



Universidad Abierta Interamericana

Diseño e Implementación de un Plan de Recuperación ante Desastres para Entidades Financieras

Profesora de Trabajo Final: Marcela Samela

Alumno: Jonathan Emil Vega Cosentino

**Trabajo Final de Carrera presentado para obtener el título de
Lic. en Gestión de Tecnología Informática**

Julio 2025

Resumen

Con el objetivo de garantizar la integridad y continuidad operativa de las entidades financieras ante posibles desastres, se plantea el diseño e implementación de un Plan de Recuperación ante Desastres (DRP) basado en una plataforma de virtualización con VMware vSphere, esta propuesta busca responder a la creciente necesidad de proteger tanto la estabilidad operativa como los datos sensibles frente a amenazas tecnológicas, naturales o provocadas por el ser humano. La presente propuesta de intervención en el campo profesional contempla la instalación y configuración de Site Recovery Manager (SRM), un software especializado en la automatización y orquestación de los procesos críticos de recuperación ante desastres. Además, se llevarán a cabo pruebas exhaustivas para validar la funcionalidad de los sistemas y se generará la documentación técnica necesaria para cumplir con las mejores prácticas y normativas del sector. Esta intervención en el ámbito profesional promueve un enfoque proactivo que integra tecnología de vanguardia con un marco normativo riguroso. La implementación de este DRP fortalecerá la capacidad operativa de las instituciones, permitiéndoles garantizar la continuidad de sus actividades ante eventos adversos. Asimismo, se logrará una notable reducción en los tiempos de inactividad y en las pérdidas económicas asociadas a interrupciones no planificadas, optimizando la respuesta ante situaciones de emergencia. Al alinearse con las normativas establecidas por el Banco Central, esta iniciativa no solo protegerá a las entidades financieras, sino que también reforzará la confianza en el sistema financiero, contribuyendo al desarrollo de un entorno más sólido, confiable y seguro.

Palabras Clave contingencia, datos, desastre, plan, recuperación, réplica

Abstract

With the aim of ensuring the integrity and operational continuity of financial institutions in the face of potential disasters, the design and implementation of a Disaster Recovery Plan (DRP) based on a virtualization platform with VMware vSphere is proposed. This initiative seeks to address the growing need to protect both operational stability and sensitive data against technological, natural, or human-induced threats. The project includes the installation and configuration of Site Recovery Manager (SRM), specialized software for automating and orchestrating critical disaster recovery processes. Additionally, comprehensive testing will be conducted to validate system functionality, and the necessary technical documentation will be produced to comply with industry best practices and regulations. This professional intervention promotes a proactive approach that integrates cutting-edge technology with a rigorous regulatory framework. The implementation of this DRP will enhance the operational resilience of institutions, enabling them to ensure the continuity of their activities in adverse scenarios. Furthermore, it will significantly reduce downtime and economic losses associated with unplanned disruptions, optimizing the response to emergency situations. By aligning with the regulations established by the Central Bank, this initiative will not only protect financial institutions but also strengthen confidence in the financial system, contributing to the development of a more robust, reliable, and secure environment.

Keywords contingency, data, disaster, plan, recovery, replication

Dedicatoria

A mi amada familia, cuyo amor y apoyo incondicional han sido mi gran sostén en este camino. A mis queridos profesores, cuya sabiduría y orientación han guiado mi trayecto académico durante todos estos años de estudio. Su aliento y respaldo han sido fundamentales para la concreción de este proyecto. Gracias por ser mi fuente de inspiración y por creer en mí en cada paso del camino. Este trabajo está dedicado a todos los colegas que se desempeñan dentro del mundo de TI con profundo agradecimiento y admiración.

Índice General

Capítulos

1	Introducción	9
1.1	Descripción.....	9
1.2	Justificación	10
1.3	Marco Institucional.....	11
1.4	Objetivo General	12
1.5	Objetivos Específicos.....	12
2	Estado del Arte	13
2.1	Antecedentes	13
3	Marco Teórico	21
3.1	El Plan de Recuperación ante Desastres (DRP)	21
3.1	Tiempo Objetivo de Recuperación (RTO)	21
3.2	Punto de Recuperación Objetivo (RPO)	23
3.3	Plan de Continuidad del Negocio (BCP)	25
3.4	Análisis de Impacto en el Negocio (BIA).....	27
3.5	Normativas BCRA.....	29
3.6	Virtualización en el contexto de un DRP	30
3.7	Herramientas para la recuperación ante Desastres	31
4	Acciones a Realizar	33
4.1	Análisis	33
4.1.1	Análisis de la infraestructura de virtualización	33
4.1.2	Elección de VMware Site Recovery Manager (SRM) como herramienta de Orquestación.....	36
4.1.3	Elección de la tecnología de replicación basada en almacenamiento (Storage Based-Array).....	37
4.2	Diseño	44
4.2.1	Diseño de la Arquitectura de Recuperación.....	44
4.2.2	Topologías.....	45
4.3	Implementación	49
4.3.1	Pre-Requisitos para la instalación.....	49
4.3.2	Instalación de Site Recovery Manager Virtual Appliance.....	51

4.3.3	Configuración de pares de Sitios y Protección	59
4.3.4	Configuración de Replicación Basada en Matrices (Based Array)	61
4.3.5	Mapeo de Recursos	63
4.3.6	Configuración Datastore Placeholder	67
4.3.7	Creación de Grupos de Protección	69
4.3.8	Creación de Planes de Recuperación	70
4.3.9	Prueba del Plan de Recuperación.....	71
4.3.10	Ejecución del Plan de Recuperación	72
4.3.11	Re-protección de Sitios	74
4.3.12	Ejecución de Failback.....	76
5	Cronograma.....	79
6	Recursos Necesarios.....	84
6.1	Recursos Humanos.....	84
6.2	Matriz RACI.....	85
6.3	Recursos Tecnológicos	86
7	Factores Externos Condicionantes	88
8	Evaluación del Proyecto	90
8.1	Factibilidad Financiera.....	90
9	Conclusiones	93
10	Referencias.....	96
11	Anexos	100

Índice de Figuras

Figura 1. RTO	22
Figura 2. Variables del RPO	23
Figura 3. Planificación, implementación, continuidad del negocio y recuperación ante desastres	25
Figura 4. Cómo interactúan las personas, los procesos y la tecnología.....	26
Figura 5. Flujo de elaboración de un BIA	28
Figura 6. RVTools	33
Figura 7. Pestañas de RVTools	34
Figura 8. Replicación Asíncrona.....	38
Figura 9. Replicación Síncrona.....	39
Figura 10. Búsqueda en la matriz.....	40
Figura 11. Aplicación de Filtros.....	41
Figura 12. Agentes SRA Disponibles.....	42
Figura 13. Matriz de Compatibilidad	43
Figura 14. Arquitectura de Sitios	44
Figura 15. Topología Activo-Pasivo	45
Figura 16. Topología Activo-Activo	46
Figura 17. Topología Bidireccional	47
Figura 18. Stretched Storage.....	48
Figura 19. Acceso Portal Broadcom.....	51
Figura 20. Versiones de SRM.....	52
Figura 21. Descarga SRM Appliance	52
Figura 22. Acceso vCenter.....	53
Figura 23. Deploy OVF Template	54
Figura 24. Virtual Appliance	55
Figura 25. Log-in SRM Appliance.....	56
Figura 26. Configuración PSC	57
Figura 27. Instancia vCenter Server	58
Figura 28. Nombre y Extensión	58
Figura 29. Conexión SRM/vCenter	59

Figura 30. Par de Sitios.....	60
Figura 31. Adaptador de replicación de almacenamiento.....	61
Figura 32. SRA	62
Figura 33. Array Manager	63
Figura 34. Mapeo de Redes	64
Figura 35. Mapeo de Carpetas.....	65
Figura 36. Mapeo de Recursos.....	66
Figura 37. Selección Datastore Placeholder	68
Figura 38. Grupo de Protección.....	69
Figura 39. Plan de Recuperación.....	70
Figura 40. Test del Plan de Recuperación	72
Figura 41. Proceso de Failback.....	77
Figura 42. Diagrama de Gantt	82

Índice de Tablas

Tabla 1. Recursos de Máquinas Virtuales y Requerimientos para el Sitio de Contingencia.....	35
Tabla 2. Comparativa Site Recovery Manager vs Zerto	37
Tabla 3. Fase Opcional	79
Tabla 4. Cronograma de Implementación: Fase 1 y Fase 2	80
Tabla 5. Cronograma de Implementación: Fase 3 y Fase 4	80
Tabla 6. Cronograma de Implementación: Fase Final	82
Tabla 7. Matriz RACI.....	85
Tabla 8. Recursos Tecnológicos	87
Tabla 9. Costos de Implementación.....	90
Tabla 10. Costos Opcionales de Implementación.....	91

1 Introducción

1.1 Descripción

La presente propuesta de intervención en el campo profesional tendrá por desafío el diseño e implementación de una solución que cumpla con las normas exigidas por el BCRA y se adapte una plataforma de infraestructura de virtualización basada en VMware Vsphere.

En la actualidad, las entidades financieras enfrentan constantes desafíos relacionados con la seguridad y la continuidad operativa, especialmente ante la amenaza de desastres naturales o ataques cibernéticos. El problema radica en la necesidad de garantizar la protección de los datos sensibles y la infraestructura tecnológica, así como la recuperación eficiente de los servicios financieros en caso de un evento catastrófico. Este problema es de suma importancia, dado el papel crucial que desempeñan las entidades financieras en la economía y la sociedad en general. Las consecuencias de la falta de un plan de recuperación ante desastres pueden ser devastadoras, afectando la estabilidad financiera, la confianza del cliente y la reputación de la institución.

El diseño de un Plan de Recuperación ante Desastres de TI (IT DRP) como menciona el autor Derick Musundi Kesa (2023) implica la creación de estrategias, políticas y procedimientos que permitan restaurar los sistemas, la infraestructura y los servicios tecnológicos tras un incidente disruptivo. Este enfoque busca asegurar la continuidad de las operaciones críticas de TI, reducir el tiempo de inactividad y preservar la integridad de los datos. El principal objetivo de un IT DRP es restablecer las capacidades tecnológicas y reanudar las operaciones normales de la organización de manera eficiente y en el menor tiempo posible. Por otro lado, la continuidad operativa de TI se enfoca en garantizar que las operaciones esenciales y los servicios críticos puedan mantenerse incluso durante y después de un incidente disruptivo. Para ello, es necesario contar con estrategias, planes y medidas que aseguren la disponibilidad, funcionalidad y resiliencia de los activos tecnológicos, apoyando así los objetivos generales de continuidad del negocio (Kesa, 2023).

El desarrollo de este proyecto permitirá abordar ambos conceptos de manera integrada, considerando los requisitos normativos y los desafíos específicos del sector financiero, a través de una herramienta de software que permita orquestar y garantizar el funcionamiento de un DRP.

1.2 Justificación

Implementar un plan de recuperación es fundamental para desarrollar estrategias efectivas de mitigación de riesgos y garantizar la continuidad del negocio en situaciones adversas. Si bien existen múltiples soluciones implementadas en diferentes nichos tecnológicos, cada contexto y en especial las instituciones financieras requieren un enfoque específico y adaptado a sus necesidades particulares, haciendo hincapié en el cumplimiento de normas y estándares que las rigen.

En este sentido, herramientas como VMware Site Recovery Manager (SRM) destacan al facilitar la automatización de procesos esenciales para la recuperación de entornos virtualizados, tales como la migración, recuperación, pruebas, reprotcción y reversión de las cargas de trabajo en máquinas virtuales. SRM coordina las operaciones entre servidores vCenter en los sitios de producción y recuperación, asegurando que las máquinas virtuales del sitio protegido se apaguen adecuadamente mientras sus réplicas en el sitio de recuperación asumen sus funciones utilizando los datos replicados. Estas operaciones están organizadas mediante planes de recuperación que definen el orden de apagado y encendido de las máquinas virtuales, los recursos asignados y las redes accesibles. Además, SRM permite probar los planes de recuperación en entornos aislados, utilizando copias temporales de los datos replicados, sin interrumpir las operaciones en curso (Cato G., 2020).

Al brindar soporte para múltiples planes de recuperación, esta solución ofrece control detallado sobre las aplicaciones y servicios que se migran, así como sobre los horarios de pruebas. De este modo, SRM amplía las capacidades de las plataformas virtuales, posibilitando una recuperación rápida y eficiente incluso ante fallos parciales o totales en los sitios productivos. (Cato G., 2020).

El presente proyecto busca abordar estas preocupaciones mediante el análisis, diseño e implementación de un plan de recuperación ante desastres para entidades financieras, con el

objetivo de minimizar los impactos negativos y garantizar la operatividad en momentos críticos.

1.3 Marco Institucional

La estrategia de implementación desarrollada aplica para todas aquellas entidades financieras reguladas por el Banco Central de la República Argentina (BCRA) bajo la normativa A 7724 – Sección 6: Gestión de la Continuidad del Negocio que establece los siguientes puntos:

- Marco de gestión de la continuidad
- Ciber resiliencia en la continuidad del negocio
- Análisis de impacto y evaluación de riesgos.
- Estrategias de continuidad del negocio.
- Programa de capacitación y concientización.
- Ejercicios y pruebas de los planes de continuidad del negocio.
- Mantenimiento de los planes de la continuidad del negocio.
- Control y reportes de gestión.

El Banco Central de la República Argentina (BCRA) es la institución que actúa como el banco central de Argentina y dentro de sus responsabilidades es quién regula y supervisa las entidades financieras en Argentina, esto incluye bancos, instituciones de crédito y otras entidades de carácter financiero. Su objetivo principal es garantizar la solidez y estabilidad del sistema financiero, proteger a los depositantes (clientes) y fomentar la eficiencia del sector.

A nivel técnico se considerará una arquitectura de infraestructura tecnológica on-premise (no Cloud), un Centro de Datos Primario (denominado sitio protegido) y un centro de datos secundario (denominado sitio de contingencia), la selección de las herramientas y tecnologías adecuadas para la implementación del DRP, considerando una herramienta de orquestación antes desastres que pueda integrarse con la plataforma de virtualización VMware Vsphere.

1.4 Objetivo General

El objetivo general de esta propuesta de intervención en el campo profesional es diseñar e implementar un Plan de Recuperación ante Desastres específicamente dirigido a entidades financieras bajo control del BCRA y utilizan como plataforma de virtualización VMware Vsphere, con el propósito de garantizar la continuidad operativa, la protección de los datos sensibles en situaciones de emergencia y cumplir con las normas y estándares que las rigen.

1.5 Objetivos Específicos

Como objetivos particulares del proyecto se mencionan los siguientes:

Implementar Site Recovery Manager (SRM) como herramienta fundamental para la automatización y gestión del Plan de Recuperación ante Desastres (DRP), de acuerdo con las normativas exigidas por el BCRA, asegurando que se adapte adecuadamente al entorno de virtualización con VMware.

Desarrollar el Plan de Recuperación ante Desastres (DRP), basándose en el análisis de impacto en el negocio (BIA), y asegurando que el plan considere todos los aspectos críticos para la continuidad operativa del negocio.

Realizar pruebas de simulación y evaluación del Plan de Recuperación ante Desastres (DRP) implementado con Site Recovery Manager (SRM), para validar su efectividad y garantizar que el plan responda de manera adecuada en situaciones reales de emergencia.

2 Estado del Arte

2.1 Antecedentes

El presente estado del arte se centra en el análisis de varios estudios que han abordado la importancia de la elaboración de planes de recuperación en la mitigación de riesgos operacionales. Este apartado ofrece una revisión cronológica destacando los avances recientes y las mejores prácticas en la implementación de un plan de recuperación ante desastres. Se presentan casos de estudio relevantes, se identifican las principales tendencias y desafíos actuales, proporcionando un marco para comprender cómo las entidades financieras pueden mejorar su preparación y respuesta ante desastres, nutriéndose de otros casos existentes en otras industrias.

Danny Puente Carrera (2014) presentó un trabajo de investigación centrado en el diseño de un Plan de Recuperación de Desastres (DRP) para Medicamenta Ecuatoriana S.A., una empresa del sector farmacéutico. Su trabajo se centró en la protección de los activos más valiosos de la empresa: la información crítica y los sistemas que soportan las operaciones clave, como el correo electrónico, el sistema ERP (Enterprise Resource Planning) y el CRM (Customer Relationship Management). La metodología aplicada incluyó un análisis exhaustivo de riesgos que evaluaba el impacto potencial de interrupciones operativas, tanto internas como externas. El DRP propuesto tiene como objetivo reducir el impacto, el riesgo y el tiempo de inactividad de estos sistemas críticos, asegurando que la organización pueda continuar operando con acceso ininterrumpido a estos recursos, incluso en situaciones de desastre. Los resultados obtenidos mostraron que Medicamenta no estaba preparada para afrontar desastres que afectaran a sus sistemas críticos, lo que podría ocasionar pérdidas significativas e incluso poner en riesgo el futuro de la empresa. En consecuencia, el autor recomendó la implementación inmediata del plan, priorizando los sistemas críticos y utilizando soluciones de virtualización para garantizar la integridad y disponibilidad de los datos (Puente Carrera, 2014).

Según Puente Carrera (2014), la virtualización optimiza el despliegue de aplicaciones y evita la multiplicación innecesaria de servidores mediante su consolidación, lo que, a su vez, elimina la necesidad de expansión física del centro de datos. Entre las ventajas destacadas de la virtualización se incluyen la disminución de costos, la reducción de puntos de falla, una

administración centralizada y simplificada, un crecimiento escalable y flexible, así como la minimización de tiempos de inactividad y una mejora en el rendimiento debido a una gestión de recursos más eficiente. En el mercado, se encuentran varios productos de virtualización, de los cuales VMware resulta de especial interés. En particular, vSphere de VMware se emplea en la estrategia de DRP debido a que el personal de TI de Medicamenta Ecuatoriana S.A. posee las habilidades necesarias para manejar esta herramienta, a diferencia de lo que ocurre con Hyper-V de Microsoft (Puente Carrera, 2014).

Por otro lado, para la recuperación ante desastres, VMware ofrece una herramienta especializada llamada VCenter Site Recovery Manager (SRM). Esta herramienta permite la ejecución automatizada de planes de recuperación centralizados para las máquinas virtuales en el entorno virtual, constituyendo así una solución ideal para la recuperación de desastres. Con el uso de SRM, es posible alcanzar tiempos de recuperación (RTO) y objetivos de puntos de recuperación (RPO) significativamente bajos para los sistemas críticos, al replicarse en tiempo real y restaurarse en el sitio de recuperación de acuerdo con el plan predefinido en la herramienta (Puente Carrera, 2014).

Continuando con el estudio de antecedentes previos, en 2018, Byron Vicente Nieto Muñoz llevó a cabo un análisis para el diseño de un Plan de Recuperación ante Desastres (DRP) aplicado a un centro de datos de empresas municipales, basado en el estándar ISO/IEC 24762:2008. Este estándar ofrece directrices para la preparación y respuesta ante desastres en centros de datos, y fue elegido por su enfoque en la recuperación de TI en situaciones críticas. El estudio destacó la necesidad de diseñar un sitio alternativo con alta disponibilidad y escalabilidad, capaz de satisfacer las demandas de continuidad del negocio. Nieto Muñoz subrayó la importancia de involucrar a la alta dirección en el desarrollo del proyecto, ya que su apoyo es crucial para su éxito. Entre los puntos clave del estudio, se establecieron procedimientos específicos para la recuperación de los servicios más importantes en el menor tiempo posible, garantizando la mínima interrupción de las operaciones municipales. El trabajo también proporcionó un marco para la evaluación y mitigación de riesgos, incluyendo la identificación de los sistemas de misión crítica y la definición de roles y responsabilidades para la ejecución del plan en situaciones de emergencia (Nieto Muñoz, 2018).

Además, propuso a la empresa municipal la implementación de un sitio alternativo que posibilite la recuperación inmediata y eficiente de sus operaciones, asegurando así la

continuidad de procesos activos y la protección de datos. Para optimizar los costos relacionados con la infraestructura y permitir una rápida reanudación de actividades, recomendó la virtualización del sitio utilizando tecnologías como VMware ESXi y vCenter Site Recovery Manager. Adicionalmente, sugirió la contratación de un enlace dedicado exclusivamente para la transferencia de copias de seguridad, a fin de evitar cualquier impacto en el rendimiento y el ancho de banda administrativo de la red (Nieto Muñoz, 2018).

Nieto Muñoz (2018) consideró que la elaboración de políticas en un plan de recuperación de desastres debe buscar formalizar de manera precisa los objetivos y el alcance que este deberá cubrir. Esto incluye la asignación clara de las responsabilidades, funciones y roles específicos de cada equipo de trabajo—ya sea de redes, infraestructura, sistemas eléctricos, administración de datos y respaldo, o administración de bases de datos—, bajo la dirección de un líder encargado de la continuidad del negocio, con el respaldo y la participación en la toma de decisiones de la gerencia general. Asimismo, recomienda la creación de un documento claro y directo, en el cual se especifiquen de manera estratégica los objetivos y puntos críticos a ser implementados en el desarrollo del plan de recuperación. El equipo encargado de este proceso debe contar con habilidades de gestión de proyectos para coordinar y establecer plazos, presupuestos, cronogramas e indicadores de éxito, en función de asegurar el cumplimiento de las políticas detalladas en el documento de planificación (Nieto Muñoz, 2018).

Las responsabilidades asignadas al equipo de recuperación incluyen la coordinación de plazos en cada fase del proyecto, la administración de los objetivos, estrategias, políticas y actividades críticas, y la presentación del plan a la alta gerencia y a los departamentos involucrados. Además, el equipo debe definir y limitar el presupuesto inicial, mantener control sobre los aspectos críticos que puedan surgir y adherirse a las recomendaciones de especialistas para garantizar la efectividad y eficiencia del plan de recuperación (Nieto Muñoz, 2018).

En base al estudio científico publicado por los autores Fani y Subriadi (2019) describen al Plan de Continuidad del Negocio (BCP) como un marco que se emplea para diseñar y validar estrategias que permitan mantener las operaciones de una organización de manera continua. Este enfoque es relevante antes, durante y después de que se produzcan desastres o interrupciones. Su objetivo principal es garantizar que las funciones esenciales del negocio se sostengan durante y después de una interrupción, al tiempo que se gestionan las operaciones

en su conjunto. Es uno de los elementos fundamentales de una estrategia de recuperación, aunque muchas organizaciones no son plenamente conscientes de su importancia ni de cómo implementarlo correctamente (Fani & Subriadi, 2019).

Cada organización tiene necesidades únicas, lo que implica que no existe un BCP estándar o universal aplicable a todas. Hasta ahora, la investigación y la literatura sobre la implementación del BCP en empresas de distintos tamaños son limitadas. Aunque algunos estudios abordan los marcos teóricos del BCP y los elementos que deben incluirse, como el análisis de impacto en el negocio, el análisis de riesgos, la capacitación y las pruebas, la mayoría se limita a describir estos componentes de manera general (Fani & Subriadi, 2019).

La implementación de planes de recuperación ante desastres (DRP) en el sector bancario ha ganado gran relevancia en los últimos años debido a la creciente dependencia de las organizaciones en los sistemas de tecnología de la información (TI) y el impacto significativo que tienen los desastres en la continuidad de las operaciones. En su estudio, Lessa y Tariku (2020) proponen un marco para la planificación de la recuperación de desastres en el sector bancario de Etiopía, identificando la necesidad de un Plan de Recuperación ante Desastres de TI (DRP) que cubra recursos clave como aplicaciones, datos, conectividad de red y hardware. Según los autores, el DRP se distingue como un documento táctico que ofrece un plan a corto plazo para responder a interrupciones específicas de TI, como ciberataques o fallos del sistema. Este plan no solo se centra en mitigar el impacto del desastre, sino también en la recuperación de los sistemas afectados (Lessa & Tariku, 2020).

El proceso o pasos de un marco de trabajo de recuperación ante desastres de TI (IT DRP) deben ser evaluados mediante un método bien ejecutado que permita demostrar la calidad y eficiencia del marco propuesto. Para esta evaluación se utilizan como criterios variables la funcionalidad, completitud, fiabilidad, usabilidad y adecuación al entorno bancario. Dichos criterios de validación representan algunos de los atributos de calidad relevantes que se deben considerar antes de utilizar el marco con el propósito propuesto. En el estudio realizado por Lessa y Tariku (2020), se empleó el método de validación de expertos mediante un grupo focal, el cual permitió obtener validación por parte de profesionales de dos bancos. Estos expertos confirmaron que el marco de trabajo será de gran ayuda en el desarrollo del IT DRP, enfatizando la inclusión de todas las áreas necesarias y afirmando que ninguna de ellas debería excluirse (Tariku & Lessa, 2020).

