

Universidad Nacional de Ingeniería
Facultad de Ingeniería Eléctrica y Electrónica



TRABAJO DE SUFICIENCIA PROFESIONAL

**Dimensionamiento e implementación de un sistema de
almacenamiento de alta disponibilidad para la empresa
Agrícola Challapampa**

Para obtener el Título Profesional de Ingeniero Electrónico.

Elaborado por

Jhonny Anderson Malca Cruzado

 [0009-0007-0617-924X](https://orcid.org/0009-0007-0617-924X)

Asesor

MSc. Mauricio Pedro Galvez Legua

 [0000-0002-4845-4218](https://orcid.org/0000-0002-4845-4218)

LIMA – PERÚ

2024

Citar/How to cite	Malca Cruzado [1]
Referencia/Reference	[1] J. Malca Cruzado, “ <i>Dimensionamiento e implementación de un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa</i> ” [Trabajo de suficiencia profesional]. Lima (Perú): Universidad Nacional de Ingeniería, 2024.
Estilo/Style: IEEE (2020)	

Citar/How to cite	(Malca, 2024)
Referencia/Reference	Malca, J. (2024). <i>Dimensionamiento e implementación de un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa</i> . [Trabajo de suficiencia profesional, Universidad Nacional de Ingeniería]. Repositorio institucional Cybertesis UNI.
Estilo/Style: APA (7ma ed.)	

Dedicatoria

A Dios por darme la vida, a mis padres Edgar y Marleni por darme amor incondicional, a mi esposa Estefany Yovera por darme su apoyo para iniciar este proyecto, a mi hermana por darme los ánimos en ser cada día mejor y a las personas que Dios puso en mi camino; que me brindaron su ayuda de manera desinteresada. Gracias a todos ellos.

Resumen

Agrícola Challapampa S.A.C. es una empresa agroexportadora que se dedica al proceso de la producción, procesamiento y exportación de la uva. Actualmente, los servidores virtuales en donde están instalados los servicios críticos trabajan sobre un sistema de almacenamiento, que no cuenta con soporte local, tiempo de garantía de los equipos expirado, no tiene suficiente espacio de almacenamiento en disco duro y no cuenta con un sistema de alta disponibilidad, que permita soportar fallos en los componentes de hardware lo que genera tiempos de inactividad de los servicios. Por otro lado, los procesos de *backups* o respaldos de los servidores críticos son guardados en un sistema de almacenamiento, que tiene las mismas condiciones descritas anteriormente; eso quiere decir, que cualquier falla en el hardware generará pérdidas económicas para la empresa. Ante ello, se propone el dimensionamiento e implementación de una nueva arquitectura de almacenamiento basada en el empleo de un sistema de alta disponibilidad denominada SAN (*Storage Area Network*), la cual asegure la continuidad de los servicios, una disminución en los tiempos de proceso de *backup* y una mayor velocidad de comunicación en la red LAN (*Local Area Network*). Se concluye que una implementación de una red SAN con equipos redundantes en componentes de hardware permite incrementar la disponibilidad de servicios de cualquier empresa.

Palabras clave – High availability, redundancia, servidores, switch, máquinas virtuales, SAN, backups, iSCSI, HBA

Abstract

Agrícola Challapampa S.A.C. is an agro-export company that is dedicated to the production, processing and export of grapes. Currently, the virtual servers where the critical services are installed work on a storage system that does not have local support, the equipment's warranty period has expired, it does not have enough hard disk storage space and it does not have a backup system. High availability, which allows failures in hardware components to be supported, which generates downtime of services. On the other hand, the backup processes of critical servers are saved in a storage system, which has the same conditions described above; that means that any hardware failure will generate economic losses for the company. Given this, the sizing and implementation of a new storage architecture based on the use of a high availability system called SAN (Storage Area Network) is proposed, which ensures the continuity of services, a reduction in storage process times. Backup and higher communication speed on the LAN (Local Area Network). It is concluded that an implementation of a SAN network with redundant equipment in hardware components allows increasing the availability of services for any company.

Keywords — High availability, redundancy, servers, switch, virtual machines, SAN, backups, iSCSI, HBA

Tabla de Contenido

	Pág.
Resumen.....	iv
Abstract.....	v
Introducción.....	xiv
Capítulo I. Parte introductoria de trabajo	1
1.1. Generalidades.....	1
1.2. Descripción del problema de investigación	2
1.2.1. Situación problemática.....	2
1.2.2. Problema a resolver	2
1.3. Objetivos del estudio.....	2
1.3.1. Objetivo general.....	2
1.3.2. Objetivos específicos	2
1.3.3. Indicadores de logro de los objetivos	3
1.4. Antecedentes investigativos.....	3
Capitulo II. Marco teórico y conceptual	5
2.1. Marco teórico	5
2.1.1. Redes de comunicaciones de datos.....	5
2.1.2. Tipos de redes de datos.....	10
2.1.3. Topología de redes de datos.....	11
2.1.4. Medios de transmisión	14
2.1.5. Arquitectura de redes de datos	19
2.1.6. Protocolos de redes de datos.....	25
2.1.7. Protocolo de capa 3 del modelo OSI.....	28
2.1.8. Redes virtuales	35
2.1.9. Equipos de comunicación en redes de datos	36
2.1.10. Arquitectura de servidores	37
2.1.11. Alta disponibilidad	38

2.1.12. Sistemas de almacenamiento de datos.....	45
2.1.13. SAN	50
2.1.14. Protocolos de almacenamiento	56
2.1.15. Virtualización.....	63
2.1.16. Copia de seguridad	67
2.2. Marco conceptual.....	69
2.2.1. Software de virtualización VMware vSphere	69
2.2.2. ESXI y SAN ISCSI	73
2.2.3. Sistema de almacenamiento HPe StoreOnce	76
2.2.4. Sistema de almacenamiento HPe Nimble	77
2.2.5. VMware vSphere y sistema de almacenamiento HPe Nimble	78
2.2.6. Topologías soportadas del sistema de almacenamiento HPe Nimble	81
2.2.7. Software de respaldo Veeam Backup & Replication.....	84
Capítulo III. Desarrollo de trabajo de investigación	87
3.1. Descripción de la ubicación y características generales de la solución actual	87
3.1.1. Diagrama esquemático de la arquitectura IT actual.....	88
3.2. Dimensionamiento de la solución.....	89
3.2.1. Cálculo del espacio de almacenamiento requerido para la solución.....	91
3.2.2. Cálculo del consumo de IOPS de las máquinas virtuales.....	93
3.2.3. Validación de los equipos de comunicaciones existentes	95
3.2.4. Diseño de la arquitectura IT de la solución.....	97
3.2.5. Elaboración de especificaciones técnicas	98
3.3. Selección de la solución a implementar	102
3.4. Instalación, implementación, configuración y puesta a punto de la solución.....	107
3.4.1. Instalación física de los sistemas de almacenamiento	107
3.4.2. Cableado de red de los sistemas de almacenamiento	111

3.4.3. Configuración lógica de los puertos físicos de los switches HPe	112
3.4.4. Configuración lógica de los servidores ESXi.....	114
3.4.5. Implementación y configuración de los sistemas de almacenamiento ...	119
3.4.6. Migración de máquinas virtuales	123
3.4.7. Implementación y configuración de servidor de respaldo	125
3.5. Pruebas de testeo de la solución	133
3.5.1. Prueba de testeo de la alta disponibilidad de la LAN.....	133
3.5.2. Prueba de testeo de la alta disponibilidad de la SAN	135
3.6. Validación de la solución.....	138
3.6.1. Cálculo de los tiempos de parada de la solución.....	138
3.6.2. Cálculo de los tiempos de respaldo.....	139
Capítulo IV. Análisis y discusión de resultados.....	145
4.1. Cumplimiento del primer objetivo específico	145
4.2. Cumplimiento del segundo objetivo específico.....	145
4.3. Cumplimiento del tercer objetivo específico	146
Conclusiones.....	147
Recomendaciones.....	148
Referencias bibliográficas.....	149

Lista de Tablas

	Pág.
Tabla 1: Indicadores de logro de objetivos.....	3
Tabla 2: Métodos guiados más comunes.....	16
Tabla 3: Bandas de frecuencias en comunicaciones no guiadas.....	19
Tabla 4: Máscaras de subred por defecto.....	33
Tabla 5: Protocolos de almacenamiento basado en IP.....	57
Tabla 6: Listado de VLANs.....	89
Tabla 7: Listado de servidores virtuales.....	90
Tabla 8: Tamaño de backups.....	92
Tabla 9: Espacio de backups según periodo de retención.....	92
Tabla 10: Consumo pico de IOPS de las máquinas virtuales.....	94
Tabla 11: Especificaciones técnicas para el sistema de almacenamiento de alta disponibilidad.....	99
Tabla 12: Especificaciones técnicas para el sistema de almacenamiento de respaldo.....	101
Tabla 13: Comparación entre sistemas de almacenamiento principal HPe y DellEMC.....	103
Tabla 14: Comparativo entre sistemas de almacenamiento de respaldo HPe y DellEMC.....	105
Tabla 15: Configuración de puertos físicos en los switches HPe.....	114
Tabla 16: Configuración de puertos VMkernel de cada servidor ESXi.....	117
Tabla 17: iSCSI initiator de cada servidor ESXi.....	117
Tabla 18: Asignación de LUN a servidores físicos ESXi.....	121
Tabla 19: Asignación de LUN a servidor SVICVEEAMPXY.....	127
Tabla 20: Tareas de respaldo tipo diario.....	129
Tabla 21: Tareas de respaldo de tipo mensual.....	130
Tabla 22: Resumen de actividades de la puesta a punto de la solución.....	132
Tabla 23: Tiempos de parada de servicio año 2022.....	138
Tabla 24: Tiempos de parada de servicio año 2023.....	139
Tabla 25: Reporte de tarea de respaldo BK_Diario_VMs_Grupo2.....	140

Lista de Figuras

	Pág.
Figura 1: Cadena de comunicación.....	6
Figura 2: Redes de datos.....	7
Figura 3: Componentes de una arquitectura Cliente-Servidor.....	8
Figura 4: Diagrama de caso de uso para el sistema servidor.....	9
Figura 5: Diagrama de caso de usos para el sistema web browser.....	10
Figura 6: Tipos de redes según alcance	11
Figura 7: Topología en bus punto a punto.....	12
Figura 8: Topología estrella	12
Figura 9: Topología anillo	13
Figura 10: Topología malla	13
Figura 11: Topología árbol.....	14
Figura 12: Espectro electromagnético para las telecomunicaciones	15
Figura 13: UTP, FTP y STP	16
Figura 14: Cable coaxial	17
Figura 15: Modo de transmisión de datos en las fibras ópticas.....	17
Figura 16: Modelo de comunicación por capas.....	20
Figura 17: Modelo OSI.....	22
Figura 18: Comunicación vertical entre capas del modelo OSI	23
Figura 19: Modelo de arquitectura de protocolo.....	25
Figura 20: Paquete de datos.....	26
Figura 21: Cabecera IPv4	29
Figura 22: Interfaces y direcciones IP	31
Figura 23: Espacio total de clases de direcciones IP	32
Figura 24: Clases de Direcciones IP	32
Figura 25: Ejemplo de utilización de subredes.....	34
Figura 26: Ejemplo de configuración de VLAN.....	35

Figura 27: Switch HPe 5940 48 SFP+ 6QSFP	36
Figura 28: Router cisco 2901	37
Figura 29: Arquitectura de un servidor	38
Figura 30: Fuentes de poder redundantes de un servidor	40
Figura 31: RAID 0	42
Figura 32: RAID 1	42
Figura 33: RAID 5	43
Figura 34: RAID 6	43
Figura 35: RAID 0+1	44
Figura 36: RAID 1+0	44
Figura 37: RAID triple paridad.....	45
Figura 38: Almacenamiento de conexión directa DAS	47
Figura 39: Almacenamiento conectado en red NAS.....	48
Figura 40: Red de área de almacenamiento SAN	50
Figura 41: Componentes de una SAN	51
Figura 42: Sistema de almacenamiento activo/pasivo.....	55
Figura 43: LUN zoning and masking.....	56
Figura 44: Protocolo iSCSI, iFCP y FCIP	57
Figura 45: Ejemplo de cadena SCSI	58
Figura 46: Pila de protocolo iSCSI	59
Figura 47: Ejemplo de sesión iSCSI.....	59
Figura 48: Encapsulamiento de datos dentro de una trama iSCSI	60
Figura 49: Ejemplo de túnel FCIP entre dos redes SAN FC.....	60
Figura 50: Formato de mensaje FCIP	61
Figura 51: Pila de protocolo FCIP	62
Figura 52: Diagrama de funcionamiento del protocolo iFCP	62
Figura 53: Recursos físicos asignados a máquinas virtuales.	66
Figura 54: Hypervisor VMware ESXi.....	67

Figura 55: Tipos de copia de seguridad	68
Figura 56: Infraestructura de VMware vSphere.....	69
Figura 57: VMware vSphere HA	71
Figura 58: VMware virtual switch	72
Figura 59: Tipos de conexiones iSCSI	74
Figura 60: Conmutación por error de rutas de acceso en un host.....	75
Figura 61: Vista frontal HPe StoreOnce 3640	77
Figura 62: Vista frontal HPe Nimble HF20	78
Figura 63: Vista trasera HPe Nimble HF20	78
Figura 64: Arquitectura de conectividad iSCSI entre servidor y sistema de almacenamiento Nimble	79
Figura 65: Topología subred y switch único	82
Figura 66: Topología subred único y switch múltiple	82
Figura 67: Topología subred múltiple y switch único	83
Figura 68: Topología subred y switch múltiple	84
Figura 69: Arquitectura de software de respaldo Veeam Backup & Replication	86
Figura 70: Arquitectura IT antigua de Agrícola Challapampa S.A.C.....	88
Figura 71: Tráfico antiguo por canal de 10 Gbps	89
Figura 72: Consumo de IOPS de la empresa Agrícola Challapampa S.A.C.....	95
Figura 73: Switches HPe Flex Fabric 5940, vista frontal	96
Figura 74: Switches HPe Flex Fabric 5940, vista trasera	97
Figura 75: Arquitectura IT propuesta.....	97
Figura 76: Diseño de sistema de almacenamiento HPe Nimble HF20	104
Figura 77: Rendimiento teórico del sistema de almacenamiento principal	104
Figura 78: Diseño de sistema de almacenamiento de respaldo	107
Figura 79: Servidores HPe DL380 Gen 10, vista frontal.....	108
Figura 80: Servidores HPe DL380 Gen 10, vista trasera.....	108
Figura 81: Descripción de puertos de servidor SRVICESX13	109

Figura 82: Sistema de almacenamiento Nimble HF20, vista frontal sin tapa	109
Figura 83: Sistema de almacenamiento Nimble HF20, vista frontal con tapa.....	109
Figura 84: Descripción de puertos del sistema de almacenamiento Nimble.....	110
Figura 85: Sistemas de almacenamiento HPE y Wester Digital	110
Figura 86: Descripción de puertos HPe StoreOnce 3640.....	111
Figura 87: Cableado fiber channel 10GbE entre los equipos HPe.....	111
Figura 88: Tráfico LAN y SAN en el servidor HPe DL380 Gen10.....	112
Figura 89: Descripción de puertos Switch HPe 1	112
Figura 90: Descripción de puertos Switch HPe 2	113
Figura 91: Diagrama de configuración de los vSwitch en el host ESXi 2.....	115
Figura 92: VLAN que pasan por la troncal NIC4	115
Figura 93: VLAN que pasan por la troncal NIC5	115
Figura 94: Grupo de puertos en vSwitch1 en ESXi2	116
Figura 95: Grupo de puertos en vSwitch1 en ESXi2	116
Figura 96: Servidor SRVICESXI2.....	118
Figura 97: Servidor SRVICESXI3.....	118
Figura 98: Servidor SRVICESXI4.....	118
Figura 99: Configuración de tarjetas de red HPe Nimble HF20.....	120
Figura 100: Capacidad efectiva del sistema de almacenamiento Nimble HF20	120
Figura 101: Host SRVICESXI2.VANGUARDFRESH.PE	120
Figura 102: Host SRVICESXI3.VANGUARDFRESH.PE	121
Figura 103: Host SRVICESXI4.VANGUARDFRESH.PE	121
Figura 104 Listado de datastores.....	122
Figura 105: Espacio eficaz de HPe StoreOnce 3640	122
Figura 106: Almacenes de tipo Catalyst.....	123
Figura 107: Herramienta VMware Storage vMotion	123
Figura 108: Espacio en uso del sistema de almacenamiento Nimble.....	124
Figura 109: Arquitectura IT de sistema de respaldo.....	125

Figura 110: Configuración de servidor de respaldo.....	126
Figura 111: Servidor SRVICVEEAMPXY	126
Figura 112: Configuración SRVICVEEAMPXY.....	127
Figura 113: Configuración de servidor proxy Veeam.....	128
Figura 114: Repositorios de respaldo	128
Figura 115: Métricas de ahorro de espacio en disco	130
Figura 116: Tarea de respaldo BK_Diario_VMs_Grupo1	131
Figura 117: vSwitch1 del servidor SRVICESXI2	133
Figura 118: Ping hacia el servidor SRVICAPPS.....	134
Figura 119: Ping hacia el servidor SRVICAPPS con la tarjeta vmnic 5 desconectada	134
Figura 120: Ping hacia el servidor SRVICAPPS con la tarjeta vmnic 7 desconectada	135
Figura 121: Path activos del servidor SRVICESXI2	135
Figura 122: vSwitch0 con tarjeta vmnic4 desconectada.....	136
Figura 123: Path activos del servidor SRVICESXI2	136
Figura 124: vSwitch0 con tarjeta vmnic6 desconectada.....	137
Figura 125: Path activos del servidor SRVICESXI2	137
Figura 126: Datastores activos en el clúster de VMware.....	138
Figura 127: Duración de los tiempos de respaldos	141
Figura 128: Variación de velocidad de respaldo GB/Min.....	142
Figura 129: Reporte de respaldo, fecha 03.05.2023, tarea BK_Diario_VMs_Grupo2..	143
Figura 130: Reporte de respaldo, fecha 02.05.2023, tarea BK_Diario_VMs_Grupo2..	143
Figura 131 Reporte de respaldo, fecha 01.05.2023, tarea BK_Diario_VMs_Grupo2...	143
Figura 132 Reporte de respaldo, fecha 04.04.2023, tarea BK_Diario_VMs_Grupo2...	144
Figura 133: Reporte de respaldo, fecha 03.04.2023, tarea BK_Diario_VMs_Grupo2..	144
Figura 134: Reporte de respaldo, fecha 02.04.2023, tarea BK_Diario_VMs_Grupo2..	144

Introducción

El presente trabajo se desarrolló en base la experiencia obtenida laborando diez años en proyectos de nuevas implementaciones de equipos de infraestructura de *datacenter*, renovación tecnológica de infraestructura de IT, migración de sistemas o aplicaciones, redes informáticas empresariales, soluciones de alta disponibilidad, sistemas de respaldo y continuidad de negocio en distintas partes del Perú.

Dicha experiencia permitió conocer las buenas prácticas de instalación y configuración de sistemas de almacenamiento y servidores en alta disponibilidad, con base en los conceptos teóricos obtenidos en la universidad como la experiencia en campo, obteniendo un trabajo de alta calidad, eficiente y sostenible en el tiempo.

El desarrollo del trabajo se divide en 4 capítulos y son los siguientes:

El capítulo I, Parte introductoria del trabajo, se explican las generalidades del trabajo, la descripción del problema de investigación, el objetivo general, los objetivos específicos, indicadores de logro de los objetivos y los antecedentes investigativos.

El capítulo II, Marcos teórico y conceptual, se desarrolla una descripción las redes de comunicaciones de datos, tipos de redes de datos, topología de redes de datos, medios de transmisión, arquitectura de redes de datos, protocolos de redes de datos, protocolo de capa 3 del modelo OSI, redes virtuales, equipos de comunicación en redes de datos, arquitectura de servidores, alta disponibilidad, sistemas de almacenamiento de datos, SAN, protocolos de almacenamiento, virtualización y copia de seguridad. En el Marco Conceptual se desarrolla el software de virtualización *VMware vSphere*, *ESXi* y *SAN iSCSI*, sistema de almacenamiento *HPe StoreOnce*, sistema de almacenamiento *HPe Nimble*, *VMware vSphere* y sistema de almacenamiento *HPe Nimble*, topologías soportadas del sistema de almacenamiento *HPe Nimble* y software de respaldo *Veeam Backup*.

El capítulo III, Desarrollo del trabajo de investigación, se explica la descripción de la ubicación y características generales de la plataforma actual, dimensionamiento de la

solución, selección de la solución a implementar, implementación y puesto a punto de la solución, pruebas de testeo de la solución y finalmente validación de la solución.

El capítulo IV, Análisis y discusión de los resultados, se realiza un análisis cuantitativo de los resultados obtenidos en el dimensionamiento e implementación del sistema de almacenamiento de alta disponibilidad, así como el cumplimiento de cada uno de los objetivos específicos definidos.

Capítulo I. Parte introductoria de trabajo

En este capítulo se explican las generalidades del trabajo, la descripción del problema de investigación, el objetivo general, los objetivos específicos, indicadores de logro de los objetivos y los antecedentes investigativos.

1.1. Generalidades

A lo largo de los años, muchas empresas tienen implementados sus servicios en arquitecturas de IT (*Information Technology*) en entornos *on premise* o *cloud*. La elección del entorno depende mucho de las aplicaciones que se brindan y sus respectivos costos.

La mayoría de las empresas agroexportadoras trabajan en entorno *on premise*, esto es debido a la funcionalidad de sus aplicaciones, nivel de seguridad y accesibilidad de internet que se tiene en zonas fuera de Lima. Por ese motivo, el diseño de un *datacenter* y la selección de equipos como servidores, switches, firewall, sistemas de almacenamiento, etc., son pasos esenciales para garantizar la disponibilidad de los servicios. Una de las claves para brindar servicios ininterrumpidamente es tener separados los equipos de redes LAN y los equipos de almacenamiento, esto con el fin de que ambos tráficos no colisionen y generen latencias.

Actualmente, la empresa Agrícola Challapampa S.A.C. tiene su *datacenter on premise*, el cual consta de un clúster de virtualización con servidores físicos de la marca HP y un sistema de almacenamiento, que no tiene configurada la alta disponibilidad, de tal manera, que está expuesto a posible fallos o pérdidas de comunicación en la red. En resumen, el actual *datacenter* está obsoleto y requiere ser modernizado para asegurar la continuidad de los servicios.

En el presente trabajo se propone el dimensionamiento e implementación de un sistema de almacenamiento de alta disponibilidad denominada SAN, el cual asegure la continuidad de los servicios, una disminución en los tiempos de proceso de *backup* y una mayor velocidad de comunicación en la red LAN.

1.2. Descripción del problema de investigación

En esta sección se desarrollará la situación problemática que da origen al presente trabajo y el problema a resolver, que es la solución que se está proponiendo.

1.2.1. Situación problemática

La empresa Agrícola Challapampa S.A.C. no cuenta con un sistema de almacenamiento de alta disponibilidad que asegure la continuidad de servicios, una mayor velocidad de comunicación en los procesos de *backup* y en la comunicación de la red LAN.

1.2.2. Problema a resolver

La empresa Agrícola Challapampa S.A.C. tiene un *datacenter* con un sistema de almacenamiento obsoleto y que no posee la característica de alta disponibilidad.

1.3. Objetivos del estudio

En esta sección se redactan el objetivo general, los objetivos específicos y los indicadores de logro por cada uno de los objetivos específicos.

1.3.1. Objetivo general

Dimensionar e implementar un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa.

1.3.2. Objetivos específicos

Estos ayudarán a cumplir con el objetivo general y son los siguientes:

- Dimensionar un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa.
- Implementar un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa.
- Disminuir los tiempos de parada de los servicios y los tiempos de *backup*.

1.3.3. Indicadores de logro de los objetivos

Tabla 1

Indicadores de logro de objetivos

N°	Objetivo específico	Indicador de logro	Métrica
1	Dimensionar un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa.	Diagrama de diseño de la arquitectura del sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa.	Documento
2	Implementar un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa	Implementación del 100% del sistema de almacenamiento para la empresa Agrícola Challapampa.	Porcentaje
3	Disminuir los tiempos de parada de los servicios y los tiempos de respaldos.	Disminuir en 80% los tiempos de parada de los servicios. Disminuir los tiempos de respaldo en 20%.	Porcentaje

1.4. Antecedentes investigativos

La primera tesis, titulada “Diseño de redes de campus utilizando tecnología de virtualización” que fue elaborada por Manuel Víctor Tello Aragón, en el año 2018, en la Universidad Nacional de Ingeniería. El autor propone un diseño de mejora de las redes de todo el campus aplicando conceptos de virtualización, alta disponibilidad y tolerancia a fallos, lo cual permitió garantizar la continuidad de las comunicaciones en caso algún elemento o equipo de la red falle. En el presente trabajo se propone adicionar el dimensionamiento de un sistema de almacenamiento de alta disponibilidad basado en una red SAN aplicando conceptos de virtualización o segmentación de redes.

La segunda tesis, titulada “Implementación del sistema de recuperación ante desastres de la Infraestructura de un *Datacenter* hacia un centro de respaldo” que fue elaborada por Gerson Manuel Chumbimuni Segura en el año 2018, en la Universidad Nacional de Ingeniería. El autor propone implementar una arquitectura LAN y SAN para interconectar dos sedes separadas por una distancia de 10 Km a través de fibra oscura, con el fin de replicar volúmenes a nivel de los sistemas de almacenamiento e integrarlo con la solución de *vmware site recovery manager* para armar el plan de recuperación de

desastres de sus servidores virtuales en caso suceda alguna incidencia con el site principal. En el presente trabajo se propone un sistema de almacenamiento de alta disponibilidad e implementar un nueva arquitectura SAN que tenga la capacidad de integrarse con el software de respaldo y replicación *Veeam Backup*, que va a permitir tener una mayor velocidad en los procesos de respaldo y ahorro de espacio de almacenamiento debido a los mejores algoritmos de duplicación/compresión que dispone.

La tercera tesis, titulada “Diseño de un modelo de Virtualización para la implementación de un sistema de servidores en alta disponibilidad” que fue elaborada por Daniel Fabian Niño Vásquez en el año 2020, en la Universidad Cooperativa de Colombia. El autor propone armar un sistema de alta disponibilidad conectando los servidores físicos (*virtualizador Hyper-V*) de manera directa al sistema de almacenamiento, es decir, no hacen uso de *switch* para la interconexión, por motivo de disponibilidad de puertos de 10Gbps en los switch LAN *core*. En el presente trabajo se propone un sistema de almacenamiento de alta disponibilidad e implementar una nueva arquitectura SAN haciendo uso de dos switches LAN HPe Flexfabric 5940, haciendo uso del protocolo iSCSI, que nos va a brindar mayor velocidad y posibilidad de crecer a futuro. La alta disponibilidad de los servidores virtuales se dará con el virtualizador *VMware vSphere ESXi*.

