

**UNIVERSIDAD POLITÉCNICA SALESIANA  
SEDE CUENCA**

**CARRERA DE INGENIERÍA DE SISTEMAS**

*Trabajo de titulación previo  
a la obtención del título  
de Ingeniero de Sistemas*

**PROYECTO TÉCNICO:**

**“DESARROLLAR UNA METODOLOGÍA PARA EL DESPLIEGUE DE UN SITIO  
ALTERNO APLICANDO LA NORMA ISO 22301 A UN CENTRO DE DATOS  
USANDO LA APLICACIÓN VEEAM”**

**AUTORES:**

MARCOS DAVID CÓRDOVA MONTESDEOCA

GABRIEL ESTEBAN SOLANO COBOS

**TUTOR:**

ING. PABLO LEONIDAS GALLEGOS SEGOVIA

CUENCA - ECUADOR

2021

## CESIÓN DE DERECHOS DE AUTOR

Nosotros, Marcos David Córdova Montesdeoca con documento de identificación N° 0103937504 y Gabriel Esteban Solano Cobos con documento de identificación N° 0105953848, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación: **“DESARROLLAR UNA METODOLOGÍA PARA EL DESPLIEGUE DE UN SITIO ALTERNO APLICANDO LA NORMA ISO 22301 A UN CENTRO DE DATOS USANDO LA APLICACIÓN VEEAM”**, mismo que ha sido desarrollado para optar por el título de: *Ingeniero de Sistemas*, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hacemos entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Cuenca, enero del 2021

.....  
Marcos David Córdova Montesdeoca  
C.I. 0103937504

.....  
Gabriel Esteban Solano Cobos  
C.I. 0105953848

## CERTIFICACIÓN

Yo, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **“DESARROLLAR UNA METODOLOGÍA PARA EL DESPLIEGUE DE UN SITIO ALTERNO APLICANDO LA NORMA ISO 22301 A UN CENTRO DE DATOS USANDO LA APLICACIÓN VEEAM”**, realizado por Marcos David Córdova Montesdeoca y Gabriel Esteban Solano Cobos, obteniendo el *Proyecto Técnico*, que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana.

Cuenca, enero del 2021

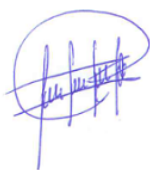


Ing. Pablo Leonidas Gallegos Segovia  
C.I: 0102593589

## DECLARATORIA DE RESPONSABILIDAD

Nosotros, Marcos David Córdova Montesdeoca con documento de identificación N° 0103937504 y Gabriel Esteban Solano Cobos con documento de identificación N° 0105953848, autores del trabajo de titulación: **“DESARROLLAR UNA METODOLOGÍA PARA EL DESPLIEGUE DE UN SITIO ALTERNO APLICANDO LA NORMA ISO 22301 A UN CENTRO DE DATOS USANDO LA APLICACIÓN VEEAM”**, certificamos que el total contenido del *Proyecto Técnico*, es de nuestra exclusiva responsabilidad y autoría.

Cuenca, enero del 2021



.....  
Marcos David Córdova Montesdeoca  
C.I. 0103937504



.....  
Gabriel Esteban Solano Cobos  
C.I. 0105953848

## **AGRADECIMIENTO**

*Queremos expresar nuestros más sinceros agradecimientos a todos los docentes que formaron parte de nuestra formación académica en la carrera de Ingeniería en Sistemas mención Telemática de la Universidad Politécnica Salesiana, de la misma manera a los directores de carrera la Ing. Bertha Tacuri y Dr. Vladimir Robles, al grupo de investigación “Cloud Computing Smart Cities & High Performance Computing”, por todos los conocimientos impartidos en el transcurso de nuestra carrera, a nuestras familias por todo el apoyo y la confianza que nos brindaron durante nuestros estudios. Y fundamentalmente al Ing. Pablo Gallegos quien a más de ser nuestro tutor fue un amigo y nuestro apoyo en todo el proyecto, impartiéndonos todos sus conocimientos para conseguir nuestro objetivo de ser Ingenieros en Sistemas.*

***Marcos Cordova - Esteban Solano***

## **DEDICATORIA**

*Primero quiero agradecer a Dios, por la vida que me dio, la sabiduría y la oportunidad para poder cumplir con los objetivos y metas que pude cumplir en mi vida profesional, así mismo por darme la fortaleza para no rendirme y seguir adelante.*

*A mis padres Beatriz y Xavier, que son el pilar fundamental que con su apoyo incondicional estuvieron presentes durante todo este tiempo, ya por medio de sus consejos, sacrificio y dedicación que mantuvieron durante todo este tiempo para poder cumplir con mis metas, a mis hermanos, que supieron apoyarme durante este camino universitario, a mi esposa que con su apoyo, comprensión y ayuda en este proceso de titulación, ya que me sigue apoyando en mi vida personal y profesional, que juntos pudimos lograr una meta más en nuestras vidas, también a mis hijos Josué y Sofía que también fueron el pilar fundamental para lograr una meta mas en mi vida profesional*

*A mi tutor de tesis el Ing. Pablo Gallegos que fue un amigo, un profesor y colega quien me ha sabido guiar en este proyecto y en las etapas de mi formación universitaria, brindándome una ayuda incondicional y compartiendo todos sus conocimientos y consejos dentro y fuera de las aulas de clase. A mi compañero de tesis Esteban Solano por haber sido un gran amigo quien estuvo presente en toda mi vida universitaria. A todos mis amigos y compañeros que me brindaron sus conocimientos y consejos, de manera especial a mi grupo de trabajos Byron Fernández y Jonnathan López, que me ayudaron a formarme como profesional y apoyarme en todo momento.*

**Marcos David Cordova Montesdeoca.**

## **DEDICATORIA**

*Primero quiero agradecer a Dios, por la vida que me dio, la sabiduría y la oportunidad para cumplir con una meta más de mi vida profesional, así mismo por darme la fortaleza para no rendirme y seguir adelante.*

*A mis padres Tito y Elsi por todo su amor, sus consejos y sobre todo por el sacrificio que hicieron para que yo pudiera cumplir mis metas, a mi hermano Daniel que fue mi apoyo en las dificultades que se me presentaban en la carrera.*

*A mi tutor de tesis el Ing. Pablo Gallegos que fue un amigo, un profesor y colega quien me supo guiar no solo en este proyecto sino en las etapas de mi formación universitaria, brindándome una ayuda incondicional y compartiendo todos sus conocimientos y consejos dentro y fuera de las aulas de clase. A mi compañero de tesis Marcos Cordova por haber sido un gran amigo quien estuvo para mí en toda vida como estudiante. A todos mis amigos y compañeros que me brindaron sus conocimientos y consejos, de manera especial a mi grupo de trabajos Byron Fernández y Jonnathan López que me ayudaron a formarme como profesional y apoyarme en todo momento.*

*A mi enamorada Joseline Brito quien me apoya de manera incondicional en todo lo que necesitaba, me supo comprender y ayudar en el proceso de realizar mi tesis y que me sigue apoyando en mi vida personal y profesional.*

**Gabriel Esteban Solano Cobos.**

## ÍNDICE GENERAL

RESUMEN	1
ABSTRACT	2
INTRODUCCIÓN	3
CAPÍTULO I	5
1.1 Problema	5
1.2 Justificación	7
1.3 Objetivos	9
1.3.1 Objetivo General	9
1.3.2 Objetivos Específicos	9
CAPÍTULO II	10
2.1 Marco teórico	10
2.1.1 Virtualización	10
2.1.1.1 Componentes de la virtualización.	11
2.1.1.2 Tipos de virtualización	12
2.1.1.2.1 Virtualización de Servidores	13
2.1.1.2.2 Virtualización de Almacenamiento	16
2.1.1.2.3 Virtualización de Redes	16
2.1.1.2.4 Virtualización de Servicios	18
2.1.1.2.5 Virtualización de Memoria	19
2.1.1.2.6 Virtualización de Software.	19
2.1.1.2.7 Virtualización Escritorio.	19
2.1.1.3 Ventajas y Desventajas de la Virtualización	20
2.1.1.3.1 Ventajas de la virtualización	20
2.1.1.3.2 Desventajas de la virtualización	20
2.1.2 Que es Hypervisor	21
2.1.2.1 Tipos de Hypervisores	21
• Tipo 1 hipervisor. También llamado metal desnudo o nativo.	21
• Tipo 2 hipervisor. También conocido como hipervisores alojados.	21
2.1.2.2 Clasificación de Hypervisores	22
• Hypervisor Huésped	22
• Hypervisor Nativa.	22
• Hypervisor Hibrida	23
2.1.2.3 Ventajas de los Hypervisores	23



2.1.3 VMware	24
2.1.3.1 Historia de VMware.	25
2.1.3.2 VMware dentro del cuadrante de Gartner	26
2.1.3.3 Redes y Seguridad.	28
2.1.3.4 Almacenamiento y disponibilidad.	28
2.1.3.5 Tipos de entorno de virtualización	29
2.1.3.6 VMware vSphere	29
2.1.3.6.1 VMware vSphere Hypervisor.	30
2.1.3.7 VMware ESXi	31
2.1.3.7.1 Características	34
2.1.3.8 VMware VCenter Server	34
2.1.3.8.1 Características	35
2.1.3.9 vCenter Server	37
2.1.3.10 vSAN	38
2.1.3.10.1 Ventajas de vSAN	38
2.1.4 Centro de Datos	39
2.2 Microsoft Azure	41
2.2.1 Herramientas y Servicios de Microsoft Azure	42
2.3 Diagrama de Flujo	44
CAPITULO III	47
3. Reseña Histórica Veeam.	47
3.1 Veeam	48
3.1.1 Veeam Backup & Replication	49
3.1.1.1 Características de Veeam Backup & Replication	49
3.2. Veeam Availability Suite	50
3.2.1 Características de Veeam Availability Suite	51
3.3 Veeam Availability Orchestrator	51
3.3.1 Características Veeam Availability Orchestrator.	52
3.4 Veeam Backup Essentials.	52
3.4.1 Características Veeam Backup Essentials.	53
3.5 Veeam en el Cuadrante de Gartner	53
CAPITULO IV	55
4.1 ISO 22301	55
4.1.1 Sistema de Continuidad del negocio según la norma ISO 22301.	56

4.1.2	Importancia de la Norma ISO 22301.	58
4.1.3	Características de la ISO 22301	58
4.1.4	Ventajas de la Norma ISO 22301.	59
4.2	Plan de Continuidad de Negocio.	59
4.2.1	Pasos para gestionar un Plan de Continuidad de Negocio	60
4.3	Plan de Recuperación de Desastres (DRP)	60
4.3.1	Características de un DRP	61
CAPÍTULO V		62
5.1	Metodología.	62
5.2	Implementación de la Metodología	62
5.2.1	Selección de la metodología	62
5.2.2	Roles Scrum	63
5.2.3	Artefactos Scrum	65
5.2.4	Eventos Scrum	66
5.2.5	Sector de Interés	66
5.2.6	Iteraciones	67
5.3	Software y Hardware Requerido	68
CAPÍTULO VI		71
6.1	Desarrollo	71
6.1.1	Planificación	71
6.1.2	Actividades	71
6.1.3	Actividades Prioritarias	71
6.1.4	Desarrollo de Actividades	72
6.1.4.1	Topologías que recomienda la empresa Veeam	72
6.1.4.2	Software necesarios	74
6.1.4.3	Instalacion del software	75
6.1.4.4	Servicios del Centro de Datos	83
6.1.4.5	Instalacion de Veeam	83
6.1.4.6	Plan de continuidad del negocio en base a la norma ISO 22301	87
CAPÍTULO VII		88
7.	Plan de Continuidad de Negocio.	88
7.1	Liderazgo.	88
7.2	Política de la Continuidad de Negocio.	88
7.2.1	Objetivo.	89

7.2.2 Respaldo de la información.	89
7.2.2.1 Seguridad de la información y Respaldo.	89
7.2.3 Roles y Responsabilidades.	90
7.2.4 Pruebas.	90
7.2.5 Consideraciones Generales.	90
7.3 Norma ISO 22301.	91
7.4 Análisis de Riesgos y Vulnerabilidades.	92
7.4.1 Identificación de Riesgos.	94
7.5 Impacto en la organización.	94
7.5.1 Estrategias en la Recuperación.	95
7.5.1.1 Recuperación de la información digital de los clientes.	96
7.5.1.2 Recuperación de Servidores.	96
7.6 Determinación del Alcance.	97
7.7 Descripción del Plan de Continuidad de Negocio	97
7.7.1 Descripción en Base a la ISO 22301	97
7.7.2 Plan de Recuperación de Desastres (Disaster Recovery Plan - DRP)	98
7.7.2.1 Introducción.	98
7.7.2.2 Descripción DRP.	98
7.7.2.3 Preparación antes de un desastre.	101
7.7.2.4 Plan de Recuperación.	101
7.7.2.4.1 Plan de Recuperación de los Servicios.	101
7.8 Socialización del plan.	102
7.8.1 Situación Actual.	102
7.8.1.1 Procesos Levantados.	102
7.8.1.2 Identificación del Escenario.	102
CAPÍTULO VIII.	103
8.1 Escenario	103
8.1.1 Caso 1	104
8.1.2 Caso 2	106
8.2 Conexión con el centro de datos principal	107
8.3 Replicación de centro de datos	110
8.4 Lanzamiento del plan para la continuidad de negocio	114
CONCLUSIONES	121
REFERENCIAS	122

## ÍNDICE DE IMÁGENES

Imagen 1. Tipos de Virtualización	12
Imagen 2. VMware en el Cuadrante de Gartner	27
Imagen 3. Proceso de Instalación	44
Imagen 4. Proceso de Instalación	45
Imagen 5. Proceso de replicación y Plan de continuidad del negocio	46
Imagen 6. Veeam en el Cuadrante de Gartner	54
Imagen 7. Características de la máquina para el Centro de Datos	68
Imagen 8. Características de la máquina para el Windows Server 2016	69
Imagen 9. Reglas para el uso de SCRUM	70
Imagen 10. Infraestructura planteada	72
Imagen 11. Infraestructura planteada	72
Imagen 12. Infraestructura planteada	73
Imagen 13. Infraestructura que va a ser desarrollada	73
Imagen 14. Especificaciones del Centro de Datos principal	76
Imagen 15. Pantalla de carga de ESXi	76
Imagen 16. Selección de disco para la instalación	77
Imagen 17. Ingreso de contraseña	77
Imagen 18. Configuración de la interfaz de red	77
Imagen 19. Configuración del DNS y Host	78
Imagen 20. Sufijo del DNS	78
Imagen 21. Pantalla de inicio del ESXi	78
Imagen 22. Centro de Datos principal	79
Imagen 23. Especificaciones del Centro de datos alterno	79
Imagen 24. Configuración de la interfaz de red	80
Imagen 25. Configuración del DNS y el Host	80
Imagen 26. Sufijo del DNS	80
Imagen 27. Especificaciones para el Windows Server 2016	81
Imagen 28. Configuración de IP para la interfaz de red	81
Imagen 29. Nombre del Windows Server 2016	82
Imagen 30. Zona principal del DNS del WS 2016	82

Imagen 31. Zona inversa del DNS del WS 2016	82
Imagen 32. Servicios configurados del Centro de Datos principal	83
Imagen 33. Términos y condiciones de Veeam	83
Imagen 34. Licencia de prueba de Veeam	84
Imagen 35. Software que se instala y ubicación de instalación	84
Imagen 36. Configuración de Veeam	85
Imagen 37. Proceso de instalación	85
Imagen 38. Primera pantalla de Veeam	86
Imagen 39. Usuario y contraseña para ingreso a Veeam	86
Imagen 40. Ventana para agregar el Centro de Datos principal y el alterno	87
Imagen 41. Conexión con el Centro de Datos	107
Imagen 42. Selección del tipo de Hypervisor	107
Imagen 43. Hypervisor físico o en la nube	107
Imagen 44. Nombre de Centro de Datos para la conexión	108
Imagen 45. Llave de ingreso	108
Imagen 46. Usuario y contraseña para la conexión	108
Imagen 47. Certificado de conexión	109
Imagen 48. Conexión establecida	109
Imagen 49. Centro de Datos principal y alterno listos para trabajar	110
Imagen 50. Servicios que van a ser replicados	110
Imagen 51. Nombre del proceso a ser realizado	111
Imagen 52. Selección del Centro de Datos principal	111
Imagen 53. Seleccionar el destino para la replicación	111
Imagen 54. Configuración para el trabajo que se va a realizar	112
Imagen 55. Datos que se van transferir	112
Imagen 56. Configurar un horario de replicación	112
Imagen 57. Información del trabajo que se va a realizar	113
Imagen 58. Proceso de replicación	114
Imagen 59. Replica realizada en el Centro de Datos alterno	114
Imagen 60. Nombre de trabajo en caso de Desastres	115
Imagen 61. Selección las máquinas para el trabajo	115
Imagen 62. Selección de la réplica realizada	115
Imagen 63. Máquinas Virtuales que van a remplazar a las principales	116
Imagen 64. Información del trabajo que se va a realizar	116

Imagen 65. En espera de que ocurra un desastre	116
Imagen 66. Empieza a trabajo	117
Imagen 67. Levantamiento de las maquinas en el Centro de datos alternativo	117
Imagen 68. Trabajo terminado y funcionando al 100%	117
Imagen 69. Maquinas activas en el Centro de Datos alternativo	118
Imagen 70. Retorno de las maquinas al Centro de Datos principal	118
Imagen 71. Selección del tipo de trabajo que va a realizar	119
Imagen 72. Retorno al Centro de Datos principal listo para empezar	119
Imagen 73. Proceso de Retorno de la Maquinas	120

## ÍNDICE DE TABLAS

Tabla 1. Cuadro comparativo de vShare ESXi	32
Tabla 2. Requerimiento de ESXI	33
Tabla 3. Hardware requerido para ESXi 6.7.0	74
Tabla 4. Hardware requerido para vCenter 6.7.0	74
Tabla 5. Hardware requerido para Windows Server 2016	74
Tabla 6. Hardware requerido para Veeam v10	75
Tabla 7. Sistemas Operativos compatibles	75
Tabla 8. Software requerido para Veeam v10	75
Tabla 9. Tabla de probabilidad y referencia	94
Tabla 10. Escenario de prueba caso 1	105
Tabla 11. Escenario de prueba caso 2	106

## RESUMEN

En el presente trabajo de investigación, se desarrolló una metodología para el despliegue de un sitio alternativo, aplicando la norma ISO 22301, la misma que permite gestionar la continuidad del negocio y aplicaciones críticas, con la finalidad de proteger, mitigar y gestionar los riesgos, de amenazas actuales o futuras, tanto físicas como humanas, y de esta manera asegurar que la información del centro de datos permanezca disponible, sin que afecten al normal funcionamiento de las organizaciones, tomando en cuenta su función primordial y la de su alta disponibilidad para el cumplimiento de los objetivos y de la continuidad del negocio.

La falta de instrucciones concisas que detallen o justifiquen, por donde se puede empezar, o cuales son los pasos a seguir, evitando la pérdida total de la información, tomando en cuenta la organización de las empresas, los datos pasarán a un sitio alternativo de manera rápida y segura, hasta que el sistema que se encuentre con fallas, se restablezca y esté en funcionamiento, manteniendo toda la información segura y ordenada, sin que existan degradaciones o pérdidas.

Por lo tanto, se desarrolló una metodología BCP (Plan de Continuidad del Negocio) que es un conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos de negocio, mediante un plan de recuperación de desastres DRP que no es más que la forma en cada una de las empresas u organizaciones enfrentan o se preparan para la recuperación de su funcionamiento ante cualquier desastre, mediante estrategias y acciones, utilizando, Veeam Hyper-Availability Platform, plataforma que cuenta con las herramientas y servicios adecuados en el cual se podrá realizar el despliegue al sitio alternativo, y de esta manera dar cumplimiento a los requerimientos o políticas de gestión para la continuidad de negocio.



## ABSTRACT

In the present research work, a methodology was developed for the deployment of an alternate site, applying the ISO 22301 standard, which allows managing business continuity and critical applications, in order to protect, mitigate and manage risks, of current or future threats, both physical and human, and in this way ensure that the data center information remains available, without affecting the normal functioning of organizations, taking into account its primary function and its high availability for fulfillment of the objectives and the continuity of the business.

The lack of concise instructions that detail or justify, where you can start, or what are the steps to follow, avoiding the total loss of information, taking into account the organization of the companies, the data will go to an alternate site so fast and safe, until the system that is faulty, is restored and is in operation, keeping all information safe and orderly, without any degradation or loss.

Therefore, a BCP methodology (Business Continuity Plan) was developed, which is a set of procedures and strategies defined to ensure the timely and orderly resumption of business processes, through a DRP disaster recovery plan that is no more than the way in which each of the companies or organizations face or prepare for the recovery of its operation in the event of any disaster, through strategies and actions, using, Veeam Hyper-Availability Platform, a platform that has the appropriate tools and services in which the deployment to the alternate site may be carried out, and thus comply with the requirements or management policies for business continuity.

## INTRODUCCIÓN

En la actualidad la información de las empresas se han convertido en uno de los recursos más valiosos e indispensables, es por ello que los centros de datos son el factor más importante de cada una de las empresas ya sean estas públicas o privadas, teniendo que almacenar una gran cantidad de información sensible y vital, en donde se situaran muchas de sus aplicaciones críticas, de ahí la importancia de necesitar un adecuado sistema de gestión y tratamiento de los datos, es por ello que la continuidad del negocio de cada una de estas empresas debe ser un factor primordial en el cual permita una excelente operatividad, integridad y disponibilidad de todos sus servicios y funciones, garantizando a cada uno de sus usuarios el uso de su información que debe estar muy bien almacenada, procesada y transmitida, quienes permitirán generar ingresos a las empresas, es por eso que encontramos la necesidad de relacionar y desarrollar una metodología basadas en las en las normas ISO, ya que el objetivo de cada una de ellas es la de ofrecer o mantener un sistema de gestión basados en la continuidad del negocio.

Con el constante avance de la tecnología y del mundo digital es necesario dar a conocer la importancia de sustentar, mantener y proteger toda la información frente a situaciones críticas en las que se las podría calificar como amenazas, sean estas físicas o humanas, tomando en cuenta que según la norma ISO 22301 en la que especifica cuáles son los requisitos y las normas preventivas que deben tener en cuenta la empresas para mantener la continuidad en la entrega de sus servicios, durante eventos en los que se produzcan daños o interrupciones en sus diferentes equipos, es así que existe la necesidad de las empresas de sustentar, mantener y proteger información y los datos críticos de las empresas que es el pilar fundamental por el cual se desarrolla sus actividades.

En la actualidad el costo de mantenimiento y seguridad de un centro de datos y de sus aplicaciones críticas de cada una de las empresas es un gran problema, y más si se trata de proteger los diferentes procesos críticos y operativos de las empresas contra las diferentes situaciones de riesgo que reducirán al máximo su operatividad y funcionamiento, por lo tanto existe la necesidad de contar con un sistema de gestión que permita realizar el respaldo de toda la información hacia un sitio alternativo, la misma que permitirá y optimizará el correcto funcionamiento y disponibilidad al acceso a los centros de datos y a la información, mediante procesos de recuperación y con la ayuda de aplicaciones que permitirán realizar el respaldo confiable y seguro de toda la información y de esa manera cumplir con todos los requerimientos de un sistema de gestión para la continuidad del negocio y de sus actividades en todas las empresas.

Con el crecimiento de los negocios y el constante aumento de las amenazas así como de las situaciones críticas las organizaciones deben estar preparadas para afrontar y superar las fallas que puedan sufrir los centros de datos y sus aplicaciones críticas, por lo tanto, es necesario la creación de una metodología que permitirá realizar el despliegue de la información a un sitio alternativo, la creación y el respaldo hacia un sitio alternativo se realizará mediante la aplicación Veeam que nos es más que un conjunto de aplicaciones que habilitan parámetros y configuraciones para respaldar la información y aplicaciones críticas desde un centro de datos principal hacia un sitio alternativo, brindando de esta manera confidencialidad, integridad y disponibilidad en las aplicaciones que se encuentran en el centro de datos cumpliendo con los estándares y normas ISO 22301.

# CAPÍTULO I

## 1.1 Problema

El activo más importante de las empresas es la información es por ello que este debe ser debidamente almacenado, procesado y transmitido desde y hacia el centro de datos, por lo que es necesario contar con sistemas de gestión que respalde hacia un sitio alternativo el cual, al existir daños, interrupciones en los sistemas principales el acceso y la disponibilidad de la información todo el tiempo. Sin embargo, estos procesos necesitan escalar a un nivel superior migrando la información a un centro de datos alternativo, por ello es necesario la utilización de aplicaciones que nos apoyen en el respaldo de información y aplicaciones críticas y de esta forma habilitar la continuidad del negocio.

Con las nuevas alternativas del mercado, y en base al crecimiento significativo de los negocios, es necesario la creación de una metodología para proteger y mantener la información y aplicaciones críticas de las empresas garantizando la continuidad del negocio, para ello las organizaciones deberán estar preparadas para afrontar y superar las fallas o amenazas que pueda sufrir el centro de datos, y de esa manera evitar una pérdida de la información, afectando y perjudicando a todos sus usuarios, la continuidad del negocio genera estrategias que permiten de una manera rápida, segura, y con alta disponibilidad el despliegue de un sitio alternativo ante situaciones adversas a su funcionamiento y mantenimiento.

Hoy en día proteger toda la información de amenazas actuales o futuras ya sean humanas o físicas y el mantenimiento de los diferentes centros de datos generan altos costos a las empresas por lo que existe la necesidad de desarrollar una metodología que permita a las empresas desplegar toda su información de un centro de datos a un sitio alternativo y de esta

manera garantizar y optimizar el buen funcionamiento de sus servicios y aplicaciones durante las diferentes situaciones críticas o amenazas en los sistemas, afectando de tal manera a los usuarios que se limitaría, reduciría, de una forma parcial o total, el acceso a toda la información que se encuentran ubicadas en el centro de datos produciendo un impacto negativo hacia la sociedad, y, por otro lado, produciendo grandes pérdidas económicas

Mediante la utilización de la plataforma Veeam, que usa un conjunto de aplicaciones que habilitan parámetros y configuraciones para respaldar de una manera íntegra la información y aplicaciones críticas desde un sitio principal a un sitio alternativo, brindando de esta manera confidencialidad, integridad y disponibilidad, el acceso de la información en las aplicaciones que se encuentran en el centro de datos por lo tanto el siguiente proyecto de investigación se centrara en empresas que utilizan un centro de datos, y sobre la continuidad del negocio, para que no se vean afectados por alguna amenaza o falla en los principales sistemas, en muchos de los sistemas se vuelve un gran problema por el costo en el mantenimiento, y la seguridad, para tratar de evitar interrupciones en la continuidad del negocio y el respaldo de toda su información.

## 1.2 Justificación

Las empresas de mantener de la información y cumplir con los requerimientos de la continuidad del negocio, se elaborará una metodología la cual permita mitigar y gestionar los riesgos que amenazan la continuidad del negocio para lo cual se desplegará un sitio alternativo, esto permitirá tener una alternativa viable si el Centro de Datos, llegara a fallar, ya sean estas por amenazas físicas, humanas, lógicas de un sistema, por lo tanto, uno de los principales inconvenientes principales dentro de un centro de datos, podría ser la de perder su funcionalidad o continuidad del servicio, las organizaciones se enfrentan a una difícil situación cuando se decide abordar cualquier iniciativa relacionada con la continuidad del negocio, la falta de instrucciones concisas que detallen por donde se puede empezar y tener en cuenta para la organización de las empresas sin que los datos se pierdan, los cuales pasarán a un sitio alternativo hasta que el servidor esté de nuevo en funcionalidad, los sistemas no tendrán degradaciones en los datos. por lo tanto se va a desarrollar una metodología BCP (Plan de Continuidad del Negocio) que viene siendo un conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos de negocio utilizando, utilizando Veeam Hyper-Availability Platform, dicha plataforma cuenta con las herramientas y servicios adecuados en el cual se podrá realizar el despliegue al sitio alternativo, deberá permanecer con una conmutación constante al Centro de Datos, de esta manera pueda permanecer en funcionamiento a pesar de amenazas o fallas, evitando una pérdida de la información; base fundamental para las organizaciones es que el Centro de Datos permanezca en funcionamiento permanente sin ninguna falla o amenaza teniendo desplegado un sitio alternativo con toda la información, de esta forma se evitará perder la continuidad de los servicios, y por lo tanto la información de suma importancia.

El desarrollo de la metodología deberá cumplir con los estándares y normas ISO 22301 la misma que menciona sobre la continuidad de los negocios para las empresas u

organizaciones, nos permitirá establecer un conocimiento para entender la continuidad del negocio, así como la de implementar políticas que permitan la continuidad de los servicios para que de una manera fácil y segura nos permita acreditar la conformidad y compromiso de una organización, en conjunto con prácticas internacionales de las mismas, protegiendo intereses propios de las organizaciones, su reputación ante la sociedad, y de una manera muy importante evitar pérdidas económicas y de esta forma brindar una mayor estabilidad a los usuarios.

## **1.3 Objetivos**

### **1.3.1 Objetivo General**

Desarrollar una metodología que permitirá realizar un despliegue de la información y sus aplicaciones críticas a un sitio alternativo con el fin de garantizar y permitir la continuidad del negocio de un Centro de Datos mediante la utilización de la plataforma Veeam Hyper-Availability Platform.

### **1.3.2 Objetivos Específicos**

- Desarrollar una metodología que permitirá ver la manera más óptima de crear un sitio alternativo para la continuación del servicio.
- Obtener conocimientos sobre la herramienta de Veeam Hyper-Availability Platform para la conmutación con un sitio alternativo.
- Desplegar un sitio alternativo que ayudará con la conmutación de la información de un Centro de Datos en situaciones adversas o fallas.



# CAPÍTULO II

## 2.1 Marco teórico

Los departamentos de TI tienen como objetivo garantizar la continuidad de servicio y aplicaciones críticas para los usuarios, como consecuencia de esta premisa hemos realizado la presente investigación, que consta del despliegue, implementación y pruebas del funcionamiento de un ecosistema integrado por un Hypervisor y un sistema de respaldo y replicación de información, por lo que es necesario poner en contexto los conceptos teóricos y técnicos que apoyen al lector a comprender el trabajo, por lo tanto explicaremos en el presente capítulo describiremos en detalle los términos de mayor relevancia en nuestra investigación.

### 2.1.1 Virtualización

La virtualización se ha convertido en una herramienta básica para la administración de los centros de datos modernos en el presente capítulo detallaremos los conceptos claves de esta tecnología.

La virtualización consiste en la creación de una o varias máquinas virtuales dentro de un ordenador físico o real, el mismo que permitirá mantener varios sistemas operativos en un mismo computador físico y puedan ejecutarse individualmente. Cada máquina virtual tiene su propio hardware virtual. De modo que, en una sola computadora física, se coordina el uso de sus recursos para que varios sistemas operativos puedan funcionar al mismo tiempo y de forma independiente. Además, sin que ellos detecten que están compartiendo recursos de la máquina con otros sistemas operativos.