Partiendo del concepto de definición de desastre, según Osaji (2023), un desastre puede afectar a una organización en cualquier momento, ya sea un desastre natural, como un huracán, o un desastre no natural, como un ciberataque. Cuando ocurre una catástrofe, las repercusiones pueden ser devastadoras para las operaciones, las finanzas y la reputación de la organización. Es por ello que las organizaciones deben contar con un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés). El DRP es un enfoque documentado y estructurado que establece las acciones necesarias para responder y recuperarse de un desastre. Un DRP debe estar diseñado para asegurar que la organización pueda continuar operando en caso de desastre. Al contar con un plan previamente establecido, se puede mitigar el impacto de la catástrofe en las operaciones, protegiendo los datos y sistemas, y manteniendo la confianza de los clientes y partes interesadas (Osaji, 2023).

Un plan de recuperación ante desastres bien estructurado es fundamental para asegurar la continuidad de las operaciones en situaciones de crisis. Este plan debe detallar los pasos a seguir en caso de desastre, incluyendo los procedimientos de respuesta de emergencia, los protocolos de comunicación, las estrategias de respaldo y recuperación de datos, así como las rutinas de prueba y mantenimiento. Asimismo, es crucial actualizar y revisar el plan periódicamente para garantizar su efectividad (Osaji, 2023).

En el año 2024, Lucille Onazi publicó un estudio sobre el análisis de impacto en el negocio (BIA) en la empresa de seguros Health Network, Inc., como parte de su proceso de planificación de emergencias. Onazi exploró la importancia de identificar las funciones empresariales esenciales y los recursos críticos, como parte de un plan más amplio para minimizar el tiempo de inactividad y garantizar la continuidad del negocio en situaciones de desastre. Su estudio hizo hincapié en la identificación de los objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO), que permiten a la organización establecer tiempos máximos aceptables de interrupción para cada una de sus funciones críticas. Además, el análisis incluyó la evaluación del impacto financiero y operativo de posibles interrupciones en los centros de datos, con el objetivo de priorizar recursos y estrategias de recuperación. Los resultados de este estudio son relevantes para cualquier organización que desee asegurar la continuidad de sus operaciones, especialmente aquellas que dependen de sistemas complejos de TI para su funcionamiento diario (Onazi, 2024).

En base a la definición de Onazi (2024), el Análisis de Impacto en el Negocio (BIA) permite a las empresas identificar y evaluar los riesgos que enfrenta la organización, centrándose en las funciones esenciales de las que depende y en las posibles consecuencias de su interrupción. El BIA es un proceso estructurado que permite identificar y analizar los efectos potenciales que pueden tener las interrupciones en las operaciones críticas de una organización. Su objetivo principal es estimar el impacto de diversas catástrofes, como desastres naturales, fallos tecnológicos o desastres provocados por el ser humano, sobre la economía, las operaciones y la reputación de la empresa (Onazi, 2024).

Mediante el uso de un BIA, las organizaciones pueden definir los Objetivos de Tiempo de Recuperación (RTO) y los Objetivos de Punto de Recuperación (RPO) para cada una de sus funciones críticas, priorizándolas según su relevancia. El proceso de BIA incluye los siguientes pasos clave: identificación de riesgos, que se enfoca en reconocer posibles amenazas y peligros que podrían afectar la operatividad de la empresa; identificación de funciones críticas, donde se priorizan las operaciones esenciales para la existencia de la organización; evaluación de impacto, con el fin de analizar los posibles efectos financieros, operativos y reputacionales de las interrupciones en las funciones esenciales; organización de RTO y RPO, para determinar el tiempo de inactividad y la pérdida de datos tolerables para cada función crítica; y, finalmente, la evaluación de recursos, en la que se identifican los recursos necesarios para reanudar las operaciones vitales dentro de los límites de RTO y RPO especificados (Onazi, 2024).

El Plan de Continuidad del Negocio (BCP) representa un enfoque integral y una serie de protocolos que las organizaciones emplean para asegurar que sus operaciones críticas puedan mantenerse tanto durante como después de una interrupción. Sus principales objetivos son reducir el impacto de las interrupciones, garantizar la continuidad de las operaciones vitales y fomentar una recuperación rápida y eficiente. La elaboración del BCP implica el desarrollo de planes detallados y aplicables, la asignación clara de roles y responsabilidades, y la disponibilidad de herramientas y recursos necesarios para asegurar la continuidad. Los elementos esenciales de un BCP incluyen: un plan de respuesta ante desastres, que establece las acciones inmediatas para proteger a las personas y los bienes durante una crisis; estrategias y protocolos específicos para asegurar la disponibilidad constante de servicios críticos en el plan de continuidad del negocio; planes de recuperación ante desastres, que se enfocan en restaurar los sistemas y datos de TI para minimizar el tiempo de inactividad y la pérdida de

datos; un esquema de comunicación en crisis, que detalla las estrategias de comunicación con los actores internos y externos durante la emergencia; y, por último, capacitación y pruebas regulares, que garantizan que los empleados estén preparados para manejar interrupciones mediante la actualización continua del BCP (Onazi, 2024).

El siguiente artículo desarrolla la implementación de una solución de orquestación por software mediante Site Recovery Manager sobre entornos de virtualización con VMware Vsphere elaborado por los autores Elgdamsi y Embarak (2024), destacan que muchas organizaciones de TI implementan servidores que operan a una fracción de su capacidad debido a la dedicación de estos servidores a aplicaciones específicas. Esto genera ineficiencias que conllevan a mayores costos operativos. Para optimizar la utilización de recursos y reducir costos, se introdujo la virtualización, que permite la creación de una capa de abstracción sobre el hardware físico, generando máquinas virtuales (VM). Esto facilita la ejecución de múltiples sistemas operativos y aplicaciones en un solo servidor físico, lo que maximiza el uso del hardware y, por consiguiente, incrementa el retorno sobre la inversión (ROI) de la empresa. (Elgdamsi & Embarak, 2024).

En cuanto a la recuperación ante desastres, los autores subrayan la importancia de planificar con anticipación para mitigar los efectos de eventos como desastres naturales o ciberataques. Un plan de recuperación ante desastres (DRP) permite a las organizaciones priorizar funciones críticas y restaurar el acceso a su infraestructura de TI mediante la replicación de datos en ubicaciones externas. En este contexto, VMware Site Recovery Manager (SRM) surge como una solución efectiva de recuperación ante desastres, compatible con herramientas como vSphere Replication y Array-Based Replication, y con otras soluciones de VMware. El SRM facilita la recuperación de máquinas virtuales de forma automatizada y no disruptiva, optimizando el tiempo de respuesta y garantizando la continuidad del negocio en situaciones de emergencia (Elgdamsi & Embarak, 2024).

Esta propuesta de intervención para la implementación de un plan de contingencia en entidades financieras reguladas por el Banco Central de la República Argentina, no solo se fundamenta en los marcos teóricos existentes, sino que también se enfoca en su aplicación práctica dentro de una infraestructura de virtualización con VMware vSphere, incluyendo la instalación y configuración de un software de orquestación ante desastres. De este modo, se busca proporcionar una guía técnica y operativa que permita fortalecer la preparación y

respuesta ante incidentes en un entorno crítico, cerrando la brecha entre la teoría y la práctica en la gestión de la continuidad del negocio.

3 Marco Teórico

3.1 El Plan de Recuperación ante Desastres (DRP)

En el contexto de la gestión de riesgos y la continuidad operativa, la recuperación ante desastres juega un rol crucial para mitigar los efectos inmediatos de una crisis. Snedaker (2024) define al DRP como una de las partes que compone al plan de continuidad del negocio (BCP) y se ocupa del impacto inmediato de un evento. La recuperación ante desastres implica detener los efectos del desastre lo más rápido posible y abordar las consecuencias inmediatas. Esto podría incluir apagar sistemas que han sido comprometidos, evaluar qué sistemas se han visto afectados por una inundación o terremoto y determinar la mejor manera de proceder. En algún momento durante la recuperación ante desastres, las actividades de continuidad del negocio comienzan a superponerse. Dónde establecer sistemas temporales, cómo adquirir sistemas o partes de repuesto, cómo establecer seguridad en una nueva ubicación: todas son preguntas que se relacionan tanto con la recuperación ante desastres como con la continuidad del negocio, pero que están principalmente enfocadas en continuar con las operaciones empresariales. La planificación, implementación y evaluación forman parte del ciclo continuo de mantenimiento de un DRP. (Snedaker, 2007).

La implementación de un DRP es fundamental para minimizar pérdidas económicas y operativas que pueden derivarse de un evento de desastre. Según la investigación realizada por Herbane, Elliott y Swartz (2004), las organizaciones que carecen de un plan de recuperación efectivo están en mayor riesgo de sufrir pérdidas financieras irreparables y daño a la imagen de la compañía. La capacidad de una organización para recuperarse rápidamente de un desastre es esencial para su sostenibilidad a largo plazo (Herbane et al., 2004).

3.1 Tiempo Objetivo de Recuperación (RTO)

En la planificación de la recuperación ante desastres, uno de los aspectos más críticos es el tiempo que una organización puede tolerar sin acceso a funciones o sistemas clave. Este período de inactividad tiene implicaciones directas en la continuidad del negocio y la minimización de pérdidas. En este contexto, el Tiempo Objetivo de Recuperación (RTO) se convierte en un parámetro fundamental. Según Wallace y Weber (2004), el RTO se refiere al tiempo máximo permitido para restaurar una función o sistema crítico después de un fallo o desastre antes que se produzcan consecuencias intolerables para el negocio. Este concepto es

clave para establecer los recursos y estrategias necesarios que garanticen la reanudación de las operaciones dentro del plazo estipulado. (Wallace y Weber, 2004).

Como se observa en la Figura 1, la definición del RTO deberá ser establecida en base a las unidades de tiempo requeridas para la recuperación de los servicios críticos.

Figura 1

RTO



Nota: Tomado de *RTO* [Imagen], de Denis G, 2020, MSP360(<https://www.msp360.com/resources/blog/rto-vs-rpo-difference/>)

Para cada función crítica dentro de una organización, es fundamental desarrollar los Objetivos de Tiempo de Recuperación (RTO). Algunas funciones críticas podrían necesitar ser recuperadas dentro de las 24 horas, mientras que las funciones vitales podrían requerir hasta 72 horas para su recuperación. Alternativamente, se puede asignar una criticidad a cada proceso y luego establecer los RTO correspondientes de manera individual. Este enfoque puede ser útil en empresas con numerosos procesos críticos que no se pueden abordar simultáneamente. La colaboración con expertos de cada división o departamento es esencial para entender los plazos de recuperación necesarios y las interdependencias entre departamentos, procesos y sistemas. (Snedaker, 2007).

También explora la relación entre el costo de recuperación y el costo de inactividad. Cada empresa debe evaluar estos costos para encontrar el punto óptimo en el que los costos de recuperación y los costos por inactividad se interceptan. A medida que aumenta el tiempo sin un proceso clave, los costos asociados con la pérdida de ventas y el aumento de los costos por la interrupción también aumentan. Sin embargo, los costos de recuperación tienden a disminuir cuando se dispone de más tiempo para recuperarse. Determinar este punto de intersección es crucial para la planificación, aunque puede ser complicado identificarlo con precisión en la práctica (Snedaker, 2007).

En el ejemplo proporcionado por Denis G. (2023) en el portal web MSP360, si una organización establece un RTO de 2 horas, la organización debería ser capaz de reanudar sus actividades dentro de ese tiempo. Sin embargo, si en una situación real de recuperación ante desastres se excede el tiempo estipulado, es necesario revisar los cálculos del RTO y actualizar el plan y los procedimientos de continuidad para garantizar que se pueda cumplir con dicho objetivo (Denis G., 2023).

Para calcular el RTO, Denis G. (2023) destaca los siguientes factores a tener en cuenta: el costo por hora de interrupción, la importancia y prioridad de los diferentes sistemas, los pasos necesarios para recuperarse (incluidos los componentes y procesos específicos), el presupuesto y los recursos disponibles para la recuperación. Estos elementos permiten a las organizaciones establecer un RTO realista que se ajuste a sus capacidades y necesidades operativas, evitando pérdidas significativas y garantizando la resiliencia ante desastres (Denis G., 2023).

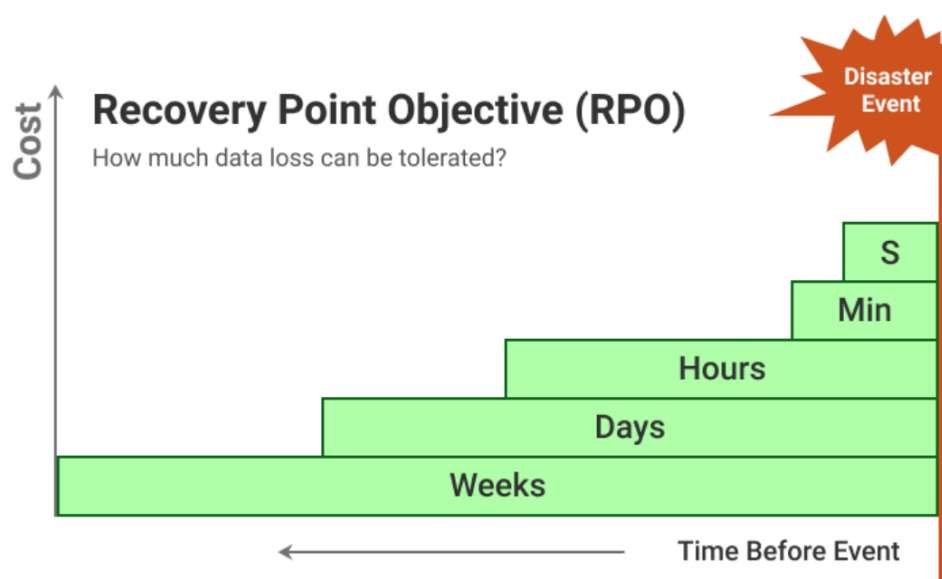
3.2 Punto de Recuperación Objetivo (RPO)

El Recovery Point Objective (RPO) o Punto de Recuperación Objetivo es uno de los conceptos fundamentales en la planificación de la recuperación ante desastres. Kesa (2023) define al RPO como el punto en el tiempo al cual los datos deben ser recuperados tras un incidente, es decir, el RPO determina la cantidad máxima de datos que una organización está dispuesta a perder (Kesa, 2023).

Las variables que definen al RPO se representan en la Figura 2, determinando la cantidad de datos que una organización está dispuesta a perder.

Figura 2

Variables del RPO



Nota: Tomado de RPO [Imagen], de Denis G, 2020, MSP360(<https://www.msp360.com/resources/blog/rto-vs-rpo-difference/>)

En su libro *Business Continuity & Disaster Recovery* (2007), Snedaker subraya cómo, mediante una estrategia de respaldo, las organizaciones realizan copias de seguridad en tiempo real, por horas, diarias o semanales, dependiendo de sus necesidades y del nivel de tolerancia a la pérdida de datos. Por ejemplo, si las copias de seguridad se efectúan semanalmente y ocurre una falla antes de la siguiente copia, podría perderse una semana completa de datos. Este es el punto de recuperación definido por el RPO. Si dicha pérdida resulta inaceptable, es imprescindible revisar y ajustar los procesos de respaldo actuales de la empresa. El RPO se basa tanto en los procedimientos operativos como en las estimaciones de posibles interrupciones, como desastres naturales. Definir un RPO adecuado es fundamental para asegurar que los procesos de recuperación puedan cumplir con los plazos establecidos (Snedaker, 2007).

Denis G. (2023) en su artículo para MSP360 introduce una capa adicional de complejidad en la definición del Recovery Point Objective (RPO) al considerar conjuntos de datos de producción en tiempo real. Como ejemplo, si una base de datos de producción queda inactiva y se establece un RPO de cuatro horas, esto implica que la organización puede tolerar la pérdida de datos de ese periodo. Sin embargo, si las copias de seguridad se realizan cada dos

horas, los datos deben recuperarse en dos horas, no en cuatro. Esto se debe a que cada hora de inactividad adicional genera una pérdida de datos que normalmente serían insertados, modificados o eliminados en la base de datos de producción. Por lo tanto, el RPO no solo se basa en la frecuencia de las copias de seguridad, sino también en la capacidad de la organización para restaurar los datos rápidamente y minimizar el impacto de la inactividad (Denis G., 2023).

Denis G. (2023) destaca tres factores clave para determinar el RPO de una organización: la cantidad máxima tolerable de pérdida de datos, el costo asociado a dicha pérdida, los recursos disponibles para implementar las soluciones de recuperación. Estos factores permiten a las organizaciones adaptar su estrategia de respaldo de manera que se ajusten a sus necesidades operativas y financieras (Denis G., 2023).

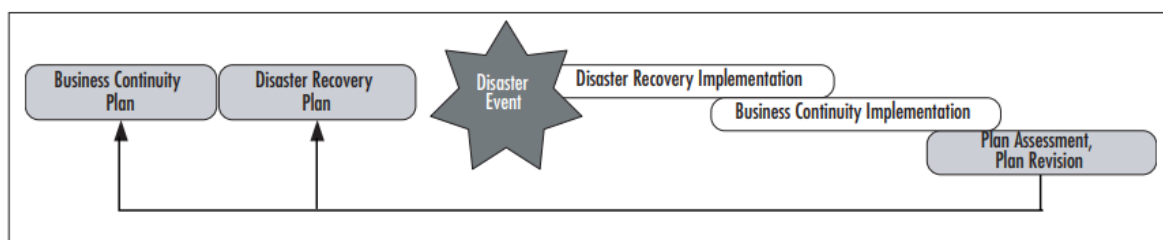
3.3 Plan de Continuidad del Negocio (BCP)

La continuidad de las operaciones es un aspecto esencial para cualquier organización, especialmente frente a situaciones de crisis o desastres. Para asegurar que una empresa pueda seguir funcionando en estos escenarios, se han desarrollado diversas estrategias y metodologías enfocadas en la planificación de la continuidad del negocio. Snedaker (2007) define al BCP como la metodología utilizada para crear y validar un plan que asegure la continuidad de las operaciones comerciales antes, durante y después de desastres y eventos disruptivos. Esta metodología es fundamental para garantizar que una organización pueda mantener su operatividad incluso en las situaciones más críticas (Snedaker, 2007).

A continuación, en la Figura 3 se destaca el orden de ejecución desde la elaboración del BCP y DRP, hasta el momento de su implementación.

Figura 3

Planificación, implementación y continuidad del negocio y recuperación ante desastres



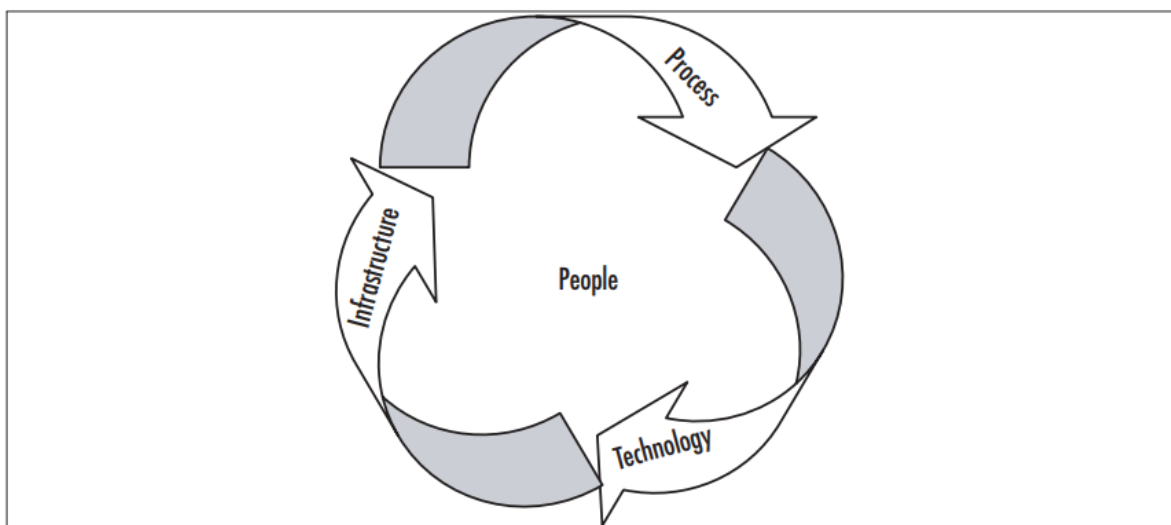
Nota: Tomado de *Business Continuity and Disaster Recovery Planning, Implementation, and Revision Cycle* (p. 5), por Snedaker, S, 2007, Syngress.

La continuidad del negocio (BCP) se enfoca en gestionar los aspectos operativos que permiten que una organización funcione de manera normal para generar ingresos. Este concepto suele aplicarse al evaluar diversas estrategias tecnológicas. Por ejemplo, algunas empresas, como las instituciones financieras, los procesadores de pagos con tarjetas de crédito y ciertos minoristas en línea de alto volumen, no pueden permitirse interrupciones en sus operaciones. Estas organizaciones consideran que invertir en sistemas totalmente redundantes es justificable, ya que incluso unos pocos minutos de inactividad podrían generar pérdidas millonarias. Para estas compañías, es fundamental mantener sus operaciones en funcionamiento de manera continua, y sus planes operativos generales reflejan esta prioridad. La continuidad del negocio, en esencia, se trata de garantizar que la empresa siga operativa independientemente del riesgo, la amenaza o la causa de una interrupción (Snedaker, 2007).

Sobre la Figura 4, podemos observar el ciclo de interacción entre Infraestructura, Proceso y Tecnología.

Figura 4

Cómo interactúan las personas, los procesos y la tecnología



Nota: Tomado de *How People, Process, and Technology Interact* (p. 5), por Snedaker, S, 2007, Syngress.

Otro aspecto fundamental es la consideración del “Costo de la Planificación frente al Costo del Trabajo”. Según Snedaker (2007), la planificación proactiva para la continuidad del negocio puede parecer costosa, pero es significativamente más económica en comparación con los costos asociados a una interrupción no planificada, la falta de preparación puede resultar en pérdidas financieras graves, daños a la reputación, y la pérdida de clientes, lo cual puede ser devastador para cualquier organización. Este análisis subraya la importancia de invertir en un BCP robusto para evitar consecuencias catastróficas (Snedaker, 2007).

3.4 Análisis de Impacto en el Negocio (BIA)

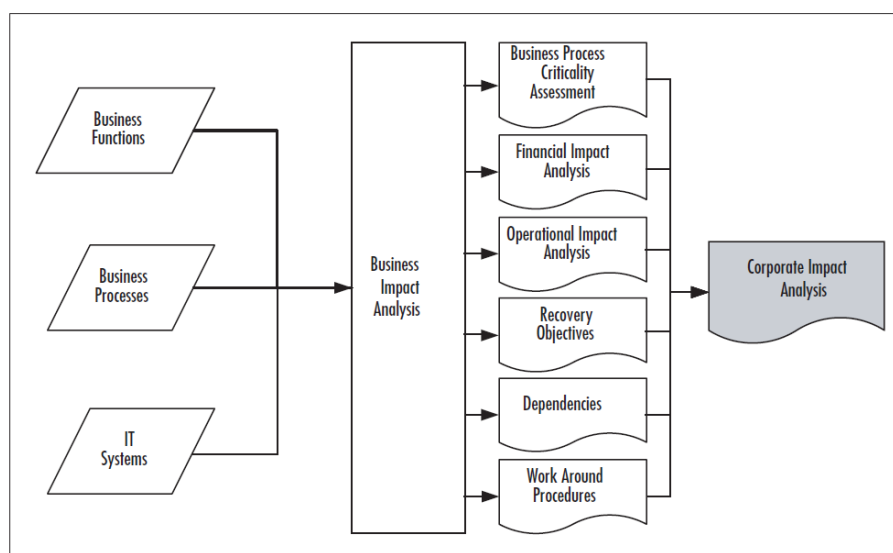
El análisis de impacto en el negocio (BIA) constituye un pilar fundamental dentro del proceso de gestión de riesgos. En base a la definición elaborada por Snedaker en su libro “Business Continuity & Disaster Recovery”, define al BIA como un proceso de análisis que permite identificar los posibles efectos que podrían derivarse de amenazas previamente detectadas y que podrían interrumpir las operaciones de una organización. A lo largo de este proceso, se analizan las diferentes fuentes de riesgo en función de la vulnerabilidad de la empresa a cada una de ellas, clasificándolas según su nivel de importancia. Es común que el BIA se enfoca en aquellas amenazas con mayor probabilidad de ocurrencia y que puedan tener un impacto significativo en la empresa. Los resultados obtenidos del BIA proporcionan

información clave para el desarrollo de estrategias de mitigación, facilitando así la toma de decisiones sobre cómo manejar posibles interrupciones en el negocio (Snedaker, 2007).

