IMPLEMENTACIÓN DEL MODELO DISASTER RECOVERY AS A SERVICE - DRAAS PARA LA INFRAESTRUCTURA IT EN SERVICIOS BACKOFFICE: CASO ESTUDIO EMPRESA SECTOR GIROS POSTALES.

Implementation of the Disaster Recovery Model as a service - DRaaS for IT Infrastructure in BackOffice services: Case study company postal money sector.

Anderson Gutiérrez Campos
Anderson.gutierrez00@usc.edu.co

Jethferson Ramírez Giraldo
Jefferson.ramirez00@usc.edu.co

Mg. Ciro Dussán Clavijo
ciro.dussan00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de Sistemas

Resumen

El propósito de una solución DRaaS *(Disaster Recovery as A Service)* es proporcionar herramientas eficientes y de menor costo a los departamentos de tecnología fundamentado en proporcionar disponibilidad a servicios críticos de las organizaciones que puedan verse afectados a causa de las interrupciones por desastres; en la actualidad la iniciativa de implementación de un DRP *(Disaster Recovery Plan)* tiene una prioridad alta y es una necesidad estratégica para las compañías; la presente investigación pretende demostrar que la implementación del DRaaS permite garantizar los indicadores de cumplimiento de tecnología, así como el cumplimiento del RTO *(Recovery Time Objetive)* y RPO *(Recovery Point Objetive)* ante incidentes o catástrofes. Se implementa una metodología de investigación construida a partir de la medición del indicador de disponibilidad de aplicativos en hora critica; fundamentada en el análisis del estado actual de la infraestructura tecnológica, inventario de servidores y servicios críticos para los procesos de BackOffice, evaluación de propuestas de proveedores y evaluación de costos de una solución DRaaS comparada con una solución DRP tradicional. Una vez recolectado los datos anteriores se realiza la evaluación de riesgos y el análisis de impacto sobre el negocio. Se evaluarán los requerimientos técnicos que se deben implementar en la solución DRaaS con el objetivo de cumplir con el funcionamiento eficiente de los servicios TI. Finalmente, la implementación del DRaaS generará un ahorro significativo en el plan de renovación de los equipos de infraestructura tecnológica para la organización, así como un modelo orientado a el cumplimiento de los indicadores estratégicos.

Palabras Clave: Recovery Time Objetive, Recovery Point Objetive, Disaster Recovery as A Service, Riesgos, Análisis de impacto al negocio.

Abstract

The purpose of a DRaaS solution is to provide efficient and low-cost tools to technology departments based on providing availability to critical services of organizations that may be affected by disaster interruptions; At present, the DRP implementation initiative has a high priority and is a strategic need for companies; The present investigation tries to demonstrate that the implementation of the DRaaS allows to determine the indicators of compliance of the technology, as well as the fulfillment of the objective time of recovery and the objective point of recovery before incidents or catastrophes. A research methodology built from the measurement of the application availability indicator at critical time is implemented; Based on the analysis of the current state of the technological infrastructure, inventory of servers and critical services for BackOffice processes, evaluation of supplier proposals and cost evaluation of a DRaaS solution compared to a traditional DRP solution. Once the previous data has been collected, the risk assessment and the business impact analysis are carried out. The technical requirements that must be implemented in the DRaaS solution will be evaluated in order to meet the efficient operation of IT services. Finally, the implementation of the DRaaS generates significant savings in the renovation plan of the technological infrastructure equipment for the organization, as well as a model oriented towards the fulfillment of the strategic indicators.

1. INTRODUCCIÓN

En los últimos años las TICs, han tenido una evolución en las redes y la Internet, es por esto por lo que ha aumentado la demanda de servicios en la nube, desde grandes multinacionales hasta pequeñas empresas, las cuales requieren que todos los recursos tecnológicos se interconecten entre sí, para subsanar los requerimientos que las organizaciones necesitan.

Actualmente el principal activo de las compañías es la información, sin embargo, están expuestas al crecimiento constante de los riesgos tecnológicos y catastróficos, que amenazan la operatividad y el buen funcionamiento de los servicios misionales.

Un desastre es un incidente que puede ocurrir de manera imprevista, pueden ser naturales y/o generados por el hombre, tales como: terremotos, inundaciones, incendios, terrorismo, virus cibernéticos, caídas en el fluido eléctrico, manipulación errónea o mal intencionada, etc. (Dhanujati y Girsang, 2018). De acuerdo con lo anterior surge la pregunta: ¿Está preparada la infraestructura actual para solventar el enfrentamiento ante una amenaza? El presente artículo, presenta la implementación de un DRaaS - Disaster Recovery as a service para la infraestructura IT en servicios BackOffice, cuyo caso de estudio se efectuó en la empresa sector giros postales. El esquema actual de su infraestructura, no contempla de manera razonable la continuidad de sus recursos tecnológicos que apoyan los servicios críticos de la organización, es por esto, que la ejecución del DRaaS es primordial para apoyar el plan de continuidad del negocio, así como el plan de recuperación ante desastres y alineado al sistema de seguridad de la información ISO 27001, iniciando con la selección de la propuesta de acuerdo con los criterios de evaluación del departamento de tecnología, que proporcione un sitio alterno que permita activar el DRP, además de obtener la infraestructura en alta disponibilidad, con las debidas políticas de Backup, RTO y RPO definidos(ISO 27001,2015).

Este documento también presenta, la identificación de los principales riesgos a lo que encuentra expuesta la infraestructura de TI, en donde se realizo una serie de actividades para la selección de los servicios críticos y el alcance de los mismos; esto llevo a definir el RTO y RPO necesarios para la implementación del sitio alterno , continuando con el especificar los requerimientos técnicos con base a los estándares definidos por el departamento de tecnología necesarios para la implementación del DRaaS que soporte cada uno de los procesos administrativos de la empresa.

Finalmente se espera obtener resultados que afronten de manera positiva la implementación del DRaaS aportando al crecimiento continuo de los procesos y al funcionamiento ininterrumpido ante alguna falla o desastre.

2. MARCO TEÓRICO.

2.1 BCP (Business Continuity Plan).

Actividad que garantiza la creación de un sistema de prevención y recuperación ante desastres y amenazas potenciales de una compañía, identificando la información crítica necesaria para garantizar que el personal y los recursos tecnológicos estén protegidos y puedan operar eficientemente ante un incidente (Alhazmi y Malaiya, 2013).