### **2.1.1.1 Componentes de la virtualización.**

Dentro de los componentes de la virtualización podemos mencionar o dar a conocer que existen varios componentes que permitirán que cada una de las máquinas virtuales mediante el uso de un software, estos puedan absorber los diferentes recursos ya sean estos CPU, RAM, discos duros, y de esta manera poder crear servidores o cualquier tipo de ordenador. Es por eso que debe mantener una estructura que constara con el uso de sus recursos físicos según sean las diferentes necesidades de las empresas, ya que se podría decir que las máquinas virtuales utilizan o absorben los recursos de su ordenador físico, mientras que toda una estructura virtual está representada por los recursos físicos que mantendrán sus diferentes departamentos de TI, por la tanto podríamos dar conocer tres componentes principales de una estructura virtual:

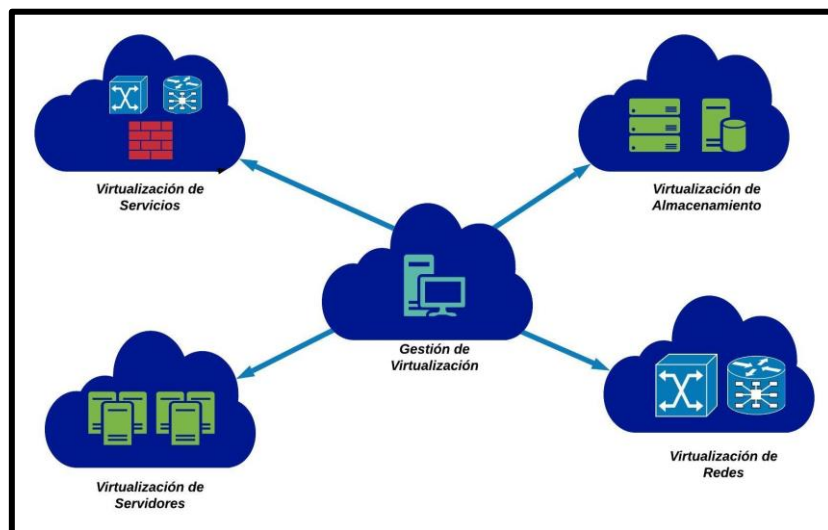
- Los Hipervisores de un nodo para la virtualización de todos los ordenadores.
- La totalidad de los servicios como la gestión de recursos los mismos que permitirán la optimización de los diferentes recursos entre las diferentes máquinas virtuales de una infraestructura virtual
- Soluciones para poder automatizar, solventar y optimizar los diferentes procesos, como una recuperación de desastres.

Con la utilización de estos componentes y otros sistemas básicos como podrían ser los diferentes servidores, que permitirá a las diferentes empresas mantener y crear una estructura virtual con características importantes como son la disponibilidad, automatización y flexibilidad, permitiendo unificar varios servidores, estructuras de almacenamiento y redes.

### 2.1.1.2 Tipos de virtualización

Dentro de la virtualización tenemos existen muchos usos y según su utilización se puede señalar cual es el tipo de virtualización, dentro de las virtualizaciones comunes se tiene:

- Virtualización de Servidores.
- Virtualización de Almacenamiento.
- Virtualización de Redes.
- Virtualización de Servicios.
- Virtualización de Memoria
- Virtualización de Software
- Virtualización de Escritorio



*Imagen 1. Tipos de Virtualización*

### **2.1.1.2.1 Virtualización de Servidores**

Se conoce también como virtualización de hardware, esto permite ejecutar múltiples máquinas virtuales en una única máquina física, compartiendo recursos a través de múltiples entornos de un mismo ordenador físico.

Cada máquina virtual está separada lógicamente de las demás, es decir que son independientes una de otra, de tal forma que cada máquina puede ejecutar su propio sistema operativo, así como sus aplicaciones como si fuera una máquina física, cada máquina virtual tiene el mismo funcionamiento de una máquina física con sus propios recursos como son CPU, RAM, disco duro, así como interfaces virtuales de red. Es decir que cada máquina virtual se considera un ordenador físico real.

Dentro de la virtualización de servidores podemos especificar que existen tres tipos de virtualización:

- Virtualización de Sistema Operativo

En esta virtualización se lo define como la virtualización completa de un sistema operativo, en la cuales se crearán varias instancias o entornos, en esta virtualización cada entorno o instancia tendrá su propio ambiente y de sus propios recursos configurados.

- Virtualización completa

El tipo completo se caracteriza por la virtualización completa de todo un hardware que se encuentra disponible dentro de un ordenador físico, esto permitirá que los paquetes de aplicaciones puedan ejecutarse tanto en el hardware nativo como las diferentes máquinas virtuales, también permitirán que al instalar cada uno de los sistemas operativos en cada máquina virtual no sufran ninguna modificación.

- **Paravirtualización**

Esta virtualización permitirá la simulación parcial de todo un hardware, así como la simulación de una gran parte de sus características, este tipo de virtualización proveerá grandes mejoras en el rendimiento a lo que la virtualización de servidores se trata en cuanto a otras soluciones existentes de la virtualización, esta técnica necesita de las modificaciones necesarias de los diferentes sistemas operativos a ser ejecutados en cada Hypervisor.

Existen varias características dentro de la virtualización de servidores que ayudaran al buen funcionamiento de cada uno de los servidores de cada una de los centros de datos de las empresas los mismos que son:

- **Compatibilidad**

Dentro de una máquina virtual se alojan el sistema operativo y sus aplicaciones, así como de sus componentes es así que todas las máquinas virtuales son compatibles con los sistemas operativos.

- **Aislamiento**

Cada una de las maquinas comparten recursos de un ordenador físico, pero como se ha mencionado anteriormente cada máquina virtual es lógicamente independiente una de otra, por lo tanto, si una falla las demás maquinas funcionarán correctamente.

- **Encapsulamiento**

Toda máquina virtual es un software que contiene recursos de hardware virtuales como son el sistema operativo y sus aplicaciones dentro de un software, por lo tanto, el encapsulamiento permite que las máquinas virtuales sean totalmente portátiles y su administración y gestión de una manera más adecuada y rápida. Es decir, un usuario puede mover una maquina a otro servidor como si se tratara de un archivo común o

también se puede copiar en un dispositivo de almacenamiento ya sea un dispositivo de bolsillo hasta un dispositivo de almacenamiento de red SAN.

- **Independencia de hardware**

Todas las máquinas virtuales son totalmente independientes de su ordenador físico, es decir cada máquina se la puede instalar y ejecutar con las configuraciones virtuales como son CPU, RAM, disco entre otras configuraciones y estas a su vez distintos sistemas operativos, fusionada con el encapsulamiento permitirán una movilidad de cada máquina sin que sus configuraciones sean afectadas.

- **Recursos**

Con la virtualización y la ejecución de varias máquinas en un ordenador o servidor, dejando atrás el modelo antiguo que trataba de tener un servicio por ordenador, permitiendo reducir recursos tanto económicos como físicos.

- **Reducción de Costos**

Con la virtualización de servidores y la utilización de menos recursos de hardware físicos y de espacio de infraestructura y con ello la reducción del consumo de la energía eléctrica permitirá a las empresas la reducción de costos en la adquisición de equipos y servicios básicos. Con la utilización de varias herramientas que permitirán la administración y gestión de un servidor de una manera centralizada y rápida, permitirá la utilización de menos personal para gestionar los recursos.

- **Disponibilidad de servicio y continuidad del negocio**

Los sistemas virtualizados permitirán realizar con gran seguridad y rapidez una migración de sus máquinas virtuales, y de igual manera realizar un respaldo de su centro de datos.

- **Flexibilidad**

Una máquina virtual en su entorno permitirá administrar sus recursos, así como recibir más recursos como son RAM o CPU, por lo tanto la flexibilidad de aumentar recursos si se dispone de los mismos en su host u ordenador físico.

#### **2.1.1.2.2 Virtualización de Almacenamiento**

En este tipo de virtualización permitirá tener una vista razonable de todo el almacenamiento mediante a la abstracción de la información o datos físicos de sus dispositivos de tal manera que los dispositivos les haga parecer que toda esa información está centralizada, proporcionando a los usuarios puedan acceder a su información almacenada sin preocuparse en donde se está gestionando o cómo se encuentra su información almacenada.

Esta virtualización se ejecuta en varios dispositivos identificando la capacidad de almacenamiento que tenga cada uno y estos pueden ser tanto de hardware como de software de tal manera que proporcione un almacenamiento fácil, rápido y confiable para el acceso a la información y sus datos.

Dentro de las opciones de esta virtualización de almacenamiento tenemos soluciones como las: Áreas de almacenamiento de red SAN, los discos independientes RAID, los almacenamientos conectados a la red NAS, NFS, AFS, GFS, iSCSI entre otros métodos de almacenamiento.

#### **2.1.1.2.3 Virtualización de Redes**

La virtualización de redes es la obtención y combinación de todos los recursos de red entregados tanto en hardware y software la misma que permitirá crear múltiples subredes de software para las distintas máquinas virtuales.

En la virtualización de redes se podrán administrar y gestionar redes basadas en software que permitirán mejorar la productividad en velocidad, confiabilidad, flexibilidad, escalabilidad y su vez en la producción y eficiencia de cada una de las empresas.

El objetivo de la virtualización de redes consiste en facilitar un uso compartido de recursos de redes eficaz, controlado y seguro para los usuarios y los sistemas.

Podemos mencionar a la VLAN es un claro ejemplo de la virtualización de redes ya que son las que permitirán realizar la segmentación de una red LAN, las VLANs están definidas en base a un puerto distinto y no existe la necesidad de que cada VLAN sean creadas contiguas ya que se tratan de una red lógica y no física, es decir que cada estación de trabajo no necesariamente debe estar ubicadas una a lado de otra.

Por otro lado, las Virtual IP que se las define como una dirección IP que no está conectada directamente a un ordenador físico o tarjeta de red del dispositivo, sino que son destinadas en dispositivos de una red que están ubicadas en la direcciones o caminos del tráfico de red. Su función principal es que todos los paquetes de datos se dirijan hacia la Virtual IP para luego ser redirigidos hacia las distintas interfaces de los dispositivos receptores de red.

Las VPN (Virtual Private Network) se la define con una red de comunicación privada que sirve para transmitir datos e información de una forma segura, completa y confiable de una red pública, toda la información es transmitida y transportada por un medio poco confiable inseguro que es el internet, para lo cual se crea un canal muy seguro para la información sensible que transmitida de un sitio a otro sitio

Dentro de la virtualización de las redes tenemos dos tipos que detallaremos a continuación:

- **Interna**

Dentro la virtualización de red interna se usa configuraciones que simulan una red física la misma que permitirá a las máquinas virtuales comunicarse con el ordenador físico.



- **Externa**

En la virtualización externa configurara herramientas físicas como adaptadores las mismas que servirán para combinar una o varias redes LAN con redes virtuales, mejorando la eficacia de una gran red del centro de datos.

Con los componentes claves de una red como el conmutador y las redes LAN los administradores podrán configurar y conectar a una red física varias redes virtuales separadas.

Dentro de las grandes empresas que permiten virtualizar las redes tenemos a Citrix y Vyatta que con la creación de protocolos combina varias funciones como son el enrutamiento, VPN, y firewall.

La virtualización de red permitirá a las empresas mejorar la seguridad y los tiempos en recuperar la información, escalamiento eficaz en los entornos de las TI, redes rápidas y eficientes en la entrega de tareas y solicitudes, y una reducción significativa en los costos de implementación.

#### **2.1.1.2.4 Virtualización de Servicios**

La virtualización de los servicios como tal está relacionada con servicios como un firewall para la seguridad, o las herramientas de balanceo de carga para el rendimiento de las aplicaciones dentro de un centro de datos, basados en la simulación de los comportamientos de las aplicaciones que no están disponibles o no se pueden acceder fácilmente presentando al mundo un servidor web, pero ocultándole los múltiples servidores por detrás de un proxy.

La interfaz virtual más conocida como una IP virtual, es la que representara a los servicios web con el mundo exterior, encargada de realizar y administrar las conexiones desde y hacia el servidor web permitiendo que el balanceo de carga administre varios entornos de servicios

web y lo muestre como un solo entorno, Esto permite que los usuarios accedan a los servicios web individualmente siendo una representación de una virtualización de uno a muchos.

#### **2.1.1.2.5 Virtualización de Memoria**

Este tipo de virtualización trata de alguna forma desvincular la memoria de los servidores la misma que será distribuida, compartida mediante una red. Esta virtualización mejorara el rendimiento para una mayor capacidad, evitando añadir más memoria física en caso de requerirlo. Esta tecnología tiene capacidad de mostrar todo el sistema físico en varios recursos siendo utilizada para consolidar varios entornos en un solo sistema con alta disponibilidad.

#### **2.1.1.2.6 Virtualización de Software.**

Esta técnica de virtualización tiene como característica principal la de proveer al equipo anfitrión la capacidad para la creación y ejecución de uno o varias máquinas virtuales con sus respectivas características, son utilizadas para permitir la creación de un entorno informático, y de esa manera permitirá la ejecución de sistemas operativos invitados, es decir esta técnica permitirá que un sistema operativo invitado Linux pueda ejecutarse en un sistema operativo Windows.

#### **2.1.1.2.7 Virtualización Escritorio.**

La virtualización de escritorio permitirá realizar un trabajo con facilidad y seguridad accediendo de una forma remota al ordenador o máquina virtual desde cualquier otra parte o computador físico, facilitará una mayor flexibilidad a realizar su trabajo desde casa u otro lugar, trabajaran de manera segura protegiendo los datos al mantenerlos en cada uno de los servidores.

Los distintos tipos existentes de virtualización permiten una configuración fácil de nuevos servidores virtuales que permitirá evitar la administración de varios servidores distintos. siendo esta una solución importante ya que permite tener el control de todo ya sean estos

recursos físicos y virtuales, ya que el administrador podrá ingresar a los servicios mediante un servidor central que permite tanto la entrada y la salida de la información entre el cliente y el servidor.

### **2.1.1.3 Ventajas y Desventajas de la Virtualización**

#### **2.1.1.3.1 Ventajas de la virtualización**

Algunas ventajas que puede ofrecer la virtualización son:

- Consolidación de las tareas de diferentes servidores con hardware subutilizado en un menor número de equipos.
- Ejecutar múltiples sistemas operativos de manera simultánea en un mismo equipo, incluso en aquellos en los que no podrían correr de forma normal, o sea en un equipo con bajas capacidades.
- Generar entornos de pruebas aisladas y seguros donde correr aplicaciones nuevas o no confiables.
- Emular recursos o dispositivos de hardware mediante software o presentar aquellos disponibles como algo diferente.
- Simplificar la administración de sistemas, al reducir los tiempos de clonado, migración e instalación de los mismos, por lo que se minimiza el tiempo de espera e independiza el hardware.

#### **2.1.1.3.2 Desventajas de la virtualización**

Dentro de las desventajas podríamos decir que:

- Dependencia de una solo equipo u ordenador físico perdiendo la ventaja de la redundancia.

- Su hardware será limitado ya que dependerá de la compatibilidad de los diferentes hipervisores.
- El hardware que será utilizado para la virtualización debe mantener recursos extensos elevando su precio.
- Según que configuren y unifiquen las máquinas virtuales sus recursos disminuyen aumentando el trabajo de administración y su seguridad.

### 2.1.2 Que es Hypervisor

Los Hypervisor son una tecnología que están compuestas por una capa de software que permitirán utilizar al mismo tiempo, diferentes sistemas operativos o máquinas virtuales en una misma computadora central. Es decir, es la parte principal de una máquina virtual que se encarga de manejar los recursos del sistema principal exportándolos a la máquina virtual.

#### 2.1.2.1 Tipos de Hypervisores

- **Tipo 1 hipervisor. También llamado metal desnudo o nativo.**

Un hipervisor simple (Tipo 1) es una capa de software que instalamos directamente sobre un servidor físico y su hardware subyacente.

No hay software ni ningún sistema operativo en el medio, de ahí el nombre de hipervisor simple. Por esta razón, los hipervisores de tipo 1 demostraron proporcionar un rendimiento y una estabilidad excelentes, ya que no se ejecutan dentro de Windows u otros sistemas operativos.

- **Tipo 2 hipervisor. También conocido como hipervisores alojados.**

Este tipo de hipervisor se ejecuta dentro de un sistema operativo de una máquina host física.

Es por esto que llamamos hipervisores alojados de hipervisores de tipo 2. A diferencia de los hipervisores de tipo 1 que se ejecutan directamente en el hardware, los hipervisores alojados tienen una capa de software debajo:

- Una máquina física.
- Un sistema operativo instalado en el hardware (Windows, Linux, MacOS).
- Un software de hipervisor de tipo 2 dentro de ese sistema operativo.
- Las instancias reales de máquinas virtuales invitadas.
- Los hipervisores de tipo 2 generalmente se encuentran en entornos con una pequeña cantidad de servidores

#### **2.1.2.2 Clasificación de Hypervisores**

- **Hypervisor Huésped**

En este tipo de Hypervisor la capa de virtualización se instala e inicia como una aplicación por encima del sistema operativo permitiendo un amplio número de configuraciones en su hardware. Es decir que estas máquinas son ejecutadas dentro un hardware anfitrión lo que permitirá que pueda supervisar el hardware y gestionar las diferentes máquinas virtuales.

Dentro de este tipo de Hypervisor encontramos los más comunes como lo son: VMware Workstation, VirtualBox de Oracle entre otros.

- **Hypervisor Nativa.**

En esta arquitectura se instala la capa de virtualización en el hardware físico en los sistemas operativos, accediendo directamente a todos los recursos del hardware, evitando que este pase por un sistema operativo, esta arquitectura es más eficaz que la arquitectura de huésped.

Dentro de este tipo encontramos diferentes hypervisores que utilizan esta tecnología moderna, aunque la más antigua de la virtualización por hardware y tomando en cuenta

las soluciones más potentes en la mayor parte de los fabricantes tenemos los siguientes hipervisores: Hyper-V de Microsoft, XEN Server de Citrix, VMWare ESX-SERVER.

- **Hypervisor Híbrida**

En esta arquitectura tanto el sistema operativo host como el Hypervisor se ejecutan directamente en el hardware físico, y sus máquinas virtuales se ejecutarán a un nivel más alto en relación al hardware, en un nivel superior al Hypervisor, y al igual que el sistema operativo y el Hypervisor las máquinas virtuales se relacionan directamente con el sistema operativo.

Esta arquitectura es usada por empresas o sistemas como: Virtual PC y Virtual Server de Microsoft, VirtualBox, VMWare Server

### **2.1.2.3 Ventajas de los Hypervisores**

- Dentro de las ventajas conocidas de los Hypervisores es de que cada uno tiene la capacidad de ejecutar uno o varios sistemas operativos un mismo hardware físico, por lo tanto, las empresas evitarán destinar presupuesto en la compra de varios equipos físicos.
- Una ventaja importante de las máquinas virtuales es la de permitir ejecutar varias de estas en un mismo hardware de una manera independiente cada una de otra, evitando que si una de estas máquinas tiene algún problema ya sean por fallas o ataques de virus, no afecten al resto. Es decir que por su separación lógica una de otra cualquier falla o ataque de una no permitirán que otras también fallen.
- Los Hypervisores o máquinas virtuales al ser independientes de su hardware adyacente les permiten ser móviles, es decir que cada una de las máquinas virtuales puedan ser ejecutadas en otra capa de virtualización o servidores virtualizados de una

forma remota y más fácil que otras aplicaciones que se encuentran en el hardware físico.

- Mejora la disponibilidad y la continuidad del negocio de las empresas tanto en sus aplicaciones como en sus servicios, de esta manera permitirá realizar migraciones y respaldos de todos los entornos virtualizados.
- La capa de virtualización permite una flexibilidad en sus operaciones permitiendo realizar cambios con el avance de la tecnología con un trabajo dinámico de todos los recursos y manteniendo una administración centralizada del centro de datos.

### **2.1.3 VMware**

VMware es una empresa encargada de optimizar y garantizar servicios como la virtualización y computación en la nube, siendo esta una de las principales empresas estadounidense en mantener éxito comercial en la virtualización de la arquitectura x86, tomando en cuenta que es un sistema de virtualización por software que sirve para simular un sistema físico, con características y configuraciones específicas como RAM, CPU, disco, ofreciendo a las diferentes organizaciones una transformación digital, permitiendo una mejor experiencia ya que cuentan con recursos informáticos, la nube, red y seguridad para sus diferentes servicios.

VMware siendo una empresa de EC Corporation la misma que proporciona los diferentes softwares de virtualización para ordenadores como VMware Server, VMware Player y VMware Workstation que son de forma gratuita. VMware está diseñada como multiplataforma, es decir para los sistemas operativos de Windows y Linux y para los entornos de Mac OS X corre con procesadores INTEL con el nombre de VMware Fusion.

### **2.1.3.1 Historia de VMware.**

VMware es una empresa creada en 1998 por Mendel Rosenblum, Diane Greene, Scott Devine, Edward Wang y Edouard Bugnion, Durante el primer año de su fundación VMware trabajo y opero de una manera reservada, manteniendo una nómina de 20 empleados hasta los finales del año 98. A principios del siguiente año VMware fue lanzada oficialmente en febrero de 1999, en una conferencia DEMO que fue organizada por Chris Shipley. Su primera producción fue entregada en mayo de 1999 la misma que fue VMware Workstation.

En el año 2001 VMware se adentró a los productos de servidores con productos como VMware GSX Server que era un sistema alojado, y VMware ESX Server era un sistema sin host.

En el año 2003, se realizó el lanzamiento de VMware Virtual Center impulsando el rendimiento y optimizando su administración y reduciendo costes, vMotion que permitió a varios clientes migrar datos y una carga de trabajos de un lugar a otro mientras las aplicaciones se encuentran ejecutándose, lo que hoy en día es una migración eficaz y una tecnología Virtual SMP, introducción un soporte de 64 bits en el año 2004.

A principios del 2004 Dell EMC adquirió la empresa con 625 millones en efectivo, en 2007 EMC vendió el 15% de sus acciones al público mediante una oferta convirtiéndose en una empresa global ya que se expandió a nivel internacional con una oficina europea en Frimley, permitiéndoles abrir varias oficinas en resto del mundo. Ese mismo año se realizó por primera vez un evento denominado VMWORLD convirtiéndose en el primer congreso sobre la virtualización e informática en la nube con cerca de 1400 participantes

En julio de 2008 la directiva de la empresa despidió a la cofundadora Diane Greene de la empresa luego de una administración financiera desastrosa siendo reemplazada por el veterano Paul Martiz quien trabajo en el departamento de negocios de EMC durante 14 años,



ese mismo año en septiembre VMware anuncio la colaboración con Cisco System obtenieod como resultado el conmutador de software distribuido Cisco Nexus 1000v.

En el 2011, VMware lanzo al mercado un sistema de plataforma con un código abierto denominado Cloud Foundry, siendo una aplicación compatible con Java, Ruby on Rails, Sinatra, Node.js, de la misma forma con un soporte de base de datos como MySQL, MongoDB, Redis, Postgres, RabbitMQ.

En 2013, se anunció spin-off corporativo de Pivotal Software realizado con General Electric en donde todos sus productos que estaban orientados a su aplicación en los cuales estaban incluidos Spring, tc Server, Cloud Foundry, RabbitMQ, GemFire y SQLFire, fueron transferidos a esta organización. Este mismo año fue promocionado su propio IaaS, vCloud Hybrid Service, en su nueva oficina en Palo Alto, en donde se anunció el acceso a un centro de datos en Las Vegas, en septiembre de 2013 luego de VMWorld que se lo realizado en San Francisco se anunció la disponibilidad de vCloud Hybrid Service en otras ciudades, de estados unidos y una versión beta en Reino Unido.

En 2016, VMware realizo el lanzamiento de VMware Workstation 12.5 y fusión 8.5 compatibles con Windows 10 y Windows server 2016.

### **2.1.3.2 VMware dentro del cuadrante de Gartner**

VMware es la compañía que ocupa una posición más avanzada en completar el eje de visión en el Cuadrante Mágico de Gartner Inc. de noviembre de 2019 por su Infraestructura hiperconvergente. Según Gartner, un Cuadrante Mágico de Gartner es “la culminación de la investigación en un mercado específico, lo que da una visión más amplia de las posiciones relativas de los competidores del mercado”. VMware también está en el cuadrante de Líderes del informe basado en la capacidad de ejecutar ejes.



Imagen 2. VMware en el Cuadrante de Gartner

VMware permitirá mediante sus sistemas de virtualización una mejor administración de los centros de datos, facilidad para la migración de datos, respaldos de la información, utilización al máximo de los recursos del ordenador o hardware físico. Es decir, VMware basa su tecnología y sus productos en herramientas de virtualización, seguridad, redes, centro de datos basados en software y almacenamiento.

Entre los avances más importantes en cuanto a la virtualización de software en los últimos años, debemos de remarcar el desarrollo de la virtualización mediante software de sistemas como VMware, vSphere y VMware ESXi entornos de virtualización profesional de la compañía líder en virtualización de todo tipo de sistema operativos y servidores.

Dentro de las diferentes tecnologías que VMware nos ofrece existe varios sistemas de forma gratuita como VMware WorkStation y VMware vSphere Hypervisor. Y por otro lado software comercial o de paga como: VMware vSphere, Site Recovery Manager, Data Protection, vCloud Suite.

### **2.1.3.3 Redes y Seguridad.**

Dentro de las configuraciones y productos creadas por VMware tenemos VMware NSX que fue creada para que los administradores pueden virtualizar componentes de red y conmutadores mediante la utilización de software y no hardware. La capa de software ubicada por encima del Hypervisor permitiendo la gestión y administración de una red física en varias redes virtuales.

La herramienta de administración VMware vRealize Network Insight permite a los administradores realizar una microsegmentación y a su vez verificar el estado VMware NSX, y es la encargada de recopilar toda la información de NSX, así como informa sobre los errores de interfaz de los usuarios y ayudando a solucionar los problemas de un entorno NSX.

### **2.1.3.4 Almacenamiento y disponibilidad.**

vSAN de VMware es una herramienta basada en software que está incorporada en el Hypervisor ESXi e incorporada con vSphere, la misma que agrupa en su espacio de disco varios host ESXi, proporcionando mediante políticas inteligentes límites de protección y borrado de códigos.

VMware Site Recovery Manager es una herramienta para la administración en la recuperación de desastres el mismo que permite a los administradores crear planes de recuperación que se ejecutarán en caso de fallas o bloqueos, los administradores podrán realizar las configuraciones para respaldar los datos mediante un failover y failback de las máquinas virtuales.

### 2.1.3.5 Tipos de entorno de virtualización

Dentro de cada uno de los diferentes entornos existen diferentes herramientas que sirven para mejorar el rendimiento, almacenamiento y continuidad de las activadas, tomando en cuenta la utilización de las diferentes aplicaciones o servicios, las mismas que cubren cada las diferentes necesidades de todos los usuarios tanto para la administración y gestión, por lo tanto a continuación daremos a conocer los diferentes entornos que permitirán ejecutar diferentes servicios o aplicaciones como: WEB, correo, Base de Datos entre otros servicios

- **VMware ESXi:** Es el sistema operativo Hypervisor en el que se apoya vSphere.
- **vCenter Server:** Herramienta cliente para gestionar las entornos o infraestructura de virtualización con máquinas virtuales de forma remota.
- **Update Manager:** Herramienta de actualización.
- **vShield Zones:** Escudo de protección para ataques maliciosos a las máquinas virtuales.
- **vRealize Operations:** Conjunto de herramientas para automatizar procesos TI en los servidores virtualizados.
- **vSphere Integrated Containers:** Conjunto de herramientas orientada a facilitar el rendimiento de máquinas virtuales en entornos de producción donde se prevén grandes cargas de trabajo.

### 2.1.3.6 VMware vSphere

Esta herramienta de virtualización es la numero uno de todas las tecnologías de virtualización, esta técnica permitirá y entregara a los usuarios los recursos suficientes para que puedan virtualizar los servicios y aplicaciones de una forma segura y confiable, aumentando el tiempo de funcionalidad de los servicios en los diferentes sistemas, de esta

manera los departamentos de las TI disminuirán notablemente la forma en que sus administradores ejecutan los diferentes centros de datos, siendo la base principal.

vSphere siendo la base principal de la virtualización y de los centros de datos ofrece de manera segura una flexibilidad para la eficacia de las actividades y de sus servicios de igual manera brindará compatibilidad en todas las cargas de trabajo, y por otro lado se ajustará a las necesidades según el avance de su tecnología e infraestructura.

Con la utilización de esta tecnología los diferentes centros de datos tendrán la oportunidad de virtualizar todas sus aplicaciones con facilidad y confianza, ya que este software ofrece una gran disponibilidad, rendimiento y escalabilidad para la virtualización de sus aplicaciones, de esta manera se simplificará la administración en los centros de datos mediante herramientas poderosas que permitirán una administración completa de máquinas virtuales, por otro lado permitirá la migración de datos en caliente y así como el mantenimiento de los entornos, y mediante estas características en la utilización de este software de virtualización permitirá reducir al máximo los costes de implementación

A diferencia de vSphere, VMware vSphere Hypervisor se trata solamente de un Hypervisor nativo capaz de virtualizar servidores y centros de datos. vSphere Hypervisor corre sobre el sistema operativo ESXi, al igual que la suite principal y lo más importante que es un Hypervisor que podremos adquirir de forma gratuita, algo realmente destacable e interesante. Esta herramienta también se podrá gestionar mediante vCenter a través de acceso remoto.

#### **2.1.3.6.1 VMware vSphere Hypervisor.**

Dentro de la definición de este Hypervisor que también se le conoce como un Hypervisor ESXi free, ya que permitirá virtualizar los diferentes servidores de una manera gratuita y a

los diferentes clientes fijar o afianzar sus diferentes aplicaciones ahorrando recursos económicos y el tiempo en la administración de sus recursos dentro de los entornos de las TI que permitirá realizar tareas de una manera rápida y eficaz, mediante una arquitectura pequeña y fuerte logrando un gran rendimiento, haciéndolo diferente a los demás Hypervisores.

VMware vSphere Hypervisor no posee de algunas de las características importantes que un Hypervisor ESXi en su versión completa, pero este Hypervisor en su pequeña y consolidada arquitectura posee características como:

- Una gestión de las diferentes máquinas virtuales las mismas que nos permitirán la creación y distribución de las diferentes máquinas virtuales.
- Asignación eficaz de almacenamiento las misma que asignará los diferentes recursos para un almacenamiento el cual permitirá obtener un almacenamiento mucho más que el almacenamiento físico.
- Un avanzado recursos de la memoria el mismo que permitirá una asignación eficiente de memoria y a su vez permitirá optimizar el rendimiento.
- Una compatibilidad de hardware de los diferentes proveedores que permitirán optimizar el rendimiento y fiabilidad.

### **2.1.3.7 VMware ESXi**

ESXi es la herramienta de VMware cuya función es la de hypervisor, esta viene en dos versiones la comunitaria tiene un conjunto de restricciones como:

- No puede administrar a través de vCenter Server
- Solo se permite 1 servidor físico (no se permite el clúster con más servidores físicos)
- Solo se permiten 2 CPU físicas por hipervisor

- Solo se permiten 128 vCPU por hipervisor
- La cantidad máxima de CPU virtuales que puede asignar a una máquina virtual está limitada a 8
- Se permite un límite de RAM física de 12 TB por hipervisor
- Necesita adquirir soporte de VM

Con la versión paga de ESXi no tiene restricciones salvo el caso de pagar una licencia Standard de ESXi a 939 € según la web de VMware y la licencia Enterprise Plus a 3305 €.

	HIPERVISOR VSPHERE GRATUITO	HIPERVISOR VSPHERE PAGADO
<b>Vencimiento</b>	Sin límites de tiempo en la versión gratuita	No aplica
<b>Tiempo de evaluación</b>	Prueba de 60 días de las funciones de Enterprise Plus	No aplica
<b>Soporte comunitario</b>	Foros de VMTN	Foros de VMTN
<b>CPU físicas máximas</b>	2	768 (lógico)
<b>Memoria física máxima</b>	16 TB	16 TB
<b>Máximo de CPU virtuales por máquina virtual</b>	8 CPU virtuales	256 CPU virtuales
<b>VRAM máximo por máquina virtual</b>	6 TB	6 TB
<b>Soporte oficial</b>	No	Varios SLA disponibles
<b>Administración central (vCenter)</b>	No	Soportado
<b>Alta disponibilidad (HA)</b>	No	Soportado
<b>Uso de la API de almacenamiento / copia de seguridad (VADP)</b>	No	si
<b>Migración en vivo de máquinas virtuales (vMotion)</b>	No	Soportado
<b>Equilibrio de carga de máquinas virtuales (DRS)</b>	No	Soportado

*Tabla 1. Cuadro comparativo de vShare ESXi*

También permite realizar particiones en su hardware fácilmente para fijar las diferentes aplicaciones y reducir los costos de su implementación, siendo de una solución eficiente

debido a su arquitectura plasmando en los entornos mayor confianza, administración y gestión de los diferentes recursos utilizados en la virtualización por hardware del host. Dentro de este sistema operativo Hypervisor, podremos crear y ejecutar otros sistemas operativos totalmente independientes.

