4 de diciembre de 2016, de <http://hp.com/support/manuals>
- IBM, 2016. *¿Qué es la nube?*. Recuperado el 7 de diciembre de 2016, de <http://www.ibm.com/cloud-computing/mx/es/what-is-cloud-computing.html>
- IBM, 2016. *DRaaS IBM*. Recuperado el 7 de diciembre de 2016, de <http://www-935.ibm.com/services/ec/es/it-services/business-continuity/cloud-server-recovery/index.html>
- ICESI, 2015. *Herramienta de apoyo para valorar la adopción efectiva de Cloud Computing en una organización*. Recuperado el 21 de diciembre de 2016, de [https://repository.icesi.edu.co/biblioteca\\_digital/bitstream/10906/68425/1/herramienta\\_apoyo\\_valorar.pdf](https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/68425/1/herramienta_apoyo_valorar.pdf)
- INTECO-CERT, 2011. *Riesgos y amenazas en cloud computing*. Recuperado el 27 de diciembre de 2016, de [https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_riesgos\\_y\\_amenazas\\_en\\_cloud\\_computing.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf)

Interoute, 2016. *What Is SaaS*. Recuperado el 23 de diciembre de 2016, de <http://www.interoute.es/what-saas>

ISACA, 2013. *COBIT 5*. Recuperado el 2 de agosto de 2016, de [https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjeysq8KbRAhWFwiYKHV1EBsoQFggqMAM&url=https%3A%2F%2Fwww.isaca.org%2FCOBIT%2FDocuments%2FCOBIT5-and-GRC\\_Espanol.ppt&usg=AFQjCNGGN6E0bKO5BvUo\\_-CbF1XqbQvZdA&sig2=Als](https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjeysq8KbRAhWFwiYKHV1EBsoQFggqMAM&url=https%3A%2F%2Fwww.isaca.org%2FCOBIT%2FDocuments%2FCOBIT5-and-GRC_Espanol.ppt&usg=AFQjCNGGN6E0bKO5BvUo_-CbF1XqbQvZdA&sig2=Als)

Mercuriana, 2016. *DraaS*. Recuperado el 3 de diciembre de 2016, de <http://www.mercuriana.es/servicios/draas/>

Mercuriana, 2016. *Recuperación de desastres como servicio*. Recuperado el 3 de diciembre de 2016, de <http://www.mercuriana.es/servicios/draas/>

Microsoft, 2016. *DRaaS Microsoft*. Recuperado el 3 de diciembre de 2016, <https://azure.microsoft.com/en-us/services/site-recovery/>

Microsoft, 2016. *Productos y tecnologías de virtualización*. Recuperado el 3 de diciembre de 2016, de <https://www.microsoft.com/spain/virtualizacion/products/server/default.mspx>

Miranda J., 2016. *¿Qué es el estudio de factibilidad en un proyecto?*. Recuperado el 4 de agosto de 2016, de <http://www.gestiopolis.com/que-es-el-estudio-de-factibilidad-en-un-proyecto/>

Nieto B., 2015. *Diseño para la implementación de un plan de recuperación ante desastres*. Recuperado el 14 de septiembre del 2016, de <http://dspace.ups.edu.ec/bitstream/123456789/10303/1/UPS-GT001200.pdf>

NIST, 2012. *Aspectos Legales de la nube*. Recuperado el 19 de diciembre de 2016, de

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf>

NIST, 2012. *Cloud Computing Synopsis*. Recuperado el 14 de noviembre de 2016, de <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf>

NTT Communications, 2016. *Drass*. Recuperado el 3 de noviembre de 2016, de <http://www.us.ntt.com/en/services/cloud/disaster-recovery-as-a-service.html>

Oracle, 2016. *Contrato de servicios en la Nube*. Recuperado el 25 de diciembre de 2016, de <http://www.oracle.com/us/corporate/contracts/saas-csa-chile-2069241.pdf>