2.2 DRP (Disaster Recovery Plan).

Es el plan que describe como se realiza el proceso de recuperación de los componentes técnicos como software y hardware, personal calificado para la operación de los servicios y el espacio físico para garantizar la continuidad del negocio ante un desastre; reanudando el trabajo de los componentes críticos de la compañía. El Plan de recuperación de desastres es una parte de la planificación de continuidad del negocio y contempla a los procesos de la compañía que dependen de infraestructura tecnológica para funcionar (Rebah y Sta, 2016).

2.3 DRaaS (Disaster Recovery as a Service).

La recuperación de desastres como servicio es un modelo tecnológico de respaldo y computación en la nube que

permite a las empresas implementar mecanismos de protección, disponibilidad y operatividad a sus servicios, aplicaciones y datos con el objetivo de garantizar la continuidad del negocio ante un desastre o falla del sistema (Wang, Zhou, Cai, Li, 2005).

2.4 RPO (Recovery Point Objetive)

Objetivo de Punto de Recuperación es el volumen de datos que tiene previsto la compañía perder en caso de presentarse un fallo en el sistema o un desastre (Wang, Ramasamy, Harper, Viswanathan y Plattier, 2015).

2.5 RTO (Recovery Time Objetive)

Es el tiempo que se tiene contemplado de la no disponibilidad de los sistemas de TI, durante la recuperación en el momento del evento no esperado que afecte la infraestructura, servicios, causada por un desastre natural, fallo en los sistemas de información o error humano (Fernando, 2017).

3. SERVICIOS TECNOLÓGICOS OFERTADOS EN CLOUD.

Desde sus inicios la computación en la nube ha permitido ampliar a gran escala aquellos requerimientos de tecnologías de información que antes eran costosos, poco escalables y de difícil administración. Su solución está basada en proporcionar ambientes de virtualización en donde una instancia o máquina virtual (VM) contiene las características de hardware y software, las cuales son gestionadas por un hipervisor encargado de aprovechar los recursos de una manera más eficiente versus la infraestructura de un centro de cómputo tradicional fundamentada en un servidor físico para cada servicio de TI (Al-Sharidah y Al-Essa, 2017).

Los sistemas en la nube permiten el rápido despliegue, seguridad, fácil uso, monitoreo, respaldo, restauración y alta disponibilidad de la información de los proyectos de TI; la flexibilidad, rentabilidad, escalabilidad, bajo costo y pagar únicamente por lo que se usa, es lo que los administradores de TI deben buscar en el momento de obtener los servicios en la nube para su infraestructura (Alshammari, Alwan, Nordin y Al-Shaikhli, 2017).

Dentro de los servicios principales ofrecidos por los proveedores de Cloud, tenemos los siguientes:

3.1 IaaS (Infraestructura como servicio).

Es la característica más básica de los tipos de servicios en la nube, en donde está relacionado el acceso y la capacidad de computo. Se paga para el acceso a la Infraestructura tales como: servidores, almacenamiento y redes de telecomunicaciones, en entornos virtualizados (Chaudhary y Maheshwari, 2015).

3.2 PaaS (Plataforma como servicio).

Ofrece servicios de acceso al entorno basado en la nube, es decir los usuarios se enfocan en desarrollar, gestionar y entregar sus aplicaciones sin preocuparse en ningún momento por las capas inferiores de infraestructura que soportan las aplicaciones, además proporciona un sin número de herramientas agiles para realizar el testing de sus desarrollos (Bohn, Messina, Liu, Tong y Mao, 2011).

3.3 SaaS (Software como servicio).

El proveedor de nube proporciona a los usuarios el acceso a través de la Internet o las API, sin preocuparse por el desarrollo e infraestructura que lo precede (Foster, Zhao, Raicu,y Lu, 2008).

A parte de los servicios anteriormente nombrados, Gartner, describe la solución DRaaS, como un servicio que permitirá de manera automatizada la recuperación y restauración ante un desastre, eliminando la carga de la operación en los equipos de TI, sin embargo, se deben estipular las reglas del negocio en un contrato entre las partes, acompañados de

SLA establecidos entre el cliente y el proveedor, para la estandarización de los servicios de recuperación (Gartner, 2019).

En el momento de la selección de las diferentes ofertas que existen de DRaaS en el mercado, los administradores de TI de las organizaciones deberán tener en cuenta las siguientes premisas: Backup, Recovery, RTO, RPO.

4. ESTADO DEL ARTE

Actualmente, no es suficiente contar con las últimas tecnologías en infraestructura de TI, sino que se debe garantizar la alta disponibilidad de sus recursos tecnológicos para brindar a las empresas el continuo desarrollo de sus actividades de negocio. El departamento de TI debe garantizar el funcionamiento continuo de todos lo aplicativos e infraestructura y telecomunicaciones apoyando la optimización de recursos tecnológicos y conocer los riesgos potenciales a los que se expone.

DRaaS, proporciona a empresas que no cuentan con una amplia infraestructura de TI, la capacidad de soportar los riesgos a que están expuestas ante la pérdida de sus datos, soportándolos en sitios alternos de un tercero, permitiendo la continuidad del negocio con sistemas de replicación, alta disponibilidad de servicios, monitoreo, políticas de seguridad, políticas de Backup, ahorro en costos en licenciamiento de hipervisores para la virtualización y licenciamiento de software(Pokharel, Lee y Park, 2010).

La implementación del DRaaS para los servicios de BackOffice consta de repotenciar la capacidad de cómputo actual en los servidores de mayores prestaciones y soporte, servicios y hardware en CLOUD como DataCenter alterno, además de provisionar el sitio alterno ante la activación del plan DRP.

A continuación, se llevará a cabo un estudio de las diferentes opciones escogidas para plasmar la propuesta de nube privada para la infraestructura IT de la compañía.

4.1 Criterios de selección del Modelo DRaaS Vs DRP Tradicional

Siguiendo los requerimientos previos para la implantación del DRaaS para la infraestructura de TI para el BackOffice de la compañía, en la tabla 1, se realizó una comparativa de gestión ofrecida en el modelo DRaaS por los proveedores seleccionados versus el DRP tradicional (Wood, Cecchet, Shenoy, Merwe y Venkataramani, 2010).