La principal característica de este sistema Hypervisor es precisamente que, al estar directamente instalado en un servidor físico, utiliza el hardware disponible en él para repartirlo entre las máquinas virtuales que en él están instaladas.

<b>REQUERIMIENTOS ESXi</b>
CPU de 2 núcleos
Procesador x86 de 64 bits
Memoria RAM de 8GB
Virtualización de (Intel VT-x o RVI AMD) en CPU x64.
Controladoras Gigabit o Ethernet
ESXi 6.7.0 requiere un disco de arranque de al menos 8 GB para dispositivos USB, y 32 GB para otros tipos de dispositivos.
Disco SCSI con espacio no particionado para las máquinas virtuales.
Para la serie ATA (SATA)

*Tabla 2. Requerimiento de ESXi*

Se ejecuta bajo un sistema operativo de Linux diseñado mediante Red Hat Enterprise Linux, que fue configurado y mejorado para la ejecución del Hypervisor y herramientas de virtualización de VMware las mismas que permitirán la consolidación del hardware mejorando la capacidad en proyectos más complejos, y de esta manera aumentar el rendimiento de los diferentes sistemas permitiendo una importante ventaja al optimizar la gestión y administración de una manera centralizada reduciendo al máximo la inversión y gastos económicos.



### **2.1.3.7.1 Características**

- Un formato más compacto con un espacio de 150 MB, esto permitirá hacer varias tareas a la vez y a su vez esto reducirá las amenazas en lo que a seguridad conc9erne en el Hypervisor.
- Un rendimiento fiable en al cual se podrá configurar máquinas virtuales con características que podrían ser de hasta 6 TB de memoria RAM, 128 CPU y una gran cantidad de dispositivos con una gran capacidad en el rendimiento de las diferentes aplicaciones de cualquier tamaño y de esa manera satisfacer las necesidades.
- Una seguridad mejorada que protegerá los diferentes datos de las máquinas virtuales con un acceso que se basa en funciones simplificando la administración, y de esta manera garantizando una mayor eficiencia en los procesos y tareas.
- Una excelente compatibilidad con los diferentes proveedores de hardware con son los diferentes sistemas operativos, servicios tecnológicos, aplicaciones, instaladas y ejecutadas para el uso de sus clientes.
- Una experiencia optima en la utilización de las diferentes plataformas mediante una interfaz sencilla y actual que permitirá a los diferentes clientes automatizar sus tareas y aplicaciones.

### **2.1.3.8 VMware VCenter Server**

Dentro de las diferentes empresas y con el pasar del tiempo y el avance de la tecnología se enfrentan a situaciones cada vez más complicadas para solventar y administrar los diferentes entornos virtualizados e infraestructura para la administración de las TI a un bajo costo y de esa manera cumplir y satisfacer las diferentes necesidades para sus aplicaciones por lo que la gestión centralizada de su infraestructura de virtualización de cada una de las empresas

permitirán que cada uno de los diferentes departamentos de TI garantizar la disponibilidad de las necesidades del negocio.

Asigna una plataforma de forma centralizada la misma que se encargara de gestionar y administrar toda una infraestructura virtual dentro de los entornos VSphere, proporcionando a todo el personal encargado de la administración d las TI tener un control eficiente y sencillo de todos los entornos virtuales y encargados de distribuir toda una infraestructura permitiendo corregir todos aquellos problemas relacionados con la rapidez, acompañada de una máxima seguridad y disponibilidad a todos los entornos.

No es más que una solución para los administradores de las TI sobre las configuraciones de los diferentes componentes de una infraestructura virtual para gestionar y administrar entornos VSphere desde una sola consola garantizando una alta disponibilidad y seguridad en el funcionamiento de los servicios, de esta manera se reducirá la administración y facilitará las diferentes tareas en los entornos virtualizados.

#### **2.1.3.8.1 Características**

Dispone de algunas características importantes que permitirán una gestión centralizada permitiendo realizar las diferentes configuraciones de cada uno de los componentes como por ejemplo la creación y administración de switches virtuales en las diferentes infraestructuras virtuales que detallaremos a continuación.

- VMware VCenter Server client basado en HTML 5 ofrecerá a los usuarios y administradores una funcionalidad que permitirá facilitar la gestión de los diferentes componentes y sus configuraciones.
- vCenter server single Sign-On reducirá su administración donde permitirá a los usuarios a iniciar sesión una vez en un entorno y a su vez le permitirán ingresar a todas las configuraciones de vCenter server sin volver a iniciar sesión otra vez.

- Acceso al inventario de vCenter server tales como máquinas virtuales, hosts, datos y redes.
- Alertas y notificaciones las mismas que permitirán advertir y prevenir problemas en los diferentes entornos utilizando parámetros y eventos para notificar y notificar a los almacenes de datos y las diferentes máquinas virtuales a los diferentes flujos de trabajo.
- Copias de seguridad y restauración de los servicios que permitirán copiar archivos y listas que serán utilizadas de manera inmediata mediante una interfaz rápida y eficaz eliminando las copias de seguridad de otras personas o empresas para la seguridad y protección de vCenter server.
- Planificar las copias de seguridad y sus restauraciones utilizando las API de REST para planificar los diferentes procesos para realizar las copias de seguridad y saber el número de copias obtenidas manteniendo la seguridad de la infraestructura.
- Herramientas de migración que permitirá la migración de todos los datos desde la activación de vCenter Server 5.5 o 6.0 compatible con Windows y para la actualización de vCenter Server Appliance.
- vCenter Server High Availability que permitirá un tiempo de recuperación no mayor a 10 minutos permitiendo la alta disponibilidad de todos sus servicios.
- Permitirá la configuración y la gestión de hosts simples bajo estándares de los Hypervisores ESXi en los que incluirá configuraciones de red, almacenamiento, seguridad para ser implementados en los directos entornos virtualizados evitando el proceso de configuración de cada uno.
- Gestionar los recursos para los diferentes entornos virtuales como procesador y memoria para cada una de las máquinas virtuales ejecutadas en un mismo servidor físico estableciendo un mínimo y máximo de recursos para cada entorno como son

CPU, memoria, disco y el ancho de banda, y a su vez permitirá editar cada una de las configuraciones mientras cada máquina se ejecuta optimizando el rendimiento.

- La asignación dinámica de cada uno de los recursos a vCenter Server el cual supervisara cada uno de los recursos disponibles y los suministrara de una manera fácil e inteligente a cada una de las máquinas virtuales mediante el uso de procesos que permitirán reflejar cada una de las necesidades de las empresas teniendo como resultado un eficiente, sofisticado, automatizado y eficaz equilibrio en el uso de los diferentes servicios y en su carga.
- Una interfaz de gestión sencilla para los usuarios que permitirán la gestión de los diferentes recursos como red, base de datos, espacio disponible de disco, así como las diferentes estadísticas de los componentes para la realización de las diferentes tareas operativas y gestión.

### **2.1.3.9 vCenter Server**

Es un servicio que funciona sobre una máquina virtual y que permite gestionarlo todo de una forma totalmente centralizada. Esta máquina se encuentra configurada y lista para poder ser importada en un entorno ESXi, y este a su vez permitirá optimizar el buen funcionamiento en la ejecución de vCenter Server, su costo es menor ya que no necesita de una licencia de Windows.

Con una base de datos vPostgres dentro de sus sistemas de VMware teniendo el control total de todo el software significando una optimización para todos los entornos vSphere por lo que en las versiones más actualizadas alcanzaran hasta 2000 hosts y un aproximando de 35,000 maquina virtual.

### 2.1.3.10 vSAN

vSAN es un software de virtualización del almacenamiento de nivel empresarial que, cuando se combina con vSphere, permite gestionar los recursos informáticos y el almacenamiento con una única plataforma. Puede reducir la complejidad y los costes asociados al almacenamiento tradicional y tomar el camino más sencillo hacia la infraestructura hiperconvergente y la nube híbrida. Evoluciona hacia una solución integrada de infraestructura hiperconvergente (HCI) con vSAN para mejorar la agilidad empresarial y, al mismo tiempo, agilizar las operaciones y reducir los costes.

Con la utilización de VMware vSAN permitirá tener un ahorro en el montaje de una infraestructura de almacenamiento para las diferentes empresas permitiendo tener un alto rendimiento permitiendo equiparar el almacenamiento de todos los entornos o servidores de un solo cluster y a su vez poder monitorearlo en redes vSphere.

#### 2.1.3.10.1 Ventajas de vSAN

- **Facilidad de Uso.** Al ser hiperconvergente se lo puede gestionar y administrar desde un sitio local único, por lo que se lo podría administrar desde un vCenter sus características principales como su almacenamiento y procesamiento.
- **Alta Disponibilidad.** Mantiene un almacenamiento compartido con los entornos o servidores En la infraestructura que no poseen SAN por lo que en su configuración e necesaria la alta disponibilidad.
- **Rendimiento.** Debido a su configuración y arquitectura de discos SSD y a su partición en diferentes discos permite el máximo en su rendimiento sin consumir recursos.

- **Escalabilidad.** Mediante sus avances vSAN permite escalar en su número de host de 3 a 64 y a su vez aumentara la capacidad de funcionamiento, capacidad en el proceso y otras características importantes.
- **Continuidad del negocio.** Dentro de sus configuraciones y mediante una réplica se la podrá integrar con soluciones como Site Recovery Manager de esta manera permitirá mantener una continuidad en el negocio.

#### **2.1.4 Centro de Datos**

Un centro de datos son espacios físicos destinados al almacenamiento, procesamiento, administración y difusión de la información de una o varias organizaciones, almacenaran las aplicaciones o sistemas más críticos de una red siendo la seguridad, confidencialidad y la disponibilidad de la información un factor primordial para la continuidad de las operaciones de las empresas, puede ser accesible desde cualquier punto, donde mantienen y operan sus infraestructuras TI.

Dispone de varios componentes que permitirán mantener la seguridad de la información creando o configurando redes virtuales a un nivel interno de los mismos y de la instalación y configuración de firewall o cortafuegos de una manera externa impidiendo de esta manera el ingreso de amenazas tecnológicas o ataques a sus sistemas y servicios. Algunas empresas disponen de un aula o de solo uno o varios racks, mientras que otras pueden disponer de salas privadas para alojar un número determinado de armarios rack, dependiendo del tamaño de la empresa, proporciona un espacio preparado con suelo falso por el cual se instalan tomas eléctricas para conectar los bastidores.

Por otro lado, todos los servidores que se encuentran en el centro de datos son de diferentes características ya que deben mantener y sustentar diferentes necesidades como pueden ser la instalación de varios sistemas operativos para le alojamientos y procesamiento de la

información de las diferentes bases de datos o como para una gran cantidad de almacenamiento de información, así como la ejecución de varias aplicaciones críticas de una empresa.

El control de clima es esencial para mantener los parámetros de temperatura y humedad correctos que garantiza el correcto funcionamiento y la integridad operativa de los sistemas alojados. Para ello, los centros de datos cuentan con sistemas de alimentación eléctrica, alimentación de reserva, refrigeración, cableado, detección y extinción de incendios, detectores de fugas de agua y controles de seguridad.

Las arquitecturas y requerimientos de un centro de datos pueden ser distintas ya que pueden cambiar según su funcionalidad y objetivos a cumplir por ejemplo podríamos decir que para la creación de servicios en la nube con VMware, se mantendrá varios requerimientos para su instalación, infraestructura, y seguridad ya que son propias de un centro de datos totalmente privado, y por otro lado la de alguna organización que solo priorizara la protección de algunos de sus datos que son clasificados.

La integración de la plataforma Veeam con el centro de datos se puede definir como la encargada de la recuperación de la información de alta velocidad, prevenir la pérdida de la información que se encuentra en el centro de datos, así como la de aplicaciones críticas o servicios, permitiendo de esta manera la mitigación de riesgos y contar con los datos cuando se los necesite, permite la administración de la información así como la recuperación y restauración de los diferentes sistemas y servicios mediante sus planes de recuperación de desastres o Backups, asegurando de esta manera la disponibilidad, visibilidad y automatización de los centros de datos.

## 2.2 Microsoft Azure

Microsoft Azure es una nube pública de pago por uso que te permite compilar, implementar y administrar rápidamente aplicaciones en una red global de centros de datos de Microsoft, existen diferentes servicios de infraestructura y de plataforma para montar los servicios que se necesitan de manera sencilla, sólo se debe elegir la región de los centros de datos donde estará el servicio y el tipo de servicio con sus características. En este proceso de creación, se define un nombre de usuario y contraseña específica para poder iniciar sesión en esta máquina virtual.

Entre los servicios que ofrece se cuenta con infraestructuras (IaaS: almacenamiento, redes, máquinas virtuales) y plataformas (PaaS: bases de datos de alta disponibilidad SQL, CMS para desarrollo de web, backend para aplicaciones móviles). Son compatibles con todo tipo de tecnología: bases de datos Oracle, Linux, php, iOS, MySQL, Android, php, etc.

Estos servicios están garantizados con una disponibilidad del 99.99%, y en caso de fallo, Microsoft se compromete a indemnizar por los daños. Además, cuenta con todas las certificaciones en seguridad y protección de datos.

Es una solución empresarial gestiona las infraestructuras y aplicaciones, presenta grandes ventajas. Con Azure no es necesario la inversión en máquinas físicas y el mantenimiento que conllevan. De esta manera, se simplifica el despliegue, se agiliza el proceso de configuración y permite adaptar sistemas a las necesidades en pocos minutos, con total flexibilidad. Además, dispone de herramientas para poder monitorizar el rendimiento y si es necesario se puede escalar o no las máquinas, solo se paga por lo que realmente se necesita.

También se recomienda como solución de backup o site recovery (continuidad de negocio) por la seguridad extra que aporta a la información de la empresa a un precio muy competitivo.



La visión de la nube de Azure parece estar orientada al mundo empresarial, tanto aquellas corporaciones de mayor tamaño como a las pequeñas y medianas empresas. Por ello, la mayoría de servicios son escalables y son capaces de responder a necesidades generales del mismo modo que a necesidades más particulares.

### 2.2.1 Herramientas y Servicios de Microsoft Azure

- **Servicios para móviles:** Creación, desarrollo y gestión de aplicaciones para distintos sistemas operativos móviles, con diferentes lenguajes de programación disponibles.
- **Almacenamiento:** Diferentes tipos de almacenamiento (SQL, BLOBs, tablas, etc.) para diferentes formatos de archivos o estructuras de almacenaje. También como almacenamiento de los datos de aplicaciones y programas empresariales.
- **Herramientas de seguridad:** Protocolos, herramientas y opciones complementarias para aumentar la seguridad de sus datos y aplicaciones locales o en la nube. Creación de sistemas de autenticación en varios pasos, recuperación ante desastres mediante copias de seguridad, etc.
- **Flujos de trabajo:** Procesos de automatización y optimización de flujos de trabajo, tareas y procesos internos de la empresa. Tareas automatizadas a través de Azure y servicios complementarios.
- **Máquinas virtuales:** Creación, administración y gestión de máquinas virtuales, con gran cantidad de imágenes a elegir en Azure Marketplace.
- **Business Intelligence:** Recolección y gestión de grandes cantidades de datos para análisis e informes internos. Herramientas de análisis y previsión empresarial.
- **Servicios multimedia y retransmisión:** Envío y recepción de audio y vídeo, retransmisión a gran escala tanto en directo como con programación pregrabada.

- **Redes híbridas y redes privadas:** Gestión y creación de redes híbridas y privadas, conexión de aplicaciones empresariales entre distintas redes, ampliación o modificación de la infraestructura interna de la empresa.

Todo lo que se trabaja en entorno local, ahora se gestiona en la nube. Esto supone un ahorro de costos (implementación, mantenimiento, electricidad, etc.) todo esto se alojado en los centros de datos de Microsoft con todas las certificaciones de seguridad y los mejores acuerdos de servicio.

Actualmente cuentan con más de 50 centros de datos repartidos por todo el mundo. Con ello, aseguran al cliente una disponibilidad total y una menor latencia con respecto a otros fabricantes.

Al ser un servicio de pago por uso, se adapta a las necesidades del usuario siendo escalable en tiempo real, tao en cantidad como en aumento del rendimiento.

## 2.3 Diagrama de Flujo

### Proceso de Instalacion



Imagen 3. Proceso de Instalación

# Proceso de Configuración

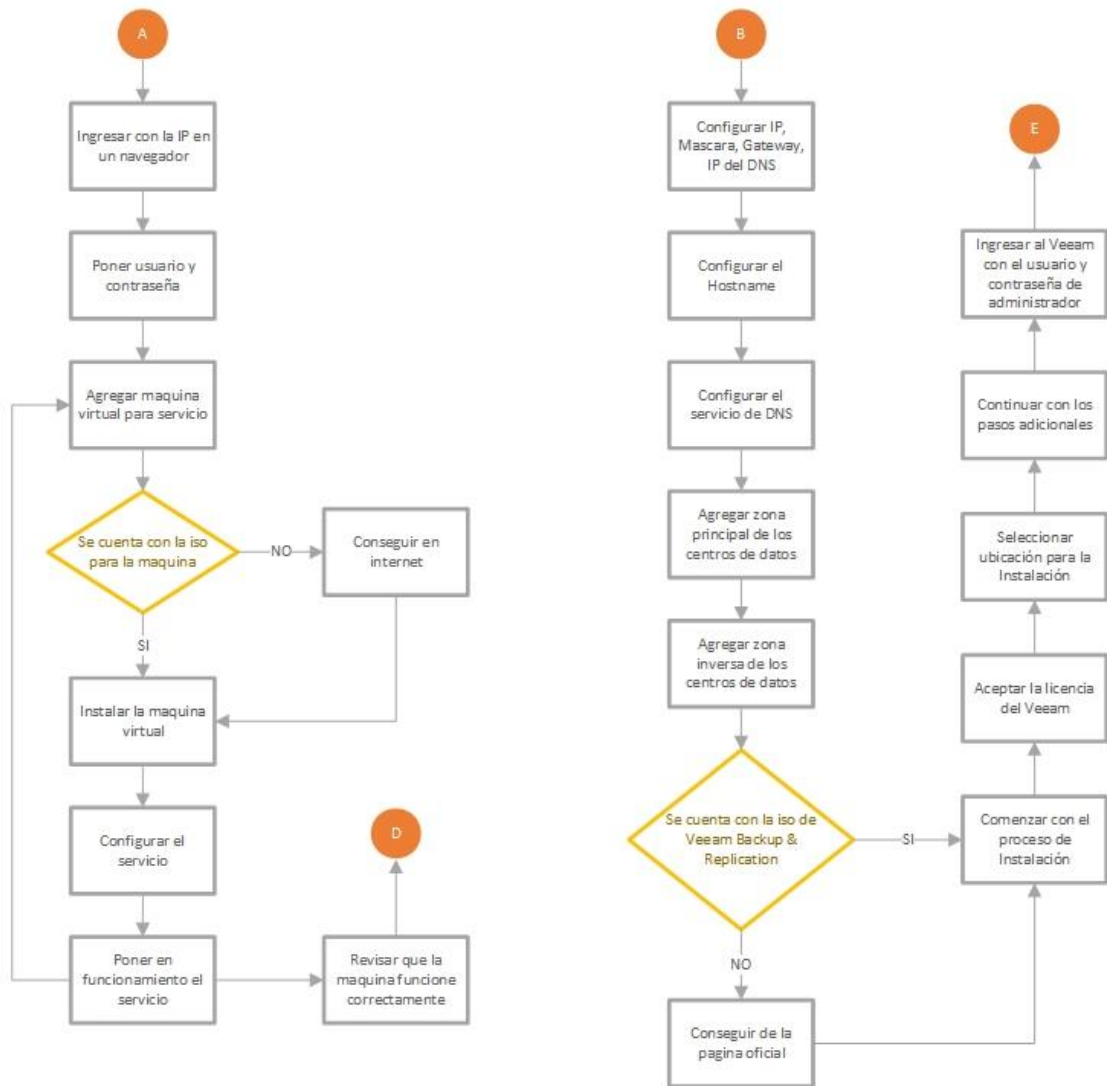


Imagen 4. Proceso de Instalación

## Proceso de Replicación y Plan de Continuidad del negocio

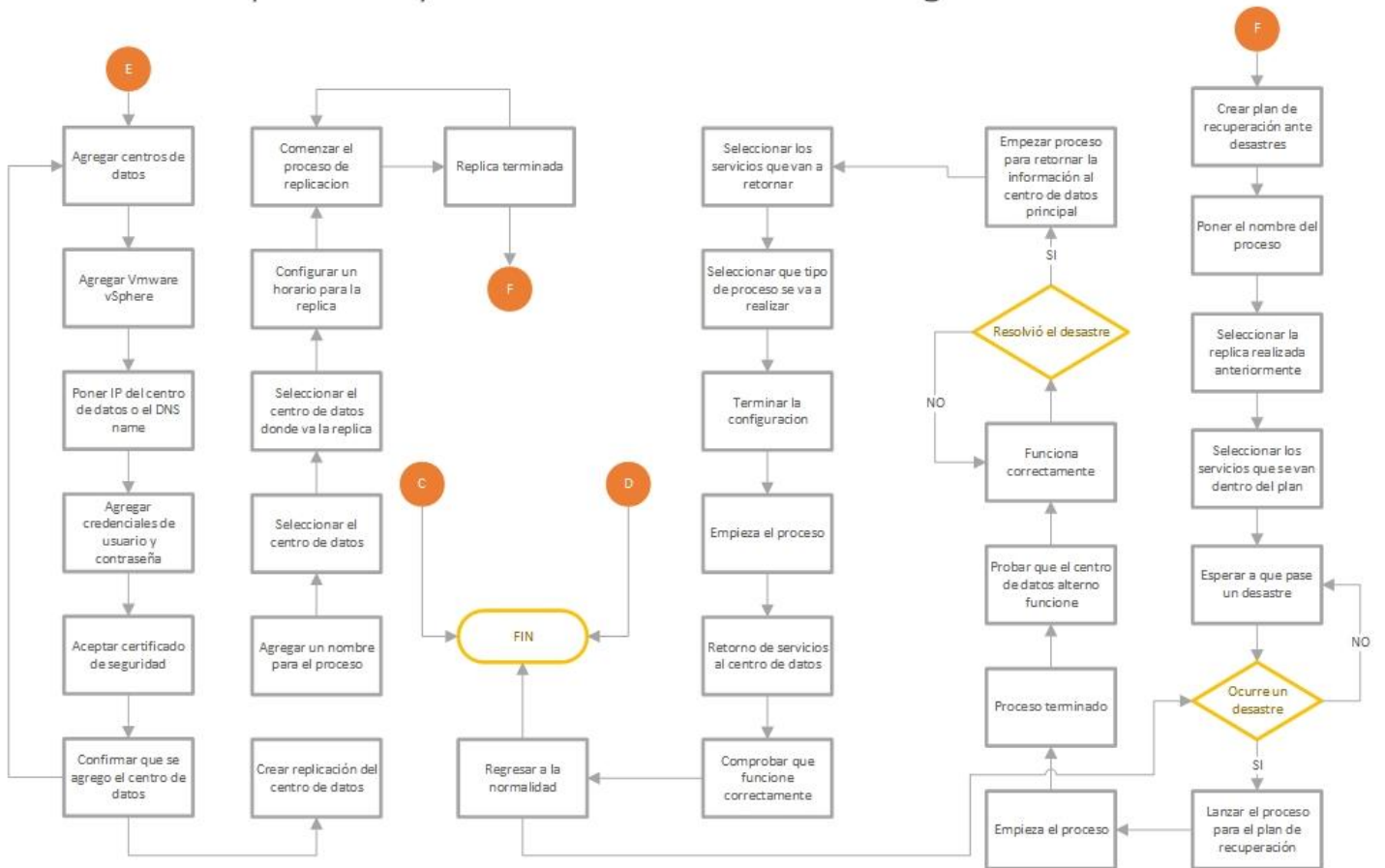


Imagen 5. Proceso de replicación y Plan de continuidad del negocio

# CAPITULO III

## 3. Reseña Histórica Veeam.

Veeam Software una empresa del área de las tecnologías de la información, está centrada en el desarrollo de software para virtualización, sus entornos están basados en copias de seguridad (Backup) y planes para la recuperación ante desastres, para ambientes virtuales como VMware y Hyper-V.

Veeam fue creada en el año 2006 por Ratmir Timashev y Andrei Boronov luego de vender su antigua empresa, Aelita Software Corporation, dentro del su primera producción que desarrollo Veeam fueron Veeam Monitor y Veeam Reporter, herramientas que sirvieron para el monitoreo, desarrollo de informes, y administración de los entornos virtuales.

Veeam en el 2007 tuvo un gran reconocimiento por el lanzamiento de su producto gratuito para las copias de seguridad de las máquinas virtuales FastSCP, el mismo que fue una parte esencial para la creación de un software que permitiría mantener la seguridad de los datos en la virtualización de hardware.

En el año 2008 Veeam desarrollo su primer software para realizar la replicación y copia de seguridad de la información Backup y Replication. La empresa Veeam consiguió adquirir en 2008 nworks que le ayudo en el desarrollo, integración y administración de varios entornos VMware y con varias plataformas empresariales de Microsoft y Hewlett-Packard, teniendo como resultado productos como:

- **Veeam nworks Management Pack** para entornos VMware, permitiendo a los clientes agregar la administración del entorno de VMware en un System Center Operations Manager de Microsoft
- **Veeam nworks Smart Plug-in** para entornos VMware el mismo que facilita a los usuarios agregar de manera directa la administración del entorno VMware en un producto HP OpenView.

En 2014 la empresa realizo su primera conferencia de protección de datos VeeamON, que tuvo lugar en Las Vegas. Ese mismo año la empresa Veeam tuvo un reconocimiento por ser una de las compañías más innovadoras en el cuadrante de Gartner, en donde se encuentran todas las empresas dedicadas al desarrollo de software que realizan copias de seguridad y recuperación. En 2015 la empresa ya con 2000 empleados logra establecer su empresa en Baar, Suiza, y luego con sedes internacionales en todo el mundo.

Durante los años que esta empresa está en el mercado ha sido catalogada como una de las empresas más innovadoras en dar soluciones a las empresas con las necesidades de la tecnología de datos moderna obteniendo los puntajes más altos en cubrir todas las demandas en la industria

### **3.1 Veeam**

Los centros de datos modernos requieren de la implementación de un plan de recuperación ante desastres (DRP por sus siglas en ingles), por lo tanto, es necesario contar con las herramientas que habiliten a los sistemas operativos, entornos de desarrollo, kubernetes, docker, DEVOPS contar con características de alta disponibilidad, replicación, copias de seguridad, por lo que luego de realizar una investigación de los software disponibles en el mercado que cumplan con estas necesidades hemos optado por Veeam.

Veeam cumple con los requerimientos demandados por los centros de datos, a un bajo costo, alto rendimiento y una interfaz amigable, así mismo existe dos versiones, la empresarial y la comunitario siendo la primera con costo y la segunda con capacidades reducidas que cumple con las demandas presentes y futuras de los centros de datos. Además, Veeam ha creado una nueva serie de soluciones para garantizar la continuidad de funcionamiento de los centros de datos y todos los servicios críticos de una empresa.

### **3.1.1 Veeam Backup & Replication**

Proporciona un conjunto de características para construir y mantener una copia de seguridad de los centros de datos, realizar tareas de protección de datos (copias de seguridad y replicación periódicas de máquinas virtuales), realización de procedimientos de recuperación ante desastres.

Veeam Backup & Replication es una solución de disponibilidad, protección de datos y recuperación ante desastres para entornos virtuales VMware, vSphere, Hyper-V, Nutanix, además de la integración con la nube privadas como Azure y Amazon. Para proporcionar la protección más completa de su infraestructura virtual, Veeam Backup & Replication complementa una copia de seguridad basada en imágenes y replicación basada en imágenes. Se puede hacer una copia de seguridad de cualquier VM, contenedor VM o disco VM, así como replicar VM en el sitio para alta disponibilidad (HA) o fuera del sitio para recuperación ante desastres (DR), en redes de área local y de área amplia.

Al aprovechar los últimos avances tecnológicos de virtualización, Veeam Backup & Replication ofrece una velocidad de replicación muy alta. Proporciona protección de datos casi continua a una fracción del costo de los sistemas CDP tradicionales: puedes capturar cambios y actualizar las imágenes VMs cada cierto tiempo, ya que el trabajo de replicación se puede configurar para ejecutarse continuamente.

#### **3.1.1.1 Características de Veeam Backup & Replication**

- Restablecer una máquina virtual fallida, lo que reduce al mínimo el tiempo de inactividad de las máquinas virtuales.
- Verifica la capacidad de recuperación de cada copia de seguridad y realiza una prueba de máquinas virtuales directamente desde las copias de seguridad de máquinas virtuales en un entorno controlado.



- Restaura elementos de cualquier aplicación virtualizada con Veeam Explorers y U-AIR.
- Restaura los archivos del sistema operativo invitado con la recuperación de nivel de archivo de múltiples sistemas operativos.

### **3.2. Veeam Availability Suite**

El entorno empresarial es para el acceso a la información y aplicaciones en cualquier momento y desde cualquier dispositivo, sin tolerancia al tiempo de inactividad o pérdida de datos. Por lo tanto, las organizaciones de TI deben crear datos y aplicaciones. disponible para todos los interesados cada minuto de cada día. Esta es la era de los negocios siempre activos.

Lograr un servicio continuo y una protección continua ha requerido tradicionalmente una importante inversión en sistemas totalmente redundantes con capacidades de conmutación por error instantánea. Este tipo de inversiones solo podría justificarse para unas pocas aplicaciones, por lo que la gran mayoría de las cargas de trabajo se sirvieron con soluciones de respaldo heredadas de menor rendimiento que permitieron objetivos de tiempo de recuperación y objetivos de punto de recuperación (RTO y RPO) de varias horas o días. Estos bajos niveles de rendimiento no cumplen con los requisitos de la empresa con negocios siempre activos, creando una brecha de disponibilidad significativa.

Veeam cierra esta brecha de disponibilidad al aprovechar los recursos del centro de datos moderno, que incluye virtualización, nueva integración de almacenamiento y capacidad en la nube, esto proporciona características clave. Estas características a su vez permiten un tiempo de recuperación y un objetivo puntual (RTPO) de menor a 15 minutos para la mayoría de las cargas de trabajo, reduciendo la brecha de disponibilidad y habilitando el negocio siempre activo.

### **3.2.1 Características de Veeam Availability Suite**

- Recuperación de alta velocidad: permite objetivos de tiempo de recuperación bajo (RTO) de menor que 15 minutos; permite la recuperación rápida de los datos que los clientes desean.
- Evitar la pérdida de datos: evita la pérdida de datos al permitir objetivos de bajo punto de recuperación (RPO) de menor que 15 minutos y al facilitar la protección de datos fuera del sitio.
- Capacidad de recuperación verificada: garantiza que los archivos, las aplicaciones y los servidores virtuales se puedan restaurar de manera confiable cuando sea necesario; garantiza la resistencia del negocio a través de respaldo automatizado y pruebas de recuperación.
- Datos apalancados: elimina los riesgos asociados con la implementación de la aplicación, los cambios de configuración y otros escenarios de prueba; permite probar los cambios en un entorno similar a la producción antes de implementarlos.
- Visibilidad completa: proporciona herramientas de monitoreo y alerta para que pueda descubrir y recibir alertas sobre problemas y posibles problemas en su entorno de TI.

### **3.3 Veeam Availability Orchestrator**

Este producto ofrece a los usuarios una herramienta como orquestador para la automatización constante, escalable y su uso sencillo basadas en las necesidades que hoy en día las empresas necesitan para mantener la continuidad del negocio y de su recuperación ante cualquier desastre, eliminando por un lado los manuales para realizar las pruebas y recuperación que hoy por hoy son inefectivos, extensos y expuestos a muchos errores errores. Es por ello que Veeam Availability Orchestrator ofrece a los usuarios estrategias para la recuperación ante desastres que hoy en día las empresas por sus ventas necesitan mantener sus servicios disponibles es por ello que esta herramienta ayuda para que, de una

manera planificada, practica y apta puedan mantener sus operaciones sin interrupciones mediante replicas y backup, para la recuperación rápida y confiable para los entornos virtualizados más resistentes.