Peter M., & Grance T., 2011. *Definition of Cloud Computing*. Recuperado el 2 de agosto de 2016, de <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Revista MyM, 2015. *La recuperacion de desastre en la nube una necesidad o un mito*. Recuperado el 20 de agosto de 2016, de <http://www.revistamym.com/2015/09/la-recuperacion-de-desastre-en-la-nube-una-necesidad-o-un-mito/>

Saraha A., 2014. *Virtualization vs. Cloud Computing: What's the Difference?* Recuperado el 3 de agosto de 2016, de <http://www.businessnewsdaily.com/5791-virtualization-vs-cloud-computing.html>

SEPS, 2014. *Normas generales para las instituciones del sistema financiero*. Recuperado el 21 de agosto de 2016, de [http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva\\_codificacion/todos/L1\\_X\\_cap\\_V.pdf](http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf)

Venkata J., & Malcom O., 2011. *Recuperación ante desastres*. Recuperado el 30 de diciembre de 2016, de [https://books.google.com.ec/books?id=TebnXjv62\\_wC&hl=es](https://books.google.com.ec/books?id=TebnXjv62_wC&hl=es)

Vmware, 2016. *Soluciones Virtuales*. Recuperado el 20 de septiembre de 2016, de <https://www.vmware.com/cl/products/vsphere/features/virtual-volumes>

Weller A., 2013. *Tipos de Computación en la Nube*. Recuperado el 24 de septiembre de 2016, de <https://www.crucial.com.au/blog/2013/05/27/types-of-Cloud-Computing/>

## **ANEXOS**

## **ANEXO 1. Glosario de Términos**

**Nist:** Instituto Nacional de Normas y Tecnología es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos, su misión es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

**CloudTweaks:** es una industria líder en la información de computación en la nube y recursos tecnológicos. Establecido en 2009 y con sede en Montreal, Canadá.

**ISO 31000** es el estándar internacional que se ocupa de la gestión de riesgos de manera genérica.

**ISO 27005** es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información

**RTO:** Es el tiempo que toma reanudar el servicio una vez producido el desastre, durante este tiempo se aplicarán los protocolos establecidos en el plan de contingencia.

**RPO:** Se refiere a la vigencia del dato que se puede recuperar y viene dado por el tiempo desde la última copia o réplica de la información.

**CSA:** La *Cloud Security Alliance* se define como una organización internacional sin ánimo de lucro para promover el uso de mejores prácticas para garantizar la seguridad en la Nube.

**ENISA:** Agencia Europea de Seguridad de las Redes y de la Información.

**SEPS:** Superintendencia de la economía popular y solidaria.

**Hipervisor:** Es el monitor de la máquina virtual que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.

## ANEXO 2. Procesos Críticos y No Críticos de Alianza del Valle

Tabla 41. Procesos Críticos y No críticos de Alianza del Valle

TIPO DE PROCESO	MACROPROCESO	PROCESO		SUBPROCESO		IMPACTO					
		CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	RENTABILIDAD	CONTINUIDAD DEL NEGOCIO	SATISFACCIÓN DEL SOCIO/CLIENTE	OBJETIVOS INSTITUCIONALES	PROMEDIO	CRÍTICO / NO CRÍTICO
Estratégicos	PIN - Planificación Institucional	PIN-01	Planificación Estratégica			5,00	4,00	2,00	5,00	4,00	Crítico
		PIN-02	Planificación Operativa			4,00	5,00	3,00	5,00	4,00	Crítico
	GIN - Gestión Institucional	GIN-01	Flujo de Información Institucional	GIN-01-01	Flujo de Información para Organismos de Control	2,00	5,00	3,00	4,00	4,00	Crítico
				GIN-01-02	Flujo de Información Interna	3,00	3,00	2,00	4,00	3,00	No Crítico
				GIN-01-03	Flujo de Información para Asambleístas, Directivos, Socios	1,00	2,00	2,00	2,00	2,00	No Crítico
		GIN-02	Prevención y Control de Lavado de Activos	GIN-02-01	Prevención y Control de Lavado de Activos	2,00	5,00	2,00	5,00	4,00	Crítico
		GIN-03	Administración de Accesos al Sistema Cobis	GIN-03-01	Administración de Accesos al Sistema Cobis y Programas Aplicativos	2,00	5,00	4,00	3,00	4,00	Crítico

