ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Sistemas de Información Gerencial

“DISEÑO BPMN PARA LA AUTOMATIZACIÓN DEL PROCESO DE RECUPERACIÓN ANTE DESASTRES EN UNA INSTITUCIÓN FINANCIERA”

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DE TITULO DE

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

SHARON JOHANA BAQUERO BALLADARES

PABLO ISAIAS VARGAS BOCCANEDES

GUAYAQUIL - ECUADOR

AÑO: 2023

AGRADECIMIENTO

En estas líneas quiero agradecer a todos quienes me apoyaron, en primer lugar, le agradezco a Dios por ser mi guía y acompañarme en el transcurso de mi vida, brindándome paciencia y sabiduría para culminar con éxito mis metas propuestas. A mis padres y mi a mami porque son los que me han formado como persona y me han impulsado siempre a perseguir mis metas y nunca abandonarlas frente a las adversidades. A mi esposo y a mi hijo, por todo su cariño y su sacrificio como familia para lograr cursar y terminar de forma satisfactoria esta meta trazada. Y por último agradecer a mis docentes por sus conocimientos impartidos.

Sharon J. Baquero B.

Mis agradecimientos al Padre de Todo, por su guía continua. A mis docentes quienes a través de su vocación me impartieron conocimientos para llevar a cabo este proyecto, al equipo de trabajo representante de la empresa financiera que nos facilitaron la documentación de la solución, a mi compañera de tesis por las horas de trabajo compartidas, y a mi familia por todo su apoyo.

Pablo I. Vargas B.

DEDICATORIA

A Dios, A mis padres, a mi mami, a mi esposo y a mis hijos que, aunque aún no lo comprendan son y serán lo más importante en mi vida, por quienes he decidido superarme y espero que este logro sirva de herramienta para guiar sus pasos como superación a nivel personal y profesional.

Sharon J. Baquero B.

A Dios, a mi familia, y a mi compañera de vida, quienes han sido mi soporte durante todo este proceso, a todos quienes lean este proyecto, que sirva de inspiración para seguir en el camino del progreso.

Pablo I. Vargas B.

TRIBUNAL DE SUSTENTACIÓN

……

MGS. Lenin Freire Cobo

DIRECTOR MSIG

……

MGS. Juan Carlos García

DIRECTOR DEL PROYECTO DE GRADUACIÓN

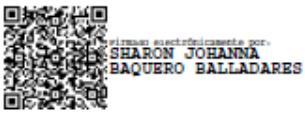
……

MGS. Lenin Freire Cobo

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

“La responsabilidad y la autoría del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual".



Sharon J. Baquero B.

Pablo I. Vargas B.

RESUMEN

Este proyecto describe la automatización del proceso de recuperación ante desastres informáticos de una institución financiera, y la ejecución de éste; a través de un software orquestador, con el fin de mejorar los tiempos de restablecimiento de los servicios informáticos y garantizar la disponibilidad para el cliente externo e interno.

El alcance del estudio es de tipo descriptivo, donde se midieron los tiempos de ejecución manual del proceso, es decir su situación actual y luego la toma de tiempos una vez implementada la automatización del proceso, el cual fue desarrollado con BPMN.

Con la aplicación de este proyecto se logró la reducción del tiempo de restablecimiento de los servicios en la institución en un 30%, únicamente en la muestra tomada. Con el desarrollo completo del proyecto, es decir incluyendo todos los servicios productivos, se garantizaría una reducción de hasta un 50% del tiempo total del DRP.

El desarrollo de este proyecto es ampliamente aplicable para cualquier tipo de empresa, donde se deba garantizar la continuidad de sus servicios tecnológicos, ayudando a resolver la pérdida de datos y recuperando la funcionalidad del sistema para que pueda funcionar después de un incidente.

ÍNDICE GENERAL

Contenido

AGRADECIMIENTO I

DEDICATORIA III

TRIBUNAL DE SUSTENTACIÓN IV

DECLARACIÓN EXPRESA V

RESUMEN VI

ÍNDICE GENERAL VIII

ABREVIATURAS Y SIMBOLOGÍA XI

ÍNDICE DE FIGURAS XII

ÍNDICE DE TABLAS XIII

INTRODUCCIÓN XIV

CAPÍTULO 1 1

MARCO GENERAL 1

1.1. Antecedentes 1

1.2. Descripción del problema 3

1.3. Solución propuesta 4

1.4. Objetivo General 5

1.5. Objetivos específicos 5

1.6. Metodología 6

1.7. Resultados esperados 8

CAPÍTULO 2 9

MARCO TEÓRICO 9

2.1. Plan de continuidad del negocio (BCP) 9

2.2. Plan de recuperación ante desastres (DRP) 10

2.3. Metodologías para modelado de procesos del negocio 12

2.4. Automatización y orquestación de DRP 16

2.5. Normas y regulaciones aplicadas en TI para entidades financieras 19

2.6. Delimitación 21

CAPÍTULO 3 23

SITUACIÓN ACTUAL 23

3.1. Levantamiento de información del proceso actual 23

3.2. Definición de alcance de la propuesta 26

3.3. Levantamiento de modelo AS-IS utilizando BPMN 34

3.4. Análisis de datos recolectados 35

3.5. Análisis de desperdicios y riesgos 36

3.6. Definición de encuesta 36

CAPÍTULO 4 38

DISEÑO DE AUTOMATIZACIÓN DEL PROCESO 38

4.1. Diseño del modelo TO BE utilizando BPMN 38

4.2. Implementación de la herramienta de automatización 40

4.3. Tableros de control 53

4.4. Tablero de control de nivel de Objetos 54

4.5. Tablero Gerencial 55

4.6. Configuración de grupos 56

4.7. Grupos de recuperación 57

4.8. Definición de casos de prueba 59

4.9. Prueba del modelo propuesto 65

4.10. Resultados de ejecución 71

4.11. Comparativa y análisis del resultado 73

CONCLUSIONES Y RECOMENDACIONES 76

BIBLIOGRAFÍA 79

ANEXOS 80

ABREVIATURAS Y SIMBOLOGÍA

AG	Applications Groups
BCP	Business Continuity Plan
BPM	Business Process Modeling
BPMN	Business Process Modeling and Notation
CRO	Cloud Resiliency Orchestrator
DC	Data Center
DR	Data Recovery
DRM	Disaster Recovery Manager
DRP	Disaster Recovery Plan
ISO	International Standardization Organization
RG	Recovery Groups
RPO	Recovery Point Objetive
RTO	Recovery Time Objetive
SLA	Service Level Agreement
TI	Technology Information
TLS	Transport Layer Security

ÍNDICE DE FIGURAS

Figura 2.1 11

Figura 3.1 35

Figura 4.1 39

Figura 4.2 41

Figura 4.3 44

Figura 4.4 46

Figura 4.5 46

Figura 4.6 47

Figura 4.7 49

Figura 4.8 52

Figura 4.9 55

Figura 4.10 56

Figura 4.11 59

Figura 4.12 62

Figura 4.13 65

Figura 4.14 67

Figura 4.15 68

Figura 4.16 69

Figura 4.17 70

Figura 4.18 71

ÍNDICE DE TABLAS

Tabla 1. Metodología 6
Tabla 2. Roles y Recursos del DRP 24
Tabla 3. Tareas y responsables del DRP 25
Tabla 4. Aplicaciones y RTOs 26
Tabla 5. Aplicaciones y plataformas 27
Tabla 6. Switchover APP1 28
Tabla 7. Switchover APP2 29
Tabla 8. Switchover APP3 29
Tabla 9. Switchover APP4 30
Tabla 10. Switchback APP1 31
Tabla 11. Switchback APP2 32
Tabla 12. Switchback APP3 33
Tabla 13. Switchback APP4 33
Tabla 14. Encuesta 37
Tabla 15. Grupo AG_Satelites 61
Tabla 16. Grupo AG_Core 62
Tabla 17. Aplication Group Satelites 64
Tabla 18. Application Group Core 64
Tabla 19. Resultados de Switchover y Switchback 72
Tabla 20. Tiempo total de ejecución de DRP 73
Tabla 21. Comparación de tiempos de DRP manual vs CRO 74
Tabla 22. Tiempos de optimización CRO 75

INTRODUCCIÓN

Para esta empresa de servicios financieros la confianza de sus clientes es un bien invaluable, por lo que se presta especial atención en el nivel de calidad que se brinda, así como facilitar la interacción con el cliente a través de múltiples canales. Estos cambios implican grandes desafíos tecnológicos para que coexista tecnología legada y moderna dentro del mismo ecosistema, soportado por la infraestructura de redes y equipos. Debido a la complejidad del sistema, suelen producirse fallos que interrumpen la producción que dejan muchos servicios caídos y que afectan el normal desarrollo de actividades de clientes.

Por ello, la empresa tiene implementado un plan de recuperación de desastres, que se ejecuta aisladamente y de forma manual en cada departamento para lograr la restauración de las operaciones normales. Este proceso suele tomar mucho tiempo debido a que cada departamento necesita esperar que finalice el proceso de otro para empezar el suyo, además, varios departamentos tienen un mismo administrador de modo que los errores humanos se vuelven más frecuentes.

El primer capítulo describe el problema que tenía la institución financiera al tomarse mucho tiempo en reestablecer sus servicios luego de un desastre, también expone los objetivos del estudio y la solución para alcanzarlos.

El segundo capítulo contiene el sustento teórico de la tecnología y métodos implementados para la ejecución del proyecto.

En el tercer capítulo se detalla el estado de situación actual de la empresa, sus procesos, sus departamentos y responsables da las diferentes tareas sobre los sistemas.

En el cuarto capítulo menciona el desarrollo del proyecto, su ejecución a través de la herramienta de orquestación CRO y pruebas de funcionamiento donde se demuestra los beneficios de la solución.

CAPÍTULO 1

MARCO GENERAL

1.1. Antecedentes

La entidad financiera inicia su actividad en el año 1900, llegando a ser actualmente uno de los líderes en el territorio ecuatoriano, además, tiene presencia en muchos países a nivel mundial. La compañía cuenta con una gran infraestructura tecnológica que consta de aplicaciones, servidores y redes que soportan todas las operaciones del negocio.

Desde sus inicios la empresa ha pasado por varias transformaciones tecnológicas, aumentando gradualmente tanto su infraestructura física, como sus aplicaciones, manejando, además, grandes

volúmenes de datos de clientes y transacciones. A medida que evoluciona la tecnología, se van actualizando parcialmente los sistemas, agregando servicios y reemplazando también parte de los equipos que la soportan, coexistiendo tecnología antigua y moderna dentro de un ambiente funcional, sin embargo, en los últimos años la empresa ha tenido varias caídas en su sistema, provocando que los clientes no tengan acceso a realizar ningún tipo de actividad financiera sobre sus cuentas, generando así grandes pérdidas de dinero, e incluso clientes, lo cual se ve reflejado en los resultados obtenidos en los reportes mensuales.

Estas caídas frecuentes, además de las normativas financieras, motivaron a la empresa a implementar un plan de recuperación de desastres (DRP) que se ejecuta de forma total o parcial toda vez que se produzca un incidente. Este plan general se compone de los diferentes procesos que realiza manualmente cada área de tecnología, debiendo ejecutarse de forma secuencial, en un orden específico que permita levantar toda la infraestructura para reestablecer el sistema en su totalidad, tomándose mucho tiempo en reestablecer totalmente los servicios y generando desconfianza y malestar en los clientes de la entidad financiera.

El presente proyecto de titulación busca a través de BPMN, proponer un diseño optimizado del proceso de DRP actual, que permita reducir los tiempos de restablecimiento de los servicios, así como minimizar errores durante la ejecución del plan de recuperación de desastres. Y de esta manera responder a la siguiente pregunta:

¿En qué medida el diseño realizado con BPMN para automatizar el proceso DRP, cumple con el objetivo de satisfacer la necesidad del cliente interno?

1.2. Descripción del problema

Los tiempos de inactividad en una empresa, juegan un papel fundamental en el logro de la calidad de servicio que se pretende brindar a los clientes, teniendo en cuenta que a partir del consumo de estos se genera la rentabilidad de la empresa. Por lo que para mantener la confianza del cliente es fundamental reestablecer los servicios en el menor tiempo posible.

Se han identificado que los tiempos altos de inactividad son generados mayormente por la ejecución manual de los procesos de DRP[1], ya que los administradores son los encargados de ejecutarlas y estos

pueden administrar varias infraestructuras a la vez, lo cual provoca que la recuperación ante desastres sea ejecutada de manera secuencial en cada una de las infraestructuras administradas por cada especialista.

1.3. Solución propuesta

Cuando se produce un desastre, los diferentes departamentos de infraestructura inician sus procedimientos de recuperación de acuerdo con lo establecido en el proceso de DRP de la institución. Se han realizado análisis [2] que permiten identificar los problemas comunes durante la ejecución de un DRP, dentro de los cuales se menciona el alto tiempo definido para este proceso, para lo cual se ha definido una guía [3], la cual contiene las mejores prácticas para la implementación de este proceso que es de gran valor para la resiliencia.

Por lo que se propone reducir el tiempo de restablecimiento del sistema a través de la automatización y optimización del proceso actual de recuperación ante desastres.

Este nuevo modelo será implementado con el software (CRO) que se encargará de orquestar los procedimientos de recuperación en cada

sistema para reducir el tiempo de inactividad de los servicios productivos de la institución, lo que permitirá realizar la ejecución del proceso de DRP de algunos departamentos de manera simultánea, logrando optimizar los tiempos de RTO y RPO que manejan hoy en día la institución.

Algunas empresas han incursionado ya, en la automatización del proceso de recuperación ante desastres de ciertas plataformas [4] [5], logrando así evitar, afectaciones por errores humanos, la dependencia de recursos técnicos y minimizando los tiempos de inactividad de dichos servicios.

1.4. Objetivo General

Diseñar la automatización del proceso de recuperación ante desastres, utilizando BPMN para minimizar los tiempos de inactividad de la empresa.

1.5. Objetivos específicos

- Analizar el proceso DRP actual (AS-IS) de la empresa.