Capítulo II. Marco teórico y conceptual

Este capítulo consta de dos partes: en el marco teórico se describen los conceptos referentes a las redes de comunicaciones de datos, tipos de redes de datos, topología de redes de datos, medios de transmisión, arquitectura de redes de datos, protocolos de redes de datos, redes virtuales, equipos de comunicaciones en redes de datos, arquitectura de servidores, alta disponibilidad, sistemas de almacenamiento de datos, SAN, protocolos de almacenamiento, virtualización y copia de seguridad. Los conceptos provienen de diversas fuentes de información académicas. En el marco conceptual se describe el *software* de virtualización *VMware vSphere ESXi*, *ESXi* y *SAN iSCSI*, sistema de almacenamiento *HPe StoreOnce*, sistema de almacenamiento *HPe Nimble*, *VMware vSphere* y sistema de almacenamiento *HPe Nimble*, topologías soportadas del sistema de almacenamiento *HPe Nimble* y *software* de respaldo *Veeam Backup & Replication*.

2.1. Marco teórico

Se detallarán los conceptos de las redes de comunicaciones, alta disponibilidad, almacenamiento de datos y virtualización, empleados en el desarrollo del trabajo, los cuales provienen de fuentes académicas.

2.1.1. *Redes de comunicaciones de datos*

Andréu (2011) menciona que las redes de comunicaciones son una serie de elementos interconectados que trabajan conjuntamente para que nos comuniquemos (p.8). En resumen, la red es el conjunto de elementos físicos y lógicos que hacen posible la comunicación de datos.

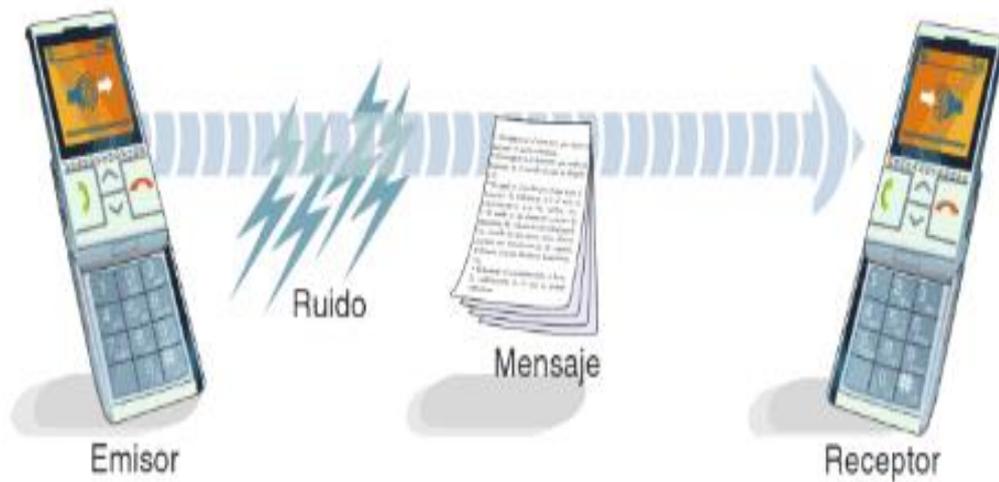
Los elementos de una red de datos son los siguientes:

- Emisor: es la persona o equipo que inicia la comunicación.
- Receptor: es la persona o equipo que recibe el mensaje
- Canal: es el medio de comunicaciones por donde se transmite el mensaje

- Ruido: es un elemento externo que se introduce en el canal.
- Mensaje: es la codificación que se desea transmitir.

Figura 1

Cadena de comunicación



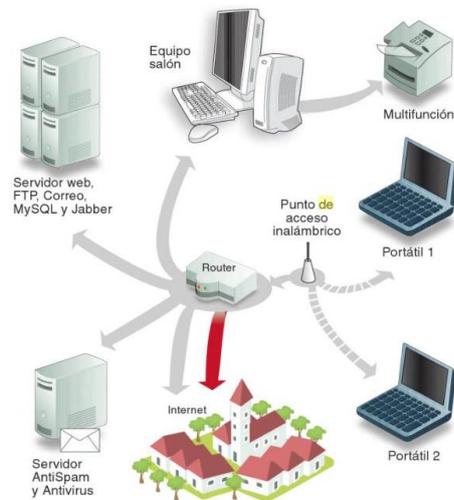
Nota: adaptado de *Redes locales* (p. 8), por J. Andreu, 2011, Editorial Editex.

Andréu (2011) explica que vivimos en una sociedad donde el proceso de envío de información es muy importante y donde cada vez crecen más necesidades de información (p.10).

Las redes de datos, comúnmente denominadas redes de ordenadores o redes informáticas son un conjunto de sistemas informáticos o interfaces interconectadas entre sí que comparten elementos con la finalidad de incrementar la eficiencia de los procesos. (Andréu, 2011, p.8). Los sistemas informáticos lo conforman componentes hardware (pantalla, teclado, *mouse*, etc.), interfaces de comunicación interna con los dispositivos e interfaces de comunicación hacia los usuarios externos.

Figura 2

Redes de datos



Nota: adaptado de *Redes locales* (p. 11), por Joaquín Andreu, 2011, Editorial Editex.

Los componentes de una red de datos pueden clasificarse en dos tipos.

- Equipos de acceso y comunicaciones dentro de una red. Tenemos los siguientes ejemplos: *router*, *módem*, *switch*, *access point*, etc.
- Los clientes que hacen uso de la red, por ejemplo: *ipad*, *tablet*, impresora, celular, televisor *Smart*, *desktop*, consola de juegos, dispositivos de control de acceso, cámaras, etc.

En cuanto a la arquitectura de red es el diseño eficiente de interconexión de una serie de elementos con el fin de establecer la comunicación. Este diseño involucra el uso de hardware, software y protocolos.

Las características más importantes de una arquitectura de red son las siguientes:

- La separación de funciones en una arquitectura de red nos va a permitir la segmentación de las redes e incrementar la seguridad de esta.
- La conectividad amplia permite tener una buena conexión entre gran cantidad de nodos.
- Recursos compartidos.

- La administración de la red es esencial para dar un buen servicio y mantener el mismo.
- Una arquitectura de red nos permite interconectar diversos equipos del tipo servidores, equipos NAS, sistemas de almacenamiento, etc.
- Una arquitectura de red nos va a permitir publicar aplicaciones comerciales de manera segura.

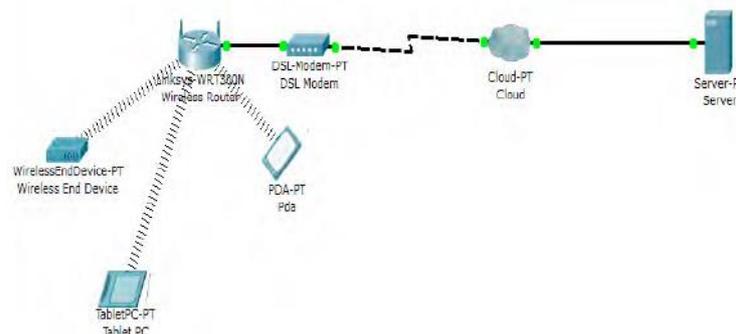
A. Arquitectura Cliente Servidor. Castillo (2019) define la arquitectura cliente servidor como un modelo en el que las transacciones o peticiones se dividen en procesos independientes con la finalidad de intercambiar información, servicios o recursos (p. 168). Este modelo nació en 1973 y fue desarrollado por Xerox-PARC.

Se tiene los siguientes conceptos:

- Cliente es el proceso que inicia la comunicación o solicitud de recursos.
- Servidor es el proceso que responde las solicitudes.

Figura 3

Componentes de una arquitectura Cliente-Servidor



Nota: adaptado de *Redes de datos* (p.168), por J. I. Castillo Velasquez, 2019, Editorial Samsara.

Las principales características de esta arquitectura son las siguientes:

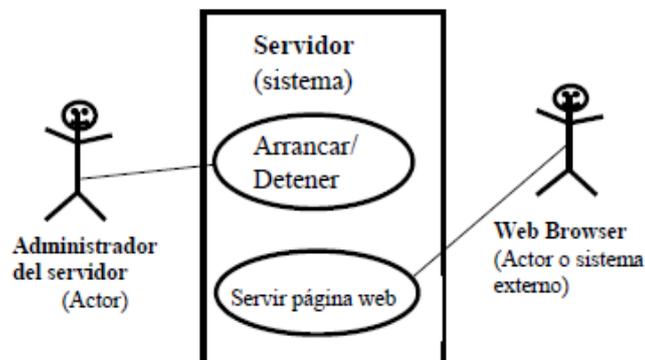
- El Servidor informático tiene una interfaz única y bien definida, que presenta a todos sus clientes.

- El cliente solo necesita conocer la interfaz externa del servidor, mas no la lógica interna.
- El cliente puede estar en todos lados y no depende de la ubicación física ni tipo de equipo.
- Cuando se genera algún cambio en el servidor, generalmente no implica cambios en los dispositivos finales.

La figura 4 es un ejemplo de modelo cliente-servidor mediante un diagrama de casos de uso en UML (*Unified Modeling Lenguaje*). En esta situación el sistema a analizar es un servidor y también se considera el web browser como sistema externo o actor que necesita información. Cabe indica que el termino servidor como sistema hace referencia al servidor de software.

Figura 4

Diagrama de caso de uso para el sistema servidor

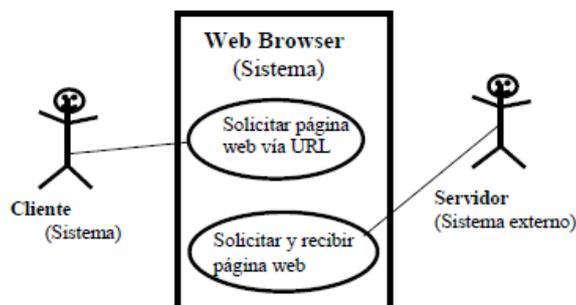


Nota: adaptado de *Redes de Datos* (p.169), por J. I. Castillo Velasquez, 2019, Editorial Samsara.

La figura 5 muestra un diagrama de caso de uso en el que un web browser o buscador es el sistema y el servidor es un actor o sistema externo. En este caso, el protocolo HTTP inicia una conversación o petición-respuesta para la comunicación entre un cliente y un servidor.

Figura 5

Diagrama de caso de usos para el sistema web browser



Nota: adaptado de *Redes de Datos* (p.169), por J. I. Castillo Velasquez, 2019, Editorial Samsara.

Un web browser o buscador es una aplicación de software que permite a un usuario visualizar e interactuar con el contenido de una página web. Los buscadores o web browser más populares son: Internet Explorer, Chrome, Firefox, Opera, etc.

2.1.2. Tipos de redes de datos

Según el alcance o extensión, Andréu (2011) clasifica las redes de datos (p.23) de la siguiente manera:

A. Redes PAN (*Personal Área Network*). Redes inalámbricas de corta distancia para conectar dispositivos o periféricos. La velocidad de transmisión es menor al megabit por segundo. Entre los estándares más reconocidos tenemos los siguientes: bluetooth, infrarrojo, RFID, TAG, UWB, ZigBee, etc.

B. Redes LAN (*Local Área Network*). Aquellas redes que tienen un alcance limitado o área bien definida pequeña, como puede ser los siguientes: un edificio, una casa, un departamento, etc.

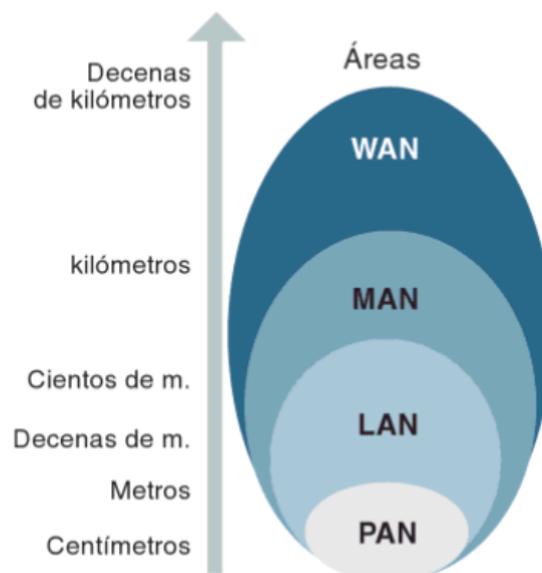
C. Redes CAN (*Campus Área Network*). Aquellas redes cuya extensión es la de un campus universitario, un grupo grande de edificios y una pequeña área geográfica.

D. Redes MAN (*Metropolitan Area Network*). Aquellas redes que se sitúan en una urbanización, ciudad o municipio pequeño (en un radio aprox. de 1-7 Km) y podría alcanzar mayores distancias usando repetidores. Generalmente estas redes trabajan con altas velocidades.

E. Redes WAN (*Wide Area Network*). Red global (conecta varios países o continentes), es decir, es una red de amplio alcance que trabaja con una alta velocidad. Esta red se ve reflejada en los satélites, redes microondas, telefonía móvil, etc. La figura 6 muestra un resumen de los tipos de redes según el nivel de alcance.

Figura 6

Tipos de redes según alcance



Nota: adaptado de *Redes Locales* (p.25), por Joaquín Andreu, 2011, Editorial Editex.

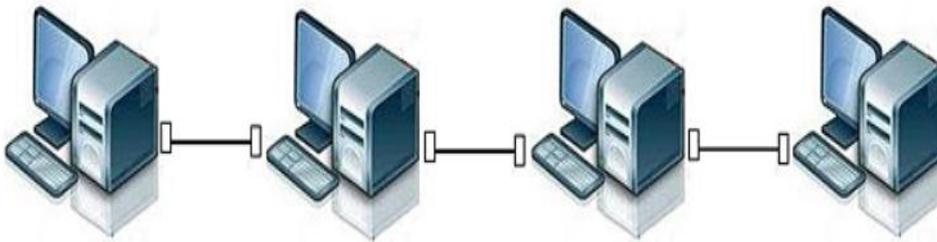
2.1.3. Topología de redes de datos

La topología de red define la estructura física, es decir, la manera en que disponen los cables o enlaces que interconectan los diversos elementos (Liberatori, 2018, p.33).

A. Topología bus. Dordoigne (2020) explica que este tipo (soporte lineal) se basa en un cableado en el que se conectan nodos (puestos de trabajo, equipos de interconexión, periféricos) y hacen uso de un elemento físico denominado el cable (p.213). Si un cable de red se corta, se pierde la comunicación entre los equipos.

Figura 7

Topología en bus punto a punto



Nota: adaptado de *Redes Informáticas* (p.214), por J. Dordoigne, 2015, Ediciones ENI.

B. Topología estrella. Liberatori (2018) explica que en este tipo de topología todas las conexiones se centralizan en un único punto central, por el que pasan todas las comunicaciones (p.33). En caso algún componente de la red inferior al punto central se desconecta o se rompe, solo ese equipo se quedará fuera de la red, y si el nodo central falla, la conectividad se cae de manera completa.

Figura 8

Topología estrella

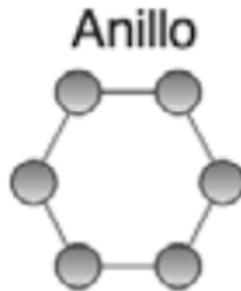


Nota: adaptado de *Redes de Datos y sus Protocolos* (p.34), por M. C. Liberatori, 2018, Editorial Eudem.

C. Topología en anillo o red circular. Liberatori (2018) explica que las conexiones de cada elemento o nodo se dan uno a uno y el ultimo se termina conectando con el primero, de tal manera que se cierra el lazo o anillo. En topología de red la comunicación depende existe un paquete testigo o *token*, que se utiliza para balancear la carga en un sistema de comunicación. Si algún elemento de la red queda fuera de servicio, la conectividad interna del anillo se pierde (p.33).

Figura 9

Topología anillo

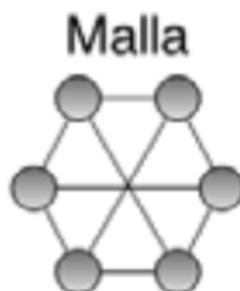


Nota: adaptado de *Redes de Datos y sus Protocolos* (p.34), por M. C. Liberatori, 2018, Editorial Eudem.

D. Topología malla. En este tipo cada nodo se conecta con todos los nodos de la red, de tal manera que tenga la posibilidad de llevar los mensajes por distintos caminos. Al tener todos los nodos interconectados, se convierte en una red muy confiable si se llega a dar alguna interrupción en las comunicaciones (Liberatori, 2018, p.33).

Figura 10

Topología malla

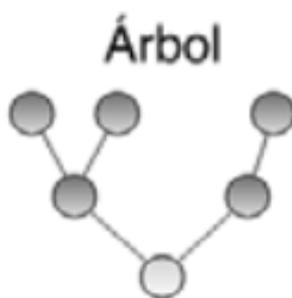


Nota: adaptado de *Redes de Datos y sus Protocolos* (p.34), por M. C. Liberatori, 2018, Editorial Eudem.

E. Topología árbol. Se define como una topología centralizada, donde hay un nodo raíz y a partir de él se despliega ramas, reflejados en componentes. Esta topología es de tipo jerárquica, en donde existe un elemento raíz y los demás tienen una relación tipo padre-hijo. Si falla un elemento de la red, se puede quedar aislada una cierta cantidad de elementos y si falla el elemento principal, todos los componentes hijos quedarán incomunicados (Liberatori, 2018, p.34).

Figura 11

Topología árbol



Nota: adaptado de *Redes de Datos y sus Protocolos* (p.34), por M. C. Liberatori, 2018, Editorial Eudem.

2.1.4. Medios de transmisión

En los sistemas de comunicación, el medio es el camino físico a través del cual el emisor envía mensajes hacia un receptor.

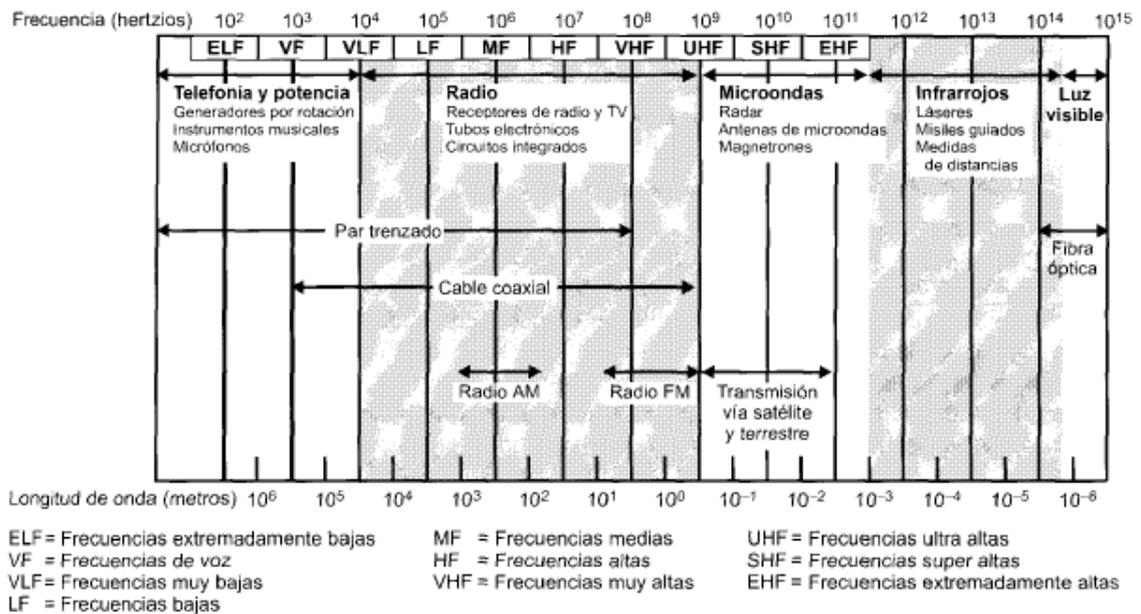
Stallings (2000) explica que la transmisión de datos se realiza a través de ondas electromagnéticas que pueden viajar de manera guiada o no. Un medio de transmisión guiado es cuando las OEM (Onda electromagnética) viajan a través de un cable o medio sólido, y un medio de transmisión no guiados se realiza de manera inalámbrica, es decir, se usan antenas. En ambos casos, las comunicaciones buscan alcanzar grandes distancias y una alta velocidad de transmisión, por ese motivo, se definen los siguientes factores (p.102) que determinan las capacidades máximas.

- El ancho de banda es el intervalo de frecuencia dentro del espectro y está relacionado con la capacidad máxima que tiene un medio para transmitir un mensaje.

- Las dificultades en la transmisión son las pérdidas de energía de la señal cuando llegue al destino. En medios guiados podría ser debido al medio físicos y en medios no guiados, podría ser debido al entorno por donde se propaga la señal.
- Las interferencias son señales cercanas a la frecuencia de comunicación que generan distorsión del mensaje o comunicación. Como ejemplo podemos tener el ruido de los motores o maquinas industriales, inducción de cables de alta tensión, etc.

Figura 12

Espectro electromagnético para las telecomunicaciones



Nota: adaptado de *Comunicaciones y Redes de Computadoras* (p.103), por W. Stallings, 2004, Pearson Educación S.A.

A. Medios de transmisión guiados. Stallings (2000) menciona que la máxima velocidad que pueda alcanzar un medio va a depender de la distancia y de la cantidad de receptores (p.103). En la tabla 2 se muestra las características de los cables más usados para establecer una comunicación.

Tabla 2

Métodos guiados más comunes

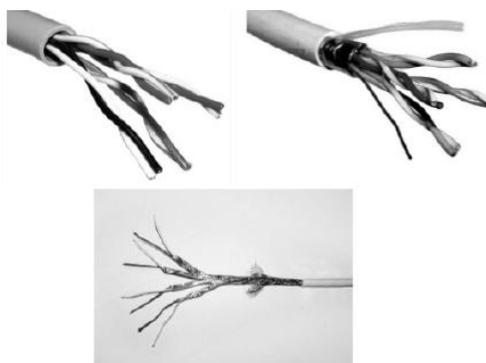
	Rango de frecuencias	Atenuación típica	Retardo típico	Separación entre repetidores
Par trenzado (con carga)	0 para 3.5 KHz	0.2 dB/km @ 1KHz	50 μ s/Km	2 Km
Pares trenzados (múltiples cables)	0 para 1 MHz	3 dB/km @ 1KHz	5 μ s/Km	2 Km
Cable coaxial	0 para 500 MHz	7 dB/km @ 10 MHz	4 μ s/Km	1 para 9 Km
Fibra óptica	180 para 130 THz	0.2 para 0.5 dB/km	5 μ s/Km	40 Km

Nota: adaptado de *Comunicaciones y Redes de Computadoras* (p.103), por W. Stallings, 2004, Pearson Educación S.A.

- Par trenzado: es el medio de transmisión más común en el mercado que consiste en tener dos conductores eléctricos aislados y trenzados para evitar todo tipo de interferencias. Entre los tipos de cables tenemos los siguientes: UTP (*Unshielded Twisted Pair*) o par trenzado no apantallado, FTP (*Foiled Twisted Pair*) o par trenzado blindado mediante una hoja de aluminio y par trenzado blindado donde cada par de cables es blindado de manera independiente STP (*Shielded Twisted Pair*). Este cable tiene mayor uso en redes cableadas tipo LAN y telefonía.

Figura 13

UTP, FTP y STP



Nota: adaptado de *Redes de Datos y sus Protocolos* (p.107), por M. C. Liberatori, 2018, Editorial Eudem.

- Cable coaxial: Stallings (2000) explica que este es un medio que tiene dos conductores contruidos de tal manera que le permita operar sobre un rango mayor

de frecuencia, es decir, permite trabajar con un mayor ancho de banda a comparación del par trenzado. A este tipo de cable le afecta menos las interferencias y diafonías a comparación del par trenzado (p.108).

Figura 14

Cable coaxial



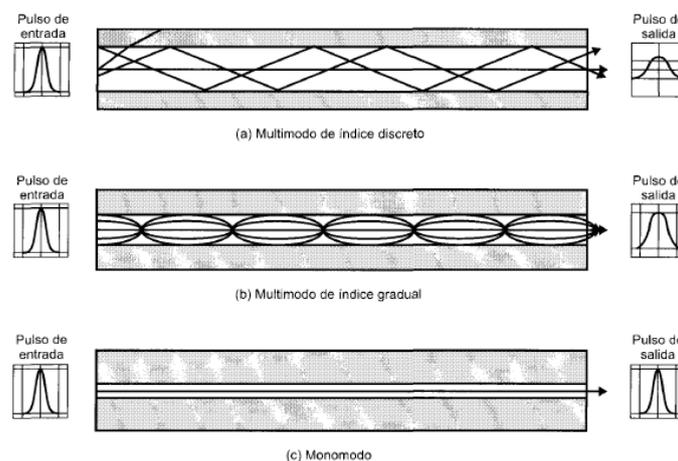
Nota: adaptado de *Redes de Datos y sus Protocolos* (p.108), por M. C. Liberatori, 2018, Editorial Eudem.

- Fibra óptica: se define como un medio flexible que permite confinar un haz de naturaleza óptica. Tiene como principal venta que dispone de gran ancho de banda no le afecta las interferencias electromagnéticas, por ende, son importantes para trabajar con transmisiones de largas distancias. La fibra óptica propaga el haz de luz internamente de acuerdo con el principio de reflexión actual (Stalling, 2000, p.109).

En la figura 15 se muestra los tipos de propagación del haz de luz.

Figura 15

Modo de transmisión de datos en las fibras ópticas



Nota: adaptado de *Comunicaciones y Redes de Computadores* (p.111), por W. Stallings, 2000, Prentice Hall.

La diferencia principal es el alcance, es decir, la fibra monomodo nos permite trabajar con distancias largas y el multimodo, con distancias cortas. Esto es debido al tamaño del núcleo y cantidad de modos o caminos que se reflejan dentro del núcleo.

B. Medios de transmisión no guiados. Estos tipos de medios de transmisión inalámbrica hacen uso de antenas. Estas antenas tienen la capacidad de radiar y capturar energía electromagnética con la finalidad de establecer la comunicación, existiendo dos tipos de transmisión: omnidireccional y direccional.