Tabla 1. Modelo DRaaS vs DRP tradicional.

Administración de Servicios	**Recursos**	
	DRP Tradicional	**DRaaS**
NOC	TI	Proveedor
Gestión de Canales de Comunicaciones	TI	Proveedor
Gestión de Hardware	TI	Proveedor
Gestión de Equipos de Seguridad Perimetral	TI	TI
Gestión de VM - Hipervisores	TI	Proveedor
Gestión de Backup - Gestión de Restauración	TI	Proveedor
Gestión de FailOver - FailBack	TI	Proveedor
Gestión de Mantenimiento Proactivo y Reactivo	TI	Proveedor
Gestión UPS	TI	Proveedor
Gestión de Software	TI	TI

Fuente: Elaboración propia.

De acuerdo a la tabla 1 se evidencia que el DRaaS ofrece gestión y servicios de administración a los departamentos de TI reduciendo considerablemente las funciones del personal operativo de tecnología, así como dando eficiencia por ser especialistas en la administración de los mismos.

5. METODOLOGÍA

5.1 Metodología Seleccionada.

La metodología seleccionada es la cuantitativa; implementando y analizando el indicador de disponibilidad de plataforma en horario critico; identificando incumplimiento en la prestación de servicios BackOffice.

Figura 1. Indicador de Gestión

INDICADORES DE GESTIÓN TECNOLOGÍA DE LA INFORMACIÓN

					AÑO 2018						AÑO 2019					
INDICADOR	METODOLOGÍA DE CALCULO	FRECUENCIA	RESPONSABLE	META	OCT		NOV		DIC		ENE		FEB		MAR	
Disponibilidad de aplicativos (Critico)	No de Horas criticas para la venta en el mes (No de dias del mes (30) * horas criticas (8) - No de horas criticas de indisponibilidad de los aplicativos	Mensual	Jefe de Infraestructura	99,00%	228	2	216	3	220	5	224	5	208	3	224	1
	No de Horas criticas para la venta en el mes				228		216		220		224		208		224	
				MEDICIÓN	99,12%		98,84%		97,73%		97,77%		98,37%		99,55%	

Analizar el comportamiento del indicador, tendencias y factores que inciden en el cumplimiento o incumplimiento del indicador.

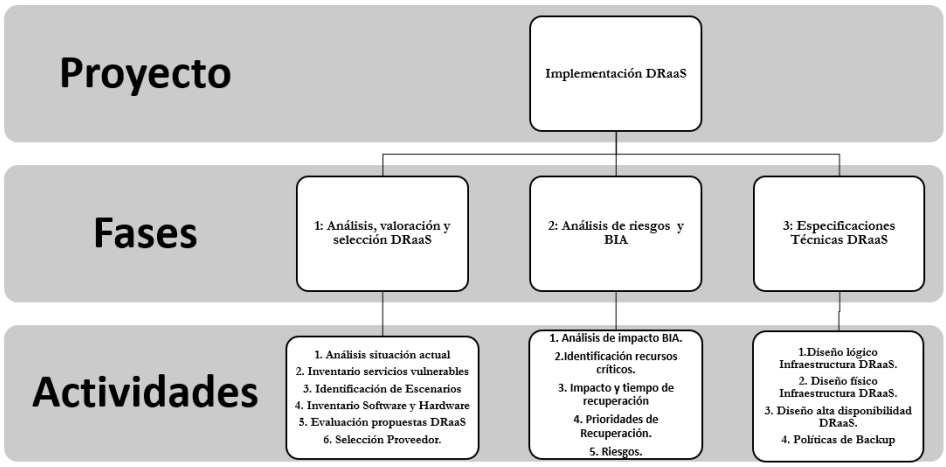
MES	ANÁLISIS DEL INDICADOR	ESTAS
DICIEMBRE	Saturacion Consumo Recursos (RAM - CPU) - Server Report	
NOVIEMBRE	Caida Canal comunicaciones Radio Enlace	
OCTUBRE	Consumo Procesamiento Servidor - Correo Electronico Zimbra	Implementacion Modelo DRaaS.
ENERO	Daño Board - Servidor FTP	
FEBRERO	Inconveniente Ataque DoS - Mesa de Ayuda	
MARZO	Inconveniente Almacenamiento - Planta telefonica PBX	

Disponibilidad de Aplicativos (crítico): *Nº Días del mes * Horas críticas (8) / Nº Horas Indisponibilidad*

Fuente: Elaboración propia.

De acuerdo con la figura 1, la identificación de las fallas presentadas durante la muestra de los meses tomados como referencia en los indicadores, definimos en la figura 2 las fases de la metodología implementada para el proyecto.

Figura 2. Metodología DRaaS.



Fuente: Elaboración propia.

5.2 Fase 1: Análisis, valoración y selección de propuesta DRaaS.

En esta fase se evaluaron los componentes de infraestructura que soportan los servicios BackOffice; además, se contemplaron los años de funcionamiento y los Backups que se efectúan a estos servicios, evidenciando fallas que justifican la implementación del DRaaS.

Se evalúan 4 propuestas de proveedores que suministran el servicio DRaaS, y de acuerdo con los criterios de evaluación definidos se elegirá el proveedor de la solución, los proveedores son: Microsoft Azure, C&W Bussiness, IBMCloud y NetGroup.

5.2.1 Inventario de Servidores Actuales

En la siguiente tabla 2, se describen los componentes de hardware que soportan los servicios de BackOffice.

Tabla 2. Inventario Servidores Actuales.