- Modelar el proceso DRP descriptivo, mediante BPMN automatizando los pasos de ejecución.
- Prueba del diseño optimizado del proceso de DRP mediante el uso de la herramienta Cloud Resiliency Orchestration (CRO).
- Evaluar el diseño de la propuesta a través de una encuesta de satisfacción, realizada al cliente interno.

1.6. Metodología

La presente investigación es de alcance descriptivo, ya que describe un diseño TO-BE de carácter analítico sobre la automatización del proceso de DRP, lo cual nos ayudará a cumplir con el objetivo principal, recogiendo información del modelo utilizado actualmente y detallando el problema y como se manifiesta.

Este estudio recolectará 2 variables:

Tabla 1. Metodología

Variable	Definición conceptual	Definición operacional
Tiempo	Tiempo total de ejecución de una prueba DRP manual.	Tiempo medido en horas y minutos.
Grado de satisfacción	Sentimiento de bienestar o placer que se tiene cuando se ha colmado un deseo o cubierto una necesidad.	Muy insatisfecho/insatisfecho/ ni insatisfecho ni satisfecho/satisfecho/muy satisfecho

La variable Tiempo será recolectada a través de la última prueba realizada en los ambientes productivos de la empresa, los cuales fueron llevados a cabo en las fechas del 30 abril hasta el 2 de mayo, lo cual permitirá tener un tiempo de referencia del total del tiempo que se lleva realizar un DRP manual.

Así mismo se prevé realizar una encuesta a los principales ejecutivos del área de infraestructura para determinar el grado de satisfacción o aceptación de la automatización del proceso de DRP, a través de la implementación de la herramienta CRO.

Mediante esta herramienta se configurará la automatización del proceso de DRP de hasta 4 aplicativos seleccionados por la empresa, para los cuales se deberá contar con ambientes de desarrollo y ventanas de trabajo (fuera de línea), para el desarrollo de las pruebas de DRP.

Se utilizará el método de muestreo no probabilístico por juicio, ya que serán seleccionados los principales ejecutivos del área de infraestructura, debido a que estos son los principales responsables y afectados en la operación.

Y se tomará el 10% del total de empleados de infraestructura (50), dando como resultado los 5 principales cargos, como son: 1 gerente de TI, 1 Líder de TI, y 3 líderes de área.

1.7. Resultados esperados

Mediante el desarrollo de este proyecto, se espera:

- Presentar un modelo BPMN del DRP optimizado y automatizado que sea aplicable para la empresa.
- Elaborar una guía de operación de la herramienta CRO.
- Demostrar la optimización de tiempos de RTO/RPO de la automatización del DRP mediante la ejecución de una prueba en 4 aplicativos seleccionados por la empresa.

CAPÍTULO 2

MARCO TEÓRICO

Esta sección introduce los conceptos básicos de los elementos utilizados en el proyecto para una mejor comprensión:

2.1. Plan de continuidad del negocio (BCP)

La Planificación y Gestión de la Continuidad del Negocio (BCP) son los actos de anticipación de interrupciones, asegurando la prevención o reducción de la posibilidad de ocurrencias y respondiendo a cualquier incidente de este tipo de manera planificada y ensayada para recuperar las pérdidas y hacer que el negocio vuelva a funcionar[6]. Las interrupciones pueden ocurrir con o sin previo aviso y los resultados pueden ser predecibles o desconocidos. El término Planificación de recuperación ante desastres (DRP) se usa con más frecuencia, pero en realidad es parte del marco más amplio de BCP[7]. DRP normalmente se ocupa de la continuidad de los servicios de

tecnología de la información (TI) y es principalmente de naturaleza técnica. Toda empresa necesita un BCP para enfrentar todas las posibles interrupciones y mantener su operación en funcionamiento con un tiempo de inactividad aceptable. Los objetivos son proteger vidas humanas, minimizar las pérdidas financieras y de reputación, continuar atendiendo a los clientes y cumplir con las leyes y reglamentos establecidos.

2.2. Plan de recuperación ante desastres (DRP)

2.2.1. Definición de DRP

Un plan de recuperación ante desastres (DRP), en inglés, es un conjunto de estrategias para proteger o recuperar su infraestructura tecnológica en caso de un desastre[8]. Por lo tanto, para lograr este objetivo son necesarios muchos factores internos y externos, como cuál es la base tecnológica, cuáles son los riesgos y cuáles son los desastres, establece el plan maestro.

Un plan de recuperación ante desastres (DRP) es un subcomponente de un plan de continuidad comercial (BCP) e incluye recursos de tecnología de la información. Garantiza que los sistemas críticos se reactiven dentro de un período de tiempo

mínimo especificado. También garantiza la recuperación de datos con una pérdida fija mínima.

2.2.2. Componentes de DRP

Figura 2.1

2.2.3. RPO

Un objetivo de punto de recuperación (RPO) es generalmente lo que se puede perder antes de que ocurra un daño significativo[2], el período de tiempo que es mejor para un negocio, desde el momento en que ocurre un evento crítico hasta que ocurre una copia de seguridad de alta prioridad. Se refiere a la cantidad de datos que se puede perder.

2.2.4. RTO

Un objetivo de tiempo de recuperación (RTO) suele ser la cantidad de tiempo que una aplicación[2], un sistema o un proceso pueden no estar disponibles y la cantidad de tiempo que se dedica a la recuperación sin daños significativos para el negocio. Restaurar la aplicación y sus componentes.

2.3. Metodologías para modelado de procesos del negocio

2.3.1. BPM

Una definición clave y detallada de lo que es BPM se puede encontrar en la guía de referencia de la Asociación Internacional de Profesionales de BPM, el cual indica que:

"Business Process Management o BPM es un enfoque sistemático para identificar, levantar, documentar, diseñar, ejecutar, medir y controlar tanto los procesos manuales como los automatizados, con la finalidad de lograr a través de sus resultados en forma consistente los objetivos de negocio que se encuentran alineados con la estrategia de la organización. BPM abarca el apoyo creciente de TI con el objetivo de mejorar, innovar y gestionar los procesos de principio a fin, que determinan los resultados de negocio, crean valor para el cliente

y posibilitan el logro de los objetivos de negocio con mayor agilidad".[9]

De lo que podemos resumir que BPM es una disciplina que ayuda a integrar las técnicas, los procesos del negocio y la tecnología, a través de los procesos.

BPM como sistema de gestión orientado a procesos incluye dos áreas principales de gestión empresarial:

- BPM Governance:

  Es un conjunto de medidas y procedimientos que rigen todos los servicios BPM que soportan la gestión de procesos de negocio, transformados en un marco que sirve como guía para entregar y operar de acuerdo con el concepto de BPM, también conocido como gobierno corporativo.

- BPM Operacional:

  Es el que incluye la gestión del ciclo BPM por procesos. Cada proceso puede estar en un estado diferente del ciclo. El ciclo comienza con dos posibles combinaciones de constelaciones:

El proceso debe ser desarrollado, documentado y/o rediseñado.

Debe ingresar un nuevo proceso que no existe en la organización.

2.3.2. BPMN

Business Process Modeling and Notation (BPMN) es una de las herramientas de modelado conceptual más populares para identificar los procesos de negocio integrados en un modelo de negocio. Ayuda a los analistas comerciales a crear un diagrama inicial regular de un diagrama de proceso comercial que puedan entender tanto los usuarios comerciales como los desarrolladores técnicos [10].

Algunas investigaciones se enfocan en analizar el modelo de procesos de negocio para asegurar el comportamiento esperado de los procesos. Los métodos obvios son simular y visualizar los comportamientos críticos de situaciones de trabajo específicas. El modelo de proceso BPMN se revisa y traduce a cualquier lenguaje de descripción de procesos específico para los simuladores de aplicaciones disponibles.

En nuestra propuesta será utilizado el software Bizagi Modeler para diseñar nuestro proceso automatizado de DRP.

Bizagi Modeler es un software gratuito capaz de modelar y documentar flujos de trabajo a través de diagramas de flujo y simulaciones gráficas que cumplen con el estándar BPMN (Business Process Modeling and Notation).

Esto le permite presentar su estrategia comercial de manera simple, y comprender y descubrir de manera sencilla e intuitiva dónde pueden ocurrir fallas en el desarrollo comercial

2.4. Automatización y orquestación de DRP

2.4.1. Automatización de DRP

La nube es uno de los avances tecnológicos más fundamentales que cualquiera puede utilizar. La forma en que usamos esta tecnología es importante. Hace tres décadas, la mayoría de los datos se almacenaban manualmente, lo que aumentaba el riesgo de pérdida de datos debido a cualquier tipo de desastre. Sin embargo, después de la introducción del almacenamiento en la nube, se redujeron los riesgos y costos. Debido a este factor, la gente aún prefiere almacenar datos muy importantes en su disco duro. Las copias de seguridad son la parte más importante de la creación de un entorno seguro. Cada aplicación se configura automáticamente para ejecutarse en la nube principal. Pero cuando la nube principal falla, el servidor tarda mucho en iniciarse. Mientras tanto, algo que se ofrece como alternativa podría llamarse la nube lejana. Esta técnica es ampliamente conocida como recuperación ante desastres [5]. En pocas palabras, es como una nube alternativa.

Incluso después de la introducción de la recuperación ante desastres en la nube y los sectores de copia de seguridad, esta actividad no se ha reducido ni remotamente. Aquí es donde entra en juego la automatización. El uso de la inteligencia artificial hace

que casi cualquier proceso sea fácil y sencillo. En este artículo, veremos algunas de las técnicas utilizadas para automatizar la recuperación ante desastres y encontraremos la solución adecuada.

Sin automatización, la única otra forma de recuperar datos es hacerlo manualmente. Esto da lugar a varios problemas como: alta probabilidad de pérdida de datos ya que está disperso y aumentará la carga para los usuarios, mayor carga de trabajo que conduce a más mano de obra/empleo simultáneo y demanda de mano de obra calificada. Aspectos técnicos de la recuperación ante desastres (es decir, todos los usuarios y administradores de bases de datos deben tener un conocimiento previo de las técnicas de recuperación), una gran cantidad de tareas que conducen a un mayor consumo de tiempo y un aumento repentino en el costo del trabajo adicional.

2.4.2. Framework IBM Cloud Resiliency Orchestration

IBM® Cloud Resiliency Orchestration (CRO) ofrece un enfoque de gestión de recuperación ante desastres (DR) unificado que ofrece validación de preparación de DR en tiempo real y pruebas y recuperación de DR automatizadas [11].

El servidor de orquestación permite la supervisión, la generación de informes, las pruebas y la automatización del flujo de trabajo de DR de infraestructuras y aplicaciones de TI complejas. La automatización y el análisis incorporados brindan DR más rápido y rentable para ayudar a mantener las operaciones comerciales diarias en funcionamiento y evitar de manera proactiva las interrupciones que conducen a la pérdida de ingresos, daños a la marca y clientes insatisfechos.

IBM CRO puede reducir los tiempos de prueba de DR y la conmutación por error de DR hasta en un 80 por ciento, lo que da como resultado una experiencia de DR más rentable que es más inteligente, personalizada y más ágil que nunca. Además, IBM CRO proporciona funciones de orquestación de procesos DR e impulsa otras plataformas y orquestadores de funciones en diferentes capas.

Algunos de sus principales características son:

- Abordar la resiliencia a nivel de proceso empresarial
- Mejore el RTO y el RPO

- Automatice la administración de conmutación por error de exploración
- Cree flujos de trabajo personalizados utilizando la biblioteca de automatización de recuperación
- Supervisión y gestión completas del ciclo de vida de DR
- Soporte de entorno heterogéneo
- Simplifique y acelere los procesos de recuperación ante desastres
- Complementos opcionales para servicios administrados
- Protección Air-gap y almacenamiento inmutable para recuperación
- Gestión de datos de copias

2.5. Normas y regulaciones aplicadas en TI para entidades financieras

Estableceremos normas y políticas internas relacionadas con la seguridad que deben ser consideradas para proteger la información.

El concepto de esta norma se deriva de las revisiones de las normas ISO 27000, 27001 y 27002 que brindan orientación sobre la seguridad de la información.

Una norma de seguridad es definida como un conjunto de reglas, recomendaciones y controles que tienen objetivos claros y apoyan las políticas de seguridad y los objetivos que desarrollan a través de capacidades, rendición de cuentas y otras técnicas, de acuerdo con las necesidades de seguridad establecidas para que la empresa lo haga.

Con base en estándares internacionales, a continuación de contemplan las principales normas ISO que son consideradas para una recuperación ante desastres de una empresa:

- ISO 27001

  Es un estándar internacional publicado por la Organización Internacional para la Estandarización (ISO) que describe cómo administrar la seguridad de la información dentro de una empresa. La última revisión de esta norma se publicó en 2013 y su nombre formal ahora es ISO/IEC 27001: 2013. La primera revisión se publicó en 2005 y se desarrolló bajo la norma británica BS 7799-2.[12]

- ISO 22301

Esta norma hace referencia a que dentro de cada empresa se debe implementar un sistema de gestión de continuidad del negocio para asegurar la continuidad de la cadena de suministro. El Sistema de gestión de continuidad de negocio, tiene por objeto proteger los procesos o servicios operativos críticos frente a la materialización de escenarios de riesgo. Las estrategias de continuidad deben probarse iniciando ejercicios para verificar el trabajo de reanudación.[13]

2.6. Delimitación

Para definir claramente el esfuerzo requerido para planificar las diversas actividades durante el diseño del DRP de la institución, primero se definirá las actividades a realizar dentro de este alcance:

- Implementación de la herramienta CRO.
- Creación de grupos de aplicación
- Creación de grupos de recuperación
- Ejecución de Dry Runs
- Ejecución de workflows de switchover y switchback [14]
- Medición de tiempos de switchover y switchback

Todas estas actividades se encuentran definidas y detalladas en el marco de la realización de este trabajo en la institución, y ya existe un

formato preestablecido para entrega del resultado de esta prueba y se encuentra definido en el capítulo 3.