Stalling (2000), explica que en el estudio de las comunicaciones inalámbricas se consideran tres rangos de frecuencias (p.112) y son las siguientes:

- El primer intervalo se llama frecuencia de microondas que abarca desde los 2 GHz (Gigahertzios = 10^9 Hertzios) hasta los 40 GHz. Estas frecuencias son ideales para enlaces punto a punto debido a la potencia de la señal.
- El segundo intervalo se llama intervalo de ondas de radio que abarca desde los 30MHz hasta 1GHz. Este intervalo de frecuencias es ideal para aplicaciones omnidireccionales.
- El tercer intervalo es para uso de dispositivos que se encuentra a corta distancia y hacen uso del espectro infrarrojo, y se encuentra en el rango de 3×10^{11} Hz hasta los 2×10^{14} Hz.

Tabla 3*Bandas de frecuencias en comunicaciones no guiadas*

Banda de frecuencia	Nombre	Datos analógicos		Datos digitales	
		Modulación	Ancho de banda	Modulación	Velocidad de transmisión
30-300 KHz	LF (frecuencia baja)		Normalmente no se usa	ASK, FSK, MSK	01 para 100 bps
300-3000 KHz	MF (frecuencia media)	AM	Para 4 KHz	ASK, FSK, MSK	10 para 1000 bps
3-30 MHz	HP (frecuencia alta)	AM, SSB	Para 4 KHz	ASK, FSK, MSK	10 para 3000 bps
30-300 MHz	VHF (frecuencia muy alta)	AM, SSB, FM	5 KHz para 5 MHz	FSK, PSK	Para 100 kbps
300-3000 MHz	UFF (frecuencia ultra alta)	FM, SSB	Para 20 MHz	PSK	Para 10Mbps
3-30 GHz	SHF (frecuencia super alta)	FM	Para 500 MHz	PSK	Para 100 Mbps
30-300 GHz	EHF (frecuencia extremadamente alta)	FM	Para 1 GHz	PSK	Para 750 Mbps

Nota: adaptado de *Comunicaciones y Redes de Computadores* (p.113), por W. Stallings, 2000, Prentice Hall.

2.1.5. Arquitectura de redes de datos

Liberatori (2018) explica que, en todo tipo de comunicación en red los sistemas usan un conjunto de protocolos que actúan de manera cooperativa, debiendo ser capaces de comunicarse entre sí (p.45).

Uno de los objetivos de todo diseño de arquitectura de red es crear entornos pequeños o módulos simples, que permitan tener gran escalabilidad y capacidad de integración.

Implementar un diseño óptimo de arquitectura de red de datos en módulos simples nos ayuda a tener las siguientes ventajas (Liberatori, 2018, p.46):

- Documentación más sencilla de entender, es decir, un buen diseño de arquitectura de red nos facilitará la administración de esta y solución de incidencias.
- La especialización de trabajar con módulos simples nos permite tener otra visión de la arquitectura y brindar propuestas de mejora.

- La facilidad de modificación de un diseño óptimo facilita tareas de mantenimiento y cambios en la topología.

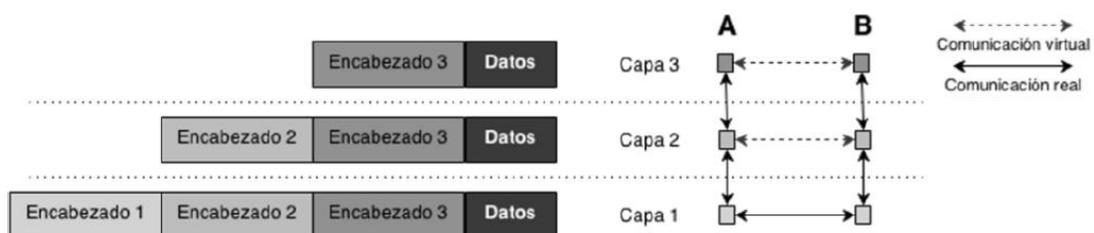
Cada módulo o bloque de la red tiene sus propias funciones y poseen sus componentes de hardware y software, y son capaces de comunicarse con otros módulos entre si o otros tipos de dispositivos.

En todo diseño se tiene la casuística de decidir cuántos niveles de capas o módulos se deben implementar y las funciones que tendrían. A partir de ello y con el pasar de los tiempos se diseñó la comunicación TCP/IP, que consiste en una pila de protocolos conformado por capas.

Por ejemplo, se tiene dos sistemas A y B (mismo conjunto de capas) localizados en distintos de tramos de una red LAN que desean entablar una comunicación. Para el ejemplo se propone un modelo de comunicación de 3 capas y estas están separadas entre sí de acuerdo con la figura 16. En cada capa se implementa un conjunto de protocolos y existe un flujo comunicación de tipo vertical entre capas adyacentes, y de tipo horizontal entre niveles de misma jerarquía.

Figura 16

Modelo de comunicación por capas



Nota: adaptado de *Redes de Datos y sus Protocolos* (p.46), por M. C. Liberatori, 2018, Editorial Eudem.

La comunicación entre sistemas funciona de manera correcta utilizando la técnica de encapsulado. Esta técnica implica agregar un encabezado a cierto mensaje que permite

tener un control de la información. Esta regla de encapsulado implica que cada sistema encapsule sus protocolos cuando pase a nivel de capas.

En el ejemplo, todo mensaje (Datos) generado en el sistema A, llegará al final inferior del nivel de capas encapsulando el mensaje de la siguiente manera: Encabezado1/Encabezado2/ Encabezado3/Datos. Una vez enviado sobre el medio llegará al sistema B, y desde la capa inferior empezará el proceso de des encapsulado, donde cada capa revisará la información relevante a su mismo nivel hasta llegar al nivel de superior del sistema B y se culminará con la entrega del mensaje.

Con este ejemplo se ha explicado la comunicación de dos sistemas a través de tres niveles de capas. En resumen, el detalle de cada capa sería el siguiente:

- La capa más baja hace referencia a los detalles de transmisión física de los datos.
- El nivel superior es el que interactúa con el usuario porque se da la entrega del mensaje. Por ejemplo, podría ser las aplicaciones de software.
- La capa media hace referencia a los posibles medios de comunicación.

En resumen, en una comunicación real los flujos pueden ser los siguientes: flujo vertical de comunicación de mensajes a nivel de cada sistema y una comunicación virtual, que vendría a ser la interacción de capas al mismo nivel entre 2 sistemas, representada por líneas punteadas según figura 16 (comunicación entre protocolos pares).

A. Modelo OSI. Liberatori (2018) explica que la iniciativa de desarrollar una arquitectura para modelar la comunicación entre sistemas dentro de una red se da en el año 1977, cuando se forma un subcomité de la ISO. El modelo desarrollado por el comité se denominó Modelo de interconexión de Sistemas Abiertos (OSI, *Open System Interconnection*) (p.47).

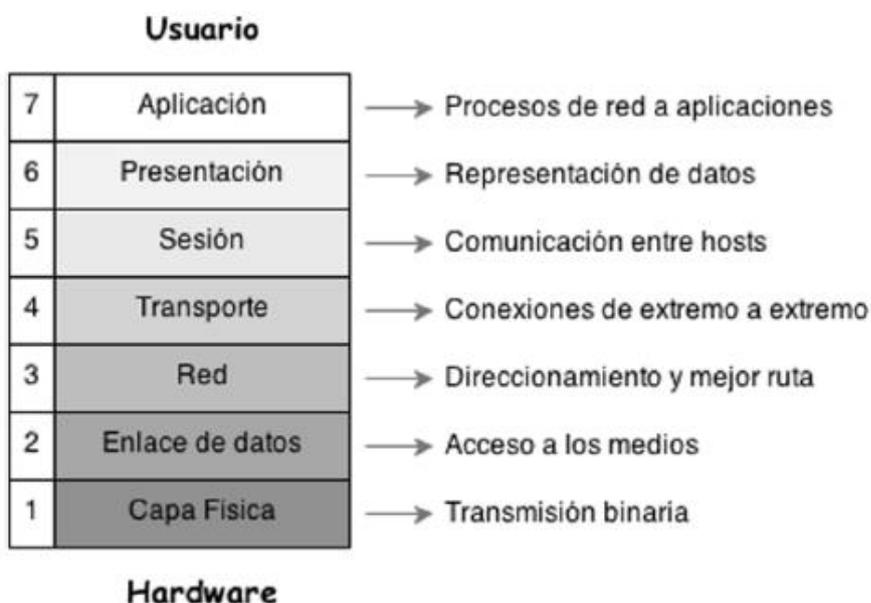
El modelo OSI plantea un conjunto jerárquico de capas para la división de funciones necesarias para establecer la comunicación entre sistemas, en el cual cada capa debe

apoyar su funcionalidad en la capa inferior y ocultar sus detalles técnicos de implementación.

El comité de la ISO (Organización Internacional de Normalización) desarrolló el modelo OSI sobre un conjunto de siete capas. El nivel inferior (1 y 2) se acerca a la capa de *hardware* y *software* para establecer una comunicación y la capa superior (7) es la capa más cercana al usuario, es decir las aplicaciones, ver figura 17.

Figura 17

Modelo OSI



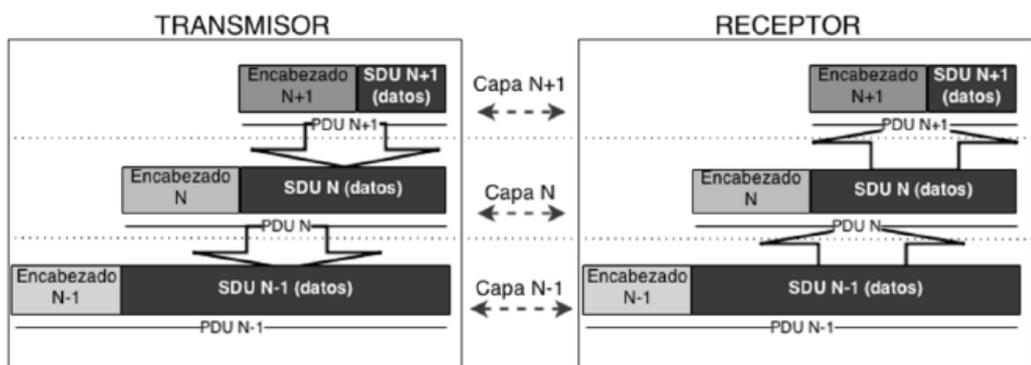
Nota: Adaptado de Redes de Datos y sus Protocolos (p.49), por M. C. Liberatori, 2018, Editorial Eudem.

En el modelo OSI, se tiene una Capa genérica N, capa inferior (N-1) y capa superior (N+1). Según el nivel de capas, la capa inferior ofrece sus servicios a la capa superior, es decir, la capa N-1 a la capa N y la capa N, a la N+1.

En este modelo, el concepto interfaz se refiere al mecanismo de comunicación entre capas adyacentes y no tiene relación al concepto que se maneja hoy en día, puesto que se refiere a la forma de comunicación a nivel de capas. En la actualidad el concepto interfaz está relacionado con la conexión física de un dispositivo.

Figura 18

Comunicación vertical entre capas del modelo OSI



Nota: adaptado de Redes de Datos y sus Protocolos (p.49), por M. C. Liberatori, 2018, Editorial Eudem.

El proceso de transmisión de un mensaje inicia desde la capa superior del dispositivo transmisor hasta su capa inferior y desde el dispositivo receptor de manera inversa. Esta comunicación vertical es una comunicación real entre capas adyacentes (Liberatori, 2018, p.50-54).

- La capa física es el medio que se utiliza para establecer la comunicación. Por ejemplo, tenemos los siguientes medios: cable coaxial, fibra óptica, medio inalámbrico, etc.
- La capa de enlace de datos tiene como función presentar a capa de Red un enlace físico seguro. En el modelo OSI la capa de enlace está dividida en dos subcapas, subcapa de control de acceso al medio (MAC, *Medium Access Control*) y subcapa de control lógico de enlace (LLC, *Logical Link Control*).
- La capa de red define la posibilidad de conectar distintas redes entre sí con la finalidad de establecer la comunicación entre dispositivos. La funcionalidad principal de esta capa es el enrutamiento, que consiste en la posibilidad de manejar paquetes desde un punto a otro en la red.

En el modelo OSI existen dispositivos que cumplen la función de enrutamiento y se conocen como *routers*. Estos se encargan de la interconexión de distintas redes y

hacer uso de protocolos de enrutamiento con la finalidad de determinar la mejor ruta para establecer una comunicación eficiente.

- La capa de transporte es el encargado de mantener una comunicación transparente y seguro a través del control de flujo de datos entre dos sistemas de comunicación. Esta capa contiene mecanismos de optimización de recursos con la finalidad de asegurar una buena calidad de conexión.
- La capa de sesión ofrece a los usuarios el acceso a la red, previa codificación de datos que realiza el nivel superior, permitiendo el establecimiento y desconexión de una sesión. La capa de sesión tiene como función relacionar, organizar, sincronizar y administrar el intercambio de información entre entidades del nivel superior. Es función de esta capa la administración de testigos o tokens para controlar el orden del diálogo.
- La capa de presentación se encarga de definir y traducir los distintos tipos de formatos de datos que se van a intercambiar entre el emisor y receptor, es decir, en esta capa se analiza las representaciones de los datos de los ordenadores o dispositivos en ambos extremos de la comunicación con la finalidad de que la comunicación sea asertiva.
- La capa de aplicación realiza el procesamiento final de la información a intercambiar, es decir, esta capa es la más cercana al entorno usuario que permite la interacción y la capacidad de proporcionar los servicios de red necesarios para que pueda ejecutarse la aplicación.

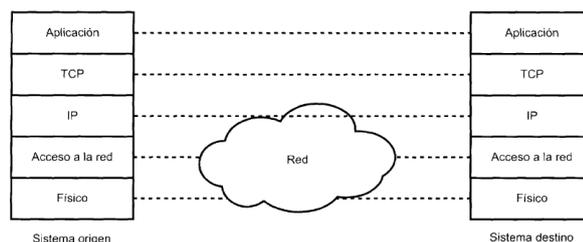
B. Modelo TCP/IP. Stallings (2000) cita que el protocolo TCP/IP es resultado de la investigación y desarrollo llevados a cabo en la red experimental de conmutación de paquetes *Arpanet*, financiada por la *Darpa (Defense Advanced Research Projects Agency)*, y se denomina la familia de protocolos TCP/IP (p.17).

No obstante, basándose en protocolos estándar que se han desarrollado para establecer una comunicación, se puede organizar en cinco capas relativamente independientes y son las siguientes (Stalling, 2000, p.17-18):

- La capa física es la encargada de gestionar la infraestructura física en un sistema de comunicación.
- La capa de acceso a la red es el encargado del intercambio de datos entre dos sistemas y está relacionado con el enrutamiento de los datos en una red.
- La capa de internet o protocolo de internet IP es aquel que permite enrutar los datos a través de dos o más redes diferentes. El elemento que permite realizar dicho enrutamiento se denomina *router*.
- La capa TCP (*Transmission Control Protocol*) es aquella capa que resume los procedimientos que aseguren la entrega de los datos o información al destino.
- La capa de aplicación es aquel nivel donde la comunicación se da entre aplicaciones que manejan información de los usuarios en una red. En esta capa se tiene todos los protocolos que se usan para ofrecer servicios a los usuarios, que por ejemplo tenemos los siguientes: Telnet, FTP, SMTP, DNS, HTTP, etc.

Figura 19

Modelo de arquitectura de protocolo



Nota: adaptado de *Comunicaciones y Redes de Computadores* (p.18), por W. Stallings, 2000, Prentice Hall.

2.1.6. Protocolos de redes de datos

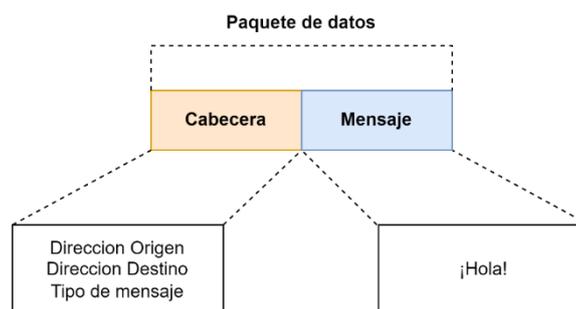
Los protocolos de redes son aquellos que permiten definir un formato común y reglas para poder establecer la comunicación entre dos dispositivos o sistemas. Cada protocolo tiene sus propias reglas y formatos para establecer la comunicación.

A. Características de protocolos. A continuación, se describe las principales características que tiene todo protocolo de comunicación de datos.

- Encapsulamiento: es el proceso por el cual se agrega un cabecera o paquete de control de datos a cierto mensaje para poder llegar al destino o receptor. Durante este proceso de encapsulado también se empaquetan los protocolos de redes.

Figura 20

Paquete de datos



- El direccionamiento es una identificación única para poder distinguir al emisor y receptor en un proceso de comunicación. Existen dos tipos:
 - Físico: número MAC (48 bits), esta numeración está grabada en la memoria ROM de la NIC.
 - Lógico: se puede modificar fácilmente: Direccionamiento IP host y subred. Pueden ser de dos tipos: IPv4 (32 bits) y IPv6 (128 bits).
- El enrutamiento es seleccionar la ruta más corta para llegar a un destino. En entornos grandes es necesario encontrar mecanismos que permitan seleccionar la ruta más eficiente para llegar a un destino.
- El secuenciamiento está basado en la conmutación de paquetes (*packet switching*), y se refiere a la capacidad de transmisión de un mensaje con opciones de distintas rutas hacia un destino. Una vez que los PDU llegan a su destino, los PDU deben ser reensamblados en su orden inicial. Para poder realizar esta acción, los PDU son numerados (número de secuencia), lo que permite su posterior reordenamiento.

- El control de flujo es una técnica para sincronizar los PDU entre dos nodos o elementos de red que están por procesar información a distintas velocidades (depende la velocidad de procesamiento de cada nodo).
- El *handshaking* es una técnica que permite que toda comunicación se realice de manera exitosa y sin errores. Para lograr ello se debe acordar los siguientes parámetros de comunicación: velocidad de transmisión de datos o velocidad de cada NIC, cantidad de información soportada (cuantos PDU se van a enviar antes de llenar la RAM de NIC destino) y solución de problemas por bloqueo de alguna de las partes.
- La gestión de errores permite corregir los errores en la transmisión de información debido a problemas causados por los medios de comunicación y/o dispositivos. Esta gestión involucra detección de errores, que por ejemplo puede ser los siguientes: bit de paridad, checksum, CRC (*Cyclic Redundancy Check*), etc. y corregir el error, haciendo una solicitud de reenvío de información y empleando un método de corrección de errores.

B. Métodos de transmisión en redes LAN. Se tienen los siguientes medios de transmisión:

- *Unicast*: es cuando él envió de un mensaje se realiza desde un único emisor host hacia un receptor. El paquete IP contiene direcciones IP tanto del origen como del destino.
- El *broadcast* tiene como dirección "1" o "255.255.255.255". Liberatori (2018) lo define como dirección especial que tiene significado todos, es decir, se envía un mensaje a todos los dispositivos de una red LAN (p.37).
- El *Multicast*: Liberatori (2018) lo denomina al tipo de comunicación en grupo, es decir, cierto dispositivo envía un mensaje a un conjunto de receptores. Para poder realizar este tipo de comunicación, se elige un grupo de direccionamiento IP destino dentro de una red local y serán los receptores del mensaje enviado. El

direccionamiento IPv4 de clase D tiene como fin este propósito de método de transmisión de datos.

- *Anycast*: en este tipo de direccionamiento múltiples host o dispositivos son agrupados en una dirección IP anycast con el fin de aplicar una regla de distribución de carga.

2.1.7. Protocolo de capa 3 del modelo OSI

Stallings (2000) define el protocolo de internet como una parte del protocolo TCP/IP, y es el protocolo más utilizado en estos años (p.501).

Este protocolo estándar se divide en dos partes y son las siguientes:

- Interfaz de capa superior, que está relacionado con los servicios.
- El formato del protocolo.

El protocolo IP tiene como función principal el enrutamiento de paquetes. Por tanto, para poder ofrecer esta característica propia, se consideró la necesidad de armar un esquema de direccionamiento IP global para identificar todos los elementos que participan en una comunicación. En un inicio este direccionamiento era de manera manual, pero con el incremento de los dispositivos, se impuso la configuración de manera automática.

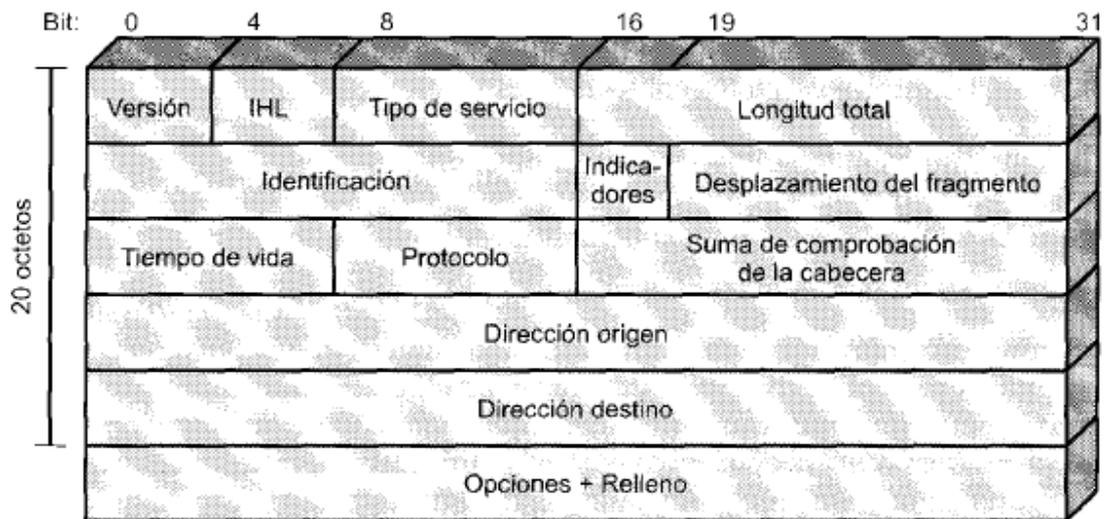
Esta forma de trabajo de enrutamiento puede conllevar a tener ciertos problemas en la transmisión de paquetes debido a la presencia de errores en las tablas. La posibilidad de la existencia de estos tipos de situaciones dio lugar a agregar un campo de información de Tiempo de Vida (TTL, *Time to Live*) de paquete, que es útil para hacer descartes de conectividad y latencia en una red.

Esta necesidad de hacer la interconexión entre distintas redes dio nacer a que los paquetes tuvieron distintos tamaños o Unidades de Transferencia Máxima (MTU, *Maximum Transfer Units*), que se define como el tamaño máximo en bytes de los paquetes de datos. Por ejemplo, si la MTU de la red destino sobre la cual se va a reenviar un paquete, es menor que la MTU de la red origen o procedencia, se impone la necesidad de un mecanismo de fragmentación de paquetes.

El protocolo entre entidades IP se describe mejor mediante la referencia al formato del datagrama IP mostrado en la figura 21 (Stalling, 2000, p.503).

Figura 21

Cabecera IPv4



Nota: adaptado de *Comunicaciones y Redes de Computadores* (p.503), por W. Stallings, 2000, Prentice Hall.

Los campos de la figura 21 son los siguientes:

- Versión de protocolo (4 bits): nos permite tener como referencia para la evolución de esta.
- IHL (*Internet Header Length*) (4 bits) o longitud de cabecera de internet.
- Tipo de servicio (8 bits): contiene parámetros de prioridad, rendimiento, seguridad y retardo.
- La longitud de datagrama (16 bits).
- El identificador (16 bits): que contiene las direcciones IP origen, IP destino, y el protocolo de comunicación.
- Los indicadores (3bits) son aquellos que definen la segmentación y no fragmentación de paquetes.
- El desplazamiento del fragmento (13 bits) es aquel que indica la posición del fragmento dentro del paquete original.

- El TTL (8 bits) es aquello que define el tiempo que permanece un datagrama en la red en unidades de segundos.
- Suma de comprobación de la cabecera (16 bits): está relacionado con el algoritmo de corrección de errores y solo es aplicado a la cabecera.
- La dirección origen (32 bits) establece la dirección IP pública de origen.
- La dirección destino (32bits) establece la dirección IP pública destino
- Las opciones (variable) son adicionales solicitados por el usuario que envía los datos o mensaje.
- El relleno (variable): es aquel campo que se usa para asegurar el tamaño del paquete múltiplo de 32 bits.
- Los datos (variable).

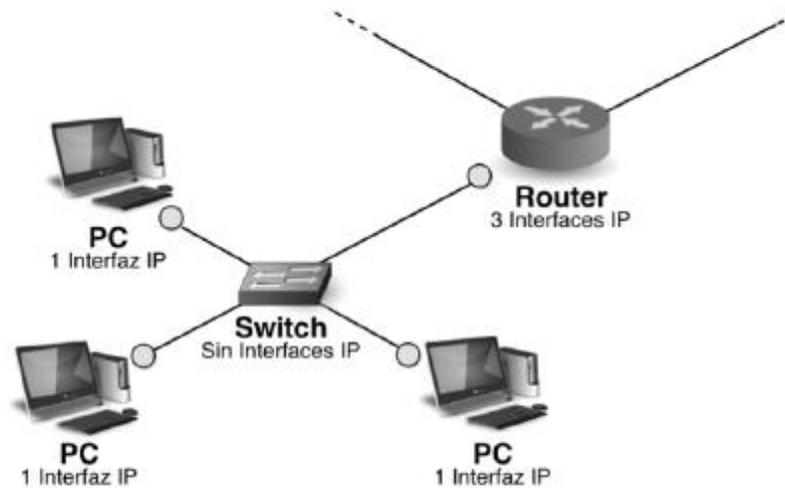
A. Direcciones IPv4. Liberatori (2018) define el direccionamiento IP como un conjunto de números asignados a interfaces de computadoras (p.336).

En la vida real el acceso a internet es a través de nombres o servicios en la red, puesto que es más sencillo recordar nombres que recordar números; esto se da gracias al servicio DNS (*System Name Domain*). Los mensajes que se desean transmitir se encapsulan en paquetes IP, que contiene datos de la dirección IP origen y destino de los protagonistas que participan en la comunicación. Esto dirección ayudan a facilitan el enrutamiento de paquetes IP entre redes.

Se debe tener en cuenta que todo dispositivo conectado a una red debe tener al menos una dirección IP en su interfaz física tal como se muestra el ejemplo de la figura 22.

Figura 22

Interfaces y direcciones IP



Nota: adaptado de *Redes de Datos y sus Protocolos* (p.336), por M. C. Liberatori, 2018, Editorial Eudem.