	GPR - Gestión por Procesos	GPR-01	Administración y Control de Documentos	GPR-01-01	Administración y Control de Documentos	1,00	2,00	1,00	2,00	2,00	No Crítico
		GPR-02	Difusión y Comunicación	GPR-02-01	Difusión y Comunicación	1,00	2,00	2,00	1,00	2,00	No Crítico
		GPR-03	Control de Políticas y Procedimientos	GPR-03-01	Control de Políticas y Procedimientos	2,00	2,00	4,00	3,00	3,00	No Crítico
Productivos	GAC - Gestión de Servicio al Cliente	GAC-01	Administrar la Mesa de Servicios y los Incidentes	GAC-01-01	Mesa de Servicios	1,00	2,00	3,00	2,00	2,00	No Crítico
				GAC-01-02	Registro de Consultas de Clientes	1,00	2,00	3,00	2,00	2,00	No Crítico
				GAC-01-03	Escalamiento de Incidentes	1,00	2,00	4,00	2,00	2,00	No Crítico
				GAC-01-04	Cierre de Incidentes	1,00	1,00	3,00	2,00	2,00	No Crítico

		GAC-01-05	Análisis de Tendencias	1,00	1,00	3,00	2,00	2,00	No Crítico		
		GAC-02	Gestión de Quejas y Reclamos	GAC-02-01	Medición del Servicio	2,00	4,00	4,00	4,00	4,00	Crítico
	CRE - Gestión Comercial	CRE-01	Crédito de Consumo / Vivienda	CRE-01-01	Crédito de Consumo	4,00	4,00	5,00	4,00	4,00	Crítico
		COB-01	Análisis de Oportunidades	COB-01-01	Cobranza Preventiva	4,00	3,00	2,00	4,00	3,00	No Crítico
	COB - Gestión Comercial	COB-02	Elaboración de ofertas económicas	COB-02-01	Cobranza Extrajudicial	4,00	4,00	3,00	4,00	4,00	Crítico
		COB-03	Mantenimiento de Clientes	COB-03-01	Cobranza Judicial	2,00	3,00	1,00	3,00	2,00	No Crítico

APOYO		GFI-02	Gestión Financiera	GFI-02-02	Elaboración de Estados Financieros	1,00	3,00	1,00	2,00	2,00	No Crítico
				GFI-02-03	Gestión Tributaria	1,00	4,00	1,00	2,00	2,00	No Crítico
				GFI-02-04	Gestión Contable	1,00	3,00	1,00	2,00	2,00	No Crítico
		GFI-03	Gestión Tesorería	GFI-03-01	Gestión de Flujo de Caja	2,00	3,00	2,00	3,00	3,00	No Crítico
				GFI-03-04	Administración de Tarjetas de Crédito y Cuentas Bancarias	1,00	2,00	1,00	2,00	2,00	No Crítico
				GFI-03-05	Reportes a Organismos de Control	1,00	4,00	1,00	2,00	2,00	No Crítico
	GAD - Gestión Administrativa	GAD-01	Gestión de Adquisiciones	GAD-01-01	Calificación y selección de Proveedores	1,00	1,00	1,00	1,00	1,00	No Crítico
						1,00	1,00	1,00	1,00	1,00	Crítico