CAPÍTULO 3

SITUACIÓN ACTUAL

3.1. Levantamiento de información del proceso actual

El departamento de infraestructura de TI se centra en la gestión de las distintas torres tecnológicas, por ejemplo: servidores Wintel, servidores iSeries, middleware, gestión de bases de datos; en donde se realizan diversos tipos de tareas con el fin de mantener el correcto funcionamiento del Servicio.

La institución ha realizado un análisis previo en donde ha identificado sus elementos críticos, conformados por aplicaciones, bases de datos, etcétera; los cuales son necesarios para mantener operativos los principales servicios que se brinda a la ciudadanía.

A su vez han levantado los procedimientos pertinentes para ejecutar paso a paso una recuperación óptima de todos los recursos que conforman este grupo.

Dentro del levantamiento de información, procuramos enlistar los elementos que conforman actualmente el DRP de la institución.

A continuación, se muestra una lista de activos identificados como significativamente afectados por la formación del desastre o que de alguna manera constituyen el DRP.

- Dispositivos de Firewall
- Servidores (Linux, Windows, AIX)
- Bases de datos (Oracle, MSSQL)
- Redes

La identificación de los principales actores de DRP, sus roles y responsabilidades es esencial para la activación exitosa de DRP, evitando interrupciones significativas en la operación del servicio, mediante la activación oportuna de las estrategias de recuperación. Es por lo que la institución ha identificado los siguientes actores como responsables de habilitar el DRP:

Tabla 2. Roles y Recursos del DRP

Roles	Recurso
Gerencia	Gerente de Infraestructura
Infraestructura	Jefe y arquitecto de infraestructura
Infraestructura	Líder de torre de base de datos
Infraestructura	Líder de torre de aplicativos
Infraestructura	Líder de torre de plataformas

De igual manera se encuentran identificados los procesos y subprocesos que deberán efectuarse de modo secuencial, estos serán ejecutados durante una prueba de switchover y switchback que se encuentra detallada en el capítulo 4.

A continuación, se detalla el responsable y el rol de los ejecutores del paso a paso del switchover y switchback de los aplicativos definidos dentro del alcance. La descripción de las tareas a realizar se visualizará en mayor detalle en la siguiente sección.

Tabla 3. Tareas y responsables del DRP

#Tarea	Responsable	Rol
1	Torre BDD	Especialista de Base de datos
2	Torre APP	Especialista de Aplicaciones
3	Torre Plataforma	Especialista de plataformas y sistemas operativos
4	Jefe de infraestructura	Jefe del departamento responsable principal del DRP
5	Usuario Final	Usuario convocado para realizar las pruebas del funcionamiento del aplicativo o servicio.

Uno de los objetivos principales de un DRP es el mantener los tiempos de RTO lo más bajos posible. Para la institución financiera se ha

recolectado los siguientes valores de acuerdo con los resultados obtenidos en sus pruebas anteriores.

Tabla 4. Aplicaciones y RTOs

APLICACIÓN	Switchover	Switchback
APP1	01:15:00	01:32:00
APP2	00:24:00	00:58:00
APP3	00:48:00	00:33:00
APP4	01:30:00	02:23:00

3.2. Definición de alcance de la propuesta

Para definir claramente el esfuerzo requerido para planificar las diversas actividades durante el diseño del DRP de la institución, primero se definirá las actividades a realizar dentro de este alcance:

- Implementación de la herramienta CRO.
- Creación de grupos de aplicación
- Creación de grupos de recuperación
- Ejecución de Dry Runs
- Ejecución de workflows de switchover y switchback [10]
- Medición de tiempos de switchover y switchback

Todas estas actividades se encuentran definidas y detalladas en el marco de la realización de este trabajo en la institución, y ya existe un formato preestablecido para entrega del resultado de esta prueba.

De acuerdo con nuestro alcance preestablecido, se realizará el análisis del proceso en 4 aplicativos que serán analizados, y medidos de manera inicial, para posterior de la prueba realizar una nueva medición que nos permita realizar comparaciones de los procesos e identificar el cumplimiento de nuestro objetivo.

A continuación, se enlistan el detalle de las plataformas que utilizan las aplicaciones que forman parte de nuestro alcance.

Tabla 5. Aplicaciones y plataformas

Aplicación	Plataforma
Aplicación 1	MSSQL + VEEAM REPLICATION + VSPHERE
Aplicación 2	ORACLE DATAGUARD+ ANSIBLE
Aplicación 3	ORACLE SINGLE + ANSIBLE + STORAGE
Aplicación 4	MSSQL + VEEAM REPLICATION + STORAGE

Estas aplicaciones han sido definidas con la institución financiera con el objetivo de validar los tiempos durante la ejecución de un DRP en las distintas plataformas que esta administra.

3.2.1. Proceso de Switchover actual

El proceso enlistado a continuación corresponde a los pasos de DRP para el switchover de cada uno de los aplicativos, basado en el formato descrito en la sección anterior. En caso de falla del switchover, se deberá escalar a los líderes de tecnología para cancelar la prueba.

- APP1

Tabla 6. Switchover APP1

#Tarea	Responsable	Tarea	Resultado esperado	Ubicación
1	Torre Plataforma	Apagado de servidores principales	Resultado 1	DC Principal
2	Torre BDD	Ejecutar actividades de réplica de MSSQL Always On	Resultado 2	DC Principal
3	Torre Plataforma	Ejecutar actividades de replicación de Vsphere	Resultado 3	DC Principal
4	Torre Plataforma	Encendido de servidores secundarios	Resultado 4	DC Secundario
5	Torre Plataforma	Levantar servicio en servidores de App	Resultado 5	DC Secundario
6	Torre Plataforma	Notificar a torre APP para validaciones	Resultado 6	DC Secundario
7	Torre APP	Realiza validaciones y confirma servicios	Resultado 7	DC Secundario
8	Jefe de infraestructura	Notifica a usuarios de prueba para validar	Resultado 8	NA
9	Usuario final	Realiza la prueba y garantiza el funcionamiento	Resultado 9	NA

- APP2

Tabla 7. Switchover APP2

#Tarea	Responsable	Tarea	Resultado esperado	Ubicación
1	Torre Plataforma	Apagado de servidores AIX con Ansible	Resultado 1	DC Principal
2	Torre BDD	Replicación de Oracle Dataguard	Resultado 2	DC Principal
3	Torre Plataforma	Encendido de servidores AIX con Ansible	Resultado 3	DC Secundario
4	Torre Plataforma	Notificar a torre APP para validaciones	Resultado 4	DC Secundario
5	Torre APP	Realiza validaciones y confirma servicios	Resultado 5	DC Secundario
6	Jefe de infraestructura	Notifica a usuarios de prueba para validar	Resultado 6	NA
7	Usuario final	Realiza la prueba y garantiza el funcionamiento	Resultado 7	NA

- APP3

Tabla 8. Switchover APP3

#Tarea	Responsable	Tarea	Resultado esperado	Ubicación
1	Torre Plataforma	Apagado de servidores AIX con Ansible	Resultado 1	DC Principal
2	Torre BDD	Replicación de Oracle Single con Storage	Resultado 2	DC Principal
3	Torre Plataforma	Encendido de servidores AIX con Ansible	Resultado 3	DC Secundario
4	Torre Plataforma	Notificar a torre APP para validaciones	Resultado 4	DC Secundario

5	Torre APP	Realiza validaciones y confirma servicios	Resultado 5	DC Secundario
6	Jefe de infraestructura	Notifica a usuarios de prueba para validar	Resultado 6	NA
7	Usuario final	Realiza la prueba y garantiza el funcionamiento	Resultado 7	NA

- APP4

Tabla 9. Switchover APP4

#Tarea	Responsable	Tarea	Resultado esperado	Ubicación
1	Torre Plataforma	Apagado de servidores principales	Resultado 1	DC Principal
2	Torre BDD	Ejecutar actividades de réplica de MSSQL Always On	Resultado 2	DC Principal
3	Torre BDD	Ejecutar actividades de replicación de storage	Resultado 3	DC Principal
4	Torre Plataforma	Encendido de servidores secundarios	Resultado 4	DC Secundario
5	Torre Plataforma	Levantar servicio en servidores de App	Resultado 5	DC Secundario
6	Torre Plataforma	Notificar a torre APP para validaciones	Resultado 6	DC Secundario
7	Torre APP	Realiza validaciones y confirma servicios	Resultado 7	DC Secundario
8	Jefe de infraestructura	Notifica a usuarios de prueba para validar	Resultado 8	NA
9	Usuario final	Realiza la prueba y garantiza el funcionamiento	Resultado 9	NA

3.2.2. Proceso de Switchback actual

El proceso enlistado a continuación corresponde a los pasos de DRP para el switchback de cada uno de los aplicativos, basado en el formato descrito en la sección anterior. En caso de falla del switchover, se deberá escalar a los líderes de tecnología para cancelar la prueba.

- APP1

Tabla 10. Switchback APP1

#Tarea	Responsable	Tarea	Resultado esperado	Ubicación
1	Torre Plataforma	Apagado de servidores principales	Resultado 1	DC Secundario
2	Torre BDD	Ejecutar actividades de réplica de MSSQL Always On	Resultado 2	DC Secundario
3	Torre BDD	Ejecutar actividades de replicación de Vsphere	Resultado 3	DC Secundario
4	Torre Plataforma	Encendido de servidores secundarios	Resultado 4	DC Principal
5	Torre Plataforma	Levantar servicio en servidores de App	Resultado 5	DC Principal
6	Torre Plataforma	Notificar a torre APP para validaciones	Resultado 6	DC Principal
7	Torre APP	Realiza validaciones y	Resultado 7	DC Principal

		confirma servicios		
8	Jefe de infraestructura	Notifica a usuarios de prueba para validar	Resultado 8	NA
9	Usuario final	Realiza la prueba y garantiza el funcionamiento	Resultado 9	NA

- APP2

Tabla 11. Switchback APP2

#Tarea	Responsable	Tarea	Resultado esperado	Ubicación
1	Torre Plataforma	Apagado de servidores AIX con Ansible	Resultado 1	DC Secundario
2	Torre BDD	Replicación de Oracle Dataguard	Resultado 2	DC Secundario
3	Torre Plataforma	Encendido de servidores AIX con Ansible	Resultado 3	DC Principal
4	Torre Plataforma	Notificar a torre APP para validaciones	Resultado 4	DC Principal
5	Torre APP	Realiza validaciones y confirma servicios	Resultado 5	DC Principal
6	Jefe de infraestructura	Notifica a usuarios de prueba para validar	Resultado 6	NA
7	Usuario final	Realiza la prueba y garantiza el funcionamiento	Resultado 7	NA

- APP3

Tabla 12. Switchback APP3

#Tarea	Responsable	Tarea	Resultado esperado	Ubicación
1	Torre Plataforma	Apagado de servidores AIX con Ansible	Resultado 1	DC Secundario
2	Torre BDD	Replicación de Oracle Single con Storage	Resultado 2	DC Secundario
3	Torre Plataforma	Encendido de servidores AIX con Ansible	Resultado 3	DC Principal
4	Torre Plataforma	Notificar a torre APP para validaciones	Resultado 4	DC Principal
5	Torre APP	Realiza validaciones y confirma servicios	Resultado 5	DC Principal
6	Jefe de infraestructura	Notifica a usuarios de prueba para validar	Resultado 6	NA
7	Usuario final	Realiza la prueba y garantiza el funcionamiento	Resultado 7	NA

- APP4

Tabla 13. Switchback APP4

#Tarea	Responsable	Tarea	Resultado esperado	Ubicación
1	Torre Plataforma	Apagado de servidores principales	Resultado 1	DC Secundario
2	Torre BDD	Ejecutar actividades de	Resultado 2	DC Secundario

		réplica de MSSQL Always On		
3	Torre Plataforma	Ejecutar actividades de replicación de storage	Resultado 3	DC Secundario
4	Torre Plataforma	Encendido de servidores secundarios	Resultado 4	DC Principal
5	Torre Plataforma	Levantar servicio en servidores de App	Resultado 5	DC Principal
6	Torre Plataforma	Notificar a torre APP para validaciones	Resultado 6	DC Principal
7	Torre APP	Realiza validaciones y confirma servicios	Resultado 7	DC Principal
8	Jefe de infraestructura	Notifica a usuarios de prueba para validar	Resultado 8	NA
9	Usuario final	Realiza la prueba y garantiza el funcionamiento	Resultado 9	NA

3.3. Levantamiento de modelo AS-IS utilizando BPMN

La imagen del (**Anexo F**) representa el diseño individual de los procesos ejecutados actualmente por los especialistas en cada uno de los aplicativos.

Estas acciones se llevan a cabo de forma sucesiva en los aplicativos satélites (AG_SATELITES) primeramente y luego los dos restantes que conforman el núcleo (AG_CORE) como se muestra en la imagen a continuación, finalizando con un reporte de los resultados de ejecución del proceso completo.

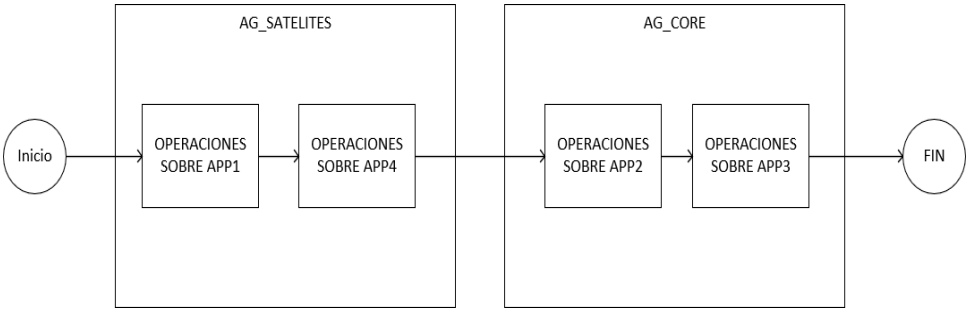


Figura 3.1

3.4. Análisis de datos recolectados

Tomando como punto de inicio la información recolectada anteriormente con la institución financiera y el Modelo AS-IS, se realizó un análisis del modelo para identificar problemas que presenta el proceso tal cual como se lo lleva actualmente.