### **3.3.1 Características Veeam Availability Orchestrator.**

- Una Herramienta que incluya un motor para la orquestación y automatización para realizar replicas ayudando a las empresas a mantener la continuidad del negocio y la recuperación de datos ante cualquier desastre.
- Garantizara la recuperación confiable de la información conforme a los servicios determinados realizando los análisis y comprobaciones periódicas en cuanto a la recuperación manteniendo una documentación actualizada.
- Los usuarios podrán realizar una planificación, reparación y ejecución de los planes de recuperación ante desastres de una manera rápida, confiable y exacta.

### **3.4 Veeam Backup Essentials.**

Hoy en día las pequeñas empresas están expuestas a los mismos retos que las grandes empresas, pero sin tener los mismos recursos ya sean tecnológicos y económicos para poder afrontarlos de la mejor manera es por ello que Veeam Backup Essentials presenta una solución para las pequeñas empresas con backup confiable económica y fácil desarrollada para permitir la continuidad de cada empresa y su negocio.

Esta herramienta ayudara a solucionar problemas de las pequeñas empresas o compañías permitiendo realizar backup, recuperación, monitoreo, y la generación de informes modernos, accesibles y fáciles para una gran cantidad de carga de trabajo virtuales, en entornos de VMware, vSphere, Microsoft Hyper-V, Nutanix AHV.

### **3.4.1 Características Veeam Backup Essentials.**

- Es una herramienta que ofrece los mismos servicios que Veeam Availability Suite, pero a un precio accesible para las empresas pequeñas con un ahorro de hasta el 60%, con una protección de datos para entornos virtuales de 2 4 0 6 sockets.
- Evita pérdida de datos mediante la protección continua y una recuperación de desastres fácil.
- Recuperación de alta velocidad de la información necesaria de una manera fácil y ágil ya sea toda una máquina virtual, archivos pequeños o aplicaciones.
- Garantiza la recuperación de sus servicios y aplicaciones críticas a través del backup automatizado.
- Crea una copia del entorno para realizar cambios mediante un virtual lab de esta manera evitar errores al momento de su implementación.
- Permite la administración y notificación de posibles problemas antes de que sufran caídas de sus servicios.

### **3.5 Veeam en el Cuadrante de Gartner**

El movimiento hacia la nube pública, la mayor preocupación por el ransomware y las complejidades asociadas con el respaldo y la administración de datos están obligando a los líderes de I&O a reestructurar su infraestructura de respaldo y explorar soluciones alternativas. Esta investigación proporciona análisis de proveedores de respaldo y recuperación.

Las soluciones de respaldo y recuperación del centro de datos están diseñadas para capturar una copia en un momento determinado de una carga de trabajo empresarial y escribir los datos en un dispositivo de almacenamiento secundario con el fin de recuperar estos datos en el futuro.



Imagen 6. Veeam en el Cuadrante de Gartner

Según las estadísticas realizadas por Cuadrante Mágico de Gartner Inc Veeam se encuentra posicionado más alta en soluciones de copia de seguridad y recuperación de centros de datos para grandes y pequeñas empresas.

# CAPITULO IV

## 4.1 ISO 22301

Las empresas a lo largo de su trayectoria es posible que hayan encontrado dificultades las cuales han hecho que peligre la continuidad del negocio de las empresas, muchas empresas, han tomado la decisión de implementar un Sistemas de Gestión de Continuidad de Negocio con la ISO 22301, una solución que beneficia a todas las organizaciones a mantener operando sus servicios y de esta manera evitar interrupciones en sus actividades y operaciones diarias.

La norma ISO 22301, priorizara y conocerá las posibles amenazas a las que se puedan enfrentar las organizaciones estableciendo los requisitos a seguir por los Sistemas de Gestión de Continuidad de Negocio para que sean mucho más eficientes emitiendo caídas o pérdidas de la información ante cualquier desastre que impidan del buen funcionamiento de sus actividades.

La norma ISO 22301 que consiste en un Sistemas de Gestión de Continuidad de Negocio (SGCN), está basada en una estructura de alto nivel (HLS por sus siglas en inglés) que permitirán a las empresas reestablecer su operatividad después de que haya sufrido interrupciones, provocando la caída de sus actividades, además de proteger la integridad, el cumplimiento de plazos, la satisfacción del cliente y la prevención de posibles pérdidas económicas.

La Nora ISO 22301 determinara los procesos, principios y términos para le gestión y administración en la continuidad del negocio, por lo cual está diseñada para poder ser implementada en organizaciones privadas o públicas, e independientemente de su tamaño o servicio, siendo de una gran prioridad para aquellas empresas que se encuentran propensas

a un alto riesgo de incidentes e interrupciones, de esa manera cada organización garantizase la funcionalidad de sus servicios

#### **4.1.1 Sistema de Continuidad del negocio según la norma ISO 22301.**

Dentro de un sistema de gestión de la continuidad del negocio apoyado por la Norma ISO 22301 tenga un resultado adecuado y sustentable en las empresas se deben considerar tres aspectos importantes que son

**Contexto de la organización.** - ya que en la cláusula 4 de la norma este definido el contexto de la organización dentro de aspectos como:

- **Organización y su contexto:** En la que se debe entender la organización la importancia de un Sistema de gestión de continuidad del Negocio para garantizar su eficiencia
- **Expectativas y Necesidades:** Se definirá todos los participantes en donde se incluirá a la empresa en donde se incluirán reglamentos y condiciones legales para cada uno.
- **Alcance del Sistema:** Se identificará cada uno de los aspectos como son el tamaño, actividad y dificultad de las empresas, para sustentar sus alcances y limitaciones, para en un futuro localizar situaciones de riesgo.
- **Sistema:** Se planteará la responsabilidad a que cada una de las empresas certificar la Gestión de Continuidad de Negocio con la respectiva Norma ISO 22301.

**Liderazgo de la Organización.** – Dentro de cada norma se debe constituir un liderazgo el cual permita cumplir con los objetivos propuestos por cada empresa a través de:

- **Garantizar la conformidad de la planificación, técnica y logros esperados:** Proporcionando la distribución adecuada y apta de los recursos humanos, tecnológicos y económicos que garantizaran los agilidad y efectividad de los Sistemas de Gestión de Continuidad de Negocio.

- **Políticas de la Continuidad de Negocio:** El líder de la organización deberá tratar, verificar y administrar las políticas de Continuidad de Negocio que fueron determinadas en su empresa.
- **Funciones y responsabilidades de su Organización:** Las Organizaciones serán las únicas responsables de cumplir con los requerimientos para la certificación de la Norma tomando en cuenta que cada líder deberá comunicar sobre el desempeño de sus respectivas gerencias.

**Planificación.** – Está relacionada con la decisión de cómo afrontar y tratar los riesgos por parte de las empresas, planificando las acciones precisas para evitar y reducir las repercusiones de los riesgos sobre la continuidad de sus actividades, contemplada en los objetivos planteados de la continuidad del negocio como:

- Fijar las comunicaciones entra la jerarquía y funciones contempladas.
- Todos los objetivos deberán encajar con las políticas establecidas para la continuidad de Negocio.
- Se establecerá un grado mínimo suficiente para la continuidad operativa
- Administrar y renovar los tiempos establecidos en la organización.
- Encargar obligaciones, actividades y grupos responsables de administrar los recursos suficientes a ser distribuidos.

La Continuidad de Negocio es el principio importante con el cual se podrá conseguir una sociedad más estable con el objetivo de alcanzar un desarrollo y avance tecnológico, en donde la rentabilidad de sobrellevar con eficacia una interrupción en los servicios de una empresa, no son únicos y relevantes para ellos, sino que favorecen a todo un entorno, y a una serie de suministros por mas excesiva y difícil que sea. La implementación de la Norma ISO 22301 será un gran avance hacia una perspectiva de las buenas prácticas para la continuidad de Negocio, aumentando sus beneficios, logrando extenderse



internacionalmente, creando una confianza comercial internacional como para proveedores y usuarios, aunque los Sistemas de Gestión de Continuidad de Negocio varían dependiendo del entorno de una organización.

#### **4.1.2 Importancia de la Norma ISO 22301.**

La utilización de la norma ISO 22301 por parte de las empresas permitirá comprobar las facilidades que tiene cada una de ellas para continuar con su funcionamiento durante interrupciones, disminuyendo las debilidades y aumentando la confianza en sus usuarios, permitiendo realizar:

- La creación, implementación y gestión de los Sistemas de Gestión de Continuidad de Negocio.
- Ajustar y ejecutar las políticas de Continuidad.
- Proporcionará confianza mediante el compromiso y buenas prácticas internacionales a sus usuarios.
- Permitirá un camino en común a toda una serie de suministros por más excesivos y difíciles que sean.
- Protegerá a los empleados, usuario y sobre todo su reputación
- Consolidará la venta de sus productos y servicios.

#### **4.1.3 Características de la ISO 22301**

- Permite localizar aquellos procesos críticos y ver su impacto en la continuidad.
- Fortalece la capacidad de recuperación.
- Superioridad frente a la competencia.
- Imagen de confianza a terceros ante condiciones negativas.
- Inspira confianza a las aseguradoras, logrando así reducir las primas de seguros.
- Reducción de costes al disminuir el impacto de los posibles incidentes e interrupciones.

- Incrementa la esperanza de vida de la organización.
- Mejora su reputación.
- Permite tener las respuestas rápidas ante los posibles desastres.
- Contribuye a generar más coordinación entre equipos.

#### **4.1.4 Ventajas de la Norma ISO 22301.**

La norma ISO 22301 permite cumplir requisitos para la planificación, revisión, implementación, pruebas y control de un Sistema de Gestión de continuidad de Negocio por lo que permitirá mantener las siguientes ventajas:

- Disponer de la capacidad para poder evitar o prevenir interrupciones, así como soportar las consecuencias de probables escenarios de riesgo.
- Gestionar las situaciones de riesgo en sus servicios disminuyendo su impacto económico, reputación de las empresas a consecuencia de las interrupciones.
- Obtener una flexibilidad ante la presencia de interrupciones de servicios.
- Reducción de costos por interrupción
- Evitará sanciones por el no cumplimiento de contratos para proveedores de productos y servicios.
- Dispone de una técnica estructurada para la reanudación de los servicios luego de una interrupción.
- Gana credibilidad y reputación con sus usuarios.
- Ventajas económicas al momento de conseguir contratos con aseguradoras.

#### **4.2 Plan de Continuidad de Negocio.**

Plan de Continuidad de Negocio es un conjunto de pasos y técnicas logísticas que pondrán en práctica las diferentes empresas para continuar y retomar las actividades de sus servicios y aplicaciones críticas, que se encuentran interrumpidas por situaciones no deseadas o desastres, de una forma parcial o total dentro de un tiempo definido.

Plan de Continuidad de Negocio BCP (por sus siglas en inglés) también se lo puede definir como la preparación que deben tener las empresas para solventar interrupciones de sus servicios ante la presencia de posibles interrupciones de sus servicios que pondrán en peligro sus objetivos.

#### **4.2.1 Pasos para gestionar un Plan de Continuidad de Negocio**

- 1. Elaboración del programa de BCP:** Se debe diseñar plan de continuidad de negocio, considerando el tamaño y la propia complejidad de la organización.
- 2. Comprensión de la empresa:** En esta etapa, se recolecta la información para priorizar las actividades, diferenciando aquellas que son claves de las que son de apoyo, así como los recursos requeridos por las mismas.
- 3. Definición de las estrategias para el plan de continuidad de negocio:** Se determinan las actividades de negocios claves por las que la organización puede recuperar su servicio dentro de un determinado plazo tras una interrupción.
- 4. Elaboración y ejecución de una respuesta:** Se desarrollarán las respuestas necesarias ante las situaciones de desastre.
- 5. Poner en práctica, cumpliendo los acuerdos definidos del BCP:** Mediante este paso se pone en marcha el plan propuesto con las estrategias, mediante la planificación de ejercicios en ciertos intervalos que permitan revisar la continuidad del negocio.
- 6. Incorporar el Plan de Continuidad de Negocio en la empresa:** Este paso es sumamente importante, pues se ha de conseguir que la Continuidad de Negocio sea parte de todos los miembros de la empresa.

#### **4.3 Plan de Recuperación de Desastres (DRP)**

Plan de Recuperación de Desastres, es la forma en que las empresas se enfrentan y preparan contra posibles desastres que puedan dañar su infraestructura tecnológica y por ende poner

fin a sus actividades. Un DRP es la estrategia y acciones a seguir para restablecer los servicios de TI ante cualquier desastre.

El objetivo de un DRP es reducir los efectos de un desastre en las funciones de las empresas, para que, ante cualquier desastre, sean capaces de reanudar sus funciones.

Para implementar un Plan de Recuperación de Desastres, es importante considerar que las características y las funcionalidades de la empresa; al diseñarlo se debe tomar en cuenta el tipo de negocio, los procesos que se involucran y el nivel de seguridad.

#### **4.3.1 Características de un DRP**

- El 30% de los daños causados a infraestructuras, es causado por desastres, el 70% de las empresas en Latinoamérica no tienen un plan de continuidad de Negocio, solamente el 18% de la información es la que pueden recuperar sin un Plan de Continuidad de Negocio.
- Contar con un plan de recuperación de desastres es de vital importancia para las empresas, ya que el 60% de las empresas que pierden sus datos no cuentan con un DRP.
- Las empresas que no son capaces de reanudar sus operaciones dentro de los diez días siguientes de un desastre, es probable que no sigan adelante con su funcionamiento.
- Tener un plan de recuperación de desastres ayuda a reducir hasta un 60% el impacto del desastre, evitando así pérdidas de los datos y pérdidas económicas.

# CAPÍTULO V

## **5.1 Metodología.**

Dentro de nuestro trabajo de investigación se describirá las diferentes situaciones críticas que cada una de las empresas puedan sufrir ya sean estas físicas o lógicas, afectando de tal manera el correcto funcionamiento de sus servicios y aplicaciones, por lo tanto, cada una de las empresas deberán cumplir diferentes normas y requisitos basados en la norma ISO 22301 los mismo que permitirán responder de una manera inmediata ante cualquier tipo de amenaza, identificando las diferentes posibilidades de cada una de las empresas para enfrentarlo y de esa manera mantener la continuidad de sus servicios y aplicaciones.

Es un trabajo ágil que se basa en mantener diferentes planificaciones y estimaciones que se hacen a lo largo del nuestro trabajo de investigación, no solo realizándolo al principio como en las metodología tradicionales, es por eso que cada 2 o 4 semanas hay que realizar nuevamente planificaciones basándose en las principales situaciones críticas de cada una de las empresas ya sean estos dentro de los diferentes sistemas o servidores, o externos comprometiendo el buen funcionamiento de los servicios y a su vez la continuidad del negocio.

## **5.2 Implementación de la Metodología**

Los departamentos de TI, tienen como objetivo garantizar a los usuarios la continuidad de todos sus servicios y aplicaciones críticas, para lo cual hemos realizado este trabajo de investigación, que tiene como objetivo desarrollar una metodología que permita realizar el despliegue de un sitio alternativo de un centro de datos mediante la utilización de la norma ISO 22301 con la ayuda de la aplicación VEEAM.

### **5.2.1 Selección de la metodología**

Dentro de los diferentes tipos de metodologías y en base a las buenas prácticas, y con la implementación de los diferentes avances tecnológicos en las empresas, la metodología

Scrum es una forma de trabajo ágil, mediante la cual a través de prácticas colaborativas se minimizan todo tipo de riesgos en la elaboración de un proyecto, de esta manera se incentivará el trabajo investigativo en equipo.

En Scrum no se realiza una entrega final del proyecto, sino que se van haciendo de forma regular entregas parciales, de forma que esto es lo que más beneficia al receptor del proyecto. Por ello, Scrum está especialmente indicado para entornos complejos, donde los cambios se producen como mucha frecuencia y sobre la marcha y donde la rapidez, la flexibilidad, la adaptabilidad y la competencia juegan un papel fundamental.

Un proyecto Scrum se basa en:

- Planificación del proyecto
- Identificación de las actividades que se llevarán a cabo.
- Priorización según el valor de negocio de las actividades.
- Estimación de tiempos
- Desarrollo de las actividades
- Evaluación del proyecto

### **5.2.2 Roles Scrum**

Los diferentes roles están basados en el cumplimiento de la planificación de cada una de los miembros de los miembros del equipo de trabajo manteniendo prioridades en el cumplimiento de los diferentes objetivos y cuales el orden de las actividades en el que se irán cumpliendo con el avance del proyecto.

Dentro de los diferentes roles podremos mencionar tres principales que son:

- **Scrum Master.** - que es el líder o jefe de proyecto que se encargara de supervisar el cumplimiento de los objetivos de cada uno de los miembros del equipo de trabajo en cada uno de los roles o funciones.
- **Dueño del Producto.** – Es el encargado de crear el proyecto en donde registrara todas sus actividades y características siendo una parte fundamental en el desarrollo del proyecto.
- **Equipo.** – Son cada uno de los integrantes del equipo de trabajo que está trabajando en el proyecto los mismos que estarán capacitados en los diferentes temas a los que el proyecto refiere para cumplir el objetivo y el proyecto final.

### **Funciones del Scrum master.**

Dentro de las principales funciones que tiene el líder del equipo de trabajo tenemos las siguientes.

- Realizara reuniones antes del inicio de cada sprint.
- Garantizara que el equipo conste con los requisitos del usuario o cliente por el dueño del producto
- Mantendrá el dialogo permanente entre el usuario o cliente con todo el equipo.
- Garantizara un acuerdo mutuo con el dueño del producto con el equipo de trabajo.
- Apoyará a su equipo de trabajo a entender cuáles son las necesidades del cliente o usuario.
- Garantizar que su equipo de trabajo ha realizado una separación y consideración de los trabajos y las diferentes tareas precisas de realizar un análisis e investigación.
- Garantizar que luego de cada reunión con el equipo estén claros los objetivos de cada sprint con sus respectivas tareas y su tiempo de duración.

### 5.2.3 Artefactos Scrum

Dentro de los artefactos podremos encontrar que son las características, requisitos, listas de los diferentes trabajos que se realizar para logras alcanzar los objetivos por cada miembro del equipo y a su vez del equipo de trabajo, dentro de los artefactos scrum podemos encontrar diferentes modelos de recolección de requerimientos y listas de trabajo para el comienzo del proyecto que se detallaran a continuación.

- **Pila de Producto.** – No es más que las listas de todas las necesidades de los usuarios que irá incrementando y evolucionando con el transcurso y avance del proyecto.
- **Pila Sprint.** – Se basa en la lista de las tareas que cada miembro deberá cumplir para el avance oportuno del proyecto.
- **Incremento.** – No es más que el resultado que obtiene cada Sprint según va avanzando cada tarea del proyecto.

Dentro de la metodología scrum para la recolección de requisitos y requerimientos de los usuarios y clientes tenemos dos formas muy importantes que son la pila de producto y la pila del sprint.

**La pila de producto.** - Registrara todos los requisitos y requerimientos ordenados de los usuarios según su punto de vista y está constituido por las diferentes listas de las funcionales según la prioridad que el usuario o cliente desea obtener o alcanzar con el proyecto.

**La pila de Sprint.** - Son los requisitos o requerimientos según el punto de vista del equipo de trabajo que realizara el proyecto mediante las diferentes tareas que llevaran a cabo el alcance del objetivo general.



### 5.2.4 Eventos Scrum

Dentro de los eventos tenemos cada una de las tareas específicas y actividades que realizara el equipo de trabajo para presentar avances y cumplimiento de cada una de las tareas, está conformada de la siguiente manera

- **Sprint.** – Controla el avance del proyecto y los tiempos de duración de cada tarea.
- **Reunión de planificación.** – Cada reunión realizada con el equipo de trabajo marca el inicio del sprint donde se especificará es objetivo de cada una de las tareas.
- **Scrum diario.** – son las tareas diarias de cada uno de los miembros del equipo donde responderá a tres preguntas que permitirán supervisar el avance del proyecto.
  1. Que trabajo se realizó cada día.
  2. Que trabajo va a realizar.
  3. Lo que se va a necesitar o algún impedimento que no permitirá realizar la tarea.

Por lo general cada miembro deberá cumplir con el tiempo y pendientes en cada una de sus tareas.

- **Revisión Sprint.** – Supervisara el avance de las tareas
- **Retrospectiva.** – Supervisara todo lo que sucede durante los sprint analizando los trabajos del equipo creando mejoras para las próximas reuniones.

### 5.2.5 Sector de Interés

Luego de un estudio nos enfocaremos a los diferentes centros de datos de las empresas que por su gran cantidad de información, servicios y aplicaciones críticas, es importante que cuenten con un respaldo de toda su información a un sitio alternativo, evitando al máximo la interrupción de cada una de sus servicios, tomando en cuenta las diferentes normas y

estrategias de planificación durante y luego de situaciones críticas, para la continuidad del negocio según la norma ISO 22301 que permitirá garantizar las actividades.

Estará de alguna manera enfocados a los departamentos de TI que realizaran y mantendrá un sistema de gestión ante situaciones críticas que permitirán el correcto funcionamiento de los centros de datos que tendrán como misión primordial la de reestablecer sus servicios de una forma ágil y en menor tiempo posible.

### **5.2.6 Iteraciones**

Dentro de las diferentes iteraciones estarán basados según el tiempo en la que se realizara cada uno de los respaldos de los centros de datos que pueden ser diarios o por horas según sea la preferencia de cada una de las empresas para la recolección de toda la información estimando tiempos en lo que se puede realizar cada uno de los respaldos.

Los Tiempos estarán estipulados según las características, estándares y requerimientos de cada una de las empresas el cual sería enmarcado a cada uno de los sprint o tareas del equipo de trabajo, permitiendo cumplir con los diferentes objetivos establecidos en cada una de las tareas.

Dentro de las diferentes iteraciones podemos mencionar las siguientes:

- Se realizará el respaldo de la información de los centros de datos con el fin de evitar pérdidas de la información en caso de producirse situaciones críticas.
- Se realizará el despliegue a un sitio alternativo de la información de los diferentes centros de datos.
- Se mantendrá la continuidad del negocio y de sus actividades según lo estipula las normas y estándares de la norma ISO 22301.

- Se realizará las respectivas pruebas verificando los tiempos de respuesta y reanudación de actividades en el centro de datos.
- Luego de las pruebas se verificará el correcto funcionamiento de los diferentes servicios y aplicaciones permitiendo mantener la continuidad del negocio.

### 5.3 Software y Hardware Requerido

Para la implementación de nuestro trabajo de investigación utilizaremos diferentes plataformas y aplicaciones, tanto para el desarrollo del centro de datos que contendrá información primordial e importante de cada una de las empresas y previamente se desarrollará el despliegue a un sitio alternativo de toda esa información en situaciones críticas de los diferentes centros de datos.

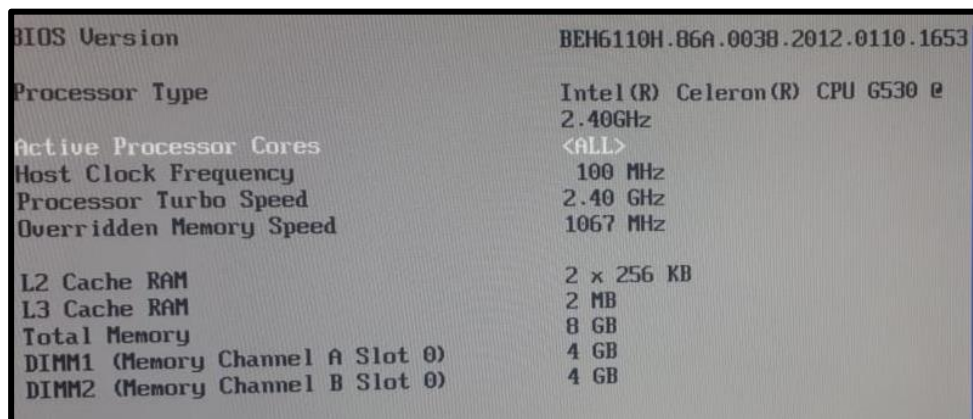
- VMware vSphere Hypervisor (ESXi) 6.7.0
- VMware vCenter Server 6.7.0
- Windows Server 2016
- Veeam Availability Suite v10

Para la generación de un centro de datos y las demás aplicaciones para el respaldo y la creación de un sitio alternativo se va a utilizar el siguiente hardware con las características y requisitos de sistema por cada aplicación o plataforma.

BIOS Version	BEH6110H.86A.0038.2012.0110.1653
Processor Type	Intel(R) Celeron(R) CPU 6530 @
Active Processor Cores	2.40GHz
Host Clock Frequency	<ALL>
Processor Turbo Speed	100 MHz
Overridden Memory Speed	2.40 GHz
L2 Cache RAM	1067 MHz
L3 Cache RAM	2 x 256 KB
Total Memory	2 MB
DIMM1 (Memory Channel A Slot 0)	12 GB
DIMM2 (Memory Channel B Slot 0)	4 GB
	8 GB

Imagen 7. Características de la máquina para el Centro de Datos

El centro de datos principal y el centro de datos alternativo cuenta con un procesador Intel Celeron 6530 que procesa a 2.40GHz, con una memoria RAM de 12GB y dos discos duros el primero de 80GB para la instalación de ESXi 6.7.0 y el segundo de 500GB que funcionará como almacenamiento de los servicios.



BIOS Version	BEH6110H.86A.003B.2012.0110.1653
Processor Type	Intel(R) Celeron(R) CPU 6530 @ 2.40GHz
Active Processor Cores	<ALL>
Host Clock Frequency	100 MHz
Processor Turbo Speed	2.40 GHz
Overridden Memory Speed	1067 MHz
L2 Cache RAM	2 x 256 KB
L3 Cache RAM	2 MB
Total Memory	8 GB
DIMM1 (Memory Channel A Slot 0)	4 GB
DIMM2 (Memory Channel B Slot 0)	4 GB

*Imagen 8. Características de la máquina para el Windows Server 2016*

El Windows Server 2016 con un procesador Intel Celeron 6530 que procesa a 2.40GHz, con una memoria RAM de 8GB y un disco duro de 500GB en el cual se instala el sistema operativo y luego se va a instalar el software Veeam que va a ser el encargado de realizar la replicación de los servicios y el proceso de despliegue del centro de datos alternativo en caso de desastres.

Para el desarrollo de la metodología se tomará en cuenta cada uno de los diferentes pasos y normas que estipulan la norma ISO 22301, las cuales especifican los requisitos que cada uno de los diferentes sistemas de gestión y los departamentos de TI encargados de cada una de las empresas tomarán en cuenta para evitar situaciones en las que se sientan amenazadas sus actividades y servicios por problemas físicos y lógicos, reduciendo al máximo la interrupción en sus actividades.

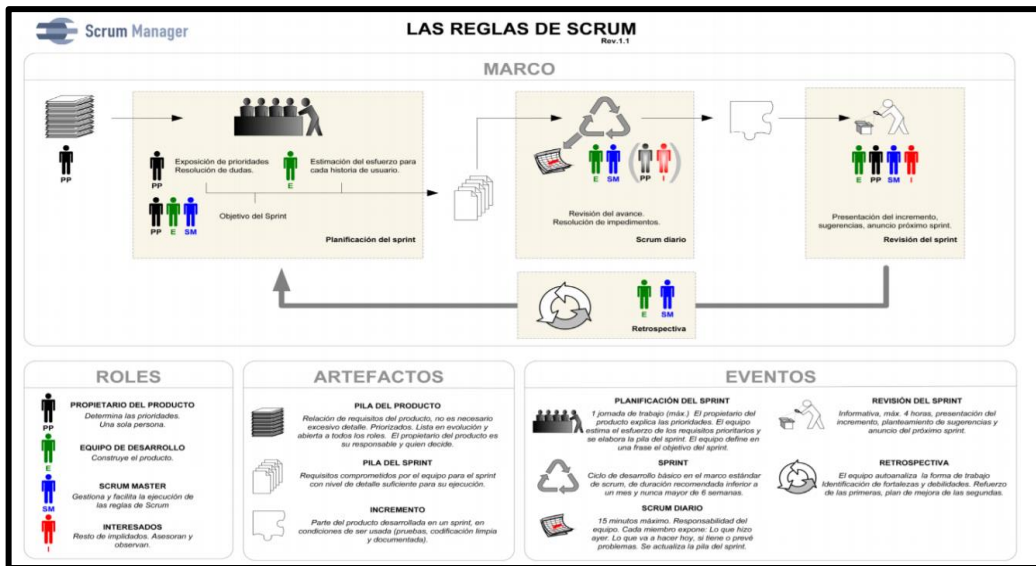


Imagen 9. Reglas para el uso de SCRUM

# CAPÍTULO VI

## 6.1 Desarrollo

### 6.1.1 Planificación

Se necesita crear una metodología la cual permita a las empresas crear un sitio alternativo en caso de desastres basándose en la norma ISO 22301 mediante la utilización de la aplicación Veeam.

La norma ISO 22301 nos indica que una empresa que tenga un centro de datos necesita contar con un sitio alternativo el cual funcione de manera inmediata en caso de desastres ya sean estos naturales o por el ser humano, este sitio alternativo debe funcionar de manera inmediata al momento de detectar de que el centro de datos principal deje de funcionar.

### 6.1.2 Actividades

- Seleccionar la topología.
- Escoger los programas necesarios.
- Adecuar los equipos en base a los requerimientos de software.
- Instalación del software en los diferentes equipos.
- En el centro de datos principal instalar los servicios requeridos.
- En otro equipo instalar el software para realizar las operaciones necesarias.
- Tener el sitio alternativo adecuado a las necesidades del centro de datos principal.

### 6.1.3 Actividades Prioritarias

Como actividades prioritarias en este proyecto tendría que ser la búsqueda de la mejor topología que sea la adecuada en base a lo que se necesite y tener el sitio alterno listo para su funcionamiento.