GRH - Gestión de Recursos Humanos	GRH-01	Gestión de Recursos Humanos	GRH-01-01	Selección de Personal	1,00	4,00	5,00	4,00	4,00	Crítico	
			GRH-01-02	Permanencia del Recurso Humano	1,00	2,00	1,00	2,00	2,00	No Crítico	
			GRH-01-03	Desvinculación del Recurso Humano	1,00	1,00	1,00	1,00	1,00	No Crítico	
	JIT - Gestión de Informática y Tecnología	GIT-01	Planificación y Control	GIT-01-01	Planificación y Control	1,00	3,00	1,00	3,00	2,00	No Crítico
		GIT-02	Soporte IT	GIT-02-01	Soporte Interno	1,00	5,00	4,00	4,00	4,00	Crítico
GIT-03		Gestión y Desarrollo de Software	GIT-03-01	Desarrollo de Software	1,00	2,00	3,00	3,00	2,00	No Crítico	
	GIT-03-02		Respaldos de Información	1,00	3,00	2,00	5,00	3,00	No Crítico		
GIT-03-03	Adquisición de Software o Servicios de Software	2,00	3,00	2,00	4,00	3,00	No Crítico				

				GIT-03-05	Calidad de Software	3,00	4,00	4,00	2,00	3,00	No Crítico
				GIT-03-06	Gestión de IT	5,00	4,00	3,00	4,00	4,00	Crítico

Tomado de (Alianza del Valle, 2016)

### ANEXO 3. Evaluación de Procesos de acuerdo a la Guía de Referencia de Procesos de COBIT 5

Para la realización de las preguntas, se ha tomado como referencia las actividades que deben cumplirse en cada proceso de COBIT 5.

Tabla 42. Evaluación de Procesos – Encuesta

PREGUNTAS	No existe	Incompleto	Gestionado	Establecido	Predecible	Optimo
<b>DSS04.1 definir la política de continuidad del negocio, objetivos y alcance.</b>						
¿Se han identificado los procesos de negocio internos y subcontratados y actividades de servicio que son críticos para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales?					x	
¿Se han identificado las partes interesadas clave y los roles y responsabilidades para definir y acordar la política de continuidad y su alcance?				x		
<b>DSS04.2 Mantener una estrategia de continuidad.</b>						
¿Se ha identificado los escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes?				x		
¿Se ha realizado un análisis de impacto en el negocio para evaluar el impacto en tiempo de una interrupción en funciones críticas del negocio y el efecto que tendría en ellas?				x		

<b>DSS04.2 Mantener una estrategia de continuidad.</b>						
¿Se ha identificado los escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes?				x		
¿Se ha realizado un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas del negocio y el efecto que tendría en ellas?				x		
¿Se ha establecido el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable??				x		
¿Se ha analizado la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio y se ha identificado medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia?				x		
¿Se ha analizado los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas?				x		
<b>DSS04.3 Desarrollar e implementar una respuesta a la continuidad del negocio.</b>						
¿Se ha desarrollado y se ha mantenido los planes de continuidad de negocio operativos que contienen los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de proceso, incluyendo enlaces a los planes de proveedores de servicio externalizados?						x



<p>¿Se define y se mantiene los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes? ¿Se asegura que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación? RR.HH.</p>			x			
<p><b>DSS04.7 Gestionar acuerdos de respaldo / DS04.9 Almacenamiento de Respaldos Fuera de las instalaciones</b></p>						
<p>¿Se realizan copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida?</p>				x		
<p>¿Se ha distribuido los planes y la documentación de soporte de modo seguro a las partes interesadas y apropiadamente autorizadas y asegurar que estén accesibles en escenarios de desastre?</p>			x			
<p>¿Se han hecho copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo con una planificación definida?</p>				x		
<p>¿Se ha asegurado que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma? Considerar el hecho de requerir el retomo de las copias de seguridad de terceras partes.?</p>			x			