En general, se intenta aprovechar la oportunidad para llevar a la empresa a iniciar un proceso de automatización de procesos, que conlleve a la mejora del proceso actual, para el cual se implementará un piloto de esta versión, la cual nos permitirá identificar los tiempos de mejora que la solución nos ofrece, brindándoles de esta manera un diseño optimizado a la institución financiera, que les permita reestablecer sus servicios de manera ágil durante cualquier tipo de desastre que se presente.

3.5. Análisis de desperdicios y riesgos

Una vez recopilada la información, se realizó un análisis objetivo y pragmático para esclarecer los desperdicios involucrados en los procesos descritos hasta el momento. A continuación, se presenta un resumen de este análisis.

- La institución financiera mantiene tiempos de ejecución de DRP muy altos, esto debido a que los procesos se ejecutan de manera secuencial, lo cual limita al recurso de la torre siguiente.
- Para la ejecución de procesos de switchover y switchback se utiliza al mismo ejecutor (especialista responsable de la torre), por lo que se debe culminar con la APP# para avanzar con la APP#.
- Existen riesgos durante la ejecución del proceso de DRP ya que se identifica que no todos los procesos están claros para su ejecución, es decir es de entendimiento únicamente para el especialista responsable de la torre.

3.6. Definición de encuesta

Dentro de nuestra metodología se encuentra definida la encuesta a realizar al departamento de infraestructura, los cuales son los principales ejecutores y responsables del proceso de DRP, para evaluar su satisfacción en cuanto a la operación de la herramienta y

cumplimiento de los objetivos, principalmente el de la reducción de tiempos de RTO.

A continuación, se define la encuesta que será realizada a los recursos indicados.

Tabla 14. Encuesta

De acuerdo con la ejecución del DRP actual, que se realiza de forma manual, como se siente respecto a..	**Muy insatisfecho**	**Insatisfecho**	**Ni insatisfecho / Ni satisfecho**	**Satisfecho**	**Muy satisfecho**
1.- Facilidad de ejecución del DRP			X		
2.- Tiempo de RTO que toma en ejecutarse el DRP			X		
3.- Entendimiento del proceso de ejecución		X			
4.- Facilidad en la generación de reporte	X				
5.- Cumplimiento de los objetivos planteados				X	

CAPÍTULO 4

DISEÑO DE AUTOMATIZACIÓN DEL PROCESO

4.1. Diseño del modelo TO BE utilizando BPMN

El proceso optimizado presenta cambios radicales frente al inicial puesto que el software orquestador interactúa directamente con los sistemas, tanto en monitoreo como en la ejecución total o parcial de recuperación ante desastres de acuerdo con la configuración aplicada.

El nuevo proceso de recuperación muestra la interacción de los diferentes actores con la herramienta de orquestación implementada.

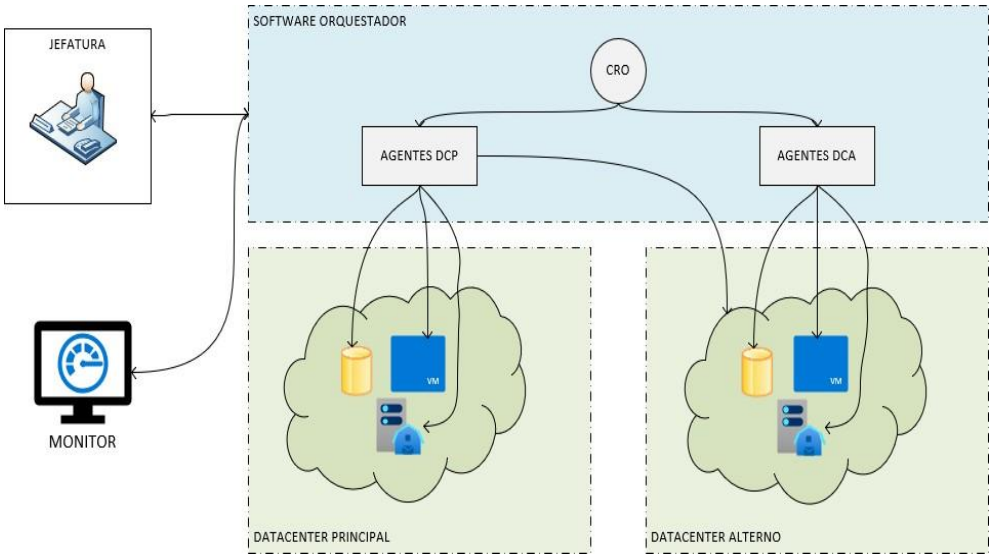


Figura 4.1

El modelo (**Anexo G**) representa el nuevo proceso DRP realizado por la herramienta de orquestación y su interacción con los usuarios que intervienen.

A diferencia del proceso inicial, que ejecuta total y secuencialmente la recuperación, la configuración en el software de orquestación permite la recuperación parcial y de forma simultánea de varios segmentos de la infraestructura, lo que permite reducir el tiempo total de ejecución.

Para realizar las comparaciones de tiempo se debe simular un máximo de tiempo utilizado por el proceso de recuperación optimizado, frente al proceso manual.

4.2. Implementación de la herramienta de automatización

4.2.1. Introducción a CRO

IBM® Cloud Resiliency Orchestration (CRO) ofrece un enfoque unificado de gestión de recuperación tras desastre (DR) que ofrece validación de preparación de DR en tiempo real y pruebas de DR y recuperaciones automatizadas.

La solución de CRO incorpora un software líder del mercado de recuperación de desastres que orquesta las infraestructuras y aplicaciones de DR para proporcionar información sobre Recovery Time Objectives (RTO). RTO y Recovery Point Objectives (RPO).

Esta solución de orquestación combina monitoreo, reporte, pruebas, y automatizaciones de workflows de infraestructuras complejas en una solución escalable proporcionando una solución unificada de resiliencia para gestionar la recuperación.

Uno de los objetivos de este proyecto es proporcionar la solución CRO para las aplicaciones en el alcance de preestablecido en la

sección anterior, describiendo la infraestructura y componentes requeridos para desplegar KYNDRYL Orchestration servers, mismos que serán usados para gestionar la recuperación de las aplicaciones antes descritas.

4.2.2. Arquitectura de la solución

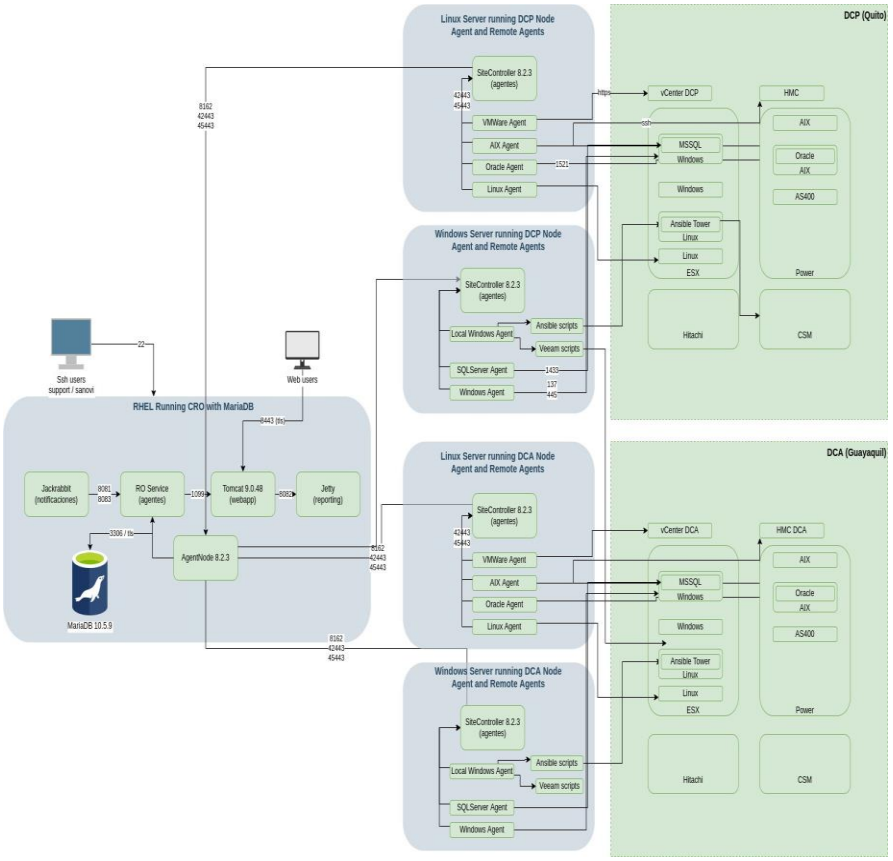


Figura 4.2

La Figura anterior proporciona una vista general de los Objetos Orquestados y como ellos interactúan con el servidor DRM en el Datacenter alterno.

Cada uno de los recuadros sombreados corresponden a cada uno de los nodos de CRO:

DRM (CRO Máster) Es el servidor principal donde reside la lógica de las orquestaciones y la interfaz de usuario para la gestión del DR. El servidor principal se encuentra en el Site de Recovery para tener visibilidad siempre de los elementos de infraestructura

- *Site Controllers* Son los servidores donde ejecutan los agentes que es el lugar donde ejecutan las orquestaciones y los comandos remotos que son ejecutados en los componentes de infraestructura.

Existen dos tipos de Site Controllers ubicados en cada Datacenter:

- *Windows* Usado para gestionar máquinas virtuales windows y servicios que operan sobre este sistema

operativo como MSSQL, Exchange, Domain Controllers, componentes .net.

- *Linux* Usado para gestionar sistemas *NX como AIX, Linux, Solaris, así como plataformas de appliances como almacenamientos, componentes de red, vcenters (vía TLS).
- *Infraestructura* En color verde oliva, son los servidores y almacenamientos de Entidad Financiera afectados por la operación de Recuperación de Desastres.

Como se observa en el diagrama, los agentes se ejecutan en los Site Controllers (gris) y se conectan a los componentes en los Esx o en los servidores power vía protocolos clientes, mientras que la comunicación entre los SiteControllers y el DRM se hacen usando puertos asegurados por TLS (42443 y 45443)

En el DRM el Agent Node coordina los SiteControllers basado en la configuración indicada por el servicio de RO (también llamado panaces), la cual esta almacenada en la base de datos MariaDB.

4.2.3. Funcionalidad de la herramienta

Para ingresar a la consola maestra de (CRO Máster GUI), se realiza a través de una URL en el navegador de internet con acceso a la IP respectiva:

Figura 4.3

En esta página se pueden visualizar en el cuadro superior derecho los sitios gestionados por CRO, así como el número de Recovery Groups (grupos de componentes) y las Application Groups (aplicaciones) gestionados por la plataforma.

De igual manera desde aquí se puede llegar a las opciones de ciclo de vida de CRO como son:

- **Discover:** Configuración de Sites, componentes, bases de datos o mecanismos de réplica, así como plataformas de

virtualización, gestión de almacenamiento, credenciales y coordinadores de agentes

- **Monitor:** Para monitorear el estado de los grupos de componentes y aplicaciones en preparación a la ejecución de operaciones de recuperación de desastres
- **Manage:** Para ejecutar y seguir los scripts de automatización y las orquestaciones en la herramienta
- **Drill:** Para ejecutar las pruebas y validaciones de ejecuciones
- **Reports:** Para la generación de informes y obtención de evidencias de las pruebas para los organismos de control interno y externo

Inicialmente se ingresa por el botón de **Monitor** el cual nos llevará a la página de monitoreo. Esta página nos muestra los sitios, Grupos de Aplicaciones (AG), Grupos de Recuperación (RG) y detalle de los Workflows en ejecución. Desde esta opción se puede redirigir directamente a las opciones de Manage, Drill, y Report en las cuales se puede seleccionar directamente los grupos para esos detalles.

Figura 4.4

➢ **Subsystems**: muestra los detalles relacionados a los Componentes (servidores físicos y virtuales, máquinas virtuales o LPARs), Datasets (bases de datos o gestores de servicios) y Protection Schemes (esquemas de protección como Dataguard, Hitachi Universal Replication y otros).

Figura 4.5

En la pestaña de componentes de los Subsystems, podemos encontrar los componentes Windows, AIX y Linux listados. Sin embargo, en el caso de componentes gestionados a través de plataformas de virtualización, podrían no aparecer en dicho listado (esto aplica para las máquinas Windows gestionadas a

través del vCenter que son replicadas mediante Veeam, o para los componentes Ansible gestionados a través de la plataforma de Ansible Tower).

Así como las definiciones de conexiones a bases de datos MSSQL (Sql Server) y oracle en la pestaña de Datasets.

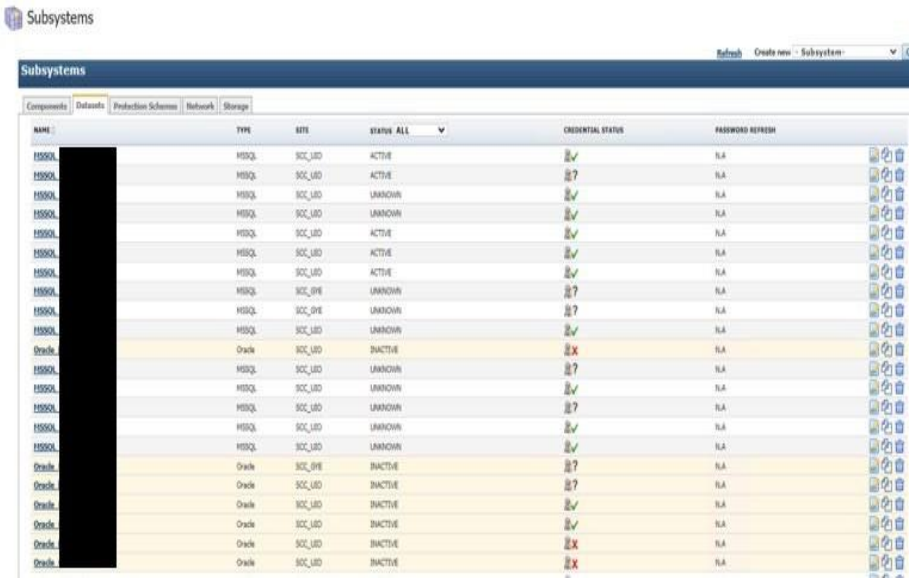


Figura 4.6

La conexión a los componentes, datasets y protection schemes se hace usando credenciales que pueden estar definidas por cada subsistema o definidas de manera general en la bóveda de credenciales (credential vault).