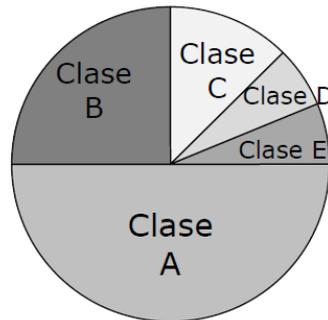
La dirección IP de las interfaces de los dispositivos se configuran de acuerdo con la red que está conectada. De tal manera, si algún dispositivo se mueve a otra red, esta dirección de red debe ser reconfigurada para que pueda establecer comunicación con los dispositivos en la nueva red.

En el libro titulado *Comunicaciones y Redes de computadores*, su autor William Stallings, clasifica el direccionamiento IP de la siguiente manera (p.504):

- Clase A es aquel grupo de pocas redes, con un grupo numerosas de computadoras o dispositivos.
- Clase B es aquel grupo medio de redes, cada una con un grupo medio de computadoras o dispositivos.
- Clase C es aquel grupo numeroso de redes, cada una con grupo de pocos computadores o dispositivos.
- Clase D es aquel grupo de uso exclusivo para comunicaciones tipo *multicast*.
- Clase E es aquel grupo de uso exclusivo para experimentos en la red global.

Figura 23

Espacio total de clases de direcciones IP

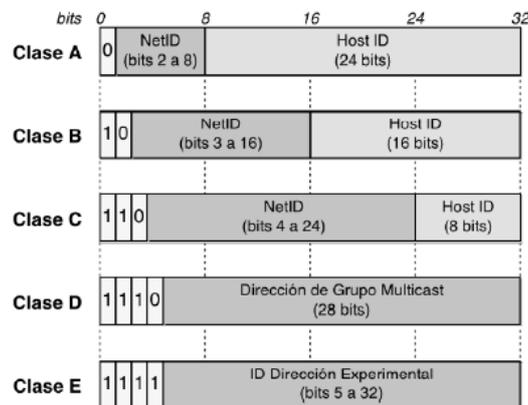


Nota: adaptado de *Redes de Datos y sus Protocolos* (p.340), por M. C. Liberatori, 2018, Editorial Eudem.

La figura 24 presenta un resumen detallado de la división en las clases de direcciones IP y numeración en binario con que inicia cada uno.

Figura 24

Clases de Direcciones IP



Nota: adaptado de *Redes de Datos y sus Protocolos* (p.341), por M. C. Liberatori, 2018, Editorial Eudem.

B. Direcciones IPv4 especiales. Liberatori (2018) menciona las siguientes direcciones IP fijas de carácter especial (p.342-343):

- Todos "0" o "0.0.0.0": es la dirección especial que tiene significado cualquier dirección en la red y es una dirección IP que no se puede asignar.
- Dirección de *loopback*: son aquellas direcciones *unicast* que se encuentran en el rango clase A: 127.0.0.0 al 127.255.255.255; generalmente se trabaja con la dirección 127.0.0.1. Esta interfaz de red virtual permite que aplicaciones de red tipo

cliente se conecten al servidor siendo una conexión local haciendo uso del protocolo TCP/IP.

C. Subredes y máscaras de subred. Stallings (2000) cita que el concepto de subred fue introducido para señalar la necesidad de tener estructuras aisladas de redes LAN interconectadas en una misma organización (p.505). Para que estas estructuras de redes LAN funcionen de manera correcta, en cada red LAN se le asigna un número de subred.

Tabla 4

Máscaras de subred por defecto

	Representación binaria	Punto decimal
Mascara de clase A por defecto	11111111.00000000.00000000.00000000	255.0.0.0
Ejemplo de mascara de clase A	11111111.11000000.00000000.00000000	255.192.0.0
Mascara de clase B por defecto	11111111.11111111.00000000.00000000	255.255.0.0
Ejemplo de mascara de clase B	11111111.11111111.11111000.00000000	255.255.248.0
Mascara de clase C por defecto	11111111.11111111.11111111.00000000	255.255.255.0
Ejemplo de mascara de clase C	11111111.11111111.11111111.11111100	255.255.255.242

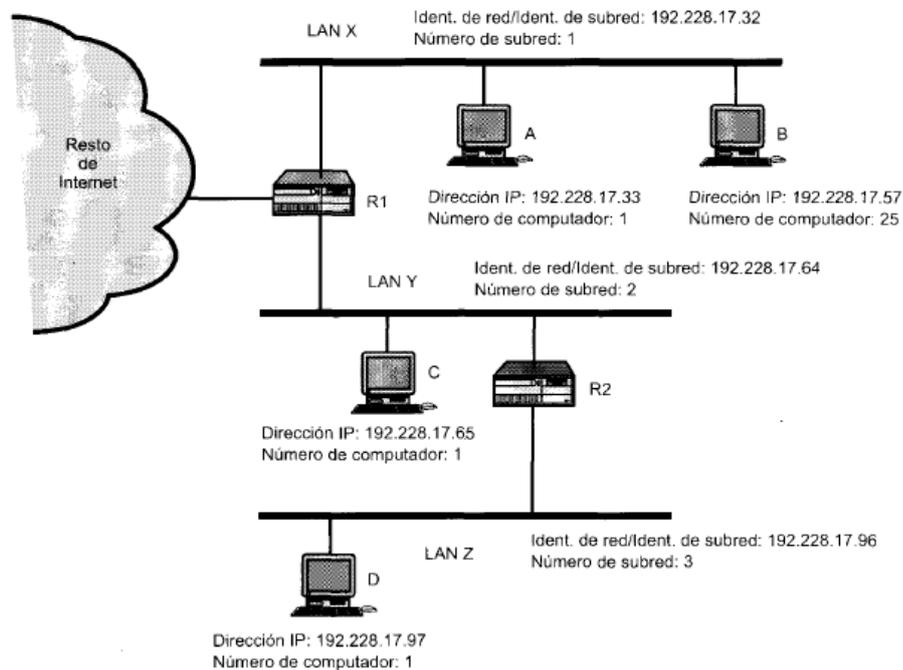
Nota: adaptado de *Comunicaciones y Redes de Computadores* (p.506), por W. Stallings, 2000, Prentice Hall.

En una red, los dispositivos de enrutamiento local deben enrutar teniendo como base una dirección IP y el número de subred o máscara. La dirección IP de la máscara de red, permite identificar si un dispositivo se va a conectar en una red local o hacia una red externa.

En la figura 25 se muestra un ejemplo de asignación de IPs en una organización.

Figura 25

Ejemplo de utilización de subredes



Nota: adaptado de *Comunicaciones y Redes de Computadores* (p.507), por W. Stallings, 2000, Prentice Hall.

D. Protocolo ICMP. Stallings (2000) define el protocolo ICMP como un medio de transferir mensajes desde los dispositivos de encaminamiento hacia computadores de la red o de manera viceversa. El protocolo ICMP proporciona información de realimentación en un entorno de comunicación (p.507).

Alguno de los tipos de mensajes ICMP (Stalling, 2000, p.508) que puede mostrar cuando se realiza una prueba de conectividad entre dos dispositivos:

- *Destination Unreachable*
- *Redirect Message*
- *Tiempo Exceeded*
- *Echo Request*
- *Timestamp*
- *Timestamp Reply*
- *Echo Reply*
- *Address Mask Request*

- *Address Mask Reply*
- *Information Reply*
- *Information Request*

2.1.8. **Redes virtuales**

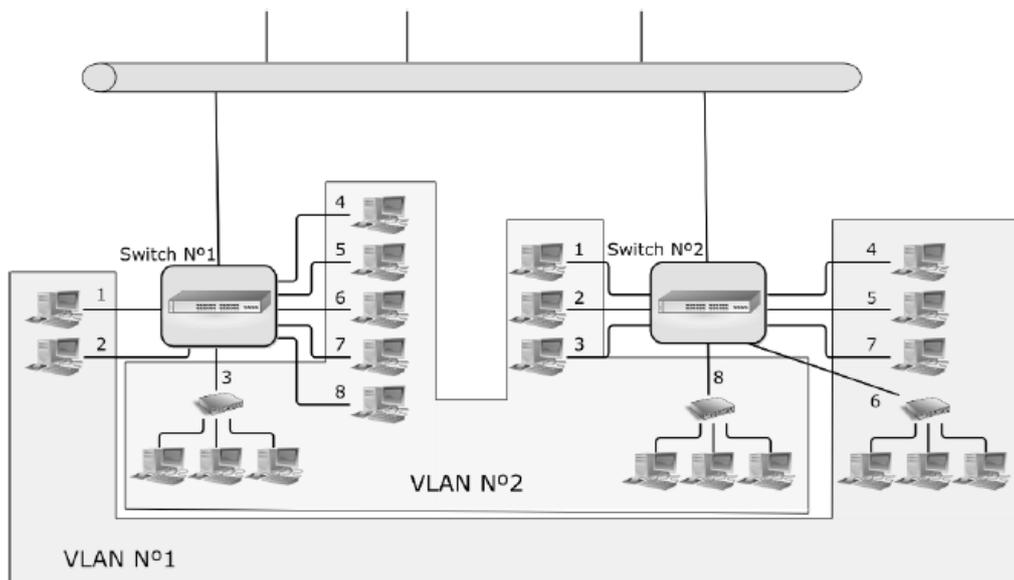
Liberatori (2018) define una red virtual, como una red lógica dentro de una red física. El objetivo principal, es agrupar equipos de trabajo con los mismos intereses o áreas, cuya data no se puede mezclar con otros dispositivos en la red. Como ejemplo se podría crear una red virtual por cada área dentro de una empresa, de tal manera que cada área tenga acceso a los recursos de red que le corresponden (p.200).

Cada VLAN se considera una red lógica independiente, y cada vez que se desea enviar paquetes a estaciones de trabajo que son parte de otra VLAN, se debe hacer uso de un dispositivo que soporte enrutamiento.

Las VLAN permite optimizar el rendimiento de la red disminuyendo el dominio de broadcast, de tal manera que solo ciertos dispositivos puedan recibir la trama de difusión.

Figura 26

Ejemplo de configuración de VLAN



Nota: adaptado de *Redes de Datos y sus Protocolos* (p.201), por M. C. Liberatori, 2018, Editorial EUDEM.

Los beneficios de utilizar VLAN son los siguientes:

- Seguridad al crear grupos de trabajos que permite separar información sensible.
- Optimizar el ancho de banda de salida a internet de acuerdo a las necesidades del grupo de trabajo.
- Identificación de grupo dispositivos de acuerdo con asignación de VLANs.
- Se disminuye el dominio de difusión al hacer agrupación de dispositivos por VLAN.
- Mayor eficiencia para el personal de IT ya que facilita el manejo red y aumenta la seguridad en la misma.

2.1.9. **Equipos de comunicación en redes de datos**

Son dispositivos físicos que se usan para interconectar computadoras u otro tipo de *hardware* con el fin de entablar un proceso de comunicación.

Entre los equipos de red principales tenemos:

A. Switch. Liberatori (2018) define el switch como un dispositivo de conexión que trabaja como un *bridge* a nivel de capa de enlace, que permite el intercambio simultaneo de tramas entre un gran número de ordenadores o estaciones de trabajo (p.186).

Figura 27

Switch HPe 5940 48 SFP+ 6QSFP



B. Router. Lopez (2018) lo define como un dispositivo de interconexión con mayor grado de relevancia en las redes informáticas (p.16). Este dispositivo tiene la capacidad de interconectar redes en el mismo nivel o entre distintos niveles.

Figura 28

Router cisco 2901



2.1.10. Arquitectura de servidores

Hoskins (2005) define un servidor como un equipo informático que se diseña para situarse en un gabinete rack o lugar dedicado dentro de una oficina con el fin del proveer servicios a clientes dentro de una red (p.9).

Este equipo informático contiene: procesador, ventiladores, memoria, chips, discos duros, ranuras PCIe, fuentes de poder, puerto de video, puertos de red, etc.; que se pueden diseñar un nivel de redundancia de acuerdo con la criticidad del servicio que se esté ejecutando.

Para mantener un nivel de redundancia, los servidores tienen componentes redundantes que pueden ser reemplazados sin necesidad de apagar todo el sistema, por ejemplo: fuente de poder, ventiladores, discos duro *hot swap*; y el *hardware* y sistema operativo están soportado para operar los 365 días del año.

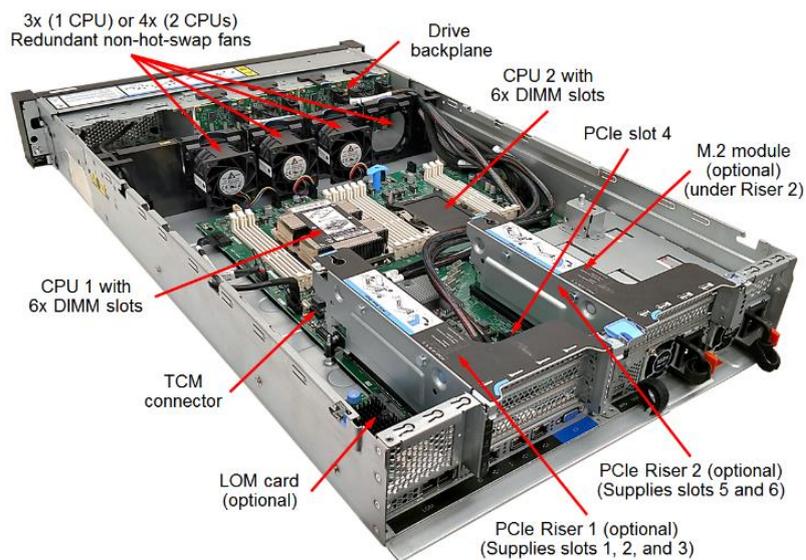
Debido a la cantidad de usuarios que se conectan al servidor, muchos de ellos tienen características especiales de componentes y gran capacidad de escalabilidad; en caso no se abaste, estos sistemas pueden conectarse a unidades externas de almacenamiento, *switch*, *router*, etc.

Según las necesidades de los clientes, los servidores se pueden catalogar de la siguiente manera:

- Los servidores de rango medio son equipos informáticos diseñados para cubrir necesidades puntuales de pequeñas empresas y permite un crecimiento limitado de recursos: memoria, disco, capacidad de I/O, etc.
- Los servidores *enterprise* son equipos diseñados para consolidar una infraestructura de IT y son armados o contruidos a necesidad de la empresa. Estos servidores se caracterizan por tener sistema redundante a nivel de componentes, soportar altas cargas de trabajo, posibilidad de crecimiento y mayor inversión por motivos de innovación. Estos sistemas generalmente son diseñados para entornos de virtualización a gran escala para optimizar cargas de trabajo, optimizar espacio y reducir costos en energía y enfriamiento del *datacenter*.

Figura 29

Arquitectura de un servidor



Nota: adaptado de: <https://lenovopress.lenovo.com/lp1046-thinksystem-sr550-server>

2.1.11. Alta disponibilidad

Costa (2019) define la alta disponibilidad como la capacidad de un sistema de disponer las aplicaciones o datos en todo momento a excepción de las interrupciones (p.186).

Se tiene 2 tipos de interrupciones las cuales son las siguientes:

- Interrupciones previstas: se da cuando se tiene mantenimientos preventivos, correctivos o actualizaciones programadas.
- Interrupciones imprevistas: que suelen suceder debido a acontecimiento externos, desastres ambientales, vulneración de seguridad o errores humanos.

Para medir el nivel de disponibilidad y fiabilidad de un sistema se tiene las siguientes métricas:

- MTTF (*Mean Time To Failure*) o tiempo promedio hasta que se dé una falla.
- MTTR (*Mean Time To Recovery*) o tiempo promedio de recuperación: es el encargado de medir el tiempo promedio en que se demora un sistema en volver estar operativo.

En todo sistema se mide la relación MTTR/MTTF para medir el nivel de disponibilidad de un sistema, y todo cliente busca aumentar su MTTR y disminuir su MTTF, para garantizar tiempos mínimos de indisponibilidad.

Tenemos los siguientes ejemplos que disponen sistemas en alta disponibilidad: sistema de aerolíneas, sistema Reniec, sistemas bancarios, bolsa de valores, sistemas de red celular, etc.

A. Soluciones de alta disponibilidad. Costa (2019) explica que toda empresa con sistemas o soluciones en alta disponibilidad debe tener las siguientes características (p.186):

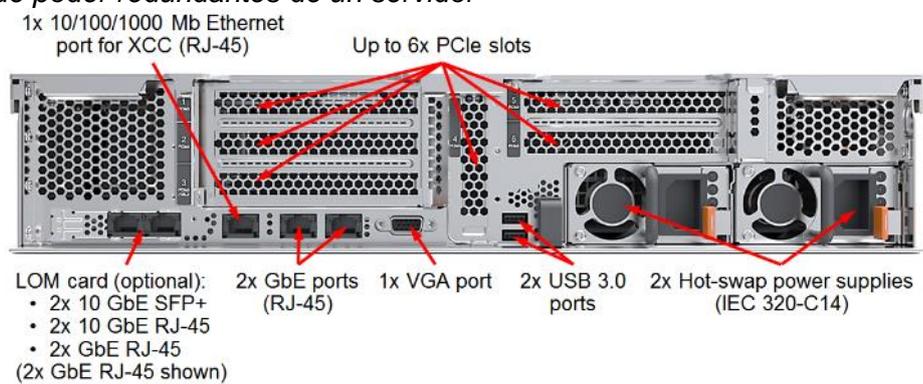
- Disponer de configuraciones que tenga tolerancia a fallos.
- Disponer de componentes y sistemas redundantes.
- Disponer de personal de contingencia y procesos para garantizar la continuidad del sistema ante algún riesgo.

En el área de IT tenemos las siguientes soluciones que permiten soportar la alta disponibilidad:

- La redundancia en dispositivos de hardware: es aquel que posibilita la continuidad del servicio a pesar de que ocurra alguna falla de *hardware*. Un ejemplo sería tener servidores duplicados, fuentes de poder redundantes, ventiladores o tarjetas de red redundantes que nos permita soportar cortes eléctricos o caídas de conectividad.

Figura 30

Fuentes de poder redundantes de un servidor



Nota: adaptado de: <https://lenovopress.lenovo.com/lp1046-thinksystem-sr550-server#power-supplies-and-cables>

- Redundancia y disponibilidad de los datos. Los procesos de respaldo y protección de datos son configuraciones necesarias para disponer la información en todo momento ante eventos fortuitos o de terceros que pueden afectar los datos. Entre las técnicas de protección conocidas tenemos las siguientes: arreglos RAID (*Redundant array of independent disks*) de discos y procesos de respaldo a través de *software* de terceros.
- Redundancia de comunicaciones. En estos años, las grandes empresas disponen de una red para la interconexión entre oficinas o sedes, y por motivo de disponibilidad de los servicios toda empresa debería tener conexiones de red independientes, que permita soportar la caída de algún enlace.

- Redundancia y distribución en el procesamiento. Un sistema de clúster de servidores permite equilibrar la carga distribuyendo recursos y disponer capacidad de crecimiento.

B. Arreglo de disco RAID. Se define RAID como un conjunto redundante de discos independientes y hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos (Costa, 2019, 187).

La distribución de datos a nivel de discos se puede gestionar de las siguientes maneras:

- *Hardware* dedicado: en este caso se requiere de una controladora RAID mediante una tarjeta tipo PCIe o integrado a la placa del servidor. Este hardware tiene como función administrar los discos y gestionar los arreglos.
- *Software*: la administración de los discos se realiza a través de una aplicación a nivel de sistema operativo.
- Híbridos: la administración de los discos se realiza a través de la BIOS.

La ventaja de tener una controladora RAID dedicada es optimizar el rendimiento y permite facilitar la instalación de sistema operativo. Una implementación basada en *hardware* suele permite hacer reemplazo de discos dañados en caliente (*hot swapping*) sin necesidad apagar el sistema operativo. Los arreglos RAID más comunes son los siguientes:

- RAID 0 o *data striping*: en este tipo de arreglos los datos se distribuyen de manera equitativa entre todos los discos sin disponer de un dato de paridad que permita soportar reconstrucción de los datos ante la falla física de un disco. Este tipo de arreglo tiene un gran rendimiento de lectura/escritura al tener varios brazos de discos, pero no es tolerante a fallos.

Figura 31

RAID 0

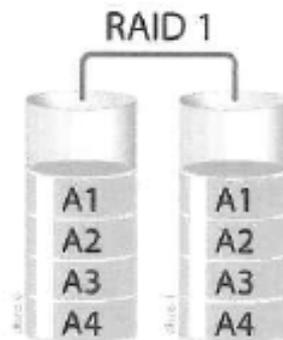


Nota: adaptado de *Seguridad y Alta Disponibilidad* (p.188), por J. Costa Ramos, 2014, Editorial RA-MA.

- RAID 1 o *data mirroring*: Es un conjunto de discos en espejo, es decir, la escritura de discos se realiza de manera paralela con el fin de disponer los mismos datos en ambos discos. Este tipo de arreglo permite soportar la caída de un disco.

Figura 32

RAID 1

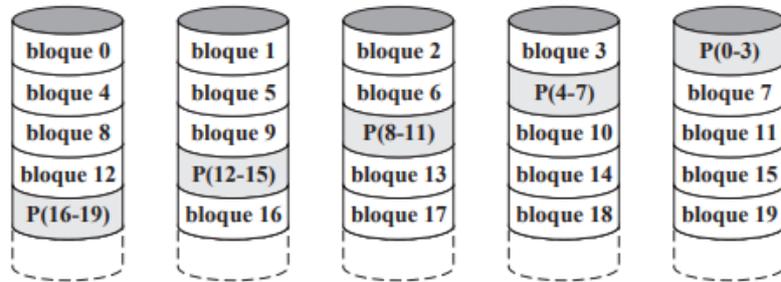


Nota: adaptado de *Seguridad y Alta Disponibilidad* (p.188), por J. Costa Ramos, 2014, Editorial RA-MA.

- RAID 5: En este tipo de arreglo se distribuye los datos entre todos los discos y adicional a ello se incluye un bloque de paridad. Esta distribución de paridad entre todos los discos permite la recuperación de la información en caso falle algún disco.

Figura 33

RAID 5

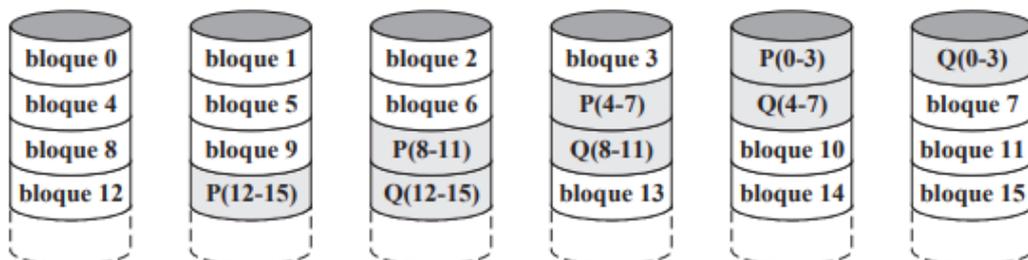


Nota: adaptado de *Organización y Arquitectura de Computadores* (p.189), por W. Stallings, 2006, Prentice Hall.

- RAID 6: Stallings (2000) explica que en un arreglo en RAID6 se distribuye los bloques de datos en todos los discos y se tiene dos bloques de paridad. Por tanto, si se necesita la capacidad de N discos RAID 6, se necesitará N+2 discos. Este tipo de arreglo de discos soporta la caída de 2 discos.

Figura 34

RAID 6

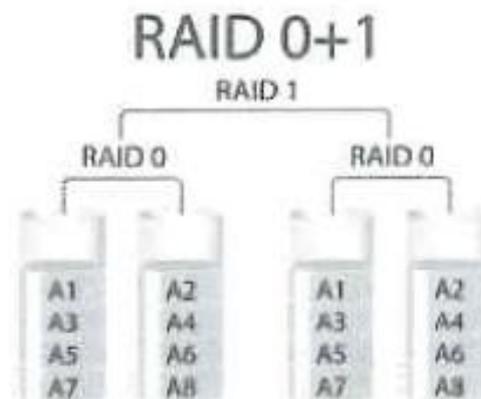


Nota: adaptado de *Organización y Arquitectura de Computadores* (p.189), por W. Stallings, 2006, Prentice Hall

- RAID Anidados: Costa (2019) explica que hay controladoras que permiten anidad niveles de RAID, es decir, que un arreglo dispone de dos niveles de protección RAID. Los arreglos RAID anidados se indican generalmente usando un + entre ellos (p.189). Un ejemplo es RAID 10 o RAID 1+0, que consiste tener un arreglo de discos divididos en múltiples RAID 1 almacenados en discos duros con un RAID 0 encima. De acuerdo con la explicación anterior y buscando un mejor rendimiento, se elige tener un arreglo RAID 0 en lo más alto y por debajo arreglos RAID 1, de tal manera que si falla algún disco habrá menos data que reconstruir.

Figura 35

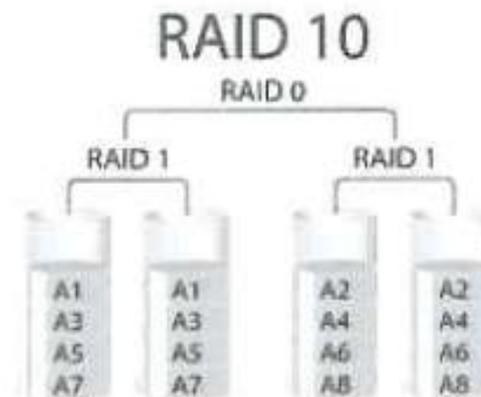
RAID 0+1



Nota: adaptado de *Seguridad y Alta Disponibilidad* (p.189), por J. Costa Ramos, 2014, Editorial RA-MA.

Figura 36

RAID 1+0



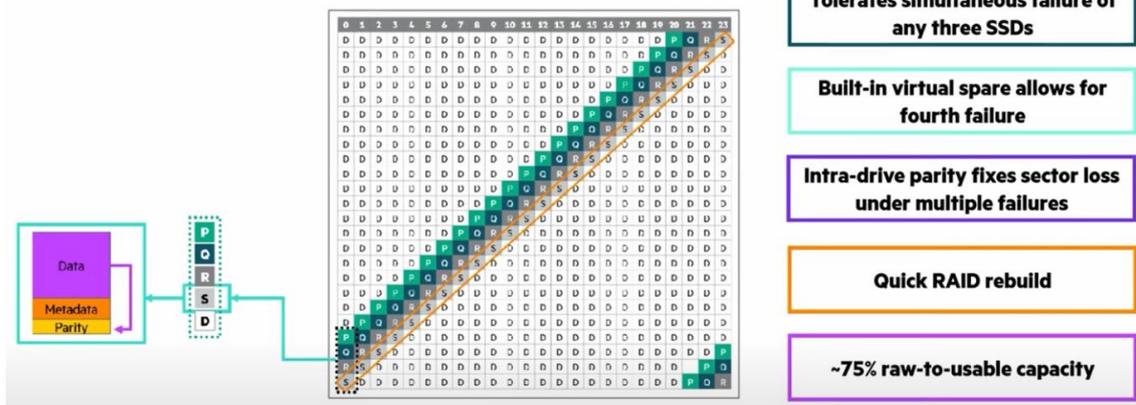
Nota: adaptado de *Seguridad y Alta Disponibilidad* (p.189), por J. Costa Ramos, 2014, Editorial RA-MA.