## 6.1.4 Desarrollo de Actividades

### 6.1.4.1 Topologías que recomienda la empresa Veeam

Dentro de la aplicación VEEAM y sus plataformas tenemos varias topologías que permitirán solventar y respaldar la información

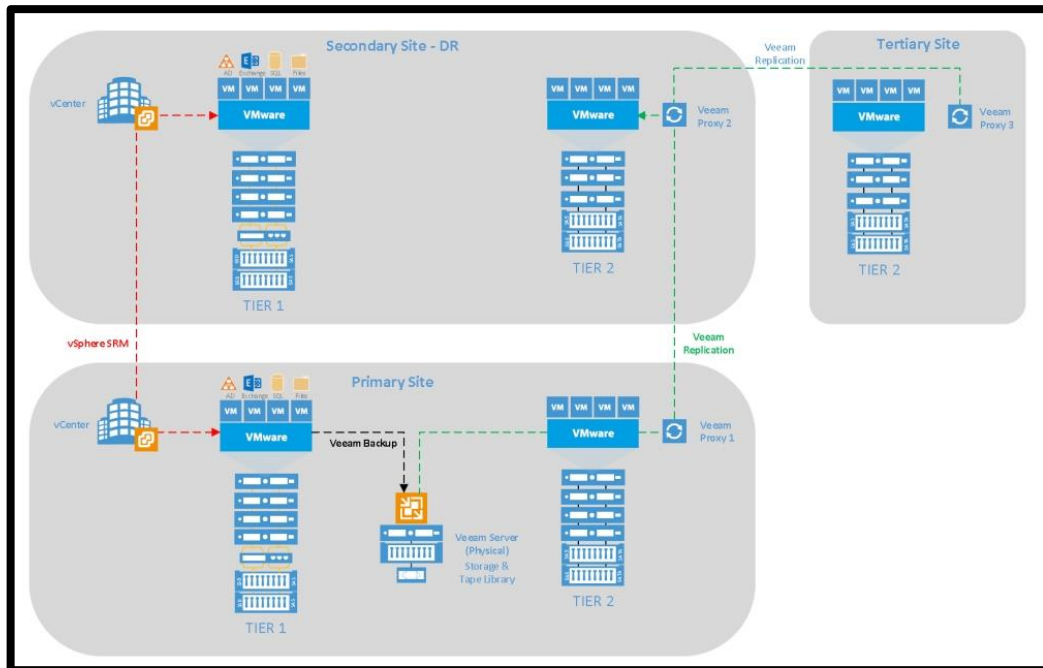


Imagen 10. Infraestructura planteada

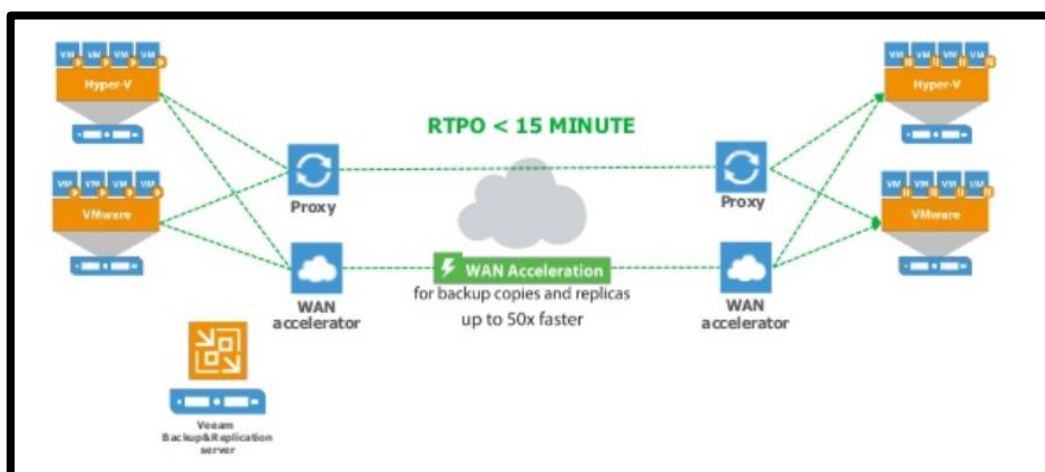


Imagen 11. Infraestructura planteada

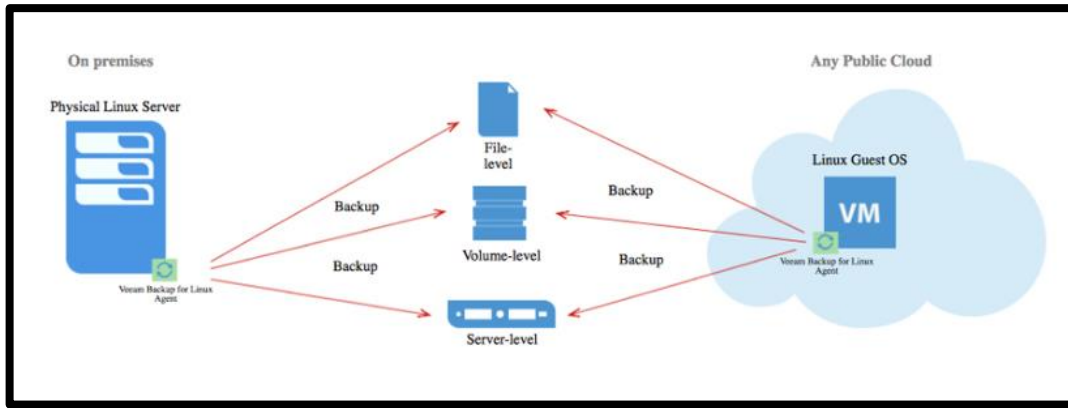


Imagen 12. Infraestructura planteada

La topología que se ha seleccionado es la que se muestra a continuación porque es la que representa de mejor manera un centro de datos y su respectivo sitio alterno, muestra la utilización del software que se requiere y da una idea de lo que se va a realizar.

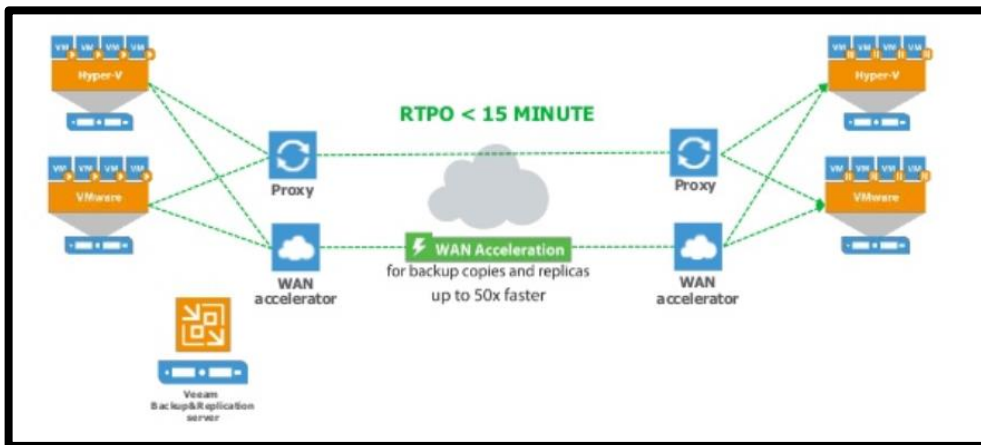


Imagen 13. Infraestructura que va a ser desarrollada



#### 6.1.4.2 Software necesarios

- VMware vSphere Hypervisor (ESXi) 6.7.0

HARDWARE
CPU de 2 núcleos
Procesador x86 de 64 bits
Memoria RAM de 8GB
Virtualización de (Intel VT-x o RVI AMD) en CPU x64.
Controladoras Gigabit o Ethernet
ESXi 6.7.0 requiere un disco de arranque de al menos 8 GB para dispositivos USB, y 32 GB para otros tipos de dispositivos.
Disco SCSI con espacio no particionado para las máquinas virtuales.
Para la serie ATA (SATA)

*Tabla 3. Hardware requerido para ESXi 6.7.0*

- VMware vCenter Server 6.7.0

HARDWARE
Procesador Intel o AMD x86 con dos o más núcleos
Memoria RAM de 4GB
Disco de 4GB. Los requisitos del disco pueden ser superiores si la base de datos de vCenter Server se realiza en la misma máquina
Se necesitan más de 2 GB de espacio libre en el disco para descomprimir el archivo de instalación.
Se recomienda una conexión de 1 Gbit.

*Tabla 4. Hardware requerido para vCenter 6.7.0*

- Windows Server 2016

HARDWARE
Procesador de 1.4Ghz de 64 bits
Memoria RAM de 512MB
Disco duro de 32GB
Adaptador Ethernet Gigabit (10/100/1000baseT)

*Tabla 5. Hardware requerido para Windows Server 2016*

- Veeam Availability Suite v10

HARDWARE
Procesador x86-64 (se recomienda un mínimo de 4 núcleos).
4 GB de RAM más 500 MB de RAM para cada trabajo simultáneo.
5 GB para la instalación del producto y 4.5 GB para la instalación de Microsoft .NET Framework 4.7.2. 10 GB por 100 VM para la carpeta del catálogo del sistema de archivos

invitado (datos persistentes). Espacio libre en disco adicional para Instant VM Recovery
carpeta de caché (datos no persistentes, se recomiendan al menos 10 GB).
1 Gbps o más rápido para la copia de seguridad y replicación en el sitio, y 1 Mbps o más rápido para la copia de seguridad fuera del sitio y replicación.
Se recomienda una conexión de 1 Gbit.

Tabla 6. Hardware requerido para Veeam v10

SISTEMA OPERATIVO
Microsoft Windows Server 2019
Microsoft Windows Server 2016
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2012

Tabla 7. Sistemas Operativos compatibles

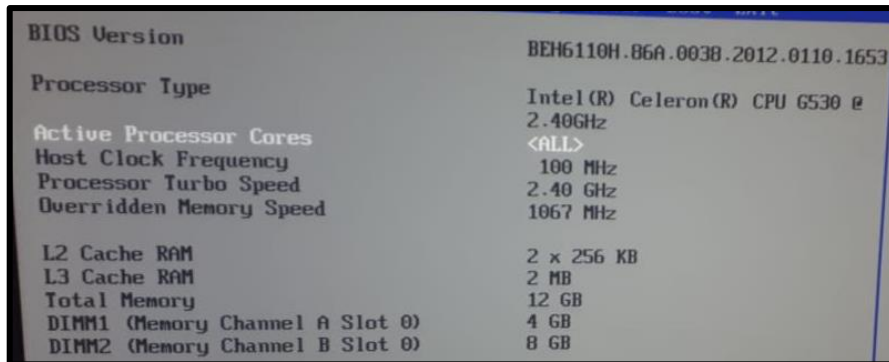
SOFTWARE
Microsoft SQL Server 2008 hasta 2019 (2016 SP1 Express está incluido)
System Center Virtual Machine Manager 2008R2 a 1807 UI de administración (opcional, para poder registrar el servidor SCVMM con la infraestructura de copia de seguridad y replicación)
Microsoft .NET Framework 4.7.2
Windows Installer 4.5
Microsoft PowerShell 2.0
Firefox, Google Chrome, Microsoft Edge o Microsoft Internet Explorer 11.0 o posterior

Tabla 8. Software requerido para Veeam v10

**6.1.4.3 Instalacion del software**

Se requiere instalar el software necesario en cada máquina para la creación del servidor principal, el servidor que va a funcionar de sitio alternativo y el administrador de las tareas adicionales.

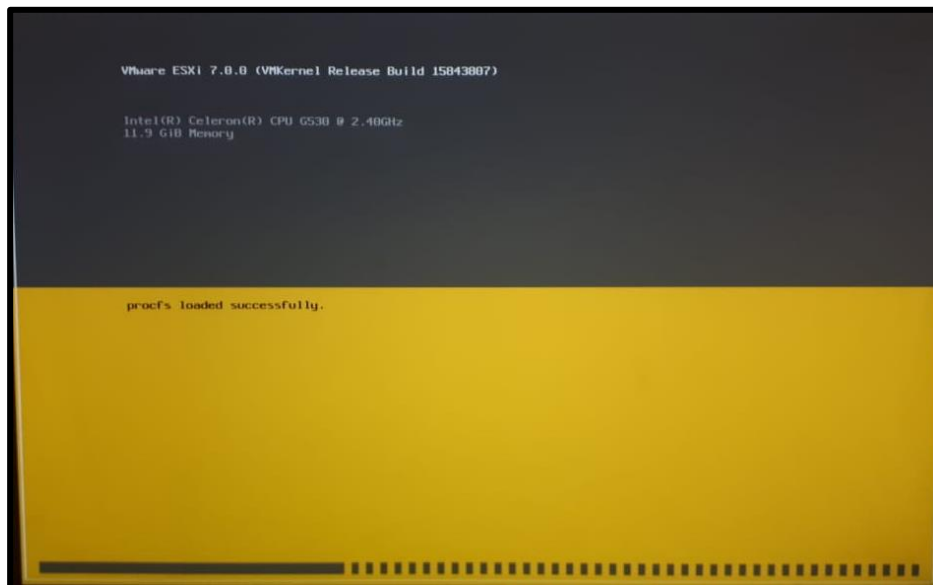
- **Centro de datos principal**



BIOS Version	BEH6110H.86A.003B.2012.0110.1653
Processor Type	Intel(R) Celeron(R) CPU 6530 @ 2.40GHz
Active Processor Cores	<ALL>
Host Clock Frequency	100 MHz
Processor Turbo Speed	2.40 GHz
Overridden Memory Speed	1067 MHz
L2 Cache RAM	2 x 256 KB
L3 Cache RAM	2 MB
Total Memory	12 GB
DIMM1 (Memory Channel A Slot 0)	4 GB
DIMM2 (Memory Channel B Slot 0)	8 GB

*Imagen 14. Especificaciones del Centro de Datos principal*

El centro de datos principal cuenta con un procesador Intel Celeron 6530 que procesa a 2.40GHz, con una memoria RAM de 12GB y dos discos duros el primero de 80GB para la instalación el EXSi 6.7.0 y el segundo de 500GB que funcionara como almacenamiento de los servicios.



*Imagen 15. Pantalla de carga de ESXi*

El proceso de instalación es fácil y rápido ya que es una interfaz muy amigable la cual indica cada paso que se tiene que dar para completar la instalación, se requiere una conexión a internet para la instalación.



Imagen 16. Selección de disco para la instalación

En esta parte de la instalación es donde se escoge el disco donde va a ser instalado el Hypervisor y cual disco va a ser de almacenamiento.

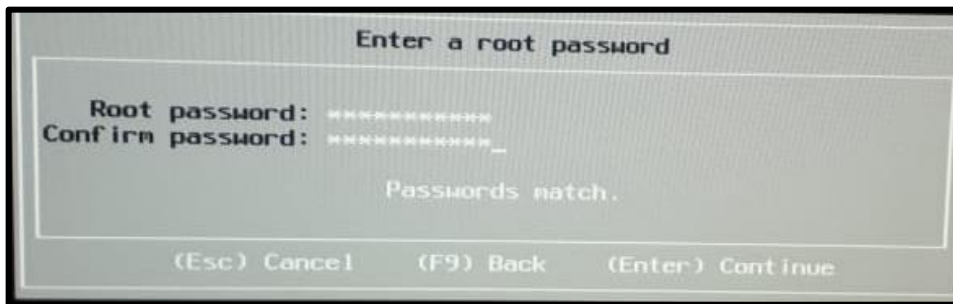


Imagen 17. Ingreso de contraseña

Es necesario una contraseña para el administrador que en este caso es el encargado de la instalación y configuración de los servicios dentro del centro de datos.



Imagen 18. Configuración de la interfaz de red

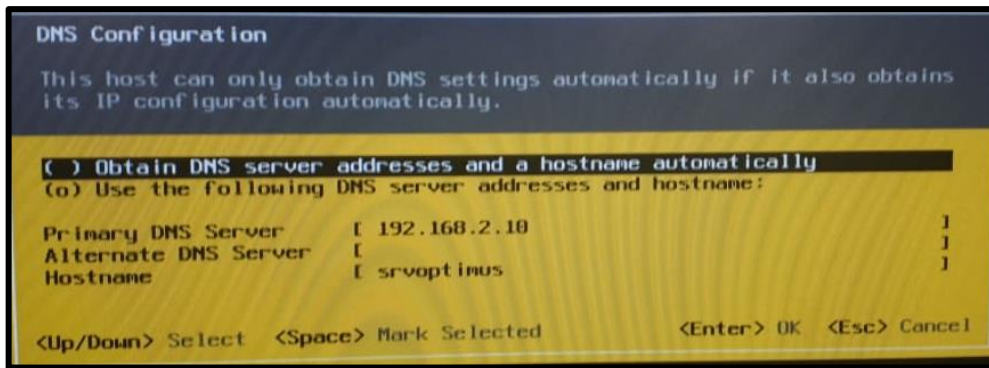


Imagen 19. Configuración del DNS y Host

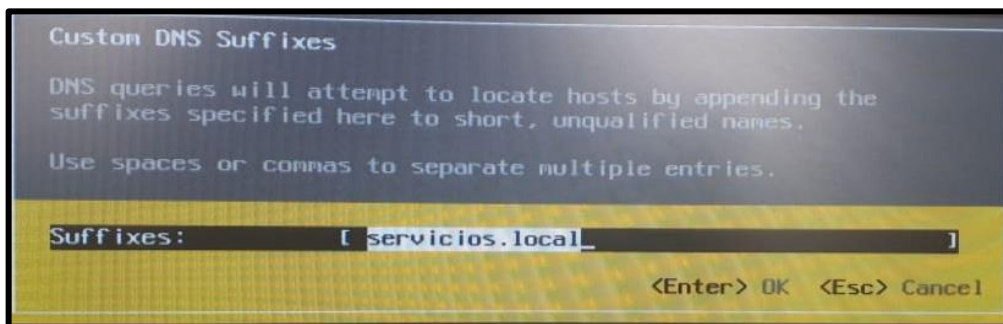


Imagen 20. Sufijo del DNS

Luego de la instalación se debe configurar la tarjeta de red con una IP estática, el nombre de la maquina con la IP del DNS y el sufijo.

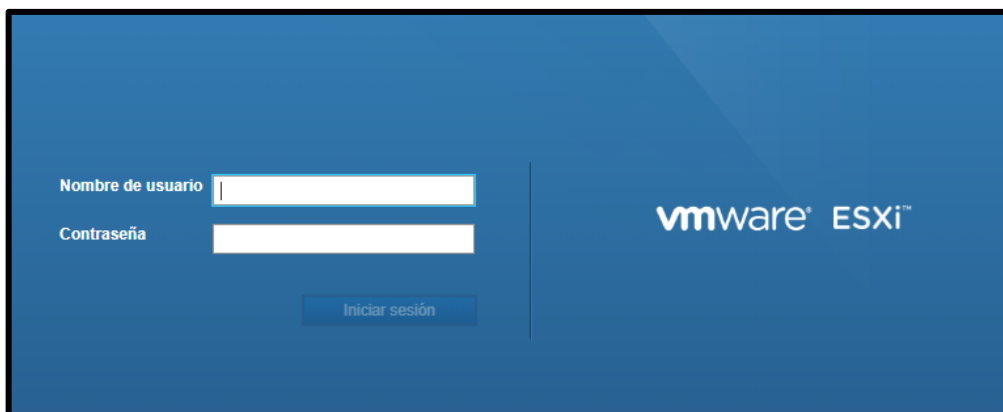


Imagen 21. Pantalla de inicio del ESXi

Una vez acabado de configurar todo mediante un navegador se puede ingresar a la ventana de configuración del centro de datos por medio del usuario root y la contraseña que fue configurada en la instalación.

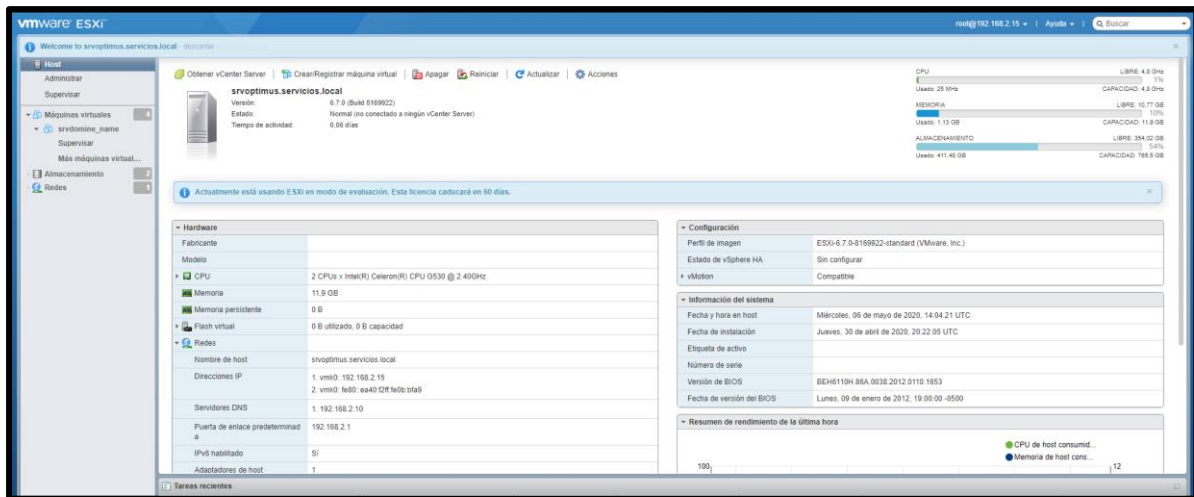


Imagen 22. Centro de Datos principal

En la siguiente ventana se puede configurar el resto de requisitos para el correcto funcionamiento del centro de datos como lo que es el disco de almacenamiento y luego se puede empezar a crear cada servicio.

- **Centro de datos para el sitio alterno**

El centro de datos para el sitio alterno cuenta con los mismos requisitos que el sitio principal lo único que en este se debe permanecer sin ningún servicio instalado ya que luego se va a realizar la replicación del centro de datos principal.

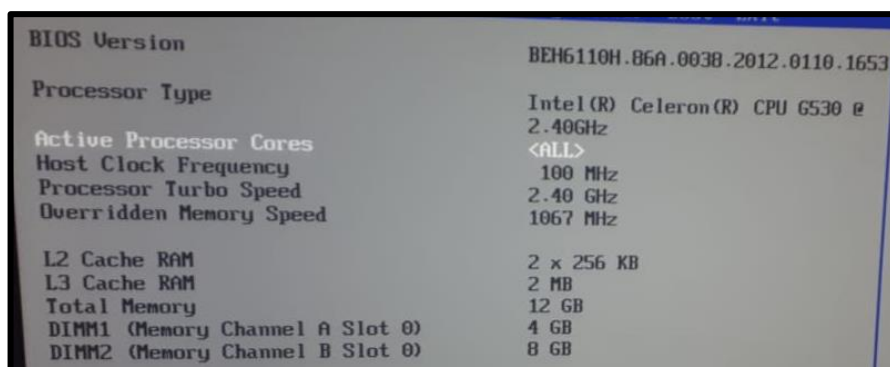


Imagen 23. Especificaciones del Centro de datos alterno

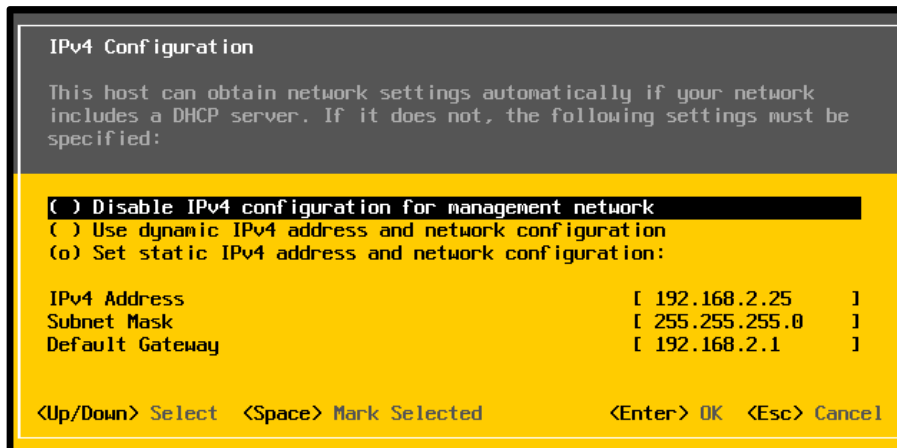


Imagen 24. Configuración de la interfaz de red

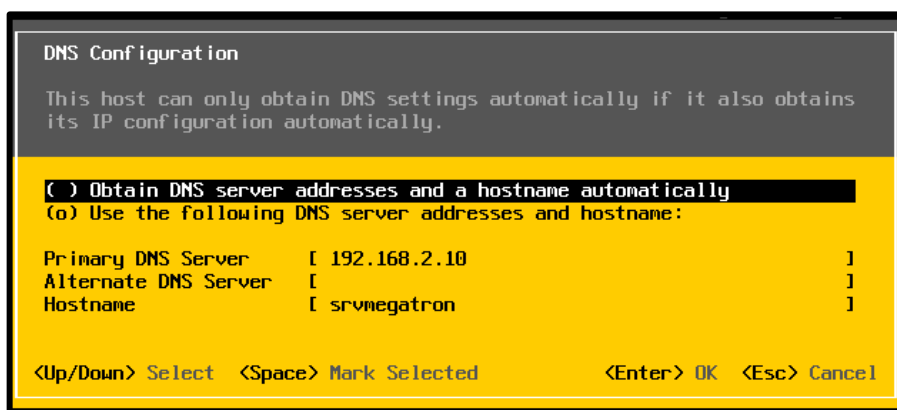


Imagen 25. Configuración del DNS y el Host

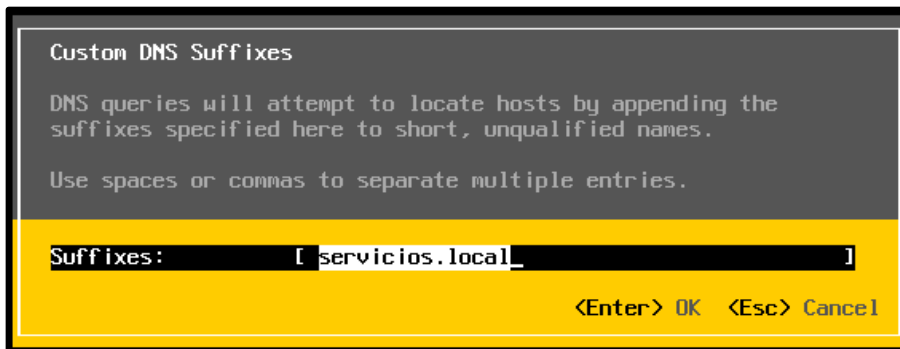


Imagen 26. Sufijo del DNS

De igual manera que en centro de datos principal se debe configurar una dirección IP estática el nombre de la maquina la IP del DNS y el sufijo.

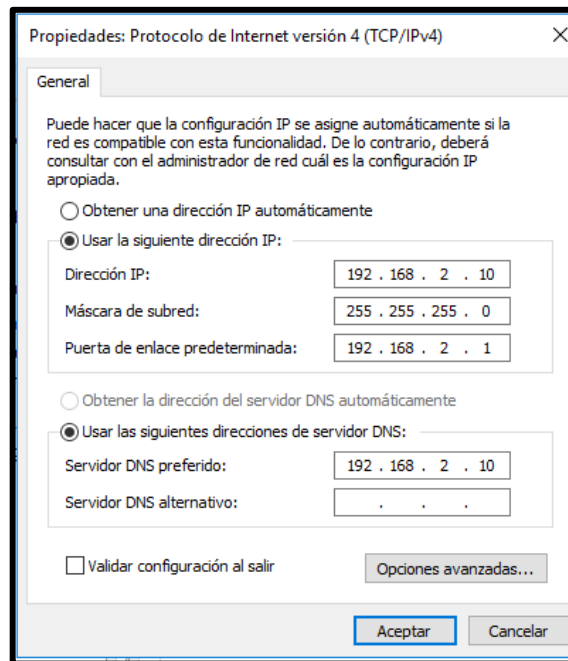


- **Windows Server 2016**

BIOS Version	BEH6110H.86A.003B.2012.0110.1653
Processor Type	Intel(R) Celeron(R) CPU 6530 @ 2.40GHz
Active Processor Cores	<ALL>
Host Clock Frequency	100 MHz
Processor Turbo Speed	2.40 GHz
Overridden Memory Speed	1067 MHz
L2 Cache RAM	2 x 256 KB
L3 Cache RAM	2 MB
Total Memory	8 GB
DIMM1 (Memory Channel A Slot 0)	4 GB
DIMM2 (Memory Channel B Slot 0)	4 GB

*Imagen 27. Especificaciones para el Windows Server 2016*

El Windows Server 2016 con un procesador Intel Celeron 6530 que procesa a 2.40GHz, con una memoria RAM de 8GB y un disco duro de 500GB en el cual se instala el sistema operativo y luego se va instalar el software que va ser el encargado de realizar la replicación de los servicios y el proceso de despliegue del centro de datos alterno en caso de desastres.



*Imagen 28. Configuración de IP para la interfaz de red*



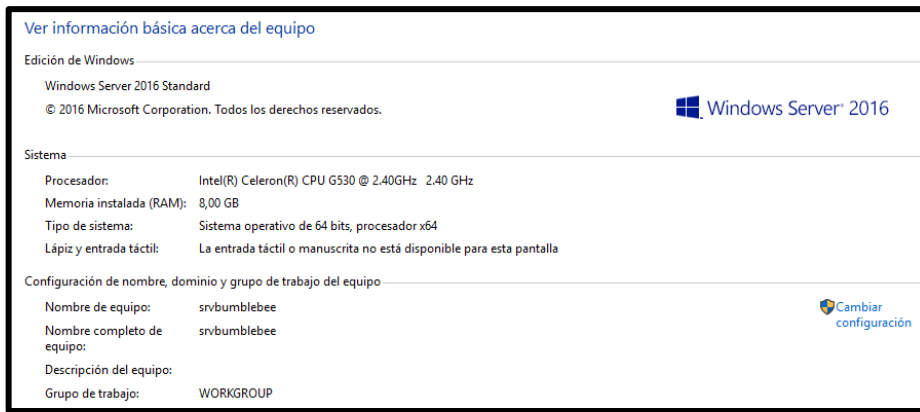


Imagen 29. Nombre del Windows Server 2016

Previa a la configuración del servicio de DNS que va a permitir la conectividad del centro de datos principal con el centro de datos alterno y a su vez con el software se debe configurar una IP estática y cambiar el nombre de la máquina.

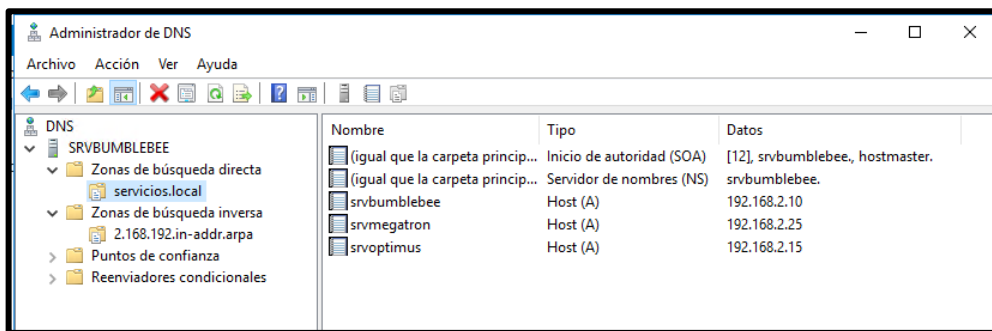


Imagen 30. Zona principal del DNS del WS 2016

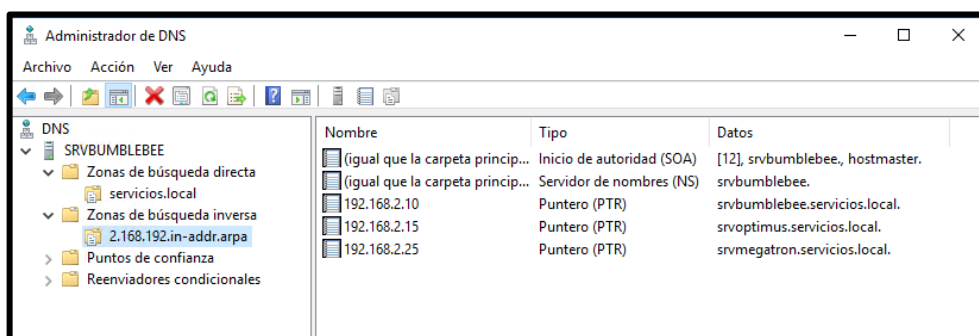


Imagen 31. Zona inversa del DNS del WS 2016

Una vez configurado el servicio de DNS contamos con los nombres de la maquinas con sus respectivas direcciones IP's, el DNS inverso el cual permitirá la conexión ya sea por la propia IP o a su vez por el nombre de la maquina con el sufijo del DNS.

#### 6.1.4.4 Servicios del Centro de Datos

Dentro del centro de datos se va a crear 4 servicios los cuales son importantes para el funcionamiento del centro de datos y para una empresa.

Máquina virtual ▲	Condición	Espacio utilizado	Sistema operativo invitado
srvactivedirectory	✓ Normal	100 GB	Microsoft Windows Server 2016 (64 bits)
srvdata_base	✓ Normal	100 GB	Ubuntu Linux (64 bits)
srvdomine_name	✓ Normal	102,21 GB	Ubuntu Linux (64 bits)
srvweb	✓ Normal	100 GB	Ubuntu Linux (64 bits)

Imagen 32. Servicios configurados del Centro de Datos principal

Los servicios instalados en el centro de datos son: DNS, Base de Datos, Web, Active Directory.

#### 6.1.4.5 Instalacion de Veeam

La instalación del software Veeam muy fácil de instalar ya que en cada paso muestra la información necesaria para la correcta instalación.