Aplicación o Servicio	HostName	RAM	Disco Duro	Sistema Operativo	Núcleos Procesador	Modelo
Correo Electrónico	Mail.corp	16GB	1TB	Centos7.5	8vCPU	HPProliant Gen6
ERP	ERP	8GB	500GB	Oracle Linux	4vCPU	HPProliant ML110 Gen6
Directorio Activo	Controlador Dominio	8GB	90GB	Windows Server 2016	4vCPU	HPProliant DL380e Gen8
Gestión Documental	Gestión Documental	8GB	50GB	Centos7.5	4vCPU	HPProliant DL380e Gen8
Telefonía IP	Vozip	8GB	150GB	Centos6.5	8vCPU	HPProliant DL380p Gen8
Service Desk	Helpdesk	16GB	500GB	FreeBSD 10.1	8vCPU	HPProliant DL380p Gen8
Reportes	Reports	16GB	500GB	FreeBSD 10.1	8vCPU	HPProliant DL380p Gen8
Pandora	Monitoreo	8GB	100GB	Centos7.0	4vCPU	HPProliant DL380p Gen8
Antivirus	Karpersky	8GB	1TB	WindowsServer R2 2012	8vCPU	HPProliant 1450StoreEasy
Intranet	Intranet	8GB	100GB	FreeBSD 12.0	4vCPU	IBM BladeCenter Hs22
SFTP	Sftp	8GB	2TB	Open BSD	8vCPU	IBM BladeCenter Hs22

Fuente: Elaboración propia.

5.2.2 Estado actual infraestructura Servicios

En la tabla 3, se describen los años de operación y el estado físico de los servidores que soportan los aplicativos BackOffice.

Tabla 3. Estado actual infraestructura servicios.

Aplicación o servicio	Años Funcionamiento	Estado Físico	Backup	Restauración Backup
Antivirus	2	Aceptable	Fuerte	2horas
Telefonía IP	4	Aceptable	Débil	N/A
Service Desk	4	Aceptable	Débil	2horas
Directorio Activo	5	Plan de renovación	Débil	5horas
Gestión Documental	5	Aceptable	Fuerte	1hora
Reportes	5	Array con alarma	Débil	2horas
Intranet	5	Obsolescencia Tecnológica	Fuerte	30minutos
SFTP	5	Obsolescencia Tecnológica	Débil	N/A
Pandora Monitoreo	5	Obsolescencia Tecnológica	Mediana	1hora
ERP	6	Pendiente renovación	Débil	8horas
Correo Electrónico	8	Pendiente renovación	Débil	24horas

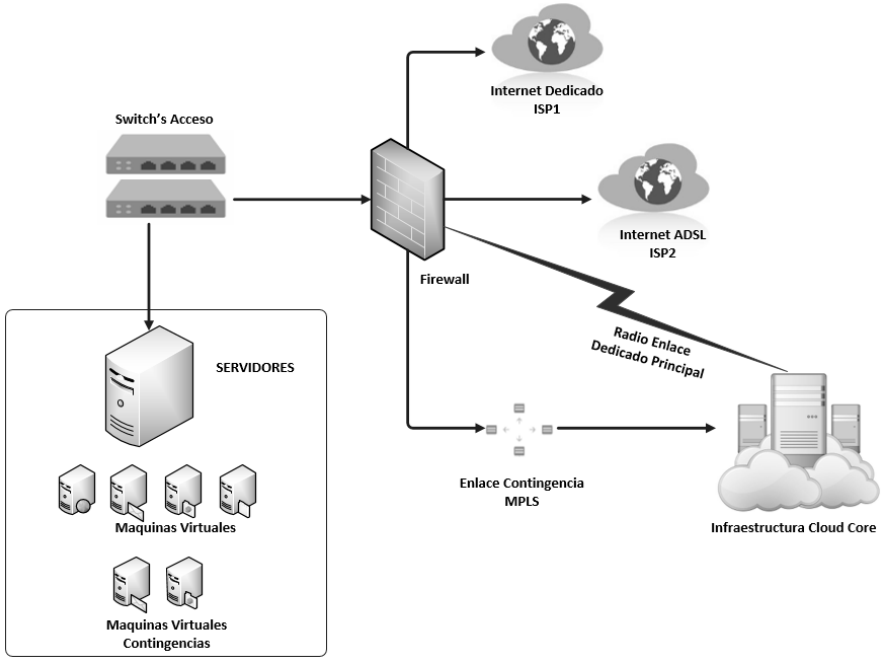
Fuente: Elaboración propia.

5.2.3 Infraestructura actual servicios.

En la figura 3, se puede observar la infraestructura actual que soporta los servicios internos de la organización, en donde no se cuentan con componentes de alta disponibilidad, evidenciando múltiples puntos de

falla que afectan la operación durante una interrupción o incidente.

Figura 3. Infraestructura BackOffice Actual.



Fuente: Elaboración propia.

5.2.4 Evaluación Proveedores DRaaS

Se realizó la evaluación de proveedores y sus propuestas de acuerdo los requerimientos necesarios para la implantación del DRaaS, previo análisis de la infraestructura actual y las necesidades de la empresa. En la tabla 4, se evidencian los criterios de evaluación y en la tabla 5 las puntuaciones de cada proveedor.

Tabla 4. Características de evaluación proveedores DRaaS.

Proveedor	Cargo Fijo Mensual	Ubicación Geográfica Sitio Alterno	Sitio de recuperación	Infraestructura dedicada	Administración seguridad perimetral	Storage Dedicado	Infraestructura Centro de Datos SG	Canales de Comunicaciones Dedicados (Radio enlaces, MPLS)	NOC
NetGroup	Si	Cali / USA	Si	Si	Si	Si	Si	Si	Si
Microsoft Azure	No	Cloud Azure	Remoto	variable	No	No	No	No	Si
Century Link	No	Cali	Remoto	variable	No	No	No	Si	Si
C&W Business	No	Bogotá	Remoto	variable	No	No	No	Si	Si

Fuente: Elaboración propia.

Tabla 5. Criterios de evaluación proveedores DRaaS.

Servicios / Proveedor	Cargo Fijo Mensual	Ubicación Geográfica Sitio Alterno	Works Área Recovery Site	Infraestructura dedicada	Puntuación
NetGroup	5	5	5	5	20
Microsoft Azure	1	1	3	3	8

CenturyLink	1	5	3	3	12
C&W Business	1	3	3	3	10

Fuente: Elaboración propia.

5.3 Fase 2: Análisis de riesgos de continuidad del negocio.

En esta fase se analizaron los factores críticos de los componentes tecnológicos (Software, Personal, Procesos Operativos) que soportan la operación, así como los principales riesgos a los que se enfrenta la compañía y sus diferentes controles y actividades que mitigan los mismos.