- RAID Triple paridad (RTP): Goel y Corbett (2012) define este tipo de RAID como un nuevo algoritmo que soporta la falla de tres discos, y es una extensión del algoritmo *Row Diagonal Parity code*, que soporta caída de 2 discos. Para cualquier cantidad de discos de datos, RTP usa tres discos de paridad. Este nivel de protección es óptimo con respecto a la cantidad de información redundante requerida y a la que se accede. RTP usa operaciones XOR y almacena todos los datos sin codificar, tiene una complejidad del cálculo de paridad del algoritmo y la capacidad de decodificación también es mucho menor que otros modelos de decodificación (p.1).

Figura 37

RAID triple paridad

TRIPLE+ PARITY RAID



Nota: fuente <https://support.hpe.com/connect/s/?language=es>.

2.1.12. Sistemas de almacenamiento de datos

Los sistemas de almacenamientos de datos son aquellos equipos que tienen la función de almacenar grandes cantidades de información de una empresa o negocio. Estos sistemas han evolucionado a lo largo del tiempo, tanto en capacidad como en complejidad, teniendo distintas opciones de configuración y arquitecturas, que hacen uso de las oportunidades que ofrecer la virtualización para dar servicio a múltiples usuarios.

Los sistemas de almacenamiento actuales se componen de los siguientes elementos:

- *Hardware*: *enclosure* o caja de discos, discos duros y otras unidades físicas.
- *Software*: viene en las controladoras, y permite la gestión del almacenamiento de datos, brindar alta disponibilidad y funcionalidades para las LUNs (*Logical Unit Number*).
- *Protocolos*: son aquellos que se usan para la transferencia de datos.

A. Funciones del sistema de almacenamiento de datos. Xing (2021) cita que “el desarrollo y progreso de la sociedad humana siempre ha sido indispensable del sistema de almacenamiento de datos y difusión de la información” (p.1). En los primeros días, la gente usaba una variedad de formas de expresión para entablar una comunicación y diversos métodos para almacenar dicha información.

Hoy en día, con el desarrollo de las comunicaciones y tecnologías de la información, se ha acelerado el proceso de transformación digital, mejora del ancho de banda de las comunicaciones y gestión de datos. Con el incremento de profesionales en el área de sistemas y redes de información, los recursos de información empezaron a tener un mejor valor agregado y como área empezó a ser un recurso estratégico para el desarrollo de toda empresa. Según una encuesta de la industria de la información global, aproximadamente una cuarta parte de los encuestados perdieron alrededor de USD \$ 250000 por hora debido a la pérdida de información o datos, y el 8 % de los encuestados, perdió casi USD \$ 1000000 por hora.

El sistema de almacenamiento de datos tiene las siguientes funciones:

- Incrementa el nivel de seguridad, capacidad y garantía de los recursos de información.
- Asegurar el acceso a los recursos de información, almacenar de manera permanente los datos y un acceso sin interrupción si es que algún usuario desea lo solicite.
- Asegurar un acceso distribución de los recursos de información y gestión unificada de esta.
- Asegurar una robustez y simplicidad de acceso de una aplicación hacia el sistema de almacenamiento. Simplificar la arquitectura de la infraestructura de IT y mejorar la interconexión, interoperabilidad e interoperabilidad entre los distintos sistemas.
- Un sistema de almacenamiento de datos unificado puede reducir los tiempos de migración y tiene la posibilidad de expandir de manera dinámica los volúmenes lógicos sin alterar el rendimiento de las aplicaciones.

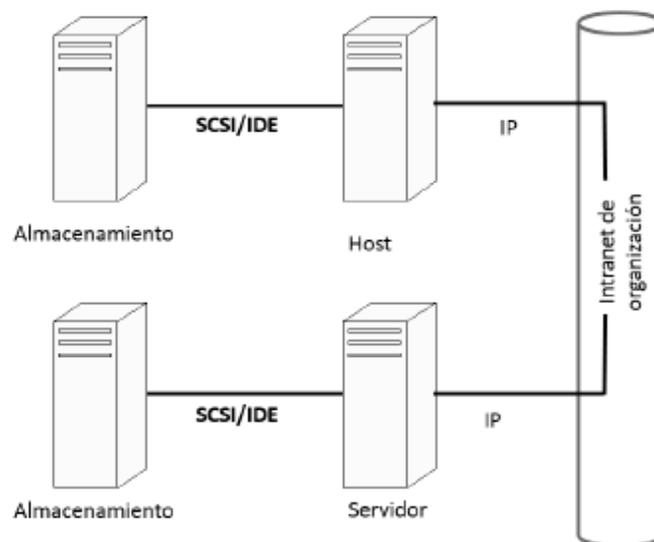
B. Almacenamiento de conexión directa DAS. Vásquez (2015) define el almacenamiento DAS (*Direct Attached Storage*) como una forma tradicional de almacenamiento de conexión directa, donde las cajas de discos se encuentran conectadas directamente con los servidores o host a través de una interfaz SCSI o IDE (p.4).

Las conexiones en DAS tienen ventajas como fácil instalación, software de administración simple, sistema de almacenamiento económico, presenta madurez técnica, etc. Sin embargo, tiene deficiencias en los siguientes puntos:

- Disponibilidad de poco espacio.
- El rendimiento del sistema está ligado a la tarjeta PCIe de interconexión del servidor.
- Los servidores que tienen conectado un almacenamiento DAS, se limitan al intercambio de información, es decir, no es de uso compartido.

Figura 38

Almacenamiento de conexión directa DAS



Nota: adaptado de *Tecnologías de almacenamiento de información en el ambiente digital* (p.5), por S. E. Vásquez, 2015, Revista electrónica semanal ISSN-1659-4142.

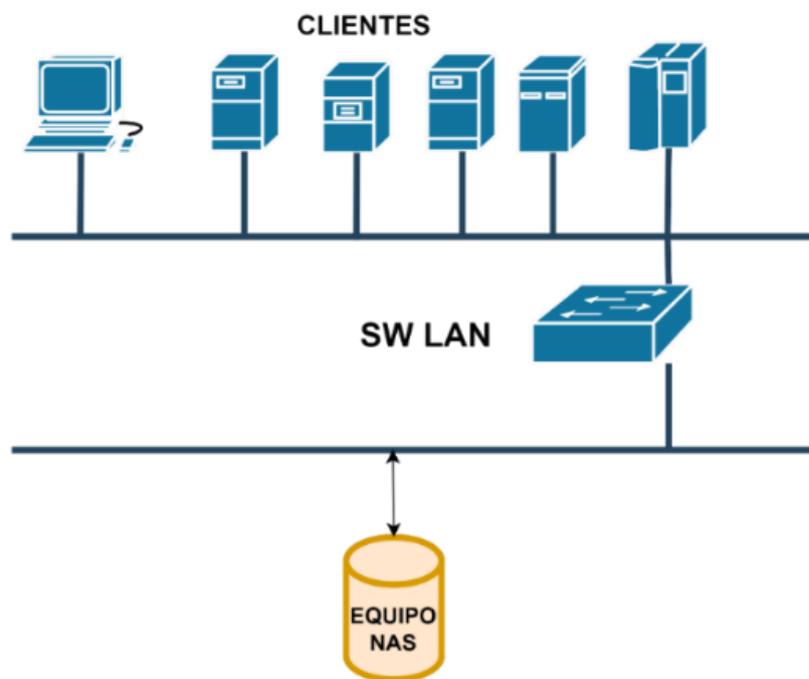
El uso ideal de este tipo de equipos es para entornos pequeños donde haya poca demanda de espacio y respuesta de disco. Por ejemplo, tenemos un minimarket, una biblioteca, una pequeña empresa, supermercado, una iglesia, etc.

C. Almacenamiento conectado en red NAS. Vasquez (2015) define el sistema NAS (*Network Attach Storage*) como un dispositivo que se conecta a la red y provee un contenedor o almacén de datos que permite a varios clientes o hosts acceder al mismo lugar de almacenamiento dentro de una red LAN (p.5). Este tipo de almacenamiento se presentan en la red a través de un servidor de archivos o de manera independiente en la red.

El almacenamiento NAS se encuentra en una red LAN, por ello, el rendimiento de este depende de las características de la LAN. Para que el equipo NAS tenga un buen rendimiento, este debe tener una buena capacidad de procesamiento y buen ancho de banda en la red, caso contrario, los clientes tendrán problemas de acceso a la información.

Figura 39

Almacenamiento conectado en red NAS



Estos sistemas son más seguros, es decir, almacena los datos en un arreglo de discos para proteger la información en caso falle alguno de ellos.

El sistema NAS tiene las siguientes ventajas:

- Sencillez al instalar un equipo nuevo
- Tiene *plugins* para la administración web
- Solución de almacenamiento económico
- Facilidad de conexión en la red LAN
- Integración con directorio activo y LDAP
- Administración de cuotas y permite escalabilidad

Por lo tanto, el sistema NAS es ideal para pequeñas empresas que buscan una solución económica para compartir archivos en la red.

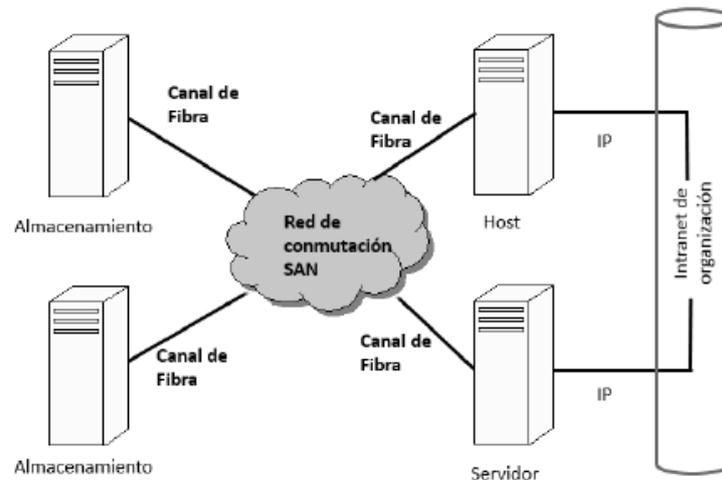
Una desventaja de estos sistemas es la escalabilidad, ya que está limitada a la capacidad del equipo y dispositivos conectados. Otro inconveniente es la gestión de copias de seguridad, cuando se ejecuta en horarios de mayor tráfico, tiene impacto en el rendimiento del equipo. Por tal motivo, la solución NAS es ideal para empresas donde la cantidad de usuarios concurrentes no es muy grande y no es adecuado para aplicaciones de grandes bases de datos.

D. Almacenamiento SAN. Según Vásquez (2015), una red SAN consiste en una red de alta disponibilidad de tipo fibra o cobre que tiene como objetivo conectar los servidores físicos con un sistema de almacenamiento; este tipo de topología permite conmutación entre múltiples nodos (ver figura 40) y generalmente se usa en entornos de nube (p.7).

En SAN, las redes de comunicación del almacenamiento de datos se encuentran en una red LAN independiente, esto con el fin de lograr una alta capacidad del canal o medio para el intercambio de datos, así como la extensión del sistema.

Figura 40

Red de área de almacenamiento SAN



Nota: adaptado de *Tecnologías de almacenamiento de información en el ambiente digital* (p.8), por S. E. Vásquez, 2015, Revista electrónica semanal ISSN-1659-4142

En una implementación de una red SAN se usan conexiones de tipo UTP, DAC (*Direct Attach Cable*) y fibra óptica.

El sistema de almacenamiento SAN es un equipo que tiene su propia capacidad de procesamiento, componentes redundantes, capacidad de crecimiento y protocolos estándar para que a través de una red SAN pueda conectarse con los servidores físicos o nodos. Este equipo tiene un alto porcentaje de disponibilidad por ser un equipo crítico para cualquier empresa.

2.1.13. SAN

La SAN es una red de alta capacidad de transferencia de datos y rendimiento.

Xing (2021) explica que, con el desarrollo de la tecnología de la información, la información se distribuye ampliamente en la red, ya que un servidor centralizado con la información no puede cumplir con los requisitos de rendimiento de I/O cuando los usuarios hacen grandes solicitudes a nivel de la red. La SAN puede ser descrito como una red *back-end*, especialmente responsable de almacenar la carga de I/O y manejar el nivel de bloque operaciones de I/O, mientras que la red *front-end* (red pública de usuarios) es responsable de la red de rutina operaciones. SAN es en realidad una extensión de la estructura del bus

de almacenamiento compartido y extiende el concepto del tradicional I/O bus al entorno de red, cambiando el modo de almacenamiento DAS tradicional (p.6).

Una SAN tiene las siguientes ventajas:

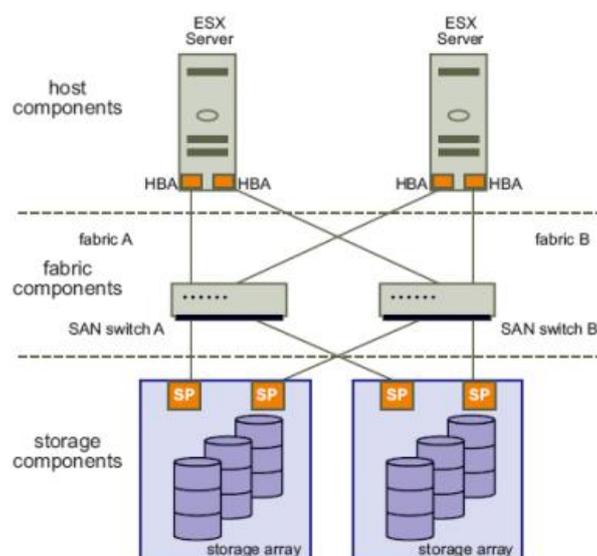
- Compartir discos lógicos a múltiples servidores
- Movilidad de datos entre arreglos dentro del mismo almacenamiento o externo.
- Procesos de *backup/restore* de manera rápida y eficiente
- Administración centralizada
- Protocolos seguros de comunicación

La integración de una solución de *VMware Vsphere ESXi* y un proveedor de almacenamiento, se puede implementar soluciones de recuperación de desastres y soluciones de alta disponibilidad. Las redes SAN pueden trabajar con sistemas de almacenamiento FC o sistemas de almacenamiento IP. El termino SAN puede usar el protocolo de canal de fibra (FCP) o el protocolo IP.

Los componentes de una SAN se pueden agrupar de acuerdo con la figura 41.

Figura 41

Componentes de una SAN



Nota: adaptado de *San System Design and Deployment Guide* (p.25), por VMware, 2010. Fuente https://www.vmware.com/pdf/vsp_4_san_design_deploy.pdf.

A. Componentes de host. Según *VMware* (2010), los componentes de host de una SAN consisten en los propios servidores y los componentes que hacen posible la conexión física a la SAN (P.26).

- HBA (*Host bus adapter*): es una tarjeta independiente del servidor con su propia capacidad de procesamiento. Esta tarjeta es la que permite la conexión de un servidor físico a una red SAN o conexión DAS hacia un servidor. Estas tarjetas están diseñadas para transferir bloques de datos y asumir carga de CPU para las tareas de almacenamiento. Pueden ser de 3 tipos: HBA FC, HBA iSCSI y HBA SAS.
- HBA *Drivers*: son los drivers que se ejecutan en cada sistema operativo y tiene como finalidad la comunicación del sistema operativo con el HBA.
- NIC: Son las tarjetas de red físicas o puertos ethernet de un dispositivo físico que trabaja a nivel de archivo. Hoy en día, las NIC tiene la capacidad de transferir archivos a nivel de bloque y lo realiza a través de una controladora iSCSI.
Cuando se usa NIC integrada a la placa del servidor y no PCIe, el servidor lleva la carga de procesamiento TCP/IP, que reduce el rendimiento del servidor. El cuello de botella en el rendimiento del procesamiento TCP/IP ha sido la fuerza que ha impulsado el desarrollo de los motores de descarga TCP/IP (*TCP/IP Offload Engines*, TOE) en las tarjetas adaptadoras. El TOE tiene la capacidad de trasladar la carga de procesamiento al HBA y así no afectar el rendimiento del servidor.
- Adaptadores iSCSI: son aquellos adaptadores a nivel de software que permite brindarle a una tarjeta NIC la capacidad de transmitir datos a nivel de bloque.

B. Componentes de fábrica. Los hosts se conectan a los dispositivos de almacenamiento en la SAN a través de la estructura SAN. El *Fabric* es la porción de red de la SAN que consta de los siguientes componentes (VMware, 2010, p.26):

- SAN Switches: es aquel equipo que permite la interconexión de los HBA y controladoras de los sistemas de almacenamiento, y permite a los administradores

configurar las rutas redundantes para la comunicación entre los servidores y sistemas de almacenamiento.

- Cables: en una red SAN se puede trabajar con fibra óptica o cobre.
- Protocolos de comunicación. los protocolos más usados son FCP, FCIP, iFCP o iSCSI.

C. Componentes de almacenamiento. Una red SAN tiene los siguientes componentes de almacenamiento (VMware, 2010, p.27):

- *Storage processors*: los procesadores de almacenamiento (SP) permiten la interconexión directa con los HBA de los hosts o los *switches* SAN. Los SP proporcionan el acceso interno a los discos y ofrece un nivel de redundancia para todo el sistema.
- *Storage Devices*: los datos pueden ser almacenados en sistema de almacenamiento de tipo disco o tape.
 - *Sistemas de almacenamiento*: es la agrupación de múltiples tipos de disco que pueden variar según la capacidad, rendimiento y otras características. Los sistemas de almacenamiento utilizan la tecnología RAID (matriz redundante de unidades independientes) para agrupar un conjunto de unidades independientes para ofrecer un nivel de redundancia.
 - *Dispositivos tapes*. Es un almacenamiento externo que se usa para procesos de respaldo de información.

D. Puertos SAN y nomenclatura de puertos. Un puerto es la conexión de un dispositivo dentro de una red SAN. Cada *host*, dispositivo de almacenamiento y componentes de la fábrica pueden tener uno o más puertos conectados dentro de una red SAN.

Los puertos se pueden identificar de la siguiente manera (VMware, 2010, p.28-29):

- WWN: el *World Wide Node Name* es el identificador único de un HBA de fibra. Un HBA de fibra puede tener múltiples puertos.
- WWPN: el *World Wide Port Name* es el identificador único de un puerto de un HBA de fibra.
- Port_ID o *Port Address*: es la dirección física del puerto de fibra.
- iSCSI *Qualified Name* (IQN): es un identificador único para un nodo iniciador o destino en una red iSCSI con nombre de formato:

iqn.aaaa-mm.naming-authority:unique

Donde

- aaaa-mm: Indica la fecha en que se creó el identificador.
- *Naming-authority*: indica el nombre inverso de dominio y generalmente lo asigna el servidor físico.
- *Unique name*: es el nombre del servidor y es único en la red. Por ejemplo, tenemos los siguientes casos: iqn.1998-01.com.local.iscsi:name1 o iqn.1998-01.com.local.iscsi:name2.

E. *Multipathing y path failover.* Un path es una ruta de comunicación desde un servidor hacia un puerto del *storage processors* del sistema de almacenamiento. Un host podría acceder a un volumen de un sistema de almacenamiento a través de una o más rutas. Cuando se tiene múltiples rutas de comunicación hacia los discos lógicos se denomina *Multipathing*.

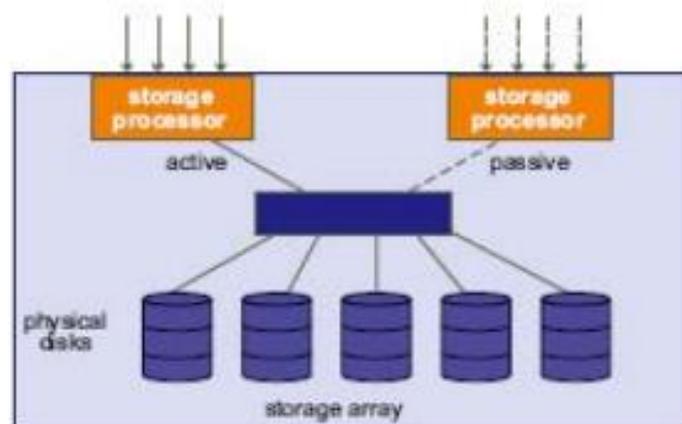
Por defecto, *VMware ESXi* solo usa un *path* de comunicación hacia desde el host hacia el disco lógico. Si este *path* falla, el servidor selecciona otro *path* disponible para mantener la comunicación. A este proceso de detección de falla de *path* y conmutación a otro *path* activo se denomina *path failover*. Un *path* puede fallar si es que algún componente físico en la SAN falla.

F. Sistemas de almacenamiento. Los sistemas de almacenamiento se pueden dividir de la siguiente manera (VMware, 2010, p.30):

- Sistema de almacenamiento activo/activo: en este tipo de sistemas se accede a los volúmenes lógicos de manera simultánea a través de todos los *storage processors* sin degradar el rendimiento del sistema. Es decir, todos los *path* se encuentran activos al mismo tiempo.
- Sistema de almacenamiento activo/pasivo: según VMware, en este tipo de sistemas el acceso a los volúmenes lógicos es a través del *storage processor* principal o activo, y el segundo *storage processor* está en estado pasivo o *stand by*, esperando que el *storage processor* principal llegue a fallar. En este caso, los *path* que se conectan al *storage processor* principal están en modo activo y los que se conectan al segundo *storage processor* estarán en *stand by*.

Figura 42

Sistema de almacenamiento activo/pasivo

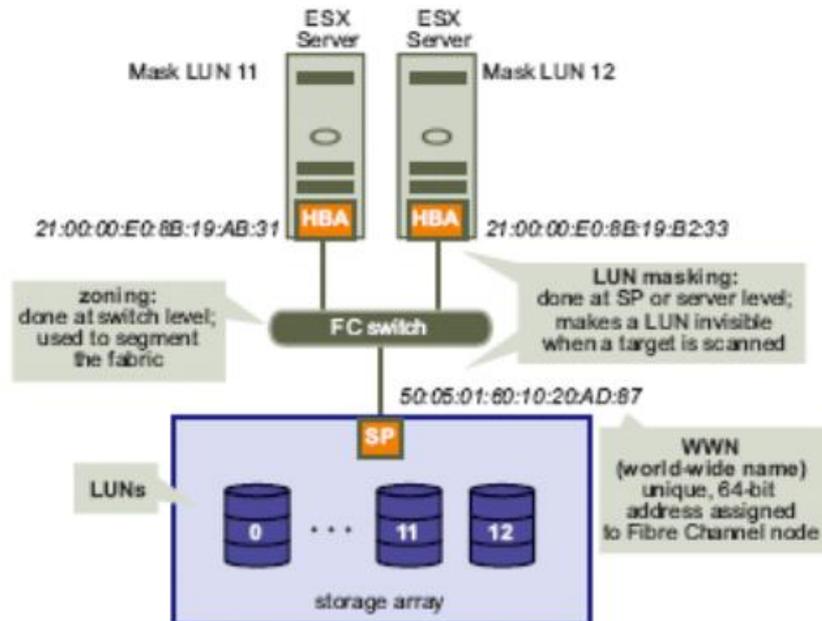


Nota: adaptado de *San System Design and Deployment Guide* (p.30), por VMware, 2010. Fuente https://www.vmware.com/pdf/vsp_4_san_design_deploy.pdf

G. LUN masking. Según VMware (2010), el enmascaramiento de la LUN es usado para la administración de permisos de acceso. El enmascaramiento de la LUN se podría dar a nivel del servidor o *storage processor*; este proceso hace posible que ciertos servidores vean ciertas LUN o discos lógicos (p.32).

Figura 43

LUN zoning and masking



Nota: adaptado de *San System Design and Deployment Guide* (p.32), por VMware, 2010, https://www.vmware.com/pdf/vsp_4_san_design_deploy.pdf.

2.1.14. Protocolos de almacenamiento

Según VMware (2010), en una red SAN se puede usar dos tipos de protocolos: FC y protocolos de almacenamiento basados en IP. Entre los protocolos de almacenamiento basados en IP tenemos (p.33): *Fibre Channel tunneling over IP (FCIP)*, *Internet Fibre Channel Protocol (iFCP)* y *SCSI encapsulado sobre protocolo IP (iSCSI)*.

Según VMware (2010), se tiene las siguientes ventajas (p.33) cuando se usa protocolos de almacenamiento basados en IP:

- Acceso global a una infraestructura IP
- No requiere muchos *skill* para la administración de la SAN
- El protocolo es adecuado para redes LAN, MAN y WAN
- El protocolo IP es escalable
- Los protocolos IP se pueden combinar con FC SAN que permite interconectar con múltiples organizaciones a través de un *iSCSI Gateway*

Tabla 5

Protocolos de almacenamiento basado en IP

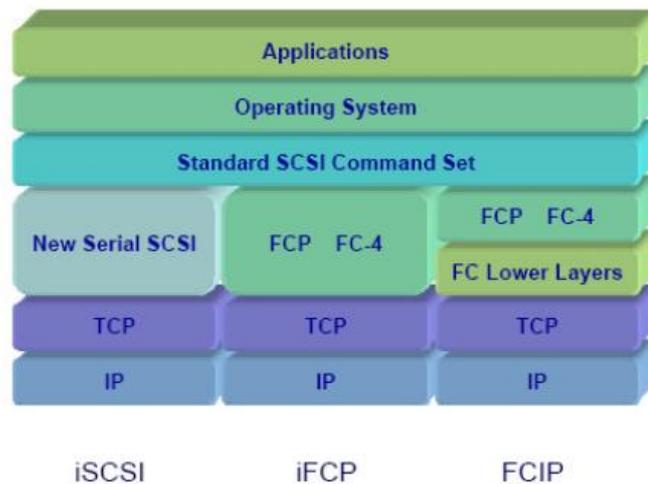
Protocolo/Aplicación	FCIP	iFCP	iSCSI
Protocolo	<i>Tunneling</i> o encapsulamiento de tramas sobre IP, que permite unir dos o más fabric.	Usa <i>Network Address Translation</i> (NAT) para transportar tramas sobre IP.	Transporta serial SCSI-3 sobre TCP/IP. Es una conexión punto a punto entre dispositivos.
Aplicación	Brinda una extensión de la <i>fabric</i> .	Brinda una extensión de la <i>fabric</i> .	Brinda una extensión de la <i>fabric</i> .
Implementación	Encapsulación y tunelado	Transporte IP Nativa	Transporte IP Nativa
Encapsulación SCSI	FCP	FCP	Capa iSCSI
Coste	\$\$\$	\$\$	\$

Nota: adaptado de *San System Design and Deployment Guide* (p.33), por VMware, 2010, https://www.vmware.com/pdf/vsp_4_san_design_deploy.pdf.