La figura 5 presenta como se desarrolla el flujo de trabajo para la elaboración de un BIA.

Figura 5

Flujo de elaboración de un BIA



Nota: Tomado de *BIA Inputs and Outputs* (p. 224), por Snedaker, S, 2007, Syngress.

La realización del BIA implica identificar y evaluar los riesgos potenciales que podrían afectar el funcionamiento de la organización, considerando factores como la probabilidad de ocurrencia, el impacto en las operaciones y el tiempo de recuperación. Como sugieren Wallace & Weber (2017), es recomendable involucrar al equipo de planificación de desastres en la evaluación para aprovechar el conocimiento institucional disponible. La evaluación se puede estructurar utilizando una escala de probabilidad (de 0 a 10) para medir la posibilidad de que un evento ocurra en un horizonte temporal definido, como los próximos 5 años. Además, se debe asignar una puntuación al impacto potencial (de 0 a 10), donde 0 indica un impacto mínimo y 10 representa una amenaza severa para la continuidad del negocio. También se debe estimar el tiempo de restauración (en una escala de 1 a 10) donde 10 representa una rápida

recuperación y 1 indica un proceso de recuperación prolongado. Este enfoque permite priorizar los riesgos más significativos. (Wallace & Weber, 2017).

3.5 Normativas BCRA

El Banco Central de la República Argentina (BCRA) es la autoridad monetaria del país, cuya misión principal es promover la estabilidad monetaria, financiera y económica, así como garantizar el buen funcionamiento del sistema financiero. Fundado en 1935, el BCRA desempeña un rol crucial en la regulación y supervisión de las entidades financieras y cambiarias del país, con el objetivo de asegurar la solidez y estabilidad del sistema financiero argentino. Las normativas comunicadas por el BCRA son directrices, resoluciones y disposiciones que establecen los lineamientos y requisitos que las entidades financieras deben cumplir para operar dentro del marco legal y regulatorio del país. Estas normativas cubren una amplia variedad de temas, incluyendo la gestión del riesgo crediticio, la gestión de liquidez, la protección al consumidor y la continuidad del negocio (Banco Central de la República Argentina, 2023a).

La normativa A 7724, es una regulación publicada por el BCRA en el año 2023 que establece los lineamientos para la gestión de la continuidad del negocio en las entidades financieras. En su sección 6, la normativa enfatiza la necesidad de que las instituciones financieras desarrollen, implementen y mantengan un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), estos deben estar diseñados para asegurar que la entidad pueda continuar operando y cumplir con sus obligaciones regulatorias, contractuales y de servicio en caso de una interrupción significativa de las operaciones. Específicamente, la normativa A 7724 requiere que las entidades financieras identifiquen las funciones críticas y los recursos necesarios para su operación continua, implementen estrategias para la recuperación y restauración de estas funciones en un tiempo razonable, y lleven a cabo pruebas periódicas para validar la efectividad de estos planes (Banco Central de la República Argentina, 2023b).

La normativa también señala la importancia de documentar adecuadamente todos los procedimientos, mantener actualizados los planes de continuidad y recuperación del negocio, capacitar al personal involucrado en ejecución de estos planes. Además de lo que se requiere que las entidades reporten al BCRA cualquier incidente significativo que afecte a la continuidad del

negocio, junto con las acciones correctivas tomadas (Banco Central de la República Argentina, 2023b).

El detalle completo de la normativa A 7724 – Sección 6 se puede consultar en el Anexo A.

3.6 Virtualización en el contexto de un DRP

Esta sección abordará la importancia y el rol de la virtualización en la implementación de un Plan de Recuperación ante Desastres (DRP), con un enfoque en cómo esta tecnología facilita la resiliencia operativa y la recuperación rápida de los sistemas críticos en un entorno financiero.

Basado en el artículo publicado por RevistaCloud, un reconocido medio de divulgación tecnológica, titulado "La virtualización en la recuperación ante desastres", se ofrece una definición clara de cómo la virtualización puede fortalecer un Plan de Recuperación ante Desastres (DRP). El artículo destaca que asegurar la continuidad del negocio es crucial en la actualidad, y una manera efectiva de lograrlo es mediante estrategias robustas de recuperación ante desastres. La virtualización ha surgido como un elemento fundamental en estas estrategias, proporcionando una mayor resiliencia y tiempos de recuperación reducidos. Según el artículo, "La virtualización puede transformar significativamente tu plan de recuperación ante desastres, haciéndolo más eficiente y confiable" (Revista Cloud, 2024). En este contexto, implica la creación de versiones virtuales de componentes físicos como servidores, dispositivos de almacenamiento o recursos de red. Este enfoque presenta varias ventajas importantes para la recuperación ante desastres:

- **Mejora en Copias de Seguridad y Restauración:** Las máquinas virtuales (VMs) facilitan las copias de seguridad y la restauración.
- **Independencia del Hardware:** La virtualización abstrae la capa de hardware, permitiendo que las VMs funcionen en distintos equipos físicos.
- **Eficiencia de Costos:** A diferencia de las soluciones tradicionales de recuperación ante desastres que requieren hardware duplicado, la virtualización minimiza la necesidad de infraestructura física adicional.

- **Pruebas y Validación:** La virtualización permite realizar pruebas de los procedimientos de recuperación de manera no disruptiva.
- **Reducción de los Tiempos de Objetivo de Recuperación (RTOs):** La virtualización contribuye a reducir significativamente los RTOs al permitir una recuperación más rápida de sistemas y aplicaciones.
- **Mejora de los Objetivos de Punto de Recuperación (RPOs):** La virtualización facilita el cumplimiento de RPOs más bajos mediante copias de seguridad frecuentes y eficientes.

Este enfoque centralizado simplifica la administración de los planes de recuperación ante desastres y asegura una mayor consistencia en toda la infraestructura (Revista Cloud, 2024).

3.7 Herramientas para la recuperación ante Desastres

Las herramientas tecnológicas juegan un papel fundamental para asegurar la continuidad operativa dentro de una organización. Estas herramientas no solo deben permitir la rápida recuperación de los sistemas, sino que también optimizan los procesos y reducen los costos asociados a la gestión de infraestructura. A continuación, se detallan las principales herramientas utilizadas en la implementación de un DRP, destacando sus características, ventajas y aplicación en entornos virtualizados.

La automatización y orquestación de los procesos de recuperación son vitales para asegurar una respuesta rápida y coordinada. En este sentido, Veeam Data Platform: Recovery Orchestration permite automatizar la recuperación de máquinas virtuales, entre sus principales características podemos mencionar la creación de planes de recuperación personalizados y flexibles, la ejecución de pruebas automatizadas de los planes de DR sin interrumpir las operaciones diarias, gestión de reportes con la posibilidad de crear informes detallados sobre las pruebas de DR y recuperaciones reales a fin de contar con la información de respaldo para auditorías y como última característica se destaca su integración nativa con el software de respaldo de datos Veeam Backup & Replication (Veeam, 2024).

Otra de las herramientas a considerar es VMware Site Recovery Manager, es una solución de recuperación ante desastres (DR) diseñada para facilitar la planificación, automatización y ejecución de la recuperación de máquinas virtuales en entornos VMware Vsphere, dentro de sus características se encuentra la posibilidad de elaboración y ejecución de planes de recuperación personalizados por grupo de aplicaciones, pruebas no disruptivas de recuperación sin afectar entornos productivos, soporte para replicación de datos: se integra con múltiples soluciones de replicación, incluida la replicación nativa de VMware con VSphere Replication y soluciones de terceros compatibles con SRM (VMware, 2024a).

Por último, podemos mencionar a Zerto Disaster Recovery, es una solución diseñada para proteger y replicar aplicaciones y datos en entornos virtualizados, nubes públicas y privadas. Se enfoca en ofrecer replicación continua de datos, lo que permite a las organizaciones minimizar la pérdida de datos y el tiempo de inactividad en caso de un desastre. Zerto utiliza replicación continua a nivel de hipervisor (Hypervisor-based Replication) eliminando la necesidad de tomar snapshots o backups programados, permite restaurar aplicaciones y datos en minutos ofreciendo un RTO muy bajo, además ofrece un amplio historial de puntos de recuperación, permitiendo a los administradores seleccionar versiones específicas de aplicaciones y datos en función de diferentes tiempos (Zerto, 2024).

4 Acciones a Realizar

4.1 Análisis

4.1.1 *Análisis de la infraestructura de virtualización*

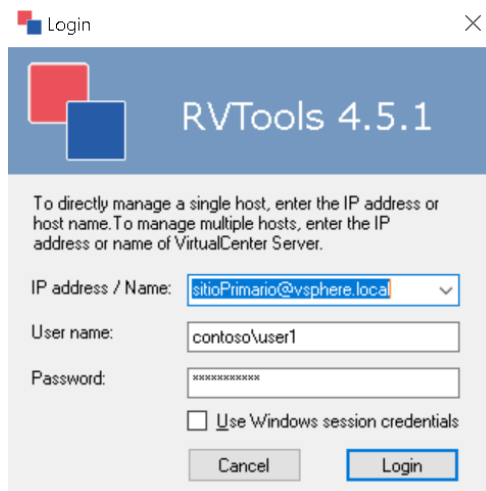
El análisis es la primera fase en la implementación de un Plan de Recuperación ante Desastres (DRP) en un entorno de virtualización con VMware Vsphere. En esta etapa se realiza la evaluación de la infraestructura actual, las necesidades de replicación de datos, las políticas de recuperación, y los requerimientos técnicos y operativos para asegurar que el DRP sea efectivo y sostenible en el tiempo.

RVTools es una herramienta gratuita desarrollada por Rob de Veij en el año 2008, diseñada para proporcionar una visión detallada de un entorno de VMware Vsphere. Esta herramienta es utilizada para recopilar información sobre máquinas virtuales, hosts, almacenamiento, redes y recursos asignados. La página de descarga proporciona acceso gratuito a la descarga del software desde la opción “Download”, se deberá completar por única vez un formulario de registro y se procede a la descarga. Además, se deben cumplir con los siguientes requisitos: un equipo con Microsoft Windows (compatible con Windows 10 o superior). NET Framework 4.5 o superior debe estar instalado en el sistema, acceso de lectura al vCenter o a los hosts ESXI directamente mediante las credenciales de usuarios con permisos administrativos (Robware, 2008).

Después de descargar e instalar la herramienta, se deberán ingresar las credenciales del vCenter ubicado en el sitio primario como se puede observar en la Figura 6.

Figura 6

RVTools



Nota: Imagen de elaboración propia.

Una vez establecida la conexión, mostrará una serie de pestañas con información sobre las máquinas virtuales (VM's), hosts ESXi, redes, almacenamiento y más. Estos datos serán fundamentales para la elaboración del plan, a continuación, se describen las áreas más importantes a analizar y cómo será utilizada la información obtenida.

En la Figura 7, podemos observar como se visualiza la información mediante RVTools.

Figura 7

Pestañas de RVTools

VM	Powerstate	Template	SRM Placeholder	Config status	DNS Name	Connection state	Guest state	Heartbeat	Consolidation Needed
BASTIONPROD02	poweredOn	False	False	green	bastionprod02.prod02.ocp.bpba	connected	running	green	False
lab01-xgrn5-intra-jstnl	poweredOn	False	False	green	lab01-xgrn5-intra-jstnl	connected	running	green	False
lab01-xgrn5-intra-#92b	poweredOn	False	False	green	lab01-xgrn5-intra-#92b	connected	running	green	False
lab01-xgrn5-intra-monitor-b9g69	poweredOn	False	False	green	lab01-xgrn5-intra-monitor-b9g69	connected	running	green	False
lab01-xgrn5-intra-monitor-g8hiz	poweredOn	False	False	green	lab01-xgrn5-intra-monitor-g8hiz	connected	running	green	False
lab01-xgrn5-intra-trnfrq	poweredOn	False	False	green	lab01-xgrn5-intra-trnfrq	connected	running	green	False
lab01-xgrn5-master-0	poweredOn	False	False	green	lab01-xgrn5-master-0	connected	running	gray	False
lab01-xgrn5-master-1	poweredOn	False	False	green	lab01-xgrn5-master-1	connected	running	gray	False
lab01-xgrn5-master-2	poweredOn	False	False	green	lab01-xgrn5-master-2	connected	running	green	False
lab01-xgrn5-thcos	poweredOff	True	False	green		connected	notRunning	gray	False
lab01-xgrn5-worker-mwvip	poweredOn	False	False	green	lab01-xgrn5-worker-mwvip	connected	running	green	False
lab01-xgrn5-worker-pr4bv	poweredOn	False	False	green	lab01-xgrn5-worker-pr4bv	connected	running	green	False
lab01-xgrn5-worker-qvthk	poweredOn	False	False	green	lab01-xgrn5-worker-qvthk	connected	running	green	False
lab01-xgrn5-worker-vx49	poweredOn	False	False	green	lab01-xgrn5-worker-vx49	connected	running	green	False

Nota: Imagen de elaboración propia.

De acuerdo con la descripción de Robware (2008), la pestaña vInfo proporciona una lista detallada de todas las máquinas virtuales, incluyendo información relacionada con la configuración de la CPU, la memoria y los discos. Las pestañas vDatastore y vDisk presentan detalles sobre el uso del almacenamiento. Por su parte, vTools y vHardware permiten identificar el estado de las VMTools y la versión de la compatibilidad de hardware de las máquinas virtuales. Finalmente, la pestaña vNetwork ofrece información detallada sobre las redes virtuales configuradas en las máquinas virtuales (Robware, 2008).

Esta información es esencial para identificar las máquinas virtuales críticas asociadas a las aplicaciones definidas en el Análisis de Impacto en el Negocio (BIA), las cuales deben ser replicadas. Asimismo, permite calcular los recursos necesarios para el sitio de contingencia, como vCPU, RAM y la capacidad de almacenamiento (discos) requerida. Es fundamental también identificar las versiones de VMTools y el hardware virtual, asegurando que estén actualizados, con el fin de prevenir futuros problemas de compatibilidad durante la replicación y recuperación de las máquinas virtuales. Además, reconocer desde esta fase inicial las redes virtuales involucradas en el plan de recuperación ayudará a evitar posibles conflictos en el momento de realizar la recuperación.

Como se muestra en la Tabla 1, los recursos necesarios para replicar las máquinas virtuales en el sitio de contingencia serán:

Tabla 1

Recursos de Máquinas Virtuales y Requerimientos para el Sitio de Contingencia

Nombre de la VM	vCPU	RAM (GB)	Disco (GB)
VM1	4	16	100
VM2	2	8	50
VM3	6	32	200
Total	12	56	350

Nota: Esta tabla muestra los recursos necesarios para las máquinas virtuales en el sitio primario, los cuales serán replicados en el sitio de contingencia. Elaboración Propia.

4.1.2 Elección de VMware Site Recovery Manager (SRM) como herramienta de Orquestación

Continuando con el análisis de la infraestructura a proteger, en segunda instancia se deberá avanzar con la definición de la herramienta de software que funcionará como orquestación del plan de recuperación, gestionará los recursos de procesamiento identificados sobre las máquinas virtuales a proteger y deberá integrarse con VMware Vsphere, tanto en el sitio Primario como en el de Contingencia. Como se mencionaba anteriormente, en un entorno de virtualización, existen diversas herramientas de orquestación que permiten automatizar y simplificar los procesos de replicación y recuperación de datos.

Basándonos en la documentación ofrecida por VMware (2024) describiendo las características técnicas de la solución, la elección de Site Recovery Manager frente a otras soluciones de orquestación de desastres se fundamenta en una serie de ventajas clave. La primera característica es su integración nativa con Vsphere, garantizando la compatibilidad entre el software de orquestación y la plataforma de virtualización. Otra característica que podemos mencionar del documento es la automatización de la recuperación, creando planes de recuperación predefinidos, incluyendo secuencia de arranque de máquinas virtuales. Gestión centralizada, tanto el sitio primario (Sitio Protegido) como el sitio de Contingencia (Sitio de Recuperación), serán gestionados desde una única consola centralizada integrada a la misma herramienta de virtualización con VMware vCenter. Site Recovery Manager ofrece la posibilidad de ejecutar pruebas no disruptivas, lo cual es posible simular un evento de recuperación sin impactar el entorno de producción. (VMware, 2024a).

Como se puede observar en la Tabla 2, VMware Site Recovery Manager destaca por su alta integración con VSphere, administración centralizada, menor despliegue de recursos y su capacidad de replicación de datos por LAN y Storage, dispositivo de almacenamiento, lo que lo diferencia de otras soluciones de orquestación como Zerto.

Tabla 2

Comparativa Site Recovery Manager vs Zerto

Característica	Site Recovery Manager	Zerto
Integración con VMware	Alta integración con Vsphere, vMotion y DRS	Integración con VMware vCenter
Automatización de la Recuperación	Automática con planes predefinidos	Automática con planes predefinidos
Pruebas de Recuperación	Sí, permite pruebas sin afectar producción	Sí, permite pruebas sin afectar producción
Compatibilidad con Replicación	Compatible con VMware vSphere Replication y soluciones de replicación por Storage	Solo Replicación por LAN, no permite integración con Storage
Gestión Centralizada	Única consola de administración integrada con vCenter	Consola de administración propia adicional a vCenter
Recursos	Un único Virtual Appliance por cada sitio	Requiere una máquina virtual por sitio para su administración, adicionalmente una máquina virtual por host por cada sitio para el rol de replica

Nota: Esta tabla realiza una comparativa de características entre Site Recovery Manager y Zerto. Elaboración Propia.

4.1.3 Elección de la tecnología de replicación basada en almacenamiento (Storage Based-Array)

Habiendo definido anteriormente las máquinas virtuales a replicar, luego seleccionando la herramienta que vamos a utilizar para realizar la orquestación de la recuperación, el siguiente punto que nos queda por analizar será la tecnología de replicación a utilizar para la elaboración de nuestro DRP, en este caso optaremos por realizar la replicación basada en almacenamiento

o Storage Based-Array, una solución que ofrece beneficios significativos en términos de rendimiento, seguridad y flexibilidad, especialmente en infraestructura que manejan grandes volúmenes de datos, como es el caso de las entidades financieras.

La replicación de almacenamiento es una técnica esencial para la protección de datos en entornos empresariales, ya que garantiza la continuidad operativa en caso de fallas en la infraestructura primaria. Esta tecnología permite replicar volúmenes de datos entre servidores o clústeres, de manera que se construyan redundancias que aseguren la disponibilidad de los datos en sitios alternativos, como parte de una estrategia integral de recuperación ante desastres (Bhardwaj, s.f.).

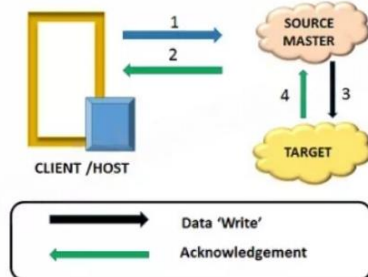
Una de las modalidades de replicación de almacenamiento es la replicación asíncrona. Bhardwaj destaca que este tipo de replicación debería ser considerado donde la replicación de datos es realizada a través de sitios geográficamente distantes. Cuando ocurre una operación de escritura en el sitio de origen, el servidor de producción recibe una confirmación inmediata sin esperar a que los datos se repliquen en el sitio remoto, esto permite una mayor eficiencia, acumulando las solicitudes de escritura en un buffer en el sitio de origen. Luego estas escrituras serán transferidas en intervalos regulares al sitio secundario, lo que exige una planificación adecuada de la capacidad de buffer basada en el RPO (previamente definido en el BIA) (Bhardwaj, s.f.).

La Figura 8 destaca el circuito de replicación asíncrona de un dispositivo de almacenamiento.

Figura 8

Replicación Asíncrona

Asynchronous Storage Replication



Nota: Tomado de *Asynchronous Replication* [Imagen], de Bhardwaj R, s.f., NetworkInterview(<https://networkinterview.com/what-is-storage-replication/>)

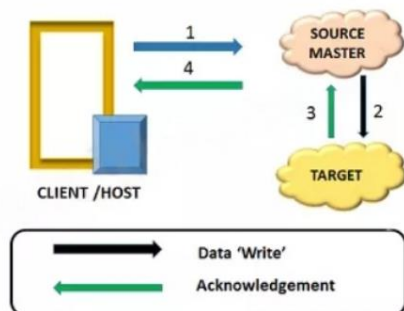
Otras de las modalidades disponibles, es la replicación de datos síncrona, en esta técnica las escrituras se comprometen tanto en el origen como en el objetivo remoto antes de enviar la confirmación de “escritura completada” al servidor de producción. Ninguna escritura adicional ocurre hasta que las escrituras anteriores se hayan completado y confirmado. Esto asegura que los datos en el origen y en el sitio remoto sean siempre idénticos, y que las escrituras se realicen en el mismo orden en que fueron recibidas, garantizando la consistencia de los datos (Bhardwaj, s.f.).

A continuación, en la Figura 9, se representa un esquema de replicación síncrona en un dispositivo de almacenamiento.

Figura 9

Replicación Síncrona

Synchronous Storage Replication



Nota: Tomado de *Synchronous Replication* [Imagen], de Bhardwaj R, s.f., NetworkInterview(<https://networkinterview.com/what-is-storage-replication/>)

Al implementar Site Recovery Manager (SRM) como herramienta de orquestación de desastres, es esencial realizar la validación de compatibilidad entre el Storage utilizado en la infraestructura de virtualización que vamos a proteger y el software de replicación. Para ello, VMware proporciona una matriz de compatibilidad que detalle las soluciones de almacenamiento compatibles con SRM, así como las características de replicación.

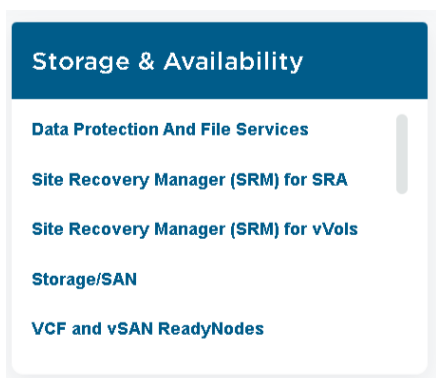
Para realizar esta validación, se debe seguir el siguiente procedimiento:

1. Acceder a la matriz de compatibilidad de VMware/Broadcom, ingresando al siguiente sitio oficial: <https://compatibilityguide.broadcom.com/>
2. Dentro de la matriz se deberá buscar el tipo de almacenamiento que se utiliza sobre la infraestructura de virtualización previamente relevada, ya sea que se trate de almacenamiento basado en discos locales, redes SAN, o dispositivos NAS. Para ello se dentro de la columna “Storage & Availability”, se deberá seleccionar la opción “Site Recovery Manager (SRM) for SRA”.

Podemos observar en la Figura 10 como debe realizarse una búsqueda sobre la matriz de VMware, teniendo en cuenta los distintos filtros que podemos aplicar.

Figura 10

Búsqueda en la matriz



Nota: Imagen de elaboración propia.

3. En la opción “Product Release Version:” debemos seleccionar la versión de SRM que se instalará, en este trabajo de intervención utilizaremos la última versión disponible SRM 9.0
4. En “Partner Name”, vamos a seleccionar el partner perteneciente al Storage, dispositivo de almacenamiento, de la infraestructura de virtualización que se esté utilizando, para este trabajo de intervención utilizaremos como partner a “Huawei Technologies”.
5. En la opción “Protocol”, debemos seleccionar todos los protocolos disponibles. En “Transport Type”, debemos seleccionar el medio de conexión físico que posea el Storage con nuestro entorno de virtualización, para este trabajo vamos a utilizar la opción “FC” (Fiber-Channel) y por último en “SRA Name”, seleccionamos “All”. En la figura 11, se pueden observar a detalle los filtros aplicados.