5.3.1 Análisis de Riesgos

La metodología para el análisis de los riesgos aplicado para los servicios BackOffice, contemplo el estándar internacional ISO 31000, esta metodología se aplica con rigurosidad para los servicios Core de la compañía, sin embargo, para servicios administrativos no se realizaba el análisis hace 3 Años, dejando controles e impactos de riesgos desactualizados y no ajustados a la realidad de los procesos actuales (ISO 31000,2018).

La gestión del riesgo se simplificó mediante la agrupación de riesgos relevantes para la organización y se implementó de acuerdo en la siguiente figura 4:

Figura 4: Metodología de riesgos.

Fuente: Elaboración propia.

5.3.2 Identificación y Plan de tratamiento de riesgos.

Con base al resultado de análisis cuantitativo y cualitativo de los riesgos y disminuir la probabilidad de que se materialicen los mismos, se proponen las siguientes acciones de mejora y correctivas con el objetivo de fortalecer la plataforma tecnológica para los servicios y así no incumplir con la prestación de servicios BackOffice.

Los planes de acción identificados en la evaluación de riesgos convergen en establecer contingencias operativas y eficientes, así como renovación de servidores obsoletos. Ver tabla 6.

Tabla 6. Plan de acción Riesgos.

No.	Código Riesgo	Riesgo	Plan de Acción
1	**GTI-03**	Imposibilidad de acceder al Service Desk	Acción de Mejora: Contingencia Service Desk.
2	**GTI-04**	Imposibilidad de acceder al servicio de correo electrónico por ataque de denegación del servicio.	1. Renovación Servidor. 2. Contingencia Correo Electrónico.
3	**GTI-06**	Imposibilidad de acceder al servidor Directorio Activo y consultar información en las unidades de RED.	1. Contingencia Directorio Activo 2. Renovación Servidor Directorio Activo
4	**GTI-07**	Imposibilidad en la ejecución de procesos administrativos.	1. Contingencia Report CORE 2. Renovación Servidor Report CORE

5	**GTI-08**	Imposibilidad en la ejecución de procesos administrativos, venta y financieros que afectan la continuidad de la operación	1. Contingencia ERP 2. Implementar Herramientas de Backup (VeemBackup)
6	**CI-02**	Fallas en la seguridad de la Información que afectan la confidencialidad, disponibilidad e integridad de la información.	Acción de Mejora: Contingencia Antivirus.
7	**CE-01**	Disminución de ingresos que afectan la maximización de la rentabilidad de los Accionistas.	Formalizar y actualizar los ANS con proveedor externos de acuerdo con la operación actual
8	**GTI-11**	Imposibilidad de acceder al Servicio de Telefonía IP y PBX	Acción de Mejora: Contingencia Telefonía IP
9	**GTI-12**	Imposibilidad en la ejecución de procesos administrativos por inconvenientes con el servidor de Gestión Documental (Gestión Documental, Riesgos, Actas).	1. Contingencia Servidor de Gestión Documental
10	**GTI-13**	Imposibilidad en la comunicación interna de actualización de procedimientos y Actividades Corporativas.	1. Contingencia Intranet 2. Renovación Servidor
11	**GTI-14**	Imposibilidad de Acceder a el Servidor FTP para procesos de conciliación de envío y recepción.	1. Contingencia FTP 2. Renovación Servidor

Fuente: Elaboración propia.

5.4 Análisis de impacto en el negocio (BIA)

El análisis de impacto en el negocio permitió identificar las aplicaciones, procesos y recursos críticos en tecnología; mediante este análisis fue posible determinar los tiempos mínimos de recuperación de cada servicio, así como la priorización y las estrategias de recuperación ante un desastre (Alshammari, Alwan, Nordin y Al-Shaikhli, 2017).

Tabla 7. Software.

		Impacto		
Aplicación / Servicio	**Descripción**	**ALTO**	**MEDIO**	**BAJO**
Correo Electrónico	Mail Server	X		
ERP	ERP	X		
Directorio Activo	WindowsServer	X		
Gestión Documental	MYSQL GlassFishServer		X	
Telefonía IP	Asterisk	X		
Service Desk	ManageEngine		X	
Reportes CORE	Reports			X
Monitoreo	Pandora		X	
Antivirus	KasperkyServer			X
Intranet	Apache			X
SFTP	SFTP		X	

Fuente: Elaboración propia.

5.4.1 Identificación del impacto y el tiempo de recuperación aceptable.

En la tabla 8, se especifican los recursos y procesos críticos con los que cuenta el departamento de tecnología, así como el impacto en la operación y el tiempo de recuperación aceptable por la dirección.

Tabla 8. Identificación de impacto y tiempo de recuperación.

Aplicación / Servicio	**Departamento**	**Proceso**	**Impacto**	**Tiempo Máximo Recuperación Individual**	**RTO**	**RPO**
Correo Electrónico	General	PQRS	No se puede Acceder a la aplicación de correo electrónico, Imposibilitando la resolución de PQRS, las activaciones y bloqueos de sucursales y los cuadres de caja.	2horas	10 horas	1 hora
ERP	Financiero.	Procesos contables y Activos fijos.	No se puede acceder a la aplicación ERP,	30minutos		

	Gestión Humana	Procesos de nómina.	Imposibilitando el acceso a la nómina, pagos a proveedores, interfaces contables, ingresos y egresos de sucursales.	
	Tesorería	Procesos de Pago proveedores y clientes.		
Directorio Activo	General	Acceso a Aplicaciones y servicios tecnológicos	No se puede acceder a las aplicaciones corporativas, imposibilitando las actividades y procesos diarios del personal administrativo.	1hora
Gestión Documental	General	Gestión Documental (Formatos, Procedimientos e Instructivos).	No se puede acceder a los documentos del sistema de gestión de calidad, así como los procesos de centralización de indicadores de gestión, matriz de riesgos y gestión de actas.	30minutos
		Indicadores Estratégicos.		
		Matriz de Riesgos.		
Telefonía IP	General	Servicio al Cliente.	No se reciben ni salen llamadas a los entes comerciales de las diferentes ciudades del País, imposibilitando la recepción de peticiones PQR.	1hora
		Atención Operativa		
Service Desk	Operaciones, Tecnología	Peticiones de Incidentes y Soluciones	No se atienden solicitudes internas y externas de tecnología y operaciones.	30minutos
Reportes CORE	General, Aliados comerciales.	Reportes Automáticos	Los entes comerciales y aliados externos no pueden acceder al sistema integrado de reportes en línea, imposibilitando el cuadre de caja, el saldo de cajas, y la información de usuarios y sucursales.	1hora
Pandora Monitoreo	Tecnología	Monitoreo Servicios y aplicaciones Networking. Monitoreo Canales Comunicaciones.	El departamento de Tecnología no puede acceder al sistema automático de monitoreo de plataforma; servicios de tecnología, monitoreo de servidores, bases de datos y dispositivos de Networking.	1hora
Antivirus	General	Administración de Consola (Políticas y Control de Aplicaciones)	Los equipos administrativos no tienen acceso a la base de datos de virus y actualización de versiones del antivirus.	1hora
Intranet	General	Comunicación Interna	Los clientes internos administrativos no tienen acceso a la intranet corporativa.	1hora
SFTP	Aliados Comerciales	Transferencia Información	Los clientes externos no tienen acceso a la extracción de la información para realizar los respectivos cuadres.	1hora