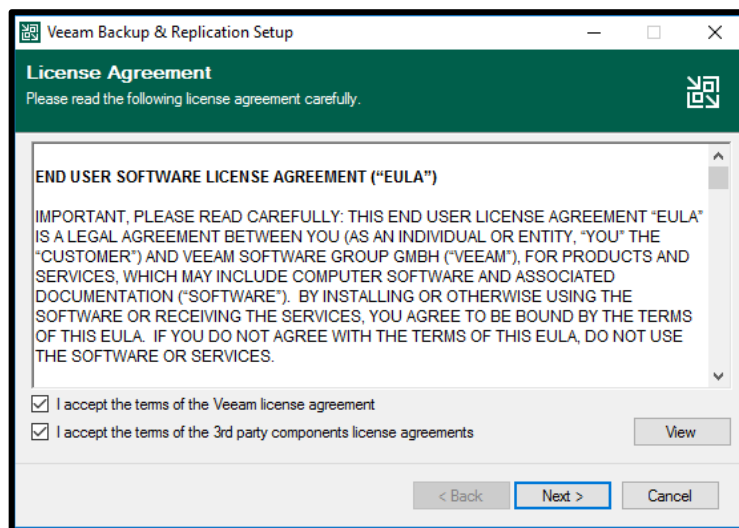
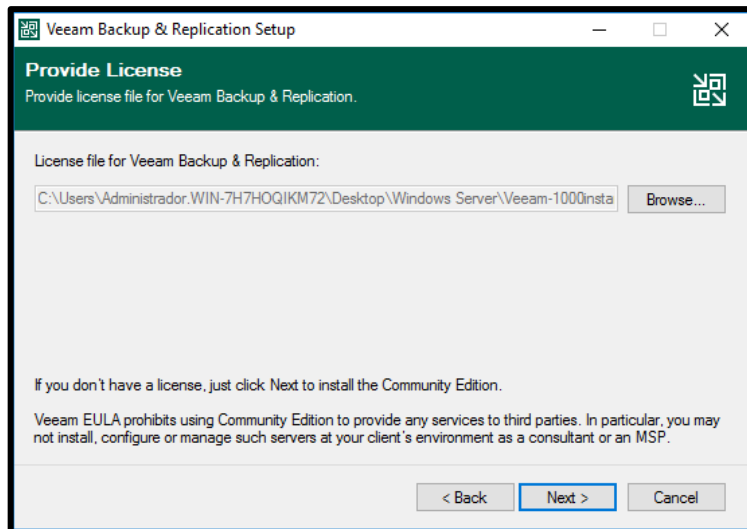


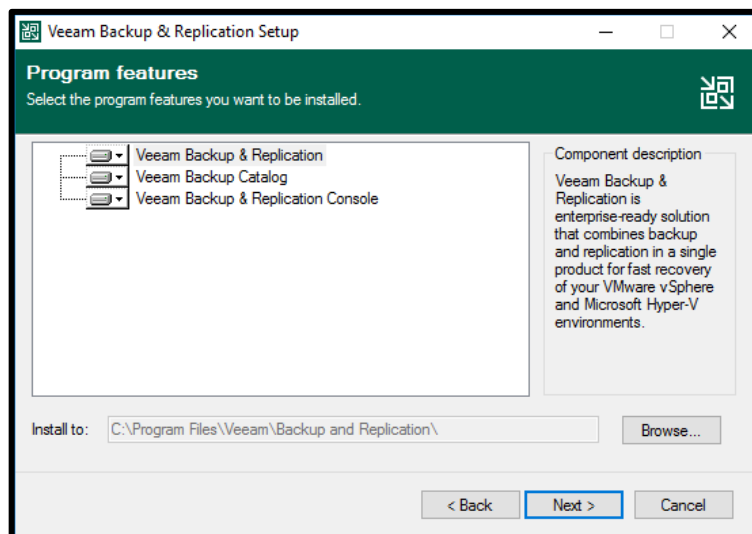
Imagen 33. Términos y condiciones de Veeam



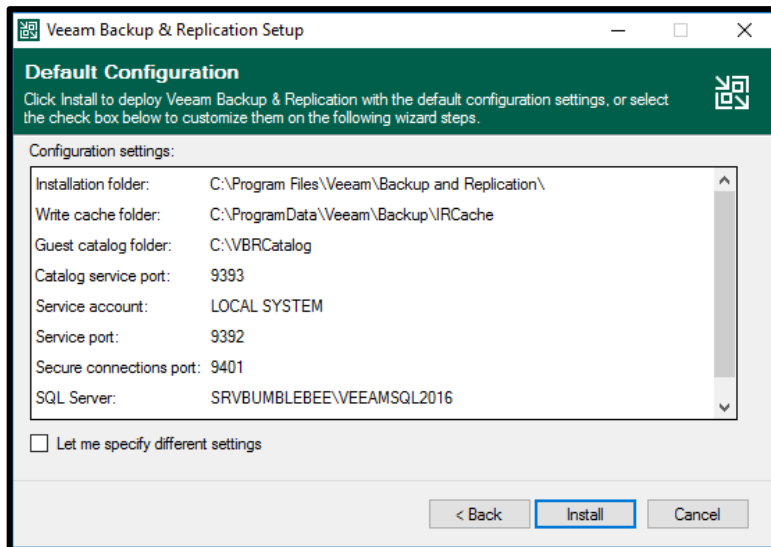
*Imagen 34. Licencia de prueba de Veeam*

Para la instalación completa del software se va a requerir una licencia la cual puede ser una de prueba de 30 días o a su vez una anual.

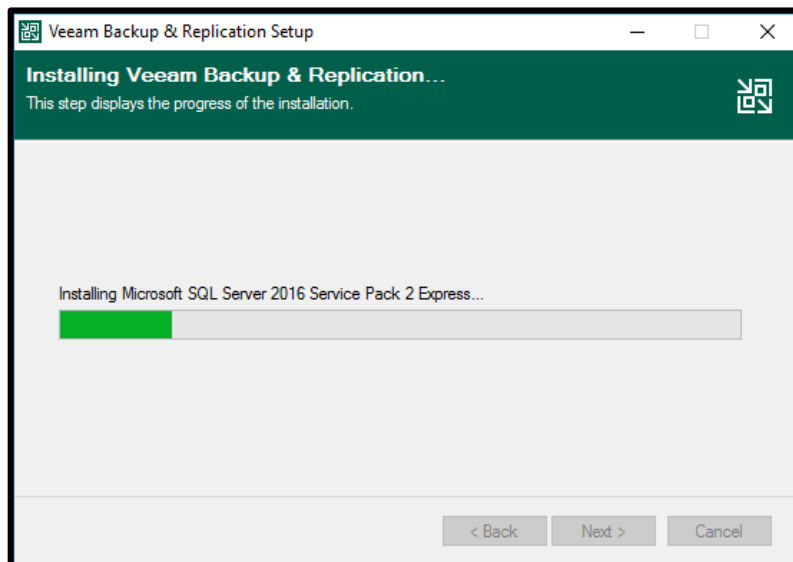
Por medio de esta licencia se va poder utilizar todas las funcionalidades que el software nos ofrece y con estas funcionalidades se va a realizar desde la replicación de los servicios del centro de datos principal hacia el centro de datos alterno, en caso de desastres el software nos permite el levantamiento del centro de datos alterno para la continuidad del negocio.



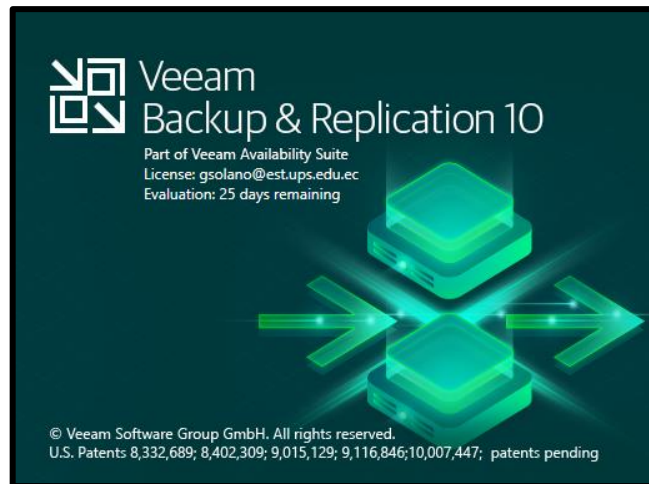
*Imagen 35. Software que se instala y ubicación de instalación*



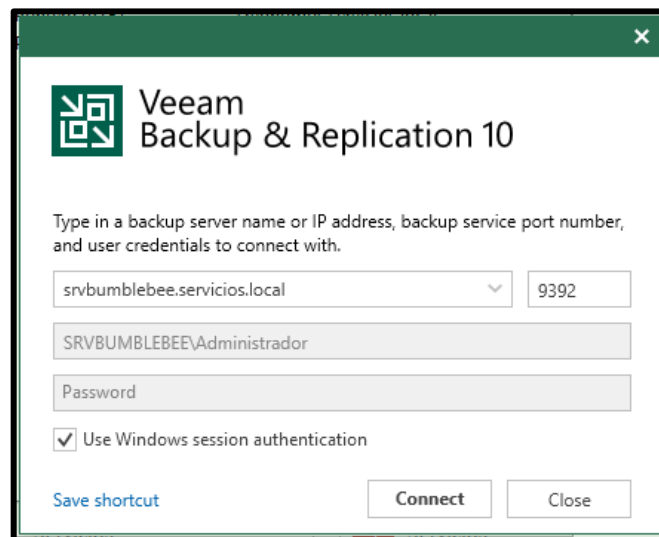
*Imagen 36. Configuración de Veeam*



*Imagen 37. Proceso de instalación*

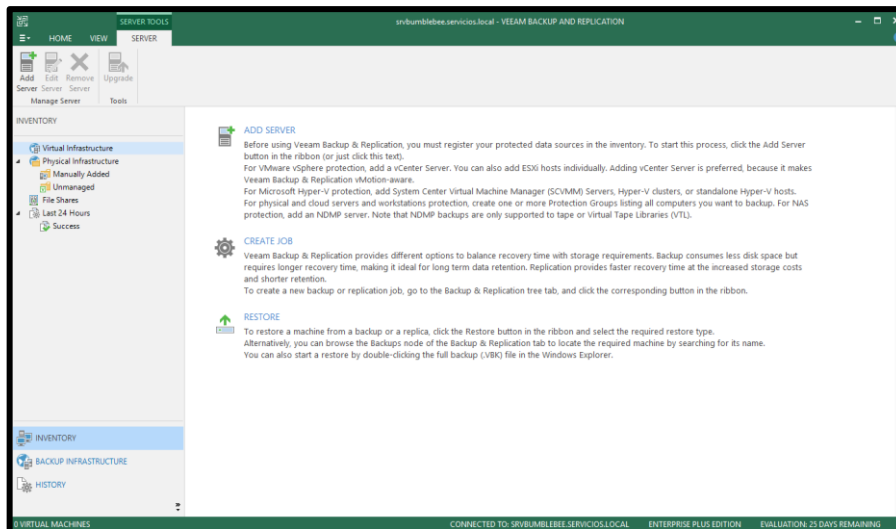


*Imagen 38. Primera pantalla de Veeam*



*Imagen 39. Usuario y contraseña para ingreso a Veeam*

Luego de la correcta instalación del software nos presenta la siguiente pantalla en la cual debemos ingresar el nombre de la maquina con el sufijo del DNS que fue configurado previo a la instalación, se va a requerir un usuario y contraseña el cual puede ser los mismo que los de la maquina o se puede crear un usuario y contraseña que tengo permisos de administrador para que pueda tener acceso al software, el software recomienda usar las mismas credenciales con las que se ingresa al Windows Server.



*Imagen 40. Ventana para agregar el Centro de Datos principal y el alterno*

Una vez que se ingresa nos muestra una interfaz muy amigable en la cual se va a realizar los procesos necesarios para la replicación del centro de datos principal y en caso de desastres el control del centro de datos alterno.

#### **6.1.4.6 Plan de continuidad del negocio en base a la norma ISO 22301**

Se necesita elaborar un plan para continuidad del negocio basándose en la norma ISO 22301 la cual permitirá que una empresa mantenga el funcionamiento de su centro de datos en un sitio alterno en caso de desastres y no perder información y posteriormente migrar toda la información almacenada al centro de datos principal y volver a la normalidad.

#### **Pasos para la continuidad de negocio**

- Identificar el tipo de amenaza
- Realizar un análisis del impacto en la empresa
- Realizar el levantamiento del sitio alterno
- Analizar el estado del sitio alterno
- Comprobar si la información que se tenía en el sitio alterno es la más actualizada
- Poner en funcionamiento el sitio alterno para la continuidad de negocio.

# CAPÍTULO VII

En el presente capítulo se dará a conocer el objetivo clave para la realización y ejecución de un plan de continuidad de negocio basados en la norma ISO 22301, para cada una de las empresas, ante la presencia de situaciones críticas que pongan en riesgo la continuidad de las actividades de los diferentes servicios y aplicaciones, manteniendo un tiempo mínimo de recuperación de sus actividades. Por lo tanto, cada una de las empresas deben estar prevenidas y protegidas, para reaccionar ante cualquier eventualidad que exista dentro de sus actividades mediante la creación e implementación de planes y preparativos de Continuidad de Negocio que permitan afrontar y prevenir la pérdida de la información de las actividades de cada empresa.

La Norma ISO 22301 definirá los procesos, y la capacidad que tendrá cada una de las estrategias utilizadas por las empresas, permitiéndoles mantener la continuidad de sus actividades.

## **7. Plan de Continuidad de Negocio.**

### **7.1 Liderazgo.**

Los Planes de continuidad de Negocio estarán liderados por cada uno de los gerentes de las empresas y por el personal encargado de los departamentos de TI que serán los responsables de gestionar y administrar los planes de continuidad de negocio y ante las diferentes situaciones críticas a las que las empresas pueden enfrentarse.

### **7.2 Política de la Continuidad de Negocio.**

El objetivo principal de cada una de las empresas es la de mantener la continuidad de sus actividades ante la presencia de posibles interrupciones, garantizando el buen funcionamiento de sus servicios y aplicaciones, mediante la implementación de medidas y estrategias planteadas mediante la norma ISO 22301 según las necesidades de cada una las

empresas, las mismas que permitirán mantener la continuidad de Negocio, en caso de existir situaciones críticas o de un desastre.

### **7.2.1 Objetivo.**

Se crearán e implementaran políticas que permitirán mantener la continuidad de Negocio, ante la existencia de posibles situaciones críticas que afecten en correcto funcionamiento de sus servicios.

### **7.2.2 Respaldo de la información.**

El encargado de los diferentes departamentos de TI será el encargado de realizar los respaldos de toda la información con mayor frecuencia ya sean estas automáticas o manuales, cumpliendo con las políticas basados en los procesos y estrategias de la Norma ISO 22301.

#### **7.2.2.1 Seguridad de la información y Respaldo.**

Dentro de la seguridad de información y respaldos tendremos varias políticas que se basan en lo siguiente:

- Los responsables del mantenimiento y respaldo de la información realizaran respaldos diarios conforme lo estipula las políticas de la empresa.
- Todo acceso a servicios y aplicaciones críticas serán restringidos mediante la utilización de un usuario y contraseña.
- Todas las sesiones personales en los equipos mantendrán el uso de una contraseña.
- Está prohibido compartir y entregar información sobre datos, contraseñas a personas ajenas a la empresa
- Todas las contraseñas y usuarios tendrán un tiempo límite de vigencia por lo que cada encargado deberá actualizar dicha información.



- Toda la documentación e información confidencial enviada por medios electrónicos deberá tener su respectiva seguridad de contraseñas.
- Se realizará actualizaciones a los equipos, servidores y demás recursos tecnológicos en lo que a seguridad y prevención de virus manteniendo la seguridad informática.

### **7.2.3 Roles y Responsabilidades.**

Las tareas de respaldo y recuperación de cada una de las áreas de trabajo deberán estar asignadas al personal capacitado el mismo que se responsabilizará de cumplir con los procesos y estrategias contempladas según la Norma ISO 22301 manteniendo la integridad y seguridad de la información, esta estará relacionada con la capacidad de mantener la continuidad de sus actividades ante situaciones críticas.

### **7.2.4 Pruebas.**

Se realizarán pruebas continuamente el plan de continuidad de negocio, en los cuales se dejará en constancia de los resultados obtenidos mediante actas, los cuales permitirán definir las diferentes situaciones, características, con el fin de mejorar en base a los resultados obtenidos y de tal manera que se pueden satisfacer necesidades o deficiencias en el plan con el objetivo de mejorar los resultados.

### **7.2.5 Consideraciones Generales.**

Las políticas creadas para mantener la Continuidad de Negocio son con el fin de mantener el compromiso de cada uno de los miembros de las áreas tecnológicas de mantener y mejorar los servicios y sus aplicaciones. Las políticas se basarán en los procesos y estrategias de la Norma ISO 22301 la misma que nos permitirá conocer los pasos que se deben seguir para obtener resultados positivos ante posibles situaciones de riesgo en la empresa y de esa manera continuar con el normal funcionamiento.

Las políticas creadas por la empresa sustentaran los principios de continuidad de Negocio que rige en la Norma ISO 22301 para lo que se registrará a las siguientes políticas generales:

- Todo empleado nuevo tendrá conocimiento de los diferentes planes de continuidad y desastres para mantener la prevención en cada una de las áreas de trabajo.
- Se designará un área de control que se encargará de mantener las actualizaciones de las diferentes políticas según exista sus requerimientos.
- Se realizarán pruebas y mantenimiento de los diferentes equipos.
- Existirán responsables de cada área que se encargara de cumplir funciones estrictas en caso de emergencias o situaciones de riesgo.
- Se realizará capacitaciones al personal responsable ante la prevención de situaciones de riesgo.

### **7.3 Norma ISO 22301.**

Dentro de la empresa es fundamental que se elija una metodología que permitirá identificar, evaluar, gestionar y controlar los posibles riesgos en sus servicios y aplicaciones críticas dentro de su Centro de Datos, que servirá para identificar las posibles amenazas y vulnerabilidades que ocasionaran interrupciones en sus sistemas, y de esa manera determinar cuáles fueron las causas, probabilidades y cuál es el impacto que puede provocar en la empresa, por lo tanto cada una de las empresas deberá realizar lo siguiente:

- Identificara las diferentes amenazas
- Identificara las vulnerabilidades.
- Determinará el impacto que puede provocar en la empresa.
- Determinará cuales son los riesgos basados en las amenazas, vulnerabilidades.
- Registrará los riesgos documentando toda la información.

- Identificar todos los riesgos en los procesos críticos y manejarlos de acuerdo a su nivel.

#### **7.4 Análisis de Riesgos y Vulnerabilidades.**

Dentro de la empresa se determinará las diferentes situaciones de riesgo tanto internas como externas, las mismas que afectaran negativamente el buen funcionamiento de sus actividades, y por otro lado se especificaran cuáles son las medidas optadas para prevenir y disminuir el impacto que si llegan a materializarse causaran daños y pérdidas económicas, así como una pérdida de la información importante. Por lo tanto, dentro de los procesos y pasos para la continuidad de Negocio contemplados en la norma ISO 22301 se sugerirá realizar los siguientes procesos para identificar las vulnerabilidades y riesgos dentro de una empresa.

##### **1. Conocimiento de las posibles pérdidas.**

- Identificarán las amenazas internas y externas que podrán causar una paralización de sus actividades tales como desastres naturales, situaciones externas, amenazas tecnológicas.
- Se identificarán por niveles los riesgos que servirán para una evaluación en el impacto y probabilidades.
- Se estimará cual será el impacto en la empresa y sus consecuencias.
- Se analizará la probabilidad de existir una amenaza
- Se calculará cual será el riesgo que mantendrá cada una de las amenazas de acuerdo a una formula.
- Se dará prioridad a las amenazas con un nivel más alto
- Se determinará los diferentes términos legales
- Realizar soporte continuo.

2. Se determinará la verificación de los procesos que servirán para prevenir impactos y pérdidas en las empresas
3. Se identificará, evaluará y escogerá la metodología apropiada que permitirá facilitar la evaluación y administración de riesgos.
4. Se revisará la eficiencia de los procesos de verificación que se implementaran.
  - Se realizará una planificación de los procesos de verificación a implementar
  - Se validará el costo/beneficio y cuáles son las prioridades
  - Se establecerá la comunicación efectiva sobre los acuerdos con los diferentes proveedores, organizaciones ligadas a la empresa, así como también con cada uno de los integrantes de la empresa.
  - Se clasificarán las respuestas significativas y productivas ante las amenazas o riesgos.
5. Evaluar y controlar riesgos
  - Se determinará los diferentes escenarios de desastres según los riesgos de la organización
  - Se clasificarán los riesgos dependiendo su nivel como riesgos de bajo control, riesgos más allá del control, riesgos con previo aviso (lluvias, tormentas, etc.) y riesgos sin previo aviso (desastres naturales como terremotos).
6. Administración de información vital.
  - Se identificará documentación e información electrónica importante para las empresas.
  - Se realizará los diferentes procedimientos para la recuperación de la documentación e información importante.

### 7.4.1 Identificación de Riesgos.

Durante el análisis de los riesgos y vulnerabilidades es necesario tomar en cuenta cuales son las medidas de impacto en la empresa o la magnitud del riesgo, por lo que se mantendrá en varios niveles o escalas simples, los mismos que permitirán a los responsables de cada área identificar cada uno y de esa manera poder actuar ante la presencia de riesgos y situaciones críticas.

Dentro de la siguiente tabla daremos a conocer cuáles son los niveles o escalas de riesgos dependiendo la probabilidad de que suceda o se presenten situaciones críticas las mismas que la empresa implementara su plan de continuidad.

Probabilidad	Referencia	Impacto	Referencia
No probable	1	Muy bajo	2
Poco Probable	2	Bajo	4
Posible	3	Medio	6
Probable	4	Alto	8
Muy probable	5	Muy alto	10

*Tabla 9. Tabla de probabilidad y referencia*

### 7.5 Impacto en la organización.

En base a los riesgos y vulnerabilidades establecidas dentro de la identificación de riesgos en la empresa, se analizará cual es el impacto en el negocio de la empresa el mismo que servirá para reducir la afectación a la continuidad de Negocio, considerando que los diferentes servicios que presta la empresa no se encuentren interrumpidos por un largo tiempo. Por lo que se definirá los diferentes tiempos de recuperación dando prioridad a los servicios de mayor importancia y necesidad.

Se tomará en cuenta todas las actividades que realiza la empresa las cuales pueden ser afectadas por una amenaza o riesgo siendo de suma importancia describir y establecer los diferentes escenarios y los puntos de afectación, Determinando en base a una categorización de los servicios y aplicaciones críticas de la empresa con el cual se podrá tener una visualización más clara de lo que puede ocurrir con la empresa.

### **7.5.1 Estrategias en la Recuperación.**

Se analizar los diferentes tiempos de recuperación basados en la visión del negocio por lo que se establecerá el tiempo de tolerancia a las interrupciones de cada uno de los procesos de las empresas y de los tiempos de recuperación a los que tienen cada uno de los dispositivos tecnológicos. Por lo que se establecerá objetivos en los tiempos de recuperación y tiempos de tolerancia.

- **Tiempo de Recuperación o RTO**

Es el tiempo en que un proceso necesita para restaurar y recuperar sus servicios después de una situación crítica antes de que entren nuevamente en funcionamiento, por lo tanto, sería la cantidad de información que se perderá durante la interrupción y la que tendrá que ser ingresada nuevamente.

- **Recovery Point Objective (RPO).**

Es la cantidad máxima en la que una organización puede perder la información, es decir que es la relación entre la última copia de seguridad realizada y el momento en que ocurrió un desastre, por lo que en sistemas críticos y de alta demanda de información este tiempo no supere los 15 min.

- **Recursos Humanos y Tecnológicos.**

Se determinarán los diferentes sistemas, aplicaciones, equipos y elementos auxiliares que necesitara cada proceso para su buen funcionamiento, y su tiempo de

recuperación, en caso de los recursos tecnológicos se considerara otras dependencias con infraestructura.

- **Working Recovery Time (WRT).**

Es el tiempo en el que ya se pudieron recuperar todos los sistemas y servicios de la empresa, es decir que sería el tiempo máximo tolerable en que la empresa necesitara para realizar la verificación de que todos sus servicios, aplicaciones y la integridad de la información se ejecuten de una manera correcta.

- **Tiempo máximo tolerable de Caída (MTD).**

Se determinará el tiempo en que un proceso pueda estar detenido antes de que los demás sistemas provoquen consecuencia o fallas significativas en los procesos que pondrán en riesgo la continuidad de Negocio.

- **Nivele mínimo de recuperación.**

Sera el nivel mínimo en que una actividad tiene para declararla recuperada, aunque el nivel de ejecución del servicio no sea óptimo.

#### 7.5.1.1 Recuperación de la información digital de los clientes.

Toda la información de los clientes es vital en la empresa ya que esto permitirá la reanudación de las actividades luego de una interrupción de sus servicios permitiendo generar la confianza de los clientes y por ende generará una gran imagen de responsabilidad de la empresa

#### 7.5.1.2 Recuperación de Servidores.

La Recuperación de todos los servidores es importantísima ya que estos permitirán continuar con las actividades, tomando en cuenta el sitio alternativo en donde se levantarán los servicios uno por uno hasta la recuperación de su sitio principal.

## **7.6 Determinación del Alcance.**

El alcance de este plan tendrá una concentración importante en los servicios y aplicaciones críticas de la empresa en donde tendrá un mayor impacto ante posibles interrupciones y pérdida de la información.

## **7.7 Descripción del Plan de Continuidad de Negocio**

### **7.7.1 Descripción en Base a la ISO 22301**

Dentro de las diferentes normas ISO que permite a las empresas mantener la continuidad de Negocio de acuerdo a diferentes análisis es la norma ISO 22301 en la misma que nos basaremos ya que nos permite identificar los escenarios y nos brinda los procesos y estrategias a seguir para ejecutar y administrar los procesos de una manera correcta frente a las diferentes situaciones que pongan en riesgo la continuidad de negocio de la empresa, planteándose en la aplicación de los recursos que dispone y brindar los servicios disponibles hasta la regulación en su menor tiempo posible y en un menor costo.

Se tomó en cuenta esta norma ISO 22301 por que abarca todos los parámetros de administración que permitirá posteriormente realizar la revisión de los riesgos para estar prevenidos ante la presencia de cualquier situación de riesgo y su efecto sea menor en la organización, de esta manera se evitará que las interrupciones sean mayores al tiempo estipulado en los diferentes planes.

La Organización Internacional de Normalización en el año 2012, dio a conocer sobre el estándar “Seguridad de la Sociedad: Sistemas de Continuidad de Negocio y Requisitos” en el que la Norma ISO 22301 implementa el ciclo Plan-Do-Check-Act (PDCA sus siglas en inglés) la misma que nos permitirá realizar una planificación, instalación, ejecución, administración, revisión, mantenimiento para mejorar la efectividad continua de las organizaciones.



## **7.7.2 Plan de Recuperación de Desastres (Disaster Recovery Plan - DRP)**

### **7.7.2.1 Introducción.**

El siguiente plan de recuperación de desastres nos permitirá estar en la capacidad de actuar ante situaciones de riesgo que pueden causar interrupciones y afecten el normal funcionamiento de las actividades de la empresa y todos sus servicios relacionados ya sean de manera interna o externa, en donde el cliente llegaría a perder su información, es por ello que la característica fundamental del plan de recuperación de desastres es la de recuperar los servicios y aplicaciones críticas.

En los procesos detallados en el Plan de Recuperación de Desastres deben constituir todos los responsables y sus roles que cumplirán para poder solventar y garantizar el correcto funcionamiento de los recursos de cada empresa como son: Recursos Humanos, Recurso de Infraestructura, Procesos, Servicios, Aplicaciones Críticas y Documentación Vital para la organización, y que el impacto en la organización sea mínimo en lo que a pérdida de la información y de los recursos.

### **7.7.2.2 Descripción DRP.**

#### **Objetivos del Plan.**

- Definir los procesos de procesos y estrategias de recuperación y reanudación de las actividades ante la presencia de situaciones riesgo y de riesgo en la ejecución de los servicios y aplicaciones críticas en los principales servidores y su red de comunicación.
- Se realizará una restauración y recuperación ordenada de los servicios y aplicaciones de la empresa quienes dependerán de una infraestructura.
- La optimización del Plan de Recuperación de Desastres implicara que todos los procesos de recuperación han iniciado y se mantendrán con prioridad para mantener la continuidad de los servicios y reanudar la funcionalidad de la empresa.

### **Servicios críticos a proteger.**

La conservación de los servidores que es uno de los factores primordiales para mantener la continuidad de Negocio en la empresa, ya que poseen todos sus servicios, aplicaciones críticas y la información vital, por lo que los principales servicios de deberán proteger y administrar son:

- La comunicación de Red sy su conectividad a internet
- DNS – DHCP
- Correo
- Controlador de Dominio
- Archivos
- Aplicaciones Criticas
- Maquina Individuales
- Respaldos
- Base de datos

### **Incidentes y Contingencia.**

El siguiente plan de Recuperación de Desastres se implementará en circunstancias o casos de:

- En situaciones de riesgo en las que se puedan ver afectadas las actividades de la empresa en sus servicios y aplicaciones por un tiempo de 24 horas.
- En situaciones de riesgo en la que se vean afectados los equipos y la infraestructura de red, por accidentes que mantengan al margen el normal funcionamiento de las actividades. En los que se incluirán los procesos de administración de los departamentos de TI.

Por otro lado, las situaciones en la que se pueden ver afectados el correcto funcionamiento de los equipos serán por las siguientes circunstancias:

- Suspensión de la energía eléctrica/variación/fluctuación.
- Fuego
- Agua
- Fenómenos Naturales
- Fenómenos Climáticos
- Robo
- Virus

En los diferentes escalones de la seguridad de las aplicaciones las cuáles serán necesarios procesos y estrategias de circunstancias en distintos tipos y escalones en la recuperación, el plan cubrirá procesos en lo siguiente:

- Una recuperación parcial: recuperación que se dará a un sitio alterno.

#### **Seguridad física.**

Por normativa y monitoreo la infraestructura contarán con sensores que permitirán verificar la humedad, temperatura y humo, así como la instalación de UPS's en cada uno de los servidores que mantendrán activos por un tiempo ante la suspensión de energía eléctrica hasta restablecerlos por otro medio.

#### **Energía eléctrica y controles.**

Se valorará el servicio de energía eléctrica y del ambiente en donde se alojan los servidores, los cuales contarán con equipos y medios que impidan el corte, variación o sobrecarga de la energía eléctrica en los servidores que podrían sufrir averías.

Se monitoreará mediante los sensores, la presencia de humedad, temperaturas altas, y que el aire acondicionado no origine aire seco ya que esto producirá falas eléctricas.

#### **Protección sobre Software Malicioso.**

La empresa cumplirá con los requisitos de mantener actualizado las licencias y Software de protección contra virus y amenazas de cualquier Software que pueda atacar las diferentes

infraestructuras de red. Por otro lado, cada uno de los equipos de la red empresarial deberá contar con el antivirus empresarial.

### **7.7.2.3 Preparación antes de un desastre.**

En este punto se detallarán los procedimientos fundamentales para prepararse y prevenir situaciones de riesgo ante un desastre, y cuáles son las acciones que se ejecutarán durante una recuperación, en donde uno de los puntos principales de la recuperación es la de garantizar los respaldos externos estén realizados y actualizados de una manera correcta, así como los servicios y aplicaciones críticas.

#### **Procedimientos Generales.**

Las acciones principales que se realizarán rápidamente ante una situación de riesgo, que estarán respaldadas por un cronograma en los que se aprobarán los tiempos de recuperación y procesos para la reanudación de las actividades de la empresa de acuerdo a sus niveles y daños que haya provocado el incidente.

### **7.7.2.4 Plan de Recuperación.**

#### **7.7.2.4.1 Plan de Recuperación de los Servicios.**

La recuperación de servicios dentro del plan, es un proceso que iniciara inmediatamente luego de que ocurrió la interrupción de las actividades por alguna situación de riesgo que afectara su funcionamiento, cuando el desastre causo daños en el sitio principal, es necesario realizar la ejecución de un sitio alternativo, reanudándose las actividades de la empresa en un tiempo menor por lo que deberá realizar lo siguiente:

- Se determinará el impacto que provoco en la empresa el incidente
- Se analizará el costo de recuperación.