Figura 11

Aplicación de Filtros

< ☰ Reset View Results

Keyword

Product Release Version ☐ ^

- ☒ SRM 9.0
- ☐ SRM 8.8
- ☐ SRM 8.7
- ☐ SRM 8.6
- ☐ SRM 8.5
- ☐ SRM 8.4

Partner Name ☐ ^

- ☒ Huawei Technologies Co., Ltd.

Protocol ☒ ^

- ☒ NFS
- ☒ NVMe
- ☒ SCSI

Transport Type ☐ ^

- ☒ FC
- ☐ iSCSI
- ☐ NAS
- ☐ RDMAroCE v2
- ☐ TCP/IP

Nota: Imagen de elaboración propia.

Posterior a realizar la búsqueda se obtendrá un listado con los agentes SRA (Adaptador de Replicación de Storage) disponibles para el partner seleccionado, en este caso en la Figura 12 obtendremos los agentes disponibles para “Huawei Technologies”.

Figura 12

Agentes SRA Disponibles

Partner Name ^	SRA Name ↕	SRM Version(s)
Huawei Technologies Co., Ltd.	Huawei eSDK_Storage_SRA 2.6	Photon SRM 8.5, SRM 8.8, SRM 9.0, SRM 8.4, SRM 8.3, SRM 8.7, SRM 8.6, SRM 8.2
Huawei Technologies Co., Ltd.	Huawei eSDK_Storage_SRA 2.2	Windows SRM 8.1, SRM 8.2, SRM 8.3 Photon SRM 8.5, SRM 8.2, SRM 9.0, SRM 8.6, SRM 8.7, SRM 8.3, SRM 8.4, SRM 8.8

Nota: Imagen de elaboración propia.

En la columna “SRA Name” tendremos disponibles los agentes compatibles y sus versiones, para el presente trabajo utilizaremos siempre las últimas versiones. Debemos realizar clic sobre Huawei eSDK_Storage_SRA 2.6.

Luego de haber seleccionado el agente SRA mencionado, la próxima pantalla nos brindará la siguiente información: en la columna “Array Models”, podemos obtener los datos de los modelos de Storage del partner Huawei que están soportados para ser integrados con SRM; “Firmware Version”, indica las versiones de firmware soportadas por los dispositivos de almacenamiento; “Transport Type”, indica el medio de transporte soportado. En la Figura 13 se puede observar con mayor detalle esta información.

Figura 13

Matriz de Compatibilidad

[Back to Search Page](#)

SRA Detail

Partner Name: Huawei Technologies Co., Ltd.	SRA Name: Huawei eSDK_Storage_SRA	SRA Version: 2.6
Notes: For further details about array firmware, storage product configurations and best practices, please contact the storage vendor.		

SRA Release Details

VMware Product Name:
SRM 9.0

Management Software Name/Version	Replication Software Name/Version	OS Type	SRA Download	SRA MD5SUM	KB Articles	Notes	View Features
OceanStor Dorado 18000 V6 6.1	HyperReplication 6.1	Photon	[object Object]	4f6170ec3a8edff38cf3f8a9c8d67ed	N/A	-	View

Nota: Modelos de Storage compatibles con SRM que será utilizado para la implementación de este proyecto. Imagen de elaboración propia.

4.2 Diseño

4.2.1 *Diseño de la Arquitectura de Recuperación*

Tras completar el análisis de la infraestructura y las necesidades del entorno virtualizado, el siguiente paso en la implementación del Plan de Recuperación ante Desastres (DRP) es la etapa de diseño y arquitectura de la solución. Esta fase implica la planificación detallada de cómo se estructurará el sistema de recuperación ante desastres utilizando Site Recovery Manager (SRM) y las tecnologías de replicación seleccionadas.

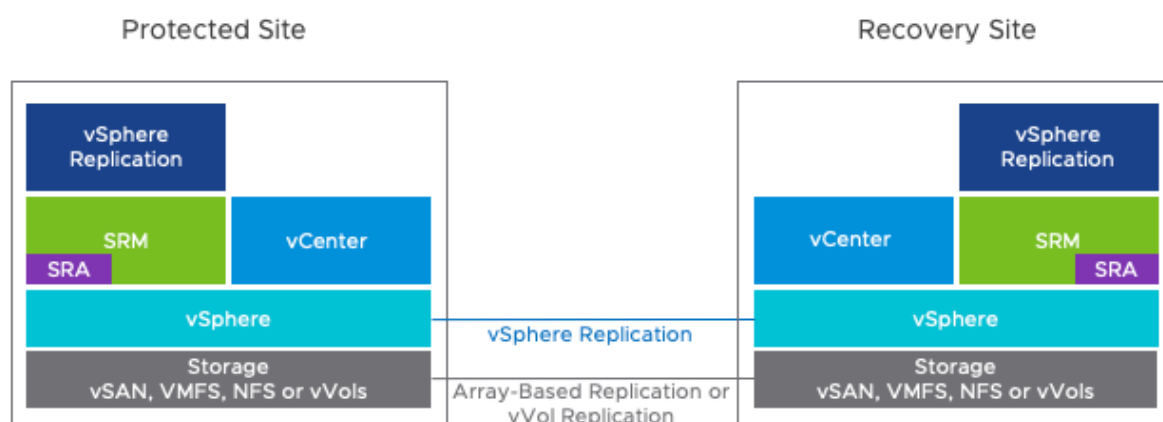
El diseño de la arquitectura de la solución de DRP con SRM debe comenzar con la definición clara de los sitios involucrados en el proceso de recuperación: el centro de Datos Primario o Sitio Protegido y el Centro de Datos Secundario o Sitio de Contingencia. El primero es el sitio que hospeda aplicaciones críticas que fueron definidas en el BIA (Análisis de Impacto del Negocio), mientras que el segundo es el sitio donde se replicarán y restaurarán dichas aplicaciones en caso de desastre.

En la web de características del producto ofrecida por VMware se detallan además otras características que deben cumplir los sitios, el sitio primario o sitio protegido se encarga de proveer los servicios críticos, mientras que el sitio remoto o sitio de contingencia actuara como alternativa para migrar estos servicios en caso de un evento de desastre. La ubicación del sitio de contingencia, es recomendable que se encuentre en otra ubicación geográfica al sitio primario, considerando dentro de ubicación que existe un menor riesgo a problemas ambientales o de infraestructura. Otra consideración respecto al sitio de contingencia, es que el mismo debe poseer recursos de hardware, red y almacenamiento compatibles con las aplicaciones e infraestructura del sitio primario, ambos sitios deben estar conectados mediante una red IP fiable, considerando el acceso a todas la redes públicas y privadas (VMware, 2023c).

A continuación, en la Figura 14 se observa un esquema básico de arquitectura entre el sitio protegido, el sitio de recuperación y sus componentes que debemos tomaremos en cuenta al diseñar nuestro proyecto de DRP.

Figura 14

Arquitectura de Sitios



Nota: Tomado de *Site Recovery Manager Technical Overview* [Imagen], Cato G., 2020, The Cloud Platform Tech Zone (<https://core.vmware.com/resource/site-recovery-manager-technical-overview#sec8949-sub1>)

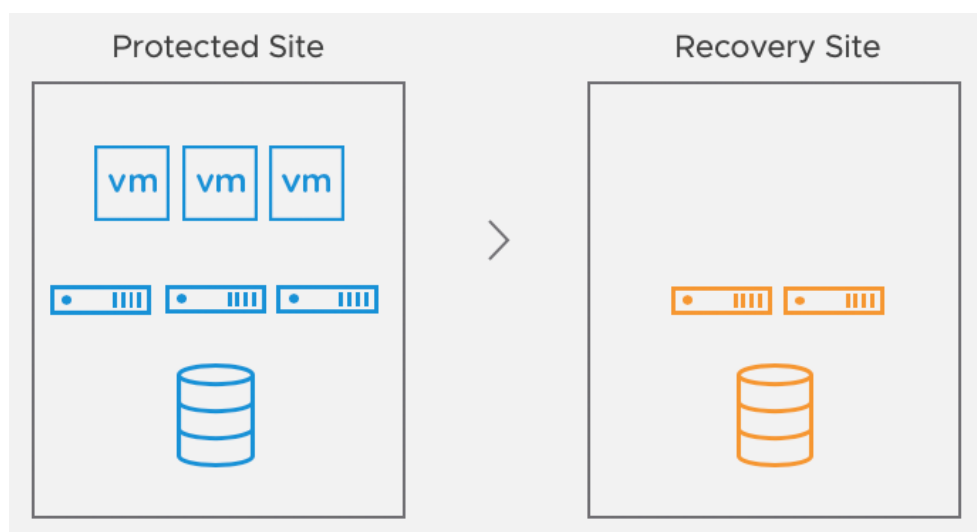
4.2.2 Topologías

Site Recovery Manager puede adaptarse a diferentes escenarios de failover, recuperación en caso de falla, según los requisitos y objetivos planteados, lo que permite una configuración flexible y sencilla de gestionar. Gracias a su integración nativa con vSphere, se facilita la gestión de múltiples topologías de sitios. El escenario más típico de todos ellos es la topología “Activo-Pasivo”, el sitio de producción se encarga de ejecutar las aplicaciones y servicios, mientras que el sitio de recuperación permanece inactivo hasta que sea necesario. Aunque este tipo de topología es muy común y ofrece recursos dedicados para la recuperación, implica un costo significativo, ya que el sitio de recuperación, los servidores y el almacenamiento permanecen subutilizados la mayor parte del tiempo (Cato G., 2020).

En la figura 15 podemos observar la topología de un esquema activo-pasivo.

Figura 15

Topología Activo-Pasivo

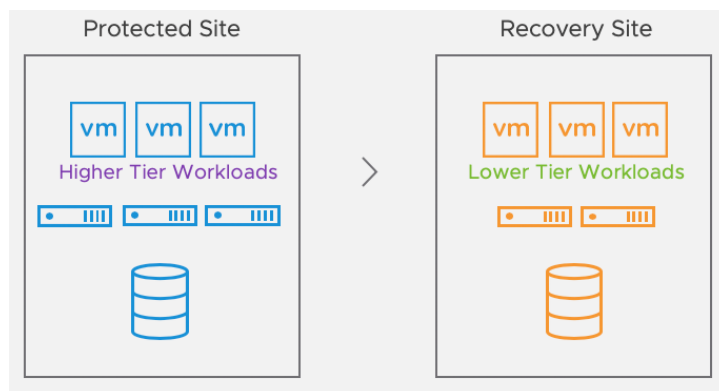


Nota: Tomado de *Site Recovery Manager Technical Overview* [Imagen], Cato G., 2020, The Cloud Platform Tech Zone(<https://core.vmware.com/resource/site-recovery-manager-technical-overview#sec8949-sub1>)

Continuando con la descripción de las posibles topologías que podemos utilizar para la implementación de SRM, otra opción disponible es la topología “Activo-Activo” que puede configurarse de manera que las cargas de trabajo de baja prioridad, como las destinadas a prueba y desarrollo, se ejecuten en el sitio de recuperación. Durante la activación del plan de recuperación ante desastres, estas cargas de trabajo se apagarán automáticamente, liberando así recursos que puedan ser utilizados en los sistemas críticos. Este enfoque permite aprovechar los recursos del sitio de recuperación durante el funcionamiento normal, mientras se asegura que haya suficiente capacidad para los sistemas esenciales en caso de emergencia, en la Figura 16 se puede apreciar la topología “Activo-Activo” (Cato G., 2020).

Figura 16

Topología Activo-Activo



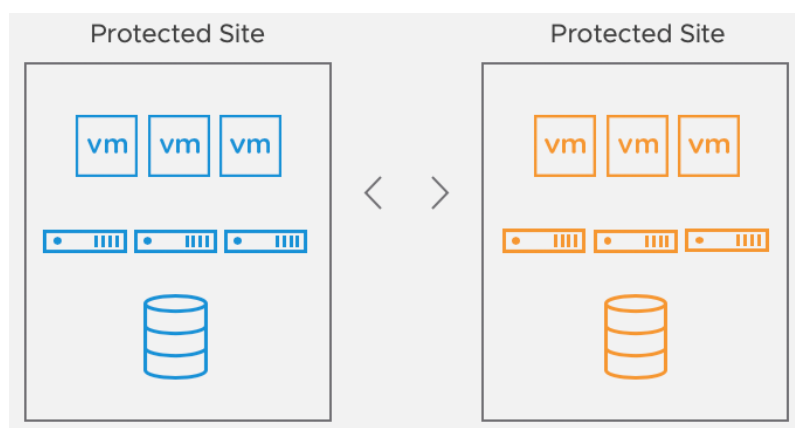
Nota: Tomado de *Site Recovery Manager Technical Overview* [Imagen], Cato G., 2020, The Cloud Platform Tech Zone (<https://core.vmware.com/resource/site-recovery-manager-technical-overview#sec8962-sub2>).

En situaciones donde las aplicaciones de producción están operando en ambos sitios, SRM permite la protección bidireccional de máquinas virtuales. Esto significa que las cargas de trabajo ejecutadas sobre el Sitio A pueden estar protegidas en el Sitio B y, viceversa, las cargas del Sitio B pueden estar protegidas en el Sitio A. Este enfoque de protección cruzada es altamente beneficioso para organizaciones que operan múltiples ubicaciones, ya que permite una mayor flexibilidad y resiliencia de los sitios, garantizando así la continuidad operativa en caso de desastres (Cato G., 2020).

El siguiente esquema representado en la Figura 17, observamos los componentes de una topología de replicación bidireccional.

Figura 17

Topología Bidireccional



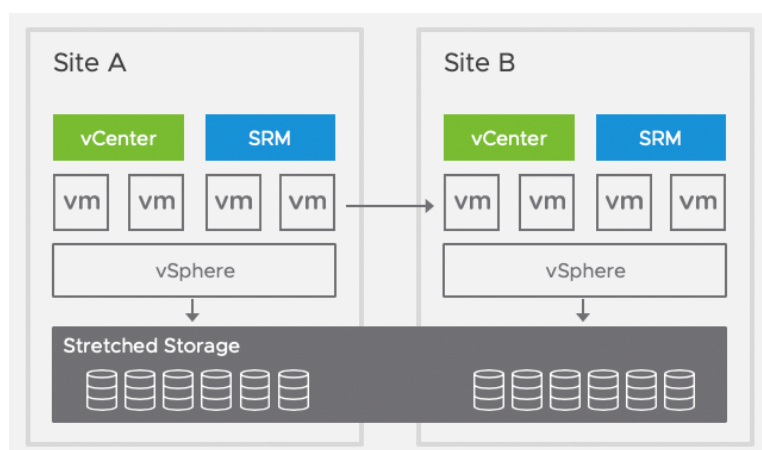
Nota: Tomado de *Site Recovery Manager Technical Overview* [Imagen], Cato G., 2020, The Cloud Platform Tech Zone(<https://core.vmware.com/resource/site-recovery-manager-technical-overview#sec8962-sub3>).

Aunque en este proyecto no se implementará la topología conocida como “Stretched Storage”, es relevante mencionarla debido a aplicabilidad en determinados entornos donde la arquitectura de la infraestructura lo permite. Esta configuración es utilizada en escenarios donde el tipo de almacenamiento permita la replicación sincrónica entre sitios geográficamente dispersos, lo que facilita alta disponibilidad de los datos. En entornos de almacenamiento extendido, ambos sitios actúan como una única entidad lógica de almacenamiento, permitiendo la continuidad de las operaciones incluso antes fallos en uno de los centros de datos. Según Cato G. (2020), la utilización de “Stretched Storage” posibilita evitar desastres sin tiempo de inactividad y realizar mantenimientos planificados sin interrupciones. Para aprovechar completamente esta tecnología y permitir la migración de máquinas virtuales protegidas mediante vMotion, es necesario contar con una conectividad de red capa 2 extendida entre sitios. VMware NSX es una solución recomendada para este propósito, ya que proporciona una serie de beneficios adicionales (Cato G, 2020).

La Figura 18 muestra un diagrama de la replicación mediante stretched storage, considerando un esquema de dos vCenter replicando sus datos.

Figura 18

Stretched Storage



Nota: Tomado de *Site Recovery Manager Technical Overview* [Imagen], Cato G., 2020, The Cloud Platform Tech Zone(<https://core.vmware.com/resource/site-recovery-manager-technical-overview#sec8962-sub5>).

Tras el análisis de las diferentes topologías, se ha concluido que todas ellas cumplen con los objetivos y requisitos necesarios para la implementación del Plan de Recuperación antes Desastres (DRP). Cada una de las topologías mencionadas ofrece flexibilidad y capacidad de adaptación a diversos tipos de infraestructura, lo que permite responder a múltiples escenarios de contingencia que pueden presentarse en las entidades financieras. No obstante, para el presente proyecto se ha decidido optar por la implementación de la topología activo-pasivo. La elección se basa en su capacidad para proporcionar una clara separación entre el sitio de producción y el sitio de recuperación. En esta configuración, el sitio de producción está completamente operativo, mientras que el sitio de recuperación permanece inactivo hasta que se produce un evento de desastre, permitirá optimizar los recursos del sitio de recuperación, que solo se activarán cuando sea necesario, reduciendo así los costos operativos mientras se garantiza la disponibilidad de los sistemas críticos en caso de una interrupción. Por estas razones, se considera que esta es la solución más adecuada para el contexto específico del proyecto.

4.3 Implementación

4.3.1 Pre-Requisitos para la instalación

Antes de proceder con la instalación de Site Recovery Manager (SRM), es esencial cumplir con una serie de tareas previas y verificar que se dispone de la información necesaria

para garantizar una implementación exitosa. Estos prerrequisitos aseguran la compatibilidad, la estabilidad y el correcto funcionamiento del sistema, minimizando los riesgos de errores durante el proceso.

En primer lugar, debemos contar previamente con la versión adecuada en ejecución de vCenter Server en ambos sitios, tanto en el primario como en el sitio de recuperación, en el contexto de este proyecto, se da por hecho que la infraestructura de virtualización ya se encuentra operativa en ambos sitios; por lo tanto, no se contempla dentro del alcance del proyecto la instalación de un nuevo vCenter Server. Luego debemos consultar la matriz de compatibilidad ofrecida por VMware para asegurar que las versiones de vCenter Server y SRM sean compatibles, lo que evitará problemas de integración durante y después de la instalación (VMware, 2023a). Esta verificación es crítica para asegurar que ambos sistemas funcionen de manera conjunta y eficiente.

Es recomendable verificar que, tanto en el sitio primario como en el sitio secundario, el vCenter Server haya sido instalado utilizando nombres de dominio (FQDN) en lugar de direcciones IP. Esto facilita la gestión y permite mayor flexibilidad en la infraestructura, ya que por ejemplo el uso de DHCP no requerirá reconfiguraciones adicionales. Además, si se emplean certificados personalizados, el uso de FQDN es obligatorio, ya que la mayoría de las entidades certificadoras no aceptan certificados que utilicen direcciones IP en los valores SAN y CN (VMware, 2023a).

Otra tarea importante es la sincronización de los relojes de los sistemas en los que se ejecutan tanto vCenter como Site Recovery Manager. Para evitar conflictos en la gestión del tiempo, se debe utilizar un agente de sincronización persistente, como el protocolo de tiempo de red (NTPD) o las herramientas de sincronización de VMware. En caso de que se ejecuten en máquinas virtuales, es necesario configurar la sincronización del tiempo NTP en el host ESXi correspondiente. Esto asegura que los sistemas mantengan una referencia temporal coherente y eviten discrepancias que pueden afectar el rendimiento o generar errores (VMware, 2023a).

Además, será necesario obtener las credenciales de Administrador de vCenter para ambos sitios, lo que permitirá realizar las configuraciones necesarias de forma segura. Si se utilizan certificados personalizados, también se deberá contar con los archivos

correspondientes, siguiendo las recomendaciones de VMware para el uso de certificados SSL/TLS con SRM (VMware, 2023a).

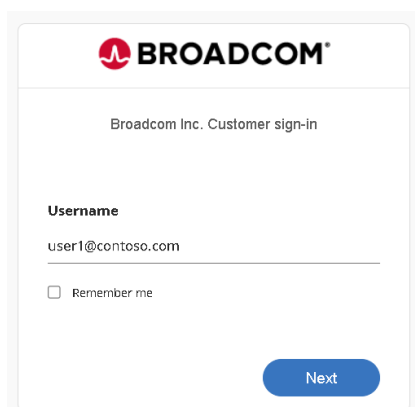
4.3.2 Instalación de Site Recovery Manager Virtual Appliance

La instalación de Site Recovery Manager se llevará a cabo mediante el despliegue de una plantilla OVF, el cual será descargado desde la página de soporte de Broadcom. Este procedimiento asegura que se utilice la versión correcta de Software para el entorno de virtualización. A continuación, se describen los pasos necesarios para realizar la descarga e instalación.

En primer lugar, se debe acceder al portal de soporte de Broadcom a través de la URL: <https://support.broadcom.com/web/ecx/home>. Al acceder al sitio, se debe iniciar sesión con una cuenta válida como se muestra en la figura 19. La creación de una cuenta puede ser necesaria si el usuario no cuenta con una previamente, ya que el acceso a los recursos de soporte técnico requiere autenticación.

Figura 19

Acceso Portal Broadcom

The image shows a web form for Broadcom customer sign-in. At the top is the Broadcom logo. Below it, the text "Broadcom Inc. Customer sign-in" is centered. The form has a "Username" label followed by a text input field containing "user1@contoso.com". Below the input field is a checkbox labeled "Remember me". At the bottom right of the form is a blue button labeled "Next".

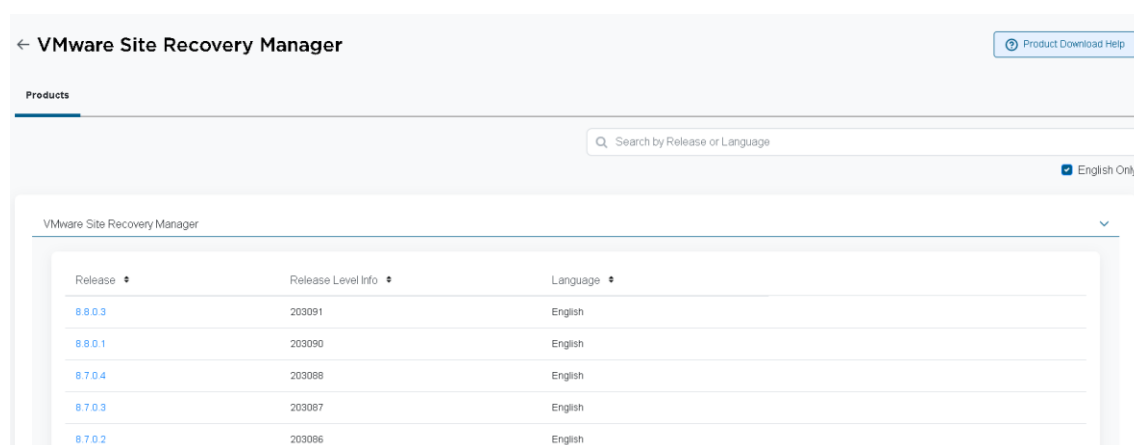
Nota: Imagen de elaboración propia. Portal de acceso al soporte de Broadcom.

Una vez dentro del portal, el siguiente paso consiste en navegar hacia la sección de productos. Esta sección puede variar del diseño actual del sitio, en la barra de búsqueda, se

debe ingresar “Site Recovery Manager” o “SRM”, al realizar clic sobre el enlace que lleva a la sección de SRM, se abrirá una página dedicada que proporciona diversas opciones de soporte, como se describe en la Figura 20.

Figura 20

Versiones de SRM



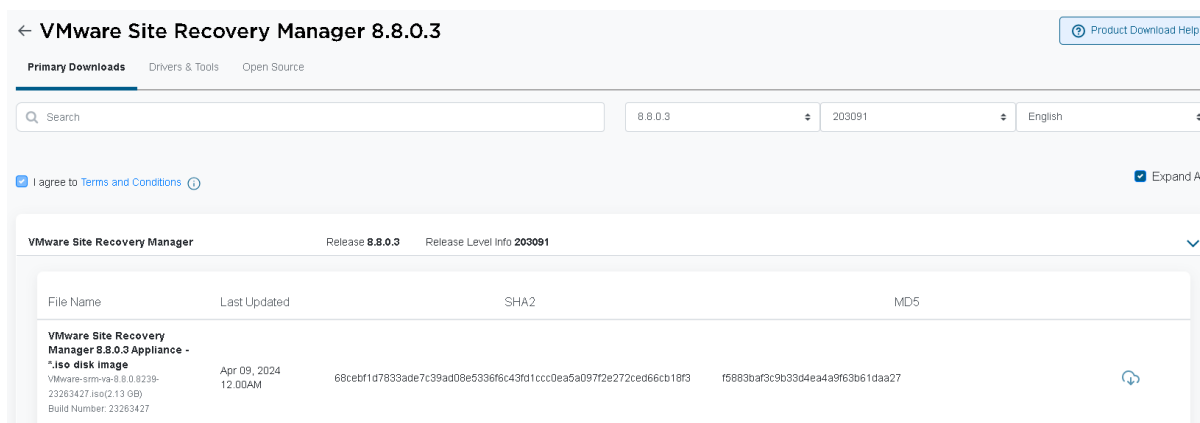
Release	Release Level Info	Language
8.8.0.3	203091	English
8.8.0.1	203090	English
8.7.0.4	203088	English
8.7.0.3	203087	English
8.7.0.2	203086	English

Nota: Imagen de elaboración propia. Versiones disponibles para la descargar de SRM.