Fuente: Elaboración propia.

5.4.2 Prioridades de recuperación para el modelo DRaaS.

Las prioridades de recuperación de los procesos y recursos críticos se fundamentan en la evaluación del impacto sobre la operación del negocio; definidas en conjunto con Riesgos, Dirección y el departamento de tecnología; a continuación, se detallan los recursos y su prioridad de recuperación:

Tabla 9. Prioridad y recursos tecnológicos.

Recurso Tecnológico	Prioridad de Recuperación
Correo Electrónico	Alta
ERP	Alta

Directorio Activo	Alta
Telefonía	Alta
Gestión Documental	Media
Service Desk	Media
Pandora Monitoreo	Media
Reportes CORE	Media
Antivirus	Baja
Intranet	Baja
SFTP	Baja

Fuente: Elaboración propia.

5.5 Fase 3: Especificación de requerimientos técnicos del DRaaS.

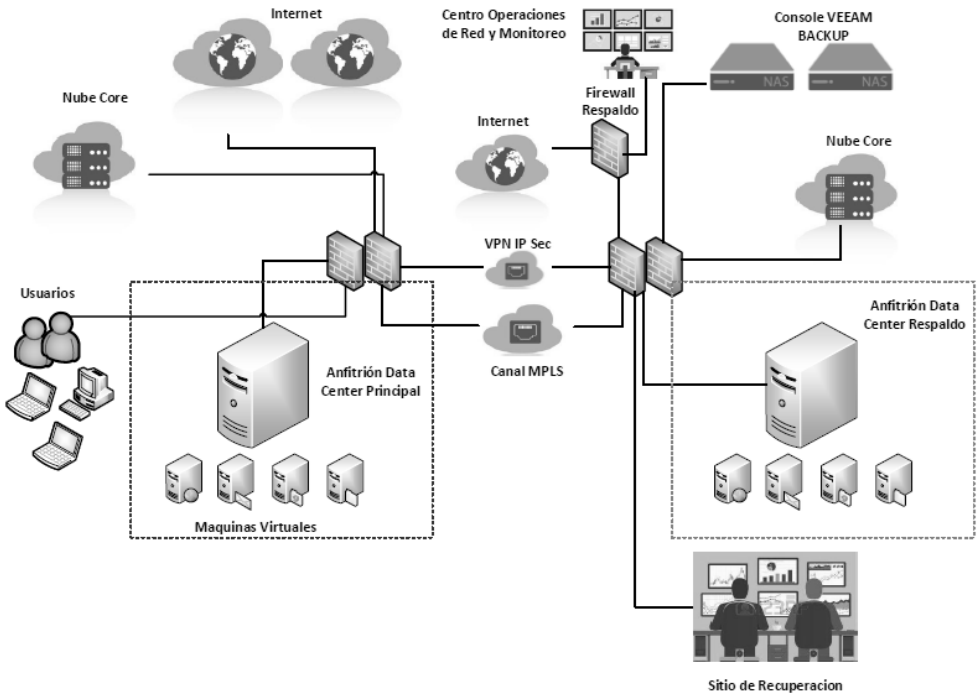
De acuerdo con el inventario de la infraestructura actual y los servicios tecnológicos definidos para la implementación del DRaaS se entregarán las especificaciones técnicas y operativas que permitan garantizar el óptimo funcionamiento de la plataforma ante un incidente; el proveedor seleccionado de acuerdo con las evaluaciones de las propuestas debe garantizar estos requerimientos y desarrollar planes de prueba del DRaaS periódicamente.

5.5.1 Modelo DRaaS.

El modelo de configuración del DRaaS para la infraestructura de la empresa consiste en definir el sitio alterno como datacenter primario y de recuperación ante un desastre o falla con replicación en el centro de cómputo en las instalaciones de la sede administrativa como datacenter secundario, además se define el modelo de conmutación por error para los servicios BackOffice (Qasmi, Siddiqui, Shehzad, Iqbal y Ilyas, 2018).

En la figura 6 se evidencia el esquema DRaaS propuesto para la implementación de los servicios BackOffice, soportado por componentes de seguridad perimetral en alta disponibilidad, canales de comunicaciones dedicados y redundantes para la interconexión de los nodos, servidores de características idénticas quienes soportan los servicios administrativos con hipervisores para la virtualización de máquinas virtuales, replicación y políticas de backup gestionados por la consola VEEAM Backup, conectividad hacia los servicios de CORE, políticas de seguridad que permiten la gestión efectuada por el proveedor para la administración y monitoreo de la infraestructura; finalmente un sitio alterno para la recuperación, el cual soportara de manera eficiente y eficaz el plan de BCP y DRP de la compañía.

Figura 6. Infraestructura propuesta DRaaS



Fuente: Elaboración propia.

5.5.2 Requerimientos de infraestructura DRaaS.

En la tabla 10, se relacionan los requerimientos tecnológicos de hardware para la implementación de la solución DRaaS y en la tabla 11 se detalla el licenciamiento, telecomunicaciones y servicios.