Para la entidad financiera se tienen definidos usuarios por plataforma con credenciales que no expiran (en caso de que expiren se deben actualizar en esta ventana mediante un procedimiento definido por la institución).

En cada uno de los menús de navegación existe más de una forma de llegar a las opciones de menú (navegación cruzada). Es importante notar que estando en los menús de Monitor, Manage o Drill es posible llegar a los otros menús vía el menú desplegable superior izquierdo. Estas pestañas contienen las siguientes opciones:

Las pestañas de CRO DRM incluyen:

- **Admin:** Contiene todas las Operaciones como Administrador.
- **Monitor:** Contiene los Sitios, Grupos de Aplicaciones (AG), Grupos de Recuperación (RG) y la pestaña de flujos de ejecución (Salud del Grupo, detalles del RPO, detalles de RTO, estado de las réplicas, estado de las bases de datos, etc).
- **Manage:** Contiene las acciones de inicio/detención de las réplicas, el botón de Failover y los workflows a ejecutar.
- **Drill:** Contiene los enlaces para ejecutar el Switch Over / Switch Back.

- **Reports:** Contiene los reportes actuales e históricos como reportes del drill, reportes de RPO, y reportes de tendencias de RPO.
- **Discovery:** Contiene toda la información de configuración de CRO DRM como detalles de direcciones IP, detalles de los grupos, definiciones de los workflows, credenciales, etc.

4.2.4. Operaciones de administración

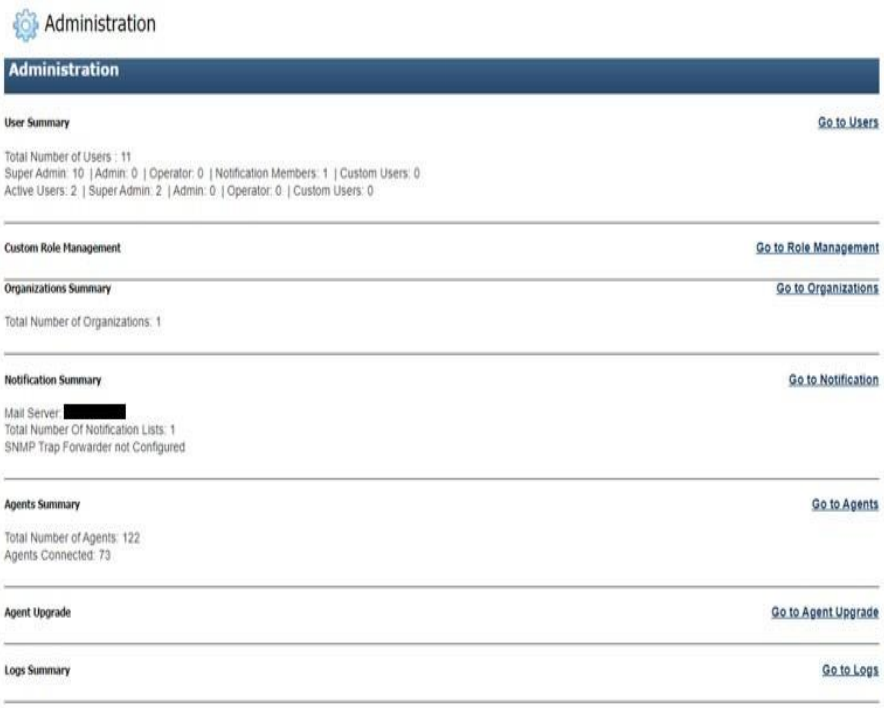


Figura 4.7

El menú de administración (rueda dentada superior derecha) comparte todos los detalles relacionados con la configuración de Usuarios, Notificaciones, Agentes, Logs, Backup, Failover del servidor CRO, Historia Operacional, Licenciamiento, y eventos del Sistema.

- **User:** Lista los usuarios creados para operaciones.
- **Notification:** Muestra la configuración de envió de correos electrónicos para alertamiento.
- **Agents:** Muestra el número de agentes conectados al servidor CRO DRM.
- **Logs:** Permite la recuperación de los logs clientes (agentes y DRM).
- **Backup:** Muestra el estado del backup de la Metadata, la ruta, así como la periodicidad con la que se toma y la retención.
- **Server Failover:** Muestra los detalles del log de María DB para el servidor Secundario, así como cuando se puede ejecutar el failover para CRO DRM.
- **Operational History:** Muestra la retención y depuración de la metadata en CRO DRM, así como la retención de los logs y permite modificarla.
- **License:** Muestra los detalles de la licencia y la fecha de expiración.

- **System events**: Muestra los detalles de los eventos con la descripción del evento, la severidad y el impacto.

A continuación, detallaremos los parámetros esenciales que se manejan para la administración de la herramienta.

- **[Admin] > Users:**

Hay 4 tipos de roles de usuarios disponibles en CRO:

1. Super Administrators: Usuarios con este rol pueden ejecutar cualquier actividad.
2. Administrators: Usuarios con este rol pueden hacer todas las actividades excepto crear usuarios.
3. Operators: Los usuarios con este rol pueden ingresar y monitorear la ejecución, pero no pueden efectuar ninguna actividad.
4. Notification Users: Estos usuarios pueden recibir notificaciones por correo, pero no tienen la posibilidad de ingresar en la plataforma.

- **[Admin] > Agents:**

La pestaña de agentes permite visualizar el estado de los agentes conectados al servidor CRO DRM incluyendo detalle de las versiones, nombre del componente, y estado de la conectividad. Si un agente no está conectado, es un indicativo que hay algún problema afectando la conectividad o con el estado del servicio que ejecuta el agente y que por lo tanto el agente está caído. Los agentes pueden ser iniciados o detenidos desde esta página.

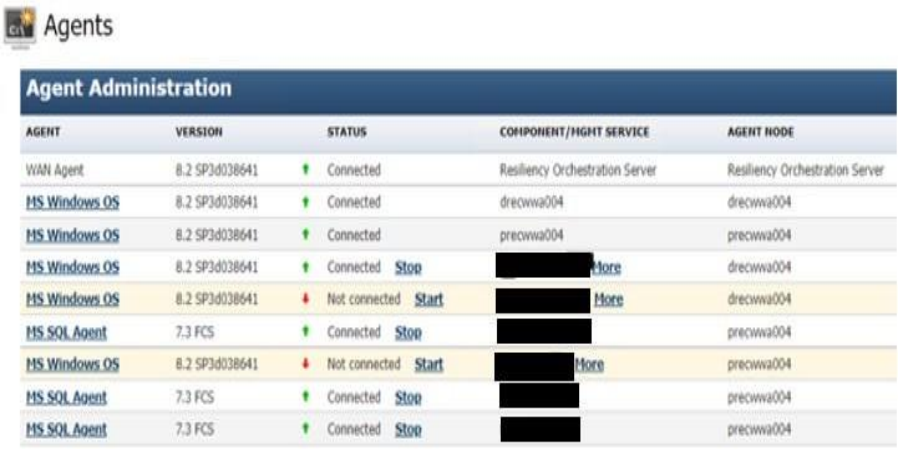


Figura 4.8

Cada agente tiene un enlace para detener (stop) o iniciar (start) el agente. En el caso de los agentes unificados (agentes que administran múltiples componentes normalmente asociados a sistema operativo) se puede ver el detalle de los componentes

administrados seleccionando el enlace (More). En el cuadro de diálogo desplegado se muestra el nombre del UNI_Agente y la ruta donde se pueden ubicar los logs de dicho agente.

Los 3 primeros agentes corresponden a los agentes asociados al servidor DRM (AgentNode) y los site controllers Windows (drecwwa004 y precwwa004)

Las columnas de Agent Node y Site Controller indican cuales son los Site Controllers que gestionan ese agente (el site controller donde se ejecuta), lo cual es importante para ubicar los archivos de log y para identificar los procesos de sistema operativo asociados al agente; y el agente de nodo, el cual es el componente a través del cual se comunica el agente con el DRM, el cual normalmente debería corresponder al SiteController que gestiona el agente

Esta distribución de los agentes impacta la distribución de cargas en la plataforma y en la mayoría de los casos es gestionada automáticamente por CRO.

4.3. Tableros de control

Para la Entidad Financiera se monitorea el estado de las réplicas para las bases de datos Oracle y SQL Server que usan AlwaysOn como mecanismo de réplica para asegurar que los grupos de consistencia estén en un estado saludable para el failover durante un evento de recuperación de Desastres (DR event).

CRO está configurado de manera que envíe correos a los operadores configurados si la réplica está detenida para una aplicación en particular. Mediante los tableros de control se puede monitorear el estado de las réplicas en una vista única en la interfaz de usuario de CRO. En el caso de presentarse un evento, se debe tomar acción inmediata para cumplir con los SLAs.

4.4. Tablero de control de nivel de Objetos

Para acceder al Tablero de Nivel de Objetos, ingrese a CRO usando sus credenciales -> clic en monitor -> clic en Recovery Groups.

Este tablero da el nivel de estado de los RPO y RTO para cada Recovery Group, detallando el estado de saludo en general para todos los componentes en ese Grupo, la comparación del RG RPO contra el umbral configurado, y el RTO del RG basado en la ejecución previa de eventos de failover.

Éste es el tablero más frecuentemente utilizado durante la operación de la plataforma

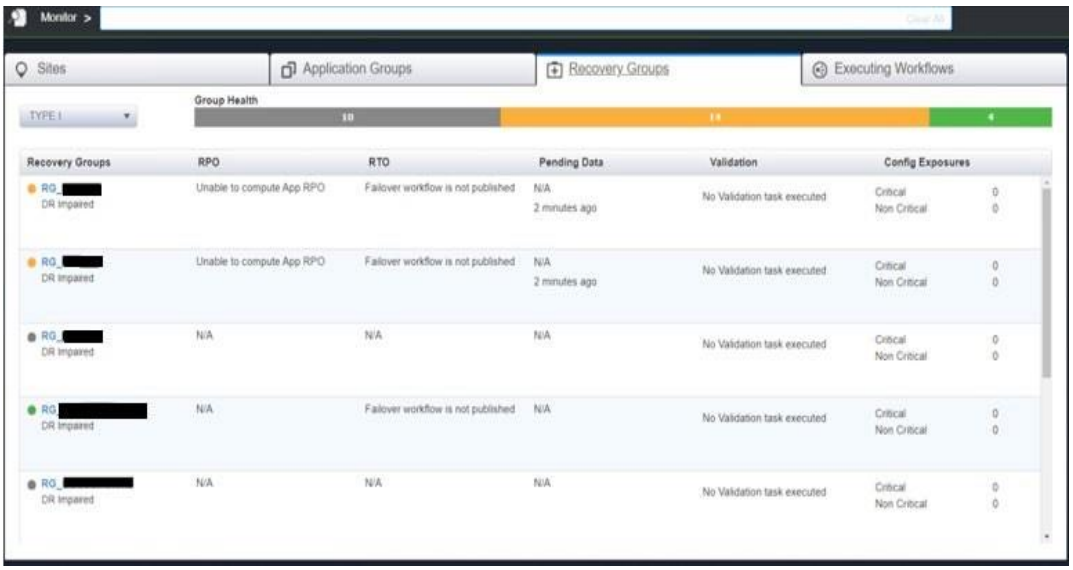


Figura 4.9

4.5. Tablero Gerencial

Para acceder al Tablero Gerencial (Managers Dashboard), ingrese a CRO usando sus credenciales. En la ventana de llegada a CRO (Landing Page) haga clic en el botón [Disaster Recovery] ubicado en la esquina inferior derecha. Esto abrirá una nueva página con el tablero Gerencial.

La imagen a continuación muestra un ejemplo del resultado del tablero y las herramientas de monitoreo proporcionadas para ver el estado de su infraestructura y aplicaciones.

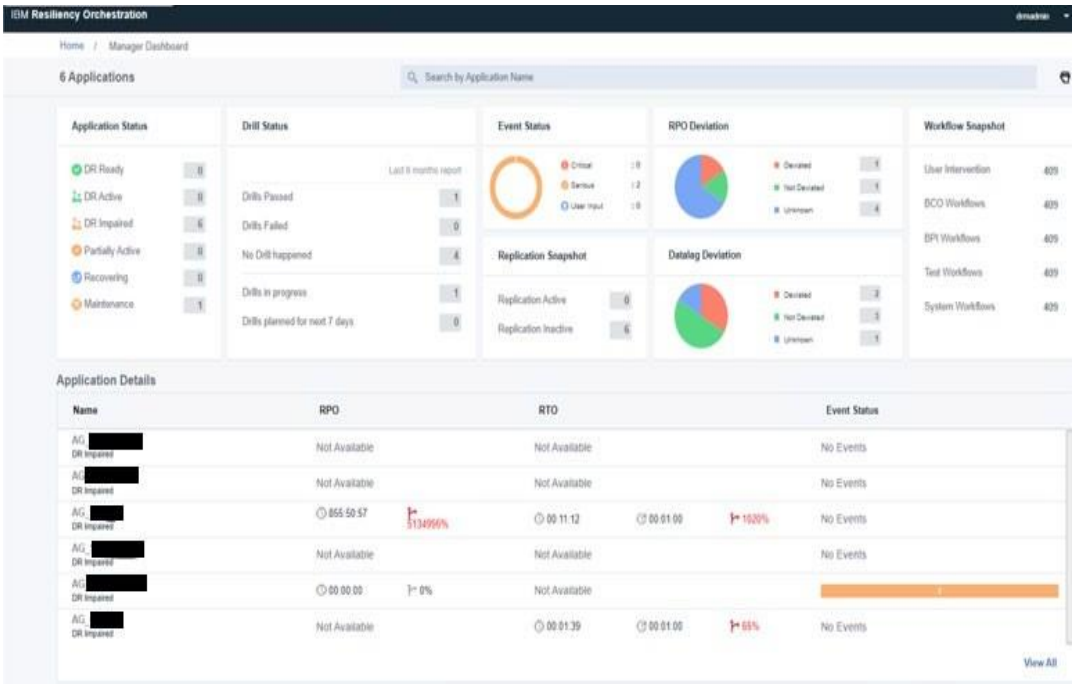


Figura 4.10

4.6. Configuración de grupos

La lógica de ejecución de CRO se encuentra configurada en los Grupos a los que se accede por el menú de Discover por la opción de Grupos o desde el menú de Drills.