Luego de seleccionar la última versión disponible, aceptar los términos y condiciones abriremos el enlace de descarga del archivo, cómo se observa en la siguiente Figura 21.

Figura 21

Descarga SRM Appliance



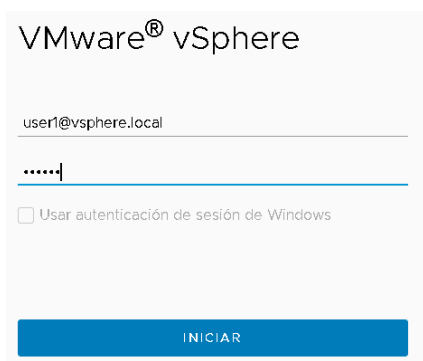
Nota: Imagen de elaboración propia. Descarga del archivo en formato ISO.

Una vez completada la descarga, en caso de ser necesario copiar el archivo ISO a una terminal desde donde realizaremos la implementación de SRM, dicha terminal debe contar con acceso a la red interna de la infraestructura de virtualización del sitio primario y conexión con el vCenter Server. Finalmente extraer los archivos desde el ISO, los archivos que se deberían obtener son: srm-va_OVF10.ovf, srm-va-system. vmdk, srm-va-support. vmdk, srm-va_OVF10.cert y srm-va_OVF10.mf.

Los siguientes pasos que se indicarán a continuación son publicados por VMware (2024b) en su portal de documentación de producto. En el vSphere Client del sitio primario, se deberá iniciar sesión con las credenciales administrativas del vCenter Server y navegar hasta el inventario de máquinas virtuales, como se detalla en el Figura 22.

Figura 22

Acceso vCenter

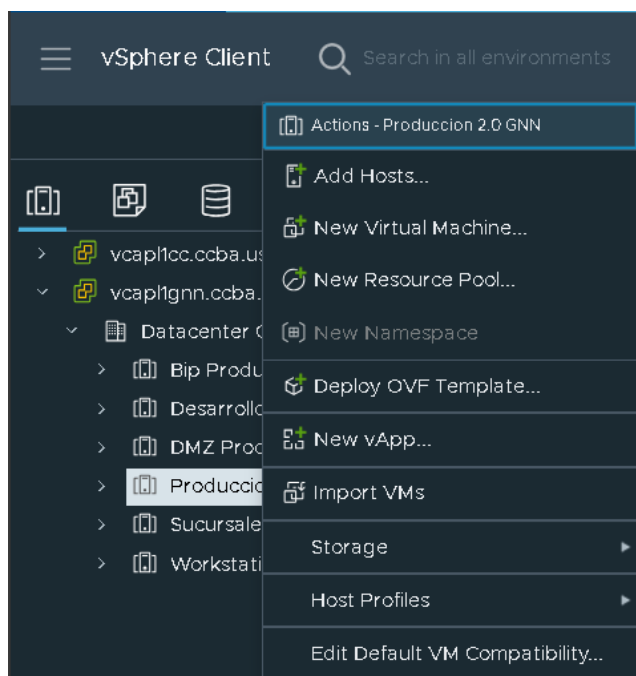


Nota: Imagen de elaboración propia. Acceso a vCenter Server.

Debemos seleccionar el clúster donde se realizará la implementación del Virtual Appliance, paquete de software preconfigurado que se ejecuta dentro de un entorno de virtualización, en esta implementación utilizaremos el clúster “Producción 2.0 GNN”. En la Figura 23, se observa la opción “Deploy OVF Template” que debemos utilizar.

Figura 23

Deploy OVF Template



Nota: Imagen de elaboración propia. Selección del clúster y despliegue del archivo OVF.

Debemos seleccionar la opción “Local File” y en el botón “Upload Files”, seleccionaremos desde el repositorio donde realizamos previamente la extracción de los archivos `srm-va_OVF10.ovf`, `srm-va-system.vmdk`, `srm-va-support.vmdk`, `srm-va_OVF10.cert` y `srm-va_OVF10.mf`. (VMware, 2024b).

Asignar un nombre a la máquina virtual de SRM, para este proyecto utilizamos el nombre: “MG-VCSRMGNN”, recomendamos utilizar nomenclaturas de fácil identificación para los administradores que gestionaran la herramienta además de cumplir con los estándares

de la entidad donde se realizará la implementación, en “Location” debemos elegir la carpeta donde se ubicará el virtual appliance. El siguiente paso será elegir el recurso de cómputo, como mencionamos anteriormente lo haremos sobre el clúster “Producción 2.0 GNN” y si queremos ser más específicos además podemos seleccionar el host ESXi, revisaremos los detalles de la implementación y daremos clic en siguiente, debemos aceptar los términos y condiciones. (VMware, 2024b).

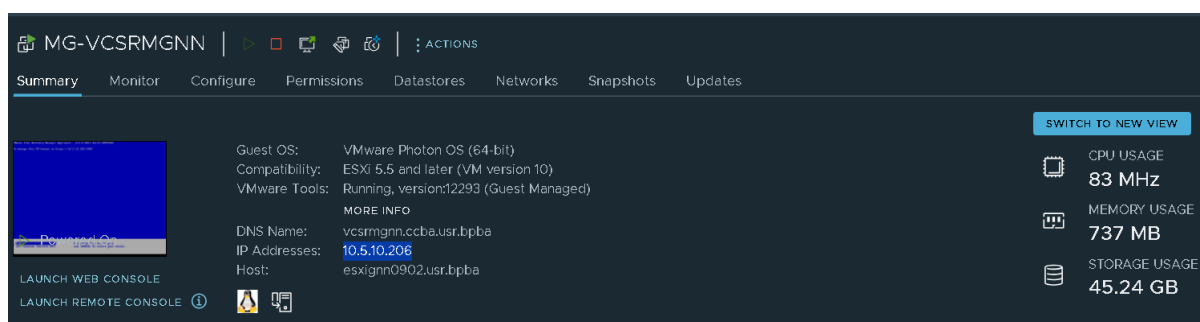
Continuando con el despliegue, será el turno de la configuración de recursos, debemos seleccionar la cantidad de vCPU para el dispositivo virtual, para el presente proyecto trabajaremos con 2 vCPU; luego seleccionaremos el almacén de datos y el formato del disco destino, que será “Thin Provision” y por último la configuración de red, donde debemos indicar la red destino donde colaremos el Appliance, utilizaremos IP Estática-Manual con protocolo IPv4 (VMware, 2024b).

Tendremos opciones adicionales para configurar nuestra máquina virtual, desde habilitar SSHD, definir la password inicial de root, la password inicial del usuario administrador, la password inicial de la base de datos, servidor NTP, IP, Hostname, DNS y Gateway. Al terminar de configurar estos ítems daremos clic en Finalizar y comenzará a realizarse el despliegue del appliance, al finalizar obtendremos la máquina virtual instalada y procederemos a encenderla (VMware, 2024b).

En la Figura 24 podemos observar en ejecución el virtual appliance sobre el clúster “Producción 2.0 GNN” seleccionado para nuestro ambiente.

Figura 24

Virtual Appliance



Nota: Imagen de elaboración propia. Virtual Appliance de SRM en ejecución.

Para acceder a la administración de SRM, el primer paso es abrir un navegador Web y acceder a la interfaz de administración del dispositivo utilizando la dirección IP o el nombre de dominio completo (FQDN) del appliance, en el siguiente formato: `https://dirección-IP-o-FQDN-del-dispositivo:5480`. Una vez allí, como se observa en la Figura 25, el administrador deberá hacer clic en la opción “Iniciar Site Recovery Manager Appliance Management”, colocando las credenciales previamente definidas en anterior paso (VMware, 2023d).

Figura 25

Log-in SRM Appliance



Nota: Imagen de elaboración propia. Pantalla de acceso a SRM Appliance Management.

Una vez accedido a la interfaz de administración del appliance, el siguiente paso es configurar los parámetros necesarios para su correcto funcionamiento. Tras iniciar sesión como administrador, se debe hacer clic en la pestaña “Resumen” y luego en “Configurar Dispositivo” (VMware, 2023e).

En la página correspondiente a la configuración del Platform Services Controller (PSC), se requiere ingresar la información del sitio donde se ha implementado el Site Recovery Manager Virtual Appliance. Para ello en el campo de nombre del host del PSC, se debe escribir el nombre del host o la dirección IP en minúsculas del vCenter Server que se utilizará para registrar SRM. A continuación, se debe confirmar el puerto del PSC, que por defecto es 443, o

bien, introducir uno nuevo si el vCenter Server utiliza un puerto diferente, tal como se aprecia en la Figura 26. Es importante señalar que vCenter solo admite conexiones HTTPS (VMware, 2023e).

Figura 26

Configuración PSC

Configurar Site Recovery Manager

1 Platform Services Controller

2 vCenter Server

3 Nombre y extensión

4 Listo para completar

Platform Services Controller

Todos los campos son obligatorios a menos que estén marcados (opcional)

Introduzca la información de Platform Services Controller de la instancia de vCenter Server para la que desea configurar Site Recovery Manager.

Nombre del host de PSC vcap1gmn.ccba.usr.bpba

Puerto de PSC 443

Nombre de usuario administrator@vsphere.local

Contraseña

Nota: Si se lo pide el programa de configuración, deberá aceptar el certificado para que la configuración continúe.

CANCELAR SIGUIENTE

Nota: Imagen de elaboración propia. Configuración de la conexión Platform Services Controller.

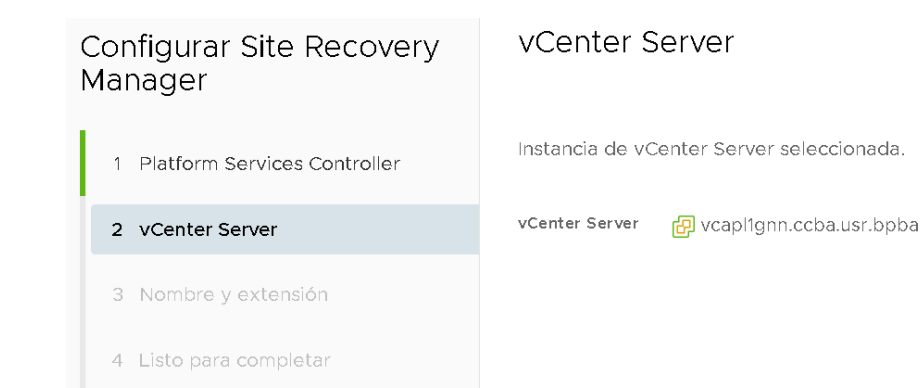
El siguiente paso es ingresar el nombre de usuario y contraseña correspondientes al administrador del vCenter Single Sign-On (SSO). Esta cuenta debe ser parte del grupo de administradores del vCenter SSO de la instancia de vCenter Server. Luego de ingresar esta información, se debe hacer clic en “Conectar” para verificar el certificado de vCenter Server y continuar con la configuración (VMware, 2023e).

En la página de vCenter Server, se debe seleccionar la instancia de vCenter Server que se usará para registrar el Site Recovery Manager Appliance. Es crucial seleccionar la instancia correcta, especialmente en entornos con “Enhanced Linked Mode”, donde pueden aparecer múltiples instancias registradas. Después de esto, en la página “Nombre” y “Extensión”, se introduce la información requerida para registrar SRM con vCenter Server, esto incluye el

nombre del sitio, la dirección de correo electrónico del administrador y el nombre o dirección IP del host local, como se ejemplifica en la Figura 27 (VMware, 2023e).

Figura 27

Instancia vCenter Server



Nota: Imagen de elaboración propia. Selección de la instancia de vCenter Server.

Figura 28

Nombre y Extensión



Nota: Imagen de elaboración propia. Configuración de Nombre y Extensión de SRM.

Una vez finalizada la conexión, se deberá obtener una imagen como la Figura 29:

Figura 29*Conexión SRM/vCenter*

Nombre del sitio	SITE SRM GNN
Clave de extensión	com.vmware.vcDr
Platform Services Controller	https://vcap1gnn.ccba.usr.bpba:443
vCenter Server	vcap1gnn.ccba.usr.bpba
Huella digital de conexión	 A2:A7:22:65:4C:CE:13:AB:7C:DE:38:4F:32:FE:38:7E:26:D8:34:21:CD:22:4E:DC:5C:50:C9:53:91:BD:8F:ED

Nota: Imagen de elaboración propia. Conectividad SRM con la instancia de vCenter Server.

4.3.3 Configuración de pares de Sitios y Protección

En primer lugar, es necesario asegurarse de que las instancias de Site Recovery Manager Server estén correctamente instaladas tanto en el sitio de recuperación como en el sitio protegido, ya que esto garantiza que ambas ubicaciones puedan interactuar y gestionar el proceso de recuperación ante desastres. Una vez confirmada la instalación, se procede con el emparejamiento de los sitios a través del cliente de Vsphere, para ello debemos hacer clic en la opción “Site Recovery” y luego en “Abrir Site Recovery”. Desde allí se selecciona la opción para crear un “Nuevo Par de Sitios”, este proceso requiere elegir un vCenter Server local de la lista y seleccionar el tipo de par, lo que dependerá de si el emparejamiento se realiza entre instancias de vCenter Server ubicadas en el mismo dominio de SSO o en dominios diferentes (VMware, 2023b).

Una vez determinado el tipo de emparejamiento, se debe proporcionar la dirección del vCenter Server correspondiente al Site Recovery Manager Server en el segundo sitio. Aquí, es crucial ingresar el nombre de usuario y la contraseña correctos para iniciar sesión y luego hacer clic en “Buscar instancias de vCenter Server”. Este importante recordar que la dirección proporcionada debe coincidir exactamente con la dirección que se utilizó durante la instalación del Site Recovery Manager Server en el sitio de recuperación, esto asegura una correcta

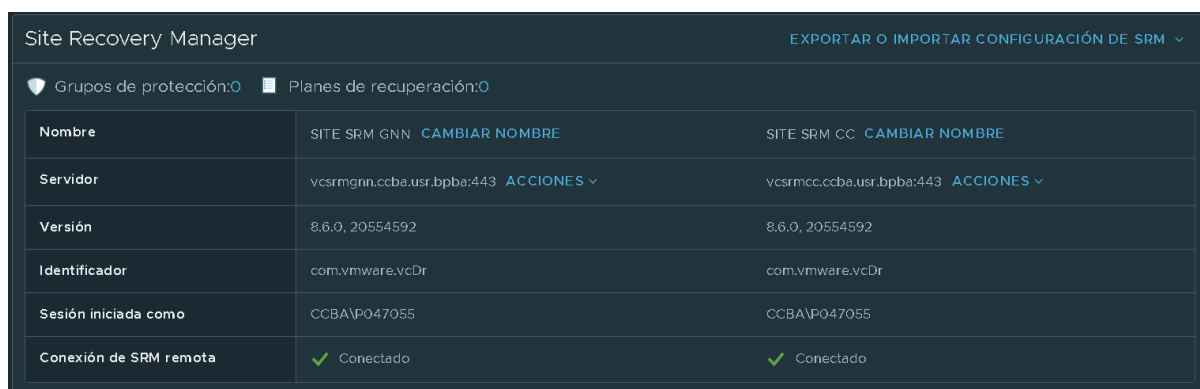
comunicación entre ambos sitios, y para facilitar futuras modificaciones de la infraestructura, es recomendable utilizar el FQDN en lugar de una dirección IP estática (VMware, 2023b).

A continuación, se selecciona la instancia de vCenter y los servicios que se desean emparejar y se hace clic en “Siguiente”. En la página “Listo para completar”, se revisa la configuración seleccionada para asegurar que todos los parámetros sean los correctos y, finalmente, se hace clic en “Finalizar”. Este proceso establece la conexión entre el sitio protegido y el de recuperación, y el par aparecerá en la sección “Pares de Sitios” dentro de la pestaña “Inicio de Site Recovery” (VMware, 2023b).

Este procedimiento es clave para garantizar que ambos sitios estén sincronizados y puedan gestionar de manera efectiva el proceso de recuperación ante desastres, cumpliendo con los objetivos del DRP diseñado. A partir de la Figura 30 podemos observar en nuestro ambiente como deben quedar configurados los “Pares de Sitios”.

Figura 30

Par de Sitios



Site Recovery Manager		EXPORTAR O IMPORTAR CONFIGURACIÓN DE SRM ▾
🛡️ Grupos de protección:0 📄 Planes de recuperación:0		
Nombre	SITE SRM GNN CAMBIAR NOMBRE	SITE SRM CC CAMBIAR NOMBRE
Servidor	vcsrmgrrn.ccbba.usr.bpba:443 ACCIONES ▾	vcsrmcc.ccbba.usr.bpba:443 ACCIONES ▾
Versión	8.6.0, 20554592	8.6.0, 20554592
Identificador	com.vmware.vcDr	com.vmware.vcDr
Sesión iniciada como	CCBA\PO47055	CCBA\PO47055
Conexión de SRM remota	✓ Conectado	✓ Conectado

Nota: Imagen de elaboración propia. Estado de conectividad entre pares de sitios.

4.3.4 Configuración de Replicación Basada en Matrices (Based Array)

Continuando con la configuración, dentro de la interfaz de administración de Site Recovery Manager, debemos hacer clic en “Storage Replication Adapters”, y seleccionar la opción “New Adapter”. Esto permite iniciar el proceso de instalación de un nuevo adaptador de replicación de almacenamiento. A continuación, es necesario hacer clic en “Upload” y navegar hasta el directorio donde se guardó previamente el archivo de “Storage Replication Adapter (SRA)” descargado, debemos seleccionar el archivo y aguardar por la finalización del proceso de carga (VMware, 2022). De acuerdo con la Figura 31, deberíamos obtener una tarjeta de “Storage Replication Adapter” dentro de la interfaz de administración de SRM.

Figura 31

Adaptador de replicación de almacenamiento

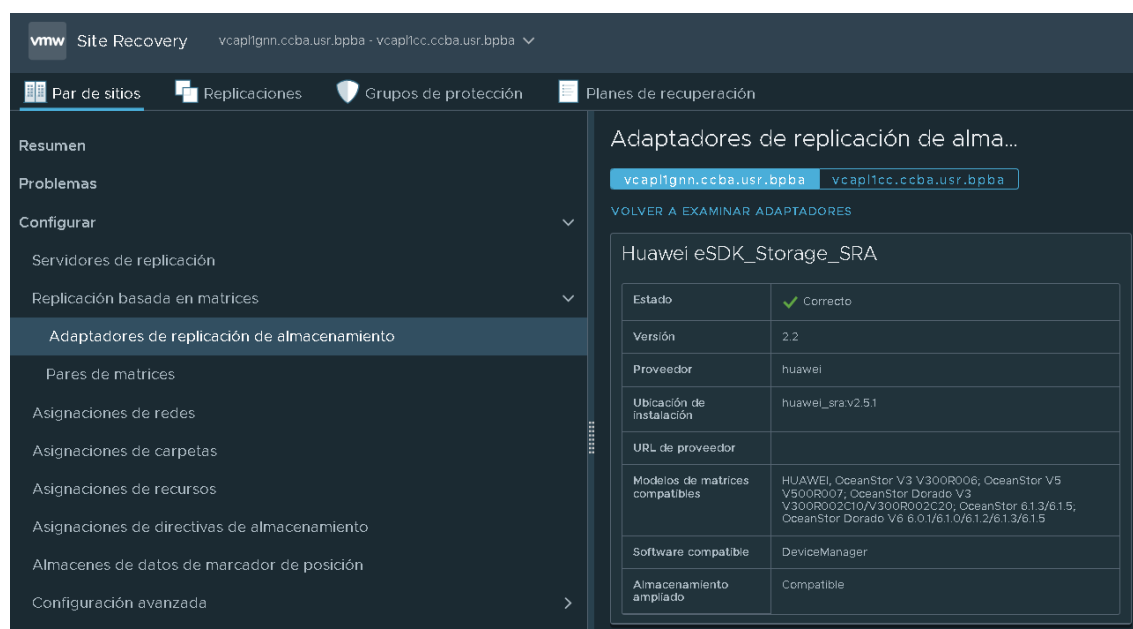


Nota: Imagen de elaboración propia. Configuración de adaptadores de almacenamiento.

Posteriormente, es necesario acceder al “vSphere Client” para finalizar la configuración. Dentro de “vSphere Client”, se debe hacer clic en “Site Recovery” y luego en “Open Site Recovery”. Allí, se selecciona el par de sitios configurados y se hace clic en “View Details” para revisar la información del emparejamiento de sitios, luego en la pestaña de “Site Pair, se debe navegar a “Configure” y a “Array Based Replication”, donde se encuentra la opción de “Storage Replication Adapters”. Finalmente, se debe hacer clic en el botón “Rescan Adapters” para garantizar que los adaptadores de replicación de almacenamiento se detecten y configuren correctamente (VMware, 2022).

Figura 32

SRA



Nota: Imagen de elaboración propia. Verificación de la instalación del SRA desde la consola de Site Recovery.

Después de emparejar el sitio protegido con el sitio de recuperación, el siguiente paso consiste en configurar los “Array Managers” correspondientes en cada sitio. Esto es esencial para que “Site Recovery Manager (SRM)” pueda descubrir los dispositivos replicados, calcular los grupos de almacenes de datos, e iniciar las operaciones de almacenamiento necesarias. Para comenzar este proceso, se debe acceder al “Vsphere Client” y hacer clic en “Site Recovery”, seguido de la opción “Open Site Recovery”. En la pestaña de inicio de “Site Recovery”, se selecciona el par de sitios que se ha configurado previamente y se hace clic en “View Details” para ver los detalles específicos del emparejamiento (VMware, 2023f).

Una vez en la pestaña de “Site Pair”, se debe hacer clic en “Configure”, seguido de “Array Based Replication” y luego en “Array Pairs”. Aquí se encuentra la opción “Add”, que permite agregar un nuevo “Array Manager”. El siguiente paso es seleccionar el adaptador de replicación de almacenamiento (Storage Replication Adapter o SRA) que se desea utilizar con “Site Recovery Manager”, y luego hacer clic en “Next” para continuar. Se debe introducir un nombre para el “Array Manager” local y proporcionar la información requerida según el tipo

de SRA seleccionado. Es importante utilizar un nombre descriptivo que permita identificar fácilmente el almacenamiento asociado a este “Array Manager”, la información requerida puede variar según el proveedor del SRA, pero generalmente incluye campos como la dirección IP, la información del protocolo, el mapeo entre los nombres de los arrays y las direcciones IP, además de las credenciales de usuario (nombre de usuario y contraseña). Para obtener detalles más específicos sobre cómo completar los campos, es recomendable consultar la documentación proporcionada por el proveedor del SRA correspondiente (VMware, 2023f).

Para este proyecto estaremos trabajando con los datos proporcionados por Huawei, en la siguiente Figura 33 se observa la configuración ya finalizada.

Figura 33

Array Manager

The screenshot shows the 'Pares de matrices' (Matrix Pairs) configuration window. It includes a table for matrix pairs and a section for detected devices.