Para la ejecución de un sitio alternativo se necesitará lo siguiente:

- Se informará al encargado y responsable del sitio alternativo para la ejecución de la recuperación.

- Disponer ordenadamente el movimiento de los equipos al sitio alterno.
- Determinar las operaciones en el sitio alterno.
- Disponer planes de largo plazo y su soporte.

## **7.8 Socialización del plan.**

### **7.8.1 Situación Actual.**

Se determinarán los diferentes componentes, beneficios, técnicas y algunas características que posee actualmente la empresa, ya que, en función de estos, se describirá los procesos críticos que se consideraran para verificar las diferentes áreas y sus diferentes equipos.

#### **7.8.1.1 Procesos Levantados.**

Se detallarán todos los procesos y dispositivos que se encuentran dentro de la empresa para poder realizar los procedimientos de recuperación para la continuidad, en donde se considerará los servidores, equipos utilizados por el personal en donde se identificara los procesos más críticos que deben ser restaurados inmediatamente.

#### **7.8.1.2 Identificación del Escenario.**

Se debe mencionar que al momento de sufrir interrupciones en la actividad de una empresa en lo que sería su agencia principal sus sucursales también perderán el acceso de sus servicios ya que se cuenta con un enlace principal entre las sucursales y la agencia principal en cuanto al acceso de servicios y aplicaciones críticas.

# CAPÍTULO VIII.

## 8.1 Escenario

En el presente capítulo mediante un escenario demostraremos los pasos previos que debe tener una empresa para la recuperación de la información ante situaciones críticas en un centro de datos evitando la pérdida de información y servicios, entre los pasos que se va a presentar se debe tener en cuenta que primero deberán contar con un sitio alternativo en el cual se pueda realizar una copia de seguridad constante de todo el centro de datos, un administrador el cual en caso de ocurrir un desastre es el encargado de realizar el levantamiento del sitio alternativo.

Dentro de los diferentes escenarios críticos que pueden presentarse dentro de una empresa en los que se vean afectados los diferentes servicios y aplicaciones críticas, y en consecuencia de ello se mantendrá una interrupción de sus actividades, produciendo un impacto en la organización y varias pérdidas económicas.

Mediante la evaluación de riesgos y vulnerabilidades utilizando una metodología contemplada en la Norma ISO 22301 que hace referencia dentro del plan de continuidad de Negocio se obtuvo que la empresa se ve amenazada por una catástrofe natural en la que se encuentran afectados los servidores en el cual se perdió el enlace de datos, comunicación y red de nuestra empresa hacia los clientes.

Se tomó en cuenta el posible escenario que puede afectar al normal funcionamiento de la empresa y cuáles fueron los posibles riesgos que se puede sufrir por lo que se detallara a continuación:

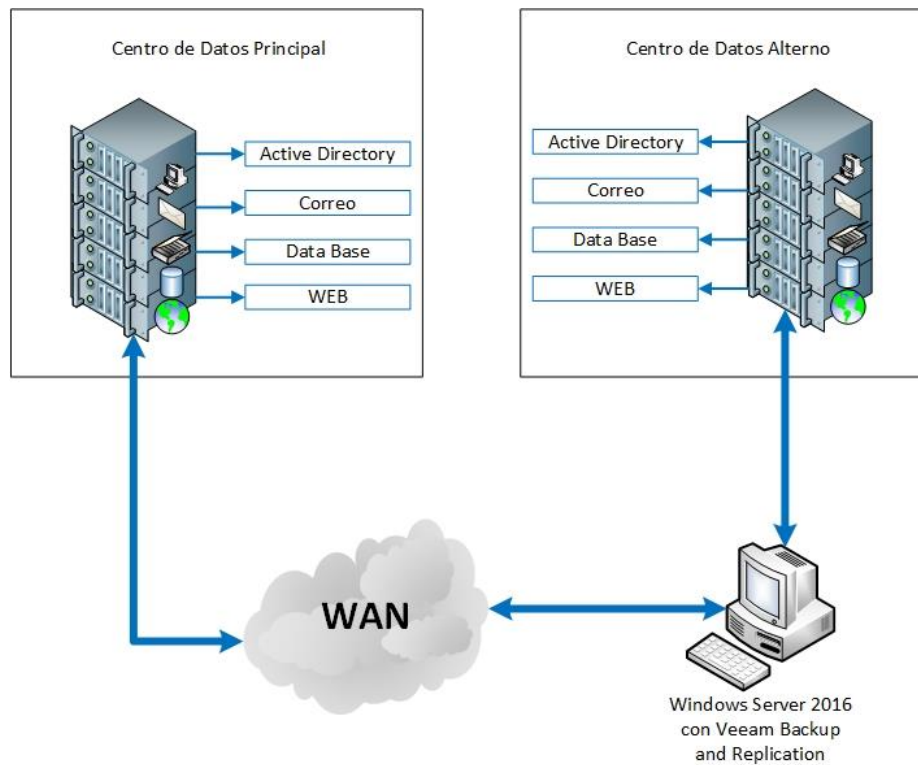


Imagen 41. Diagrama de ubicación de Equipos

### 8.1.1 Caso 1

Riesgo:	Incendio
Probabilidad:	Posible
Impacto:	Alto
Escenario:	<p>En caso de producirse un incendio de gran magnitud en nuestras instalaciones, el impacto en nuestra empresa será de: pérdidas humanas, información vital de los clientes, servicios digitales, ya que dentro de las instalaciones se encuentra personal que se encuentra monitoreando y administrando cada uno de los procesos que ahí funcionan, quienes se verían afectados rápidamente.</p> <p>Al momento de producirse el incendio este afectaría directamente al centro de datos ubicado en la planta baja del edificio en un cuarto</p>

	<p>acondicionado para su funcionamiento, provocando una gran pérdida económica y una interrupción en los servicios y aplicaciones, ya que los servidores centrales se destruirán y a consecuencia de ello toda la información en ellos almacenado, dejando como resultado una pérdida total.</p>
<b>Afectación:</b>	<p>Durante el incendio se verán afectados las instalaciones en donde están ubicadas las diferentes dependencias las mismas que están equipadas con materiales de oficina altamente combustibles que aumentara la propagación del fuego por todo el edificio.</p> <p>Por otro lado, se vería afectado el centro de datos ubicado en la planta baja ya que ahí esta almacenada información vital, servicios y aplicaciones críticas de los clientes por lo que produciría una pérdida total de comunicación.</p>
<b>Acción:</b>	<p>Se evacuará a los empleados de las diferentes oficinas para evitar que existan pérdidas humanas.</p> <p>Dependiendo del grado y magnitud del incendio los responsables de realizar la recuperación de la información dentro de los servidores mediante los procesos y estrategias planteadas en la norma ISO 22301 que permita y regula la continuidad de Negocio.</p>
<b>Responsable:</b>	Departamento de tecnología

*Tabla 10. Escenario de prueba caso 1*



### 8.1.2 Caso 2

<b>Riesgo: Fallas de Comunicación y de Red</b>	
<b>Probabilidad:</b>	Posible
<b>Impacto:</b>	Alto
<b>Escenario:</b>	Nuestra empresa mantiene un enlace tanto para las comunicaciones y red de datos, por lo que la producirse un fallo en este enlace se perderá la conexión a los diferentes servicios y aplicaciones entre la empresa y los clientes
<b>Afectación:</b>	Se verían afectados los clientes ya que no podrían ingresar y ocupar los servicios brindados por la empresa.  También se afectaría el respaldo automático de la información vital del centro de datos.
<b>Acción:</b>	Se mantendrá protegido y asegurado el centro de datos, realizando un mantenimiento y verificación del cableado que comunica tanto interna como externa a los clientes y empleados.  En caso de un fallo o daño en la estructura de red se realizará la recuperación de la información al sitio alternativo de la empresa para evitar una pérdida de la información mientras dure el arreglo del sitio principal.
<b>Responsable</b>	Departamento de tecnología

*Tabla 11. Escenario de prueba caso 2*

Al mantener estos dos escenarios en lo que la probabilidad de que suceda es alta, se realizara los siguientes pasos para realizar la recuperación de la información en caso de que exista una pérdida total de los servidores o una falla en la comunicación entre el enlace de datos.

## 8.2 Conexión con el centro de datos principal

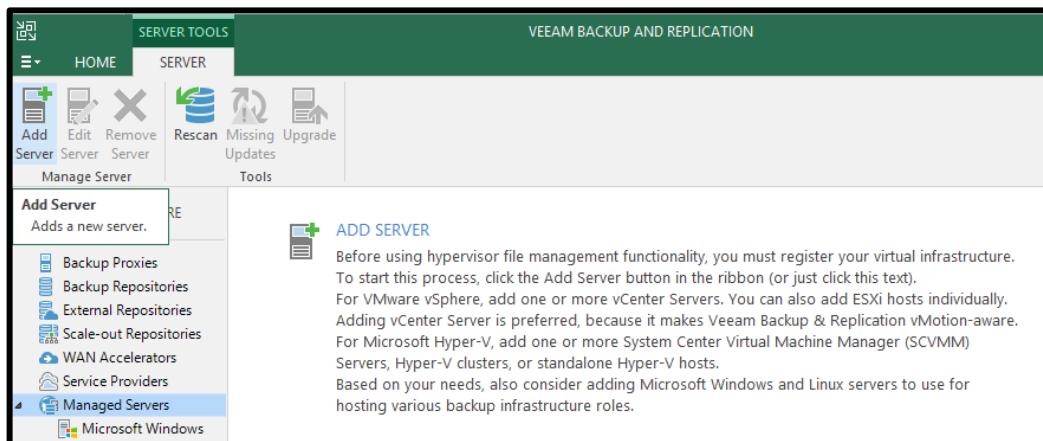


Imagen 42. Conexión con el Centro de Datos

Lo primero que se realiza es agregar el centro de datos principal por medio de los siguientes pasos los cuales se realiza de una manera fácil e intuitiva.

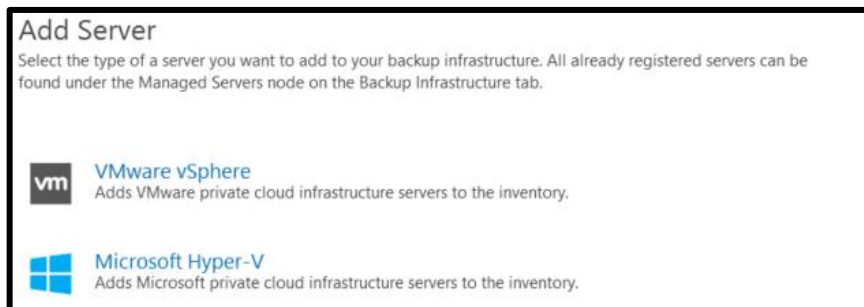


Imagen 43. Selección del tipo de Hypervisor

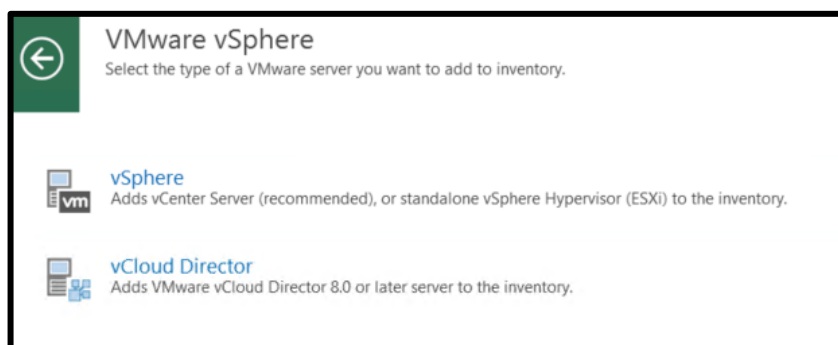


Imagen 44. Hypervisor físico o en la nube

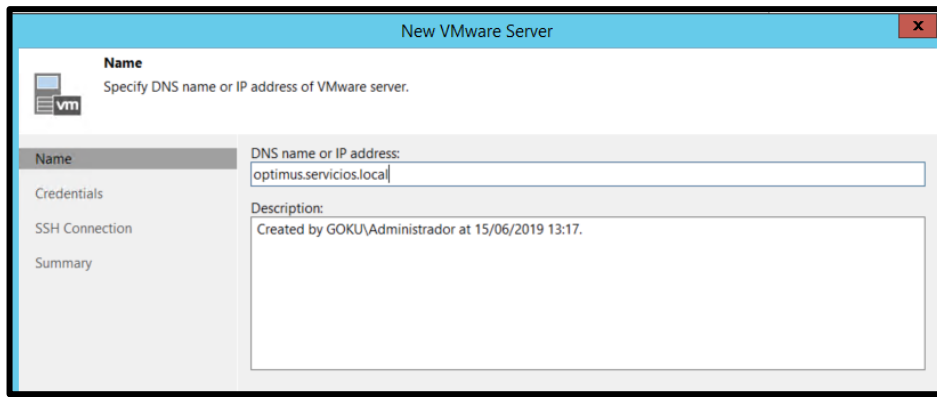


Imagen 45. Nombre de Centro de Datos para la conexión

Escoger la conexión mediante vSphere ya que se está ocupando el Hypervisor ESXi, luego de eso se escoge dentro de las dos opciones que nos dice si el centro de datos es físico o se encuentra en la nube, se agrega ya sea el nombre de la máquina con el sufijo DNS o la IP del centro de datos.

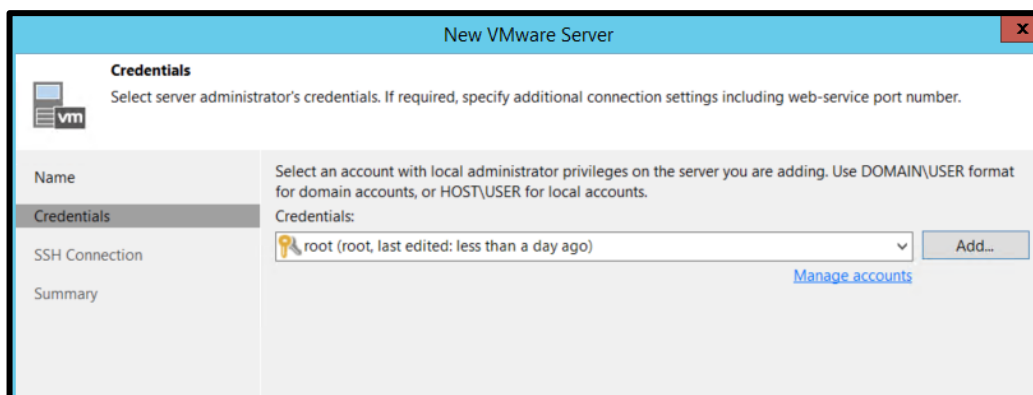


Imagen 46. Llave de ingreso

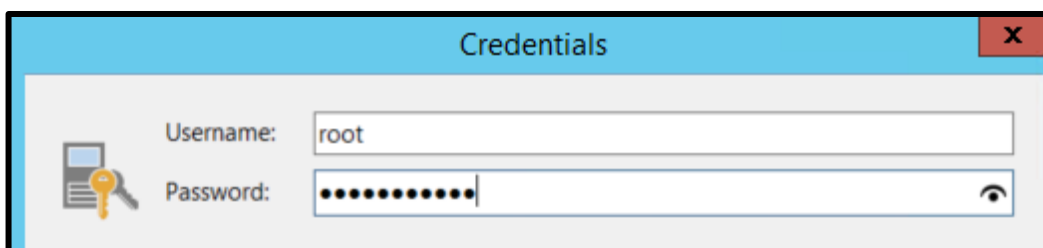


Imagen 47. Usuario y contraseña para la conexión

Se proporciona las credenciales con las cuales se va dar acceso al centro de datos, estas credenciales son las mismas con las que se configuro en centro de datos.

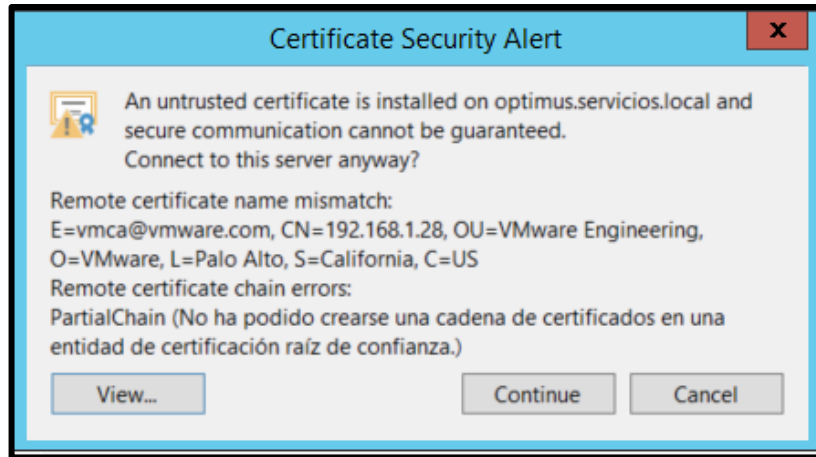


Imagen 48. Certificado de conexión

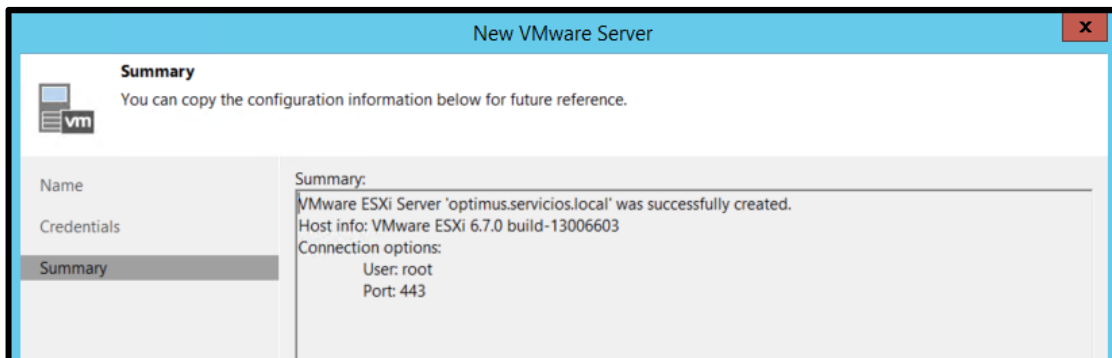


Imagen 49. Conexión establecida

Se aceptan los certificados de seguridad que proporcionen el software y se realizó la primera conexión del centro de datos con el Veeam.

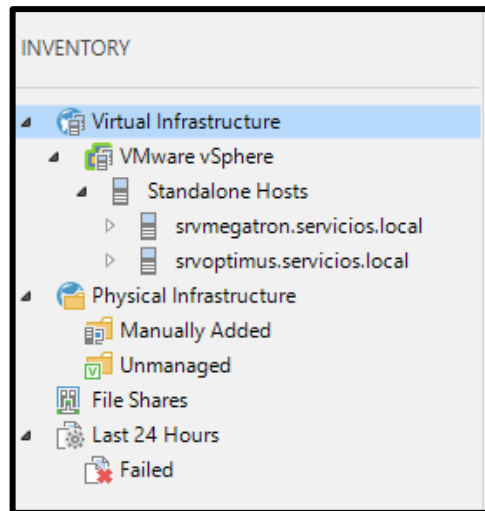


Imagen 50. Centro de Datos principal y alterno listos para trabajar

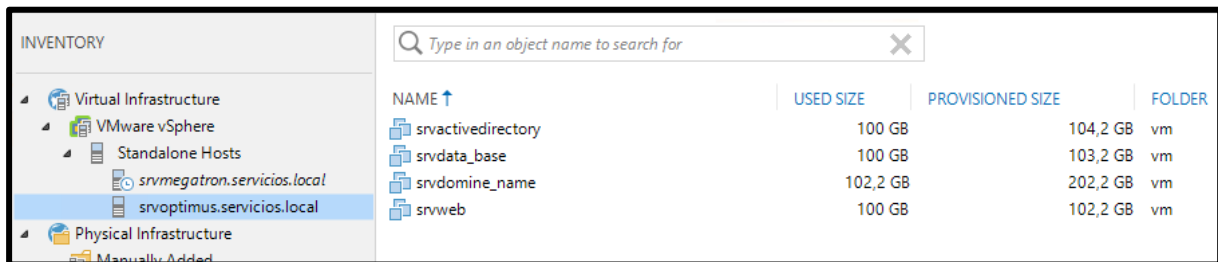


Imagen 51. Servicios que van a ser replicados

Cuando el centro de datos ya se agregó al software aparece todas las máquinas virtuales que contienen los servicios configurados previamente.

De igual manera se realiza el mismo proceso para el centro de datos alterno y de esta manera se tendría lista las conexiones para empezar con replicación del centro de datos.

### 8.3 Replicación de centro de datos

Dentro de la replicación del Centro de Datos principal al sitio alterno luego de realizar el análisis de riesgos y vulnerabilidades enmarcados en la norma ISO 22301 y que puedan afectar al normal desarrollo de las actividades se realizara los siguientes procedimientos

Se ingresara el nombre del procedimiento en este caso ingresaremos el nombre como Replicacion:

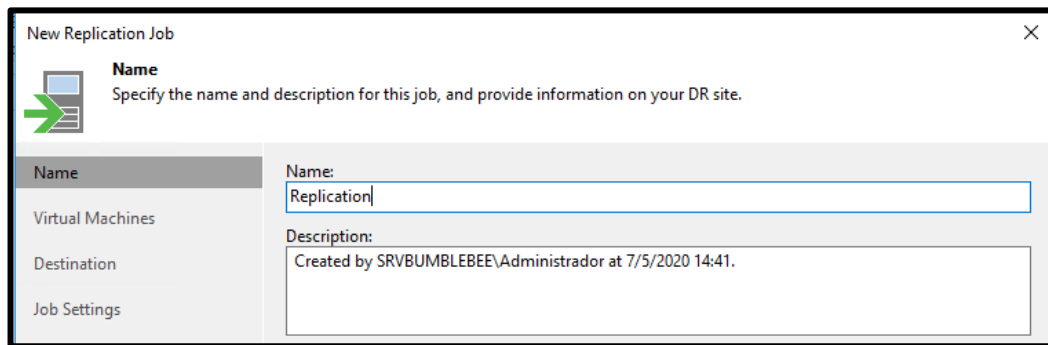


Imagen 52. Nombre del proceso a ser realizado

A continuación, se seleccionará el nombre de las diferentes máquinas virtuales o servidores a ser replicados:

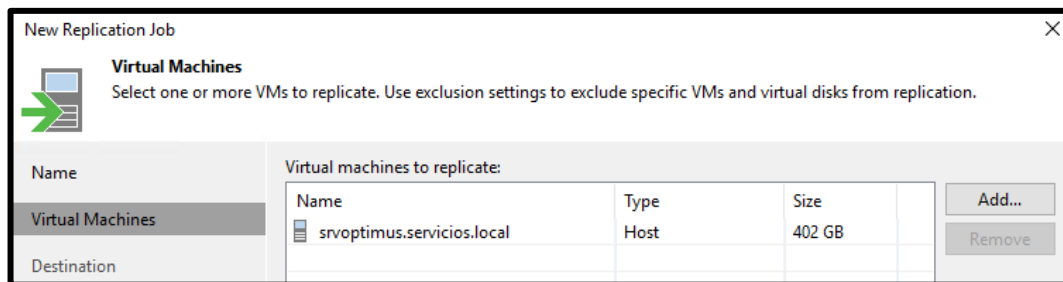


Imagen 53. Selección del Centro de Datos principal

Se seleccionará el destino a la que se va a realizar la replicación en este caso se seleccionara el sitio alterno el mismo que permitirá el normal funcionamiento de las actividades ante posibles interrupciones.

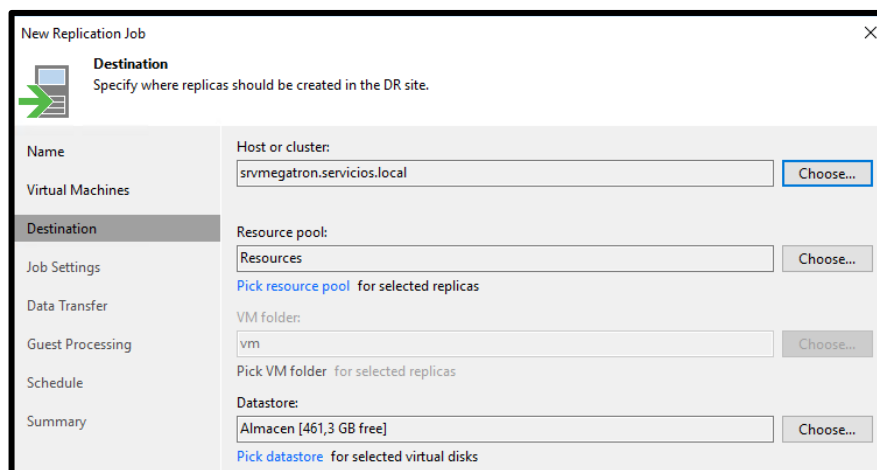


Imagen 54. Seleccionar el destino para la replicación

Luego se realizará las configuraciones necesarias para la realización de la replicación.

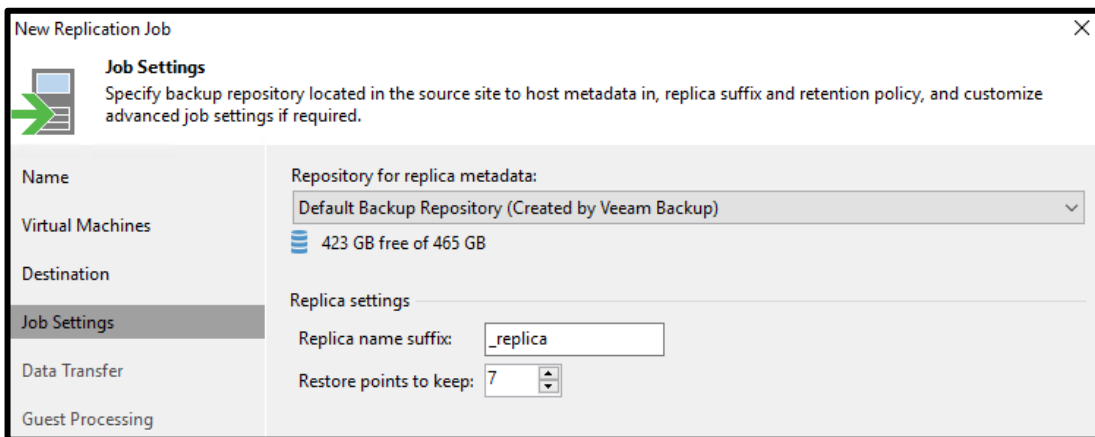


Imagen 55. Configuración para el trabajo que se va a realizar

Se verificará los datos que van a ser transferidos durante la replicación.

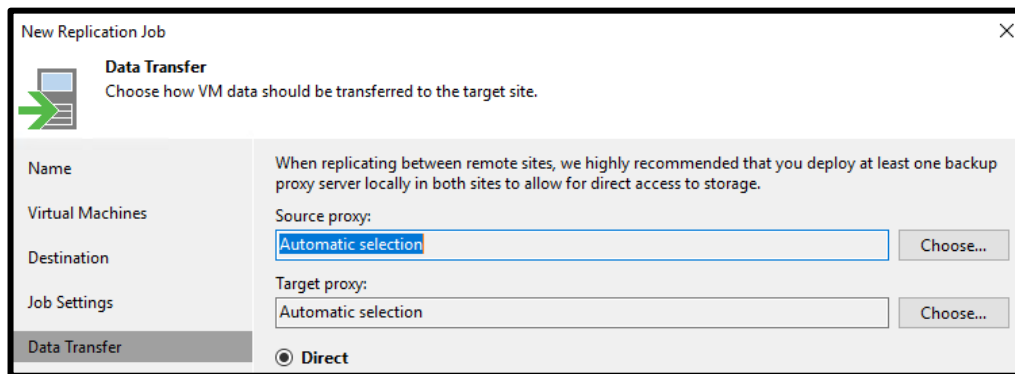


Imagen 56. Datos que se van transferir

Se configurara el periodo o tiempo en que el sistema realizara la replicación 112 automática

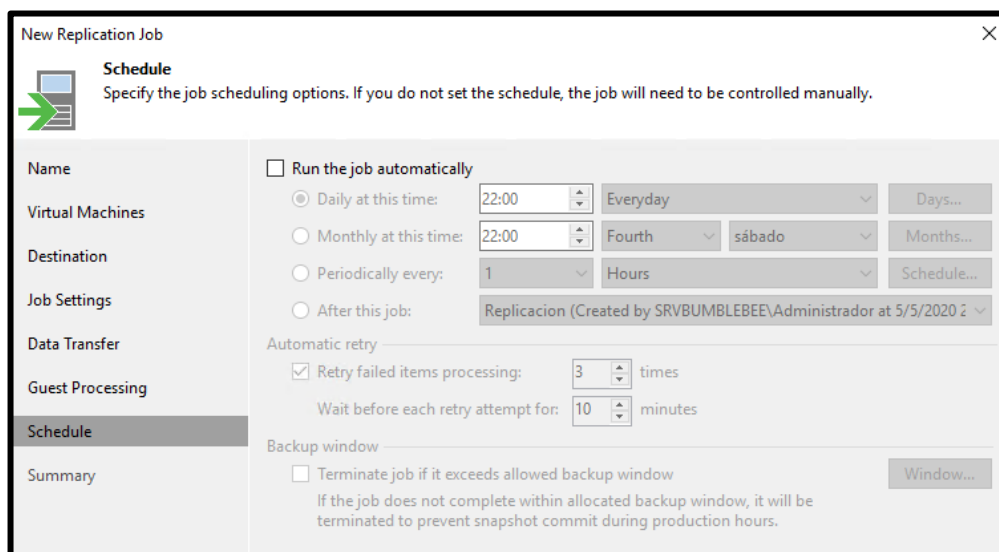


Imagen 57. Configurar un horario de replicación

No muestra la información del trabajo a replicación que se va a realizar

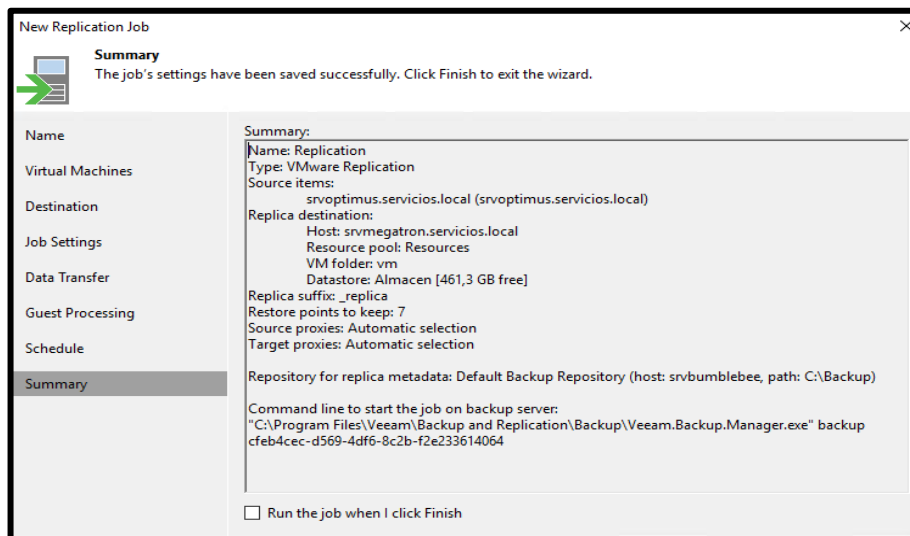


Imagen 58. Información del trabajo que se va a realizar

El proceso de replicación del centro de datos principal al alternativo se realiza ya sea máquina por máquina o su vez el centro de datos completo, en este caso se va a realizar una replicación del centro de datos completo, lo primero que se tiene que hacer es dar un nombre a la tarea que se va a realizar y luego de eso escoger el centro de datos principal, escoger el destino a donde se va ir en este caso a centro de datos alternativo, los pasos siguientes se los deja por defecto hasta llegar a un paso que es de suma importancia para la funcionalidad del centro de datos alternativo el cual es definir si se quiere realizar una replicación por una sola vez o crear un horario de replicación el cual permite tener el centro de datos actualizado, una vez acabada esta configuración empezará el proceso de replicación el cual puede tomar un tiempo por ser la primera vez luego va a ser un proceso más rápido.