Para la entidad financiera se realizó la creación de 2 grupos de aplicaciones, que se encuentran operacionales.

4.7. Grupos de recuperación

Para la institución financiera se encuentran configurados 10 grupos de aplicaciones:

Existen 3 grupos de aplicaciones que son de pruebas

- **RG_Sanbox** Usado para hacer pruebas de concepto de nuevas funcionalidades como automatizaciones de Veeam o de Ansible. La idea es que los nuevos usuarios que se adicionen solo puedan conectarse a este grupo para no ejecutar operaciones contra componentes productivos
- **RG_Tests** Usado para pruebas en ambientes no productivos (ejemplo BANCS de pruebas)
- **RG_Veeam** Usado para pruebas con Veeam

Los grupos configurados para entornos productivos se clasifican en dos tipos: aplicaciones y bases de datos, eventualmente en aplicaciones multi-tier podría existir grupos adicionales de integración, pero lo que está configurado actualmente para institución financiera solo considera aplicaciones y bases de datos

- *Aplicaciones*

  1. RG_APP1 Aplicación Webteller
  2. RG_APP2 Aplicación Notificador
  3. RG_APP3 Aplicación Omni
  4. RG_APP4 Aplicación CNB

- *Bases de datos de APP1*

  1. RG_DB1

- *Bases de datos de APP2 (Oracle single)*

  1. RG_DB2 Base de datos de Automatizaciones del Notificador
  2. RG_DB3 Base de datos del Notificador

- *Bases de datos de APP3 (Oracle RAC Multi-tenant)*

  1. RG_DB4 Base de datos de Omni
  2. RG_DB5 Base de datos log de Omni
  3. RG_DB6 Base de datos 2 de Omni

- Bases de datos APP4

1. RG_DB7 Base de datos de la aplicación CNB

Como regla general los Recovery Groups no probados se configuran en modo mantenimiento para que no sean ejecutados y los componentes no en operación ni en pruebas se sacan de gestión colocándolos también en modo mantenimiento.

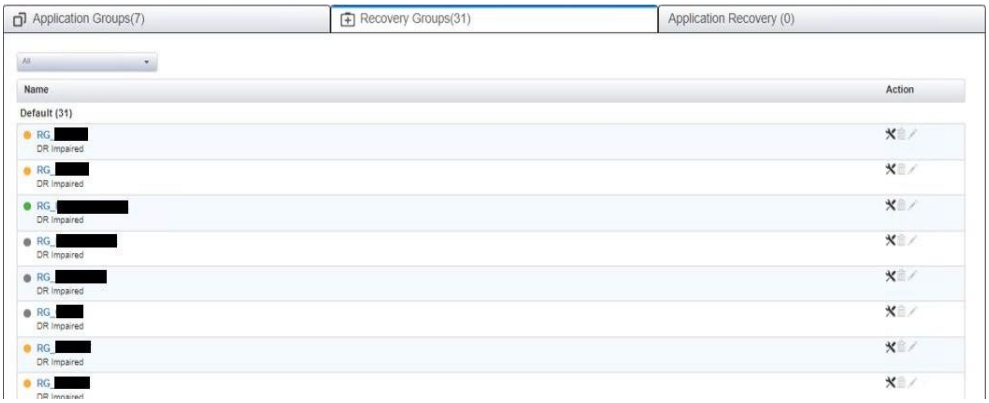


Figura 4.11

4.8. Definición de casos de prueba

Tal como se mencionó en la introducción, el alcance de las pruebas se basará en la funcionalidad de 4 aplicativos, los cuales contarán con la ejecución de un “switchover” y un “switchback” para determinar los tiempos de RTO y RPO de cada uno de estos aplicativos.

Hay dos operaciones de recuperación de desastres configuradas para cada uno de los Recovery Groups:

- Switchover
- Switchback

Todos esos workflows pueden ser ejecutados únicamente por usuarios con privilegios Admin o Super Admin. Se sugiere que tres días antes a la ejecución de la prueba se ejecuten los DryRun y se revisen los reportes de ejecución previos a la ejecución del evento de Recuperación de Desastres programado.

Switchover es el escenario donde el ambiente de DR se activa moviendo la operación desde el ambiente de producción. Esta modalidad se usa para validar la operación en el sitio alterno e impacta

la operación en producción y no es exactamente igual a un Failover ocurrido durante un evento de desastre.

En la detención se comienza por la detención de las aplicaciones de CORE previo a la detención de aplicaciones externas entre las que se encuentran las APP definidas anteriormente (APP1-4). Se describe a continuación los escenarios validados en las pruebas.

- **Switchover Start**

Para detener la aplicación de CORE se realiza la detención de las aplicaciones satélites inicialmente para finalizar deteniendo los servicios propios de la aplicación CORE como se describe a continuación.

AG_SATELITES (Aplicaciones Windows replicadas por Veeam)

Tabla 15. Grupo AG_Satelites

Aplicación	Nombre de la aplicación	Recovery Group	Workflow	Secuencia
APP1	APP1	RG_APP1	StopAppPR	1
	DB1	RG_DB1	switchover	2
	APP1	RG_APP1	StartAppDR	3
APP4	APP4	RG_APP4	StopAppPR	4
	DB7	RG_DB7	switchover	5
	APP4	RG_APP4	StartAppDR	6

AG_CORE (Aplicaciones AIX y Oracle)

Tabla 16. Grupo AG_Core

Aplicación	Nombre de la aplicación	Recovery Group	Workflow	Secuencia
APP2	APP2	RG_APP2	StopAppPR	1
	DB2	RG_DB2	switchover	2
	DB3	RG_DB3	switchover	3
	APP2	RG_APP2	StartAppDR	4
APP3	APP3	RG_APP3	StopAppPR	5
	DB4	RG_DB4	switchover	6
	DB5	RG_DB5	switchover	7
	DB6	RG_DB6	switchover	8
	APP3	RG_APP3	StartAppDR	9

A continuación, se muestra el flujo integrado donde se visualiza el Application Group denominado AG_CORE en el workflow denominado Switchover.

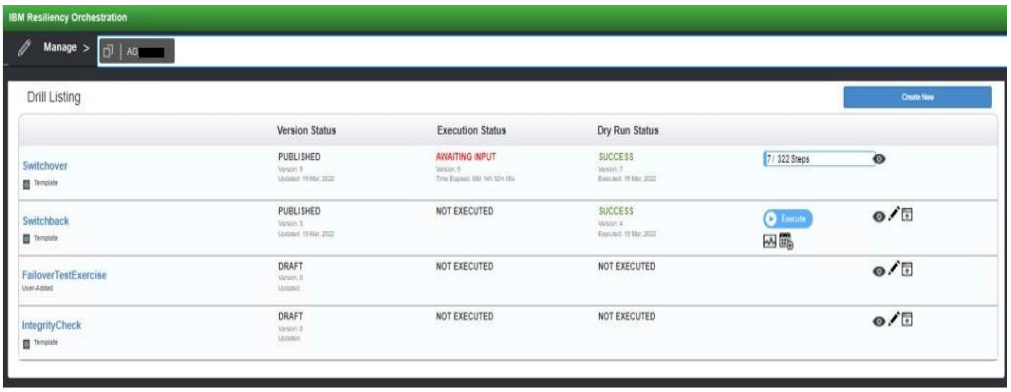


Figura 4.12

Algunas de las aplicaciones pueden ser detenidas al tiempo que otras, por lo que la secuencia es una guía, pero corresponde al orden implementado en el workflow maestro de esta aplicación.

Switchback es el escenario donde el ambiente de DR se activa moviendo la operación desde el ambiente de producción. Esta modalidad se usa para validar la operación en el sitio alterno e impacta la operación en producción y no es exactamente igual a un Failover ocurrido durante un evento de desastre.

En la detención se comienza por la detención de las aplicaciones de CORE previo a la detención de aplicaciones externas entre las que se encuentran las APP definidas anteriormente (APP1-4). Se describe a continuación los escenarios validados en las pruebas.

- **Switchback Start**

Para detener la aplicación de CORE se realiza la detención de las aplicaciones satélites inicialmente para finalizar deteniendo los

servicios propios de la aplicación CORE como se describe a continuación.

AG_SATELITES (Aplicaciones Windows replicadas por Veeam)

Tabla 17. Aplication Group Satelites

Aplicación	Nombre de la aplicación	Recovery Group	Workflow	Secuencia
APP1	APP1	RG_APP1	StopAppDR	1
	DB1	RG_DB1	switchback	2
	APP1	RG_APP1	StartAppPR	3
APP4	APP4	RG_APP4	StopAppDR	4
	DB7	RG_DB7	switchback	5
	APP4	RG_APP4	StartAppPR	6

AG_CORE (Aplicaciones AIX y Oracle)

Tabla 18. Application Group Core

Aplicación	Nombre de la aplicación	Recovery Group	Workflow	Secuencia
APP2	APP2	RG_APP2	StopAppDR	1
	DB2	RG_DB2	switchback	2
	DB3	RG_DB3	switchback	3
	APP2	RG_APP2	StartAppPR	4
APP3	APP3	RG_APP3	StopAppDR	5
	DB4	RG_DB4	switchback	6
	DB5	RG_DB5	switchback	7
	DB6	RG_DB6	switchback	8
	APP3	RG_APP3	StartAppPR	9

A continuación, se muestra el flujo integrado donde se visualiza el Application Group denominado AG_CORE en el workflow denominado Switchback.

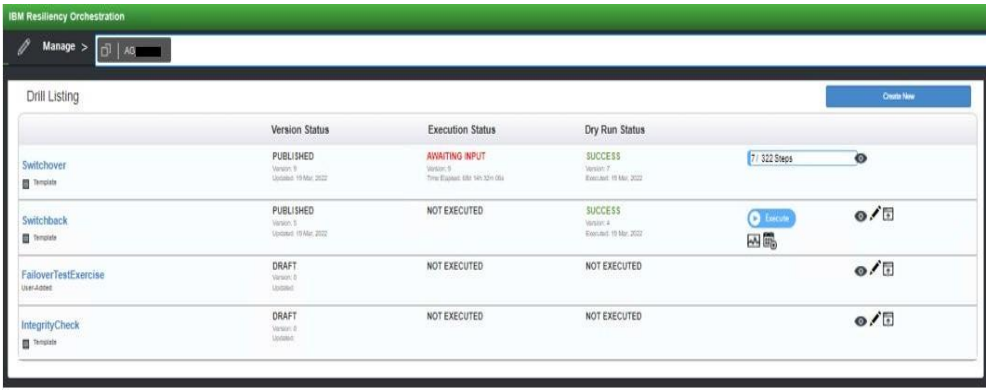


Figura 4.13

4.9. Prueba del modelo propuesto

Previo a las pruebas de switchover y switchback se ejecutarán "Dryruns", para validar la funcionalidad de las workflows configurados.

4.9.1. Ejecución DryRun

El DryRun es una simulación de la ejecución del workflow con el fin de obtener un reporte detallado de las conexiones, permisos, credenciales, comandos, y scripts a ejecutar en la operación de DR. Éste no ejecuta las acciones actuales, es decir es una ejecución en background, por lo que es seguro ejecutar el DryRun cualquier número de veces.

El DryRun puede ser ejecutado en los workflows maestros o en cada uno de los workflows detallados individuales.

Para ejecutar el DryRun, haga clic en el workflow denominado StopAppPR en el botón con el ícono de un gráfico de líneas inmediatamente bajo el botón de ejecutar (aun no ejecutar) para realizar la operación de validación.

4.9.2. Verificar reporte de DryRun

Ejecute el DryRun y compárelo con los reportes previos del mismo workflow ayuda a mejorar el éxito de la prueba. En el caso que se encuentren diferencias, se debe tener un entendimiento y solucionar los incidentes presentados.

Para ver el resultado de los DryRun navegue a la opción de Reports desde la pantalla del GUI principal.

Se selecciona el recovery Group deseado, desde el cuadro de la derecha.

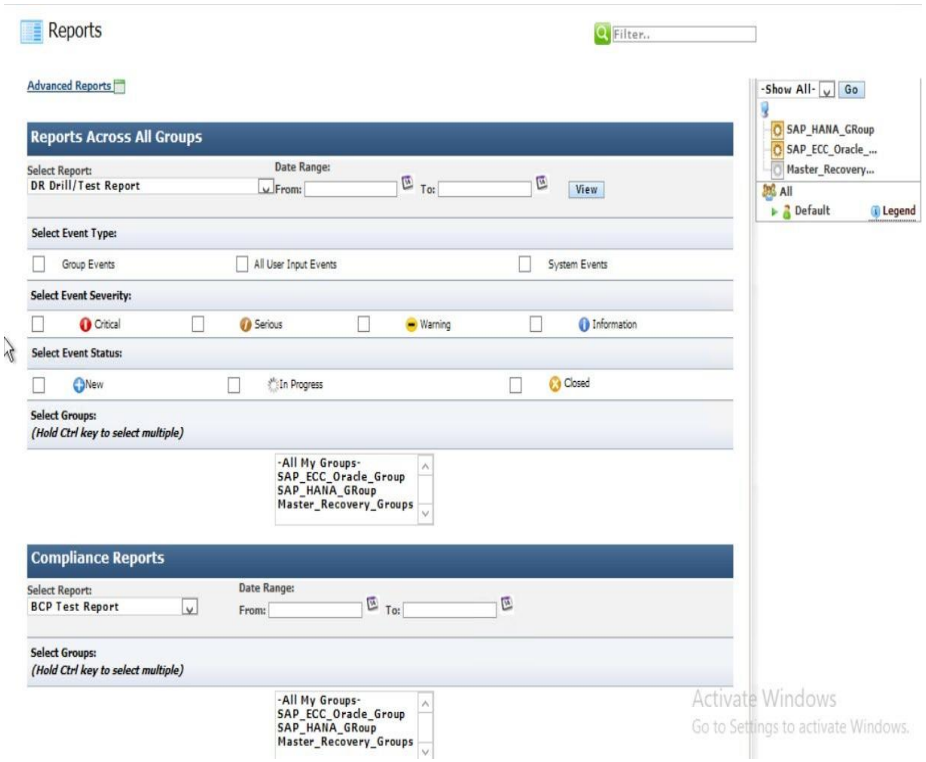


Figura 4.14

Y a continuación, del menú desplegable “Select Report”, seleccione “DryRun Execution” y entre el rango de fechas de ejecución en los campos “from” y “to” del grupo “Date Range”.