En la figura 44 se muestra las comparativa de la pila de protocolos.

Figura 44

Protocolo iSCSI, iFCP y FCIP



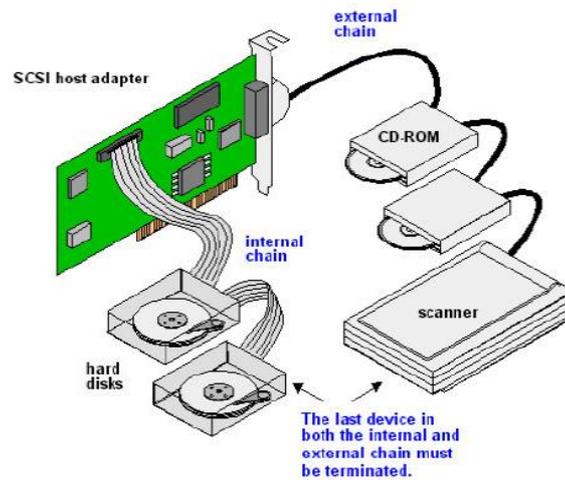
Nota: adaptado de *Almacenamiento Distribuido en Red III* (p.16), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

A. Protocolo SCSI (Small Computer System Interface). Es aquel protocolo que permite la comunicación entre un ordenador y sus partes o periféricos. Esta comunicación se da a través de un bus de datos en paralelo.

El protocolo iSCSI hace uso de comandos SCSI-3 (sistema estándar que permite extender las funcionalidades del protocolo SCSI), los cuales encapsula dentro de paquetes TCP/IP que son enviados a través de redes IP (Aragón, 2006, p.3).

Figura 45

Ejemplo de cadena SCSI



Nota: adaptado de *Almacenamiento Distribuido en Red III* (p.5), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

B. Protocolo iSCSI. Es aquel protocolo que permite implementar soluciones SAN en empresas donde se desea ahorrar costos. iSCSI es un protocolo de comunicación que se implementa sobre una red IP. El protocolo se usa en servidores (*initiators*), dispositivos de almacenamiento (*target*) y dispositivos de puertos de acceso de transferencia de protocolo (Aragón, 2006, p.6).

Una red SAN iSCSI usa switches o router para transportar los datos desde un servidor hacia un sistema de almacenamiento. Al ser ethernet, le permite trabajar en una red local y extenderlo hacia otras sedes. Una de las ventajas del protocolo es que trabaja a nivel de bloque.

En la figura 46 se muestra la pila de protocolo iSCSI y se observa que se basa en redes TCP/IP, y no hace referencia a *fiber channel*.

Figura 46

Pila de protocolo iSCSI

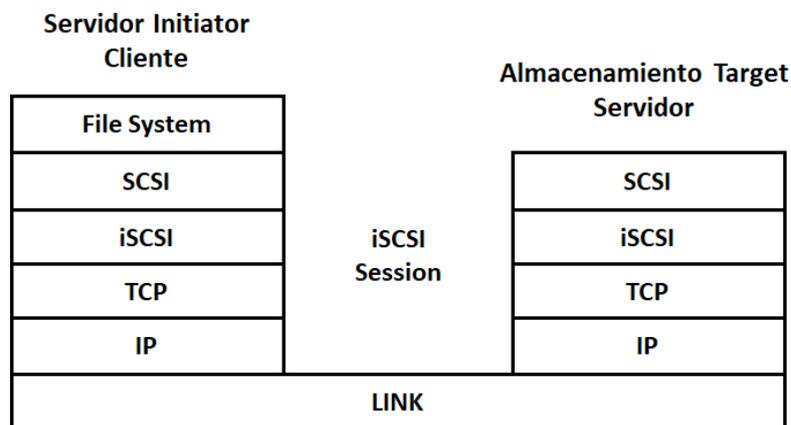


Nota: adaptado de *Almacenamiento Distribuido en Red III* (p.6), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

En la figura 47 se muestra la sesión de comunicación del protocolo iSCSI entre el *initiator* y *target*, suministrándose métodos de autenticación entre ellos.

Figura 47

Ejemplo de sesión iSCSI

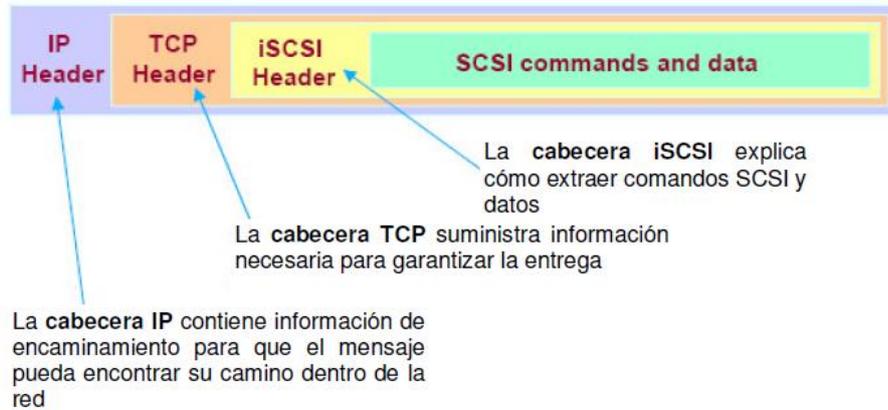


Nota: adaptado de *Almacenamiento Distribuido en Red III* (p.6), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

En resumen, iSCSI es un protocolo de transporte que suministra un modo de encapsular comandos SCSI-3 dentro de paquetes TCP/IP, tal como se muestra en la figura 48 y permite que estos paquetes sean transportados y encaminados sobre conexiones de red TCP/IP (Aragón, 2006, p.7).

Figura 48

Encapsulamiento de datos dentro de una trama iSCSI



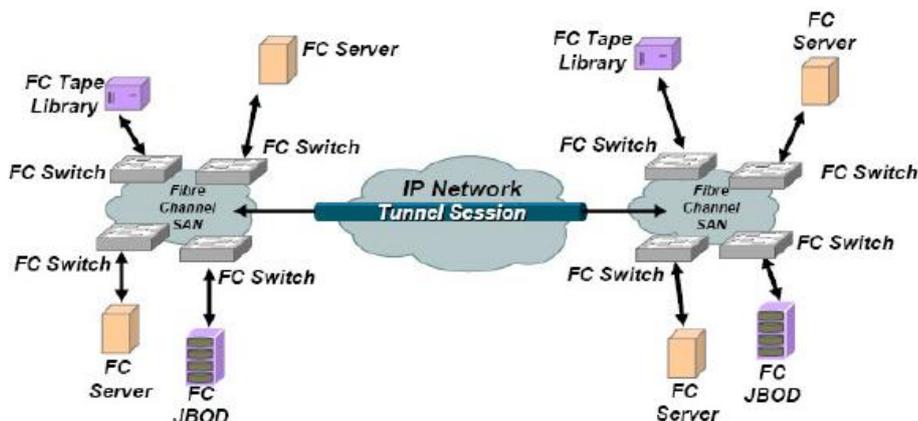
Nota: adaptado de *Almacenamiento Distribuido en Red III* (p.7), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

C. Protocolo FCIP. Este protocolo también es conocido como *Fibre Channel tunneling* (tunelaje *Fibre Channel*) o *storage tunneling* (tunelaje de almacenamiento). FCIP usa una especie de técnica de tunelado o tunelaje para transportar tramas *Fibre Channel* en el interior de paquetes IP, realizando también una correspondencia entre los dominios del entramado *Fibre Channel* y direcciones IP (Aragón, 2006, p.10).

El protocolo FCIP permite extender infraestructura SAN FC corporativa a través de un enlace troncal con protocolo IP.

Figura 49

Ejemplo de túnel FCIP entre dos redes SAN FC



Nota: adaptado de *Almacenamiento Distribuido en Red III* (p. 11), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

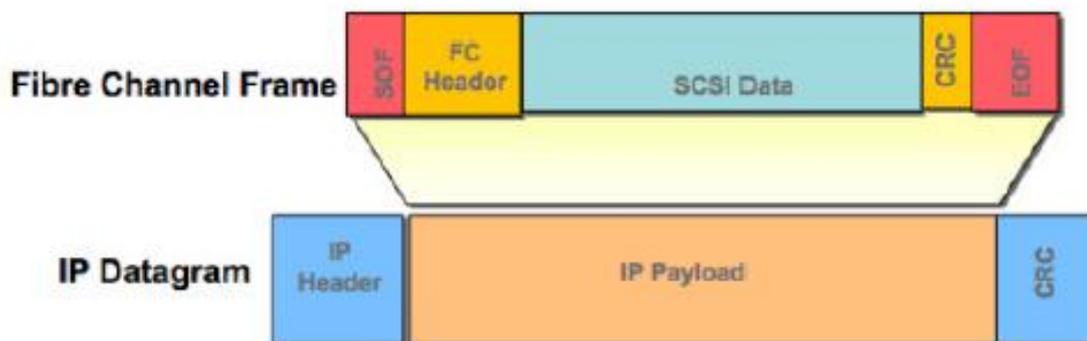
En la figura 49, FCIP permite la interconexión de dos redes SAN FC de manera transparente sobre una red FC existente, creando una conexión punto a punto que va a través de una red IP. El tráfico FC se encapsula antes de ingresar al túnel y des encapsula al llegar al otro extremo, y de manera viceversa. Este tipo de conexión posibilita la ejecución de aplicaciones a distancia, por ejemplo, replicación entre sistemas de almacenamiento ubicadas en sedes distintas (solución de *disaster recovery*).

Una red SAN FC soporta la implementación de múltiples túneles de manera simultánea, ya sea por motivo de interconectar sedes remotas o soluciones de alta disponibilidad.

En la figura 50 se muestra el formato de trama FCIP:

Figura 50

Formato de mensaje FCIP

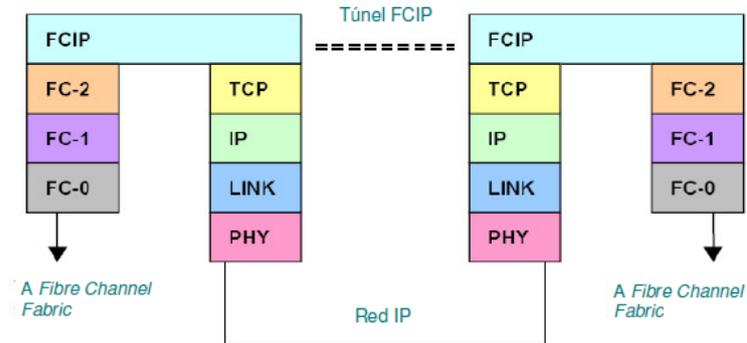


Nota: adaptado de *Almacenamiento Distribuido en Red III* (p.12), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

En la figura 51 se muestra la pila de protocolo FCIP, donde se observa que el túnel FCIP usa servicios TCP/IP para establecer la conexión entre dos redes SAN FC y controlar los errores en el proceso de transmisión de datos.

Figura 51

Pila de protocolo FCIP



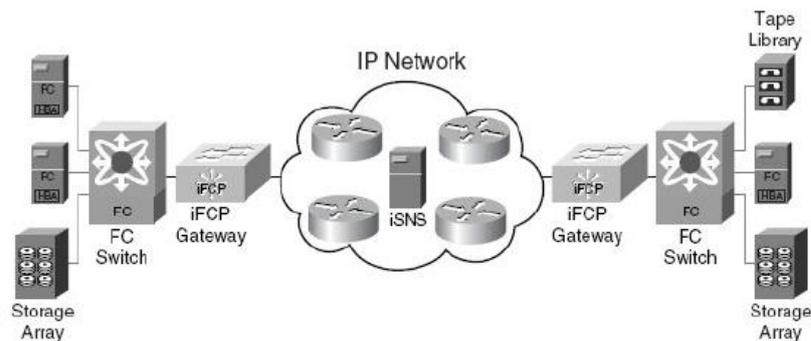
Nota: adaptado de *Almacenamiento Distribuido en Red III* (p.12), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

D. Protocolo iFCP. El protocolo *Internet Fiber Channel Protocol*, es un protocolo a nivel de *gateway* o puerta de enlace, que permite la implementación de servicios FC sobre una red TCP/IP. iFCP permite que las redes SAN FC se puedan interconectar mediante redes TCP/IP haciendo uso de switches y routers, y usa el protocolo TCP para el control de gestión, detección y corrección de errores (Aragón, 2006, p.12-13).

En la figura 52 se muestra la conexión de dispositivos FC (HBAs, switches, sistemas de almacenamiento) entre sedes, haciendo uso de equipos iFCP Gateway y una infraestructura de red existente. Cada sesión FC termina en un iFCP Gateway, luego se convierte en una sesión TCP/IP y por último se transporta por protocolo iFCP a través de internet y tiene como destino un segundo iFCP gateway para la recepción de los datos.

Figura 52

Diagrama de funcionamiento del protocolo iFCP



Nota: adaptado de *Almacenamiento Distribuido en Red III* (p.13), por J. M. Aragón Yuste, 2006, http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf.

En la figura 52, en la red IP se hace uso del servicio iSNS, que es el servicio de nombres de almacenamiento de internet. Este servicio permite hacer el registro de todos los host y dispositivos de almacenamiento, que posteriormente se pueden hacer consultas para hacer el estatus de estos. El uso de iFCP requiere usar el servicio iSNS para poder identificar el origen y destino en este tipo de comunicación.

El protocolo iFCP se creó con el objetivo de reducir el coste total en implementaciones de tecnologías de almacenamiento haciendo uso del protocolo IP, ya que la tecnología FC es una solución muy costosa. De manera paralela también se desarrolló el protocolo iSCSI, que es una alternativa IP/Ethernet eficiente en coste que iFCP.

Una de las diferencias entre el protocolo FCIP y iFCP, es que el FCIP crea una conexión dedicada para la transmisión de los datos y el iFCP está sujeto a la sesión iFCP que pueda soportar el iFCP *gateway*.

2.1.15. Virtualización

VMware define la virtualización como una tecnología basada en software que permite ejecutar varias máquinas virtuales sobre un ordenador o servidor físico, permitiendo el uso eficiente de los recursos físicos del servidor y asimismo compartir con todas las máquinas virtuales que están sobre ella. Cada máquina virtual tiene su propio sistema operativo, dirección IP y servicios que les permite trabajar de manera independiente.

Los objetivos de usar la virtualización son los siguientes: mejorar niveles de performance, disponibilidad, escalabilidad, agilidad, confiabilidad y seguridad unificada.

La virtualización tiene como elemento fundamental el hypervisor, que permite gestionar los recursos de las máquinas virtuales (procesador, y administración de estos.

Según la Universidad de Massachussets Amherst, la virtualización esta subdividida de la siguiente manera: Virtualización Nativa/Servidor, Para-Virtualización, Emulación, Virtualización a nivel de aplicación y sistema operativo.

A. Emulación. Integración de *hardware* y *software*. La emulación se define como la funcionalidad de un software para emular una aplicación o sistema operativo dentro de otro ordenador. De esta manera se puede ejecutar programas dentro de un servidor o equipo que no estaba proyectado para este fin.

B. Virtualización Nativa/Servidor. La virtualización nativa o de servidor se denomina a la partición lógica de un servidor en pequeños servidores o máquinas virtuales, donde cada máquina virtual trabaja o interactúa de manera independiente en una red.

La virtualización de servidor permite que la máquina virtual simule hardware del host físico necesario para que los sistemas operativos que se hospedan en ellas puedan compartir recursos sin afectar el uno al otro. Los ejemplos de este tipo de virtualización se presentan en las siguientes aplicaciones: *VMware Workstation*, *IBM VM* y *Parallels*.

C. Paravirtualización. En este caso, la virtualización no se realiza sobre el sistema operativo instalado en el hardware físico, sino sobre una interfaz de programación capaz de gestionar los recursos físicos (CPU, memoria, tarjetas NIC, etc.). Como ejemplos que hace uso de esta tecnología tenemos: *VMware ESXi Server* y *Citrix Xen Server*.

D. Virtualización a nivel de sistema operativo. Este tipo de virtualización permite compartir el mismo sistema operativo sin que uno afecte a la operatividad del otro y tiene un nivel de seguridad alto para la ejecución de estos.

E. Virtualización de aplicación. Este tipo de virtualización permite ejecutar una o más aplicaciones en cualquier sistema operativo sin necesidad de que esté instalado. Este tipo de virtualización permite lo siguiente:

- Reinicio de aplicaciones en caso de fallo
- Iniciar instancias de aplicación a demanda de solicitudes de servicio

- Escalabilidad y balanceo de carga para altas cargas de trabajo

F. Virtualización de almacenamiento. Este tipo de virtualización permite centralizar la administración de distintos sistemas de almacenamiento y brindar funcionalidades de software de la cabina principal.

La virtualización de almacenamiento se puede clasificar en dos grupos y son los siguientes:

- Virtualización basada en dispositivo: se hace a nivel del servidor físico, es decir, hacen uso de las controladoras de discos para la creación de los discos lógicos.
- Virtualización basada en red: realizada a través de switches.

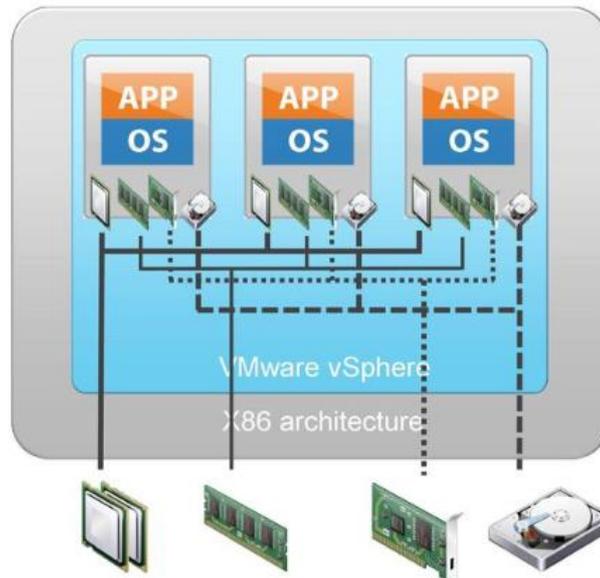
Este tipo de virtualización ofrece los siguientes beneficios: almacenamiento compartido y de forma transparente para los clientes o host, copias de seguridad de aplicaciones o discos lógicos, escalabilidad para incremento de discos y permite replicación de datos entre *datacenter*.

G. Virtualización de red. Este tipo de virtualización agrega una capa de software, que permite la separación lógica de una red física. De esta manera, ciertos ordenadores pueden conectarse con los sistemas que tienen permiso a ellos y permite que diversas cargas en la red fluyan por un mismo medio de forma segura.

H. Máquinas virtuales. Una máquina virtual es un contenedor aislado que se comporta como si fuese un ordenador físico y tiene los siguientes componentes: virtual CPU, virtual memoria RAM, disco virtual y virtual NIC propios.

Figura 53

Recursos físicos asignados a máquinas virtuales.



Nota: adaptado de *Virtualización con VMware vSphere*, por R. de la Rosa, <https://docplayer.es/679778-Virtualizacion-con-vmware-vsphere.html>.

I. Sistema *hypervisor*. El *Hypervisor* es el componente (software) de virtualización más básico que permite independizar los sistemas operativos y aplicaciones de los recursos físicos de *hardware*. El *hypervisor* tiene kernel propio y se sitúa en encima del hardware. Estos *hypervisores* permiten que diversos sistemas operativos se ejecuten de manera concurrente en el mismo hardware. El rendimiento de este no está ligado de manera directa a los sistemas operativos que se ejecutan dentro de las máquinas virtuales. El uso de *hypervisores* garantiza una optimización de uso de recursos de hardware, ya que se tendrá un pool de recursos donde los servidores virtuales harán uso según las necesidades de estas.

- *Hypervisor* tipo I: son aquellos que son instalados directamente en el *hardware*, por ejemplo: *VMware ESXi*, *Citrix XenServer*, etc. y los sistemas operativos invitados (*guests*) son aquellos que se ejecutan sobre estos (*hosts*).

Figura 54

Hypervisor VMware ESXi



Nota: adaptado de *Virtualización con VMware vSphere*, por R. de la Rosa, <https://docplayer.es/679778-Virtualizacion-con-vmware-vsphere.html>

- *Hypervisor* tipo II: son aquellos que son ejecutados dentro de un sistema operativo existente; de esa forma, los sistemas operativos se ejecutan en un tercer nivel por encima de hardware con recursos agregados y disponibles para el *hypervisor*. Como ejemplo tenemos *Hyper-V*.

2.1.16. Copia de seguridad

Se define la copia de seguridad como el salvaguardia del negocio, es decir, es un proceso crítico que tiene como objetivo disponer la información crítica ante cualquier fallo del sistema de almacenamiento principal.

Se tiene 3 tipos de copias de seguridad.

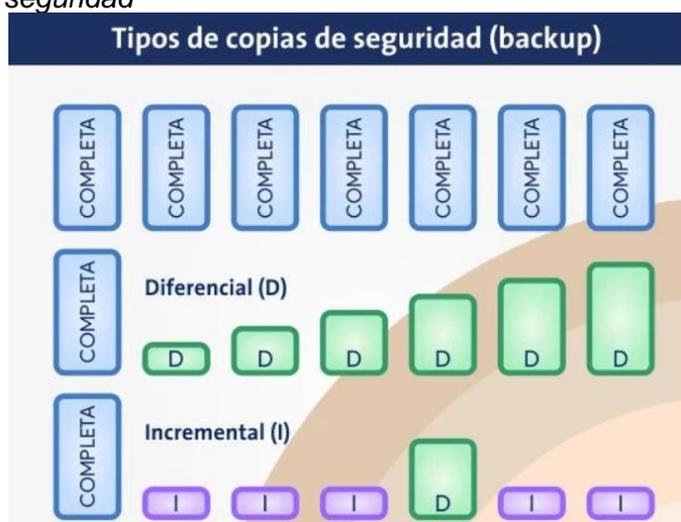
A. Copia de seguridad total o *full backup*. Consiste en realizar un respaldo total de la información que reside en un sistema en otro soporte o medio. Tiene como ventaja una restauración total de la información y como desventajas, tiempo de ejecución más largo y ocupa más espacio en disco.

B. Copia de seguridad incremental o *incremental backup*. Es aquella copia de seguridad que solo contiene los datos que han cambiado con respecto a la última ejecución de la tarea de respaldo. Las ventajas de este proceso de respaldo es que su tiempo de ejecución es más corta y requiere menos espacio en disco. La desventaja de este tipo de copia de seguridad reside en la recuperación de la información, ya que, si se desea recuperar la data de una fecha en particular, el software de respaldo tiene que sintetizar el respaldo full en disco e incrementales, haciendo más lento el proceso de recuperación.

C. Copia de seguridad diferencial o *differential backup*. Es aquella copia de seguridad que contiene todos los datos que han cambiado desde su ejecución hasta el anterior *full backup*. Esto significa que, con el tiempo, estas copias de seguridad empiezan a ocupar más espacio en disco hasta que se ejecute la copia de seguridad completa. Una de las ventajas que tiene un mejor tiempo de restauración con respecto a la copia de seguridad incremental.

Figura 55

Tipos de copia de seguridad



Nota: adaptado de *Copias de seguridad (backup) ¿cómo recuperar los datos en caso de pérdida?*, por European Knowledge Center for Information Technology (Ed.). (2020, 5 noviembre). TIC Portal. Fuente <https://www.ticportal.es/glosario-tic/copia-seguridad-backup>.

D. Plan de contingencia y continuidad del negocio. Es aquel documento que contiene el paso a paso para restablecer los servicios de IT en el menor tiempo posible antes un incidente de seguridad, evento de la naturaleza, etc., reduciendo el impacto hacia el negocio. Este plan contiene que información es crítica para el negocio, medios de almacenamiento, frecuencia de respaldo, datacenter y procesos de recuperación. Asimismo, se debe definir pruebas de recuperación de respaldos para garantizar la integridad de estos.

2.2. Marco conceptual

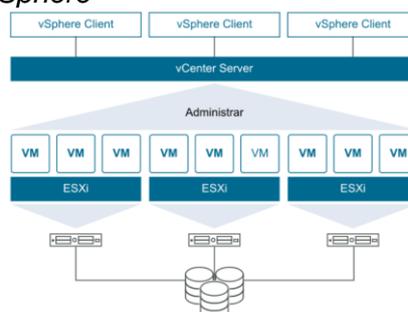
Se describirá el software de virtualización *VMware vsphere*, *san iSCSI* en entornos de *VMware ESXi*, el sistema de almacenamiento *HPE*, integración de *VMware vsphere* con el sistema de almacenamiento y topologías de configuración en una SAN.

2.2.1. Software de virtualización VMware vSphere

Es aquella plataforma propietaria de VMware, que permite a los usuarios virtualizar aplicaciones de escalabilidad vertical y horizontal, brindar alta disponibilidad y la consolidación de recursos del centro de datos virtual. Estas características dan como resultado una infraestructura altamente disponible, flexible y uso a demanda, lo cual es una característica fundamental para entornos de nube.

Figura 56

Infraestructura de VMware vSphere



Nota: adaptado de VMware vSphere 8.0, por VMware, <https://docs.vmware.com/es/VMware-vSphere/index.html>.

Un entorno de virtualización con *vmware vsphere* tiene los siguientes componentes:

A. VMware vSphere ESXi. Es el *hypervisor* de *vmware* que se ejecuta en el servidor físico. Este se encarga de virtualizar el hardware y gestionar de manera eficiente la asignación de recursos físicos a las máquinas virtuales que residen en él.