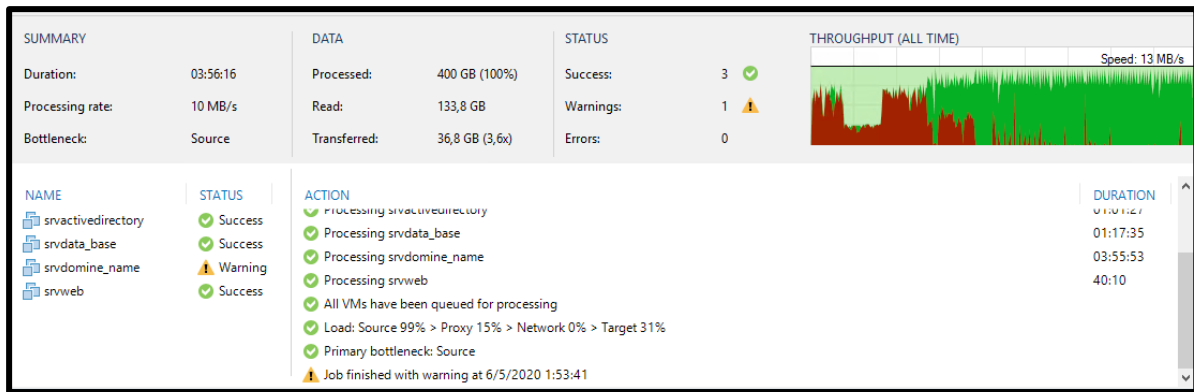


Imagen 59. Proceso de replicación

En todo el proceso de la réplica se va viendo cada paso que se realiza y de esta manera se asegura que el proceso se finalizó de manera efectiva.

En nuestro caso este proceso fue el más largo aproximadamente tomo unas 4 horas por el tipo de infraestructura que contamos, en una situación real este proceso va a ser más rápido y eficiente para la empresa.

## 8.4 Lanzamiento del plan para la continuidad de negocio

Una vez que se realizó el proceso de replicación de los servicios un administrador debe estar pendiente de que cuando suceda algún tipo de desastre debe crear un plan de conmutación por error, en este caso viene siendo en caso de suceda algún desastre debe funcionar de manera inmediata el centro de datos alterno.

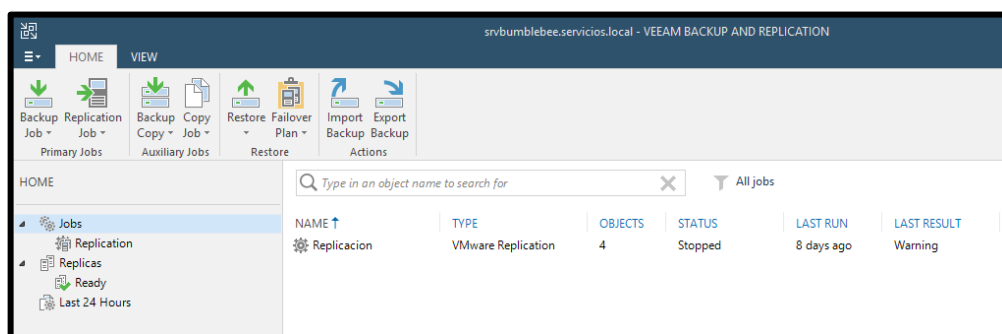


Imagen 60. Replica realizada en el Centro de Datos alterno

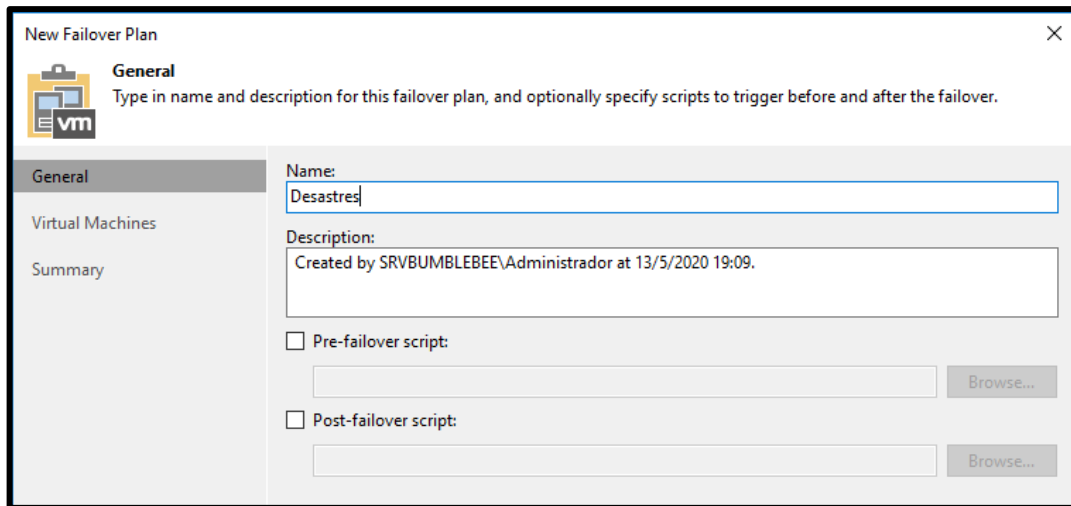


Imagen 61. Nombre de trabajo en caso de Desastres

Se debe dar un nombre con el que se pueda identificar el tipo de trabajo que se va a realizar en caso de que suceda un desastre.

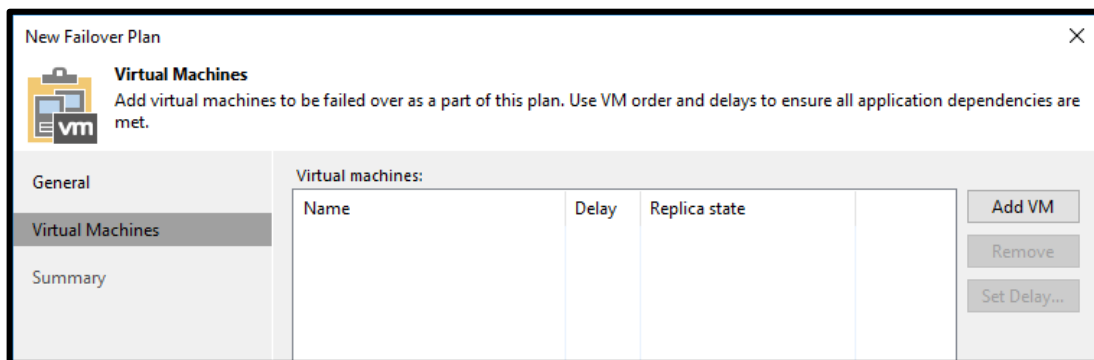


Imagen 62. Selección las máquinas para el trabajo

Agregar las máquinas virtuales que en este caso son los servicios que fueron replicados previamente.

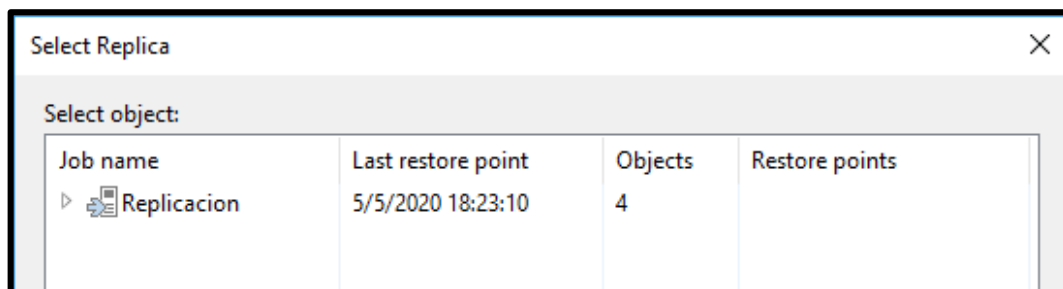


Imagen 63. Selección de la réplica realizada

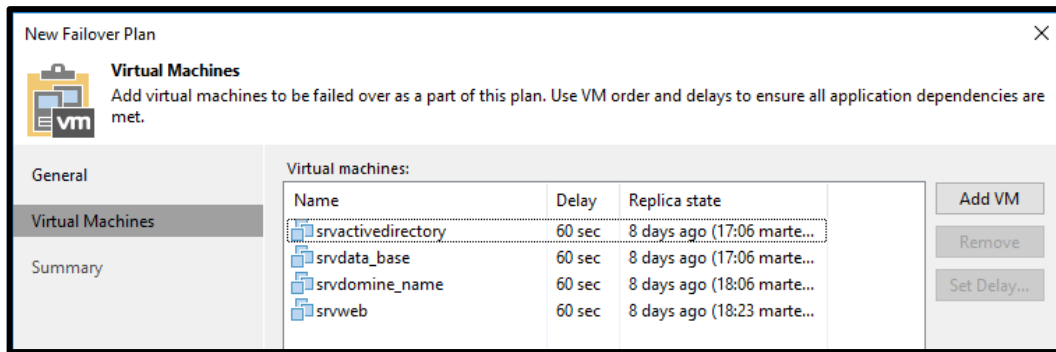


Imagen 64. Máquinas Virtuales que van a reemplazar a las principales

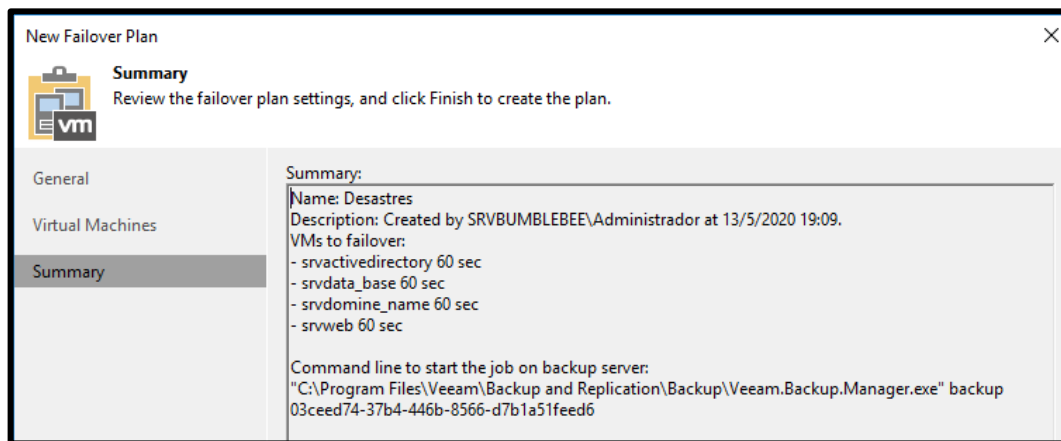


Imagen 65. Información del trabajo que se va a realizar

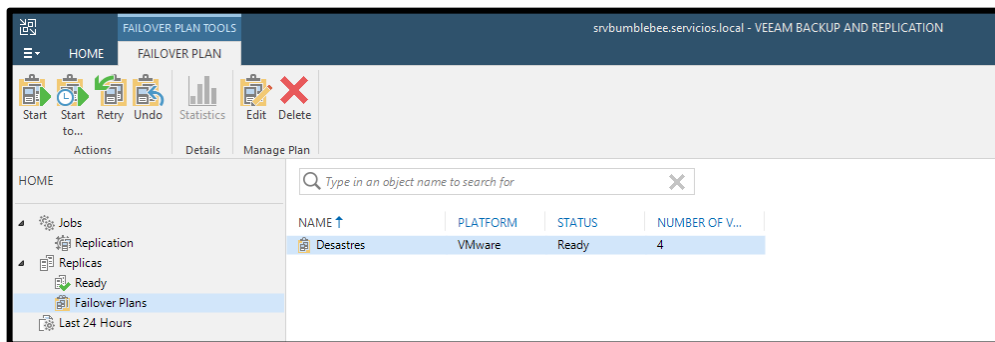


Imagen 66. En espera de que ocurra un desastre

Una vez creado el plan de conmutación por error ya está todo listo en caso de un desastre o una falla del centro de datos principal, un administrador debe estar pendiente en caso de que esto llegue a pasar para poner en funcionamiento lo que fue creado.

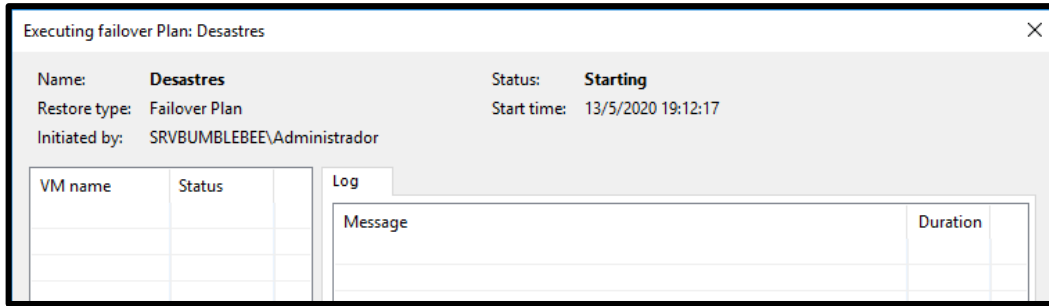


Imagen 67. Empieza a trabajo

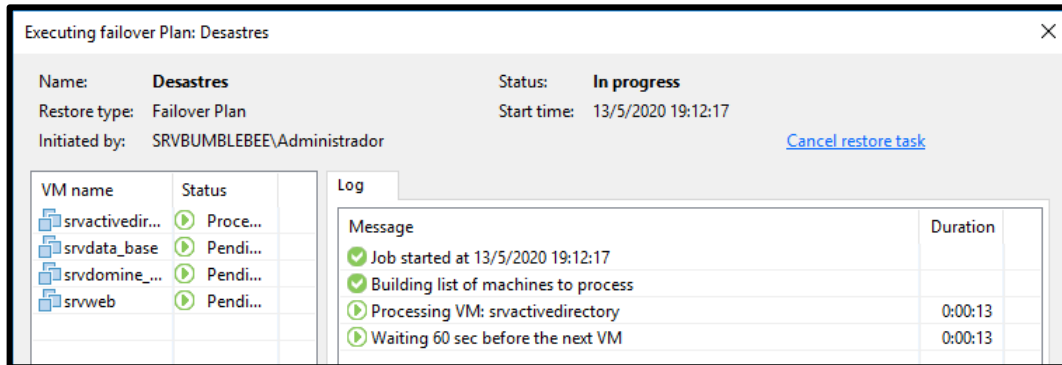


Imagen 68. Levantamiento de las maquinas en el Centro de datos alterno

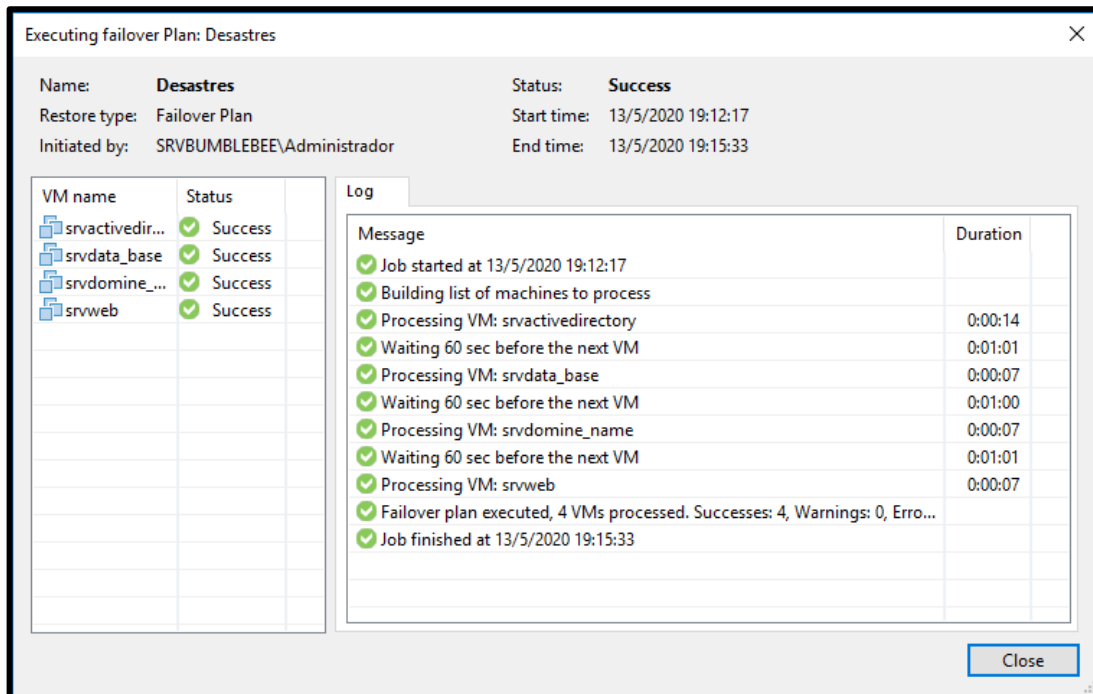


Imagen 69. Trabajo terminado y funcionando al 100%

El tiempo que los servicios vuelvan a su funcionamiento mediante el centro de datos alterno depende en las características del mismo centro de datos y con qué velocidad se prendan las máquinas virtuales.

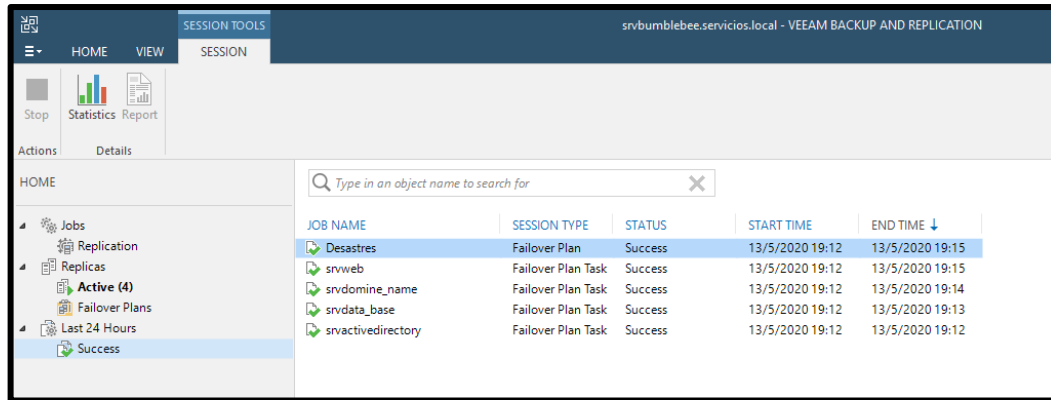


Imagen 70. Maquinas activas en el Centro de Datos alterno

Una vez que la empresa resolvió los problemas del centro de datos principal nos da la opción para retornar las maquinas hacia el centro de datos.

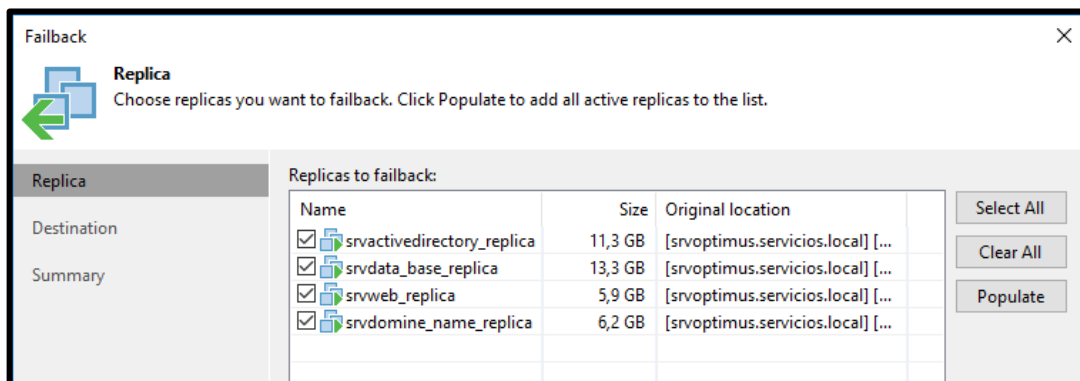


Imagen 71. Retorno de las maquinas al Centro de Datos principal

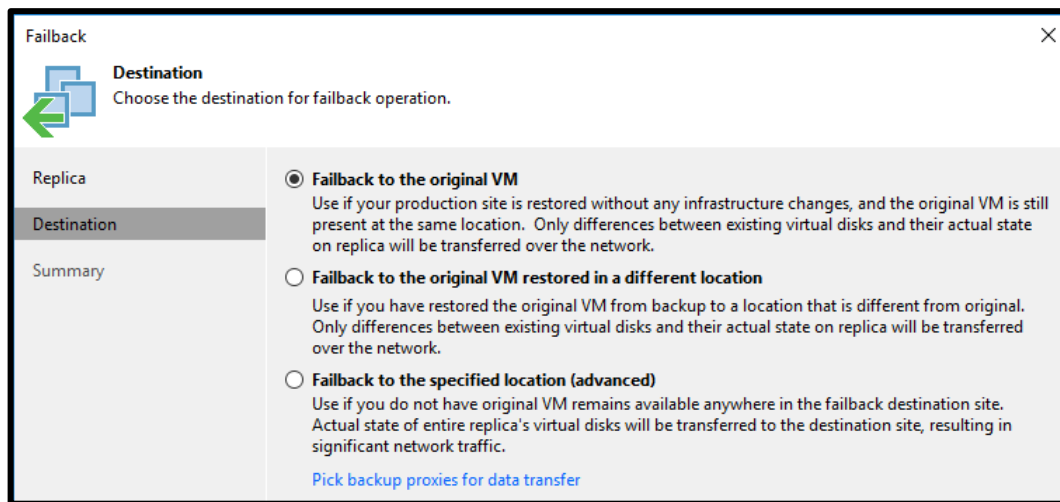


Imagen 72. Selección del tipo de trabajo que va a realizar

Veem ofrece un opción que permite recuperar la información que fue almacenada en las maquinas replicadas, ofrece tres tipos de opciones la primera mantiene la misma estructura original y solo agrega la información que falta, las otras dos mueve las maquinas a una ubicación diferente, el más factible para cualquier empresa es regresar a su propio centro de datos el único inconveniente en que tiene que analizar todo el centro de datos y luego de eso puede empezar agregar la información restante.

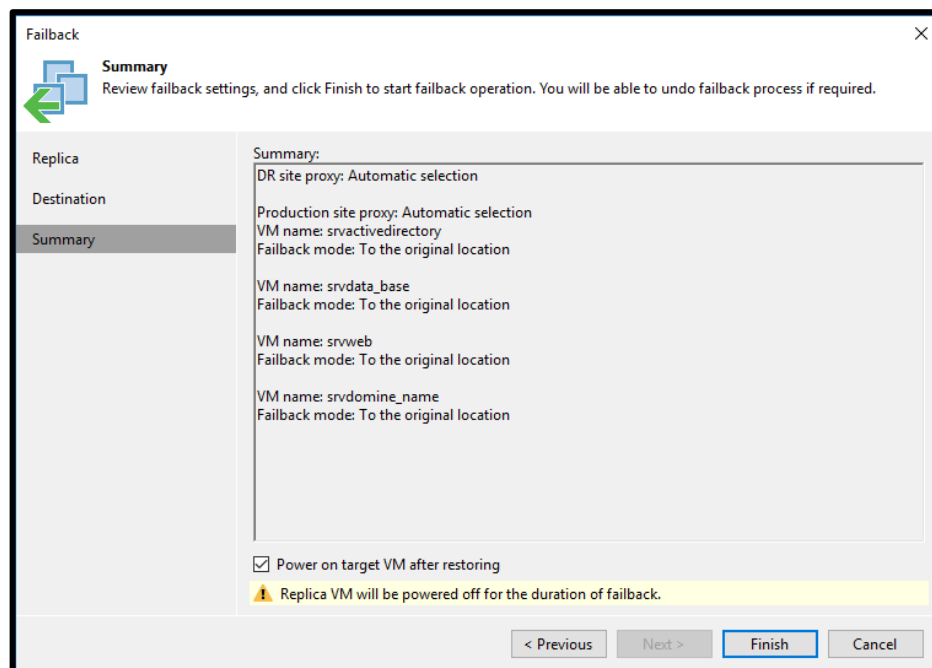
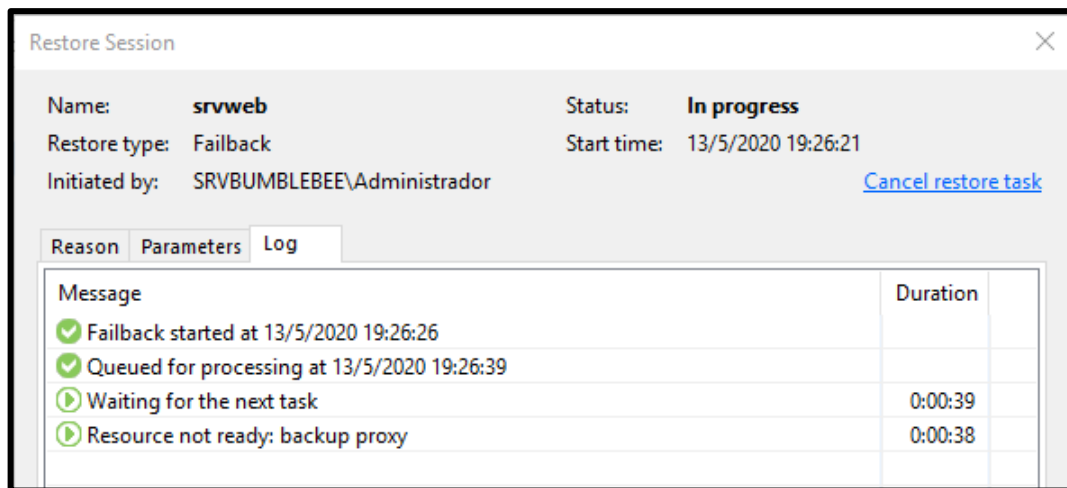


Imagen 73. Retorno al Centro de Datos principal listo para empezar



*Imagen 74. Proceso de Retorno de la Maquinas*

El tiempo que demore en analizar y restaurar la información adicional dependerá netamente de la red que se tenga y de la velocidad de procesamiento de los dos centros de datos.

Cuando acabe todo el proceso va a volver a funcionar con normalidad en el caso del centro de datos principal, en el caso del centro de datos alterno seguirá existiendo y recibiendo la replicación del centro de datos principal, estará en espera hasta que suceda cualquier otro problema con el principal ya sea por desastre o por fallas de funcionamiento.

## CONCLUSIONES

Este es nuestro capítulo final en el que vamos a exponer las conclusiones que consideramos más relevantes de nuestro trabajo de investigación.

- Determinamos la importancia de mantener la seguridad de la información en cada una de los escenarios al momento de experimentar situaciones críticas y/o fallas ya sean estas de origen humano, hardware y software; Aplicando la ISO 22301 y sus recomendaciones en el plan de continuidad de Negocio.
- Las funcionalidades de Veeam no se limitan a la replicación y respaldo de datos, su correcta configuración habilita la alta disponibilidad de las aplicaciones críticas de forma automática entre el centro de datos principal y el centro de datos alterno.
- De igual forma es necesario el licenciamiento de VMware para que Veeam pueda integrar a esa plataforma, ya que las funcionalidades básicas de Veeam Community no incluyen alta disponibilidad.
- También hemos determinado que el tiempo promedio de conmutación del centro de datos principal al centro de datos alterno usando un proveedor de fibra óptica es de cuatro minutos.
- En la actualidad la integración de VMware y Veeam permite la conexión a una nube híbrida por un la VCloud que es propietario de VMware y la nube pública de Azure.



## REFERENCIAS

- 22301, I. (28 de Diciembre de 2017). *SGSI*. Obtenido de Blog especializado en Sistemas de Gestión: <https://www.pmg-ssi.com/2017/12/iso-22301-continuidad-negocio/>
- Arbiol, J. (24 de Julio de 2019). *hiberus Tecnologia*. Obtenido de ¿Qué es Microsoft Azure y para qué sirve? Por qué elegir la plataforma cloud de Microsoft: <https://www.hiberus.com/crecemos-contigo/azure-la-plataforma-cloud-de-microsoft/>
- Carbonell, I. A., Enríquez, D. H., & Muro, I. Y. (2016). LA VIRTUALIZACION Y EL CENTRO DE DATOS COMO PUENTE PARA LA CONVERGENCIA EN OPERADORES DE TELECOMUNICACIONES. *Telem@tica*, 93-106.
- Casillas, M. (13 de Junio de 2018). *iNBest.solutions*. Obtenido de ¿Qué es un DRP?: <https://inbest.solutions/que-es-un-drp/>
- CASTILLO, G. G. (2017). *PLAN DE CONTINUIDAD DEL NEGOCIO BASADO EN SERVICIOS EN LA NUBE PARA EL ÁREA DE TECNOLOGÍA*. Guatemala: Galileo Universidad.
- Ekcit. (2016). *tic.PORTAL*. Obtenido de Microsoft Azure: <https://www.ticportal.es/temas/cloud-computing/microsoft-cloud/microsoft-azure>
- Hernández, J. (27 de Diciembre de 2012). *Blog Hostalia*. Obtenido de <https://blog.hostalia.com/hostalia/que-es-un-data-center-centro-de-datos/>
- Hernández, J. (27 de Diciembre de 2012). *Blog Hostalia*. Obtenido de ¿Qué es un Data Center (Centro de datos)?: <https://blog.hostalia.com/hostalia/que-es-un-data-center-centro-de-datos/>
- Josyula, V., Orr, M., & Center, G. P. (2012). *Cloud Computing: Automating the Virtualized*. USA: Cisco Press.
- Kyocera. (14 de Julio de 2017). *Kyocera Document Solutions*. Obtenido de 7 tipos de virtualización para cloud computing: <https://smarterworkspaces.kyocera.es/blog/7-tipos-virtualizacion-cloud-computing/>
- Lugo Cardozo, N. (2014). *TECNOLOGÍAS DE VIRTUALIZACIÓN EN LOS SISTEMAS INFORMÁTICOS DE LAS ORGANIZACIONES EMPRESARIALES DEL ESTADO ZULIA*. Zulia: Universidad Privada.
- Márquez, A. (2011). *Virtualización de servidores*. Barcelona: BarcelonaTech.
- Medina, A. L. (2010). *Análisis de la virtualización de sistemas operativos*. Barcelona.
- Ortiz, A. E. (31 de Julio de 2018). *Host dime*. Obtenido de Que es VMware: <https://blog.hostdime.com.co/que-es-vmware/>
- OSI, O. d. (2018). *PLAN DE CONTINUIDAD DEL NEGOCIO BCP*. Colombia: Escuela Superior de Administracion Publica.
- Pacheco, O., & D, L. (2009). *LA TECNOLOGÍA DE VIRTUALIZACIÓN EN LAS COMPUTADORAS*. Mexico: CienciaUAT.
- RAKOV, M. R. (2017). *VIRTUALIZACION DE SERVIDORES CON VMWARE*. VMWare.
- Software, V. (2016). Veeam Certified Engineer v9.5. En *Veeam Certified Engineer v9.5* (pág. 241). Veeam Software Inc.
- Soto, E. I. (2012). *Virtualización*. Murcia: Universidad de Murcia.

- Stackscale. (10 de Enero de 2019). *Stackscale*. Obtenido de ¿Qué es un centro de datos?: <https://www.stackscale.com/es/blog/que-es-un-centro-de-datos/>
- Tecon. (10 de Abril de 2017). *Soluciones Informaticas*. Obtenido de ¿Qué es Microsoft Azure? ¿Cómo funciona?: <https://www.tecon.es/que-es-microsoft-azure-como-funciona/>
- Villar, E., & Gómez, J. (s.f.). *VIRTUALIZACION DE SERVIDORES DE TELEFONIA IP EN GNU/LINUX*.