Por último, hacemos clic en el botón View DryRun Reports como se muestra a continuación.

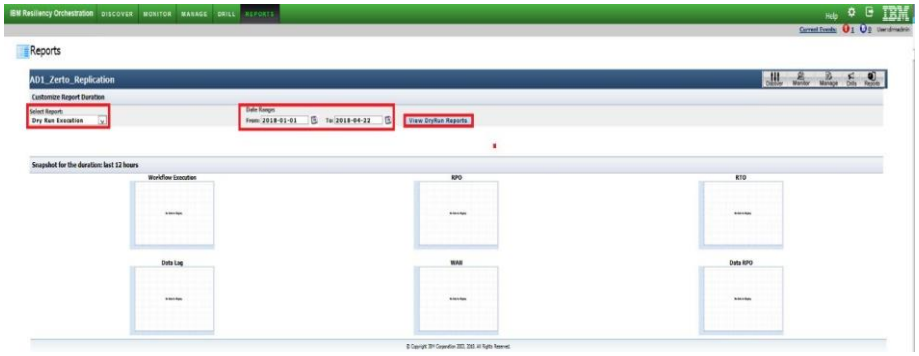


Figura 4.15

De esta manera se obtiene los reportes de DryRun en las fechas seleccionadas para este Recovery Group. Abrimos el reporte deseado y lo analizamos. Comparamos con un reporte previo de una prueba exitosa.

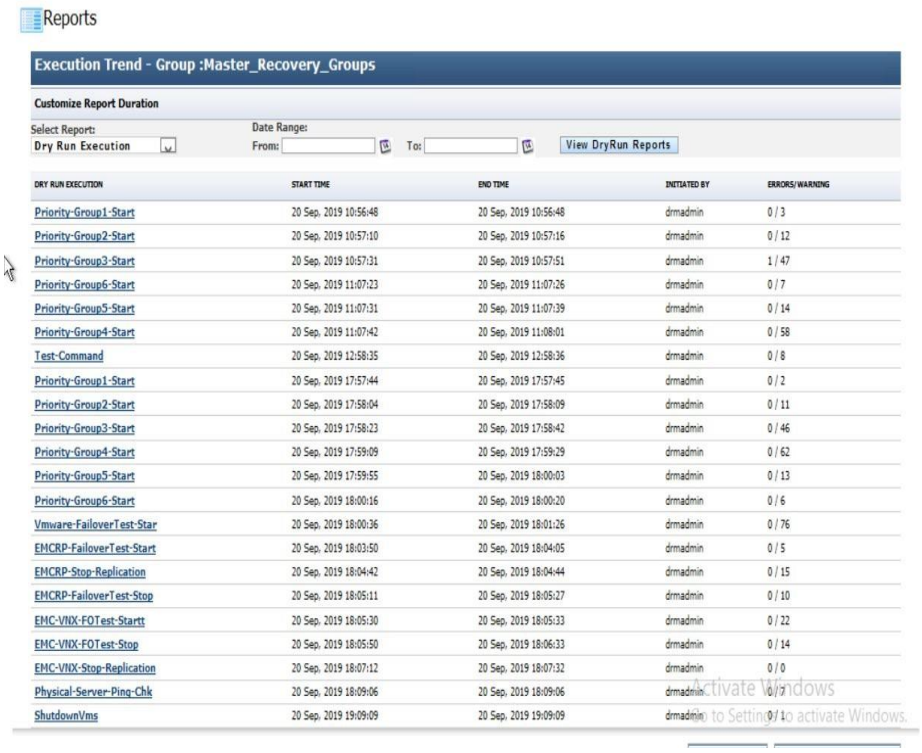


Figura 4.16

El reporte DryRun genera un reporte de estado que muestra el resultado de cada paso en la ejecución del workflow. Para ver los detalles de una tarea en particular, haga clic en la vista detallada View Details

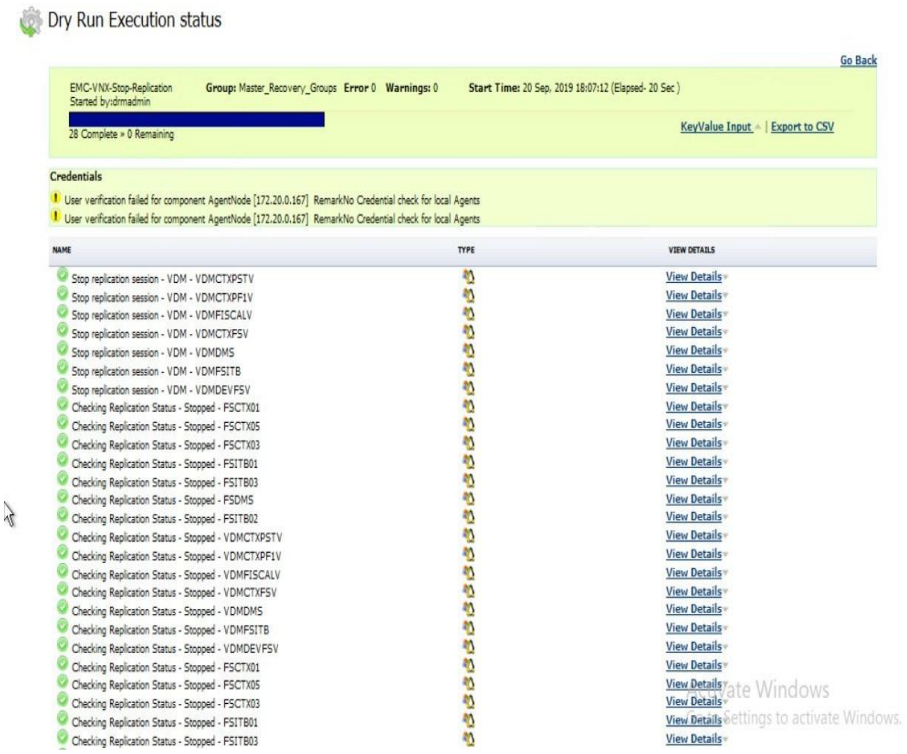


Figura 4.17

4.9.3. Ejecución de workflow

Un workflow, o flujo de trabajo en español, es un conjunto de actividades relacionadas, que son completadas en un determinado orden para alcanzar un objetivo de la organización. Estas actividades, o tareas, son realizadas por los llamados «participantes» del proceso, que pueden ser humanos o no (en ese caso, pueden ser software, máquinas, etc.).

Para ejecutar un workflow se hace clic en el workflow denominado StopAppPR (de la aplicación deseada), luego en el botón de Execute para realizar la operación de Disaster Recovery y repita la secuencia para los restantes grupos y workflows de acuerdo con lo especificado en la tabla de switchover y switchback.

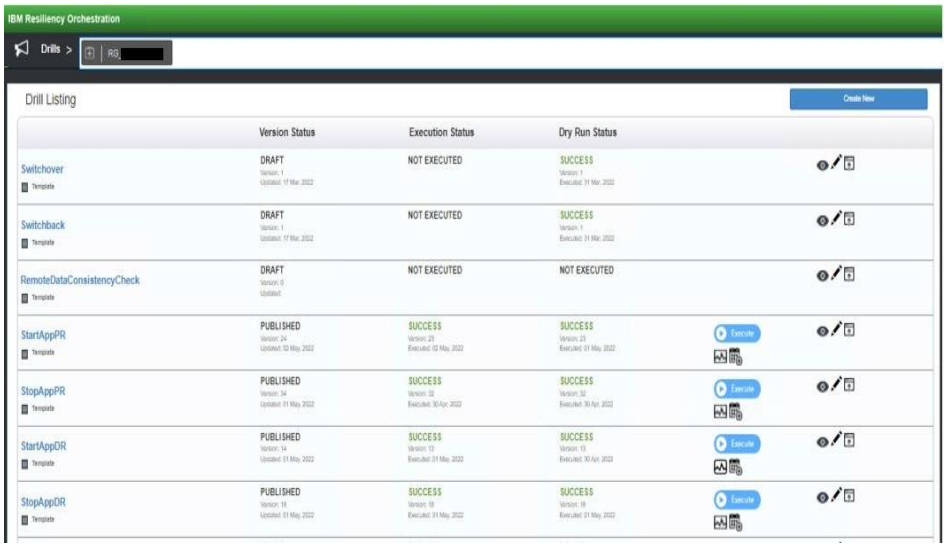


Figura 4.18

4.10. Resultados de ejecución

Para realizar la validación de los 4 aplicativos definidos en el alcance, se solicitó una ventana de trabajo a la gerencia, para que se definan las fechas y horario de menor impacto, y esta a su vez gestionó la aprobación de la superintendencia de bancos, para

que quede en su conocimiento que la caída de servicios es controlada y no por afectación directa.

Se definieron una ventana de 7 horas iniciando un viernes desde las 23:00 hasta las 06:00am del sábado siguiente. Esto teniendo en consideración los tiempos obtenidos de las pruebas anteriores, y que se encuentran detallados en el capítulo 3.

Una de las premisas de la ejecución, fue contar con todo el personal responsable de la ejecución manual del DRP, para que, en caso de falla de la herramienta, se pueda tomar el control inmediato, con intervención humana, considerando que se realizaría sobre ambiente productivo.

A continuación, se visualizan los resultados de los tiempos obtenidos para las pruebas de switchover y switcback de los 4 aplicativos definidos en el alcance.

Tabla 19. Resultados de Switchover y Switchback

Aplicación	Switchover Workflows	Time	Switchback Workflows	Time
APP1	StopAppPR Switchover DBs StartAppDR	00:28:37 00:08:34 00:04:33	StopAppDR Switchback DBs StartAppPR	00:45:38 00:10:01 00:05:13
APP2	StopAppPR Switchover DBs StartAppDR	00:03:43 00:05:27 00:04:11	StopAppDR Switchback DBs StartAppPR	00:01:40 00:05:21 00:18:36
APP3	StopAppPR	00:03:22	StopAppDR	00:08:29

	Switchover DBs StartAppDR	00:07:43 00:29:31	Switchback DBs StartAppPR	00:07:02 00:13:42
APP4	StopAppPR Switchover DBs StartAppDR	00:12:35 01:40:57 00:27:39	StopAppDR Switchback DBs StartAppPR	00:34:02 01:30:42 00:02:23

Con estos tiempos podemos definir que el tiempo total ejecutado por aplicación es la siguiente:

Tabla 20. Tiempo total de ejecución de DRP

Aplicación	Switchover	Switchback
APP1	00:41:44	00:59:52
APP2	00:13:21	00:45:37
APP3	00:40:36	00:29:13
APP4	01:19:11	02:07:07
TOTAL	**02:44:52**	**04:22:19**

4.11. Comparativa y análisis del resultado

A continuación, se detallan los tiempos obtenidos durante las pruebas realizadas con la herramienta CRO, vs los tiempos iniciales que manejaba la institución cuando las pruebas se realizaban de forma manual.

En la misma podemos visualizar que los tiempos de ejecución manuales son mayores a los otros, esto debido a que la ejecución pese a que se realiza de igual manera de forma secuencial, lo ejecuta un solo responsable (la herramienta), lo cual evita delays durante la secuencia, así también se evita la introducción de comandos de forma manual y la validación visual del resultado, ya

que dentro de la herramienta se ingresan parámetros que indican que ejecutar en caso exitoso o fallido.

Tabla 21. Comparación de tiempos de DRP manual vs CRO

Aplicación	Switchover manual TIEMPO REAL	Switchback manual TIEMPO REAL	Switchover CRO TIEMPO MAXIMO	Switchback CRO TIEMPO MAXIMO
APP1	01:15:00	01:32:00	00:41:44	00:59:52
APP2	00:24:00	00:58:00	00:13:21	00:45:37
APP3	00:48:00	00:33:00	00:40:36	00:29:13
APP4	01:30:00	02:23:00	01:19:11	02:07:07
TOTAL	03:27:00	05:26:00	02:44:52	04:22:19

Cabe mencionar que estos tiempos pueden ser optimizados, ya que la ejecución actual se realizó de forma secuencial, sin embargo, se validó con los ejecutores y responsables del DRP que la ejecución de las APP1 y APP4 se puede realizar en paralelo, así como las APP2 y APP3, lo cual reduciría en aproximadamente un 30% del tiempo obtenido durante la prueba actual. Según se muestra en la siguiente tabla, en la cual se han tomado los tiempos más altos de switchover y switchback como referencia.