Tabla 10. Hardware

Hardware		Licenciamiento	Servicios	Telecomunicaciones
2 servidores HP Proliant DL380 Gen10 6130	8 procesadores - 160 v'CPU	SAAS Windows 2016 Server Datacenter N Máquinas Virtuales	Implementación y Migración plataforma actual	Radio Enlace Dedicado con Licencia de 150 Megas
	320 GB Memoria RAM	SAAS & Soporte VEEAM Backup EnterprisePLUS	Ambientes Pruebas 25 Días	
	Disco Duro 6.1 TB	Antivirus Symantec por Maquina	Administración Servidor y NAS	LAN 10 GB Backbone
Servidor NAS HP 1450 Storage	Discos Duros Estado Solido - 12 TB	Controlador de Dominio SAM especializado del Directorio Activo Microsoft	Administración 2 Radios VPN Internet	

Fuente: Elaboración propia.

6. RESULTADOS Y DISCUSIÓN

La solución DRaaS permitió implementar un sitio alterno (Works área Recovery site), que apoya al plan DRP y BCP de la compañía; adicionalmente los procedimientos de recuperación establecidos permitieron definir el RTO en 10 horas y el RPO en 1 hora para los servicios BackOffice, garantizando así el cumplimiento de los tiempos concertados con la gerencia general. En la tabla 8 se evidencian los tiempos de recuperación ante un desastre.

Cuando se presente una falla individual de los servicios de tecnología los tiempos de recuperación establecidos en el BIA permitirán que el indicador de cumplimiento de disponibilidad de aplicativos críticos no sea incumplido en su medida de 99%, el procedimiento inicial de recuperación será la migración de la operación a el servidor contingente, y en segunda instancia de la recuperación de la máquina virtual con 10 minutos de perdida de información. En la tabla 8 se evidencian los tiempos de recuperación ante un incidente por servicios.

La matriz de riesgos permitió identificar que los procedimientos de recuperación establecidos ante un incidente por tecnología para los servicios BackOffice son las copias de seguridad, sin embargo se evidencio que de los 11 servicios administrativos prioritarios 8 Backups tiene una fortaleza débil ya que no se encuentran documentados (Ver tabla 3 Estado actual infraestructura servicios), no tienen plan de restauración, el tiempo de restauración es muy alto o en su defecto no se realiza; teniendo así un 73% de riesgos de perdida de información ante un desastre; generando pérdidas económicas y el deterioro de la imagen de los servicios prestados por la organización.

En la implementación del DRaaS se unifico la renovación de hardware y el servicio de recuperación de desastres, la evaluación económica proporciono un ahorro de un 51% comparado con la implementación de una solución DRP in House; el valor del ahorro es $806'705.120 Millones de pesos proyectado a 4 años, generando aceptación y agrado ante la dirección de la compañía; en la figura 7 se relacionan los costos de una solución DRP in House Vs el DRaaS.

Figura 7. DRP in House Vs DRaaS

DRP Tradicional			
Equipos	**Cantidad**	**Valor Unitario**	**Valor Total**
Servidor Hpe Proliant DL380 Gen10 6130 320gb 879938-b21	2	$ 64.000.000	$ 128.000.000
Servidor NAS HP 1450 Storage	2	$ 25.000.000	$ 50.000.000
Firewall 200 E - Licencia 1 Año	4	$ 12.529.176	$ 50.116.704
Licencia Fortigate 200 E (3 Años)	2	$ 10.013.000	$ 20.026.000
Call Licencia Windows Server DataCenter (1 Año)	4	$ 22.385.160	$ 89.540.640
Renovacion Licencia Windows Server Data Center 3 Años	3	$ 26.862.192	$ 80.586.576
Instalacion Aplicaciones	2	$ 30.000.000	$ 60.000.000
Instalacion y configuracion Maquinas Virtuales	2	$ 15.000.000	$ 30.000.000
Mantenimiento Servidores Fisicos		$ 18.000.000	$ 72.000.000
Costo Analista Infraestructura - Analista Base de Datos	2	$ 72.000.000	$ 288.000.000
Hosting Servidores Data Center Alterno 7 Unidades	7	$ 34.272.000	$ 137.088.000
Canal de Comunicaciones MPSL Claro 2 MB	1	$ 2.400.000	$ 115.200.000
Canal de Comunicaciones Internet Century Link - 100 MB	1	$ 2.600.000	$ 124.800.000
Licencia Veam Backup Availability	1	$ 9.136.800	$ 36.547.200
Alquier Sitio Alterno		$ 4.000.000	$ 192.000.000
Computadores Analistas - Operaciones	6	$ 3.000.000	$ 18.000.000
Canal Comunicación Sitio Alterno Banda Ancha	1	$ 1.600.000	$ 76.800.000
Care Pack Server HP	2	$ 3.000.000	$ 6.000.000
	Total	**$ 355.798.328**	**$ 1.574.705.120**

Comparativa economica DRP vs DraaS	
Costo mensual DRaaS (Año1)	$ 16.000.000
Costo Anual DRaaS	$ 192.000.000
Costo DRaaS 4 Años	$ 768.000.000
Solucion DRP in House	$ 1.574.705.120
DRaaS (4 Años)	$ 768.000.000
Diferencia	**$ 806.705.120**
% Gasto	**49%**
% Ahorro	**51%**

Fuente: Elaboración propia.

7. CONCLUSIONES

En la actualidad las organizaciones deben implementar, administrar, e incluir en sus presupuestos y en sus planes estratégicos de tecnología sus modelos de recuperación de desastres; estos planes deben estar alineados con los objetivos estratégicos de la compañía y garantizan que los servicios críticos operen de forma eficiente y eficaz alineados con valores aceptados por la organización RTO y RPO. La implementación del DRaaS es un desafío para tecnología, así como una oportunidad de reducir costos de hardware, software, personal y locativos y quizás el principal beneficio es que su dinámica hace posible pruebas constantes y eficientes de recuperación comparados con un DRP tradicional que implica mayores costos de implementación, y procedimientos engorrosos de activación y monitoreo.

La compañía cuenta con procedimientos de contingencia y recuperación a partir de restauración de Backup ante desastres; sin embargo estos mecanismos no tienen la capacidad necesaria para mantener la operación y la disponibilidad de los servicios BackOffice de forma oportuna y eficiente, garantizando el no cumplimiento del indicador de disponibilidad de aplicativos en hora critica así como los indicadores de continuidad de negocio RTO y RPO, esta oportunidad de mejora fue una de las justificaciones por las que la gerencia general apoyo el proyecto de implementación del DRaaS.