Par de matrices	Par de administradores de matrices	Ultimo ping del administrador de matrices
Dorado18000.GNN ↔ Dorado1... Adaptador de replicación de almacenamiento: Huawei eSDK_Storage_SRA	Dorado_GNN ↔ Dorado_CC Dorado_GNN Versión de SR 2.2	Correcto, 15/10/24, 11:41:16 -0300 Dorado_CC Versión de S 2.2

EXPORTAR

1 elemento

DETECTAR DISPOSITIVOS

Dispositivo (vcapi1ggn.ccba.usr.bpba)	Almacén de datos	Estado	Dispositivo (vcapi1cc.ccba.usr.bpba)	Grupo de protecc
R1_10TB10000	Local: [doradogNN091-transf]	→ Hacia adelante	R2_10TB10000	
R1_10TB10001	Local: [doradogNN092-transf]	→ Hacia adelante	R2_10TB10001	
R1_10TB10002	Local: [doradogNN093-transf]	→ Hacia adelante	R2_10TB10002	
R1_10TB10004	Local: [doradogNN190-20]	→ Hacia adelante	R2_10TB10004	
R1_10TB10006	Local: [doradogNN197-20]	→ Hacia adelante	R2_10TB10006	
R1_10TB10040	Local: [doradogNN232-20]	→ Hacia adelante	R2_10TB10040	

EXPORTAR

627 elementos

Nota: Imagen de elaboración propia. Configuración de Array Manager.

4.3.5 Mapeo de Recursos

Los mapeos en “Site Recovery Manager” permiten especificar cómo se asignan los recursos de las máquinas virtuales en el sitio protegido a los recursos correspondientes en el sitio de recuperación. Esto es fundamental para garantizar que, durante la recuperación, las

máquinas virtuales utilicen los recursos adecuados en el sitio de recuperación, lo que asegura la continuidad operativa. Estos mapeos pueden abarcar varios elementos del inventario de vCenter Server, como redes, centros de datos, carpetas de máquinas virtuales (VMware, 2023g).

Es posible configurar mapeos a nivel de sitio, lo que permite que los objetos en el inventario de vCenter Server en el sitio protegido se asignen a objetos correspondientes en el inventario del sitio de recuperación. Entre los elementos que pueden mapearse se encuentran las redes, con la opción de especificar una red diferente para las pruebas de planes de recuperación, los centros de datos o carpetas de máquinas virtuales, y los recursos computacionales, como “resource pools”, hosts independientes, “vApps” o clústeres. Durante una recuperación, las máquinas virtuales que se inicien en el sitio de recuperación utilizarán los recursos que se especificaron en los mapeos, para habilitar la protección bidireccional y las operaciones de re-protección, se pueden configurar mapeos inversos, que asignan los objetos del sitio de recuperación a sus correspondientes en el sitio protegido. También es posible configurar mapeos en la dirección opuesta, para que las máquinas virtuales recuperadas en un sitio utilicen recursos diferentes a los que tenían en su estado protegido (VMware, 2023g).

En la pestaña de “Site Pair”, se expande el menú “Configure” y se selecciona el tipo de recurso que se desea configurar. Existen tres tipos principales de mapeos que se pueden crear:

Network Mappings: permite mapear redes en el sitio protegido a redes en el sitio de recuperación, como se puede observar en la Figura 34.

Figura 34

Mapeo de Redes



Nota: Imagen de elaboración propia. Configuración de mapeo de redes entre el sitio protegido y el sitio de recuperación.

Folder Mappings: permite mapear centros de datos o carpetas de máquinas virtuales entre el sitio protegido y el sitio de recuperación, se detalla en la Figura 35.

Figura 35

Mapeo de Carpetas



Nota: Imagen de elaboración propia. Configuración de mapeo de carpetas de máquinas virtuales entre el sitio protegido y el sitio de recuperación.

Resource Mappings: La Figura 36 describe como mapear resource pools, hosts independientes, vApps o clústeres entre los dos sitios.

Figura 36

Mapeo de Recursos



Nota: Imagen de elaboración propia. Configuración de mapeo de recursos de máquinas virtuales entre el sitio protegido y el sitio de recuperación.

Para crear un nuevo mapeo, se debe hacer clic en New y seleccionar si el mapeo se realizará de forma automática o manual. El mapeo automático solo está disponible para redes y carpetas, mientras que los mapeos de recursos deben configurarse manualmente. El mapeo automático asigna redes y carpetas en el sitio protegido a redes y carpetas con el mismo nombre en el sitio de recuperación. En el caso del mapeo manual, se seleccionan elementos específicos en el sitio protegido y se asignan a los objetos correspondientes en el sitio de recuperación (VMware, 2023g).

4.3.6 Configuración Datastore Placeholder

La configuración de un datastore placeholder (datastore de reservación) en ambos sitios de la infraestructura permite que el SRM almacene temporalmente las configuraciones y metadatos de las máquinas virtuales protegidas sin realizar una replicación completa de los datos. Esto es necesario para que el sistema pueda restaurar rápidamente las operaciones en el sitio de recuperación en caso de que ocurra un desastre en el sitio primario. Es importante que el datastore esté visible para todos los hosts del clúster en el que opera para garantizar que los datos estén disponibles en caso de activación del DRP (VMware, 2023h).

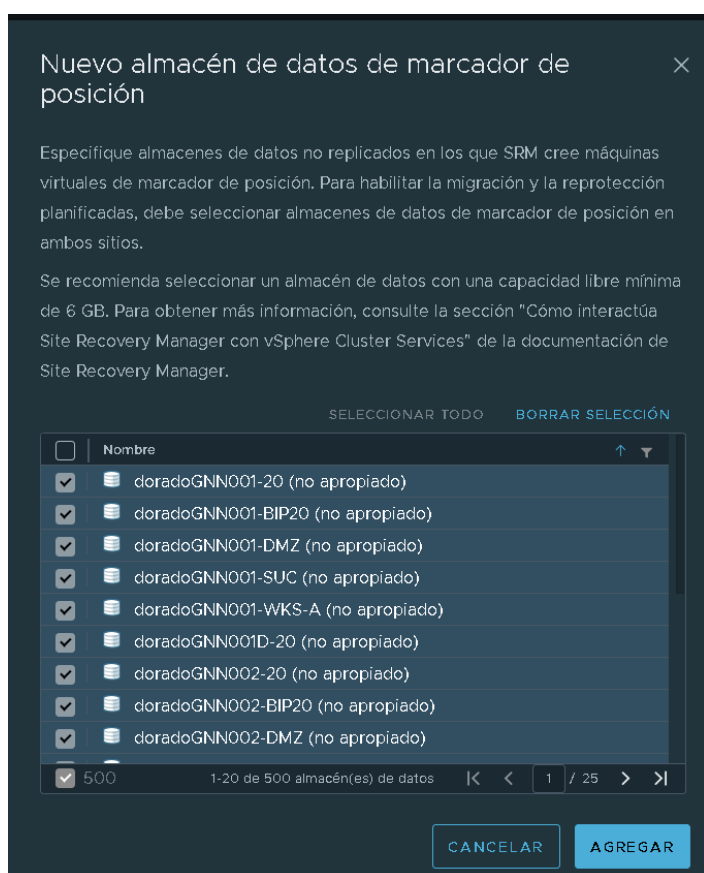
Durante el proceso de configuración, es esencial evitar la selección de datastores replicados a través de replicación basada en arreglos (Array-Based Replication), que no están gestionados directamente por SRM, ya que esto podría causar conflictos en la gestión de datos. SRM requiere un array manager adecuado que supervise los datastores replicados, de modo que la replicación sea controlada y administrada dentro de los estándares del sistema (VMware, 2023h).

Para configurar los placeholder datastores en el entorno de SRM, primero se debe acceder al cliente Vsphere y dirigirse a la sección de Site Recovery, desde donde se abre la configuración de SRM. En la pestaña principal de Site Recovery, se selecciona el par de sitios y se hace clic en View Details. Dentro de la pestaña Site Pair, se selecciona la opción Configure, seguida de Placeholder Datastores. A continuación, para cada sitio, se elige un datastore

específico que funcionará como la ubicación para las máquinas virtuales de reservación y, finalmente, se confirma la selección haciendo clic en OK. Este proceso debe repetirse para cada sitio en la infraestructura para completar la configuración bidireccional. La selección de los datastores de reservación debe estar alineada con los requisitos de cada entorno, garantizando así la efectividad del DRP en situaciones de contingencia y la continuidad operativa, la Figura 37 ilustra la selección de los Datastores Placeholder (VMware, 2023h).

Figura 37

Selección Datastore Placeholder



Nota: Imagen de elaboración propia. Configuración de los datastores placeholder.

4.3.7 Creación de Grupos de Protección

Antes de crear un grupo de protección en SRM, se debe verificar que las máquinas virtuales estén almacenadas en datastores configurados para la replicación basada en arrays. Además, si en la sección de mapeos de recursos del par de arrays se emplean resource pools, es necesario configurar un mapeo adicional que provenga del clúster principal (VMware, 2023i).

Para crear un grupo de protección en Site Recovery Manager (SRM), primero es necesario acceder a la configuración de SRM desde el cliente de Vsphere, ingresando a la sección de Site Recovery. En la pestaña principal de Site Recovery, se debe seleccionar el par de sitios correspondiente y hacer clic en View Details. Una vez dentro, en la pestaña Protection Groups, se elige la opción New Protection Group para crear un nuevo grupo de protección. En la página denominada Name and Direction, se ingresan un nombre y una descripción para el grupo de protección, se selecciona la dirección de protección y se continúa haciendo clic en Next. En la página de Type, se eligen los Datastore groups (array-based replication), se selecciona el par de arrays adecuado y nuevamente se avanza haciendo clic en Next. A continuación, se seleccionan los grupos de datastores que se integrarán al grupo de protección; al hacer esto, las máquinas virtuales incluidas en dichos grupos se visualizarán en la tabla de máquinas virtuales. En la página de Recovery plan, se ofrece la posibilidad de añadir el grupo de protección a un plan de recuperación específico. Finalmente, se revisa toda la configuración y se concluye el proceso haciendo clic en Finish (VMware, 2023i).

Una vez que el grupo de protección ha sido creado, su progreso puede ser monitorizado en la pestaña Protection Group. SRM comprobará la correcta aplicación de los mapeos de inventario a las máquinas virtuales protegidas. En caso de que SRM haya aplicado los mapeos exitosamente, el estado de protección del grupo se mostrará como OK, como se expone en la Figura 38 (VMware, 2023i).

Figura 38

Grupo de Protección



Nota: Imagen de elaboración propia. Creación del grupo de protección para máquinas virtuales.

4.3.8 Creación de Planes de Recuperación

Para crear un plan de recuperación en Site Recovery Manager (SRM), primero es necesario definir cómo SRM recuperará las máquinas virtuales en caso de una interrupción. El procedimiento se inicia en el cliente de Vsphere, accediendo a Site Recovery y seleccionando Open Site Recovery. En la pantalla principal de Site Recovery, se selecciona el par de sitios deseado y, posteriormente, se hace clic en View Details. En la pestaña Recovery Plan, se selecciona New Recovery Plan para crear un nuevo plan de recuperación (VMware, 2023j).

Es fundamental asignar un nombre, una descripción y la dirección del plan, así como seleccionar una carpeta específica para el almacenamiento. Cabe señalar que el nombre del plan debe diferir del nombre de la carpeta seleccionada. A continuación, se eligen uno o varios grupos de protección que el plan debe recuperar, y se hace clic en Next para continuar. En la página correspondiente a Test Network, se debe hacer clic en Change para seleccionar una red que será utilizada durante la prueba de recuperación, tras lo cual se avanza nuevamente con Next. En ausencia de mapeos a nivel de sitio, SRM ofrece la opción predeterminada Use site-level mapping, la cual crea una red de prueba aislada. Finalmente, se revisa la información resumen y se confirma la creación del plan de recuperación haciendo clic en Finish, puede verse en la Figura 39 como ha quedado conformado el plan de recuperación (VMware, 2023j).

Figura 39

Plan de Recuperación

Name	Status	Protected Site	Recovery Site
Test-RecoveryPlan01	Ready	SITE SRM GNN	SITE SRM DC

Nota: Imagen de elaboración propia. Asignación del plan de recuperación al grupo de protección.

4.3.9 Prueba del Plan de Recuperación

Para realizar una prueba de un plan de recuperación, Site Recovery Manager (SRM) ejecuta las máquinas virtuales del plan de recuperación en una red de prueba y en un snapshot temporal de los datos replicados en el sitio de recuperación, sin interrumpir las operaciones en el sitio protegido. Durante la prueba, SRM realiza todos los pasos del plan, excepto apagar las máquinas virtuales en el sitio protegido y forzar que los dispositivos en el sitio de recuperación asuman el control de los datos replicados. Si el plan requiere suspender las máquinas virtuales locales en el sitio de recuperación, SRM efectúa esta acción mientras se realiza la prueba. Este proceso de prueba no afecta de manera alguna el entorno de producción en ninguno de los sitios (VMware, 2020).

La ejecución de la prueba genera un snapshot en el sitio de recuperación de todos los archivos de disco de las máquinas virtuales incluidas en el plan. Este proceso puede aumentar la latencia de entrada y salida (I/O) en el almacenamiento. En caso de observar tiempos de respuesta más lentos durante la prueba y utilizar VMware Virtual SAN, es recomendable monitorear la latencia de I/O mediante la herramienta de monitoreo de la interfaz de Virtual SAN. Para realizar la prueba en el cliente de Vsphere, es necesario hacer clic en Site Recovery > Open Site Recovery, seleccionar el par de sitios en la pestaña de inicio de Site Recovery, y luego hacer clic en View Details. Dentro de la pestaña “Recovery Plan”, el usuario debe hacer clic derecho sobre un plan de recuperación y seleccionar Test; también es posible iniciar la prueba seleccionando el ícono de prueba en la vista de pasos de recuperación del plan (VMware, 2020).

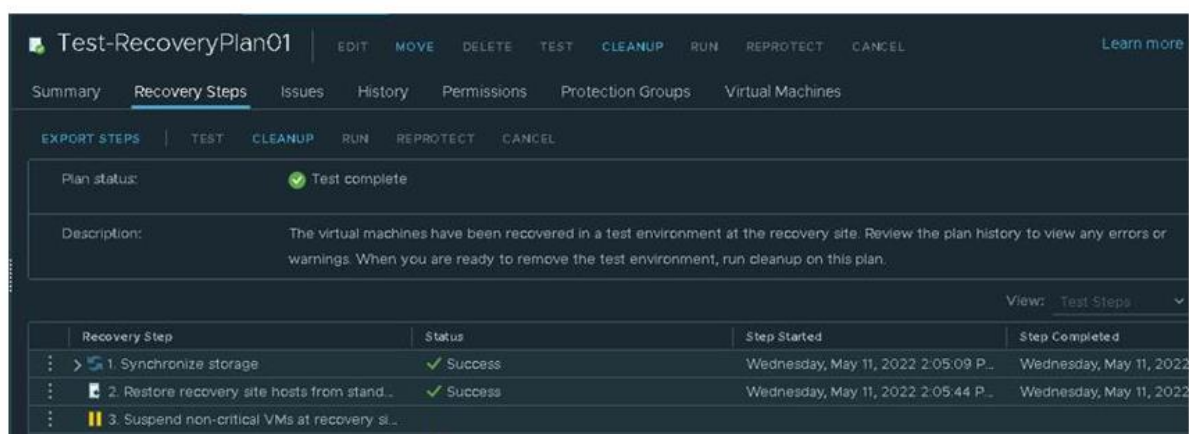
De manera opcional, se puede marcar la casilla “replicate recent changes to recovery site” para asegurar que el sitio de recuperación cuente con la versión más actualizada de las

máquinas virtuales protegidas, aunque esto puede extender el tiempo de sincronización. Después de revisar la información de la prueba, el proceso se finaliza haciendo clic en Finish. Durante la prueba, en la pestaña “Recovery Steps” del plan de recuperación, es posible monitorear el progreso de cada paso y responder a cualquier mensaje relevante. En la sección de tareas recientes, la tarea de prueba rastrea el progreso general del proceso (VMware, 2020).

En la Figura 40 se puede identificar los pasos ejecutados del plan de recuperación.

Figura 40

Test del Plan de Recuperación



Test-RecoveryPlan01				
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines				
EXPORT STEPS TEST CLEANUP RUN REPROTECT CANCEL				
Plan status:		✔ Test complete		
Description:		The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.		
View: Test Steps				
Recovery Step	Status	Step Started	Step Completed	
> 1. Synchronize storage	✔ Success	Wednesday, May 11, 2022 2:05:09 P..	Wednesday, May 11, 2022	
2. Restore recovery site hosts from stand...	✔ Success	Wednesday, May 11, 2022 2:05:44 P..	Wednesday, May 11, 2022	
3. Suspend non-critical VMs at recovery si...				

Nota: Imagen de elaboración propia. Ejecución del test del plan de recuperación, se pueden observar cada paso en la ejecución de las tareas.

4.3.10 Ejecución del Plan de Recuperación

Al ejecutar un plan de recuperación, Site Recovery Manager (SRM) migra todas las máquinas virtuales incluidas en dicho plan hacia el sitio de recuperación, tratando a su vez de apagar las máquinas virtuales correspondientes en el sitio protegido. Este proceso implica modificaciones significativas en las configuraciones tanto del sitio protegido como del sitio de recuperación, además de detener el proceso de replicación entre ambos. Por lo tanto, es fundamental no ejecutar un plan de recuperación que no se haya probado previamente, ya que

revertir estos cambios podría demandar un esfuerzo considerable y generar un tiempo prolongado de inactividad en los servicios críticos (VMware, 2019a).

Para usar la función de recuperación forzada, primero es necesario habilitar la configuración del parámetro “recovery. forceRecovery”. Además, es esencial que las asignaciones de inventario estén completamente configuradas. Si solo se han definido asignaciones temporales de inventario y se intenta realizar una migración planificada con la opción "Enable vMotion of eligible VMs", es posible que la migración falle, incluso si ambos sitios están operativos. Para evitar este tipo de fallos al usar la opción "Enable vMotion of eligible VMs", debe habilitarse vMotion en las máquinas virtuales implicadas (VMware, 2019a).

En el cliente de Vsphere, se accede a la ejecución de un plan de recuperación mediante el menú de Site Recovery. Primero, se selecciona la opción “Site Recovery > Open Site Recovery” y luego el par de sitios en la pestaña principal de Site Recovery, donde se hace clic en “View Details”. Una vez dentro de la pestaña “Recovery Plan”, se selecciona el plan de recuperación a ejecutar, y tras hacer clic derecho, se elige la opción “Run”. A continuación, se revisa la información en el mensaje de confirmación y se selecciona la casilla de verificación para confirmar que el usuario comprende que este proceso alterará de forma permanente las máquinas virtuales y la infraestructura de ambos centros de datos, tanto en el sitio protegido como en el de recuperación (VMware, 2019a).

En el contexto de recuperación, existen dos opciones para ejecutar el plan: la migración planificada y la recuperación ante desastres. La migración planificada permite recuperar las máquinas virtuales en el sitio de recuperación cuando ambos sitios están en operación. Sin embargo, si se producen errores en el sitio protegido durante la migración planificada, esta operación fallará. En caso de que el sistema de almacenamiento admita la función de almacenamiento extendido, puede habilitarse la opción "Enable vMotion of eligible VMs". Por otro lado, la recuperación ante desastres permite que las máquinas virtuales sean recuperadas en el sitio de recuperación si el sitio protegido sufre un problema. En este escenario, si se presentan errores en el sitio protegido, la recuperación continúa sin interrupción. Existe además una opción de recuperación forzada, denominada “Forced Recovery - recovery site operations only” que puede ser habilitada en casos de recuperación ante desastres (VMware, 2019a).

Una vez seleccionadas las opciones y revisada la configuración, se da clic en “Next” para revisar toda la información sobre el proceso de recuperación y luego en “Finish” para iniciar la ejecución del plan. El progreso de cada paso del plan de recuperación se puede monitorear en la pestaña “Recovery Steps” del plan de recuperación seleccionado. Esta visualización detallada permite realizar un seguimiento del avance de cada etapa del proceso (VMware, 2019a).

4.3.11 Re-protección de Sitios

En el proceso de re protección utilizando replicación basada en almacenamiento (array-based replication), Site Recovery Manager (SRM) revierte la dirección de la protección y luego forzar la sincronización del almacenamiento, de modo que los datos del nuevo sitio protegido se repliquen hacia el nuevo sitio de recuperación. Esta operación es fundamental para garantizar que el sitio de recuperación esté preparado para actuar de inmediato en caso de falla en el nuevo sitio protegido. Al iniciar el proceso de re protección, SRM instruye a los arreglos de almacenamiento subyacentes para que inviertan la dirección de la replicación. Tras esta reversión, SRM crea máquinas virtuales de marcador de posición (placeholder virtual machines) en el nuevo sitio de recuperación, que era originalmente el sitio protegido antes de la operación de re protección. La función de estas máquinas de marcador es preservar la estructura de inventario y configuración para permitir una futura recuperación sin necesidad de realizar una recreación completa (VMware, 2019b).

Al crear estas máquinas de marcador (placeholder) en el nuevo sitio protegido, SRM utiliza la ubicación de las máquinas virtuales protegidas originales para decidir el lugar adecuado en el que colocar las máquinas de marcador en el inventario. Además, SRM emplea la identidad de la máquina virtual protegida original como base para la creación del marcador. En los casos en que las máquinas virtuales protegidas originales ya no estén disponibles, SRM emplea las asignaciones de inventario (inventory mappings) del sitio de recuperación original al sitio protegido original para determinar los grupos de recursos y carpetas donde colocar los marcadores. Es indispensable configurar estas asignaciones de inventario en ambos sitios antes de ejecutar el proceso de re protección, pues de no hacerlo, el proceso podría fallar (VMware, 2019b).

En el contexto de la re protección de máquinas virtuales mediante replicación basada en almacenamiento, SRM sitúa los archivos de las máquinas virtuales de marcador en el almacenamiento de marcador correspondiente al sitio protegido original, en lugar de colocarlos en el mismo almacenamiento donde se hallaban las máquinas virtuales protegidas originales. Este cambio en la ubicación de los archivos asegura que las máquinas virtuales de marcador estén en el sitio protegido, facilitando así una recuperación ordenada y segura en futuros eventos de recuperación. Finalmente, la sincronización forzada de datos desde el nuevo sitio protegido hacia el nuevo sitio de recuperación asegura que el sitio de recuperación posea una copia actualizada de las máquinas virtuales protegidas en operación en el sitio de protección. Esta sincronización es esencial, ya que garantiza que la recuperación será posible de forma inmediata tras la finalización del proceso de re protección, sin necesidad de realizar transferencias adicionales que podrían retrasar el proceso de recuperación en un evento de contingencia (VMware, 2019b).

El proceso de re protección en Site Recovery Manager (SRM) implica la reconfiguración de los grupos de protección y los planes de recuperación para que funcionen en dirección opuesta a la configuración original. Tras una operación de re protección, se habilita la posibilidad de recuperar las máquinas virtuales de vuelta al sitio original mediante un flujo de trabajo de migración planificada. Para iniciar este proceso en el cliente de vSphere, se accede a Site Recovery y, dentro de la pestaña principal de SRM, se selecciona el par de sitios configurados. Una vez ahí, en la pestaña de planes de recuperación, al hacer clic derecho en un plan de recuperación, aparece la opción de re protección. Al iniciar la operación de re protección, es necesario confirmar la irreversibilidad de la misma mediante una casilla de verificación. Adicionalmente, en caso de haber errores en el proceso de limpieza del sitio de recuperación, existe la opción de selección de "Forzar limpieza", aunque solo estará disponible tras una operación de re protección inicial con errores. Luego de revisar la información sobre el proceso de re protección, se da clic en finalizar para comenzar la operación (VMware, 2019c).

Durante la re protección, SRM permite monitorear el progreso en la pestaña de pasos de recuperación del plan seleccionado. Al finalizar, el estado del plan de recuperación se puede revisar en la pestaña de historial, donde además es posible exportar un informe detallado de la operación. Es importante revisar este informe para verificar que no hayan ocurrido errores, ya

que, aunque el plan de recuperación pueda retornar a un estado de disponibilidad, es posible que se presenten errores durante la re protección. En caso de errores, se recomienda intentar resolverlos y ejecutar una prueba de recuperación para asegurarse de que los mismos hayan sido corregidos. Si estos errores no se solucionan y posteriormente se intenta realizar una migración planificada o recuperación de desastres, algunas máquinas virtuales podrían no recuperarse correctamente (VMware, 2019c).

Los resultados de la operación de re protección incluyen la inversión de los roles entre el sitio de recuperación y el sitio protegido. SRM crea copias de marcador de las máquinas virtuales en el nuevo sitio de recuperación, permitiendo así mantener una estructura de referencia para las futuras operaciones de recuperación. Esta configuración asegura que, en un eventual proceso de recuperación, el sistema esté correctamente preparado para una migración ordenada y controlada de regreso al sitio de origen (VMware, 2019c).