Tabla 22. Tiempos de optimización CRO

Aplicación	Switchover CRO	Switchback CRO	Switchover CRO	Switchback CRO
APP1	00:41:44	00:59:52	01:19:11	02:07:07
APP4	01:19:11	02:07:07		
APP2	00:13:21	00:45:37	00:40:36	00:45:37
APP3	00:40:36	00:29:13		
TOTAL	02:44:52	04:22:19	01:59:47	03:02:44

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Dada la importancia y la criticidad de los servicios que maneja la institución financiera es de vital importancia contar con un plan de DRP que satisfaga las necesidades de esta, y que se lleve a cabo en el menor tiempo posible, para de esta manera activar los servicios que son fundamentales para el negocio y para los clientes que esta posee.
2. Obviamente para lograr tener éxito en la realización de esta tarea, se debe tener en cuenta todos los factores que esta conlleva, tales como: el apoyo de la alta gerencia, el presupuesto, y la planificación adecuada que contemple todas las etapas de este; como el diseño, la implementación, las pruebas y la mejora continua del plan.
3. Para el desarrollo de este proyecto solo se contempló la prueba de 4 aplicativos, enfocándonos en la comprobación de ejecución y mejora de los tiempos de RTO sobre las distintas plataformas que la institución posee, para cumplir con cada uno de los objetivos planteados de manera inicial.

4. Se realizó el análisis del proceso de DRP actual, en donde se recopilo la información de la situación actual, y se levantó el modelo AS IS, lo cual nos permitió identificar los riesgos y desperdicios este.
5. Se modeló el proceso DRP descriptivo, mediante BPMN optimizando todos aquellos pasos que se identificaron como automatizables, para lo cual se definió la implementación de una herramienta de orquestación que permitiría la ejecución de estos.
6. Se validó la funcionalidad de la herramienta (CRO) dentro del proceso optimizado, automatizando los pasos de las diferentes áreas tecnológicas involucradas dentro del paso a paso de las 4 aplicaciones que se encontraban definidas dentro del alcance.
7. Se evaluó el diseño optimizado, luego de la ejecución de las pruebas, para medir la satisfacción del cliente interno, comprobando los resultados de los tiempos de ejecución y comparándolos con los tiempos iniciales.

RECOMENDACIONES

1. Los planes de DRP deben ser actualizados cada vez que se realice un cambio en las plataformas, para mantener una versión real y evitar afectación en las pruebas durante la ejecución.
2. Realizar una revisión a detalle del uso de las herramientas actuales en cada una de sus plataformas, ya que se identifican mejoras en el proceso de replicación, para reducción de tiempos de RTO.
3. Los planes de DRP deben ser escritos de manera entendible y simple, para que cualquier persona pueda ejecutarlas y configurarlas en la herramienta.
4. El plan de DRP debe ser de conocimiento de todas las áreas tecnológicas, con el objetivo de conocer los cambios realizados y en qué momento deben intervenir como parte del proceso.
5. Capacitar a los especialistas de manera formal en el uso de la herramienta para que estos puedan realizar la implementación de workflows de forma directa.
6. Realizar pruebas previas con cada uno de los aplicativos, para garantizar la funcionalidad exitosa del plan de DRP escrito.
7. Una vez validados las aplicativos, se podrá configurar estos, en la herramienta de orquestación y así automatizar la ejecución de DRP, esta tarea se ejecutará de forma repetitiva hasta que se finalicen los 84 aplicativos de la institución.
8. Realizar una prueba globalizada de DRP, es decir en donde los 84 aplicativos se encuentren automatizados en la herramienta, para calcular los nuevos tiempos de RTO.

BIBLIOGRAFÍA

[1] J. F. Gustin, *Disaster and Recovery Planning: A Guide for Facility Managers, Sixth Edition*, 6.ª ed. New York: River Publishers, 2020. doi: 10.1201/9781003151777.

[2] Y. P. Baginda, A. Affandi, y I. Pratomo, «Analysis of RTO and RPO of a Service Stored on Amazon Web Service (AWS) and Google Cloud Engine (GCE)», en *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, jul. 2018, pp. 418-422. doi: 10.1109/ICITEED.2018.8534758.

[3] F. Dickson, P. Goodwin, y M. Marden, «The Business Value of IBM's DRaaS and Resilience Orchestration Services», p. 2.

[4] S. Bae y Y. Shin, «An Automated System Recovery Using BlockChain», en *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, jul. 2018, pp. 897-901. doi: 10.1109/ICUFN.2018.8437040.

[5] T. F. Kappukalar Nasurudeen, V. K. Shukla, y S. Gupta, «Automation of Disaster Recovery and Security in Cloud Computing», en *2021 International Conference on Communication information and Computing Technology (ICCICT)*, jun. 2021, pp. 1-6. doi: 10.1109/ICCICT50803.2021.9510110.

[6] M. Dey, «Business Continuity Planning (BCP) methodology — Essential for every business», en *2011 IEEE GCC Conference and Exhibition (GCC)*, feb. 2011, pp. 229-232. doi: 10.1109/IEEEGCC.2011.5752503.

[7] (ISC) Corporate, *Official (ISC)2 Guide to the ISSAP CBK*. CRC Press, 2010.

[8] P. Fallara, «Disaster recovery planning», *IEEE Potentials*, vol. 23, n.º 5, pp. 42-44, dic. 2004, doi: 10.1109/MP.2004.1301248.

[9] D. B. Hitpass, *BPM: Business Process Management: Fundamentos y Conceptos de Implementación 4a Edición actualizada y ampliada*. Dr. Bernhard Hitpass, 2017.

[10] P. Ray, «IT Recovery for Business to Take Off», vol. 2, n.º 1, p. 6.

ANEXOS

Anexo A

Encuesta a Gerente de TI

De acuerdo con la ejecución del DRP en los 4 aplicativos mediante el uso de la herramienta CRO como se siente respecto a..	Muy insatisfecho	Insatisfecho	Ni insatisfecho / Ni satisfecho	Satisfecho	Muy satisfecho
1.- Facilidad de ejecución del DRP					X
2.- Tiempo de RTO que toma en ejecutarse el DRP				X	
3.- Entendimiento del proceso de ejecución				X	
4.- Facilidad en la generación de reporte					X
5.- Cumplimiento de los objetivos planteados				X	

Anexo B

Encuesta a líder de TI

De acuerdo con la ejecución del DRP en los 4 aplicativos mediante el uso de la herramienta CRO como se siente respecto a..	Muy insatisfecho	Insatisfecho	Ni insatisfecho / Ni satisfecho	Satisfecho	Muy satisfecho
1.- Facilidad de ejecución del DRP				X	
2.- Tiempo de RTO que toma en ejecutarse el DRP				X	
3.- Entendimiento del proceso de ejecución				X	
4.- Facilidad en la generación de reporte					X
5.- Cumplimiento de los objetivos planteados				X	

Anexo C

Encuesta a líder de área de Plataformas

De acuerdo con la ejecución del DRP en los 4 aplicativos mediante el uso de la herramienta CRO como se siente respecto a..	**Muy insatisfecho**	**Insatisfecho**	**Ni insatisfecho / Ni satisfecho**	**Satisfecho**	**Muy satisfecho**
1.- Facilidad de ejecución del DRP					X
2.- Tiempo de RTO que toma en ejecutarse el DRP				X	
3.- Entendimiento del proceso de ejecución					X
4.- Facilidad en la generación de reporte					X
5.- Cumplimiento de los objetivos planteados				X	

Anexo D

Encuesta a líder del área de Base de Datos

De acuerdo con la ejecución del DRP en los 4 aplicativos mediante el uso de la herramienta CRO como se siente respecto a..	**Muy insatisfecho**	**Insatisfecho**	**Ni insatisfecho / Ni satisfecho**	**Satisfecho**	**Muy satisfecho**
1.- Facilidad de ejecución del DRP					X
2.- Tiempo de RTO que toma en ejecutarse el DRP					X
3.- Entendimiento del proceso de ejecución				X	
4.- Facilidad en la generación de reporte				X	
5.- Cumplimiento de los objetivos planteados				X	

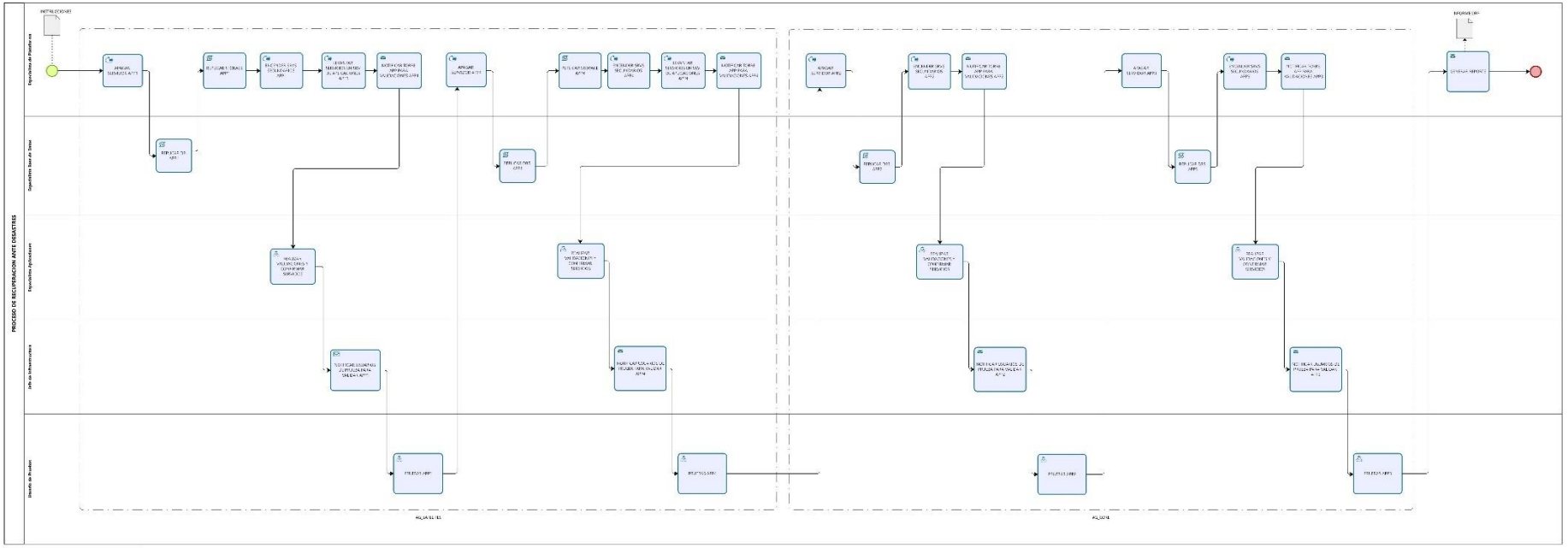
Anexo E

Encuesta a líder del área de Aplicaciones

De acuerdo con la ejecución del DRP en los 4 aplicativos mediante el uso de la herramienta CRO como se siente respecto a..	**Muy insatisfecho**	**Insatisfecho**	**Ni insatisfecho / Ni satisfecho**	**Satisfecho**	**Muy satisfecho**
1.- Facilidad de ejecución del DRP				X	
2.- Tiempo de RTO que toma en ejecutarse el DRP				X	
3.- Entendimiento del proceso de ejecución			X		
4.- Facilidad en la generación de reporte					X
5.- Cumplimiento de los objetivos planteados				X	

Anexo F

Modelo AS IS del DRP

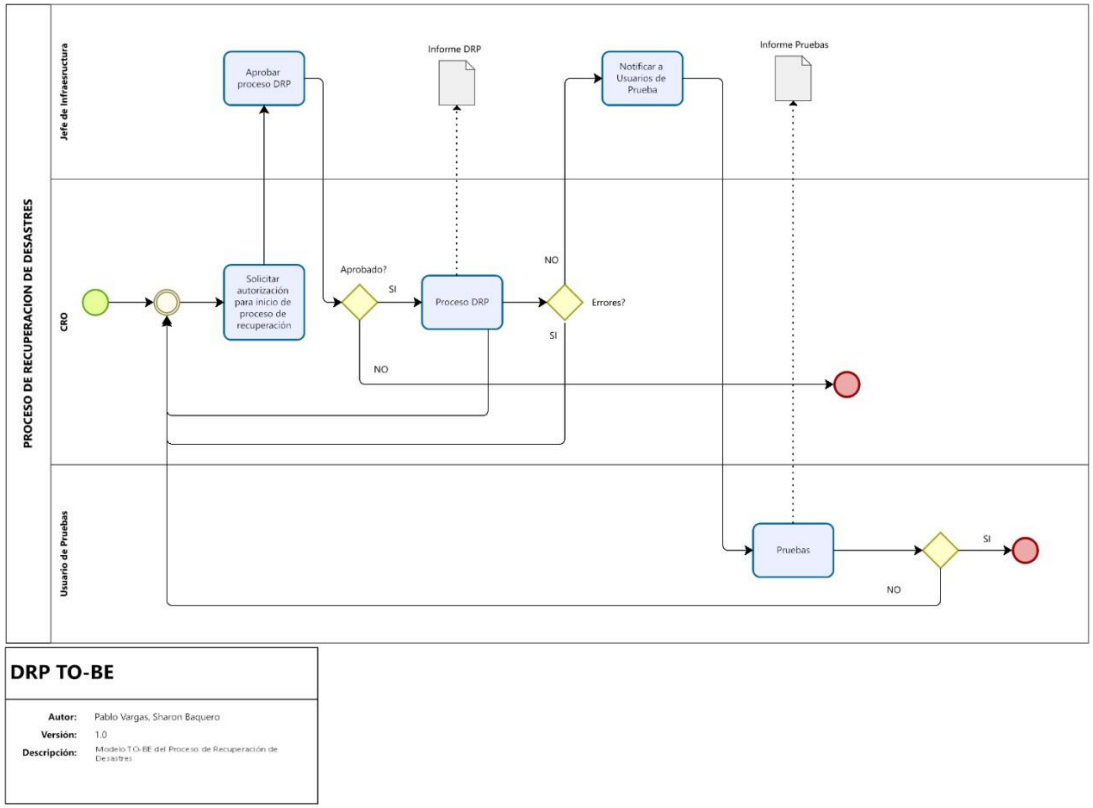


DRP AS-IS

Autor:
Versión:
Descripción:

Anexo G

Modelo TO BE del DRP



DRP TO-BE

Autor: Pablo Vargas, Sharon Baquero
Versión: 1.0
Descripción: Modelo TO-BE del Proceso de Recuperación de Desastres