¿Se ha definido los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio? ¿Considerar la accesibilidad requerida a las copias de seguridad?			x			
¿Se ha probado y mantenido legible las copias de seguridad y las archivadas periódicamente??			x			
<b>DSS04.8 Recuperación y Reanudación de los Servicios de TI. / DSS04.10 Revisión Post Reanudación.</b>						
¿Se han planificado ejercicios y actividades de prueba tal como está definido en el plan de continuidad?			x			
¿Se ha realizado un análisis y revisión post-ejercicio para considerar el logro?			x			
¿Se ha determinado la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a Incidentes, infraestructura técnica y estructuras organizativas y relaciones?		x				
¿Se han identificado debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora?		x				
¿Se ha obtenido la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la empresa?			x			
<b>Contabilización</b>			<b>2</b>	<b>10</b>	<b>11</b>	

Adaptado de (ISACA, 2013)

## ANEXO 4 - Procesos COBIT 5

Tabla 43. Procesos Cobit 5

<b>EDM01</b>	<b>Asegurar la configuración y mantenimientos de un marco de Gobierno</b>
EDM01.02	Dirigir el sistema de gobierno
<b>EDM02</b>	<b>Asegurar la entrega de beneficios</b>
EDM02.03	Monitorear la optimización de valor
<b>EDM03</b>	<b>Asegurar la Optimización de Riesgos</b>
EDM03.01	Evaluar la gestión de riesgos
EDM03.02	Dirigir la gestión de riesgos
<b>APO01</b>	<b>Gestión del marco de gestión de TI</b>
APO01.07	Gestionar la mejora continua de los procesos
<b>APO02</b>	<b>Gestión de la Estrategia</b>
APO02.01	Entender la dirección de la organización
APO02.02	Evaluar el ambiente actual, capacidades y rendimiento
APO02.03	Definir el objetivo de las capacidades de TI
<b>APO03</b>	<b>Gestión de Arquitectura Empresarial</b>
APO03.03	Seleccionar oportunidades y soluciones
<b>APO05</b>	<b>Gestión del Portafolio</b>
APO05.06	Gestionar el logro de beneficios
<b>APO06</b>	<b>Gestión de Costos y Presupuestos</b>
APO06.02	Dar prioridad a la asignación de recursos
APO06.03	Crear y mantener los presupuestos
<b>APO07</b>	<b>Gestión de Recursos Humanos</b>
APO07.01	Mantener un adecuado y apropiado personal de apoyo
APO07.02	Identificar personal de TI clave
APO07.03	Mantener las habilidades y competencias del personal
<b>APO08</b>	<b>Gestión de las relaciones</b>
APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio
<b>APO09</b>	<b>Gestión de acuerdos de servicios</b>

APO09.01	Identificar los servicios de TI
APO09.02	Catálogo de servicios de TI habilitados
APO09.03	Definir y preparar los acuerdos de servicio
<b>APO10</b>	<b>Gestión de Proveedores</b>
APO10.02	Seleccionar a los proveedores
APO10.03	Gestionar las relaciones con proveedores y contratos
<b>APO11</b>	<b>Gestión de la Calidad</b>
APO11.02	Definir y gestionar los estándares de calidad, prácticas y procedimientos
<b>APO12</b>	<b>Gestión del riesgo</b>
APO12.02	Análisis de riesgo
APO12.03	Mantener un perfil de riesgo
APO12.04	Articular riesgo
<b>APO13</b>	<b>Gestión de la seguridad</b>
APO13.01	Establecer y mantener un SGSI
<b>BAI01</b>	<b>Gestión de Programas y Proyectos</b>
BAI01.07	Colocar en marcha e iniciar los proyectos dentro del programa
BAI01.08	Planear los Proyectos
<b>BAI02</b>	<b>Gestión de la definición de los requerimientos</b>
BAI02.02	Realizar un estudio de factibilidad y formular soluciones alternativas
BAI02.03	Gestionar el riesgo de los requerimientos
<b>BAI03</b>	<b>Gestión de la identificación y construcción de soluciones</b>
BAI03.06	Realizar control de calidad
BAI03.09	Gestionar los cambios en los requerimientos
BAI03.11	Definir los servicios de TI y mantener un portafolio de servicios
<b>BAI04</b>	<b>Gestión de Disponibilidad y Capacidad</b>
BAI04.02	Evaluar el impacto en los negocios
BAI04.03	Planear los requerimientos de servicios nuevos o modificados
<b>BAI05</b>	<b>Gestión del Cambio Organizacional</b>
BAI05.01	Establecer el deseo de cambiar
BAI05.04	Empoderar el rol de los jugadores e identificar las metas a corto plazo
<b>BAI06</b>	<b>Gestión de Cambios</b>
BAI06.01	Evaluar, priorizar y autorizar las solicitudes de cambio
BAI06.02	Gestionar los cambios de emergencia
BAI06.03	Realizar un seguimiento y reportar los estados de los cambios
<b>BAI07</b>	<b>Gestión de la aceptación y transición al cambio</b>
BAI07.01	Establecer un plan de implementación
BAI07.03	Plan de pruebas de aceptación
BAI07.04	Establecer un entorno de pruebas
BAI07.05	Realizar pruebas de aceptación