4.3.12 Ejecución de Failback

Para restaurar la configuración original de los sitios protegidos y de contingencia después de un proceso de recuperación, es posible realizar una serie de procedimientos opcionales conocidos como failback, proceso de restaurar o volver un sistema a su estado original, este conjunto de operaciones permite devolver la estructura de protección a su disposición inicial antes de la recuperación (VMware, 2019d).

Después de completar una migración planificada o una recuperación ante desastres, el sitio de recuperación anterior se convierte en el nuevo sitio protegido. En este momento, el nuevo sitio protegido no tiene un sitio de recuperación hacia el cual protegerse. Al ejecutar la operación de re protección (reprotect), el sitio de recuperación anterior retoma su rol de sitio de protección, invirtiendo así la dirección de protección original y permitiendo que el sitio protegido esté nuevamente bajo respaldo. Este proceso de re protección asegura la integridad de la infraestructura, permitiendo la continuidad en la disponibilidad de los recursos, aunque en la dirección inversa a la original (VMware, 2019d).

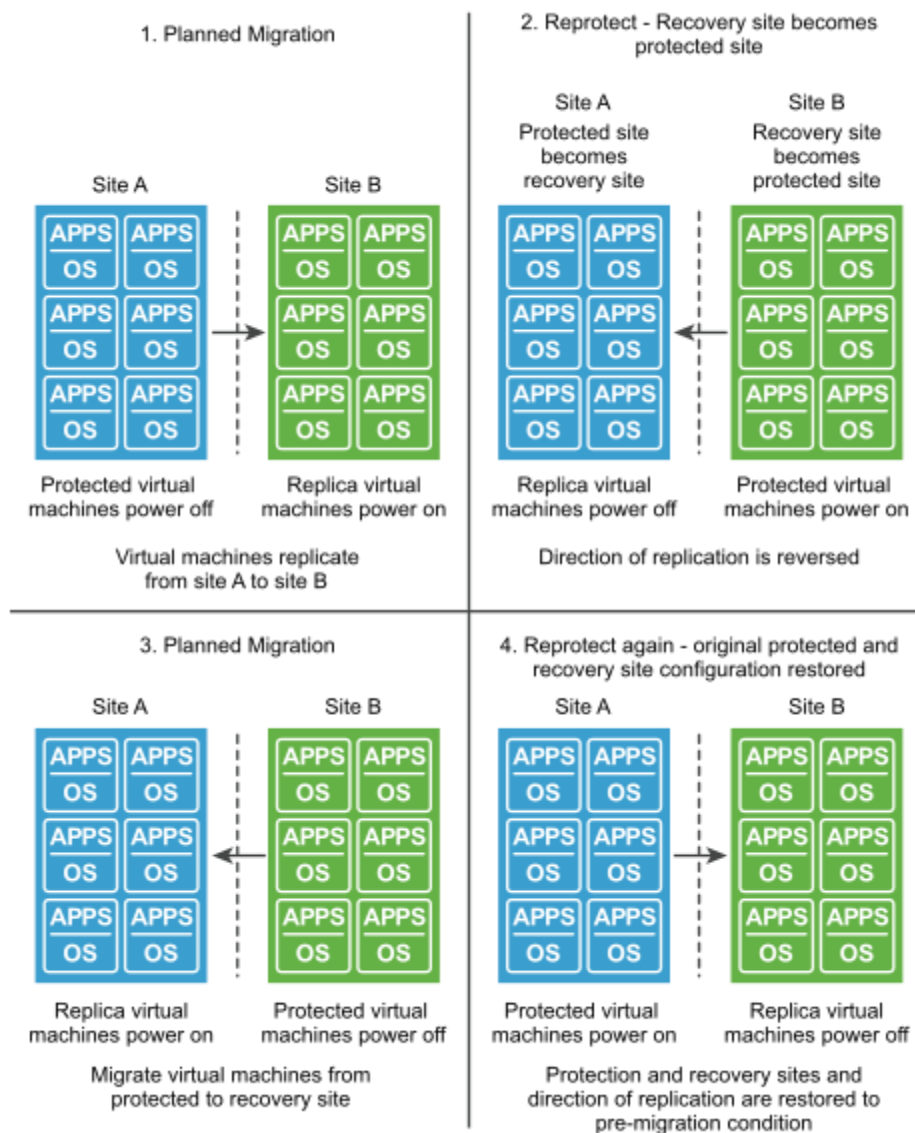
Para restaurar la configuración de los sitios protegido y de recuperación a su disposición inicial, es necesario realizar el procedimiento de failback, que consiste en una secuencia de

operaciones de re protección y migración planificada. En primer lugar, se realiza una re protección para invertir los roles de los sitios, de manera que el sitio de recuperación asume la posición de sitio protegido y viceversa. A continuación, se ejecuta una migración planificada para apagar las máquinas virtuales en el sitio de protección y activarlas en el sitio de recuperación. Esta etapa de migración permite resolver cualquier error de sincronización o configuración detectado, ya que se puede realizar una prueba previa para identificar y corregir problemas antes de llevar a cabo la migración completa. Finalmente, se ejecuta una segunda re protección, lo que devuelve los sitios a su configuración original antes del evento de recuperación (VMware, 2019d).

El proceso de failback permite restaurar los servicios al sitio protegido original una vez que este se encuentra nuevamente en línea después de un incidente. Con esta estructura, se asegura que los sitios puedan retomar su configuración inicial y estar preparados para futuras contingencias, asegurando la continuidad operativa y minimizando el tiempo de inactividad en la infraestructura virtualizada, la Figura 41 describe las 4 etapas que componen el proceso de recuperación (VMware, 2019d).

Figura 41

Proceso de Failback



Nota: Tomado de *Restoring the Pre-Recovery Site Configuration by Performing Failback* [Imagen], VMware by Broadcom, 2019, VMware Docs (<https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-91E89C7C-F43D-42DB-BB42-CF01A797D919.html>)

5 Cronograma

El siguiente cronograma ha sido diseñado como una guía para la instalación básica de Site Recovery Manager (SRM) en una entidad financiera. Los tiempos y duraciones de las tareas deberán adaptarse según la complejidad de la infraestructura de cada entidad. Es importante destacar que este proyecto no incluye la implementación o configuración del centro de datos secundario. Se asume que dicho centro ya está en funcionamiento, ya sea on-premise en otra sucursal o mediante la contratación de un servicio de housing con un proveedor externo. En caso de que el centro de datos secundario no esté instalado, se presentan las tareas correspondientes como referencia opcional para su implementación, como de detalla en la Tabla 3.

Tabla 3

Fase Opcional

Fase	Tareas	Duración Estimada	Dependencias
Fase opcional: Preparación Sitio de Contingencia			
1.Instalación de Hardware	Instalación de Servidores, almacenamiento y redes.	7 días	
2.Configuración de Vsphere	Configuración vCenter Server.	3 días	1
3.Configuración de Red	Conectividad entre ambos sitios.	2 días	2
4.Configuración Storage	Configurar replica de datos.	2 días	3

Nota: Elaboración Propia. Instalación y configuración del datacenter secundario.

Tabla 4*Cronograma de Implementación: Fase 1 y Fase 2*

Fase	Tareas	Duración Estimada	Dependencias
Fase 1: Preparación del Entorno			
1.1 Revisión de la Infraestructura	Evaluación de los servidores, almacenamiento y red	3 días	
1.2 Verificación de compatibilidad	Confirmación de compatibilidad de hardware y software	1 día	1.1
1.3 Instalación del SRM Appliance	Instalación del SRM en el sitio protegido y secundario	2 días	1.2
Fase 2: Configuración del SRM			
2.1 Configuración de SRM en Vsphere	Configuración de SRM en ambos sitios (vCenter Server)	3 días	1.3
2.2 Instalación de SRA	Instalación Storage Replication Adapter	1 día	2.1
2.3 Configuración Array Managers	Configuración de los administradores de arrays	2 días	2.2

Nota: Elaboración Propia. Fases de Preparación y Configuración.

Tabla 5*Cronograma de Implementación: Fase 3 y Fase 4*

Fase	Tareas	Duración Estimada	Dependencias
Fase 3: Mapeo de Recursos y Configuración Avanzada			
3.1 Mapeo de Redes	Configuración de las redes en ambos sitios	2 días	2.3
3.2 Mapeo de Carpetas y Recursos	Configuración de carpetas y recursos virtuales	1 día	3.1
3.3 Configuración Datastore Placeholder	Configuración del datastore pivot para máquinas virtuales	1 día	3.2
3.4 Creación de Grupos de Protección	Configuración de grupos de protección en SRM	1 día	3.3
3.5 Creación de Planes de Recuperación	Definición y configuración de planes de recuperación	2 días	3.4
Fase 4: Pruebas y Validaciones			
4.1 Pruebas de conectividad	Verificación de conectividad entre los sitios	1 día	3.5
4.2 Pruebas de replicación	Validación de la replicación de datos entre sitios	2 días	4.1
4.3 Pruebas de Failover (recuperación en caso de falla)	Simulación de failover para verificar recuperación	3 días	4.2
4.4 Documentación del proceso	Creación de la documentación	2 días	4.3

Nota: Elaboración Propia. Fases de Configuraciones Avanzadas y Pruebas.

Tabla 6

Cronograma de Implementación: Fase Final

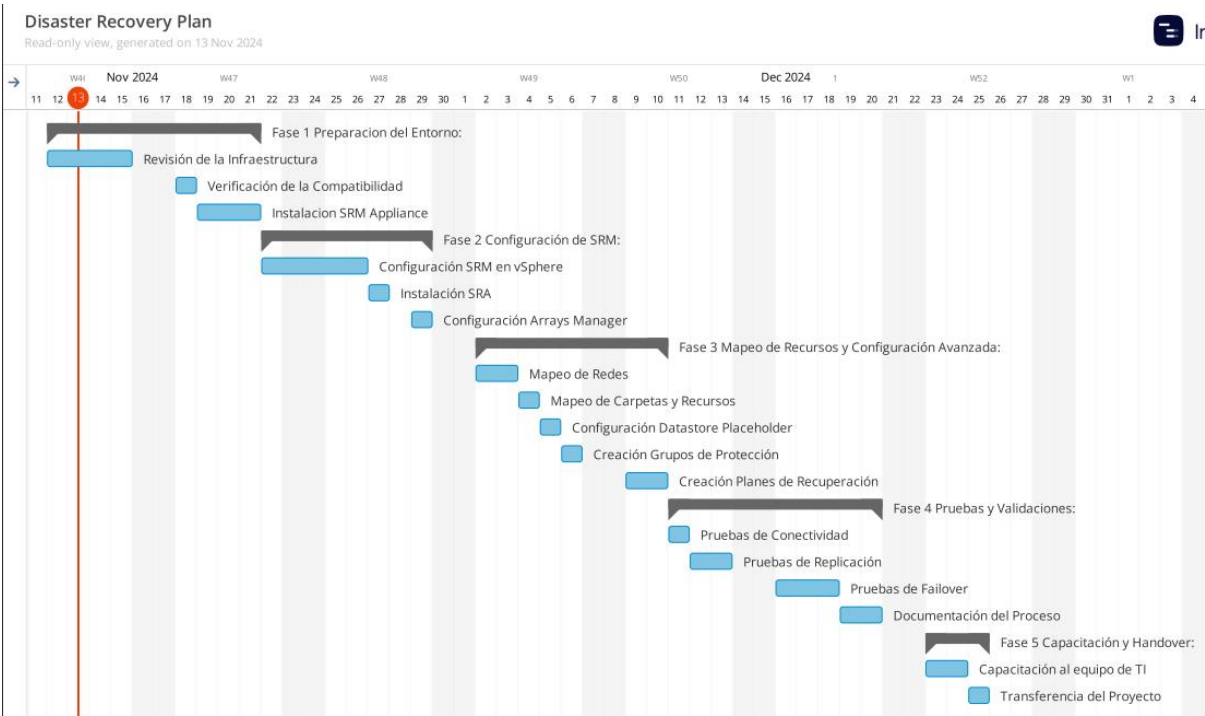
Fase	Tareas	Duración Estimada	Dependencias
Fase 5: Capacitación y Traspaso			
5.1 Capacitación al equipo de TI	Capacitación sobre el uso y gestión de SRM	2 días	4.4
5.2 Transferencia del Proyecto	Traspaso formal del sistema implementado	1 día	5.1

Nota: Elaboración Propia. Fases de Capacitación y Traspaso.

La Figura 42 describe en un diagrama de Gantt, las fases y tareas que componen el proyecto de implementación.

Figura 42

Diagrama de Gantt



Nota: Elaboración Propia. Diagrama de Gantt, donde se puede visualizar las Fases y Tareas que componen la implementación.

6 Recursos Necesarios

6.1 Recursos Humanos

Para la implementación del Plan de Recuperación ante Desastres (DRP) con VMware Site Recovery Manager (SRM), es fundamental contar con los recursos humanos adecuados, ya que la coordinación efectiva y el conocimiento técnico son esenciales para garantizar el éxito del proyecto. A continuación, se detalla la estructura de los recursos necesarios, enfatizando los roles clave para la ejecución del proyecto:

El Project Manager (PM) será el responsable general de la planificación, coordinación y seguimiento del proyecto. Su rol implica gestionar los plazos, asignar tareas y asegurar que todas las fases del proyecto se ejecuten conforme al cronograma establecido. Además, el PM deberá actuar como enlace entre las distintas áreas de la entidad financiera y los equipos técnicos, garantizando que los objetivos se alineen con las necesidades del negocio. El PM también deberá gestionar los riesgos del proyecto y establecer mecanismos de comunicación y reporte efectivos.

Un analista técnico especialista en virtualización en VMware y Site Recovery Manager, este recurso tendrá un rol técnico central en la implementación del SRM. Su función principal es la configuración de la infraestructura virtual en los sitios protegidos y de recuperación, incluyendo la integración de los SRAs (Storage Replication Adapters), la configuración del array managers, y la creación de grupos de protección y planes de recuperación. Debe poseer un conocimiento avanzado de VMware vSphere y SRM, así como una comprensión detallada de las tecnologías de replicación de almacenamiento involucradas. Este analista será el principal responsable de la ejecución técnica del proyecto.

Adicionalmente se requerirán al menos dos Analistas de Infraestructura SSR para brindar soporte técnico y operativo durante la implementación. Estos recursos apoyarán en la configuración de las redes, datastores, y otros componentes de la infraestructura necesaria. Participarán en tareas como la configuración de los mappings entre los recursos de los sitios protegidos y de recuperación, y asistirán en las pruebas de failover y re protección.

Por cada aplicación que deba someterse a pruebas de failover, será necesario un Coordinador o Product Owner que sirva como punto de contacto entre los equipos técnicos y los usuarios finales. Este recurso debe tener un conocimiento profundo de la aplicación y su

funcionamiento dentro del entorno productivo. El coordinador/producto owner es responsable de validar que la aplicación se comporte correctamente después de la activación del plan de recuperación, y de asegurar la integridad de los datos y la continuidad del servicio.

6.2 Matriz RACI

A continuación, en la Tabla 5, se presenta una matriz de roles y responsabilidades (RACI) para la implementación del proyecto, dicha matriz define los roles y las responsabilidades asociadas a cada tarea.

Tabla 7

Matriz RACI

Tarea	PM	Analista SR	Analista SSR	Product Owner	Representante Comité de Riesgos
Planificación del Proyecto	R	C	A	I	I
Diseño de la Arquitectura de SRM	C	R	A	I	I
Configuración de SRM y SRA	I	R	A	I	I
Configuración Datastore Placeholder	I	R	A	I	I
Creación Grupos de Protección	C	R	A	I	I

Creación Planes de Recuperación	C	R	A	I	I
Pruebas de Failover (recuperación en caso de falla)	I	R	A	R	I
Validación de Pruebas	C	C	A	R	R
Supervisión de riesgos y cumplimiento normativo	I	C	I	I	R
Documentación	R	A	A	I	C

Nota: Elaboración Propia. Referencias: Responsable (R), Apoyar (A), Consultado (C) e Informado (I).

6.3 Recursos Tecnológicos

En esta sección, se detallarán los recursos tecnológicos que serán necesarios para la implementación de SRM como herramienta de orquestación ante desastres:

Se parte de la premisa de que la organización ya cuenta con un Centro de Datos Principal y un Centro de Datos Secundario para replicar los datos y alojar las máquinas virtuales protegidas, teniendo en cuenta lo mencionado el entorno de virtualización deberá estar basado en VMware vSphere, el cual será el componente principal para la integración con SRM.

Site Recovery Manager, será el software de orquestación instalado sobre el sitio de protección y de recuperación para automatizar la replicación de datos, failover, failback y re protección de máquinas virtuales.

Un sistema de almacenamiento compatible con SRM y contar los SRA (Storage Replication Adapters) adecuados para habilitar la replicación basada en arrays de almacenamiento, como así también una topología de red entre el sitio protegido y el de recuperación correctamente configurada para la visibilidad entre vlans y segmentos de red. En la Tabla 6 se presenta el listado de todos los recursos tecnológicos necesarios para el desarrollo del proyecto.

Tabla 8

Recursos Tecnológicos

Recurso	Descripción	Función	Comentarios
Centro de Datos Primario	Servidores y almacenamiento donde residen las VM's productivas	Plataforma de ejecución de la carga de trabajo productiva	Integrado con SRM
Centro de Datos Secundario	Infraestructura de respaldo	Ejecución de las VMs en caso de failover	On-Premise o housing externo
VMware Vsphere	Plataforma de Virtualización	Gestión de VMs y SRM	Instalado en ambos centros de datos
Site Recovery Manager (SRM)	Herramienta de recuperación ante desastres	Orquestación de failover y replicación	Implementado en ambos sitios
Sistema de Almacenamiento	Soluciones de almacenamiento compatibles con SRM	Replicación de datos entre sitios.	Con SRA compatible
Storage Replication Adapter (SRA)	Controladores para replicación de almacenamiento	Facilita la replicación a través de SRM	Debe estar instalado en ambos sitios
Licencias VMware	Licencias de Site Recovery Manager	Licenciar las VMs sobre el grupo de protección	Se licencia por pack de 25 VMs

Nota: Elaboración Propia. Descripción de los recursos tecnológicos necesarios.

7 Factores Externos Condicionantes

La implementación del presente proyecto se verá influenciada por una serie de factores externos que pueden condicionar el éxito del proyecto. Entre estos factores se incluyen el entorno regulatorio y la adquisición reciente de VMware por parte de Broadcom, que puede tener implicaciones directas en el soporte y evolución de las soluciones de recuperación ante desastres. A continuación, se detalla cada uno de estos factores:

El entorno regulatorio constituye uno de los factores externos más relevantes en la implementación de un Plan de Recuperación ante Desastres (DRP) con SRM para entidades financieras. En Argentina, las normativas del Banco Central de la República Argentina (BCRA) son estrictas en cuanto a la continuidad operativa de los servicios financieros, dado que cualquier interrupción en las actividades de una entidad puede tener graves consecuencias económicas y sociales. El BCRA, a través de la Comunicación A 7724, establece que todas las entidades financieras deben contar con un Plan de Contingencia y Continuidad Operativa que garantice la disponibilidad de los servicios esenciales en situaciones de desastre o interrupción grave. Esta normativa impone la obligación de implementar mecanismos de recuperación ante desastres, tanto en el sitio principal como en un sitio alternativo o secundario, el cual debe estar preparado para entrar en funcionamiento ante cualquier contingencia. El plan debe asegurar que los sistemas críticos se mantengan operativos o puedan ser restaurados en un plazo razonable, sin comprometer la seguridad o integridad de la información financiera (Banco Central de la República Argentina, 2023b).

Es fundamental que las entidades financieras se ajusten continuamente a las actualizaciones de la normativa, ya que el BCRA realiza modificaciones periódicas en sus políticas para adaptarse a las nuevas amenazas y riesgos en el entorno financiero. La normativa también enfatiza la responsabilidad de las entidades de mantener un enfoque preventivo, considerando la resiliencia operativa como un aspecto estratégico en la gestión de riesgos (Banco Central República Argentina, 2023b).

El segundo factor externo condicionante sucedió en noviembre de 2023, donde Broadcom completó la adquisición de VMware por 69 mil millones de dólares, consolidando su estrategia de ofrecer servicios en la nube y multicloud, y ampliando su alcance en el mercado de virtualización y gestión de infraestructura. Este cambio de propiedad, luego de la separación

de VMware de Dell en 2021, marca una nueva etapa para la empresa de virtualización, con efectos importantes en su portafolio de productos y en la relación con sus clientes (Saran, 2024).

Uno de los impactos principales de la adquisición es el cambio hacia un modelo de licenciamiento por suscripción. Broadcom está impulsando una transición desde las licencias perpetuas hacia suscripciones anuales para la mayoría de los productos de VMware, incluyendo VMware Cloud Foundation, lo que implica una alteración significativa en el modelo de costos a largo plazo para las empresas que dependían de licencias de por vida. Además, Broadcom ha confirmado que retirará su oferta de infraestructura de escritorio virtual (VDI) VMware Horizon y otras soluciones de computación para usuarios finales (EUC, por sus siglas en inglés), lo cual sugiere un enfoque más enfocado en soluciones de infraestructura y menos en productos para usuarios finales. La división de EUC será transferida a KKR, lo cual también implica un cambio de proveedor para las empresas que dependen de estas herramientas (Saran, 2024).

Para las entidades financieras que utilizan VMware SRM, este cambio de licenciamiento implica la necesidad de revisar y ajustar presupuestos, considerando la obligatoriedad de una suscripción que podría resultar en un incremento de costos. Además, Broadcom ha introducido un esquema de “lleve-su-propia-suscripción” (BYOS, por sus siglas en inglés), diseñado para permitir la portabilidad de las licencias hacia entornos de nube híbrida validados por VMware. Sin embargo, estas modificaciones en el modelo de licenciamiento pueden afectar las decisiones de continuidad y disponibilidad de productos (Saran, 2024).

8 Evaluación del Proyecto

8.1 Factibilidad Financiera

Los costos de implementación incluyen los recursos necesarios para la adquisición de software, hardware adicional y servicios de apoyo, como consultoría y capacitación. Esta sección se ha estructurado en dos tablas: la Tabla 7 detalla los costos principales y la Tabla 8 muestra costos adicionales opcionales.

Tabla 9

Costos de Implementación

Concepto	Descripción	Cantidad	Costo Unitario	Costo Total
Licencias de Software	VMware SRM	1 (Pack por 25 VM's)	USD 17000	USD 17000
Soporte y Mantenimiento	VMware SRM	3 (años)	USD 3000	USD 9000
Hardware Adicional	Servidores adicionales para failover.	2 (Dell PowerEdge R660 Rack Server + 3 años Soporte)	USD 10000	USD 20000
Consultoría	Servicio de consultoría para implementación	40 hs	USD 120	USD 4800
Capacitación	Capacitación Técnica para equipo de TI	Pack de 20hs (hasta 6 personas)	USD 3000	USD 3000
Total				USD 53800

Nota: Elaboración Propia. Costos de Implementación, considerando licencias, soporte y mantenimiento, hardware y recursos de consultoría.

Los costos presentados son estimativos y se ofrecen como guía para el análisis financiero; deberán ajustarse a la infraestructura específica en la que se implemente la solución. En este caso, se consideró un único paquete de licencias de SRM, con capacidad para proteger hasta 25 máquinas virtuales en el sitio de recuperación. Si se requieren recursos adicionales de procesamiento, como CPU y RAM, se incluyeron dos servidores Dell PowerEdge R660 como referencia, aunque pueden optarse por otras marcas que cumplan con los requisitos de procesamiento definidos en el análisis final. Asimismo, las horas de consultoría necesarias dependerán del tamaño de la infraestructura, por lo que es fundamental considerar estos elementos y ajustarlos según las necesidades particulares de cada entorno durante el desarrollo del proyecto.

En caso de que la organización no cuente con un sitio de contingencia, estos costos adicionales servirán como referencia para una implementación de este tipo:

Tabla 10

Costos Opcionales de Implementación

Concepto	Descripción	Cantidad	Costo Unitario	Costo Total
Infraestructura	Alquiler o compra de espacio en Datacenter	1	USD 20000	USD 20000
Servidores de Contingencia	Servidores Físicos	4 (Dell PowerEdge R660 Rack Server + 3 años Soporte)	USD 10000	USD 40000
Almacenamiento Adicional	Capacidad de almacenamiento dedicada	1	USD 15000	USD15000

Networking	Equipos de red y configuración en sitio	1	USD 8000	USD 8000
Instalación y configuración	Servicios de implementación y pruebas		USD 12000	USD12000
Total				USD 95000

Nota: Elaboración Propia. Costos de Implementación, considerando licencias, soporte y mantenimiento, hardware y recursos de consultoría.