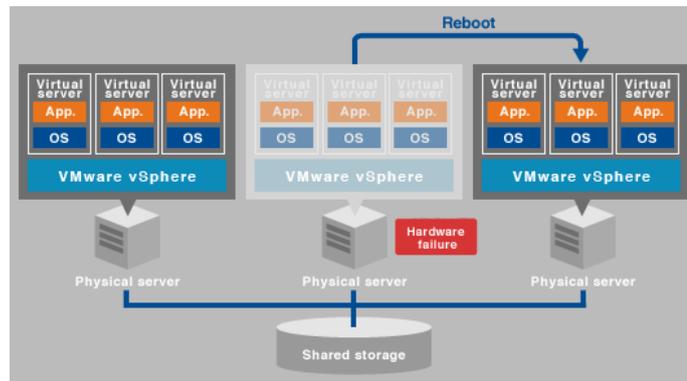
B. VMware vcenter server. En un servicio de *VMware vSphere* que permite la administración centralizada y gestión de recursos de una infraestructura con *VMware vSphere ESXi*. La aplicación se instala sobre una máquina virtual preconfigurada y se ejecuta en segundo plano, es decir, no depende de alguna conexión con el cliente *vsphere*.

El *vcenter server* contiene las siguientes funcionalidades:

- *vSphere Distributed Resource Manager (DRS)*: esta funcionalidad permite distribuir de manera equitativa el consumo de recursos de los hosts dentro de un clúster.
- *vSphere Storage vMotion*: esta funcionalidad tiene como objetivo el movimiento de servidores virtuales encendidos a nivel de los *datastore* o dispositivos de almacenamiento sin realizar algún corte de servicio.
- *vSphere Client*: en las nuevas versiones de *VMware vSphere* se ha desarrollado un cliente en versión HTML5, similar al cliente nativo de *host ESXi*. Este cliente permite conectarse a los servidores *vmware vsphere ESXi* y servicio de *vcenter server*.
- *vSphere High Availability (HA)*: esta funcionalidad permite mantener disponible el servicio ante la caída de un host físico dentro de un clúster. Este servicio permite iniciar de manera automática las máquinas virtuales que ejecutaban dentro de un servidor que presentó fallas e iniciarla dentro de otro host del clúster.

Figura 57

VMware vSphere HA



La característica vSphere HA, no utiliza la tecnología vMotion para hacer el movimiento de servidores virtuales, ya que es un movimiento no planificado. Cuando se configura un clúster de vSphere HA, un host del clúster se configura como host primario y este monitorea a través de un *heartbeat* el estado de las máquinas virtuales y host secundarios, de tal manera que pueda detectar la falla de un host y pueda ejecutar el reinicio de los servidores virtuales.

C. Virtual Switch (vSwitch). Es el principal componente que permite la conectividad entre máquinas virtuales y redes externas al servidor.

La conexión entre una máquina y un conmutador virtual es similar a la conexión entre el adaptador de red físico (NIC) de una computadora y un switch físico, pero en lugar de utilizar un cable ethernet, la máquina virtual se conecta al puerto del conmutador virtual mediante un cable virtual.

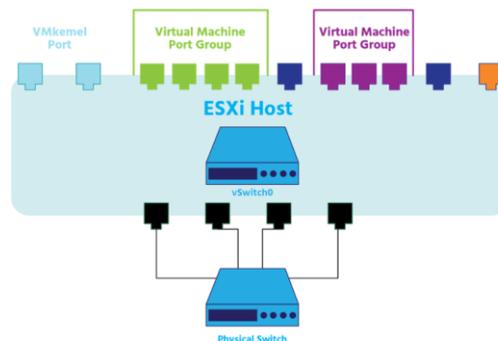
Al igual que con un switch físico, los *frame* de capa 2 entran y salen de un *virtual switch* y tienen cierta cantidad de puertos que se agrupan en *port groups*. Los puertos de enlace ascendentes son de red físicos, que se encuentran dentro de cada servidor ESXi y a través de él nos permite hacer la interconexión de un switch virtual con un *switch* físico de forma predeterminada. Cada *host ESXi* tiene un solo conmutador virtual llamado vSwitch0.

Los elementos más importantes son los siguientes:

- *vSphere standard switch*: el virtual switch que se configura a nivel de cada servidor ESXi.
- *vSphere distributed switch*: el virtual switch que se configura a nivel del *vcenter server* y su configuración se aplica para todos los servidores del clúster.
- *Standard port group*: la agrupación de puertos a nivel del *virtual switch*, que permite configurar características como limitaciones de ancho de banda, *vlan tagging*, etc.
- *VMkernel TCP/IP Networking layer*: la capa de red *VMkernel* es la que proporciona conectividad a los *host ESXi* y se usa para manejar tráfico de: *vMotion*, *Fault Tolerance*, almacenamiento IP y *vSAN*.

Figura 58

VMware virtual switch



Nota: adaptado de *What are Virtual Switches and Standard Switches?*, por S. Varshney, 2020, <https://www.c-sharpcorner.com/article/what-is-virtual-switches-and-standard-switches/>

D. Datastore o almacén de datos. Los datastore son almacenes lógicos que contiene un formato de sistema de archivos, y permiten optimizar el rendimiento de ejecución de las máquinas virtuales. Adicional a las máquinas virtuales, también se puede guardar imágenes ISO para la instalación de sistemas operativos, plantillas, *driver*, etc. Y se clasifican de la siguiente manera:

- *VMFS (Virtual Machine File System)*: es el formato de sistema de archivos propietario de VMware usado para el almacenamiento en bloque y permite optimizar la ejecución de múltiples máquinas virtuales como si fuese una sola.

- NFS (*Network File System*): aquel almacén de datos que usa el protocolo NFS. Vmware soporta protocolo NFS v3 y v4.1. Los discos son presentados desde un servidor NFS o NAS. La forma de trabajo es como si fuese una carpeta compartida.
- vVOL: es el datastore que puede ser presentados por ciertos sistemas de almacenamiento de datos con un nivel de *firmware* que soporta esta tecnología y que permite almacenar de manera nativa las máquinas virtuales y se puede aplicar políticas de almacenamiento para hacer uso de funcionalidades como replica, *snapshot*, etc.
- Datastore vSAN: aquel almacén de datos que se presenta en una solución vSAN.

2.2.2. ESXI y SAN ISCSI

El almacenamiento SAN puede conectarse a un servidor ESXi mediante el protocolo de iSCSI y usa la arquitectura cliente-servidor.

La SAN iSCSI utiliza equipos de comunicaciones y conexiones de alto rendimiento entre los servidores y los sistemas de almacenamiento. Entre los componentes tenemos:

- Tarjeta NIC o HBA del servidor
- Conmutadores switches o router
- Puertos ethernet de las controladoras del sistema de almacenamiento
- Cables UTP, FC o DAC.

Generalmente el iSCSI *target* representa un sistema de almacenamiento en la red, pero hay casos que podría ser una SAN iSCSI virtual.

A. Nodos y puertos en la SAN iSCSI. En una SAN iSCSI, un *initiator* o *target* representa un nodo iSCSI. Cada puerto tiene un determinado identificador en la red SAN y el servidor ESXi usa los siguientes métodos para identificar un nodo:

- Cada nodo iSCSI tiene una dirección IP, de tal manera que sean únicos en la red y asimismo puedan comunicarse.

- El IQN es el nombre universal único para identificar un nodo iSCSI.
- El ESXi genera identificadores únicos para sus iSCSI *initiators*.
- El alias iSCSI es un nombre corto para un puerto, que se utiliza para facilitar la identificación y configuración. Cada nodo puede tener uno o más puertos que se conecta a la SAN y cada puerto genera una única sesión iSCSI.

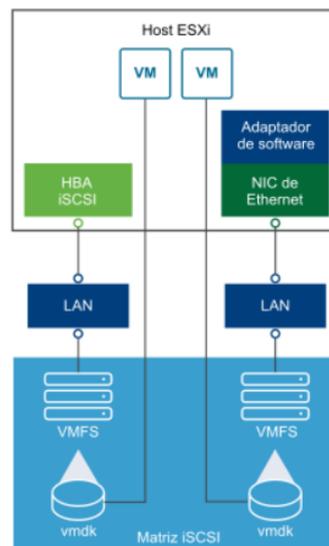
B. iSCSI Initiator. Para que los servidores con vmware vsphere ESXi pueda conectarse a iSCSI targets, el host debe usar iSCSI initiators.

El *initiator* tiene como funcionalidad originar la comunicación en una red SAN iSCSI. Tenemos dos tipos y son los siguientes:

- Hardware iSCSI: En este caso el host se conecta al almacenamiento a través de tarjetas PCIe.
- Software iSCSI: En este caso el host usa un iniciador iSCSI basado en software que hace uso de una tarjeta de red.

Figura 59

Tipos de conexiones iSCSI



Nota: adaptado de *Almacenamiento de vSphere 8* (p. 65), por VMware, <https://docs.vmware.com/es/VMware-vSphere/8.0/vsphere-esxi-vcenter-80-storage-guide.pdf>.

En la figura 59, la imagen de la izquierda el host hace uso de un adaptador iSCSI de hardware; y en el lado derecho, hace uso de un iSCSI de software y una NIC física.

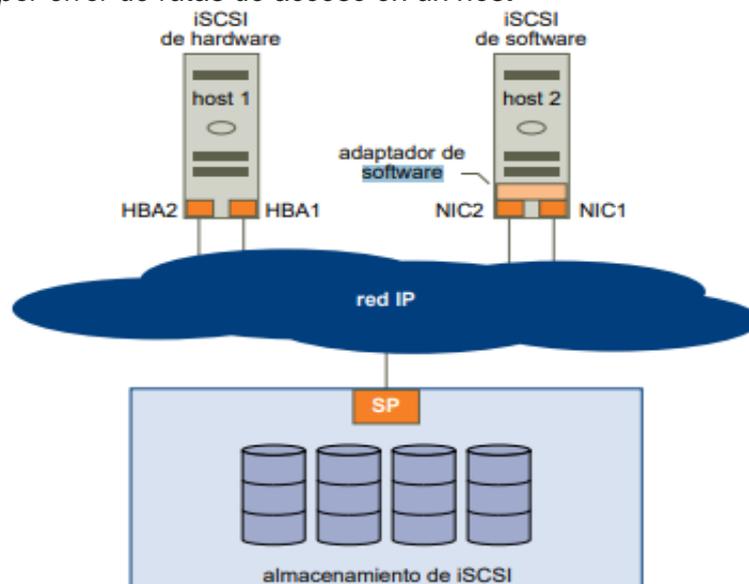
C. Conmutación por error de path iSCSI en VMware vSphere ESXi. Cuando se configura un host ESXi para usar *multipathing* y *path failover*, se debe tener varios HBA físicos o NIC físicas. El uso de múltiples path nos permite tener redundancia de los *path* ante la caída física de alguno de ellos.

Cuando se realiza configuraciones de *multipath* en VMware vSphere ESXi, se debe tener en cuenta las siguientes consideraciones:

- ESXi no acepta *Multipathing* entre adaptadores iSCSI físicos y virtuales.
- Trabajar con adaptador iSCSI de software permite trabajar con múltiples rutas.
- En diferentes hosts se pueden combinar adaptadores dependientes e independientes.

Figura 60

Conmutación por error de rutas de acceso en un host



Nota: adaptado de *Almacenamiento de vSphere 8* (p. 234), por VMware, <https://docs.vmware.com/es/VMware-vSphere/8.0/vsphere-esxi-vcenter-80-storage-guide.pdf>.

2.2.3. Sistema de almacenamiento HPe StoreOnce

Estos equipos son sistemas de copias de seguridad de deduplicación basados en disco que proporcionan copia de seguridad automatizada, recuperación de datos y retención de datos para la IT híbrida.

El sistema *HPe StoreOnce* permite reducir los costes de la protección de datos en una única arquitectura de deduplicación unificada que ofrece el rendimiento con el mejor precio de su categoría de toda la gama.

Esta familia de equipos permite reducir el riesgo con velocidades de copia de seguridad líderes del sector de hasta 288 TB/hora gracias a un sistema federado de 8 nodos y alta disponibilidad que utiliza *HPe StoreOnce VSA* para reducir las ventanas de copia de seguridad. En el ámbito de la copia de seguridad, la recuperación de datos y la retención de datos, *HPe StoreOnce* incluye todas las funcionalidades que esperarías de una copia de seguridad en disco, entre las que destaca el cifrado de datos, para protegerlos en reposo, en tránsito (solo *HPe StoreOnce Catalyst*) y en la nube.

El sistema *HPe StoreOnce 3640* proporciona copia de seguridad escalable y recuperación para centros de datos pequeños y medianos. Asimismo, constituye un dispositivo de destino de replicación ideal para hasta 36 oficinas remotas y sucursales. Este equipo escalable de 2U de rack proporciona de 36 a 108 TB de capacidad local utilizable empleando kits de actualización, y hasta 324 TB con Cloud Bank Storage. Asimismo, resuelve con facilidad las ventanas de copia de seguridad cada vez más reducidas con velocidades de hasta 18 TB/hora utilizando *HPe StoreOnce Catalyst*, pero siempre se debe tener en cuenta que el rendimiento real va a depender de la configuración, tipo de información, flujo de comunicación, etc.

La figura 61 muestra la vista frontal del sistema de almacenamiento *HPe StoreOnce 3640*.

Figura 61

Vista frontal HPe StoreOnce 3640



2.2.4. Sistema de almacenamiento HPe Nimble

La familia de sistemas de almacenamiento *HPe Nimble Storage* son un conjunto de equipos optimizados para usar discos satas / flash y brindar alta seguridad para lo datos, que contiene tecnologías de deduplicación, compresión, replicación, virtualización, etc, que permiten ofrecer el mejor rendimiento de los discos. Su tecnología *Infosight* de análisis predictivo previene incidencias sobre el equipo o servidores virtuales o físicos que acceden al sistema de almacenamiento, ya que supervisa el flujo de datos desde el sistema de almacenamiento hasta la aplicación, y además tiene la capacidad de monitorear la infraestructura de redes, servidores y máquinas virtuales.

HPe Nimble Storage reinventa la experiencia de almacenamiento con una plataforma de almacenamiento inteligente y autogestionada que desbloquea la agilidad de IT, garantiza que las aplicaciones estén siempre activas y sean rápidas, brinde la experiencia en la nube en todas partes y sea consumible como un servicio. *HPe Nimble Storage* facilita la aceleración de la innovación sin preocuparse por su almacenamiento. Está listo para aplicaciones críticas para el negocio con una resistencia absoluta con más de 6 nueves de disponibilidad (99,9999%) de datos medidos y baja latencia con un rendimiento alto y constante.

La figura 62 muestra la vista frontal del sistema de almacenamiento *HPe Nimble HF20*.

Figura 62

Vista frontal HPe Nimble HF20

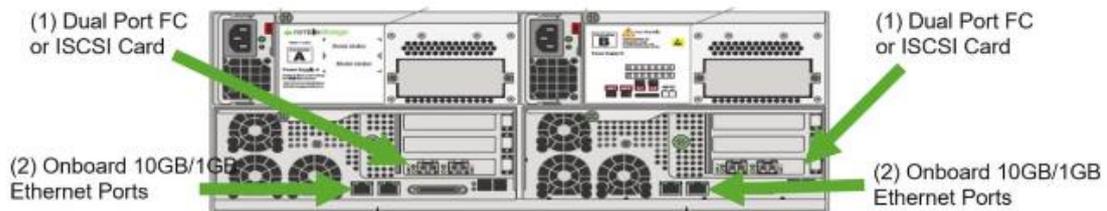


Nota: adaptado de *HPe Nimble Storage Adaptive Flash Array* (p.1), por HPe, 6 de junio de 2022, <https://www.hpe.com/psnow/doc/a00008274enw?ver=31>.

La figura 63 muestra la vista trasera del sistema de almacenamiento *HPe Nimble* HF20.

Figura 63

Vista trasera HPe Nimble HF20



Nota: adaptado de <https://www.xbsasia.ph/product/hpe-nimble-storage-af20-all-flash-dual-controller-10gbase-t-2-port-configure-to-order-base-array/>

2.2.5. *VMware vSphere* y sistema de almacenamiento *HPe Nimble*

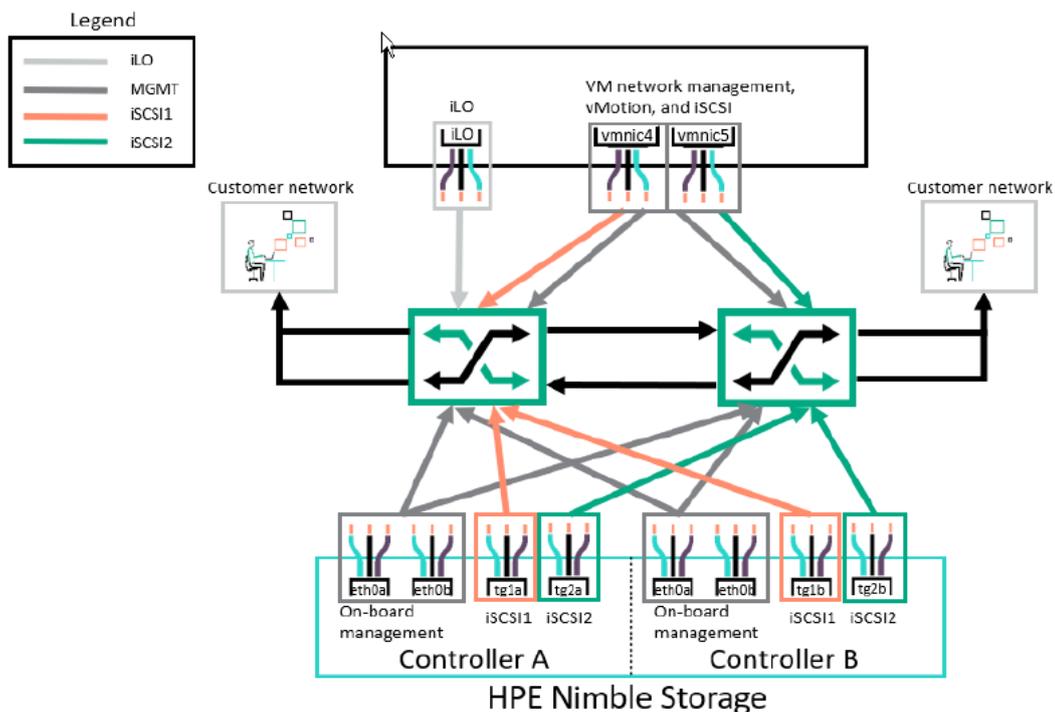
Con respecto a la conectividad iSCSI entre un *VMware vSphere ESXi* y el sistema de almacenamiento *HPE Nimble* se debe considerar los siguientes criterios de diseño:

- El *host ESXi* debería tener al menos dos tarjetas de red físicas dedicadas para conexión iSCSI. Deben ser dos tarjetas por motivos de tener conexiones redundantes.
- El *Vmware iSCSI software initiator* es el preferible método para conectarse con el sistema de almacenamiento *HPe Nimble*.

- En un entorno de alta disponibilidad, se debe tener al menos dos switches iSCSI y las conexiones se deben redundantes entre los componentes, de tal manera que la conectividad debe persistir a pesar de que algún componente físico falle.
- Cuando los puertos *VMkernel* del *software iSCSI Multipathing* están en el mismo dominio de broadcast capa dos y subred IP, se puede vincular los puertos *VMkernel* en el adaptador de *software iSCSI*. Los destinos iSCSI que están los SP del sistema de almacenamiento también tiene que estar en el mismo subred IP para que exista comunicación
- Cuando los puertos *VMkernel* del *software iSCSI Multipathing* están en distintos dominios de broadcast capa dos y subred IP, no se puede vincular los puertos *VMkernel* en el adaptador de *software iSCSI*.
- La política de *NIC teaming* en el *virtual switch* de comunicación con el *storage* debe ser tipo *activo/standby* por cada puerto *VMkernel*.

Figura 64

Arquitectura de conectividad iSCSI entre servidor y sistema de almacenamiento Nimble



Nota: adaptado de *Best Practices for Implementing HPE Nimble Storage with VMware vSphere 7* (p.8), por HPE, <https://www.hpe.com/psnow/doc/a00104406enw>.

- HPe recomienda que del sistema de almacenamiento se dedique un par de interfaces para tráfico de administración y el resto de las interfaces para tráficos de datos. Se debe asegurar que todas las interfaces de tráfico de datos se conecten al *switch* físico dedicado para tráfico de datos. En caso el *switch* se comparta con otros tipos de tráfico, se debe crear VLAN para separar el tráfico entre el puerto *ESXi VMkernel* y las interfaces de acceso del sistema de almacenamiento HPe Nimble.
- HPe recomienda habilitar el Flow control en los puertos del switch en el cual las interfaces del ESXi y del sistema de almacenamiento HPe estas conectados. Si no se llega a habilitar el Flow control, es posible que paquetes de nivel TCP se retransmitan o tareas de nivel iSCSI aborten.
- HPe recomienda el uso de *jumbo frames* de 9000 bytes en lugar del valor por defecto de 1500 bytes. Usa tramas (*frames*) grandes, reduce la potencia de procesamiento para procesar los encabezados de las tramas. La configuración se deber realizar en los siguientes componentes: puerto *VMkernel* de servidor ESXi para tráfico iSCSI, puertos físicos del switch e interfaces del sistema de almacenamiento *HPe Nimble*.

A. HPe Nimble Storage Connection Manager. El *HPe Storage Connection Manager* (NCM) para *VMware ESXi* administra las conexiones desde los hosts hacia los volúmenes del sistema de almacenamiento *HPe Nimble*. Para simplificar la configuración de las múltiples conexiones y MPIO (*Multipath IO*), el *Nimble OS* requiere solo una dirección IP (dirección IP de descubrimiento iSCSI) al momento que se establezca la comunicación y no el conjunto completo de direcciones IP de las interfaces iSCSI. El NCM consta de dos elementos esenciales para optimizar las sesiones iSCSI desde el host ESXi al sistema de almacenamiento HPe y son los siguientes:

- *HPe Nimble Storage Connection Service* (NCS)
- *HPe Nimble Storage Path Selection Policy* (PSP)

En toda implementación de un nuevo sistema de almacenamiento se debe tener en cuenta los siguientes criterios de diseño:

- El NCM se instala en los hosts ESXi que requieren conexión con el sistema de almacenamiento.
- En implementaciones de HPe Nimble Storage dHCI (*Dissaggregated Hyperconverged Infrastructure*), las actualizaciones NCM se gestionan desde el vcenter usando la aplicación VMware vRealize Suite Lifecycle Manager.
- Si se requiere escalar con múltiples sistemas de almacenamiento, es necesario el uso de NCM.

2.2.6. Topologías soportadas del sistema de almacenamiento HPe Nimble

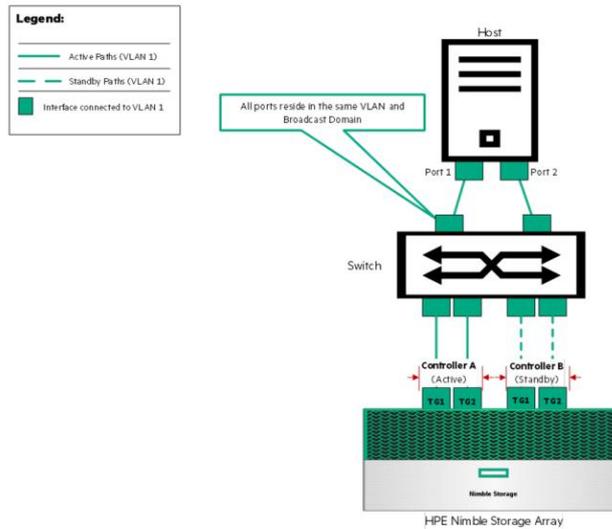
El sistema de almacenamiento *HPe Nimble* tiene una opción de configuración avanzada conocida como zonas de dirección IP. Las zonas de dirección IP le permiten controlar las rutas que se establecen entre los hosts conectados y el sistema de almacenamiento. Se puede usar esta función para evitar enviar tráfico iSCSI a través de una conexión ISL (*Inter Switch Link*) entre *switches* cuando utiliza una única subred entre varios switches.

HPe describe cuatro tipos de topologías y son los siguientes:

A. Subred y switch únicos. Este tipo de topología es de configuración simple y no tiene redundancia, y el switch representa un único punto de fallo.

Figura 65

Topología subred y switch único

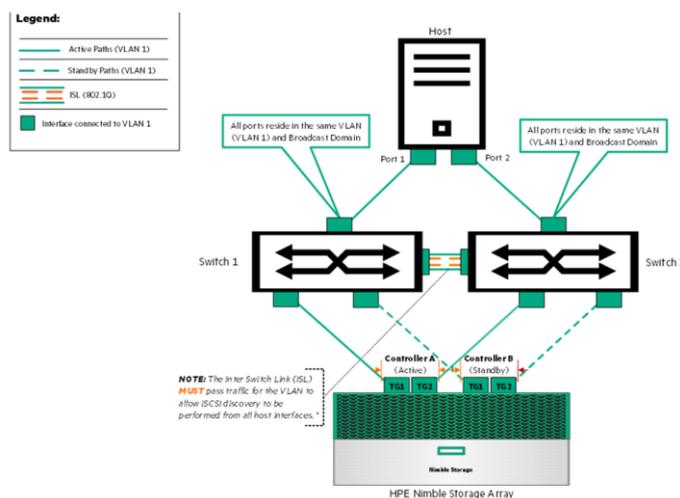


Nota: adaptado de *HPE Nimble Storage Deployment Considerations for Networking* (p.14), por HPE, 2021, https://infosight.hpe.com/InfoSight/media/cms/active/public/HPE_Nimble_Storage_Deployment_Considerations_for_Networking.pdf.

B. Subred única y múltiples switch. En este tipo de topología se provee redundancia a nivel de la infraestructura de la red. El tráfico de datos se transmite inalterado e interrumpido entre todos los *hosts* y puertos físicos del sistema de almacenamiento, que están configurados dentro de la misma subred.

Figura 66

Topología subred único y switch múltiple



Nota: adaptado de *HPE Nimble Storage Deployment Considerations for Networking* (p.15), por HPE, 2021, https://infosight.hpe.com/InfoSight/media/cms/active/public/HPE_Nimble_Storage_Deployment_Considerations_for_Networking.pdf.