<b>BAI08</b>	<b>Gestión del conocimiento</b>
BAI08.01	Nutrir y facilitar una cultura de conocimiento compartido
BAI08.02	Identificar y clasificar las fuentes de información
BAI08.03	Organizar y contextualizar la información en conocimiento
BAI08.04	Utilizar y compartir conocimientos
<b>DSS01</b>	<b>Gestión de Operaciones</b>
DSS01.01	Realizar los procedimientos operativos
DSS01.02	Gestión de los servicios de TI tercerizados
DSS01.03	Monitorear la infraestructura de TI
<b>DSS03</b>	<b>Gestión de Problemas</b>
DSS03.01	Identificar y clasificar los problemas
DSS03.02	Investigar y diagnosticar problemas
DSS03.03	Elevar los errores conocidos
DSS03.04	Resolver problemas y cerrarlos
<b>DSS04</b>	<b>Gestión de la Continuidad</b>
DSS04.01	Definir la política de continuidad del negocio, objetivos y ámbito de aplicación
DSS04.02	Mantener una estrategia de continuidad
DSS04.03	Desarrollar e implementar una respuesta a la continuidad del negocio
DSS04.05	Revisar, mantener y mejorar el plan de continuidad
DSS04.06	Organizar cursos de capacitación de plan de continuidad
DSS04.07	Gestión de los acuerdos de copias de seguridad
<b>DSS05</b>	<b>Gestión de Servicios de Seguridad</b>
DSS05.02	Gestión de la seguridad de la red y la conectividad
DSS05.04	Gestión de la identidad de usuarios y acceso lógico
DSS05.05	Gestión del acceso físico a los activos de TI
<b>DSS06</b>	<b>Gestión de controles en los procesos de negocio</b>
DSS06.01	Alinear las actividades de control integradas en los procesos del negocio con los objetivos de la organización
DSS06.02	Controlar el procesamiento de la información
DSS06.06	Asegure los activos de información
<b>MEA01</b>	<b>Monitorear, evaluar y valorar el desempeño y la conformidad</b>
MEA01.01	Establecer un enfoque de supervisión
<b>MEA02</b>	<b>Monitorear, evaluar y valorar el Sistema de Control Interno</b>
MEA02.01	Supervisar los controles internos
MEA02.02	Revisión efectiva de los controles de los procesos del negocio
MEA02.03	Realizar el control de auto-evaluaciones
<b>MEA03</b>	<b>Monitorear, evaluar y valorar el cumplimiento de los requisitos externos</b>
MEA03.01	Identificar los requisitos externos de cumplimiento
MEA03.02	Optimizar la respuesta a los requerimientos externos

Adaptado de (ISACA, 2013)