Los siguientes costos de implementación deben contemplarse en caso de disponer de un sitio de contingencia o un centro de datos secundario en la compañía. Aunque la creación de un sitio de contingencia completo está fuera del alcance de este proyecto, si se requiere una implementación desde cero en dicho sitio, los costos aumentarán considerablemente debido a la inclusión de servidores, redes y almacenamiento.

Cabe destacar que estos costos son estimativos y referenciales, y deberán ajustarse a la infraestructura específica del sitio donde se lleve a cabo la implementación. Otros gastos relevantes a considerar incluyen el alquiler de espacio en un centro de datos, que generará un costo mensual para mantener este servicio. Este análisis de costos proporciona una base detallada sobre los recursos financieros necesarios para implementar el Plan de Recuperación ante Desastres (DRP), considerando tanto un escenario con infraestructura existente como otro que requiere infraestructura adicional en el sitio de contingencia.

9 Conclusiones

La implementación de un Disaster Recovery Plan (DRP) con VMware Site Recovery Manager (SRM) para entidades financieras reguladas por el BCRA como el propuesto en este proyecto de intervención, representa una transformación significativa en la manera de abordar la continuidad operativa. La propuesta de intervención en el campo profesional presentada integra tecnología avanzada de virtualización con un enfoque automatizado para la recuperación ante desastres, alineándose con las exigencias regulatorias y con los estándares de mejores prácticas de la industria. A través del desarrollo de este proyecto, hemos demostrado cómo SRM permite gestionar y orquestar eficientemente el failover y failback de los sistemas críticos, logrando una recuperación más rápida, segura y coherente frente a interrupciones operativas imprevistas. Se estableció una mejora sustancial respecto a los métodos tradicionales de recuperación, que anteriormente dependían de procesos manuales, presentaban tiempos de respuesta prolongados y requerían una alta dependencia de personal especializado durante situaciones de contingencia. La integración de SRM permite reducir considerablemente estos tiempos de respuesta, optimizando la capacidad de la organización para reaccionar y adaptarse eficazmente en contextos de crisis. Esta solución mejora la disponibilidad de los servicios críticos al estandarizar los procedimientos de recuperación, reduciendo los errores humanos y asegurando una recuperación uniforme y confiable en todos los entornos protegidos.

Además, este proyecto ha evidenciado cómo la adopción de SRM facilita el cumplimiento de los requisitos regulatorios establecidos por el Banco Central de la República Argentina (BCRA) en términos de continuidad de negocio. La posibilidad de realizar pruebas periódicas de failover sin afectar la operación normal permite verificar la eficacia del plan de recuperación y ajustarlo conforme a los cambios en la infraestructura o a las nuevas regulaciones, contribuyendo así a una estrategia de continuidad más robusta y flexible. Este enfoque no solo asegura la resiliencia de los sistemas críticos de la organización, sino que también proporciona un modelo replicable para otros actores del sector financiero que buscan adherirse a normativas de recuperación ante desastres.

Sin embargo, también se deben reconocer las limitaciones del proyecto. La dependencia de una infraestructura robusta y compatible en ambos sitios, tanto en el primario como en el de

contingencia, representa un desafío considerable en términos de inversión y mantenimiento. La necesidad de contar con una infraestructura de almacenamiento capaz de soportar replicaciones frecuentes y una conectividad de red con baja latencia puede elevar los costos operativos y logísticos, especialmente para entidades que no cuenten previamente con este tipo de recursos. Asimismo, SRM, aunque simplifica la orquestación de procesos, requiere personal altamente capacitado para su administración, lo cual demanda una inversión adicional en capacitación continua para mantener el nivel de especialización necesario.

En cuanto a la efectividad y sostenibilidad de SRM en el mediano y largo plazo, el proyecto destaca que cualquier modificación significativa en la arquitectura de TI o en los parámetros de seguridad y networking de la organización puede afectar el correcto funcionamiento de los flujos de replicación. Esto implica que se debe contemplar un proceso constante de revisión y ajuste de los parámetros de SRM, en función de la evolución de la infraestructura tecnológica de la entidad. Además, si bien SRM ha mostrado ser una herramienta robusta para entornos on-premise, la evolución hacia entornos híbridos o en la nube podría presentar nuevos desafíos y oportunidades para mejorar aún más los tiempos de recuperación y reducir la dependencia de la infraestructura física.

A partir de esta experiencia, se identifican diversas oportunidades para futuras investigaciones que podrían ampliar los beneficios de un DRP basado en SRM. En primer lugar, la integración de servicios de recuperación en la nube podría disminuir la carga sobre la infraestructura local, proporcionando una opción de recuperación más escalable y flexible. También, se podrían realizar estudios que exploren la automatización completa de las pruebas de failover, lo cual permitiría validar de forma más eficiente el DRP en entornos altamente dinámicos, optimizando aún más los recursos y tiempos de administración. Finalmente, se recomienda la exploración de SRM en otros sectores con requerimientos de alta disponibilidad y cumplimiento normativo para evaluar su adaptabilidad y efectividad en industrias con estructuras operativas distintas.

En conclusión, el desarrollo e implementación de este DRP con VMware SRM representa un avance notable en la adopción de soluciones tecnológicas avanzadas para la recuperación ante desastres en el sector financiero. Los resultados alcanzados evidencian que SRM puede convertirse en un pilar esencial para una estrategia de continuidad de negocio resiliente, ofreciendo a las organizaciones la capacidad de minimizar interrupciones operativas,

cumplir con normativas regulatorias y proteger sus activos críticos. La aplicación de SRM en este contexto no solo contribuye a una mayor estabilidad operativa, sino que también establece un estándar de referencia para otras instituciones financieras que busquen fortalecer sus estrategias de recuperación y adaptación ante un entorno cada vez más digital y vulnerable a las interrupciones tecnológicas.

10 Referencias

- Banco Central de la República Argentina. (2023a). *Historia del BCRA*. <https://www.bcra.gob.ar/Institucional/Historia.asp>
- Banco Central de la República Argentina. (2023b). *COMUNICACIÓN “A” 7724: Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información*. <https://www.bcra.gob.ar/Pdfs/comytexord/A7724.pdf>
- Bhardwaj, R. (s.f.). *What is Storage Replication? Detailed Explanation*. Network Interview. <https://networkinterview.com/what-is-storage-replication/>
- Cato, G. (2020). Site Recovery Manager Technical Overview. The Cloud Platform Tech Zone. <https://core.vmware.com/resource/site-recovery-manager-technical-overview#sec8949-sub1>
- Denis G. (2023). Understanding RPO and RTO. MSP360. <https://www.msp360.com/resources/blog/rto-vs-rpo-difference/>
- Elgdamsi, K., & Embarak, M. (2024). *Implementing a disaster recovery solution for datacenters using VMware Site Recovery Manager*. Electrical and Electronic Department, Faculty of Engineering, University of Tripoli, Libya. https://www.researchgate.net/publication/383947903_Implementing_a_Disaster_Recovery_Solution_for_Datacenters_Using_VMware_Site_Recovery_Manager
- Fani, S. V., & Subriadi, A. P. (2019). *Business Continuity Plan: Examining of Multi-Usable Framework*. Department of Information Systems, Institut Sepuluh Nopember. <https://doi.org/10.1016/j.procs.2019.11.124>
- Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business continuity management: Time for a strategic role? *Long Range Planning*, 37(5), 435-457. <https://doi.org/10.1016/j.lrp.2004.07.011>
- Kesa, D. (2023). *Integrating IT disaster recovery planning and business continuity for sustainable information technology operations*. Jaramogi Oginga Odinga University of Science & Technology, Kenya. <https://doi.org/10.30574/wjarr.2023.18.3.1166>
- Nieto Muñoz, B. V. (2018). *Análisis y evaluación para el diseño de un plan de recuperación ante desastres (DRP) aplicado en un centro de datos para empresas municipales basado en la norma ISO/IEC 24762:2008*. Universidad Politécnica Salesiana. <https://dspace.ups.edu.ec/handle/123456789/10303>
- Onazi, L. (2024). *Business Impact Analysis (Bia) / Business Continuity Planning (Bcp)*. University of Illinois Springfield. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4821926
- Osaji, F. (2023). *Week 7 Research Paper on Disaster Recovery Plan*. The University of the Cumberlands, Kentucky.

https://www.researchgate.net/publication/370264195_Research_Paper_on_Disaster_Recovery_Plan_for_Organizations

Puente Carrera, D. F. (2014). *Diseño de un plan de recuperación de desastres que garantice la continuidad de operaciones de Medicamenta Ecuatoriana S.A.* (Tesis de maestría). Universidad de las Américas, Quito. <https://dspace.udla.edu.ec/handle/33000/1557>

Revista Cloud. (2024). *La virtualización en la recuperación ante desastres*. Revista Cloud. <https://revistacloud.com/virtualizacion-recuperacion-ante-desastres-mejorando-la-continuidad-empresarial/>

Robware. (2008). RVTools. <https://www.robware.net/>

Saran, C. (2024, 28 de febrero). *Broadcom's VMware acquisition explained: The impact on your IT strategy*. Computer Weekly. <https://www.computerweekly.com/feature/Broadcoms-VMware-acquisition-explained-The-impact-on-your-IT-strategy>

Snedaker, S. (2007). *Business Continuity and Disaster Recovery Planning for IT Professionals* (1st ed.). Syngress.

Lessa, L & L Tariku. (2020). *Information technology disaster recovery plan (ITDRP) framework for banks in Ethiopia*. School of Information Science, Addis Ababa University. <https://www.researchgate.net/publication/342642908>

Veeam. (2024). *Veeam Data Platform: Recovery Orchestration*. Veeam. <https://www.veeam.com/products/veeam-data-platform/recovery-orchestration.html>

VMware. (2019a, 31 de mayo). *Run a Recovery Plan*. VMware by Broadcom. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-D8125217-825C-426F-B275-225F99AAD16B.html>

VMware. (2019b, 31 de mayo). *How Site Recovery Manager Reprotects Virtual Machines with Array-Based Replication*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-48FEC027-6A2C-4FE9-82C9-22FA020A2941.html>

VMware. (2019c, 31 de mayo). *Reprotect Virtual Machines*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-5C98A32E-6101-48D5-8AD9-826E3B456E00.html>

VMware. (2020, 30 de julio). *Test a Recovery Plan*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-1BEBD621-42B1-41D7-8FB7-AF259B60FC40.html>

- VMware. (2022, 18 de agosto). *Add Storage Replication Adapters to the Site Recovery Manager Appliance*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-A16E7F4D-8C63-4E4A-8300-3244F41C53DD.html>
- VMware. (2023a, 21 de marzo). *Requisitos previos y prácticas recomendadas para la implementación de Site Recovery Manager Server*. VMware by Broadcom. Recuperado el 13 de octubre de 2024 de <https://docs.vmware.com/es/Site-Recovery-Manager/9.0/srm-installation-and-configuration/GUID-BB0C03E4-72BE-4C74-96C3-97AC6911B6B8.html>
- VMware. (2023b, 21 de marzo). *Conectar las instancias de Site Recovery Manager Server en los sitios protegido y de recuperación*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de https://docs.vmware.com/es/Site-Recovery-Manager/8.7/com.vmware.srm.install_config.doc/GUID-8C233913-6C62-4068-BDD0-49B35D796868.html
- VMware. (2023c, 22 de marzo). *Sitios locales y remotos*. VMware by Broadcom. Recuperado el 13 de octubre de 2024 de <https://docs.vmware.com/es/Site-Recovery-Manager/9.0/srm-installation-and-configuration/GUID-08B7DF70-559C-429C-BC5F-8E08C6638E35.html>
- VMware. (2023d, 21 de septiembre). *Iniciar sesión en la interfaz de administración de VMware Site Recovery Manager Appliance*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/es/Site-Recovery-Manager/9.0/srm-installation-and-configuration/GUID-8EE47C7D-4A6B-40ED-9E89-840331CEFDDC.html>
- VMware. (2023e, 21 de septiembre). *Configurar el Site Recovery Manager Appliance para que se conecte a vCenter Server*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/es/Site-Recovery-Manager/9.0/srm-installation-and-configuration/GUID-2945E98F-4287-4A8F-A822-B18F34C21E25.html>
- VMware. (2023f, 2 de octubre). *Configure Array Managers*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-FAA4F4A5-D89B-425C-A0FD-C29057118C35.html>
- VMware. (2023g, 22 de agosto). *Configure Inventory Mappings*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-DEA90D45-A6DE-48F5-8489-0CFA6D1DF3CB.html>
- VMware. (2023h, 01 de septiembre). *Select a Placeholder Datastore*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-5D4C9F38-37CA-47D1-B43A-A1FED48A05A3.html>

- VMware. (2023i, 21 de noviembre). *Create Array-Based Replication Protection Groups*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-71D4CAE8-9AF8-4829-80EA-BFC3DEC36D09.html>
- VMware. (2023j, 27 de julio). *Create a Recovery Plan*. VMware by Broadcom. Recuperado el 14 de octubre de 2024 de <https://docs.vmware.com/en/Site-Recovery-Manager/9.0/srm-administration/GUID-53DAEF1D-EE38-4895-AD00-598AAA702B8C.html>
- VMware. (2024a). *Documentación de VMware Site Recovery Manager*. VMware by Broadcom. <https://docs.vmware.com/es/Site-Recovery-Manager/index.html>
- VMware. (2024b, 28 de mayo). *Implementar el Site Recovery Manager Virtual Appliance*. VMware by Broadcom. Recuperado el 13 de octubre de 2024 de <https://docs.vmware.com/es/Site-Recovery-Manager/9.0/srm-installation-and-configuration/GUID-3FE5A617-AB08-4EE1-B9DD-EC1F227F304A.html>
- Wallace, M., & Webber, L. (2004). *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*. AMACOM.
- Zerto. (2024). *Disaster Recovery You Can Trust*. Zerto. <https://www.zerto.com/solutions/use-cases/disaster-recovery/>

11 Anexos

Anexo A: Normativa A 7724 – Sección 6

Sección 6: Gestión de la continuidad del negocio

6.1. Marco de gestión de la continuidad

Las entidades deberán establecer un marco de gestión de la continuidad del negocio que considere:

- Las disposiciones vigentes sobre “Lineamientos para la Gestión de Riesgos en las Entidades Financieras”, “Agregación de Datos sobre Riesgos y Elaboración de Informes” y “Lineamientos para la respuesta y recuperación ante ciber incidentes (RRCI)”.
- Los principios para la resiliencia operacional.
- Los resultados de la gestión integral de riesgos, y el apetito por el riesgo definido.
- Los objetivos estratégicos del negocio.
- La gestión de la tecnología y la seguridad de la información, y el modelo de arquitectura empresarial

Este marco de gestión deberá establecer como mínimo:

- Criterios para la realización de análisis de impacto y la definición de las estrategias de continuidad.
- Lineamientos para la elaboración de planes de recuperación.
- Medidas para la mejora continua del marco de gestión.
- Un programa de ejercicios y testeo alineado con los realizados en la gestión de ciber incidentes.
- Planes para la capacitación y concientización.

- La gestión de los recursos vinculados con este marco de gestión.

En función de las operaciones, procesos y estructura de la entidad, se deberá designar un área, sector o responsable de la coordinación de las actividades vinculadas con la gestión de la continuidad del negocio. Asimismo, se deberán definir roles y responsabilidades para las distintas actividades que conforman el marco de gestión.

6.2. Ciber resiliencia en la continuidad del negocio

Las entidades deberán establecer medidas proactivas en el diseño de las operaciones y procesos que les permitan mitigar el riesgo de eventos disruptivos y mantener la confidencialidad, integridad y disponibilidad. De acuerdo con los objetivos estratégicos del negocio, los resultados de la gestión de riesgos y las lecciones aprendidas, se deberán aplicar medidas que fortalezcan las capacidades de recuperación ante eventos disruptivos de la entidad respecto de:

- Las instalaciones, la arquitectura tecnológica y la infraestructura.
- Los ciberataques.
- Las estrategias de resguardos de datos y los mecanismos de replicación.
- Disponibilidad de personal esencial.
- Servicios provistos por terceras partes, interconexiones y dependencias.
- Los suministros de energía y abastecimiento.
- La gestión de cambios de emergencias.

6.3. Análisis de impacto y evaluación de riesgos

Las entidades deberán considerar como base para la gestión de continuidad del negocio el análisis de impacto del negocio (BIA), los resultados de la gestión de riesgos de tecnología y seguridad de la información, y de la gestión integral de riesgos de la entidad. El

análisis de impacto del negocio y las evaluaciones de riesgos deberán ser revisadas periódicamente o ante cambios significativos en la entidad o en su contexto de operación.

6.3.1. Análisis de impacto del negocio

Las entidades deberán implementar un proceso para la elaboración de análisis de impacto del negocio (BIA) que involucre a todas las áreas de la entidad y permita definir las necesidades y prioridades de recuperación. Este proceso deberá incluir:

- La definición de criterios para la evaluación del impacto relevantes para la resiliencia y la continuidad.
- La identificación de las actividades que soportan la prestación de los productos y servicios.
- La identificación de las interdependencias de los procesos.
- La identificación de las dependencias de los procesos respecto de terceras partes.
- La identificación de los posibles incidentes disruptivos y la evaluación de su impacto.
- Los objetivos de recuperación en relación con el tiempo y a la pérdida de datos. (RTO/RPO).
- La razonabilidad de los objetivos de recuperación
- La comunicación de los resultados obtenidos a la Alta Gerencia.

6.3.2. Evaluación de riesgos y escenarios

Las entidades deberán realizar evaluaciones periódicas de los riesgos de escenarios disruptivos. En concordancia con el marco establecido para la gestión integral de riesgos, se deberán establecer planes de tratamiento acordes al apetito de riesgo. Se deberán analizar los riesgos asociados con la ubicación geográfica, la susceptibilidad a las amenazas y la proximidad con infraestructuras críticas de todas las instalaciones, incluidas las provistas por terceras partes. Además, para los escenarios que correspondan, se deberán evaluar las amenazas de interrupción que pudieran afectar de manera simultánea a los distintos sitios.

6.4. Estrategias de continuidad del negocio

Las entidades deberán desarrollar estrategias de continuidad del negocio para cumplir con los objetivos de resiliencia y recuperación definidos, en función de los escenarios de amenaza identificados y de los procesos de negocio. En su alcance, se deberán considerar los siguientes puntos:

- Detalle de la infraestructura de tecnología de la información, recursos involucrados y facilidades de procesamiento.
- Esquemas de copia de seguridad, replicación y almacenamiento para la protección de datos.
- La existencia de entornos aislados de recuperación.
- Niveles de redundancia en la infraestructura de telecomunicaciones.
- Inclusión de los riesgos no tecnológicos (por ejemplo, riesgos de transacción, liquidez y reputación).

6.4.1. Planes de continuidad del negocio

En función de las estrategias definidas, las entidades deberán establecer e implementar planes para la continuidad del negocio que permitan continuar las operaciones durante el período de restablecimiento del servicio afectado. Los planes deberán contemplar las estrategias de continuidad definidas e incluir, como mínimo:

- Los procedimientos para la declaración de una situación de crisis y los criterios para la activación de planes vinculados.
- La asignación de responsabilidades para la ejecución de planes de recuperación.
- Los procedimientos detallados de recuperación, la identificación de la infraestructura, los sistemas y componentes críticos, y su prioridad para la recuperación.

- Los procedimientos para el traslado de actividades esenciales a las ubicaciones alternativas.
- El establecimiento de canales de atención alternativos para los clientes.
- Medidas que aseguren la integridad y confidencialidad de la información crítica durante los procesos de recuperación.

En función de sus operaciones, procesos y estructura, las entidades deberán establecer procedimientos automatizados que permitan mitigar los riesgos asociados a los procesos de recuperación manuales.

6.4.2. Gestión de crisis y estrategias de comunicación

La entidad deberá designar responsables para la toma de decisiones y la elaboración de planes de gestión de crisis. Además, deberá establecer procedimientos ante situaciones de crisis que estén vinculados con la gestión de incidentes y consideren escenarios de disrupción. Asimismo, deberán definir estrategias de comunicación que alcancen:

- A los participantes en la ejecución de los procedimientos, tanto de la entidad, como de terceros.
- A las autoridades que correspondan y a otros interesados.

Se deberán establecer procedimientos de comunicación que aseguren la notificación a las partes interesadas, la definición de listas de contactos, y la participación de las áreas técnicas en la definición del contenido de la comunicación.

6.5. Programa de capacitación y concientización

Las entidades deberán establecer un programa y planes de capacitación que alcance a toda la organización y considere, como mínimo, la resiliencia operacional, los objetivos de continuidad del negocio, el impacto de los posibles escenarios disruptivos, los roles y responsabilidades del personal, y las lecciones aprendidas. Para el desarrollo de los planes que componen el programa se deberá tener en cuenta, como mínimo, la identificación y

segmentación de públicos, incluyendo al Directorio, la Alta Gerencia y las áreas responsables de atención al cliente.

Los planes deberán ser revisados periódicamente, con el objetivo de evaluar e informar a la Alta Gerencia acerca de la efectividad de las actividades realizadas.

6.6. Ejercicios y pruebas de los planes de continuidad del negocio

Las entidades deberán desarrollar un plan de ejercicios y pruebas a fin de verificar que las estrategias de continuidad definidas y los planes establecidos respaldan adecuadamente los objetivos de continuidad del negocio. El plan deberá contener un cronograma anual formalizado, acorde a sus operaciones, procesos y estructura, que indique los escenarios contemplados, las fechas, áreas involucradas, procesos de negocio y sistemas alcanzados, entre otros aspectos. El cronograma deberá contemplar al menos uno de los escenarios de más alta criticidad. En los ejercicios y pruebas de los planes de continuidad deberán participar, como mínimo, el responsable de la gestión de continuidad del negocio, las áreas de tecnología y seguridad de la información, las áreas usuarias relacionadas con los procesos de negocio, las terceras partes vinculadas y las áreas de auditoría interna. Además, los resultados deberán permitir la evaluación de:

- La eficacia de las estrategias de continuidad adoptadas.
- El desempeño de las actividades de los participantes de acuerdo sus roles y responsabilidades.
- Los aspectos técnicos, logísticos y administrativos.
- El funcionamiento de la infraestructura de recuperación.
- La factibilidad de los procesos de reubicación del personal.
- Las deficiencias y oportunidades de mejora de los planes de continuidad.
- La efectividad de las estrategias de comunicación.

Se deberá mantener un registro detallado de los resultados de cada ejercicio, las observaciones y problemas detectados, y los planes de acción definidos para su corrección.

6.7. Mantenimiento de los planes de la continuidad del negocio

Las entidades deberán revisar y actualizar periódicamente los planes de continuidad del negocio y sus procedimientos vinculados a fin de asegurar su alineación con los objetivos del negocio, considerando, como mínimo:

- Cambios en las estrategias del negocio.
- La implementación de nuevos productos, servicios y/o infraestructuras tecnológicas.
- Cambios en los productos y servicios de terceras partes.
- Surgimiento de nuevos escenarios de amenazas.
- Cambios regulatorios.
- Indicadores clave de riesgo.
- Resultados de los ejercicios y pruebas realizadas.
- Resultados de las actividades de auditoría o evaluaciones internas o externas.

6.8. Control y reportes de gestión

Las entidades deberán definir un proceso de control sobre la gestión de la continuidad del negocio, mediante procedimientos, herramientas y métricas que permitan realizar un seguimiento y evaluación de las tareas desarrolladas y del cumplimiento de objetivos. Las métricas deberán incluir indicadores o umbrales que permitan controlar los desvíos respecto de lo planificado, tanto para los planes de continuidad, los de capacitación como los de pruebas. Entre las actividades de mejora continua, se deberán documentar, analizar e incluir las lecciones aprendidas de la ejecución de los planes, del análisis de impacto del negocio, la evaluación de riesgos y de los ejercicios y pruebas realizadas. Se deberá establecer la frecuencia y los canales formales de comunicación de los resultados de la gestión de las áreas

al Directorio y la Alta Gerencia. A su vez, la Alta Gerencia deberá informar sobre la gestión de la continuidad del negocio al Directorio o autoridad equivalente.