La implementación del DRaaS debe contar con el apoyo fundamental de tecnología y la dirección general, es una herramienta efectiva de renovación y solución a fallos de hardware y mitigación de riesgos; con una evaluación eficiente del estado actual de la infraestructura, los procedimientos de restauración y los recursos de tecnología; se convierte en un aliado estratégico interno en el cumplimiento de los indicadores de tecnología e indicadores comerciales y misionales; adicionalmente genera beneficios de administración, implementación, operatividad y control de los componentes de

infraestructura (Hardware, Software, Procesos de TI, Licenciamiento) y ahorros significativos en costos de renovación de hardware.

En el análisis de riesgos se evidencia que el departamento de tecnología tiene controles documentados, eficientes y actualizados para los servicios Core; sin embargo, esta misma rigurosidad no se aplica para los servicios BackOffice dejando desactualizados controles de riesgos, efectividad de estos; generando riesgos residuales de procesos que pueden generar pérdidas económicas y afectación a servicios Core.

De acuerdo al análisis de impacto de negocio, se evidenció que los servicios BackOffice están siendo soportados por servidores con fallas de hardware, pendientes de renovación y obsoletos; dejando así vulnerables los mismos y agregando valor al proyecto de implementación del DRaaS; cabe mencionar que el departamento de tecnología cuenta con personal técnico bien capacitado en el software, administración y la operación tecnológica, y contempla el respaldo para cada líder supliéndolo ante un siniestro personal u organizacional.

8. REFERENCIAS

A. H. Al-Sharidah and H. A. Al-Essa, "Toward cost effective and optimal selection of IT disaster recovery cloud solution," 2017 9th Computer Science and Electronic Engineering (CEEC), Colchester, 2017, pp. 43-48. doi:10.1109/CEEC.2017.8101597

Gartner's 2019 Magic Quadrant for Disaster Recovery as a Service: Key Takeaways, recuperado de https://solutionsreview.com/backup-disaster-recovery/gartners-magic-quadrant-for-disaster-recovery-as-a-service-key-takeaways-2/

H. B. Rebah and H. B. Sta, "Disaster Recovery as a Service: A Disaster Recovery Plan in the Cloud for SMEs," 2016 Global Summit on Computer & Information Technology (GSCIT), Sousse, 2016, pp. 32-37. doi:10.1109/GSCIT.2016.9

I. Foster, Y. Zhao, I. Raicu, S. Lu, Cloud Computing and Grid Computing 360-Degree Compared, 2008 URL: https://arxiv.org/pdf/0901.0131

J. Chaudhary, V.Maheshwari, Proposed Architecture for Virtual Lab Using Amazon Services, Int. Journal of Advanced Research in Computer Science and Software Engineering, 5 (5), 2015, pp.1637-1640.

Kun Wang, Lihua Zhou, Zhen Cai and Zengxin Li, "A Disaster Recovery System Model in an E-government System," Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05), Dalian, China, 2005, pp.247-250. doi:10.1109/PDCAT.2005.6

L. Wang, H. V. Ramasamy, R. E. Harper, M. Viswanathan and E. Plattier, "Experiences with Building Disaster Recovery for Enterprise-Class Clouds," 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio deJaneiro, 2015, pp. 231-238. doi:10.1109/DSN.2015.53

ISO 27001: Pilares fundamentales de un SGSI. Recuperado el 2 de 6 de 2019, de https://isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi, (2017).

ISO 31000: Gestión del Riesgo. Recuperado el 4 de 7 de 2019, de https://www.isotools.org/2018/10/15/resumen-nueva-norma-iso-31000-gestion-riesgos/, (2018).

M. M. Alshammari, A. A. Alwan, A. Nordin and I. F. Al-Shaikhli, "Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges," 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), Salmabad,2017, pp.1-7.
doi:10.1109/ICETAS.2017.8277868

M. Pokharel, S. Lee and J. S. Park, "Disaster Recovery for System Architecture Using Cloud Computing," 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, Seoul, 2010, pp. 304-307.
doi: 10.1109/SAINT.2010.23

M. S. Fernando, "IT disaster recovery system to ensure the business continuity of an organization," 2017 National Information Technology Conference (NITC), Colombo, 2017, pp. 46-48.
doi:10.1109/NITC.2017.8285648

M. Tsugawa, R. Figueiredo, J. Fortes, T. Hirofuchi, H. Nakada and R. Takano, "On the use of virtualization technologies to support uninterrupted IT services: A case study with lessons learned from the Great East Japan Earthquake," 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, 2012, pp. 6324-6328.
doi:10.1109/ICC.2012.6364838

N. Dhanujati and A. S. Girsang, "Data Center-Disaster Recovery Center (DC-DRC) for High Availability IT Service," 2018 International Conference on Information Management and Technology (ICIMTech), Jakarta, 2018, pp. 55-60.
doi:10.1109/ICIMTech.2018.8528170

O. H. Alhazmi and Y. K. Malaiya, "Assessing Disaster Recovery Alternatives: On-Site, Colocation or Cloud," 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops, Dallas, TX, 2012, pp. 19-20.
doi:10.1109/ISSREW.2012.20

O. H. Alhazmi and Y. K. Malaiya, "Evaluating disaster recovery plans using the cloud," 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, 2013, pp. 1-6.
doi:10.1109/RAMS.2013.6517700

R. B. Bohn, J. Messina, F. Liu, J. Tong, J. Mao (2011): NIST Cloud Computing Reference Architecture (IEEE World Congress on Services), VOL 54 ISSN 224-378.

R. E. Krock, "Lack of emergency recovery planning is a disaster waiting to happen," in IEEE Communications Magazine, vol. 49, no. 1, pp. 48-51, January 2011.
doi: 10.1109/MCOM.2011.5681014

T. Wood, E. Cecchet, P. Shenoy, J. V. D. Merwe, A. Venkataramani," Disaster recovery as a cloud service: economic benefits & deployment challenges", Published in Proceeding HotCloud'10 Proceedings of the 2nd USENIX conference on Hot topics in cloud computing. Pages 8-8 June 2010.

W. N. A. Qasmi, T. Siddiqui, M. K. Shehzad, A. Iqbal and M. S. Ilyas, "A comparative study of failover schemes for IaaS recovery," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 25-30.

doi:10.1109/ICOIN.2018.8343078