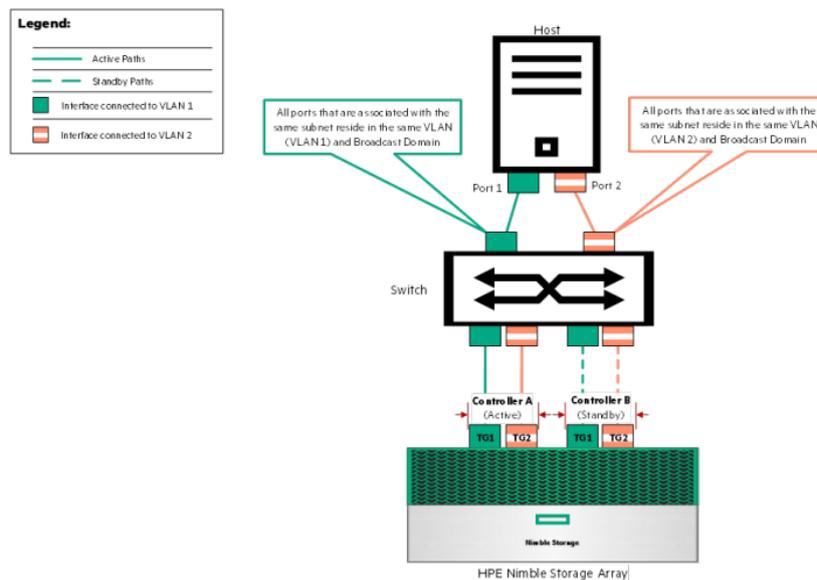
Se recomienda usar la característica de zona de direccionamiento IP para reducir la carga de tráfico sobre el enlace ISL.

Separar las conexiones de las controladoras activo y *stand by*, es una forma de conectar cada controladora a múltiples switches.

C. Múltiples subredes y *switch* único. En este tipo de topología se tiene múltiples subredes y un único switch, y es típicamente usado cuando el entorno no requiere redundancia, ya que el switch es el único punto de fallo. El tráfico de pasos se debe transmitir de manera inalterada e interrumpida entre todos los puertos configurados dentro de la misma subred. Trabajar con varias subredes disminuye el dominio de broadcast.

Figura 67

Topología subred múltiple y switch único

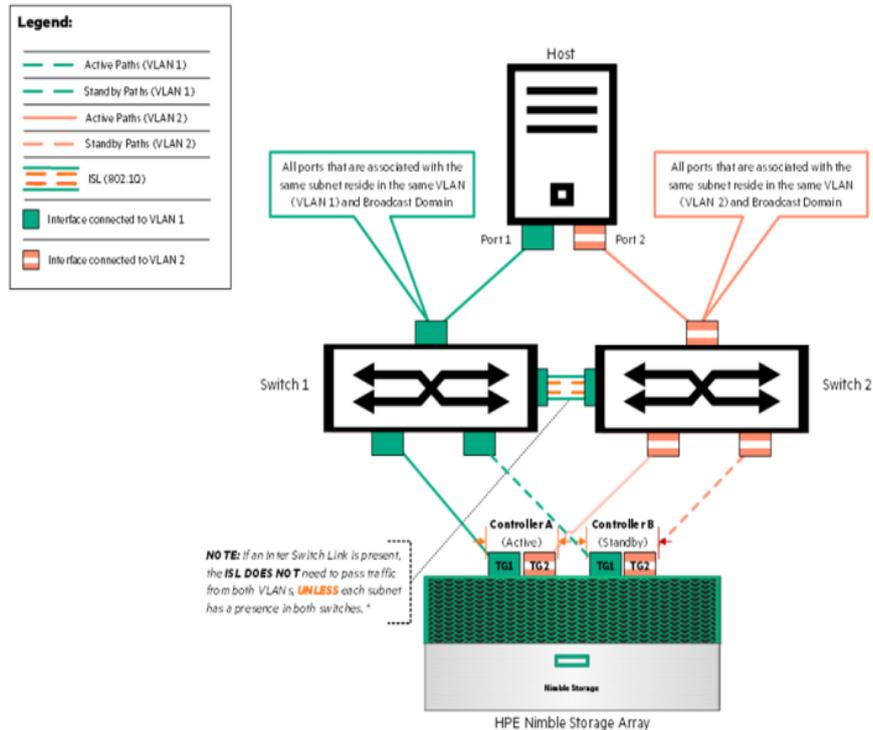


Nota: adaptado de *HPE Nimble Storage Deployment Considerations for Networking* (p.16), por HPE, 2021, https://infosight.hpe.com/InfoSight/media/cms/active/public/HPE_Nimble_Storage_Deployment_Considerations_for_Networking.pdf.

D. Múltiples subredes y *switch*. Este tipo de topología proporciona redundancia a nivel de la infraestructura de la red. Separando el tráfico en múltiples subredes ofrece más ventajas que trabajar una sola subred y varios switches.

Figura 68

Topología subred y switch múltiple



Nota: adaptado de *HPE Nimble Storage Deployment Considerations for Networking* (p.17), por HPE, 2021, https://infosight.hpe.com/InfoSight/media/cms/active/public/HPE_Nimble_Storage_Deployment_Considerations_for_Networking.pdf.

La función de zonas de direccionamiento IP del sistema de almacenamiento HPE Nimble, permite balancear las conexiones iSCSI (subredes distintas) a través de los switch iSCSI y así evitar que sucedan cuellos de botella en los ISL.

2.2.7. Software de respaldo Veeam Backup & Replication

Veeam Backup & Replication es una solución de copias de seguridad, recuperación y gestión de datos líder en el sector que es compatible con todo tipo de cargas de trabajo tanto on premise como *cloud*.

El *software Veeam backup* tiene las siguientes funcionalidades:

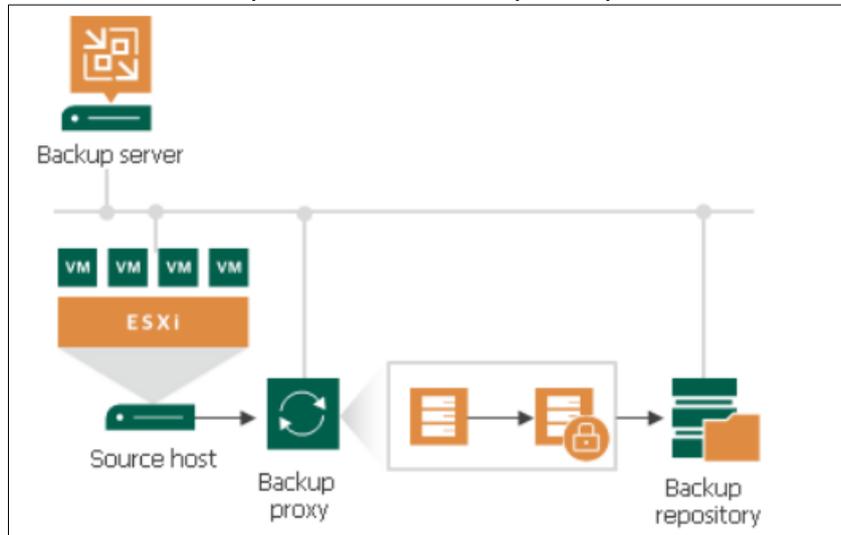
- Tiempos de copias de seguridad cortos y menos costos operativos.
- Recuperación rápida de archivos de máquinas virtuales y archivos a nivel de sistema operativo.
- Portabilidad en nube.

- Permite hacer copias de seguridad en distintos medios (*backup local, backup remoto y cinta*).
- Permite hacer copias de seguridad por la red SAN o LAN.
- Amplia protección: *Automatic backups* integrales en entornos de nube, virtuales, físicos y NAS.
- Recuperación instantánea: permite hacer una recuperación instantánea desde un *backup*, permitiendo la disponibilidad del servicio en el menor tiempo posible.
- Agentes integrados en la nube: *Backup* y recuperación centralizados de AWS, *Microsoft Azure* y *Google Cloud*.
- Los datos se mantienen seguros: Inmutabilidad de extremo a extremo para sus *backups* en cualquier lugar, desde el centro de datos hasta la nube.
- Escaneos de *backups* automáticos: Permite configurar tareas de escaneos de *backups* para detectar la presencia de algún *malware*.
- Restaure en cualquier lugar: Permite la restauración del *backup* en distintas plataformas *on premise* o *cloud*.
- Recuperación confiable: Permite hacer pruebas de restauración de *backups* y replicas en entornos aislados, para garantizar la restauración en caso suceda alguna catástrofe.
- Permite hacer respaldo consistente y restauraciones granulares de las siguientes aplicaciones: *Microsoft SQL Server, Microsoft Active Directory, Microsoft Exchange, Oracle, Microsoft Sharepoint* y *PostgreSQL*.

El software de *backup* tiene los siguientes componentes (figura 69):

Figura 69

Arquitectura de software de respaldo Veeam Backup & Replication



Nota: adaptado de *Veeam Backup & Replication, User Guide for VMware Vsphere* (p.595), por Veeam Software, Setiembre 2023, https://www.veeam.com/veeam_backup_12_user_guide_vsphere_pg.pdf.

A. Veeam backup Server. Es la consola de administración y gestión de tareas de respaldo, tareas de réplica, procesos de restauración, *backup* de la configuración, etc.

B. Backup proxy Veeam. Es el encargado de procesar las tareas de respaldo o replica. Tiene como funciones: retribuir la *data* del *storage* de producción, compresión, deduplicación, encriptación y envío de respaldos a un repositorio.

C. Backup repositorio. Es el almacenamiento donde se guardar los respaldos.

Capítulo III. Desarrollo de trabajo de investigación

En este capítulo se describen todos los procedimientos realizados para el dimensionamiento e implementación de un sistema de almacenamiento en alta disponibilidad. Empezando desde el dimensionamiento de la solución, selección de la solución a implementar, puerto a punto de la solución, pruebas de testeo de la solución y validación de la solución.

3.1. Descripción de la ubicación y características generales de la solución actual

El *datacenter* de la empresa Agrícola Challapampa S.A.C. se encuentra dentro de la planta de procesamiento ubicado a la altura del Km.280 de la carretera Panamericana Sur, distrito de Salas, provincia de Ica, región Ica.

Los equipos que forman parte de la infraestructura tecnológica son los siguientes:

- 4 servidores físicos HPe DL380 Gen 10 con 2 procesadores Intel Xeon Gold 6130 2.1 GHz de 32 *cores*, 384 GB RAM, 2 Discos de 600 GB de 10krpm y 2 puertos de red de 10Gbps
- 1 sistema de almacenamiento *Wester Digital Tegile 4600* de 7.7 TiB (obsoleto)
- 1 sistema de almacenamiento NAS Synology RP3617 RPXs de 20 TB (obsoleto)
- 2 switch HP Flex Fabric 5940 de 48 puertos de 10GbE SFP+

De los equipos descritos, los dos sistemas de almacenamiento se encuentran obsoletos y empezaron a presentar cortes de servicio, poniendo en riesgo la información que reside en ellos.

Los *softwares* empleados en la presente infraestructura son los siguientes:

- *Hypervisor* con *VMware vSphere ESXi 6.7 u3*
- Servidores virtuales con *Windows server* y *Linux*
- *Windows Server Standard 2019*
- *VMware vSphere Enterprise Plus (8 sockets)*

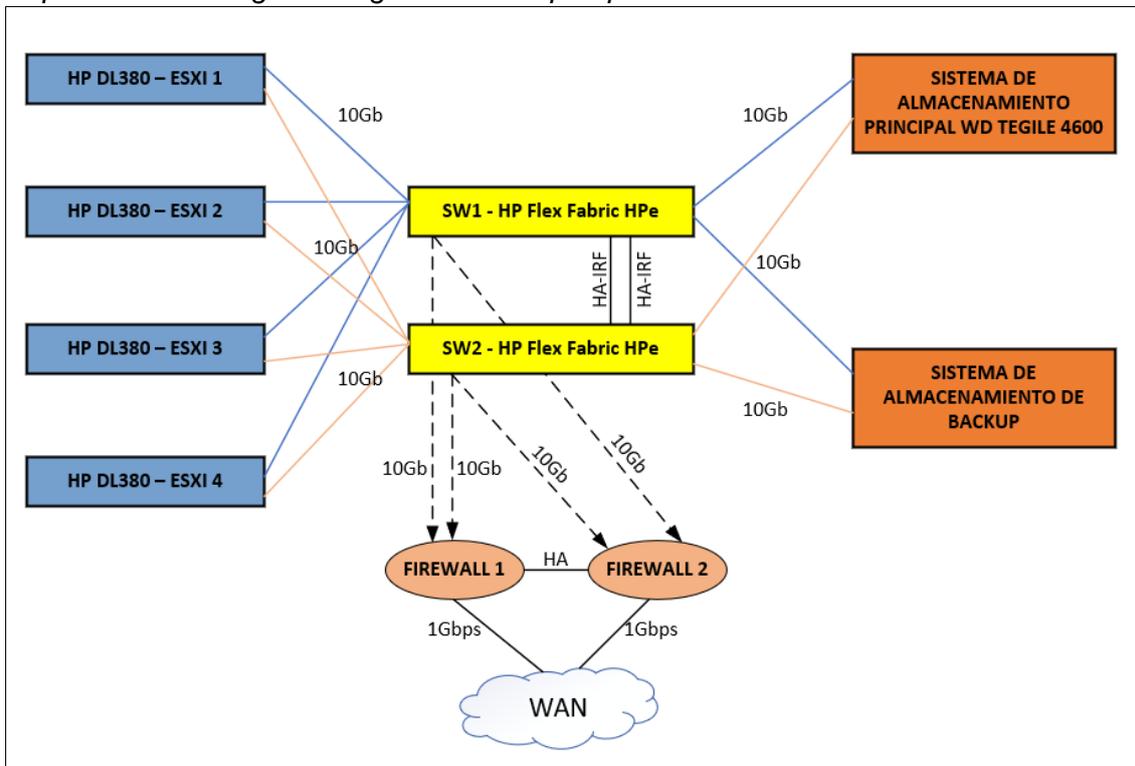
- VMware vcenter server standard (1 instancia)
- Veeam Backup Enterprise plus. (8 sockets)

3.1.1. Diagrama esquemático de la arquitectura IT actual

El diagrama de la arquitectura IT existente se describe en la figura 70.

Figura 70

Arquitectura IT antigua de Agrícola Challapampa S.A.C.



A continuación, describimos las siguientes configuraciones de los componentes de la solución:

- Los dos switches HPe Flex Fabric 5940 se encuentran configurados en una estructura IRF (Intelligent Resilient Framework), la cual brinda alta disponibilidad, escalabilidad y capacidad de administración.
- Los 4 servidores físicos tienen el hypervisor VMware vSphere ESXi 6.7 U3 y cada uno de ellos está instalado sobre un arreglo RAID1 en dos discos duros locales de tipo SAS con 600GB de capacidad

- Los 4 servidores HPe con *VMware vSphere ESXi*, el sistema de almacenamiento principal (*WD Tegile*) y el sistema de almacenamiento de *backup* tienen conectividad a los 2 switches HP *Flex Fabric* con cables DAC de 10Gb.
- En el sistema de almacenamiento principal se configuraron 2 discos lógicos para asignar a los 4 servidores con *VMware vSphere ESXi*.
- Los servidores virtuales residen sobre los discos lógicos presentados del sistema de almacenamiento principal NAS.

La relación de VLAN existentes en la infraestructura se detalla en la tabla 6:

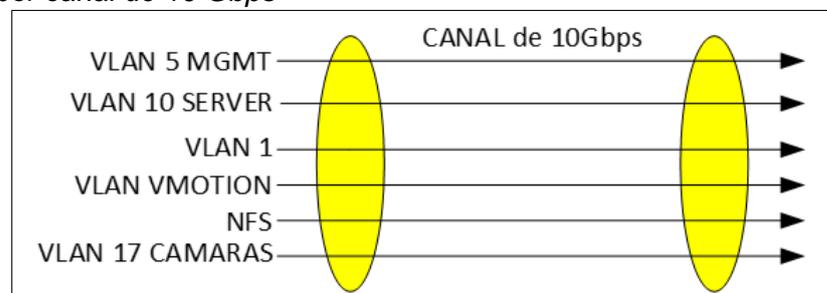
Tabla 6
Listado de VLANs

ID VLAN	Descripción
5	Administración de Equipos
10	Servidores
1	Defecto
8	VMware vMotion
6	NFS
17	Cámaras

- Cada servidor de *VMware ESXi* tiene una tarjeta *PCIe dual port* de 10Gb *Ethernet*, y por un puerto de red se transmite el tráfico LAN, NAS y cámaras (ver figura 71).

Figura 71

Tráfico antiguo por canal de 10 Gbps



3.2. Dimensionamiento de la solución

La infraestructura TI de la empresa Agrícola Challapampa S.A.C. tiene la siguiente relación de servidores físicos y virtuales:

Tabla 7*Listado de servidores virtuales*

Hostname	IP	VCPU	MEMORIA (GB)	DISCO (GB)
SRVICDCPRI	10.13.10.10	4	12	150
SRVICDCSEC	10.13.10.11	2	12	150
SRVICNISTAREO	10.13.10.13	4	8	200
SRVICPRINT	10.13.10.30	6	16	120
SRVICNISPACK-QA	10.13.10.14	4	8	200
SRVICNISWEB	10.13.10.15	4	10	100
SRVICFS	10.13.10.16	2	8	2148
SRVICADCONNECT	10.13.10.23	2	8	100
SRVIHELPDESK-QA	10.13.10.24	2	12	150
SRVICRDS	10.13.10.25	14	36	350
SRVICRDG	10.13.10.26	4	8	100
SRVICMAMUT	10.13.10.28	4	16	1280
SRVICVEEAM	10.13.10.29	6	20	350
SRVICAPPS	10.13.10.31	6	24	200
SRVICAPPS2	10.13.10.21	4	8	100
SRVICNISCAMPO	10.13.10.32	2	8	150
SRVICNISAPPPROD	10.13.10.33	4	12	100
SRVICHELPDESPK	10.13.10.80	2	16	250
SRVICILOAMP	10.13.10.35	4	8	100
SRVICPLANIF	10.13.10.36	4	8	100
SRVICAPPWEB1	10.13.10.37	2	8	100
SRVICAPPWEB2	10.13.10.38	4	8	100
SRVICRDS2	10.13.10.39	4	8	100
SRVICMILESTONE	10.13.17.5	18	24	100
SRVICVCENTER	10.13.5.10	4	16	586
SRVICNISIRA	172.16.105.20	10	96	2348
SRVICAGRO	172.16.105.23	8	32	2048
SRVICINV	10.13.10.51	2	4	100
SRVICWEBCONSULTA	10.13.10.50	2	4	100
SRVICPARECORD	10.13.17.8	10	16	100
SRVICAPPCERT	10.13.10.52	2	4	100
HP – Observer	10.13.10.100	2	8	12
SRVICAPPS3	10.13.10.53	2	4	100
SRVICHELPDESK-test	Serv. Apagado	2	12	150
SRVICRFID	10.13.10.55	2	8	100
SRVICWSUS	Serv. Apagado	2	8	600

3.2.1. Cálculo del espacio de almacenamiento requerido para la solución

Para poder dimensionar el espacio mínimo necesario que debiera soportar los dos sistemas de almacenamiento se debe considerar los siguientes criterios:

- En el caso del sistema de almacenamiento principal se debe considerar el espacio provisionado total más el crecimiento anual (% del espacio total).
- En el caso del sistema de almacenamiento de *backup* se debe considerar el espacio ocupado aprox. según la política de retención de la empresa.

A. Cálculo del espacio del sistema de almacenamiento principal. De la tabla 7 se calcula el espacio total provisionado.

$$C_A = 13142 \text{ GB} \approx 12.83 \text{ TB.}$$

La empresa Agrícola Challapampa S.A.C. estima crecimiento anual de 5% a lo largo de 4 años.

Capacidad mínima requerida del sistema de almacenamiento principal es

$$C_M = 12.83 * 1.05 * 1.05 * 1.05 * 1.05 \text{ TB}$$

$$C_M \text{ Aprox} \approx 16 \text{ TB}$$

B. Cálculo del espacio del sistema de almacenamiento de respaldo. Teniendo el espacio mínimo necesario para el sistema de almacenamiento principal, se puede estimar la capacidad mínima aprox. necesaria para soportar la política de retención de los respaldos de la empresa.

Política de retención en disco

- Retención diaria : 90 Días
- Retención mensual : 8 Meses
- Retención anual : 1 Año

Según la tabla 8 se estima el tamaño *full backup* (50% de 16TB) y 200GB de incremental diario para el total de servidores virtuales:

Tabla 8*Tamaño de backups*

Capacidad	GB	TB
Tamaño Total	16384	16
Full Backup	8192	8
Incremental	200	0.1953

En base a la tabla 8, se estima el espacio full e incremental asumiendo la cantidad total asignada por los servidores virtuales. Se debe tener en cuenta que el tamaño del *backup full* va a depender del espacio real ocupado en cada servidor virtual y el incremental, de los cambios diarios a nivel de bloque.

En la tabla 9, se estima el espacio ocupado en disco según el tiempo de retención de 1 semana, 1 mes, 2 meses y 3 meses.

Se debe tener en cuenta que los *backups* diarios con el software Veeam *backup* se configura con full semanal para que la cadena de incrementales no crezca de manera considerable, es decir, una semana tendrá 1 *backup full* y 6 incrementales. Esto se da por el motivo de acortar el tiempo del proceso de restauración y minimizar el riesgo de pérdida de datos cuando un *backup* se corrompe.

Tabla 9*Espacio de backups según periodo de retención*

Periodo	1 Semana	1 Mes	2 Meses	3 Meses
Tamaño total de backup en disco (TB)	8	32	64	96
Tamaño total de Incrementales (TB)	1.1718	4.6872	9.3744	14.0616
Tamaño total (TB)	9.1718	36.6872	73.3744	110.0616

En el caso de retención mensual piden 8 meses, la capacidad estimada es de 64 TB.

El espacio ocupado del *backup* anual es de 8 TB.

Para conseguir la capacidad mínima que debe soportar el sistema de almacenamiento de *backup* se debe sumar las 3 cantidades anteriores:

$$C_{\text{APROX.}} = 110.0616 + 64 + 8 \approx 182 \text{ TB}$$

Se tiene dos opciones de sistema de almacenamiento de backup y son los siguientes:

- Sistema de almacenamiento con arreglos raid de discos grandes.
- Sistema de almacenamiento con software deduplicación/compresión. Este sistema viene con *software* especializado capaz de deduplicar y comprimir archivos de *backup* de tal manera que se ahorre espacio en disco duro, y tienen la capacidad de integrarse con los softwares de respaldo.

Entre los dos tipos de sistemas de almacenamiento conviene elegir un sistema de almacenamiento con software especializado para disponer de mayor tiempo de retención en disco, ya que aparte de los respaldos en disco, también se puede almacenar data histórica de file server, *backup* de SQL, respaldo de volúmenes del sistema de almacenamiento, etc.

3.2.2. Cálculo del consumo de IOPS de las máquinas virtuales

Se instaló la herramienta de Liveoptics de DellEMC en un servidor virtual y se vinculó con el vcenter server para que pueda estimar métricas de consumo de recursos de los servidores físicos y servidores virtuales. La herramienta se dejó ejecutando por una semana y se obtuvo los datos de la tabla 10.

Tabla 10
Consumo pico de IOPS de las máquinas virtuales

Máquina virtual	Pico IOPS
SRVICAGRO	1096
HP-Observer	5
SRVICADCONNECT	1102
SRVICAPPCERT	17
SRVICAPPS	3657
SRVICAPPS2	2940
SRVICAPPS3	16
SRVICAPPWEB	905
SRVICAPPWEB2	14
SRVICDCPRI	1166
SRVICDCSEC	1218
SRVICFS	5098
SRVICHELPDESK	696
SRVICHELPDESK-TEST – Servidor Apagado	0
SRVICHPILOAMP	9
SRVICINV	14
SRVICMAMUT	2762
SRVICMILESTONE-r2	3788
SRVICNISAPPPROD	2349
SRVICNISCAMPO	2268
SRVICNISIRA	18565
SRVICNISPACK_QA	2149
SRVICNISTAREO	2367
SRVICNISWEB	1405
SRVICPARECORD	3577
SRVICPLANIF	2684
SRVICPRINT-R2	3747
SRVICRDG	639
SRVICRDS	1919
SRVICRDS2 – Servidor Apagado	0
SRVICRFID	597
SRVICVCENTER2	686
SRVICVEEAM	2106
SRVICWEBCONSULTA	15
SRVICWSUS – Servidor Apagado	0
SRVSERVICEDESK_PROD	225

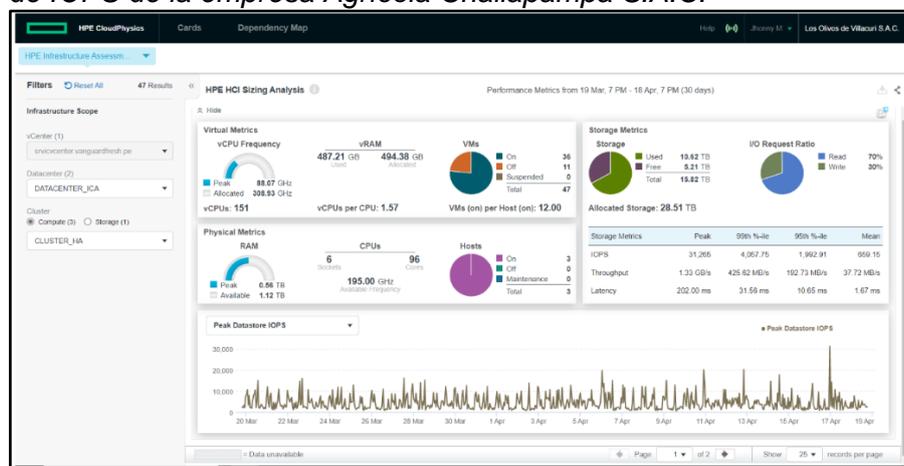
De la tabla 10 se obtiene que el consumo pico de IOPS para el servidor virtual SRVICNISIRA es de 18565 y es un valor referente para poder dimensionar el sistema de almacenamiento principal.

El consumo de IOPS del nuevo sistema de almacenamiento debe ser mayor al valor calculado del servidor SRVICNISIRA, ya que se debe tener en cuenta que el sistema de almacenamiento es compartido para todos los servidores virtuales.

A través de la herramienta cloud de HPe CloudPhysics, se analizó el consumo de IOPS de los servidores virtuales para hacer una comparativa con los datos que ofreció la herramienta de DellEMC.

Figura 72

Consumo de IOPS de la empresa Agrícola Challapampa S.A.C.



De la figura 72, se tiene el pico promedio de IOPS esta alrededor de los 20000, y existe un pico de 31k aprox., pero debe ser por eventos fortuitos de tareas de respaldo, ejecución de planillas, procesos de planta, etc.

En base a las dos herramientas, se puede concluir que el nuevo sistema de almacenamiento debe ofrecer mínimo 19000 IOPS para que no se vea afectado el rendimiento de los servidores virtuales.

3.2.3. Validación de los equipos de comunicaciones existentes

La infraestructura actual tiene 2 switches HPe FlexFabric 5940 48SFP+ 6QSFP+ (número de parte JH395A), el cual tiene las siguientes especificaciones técnicas:

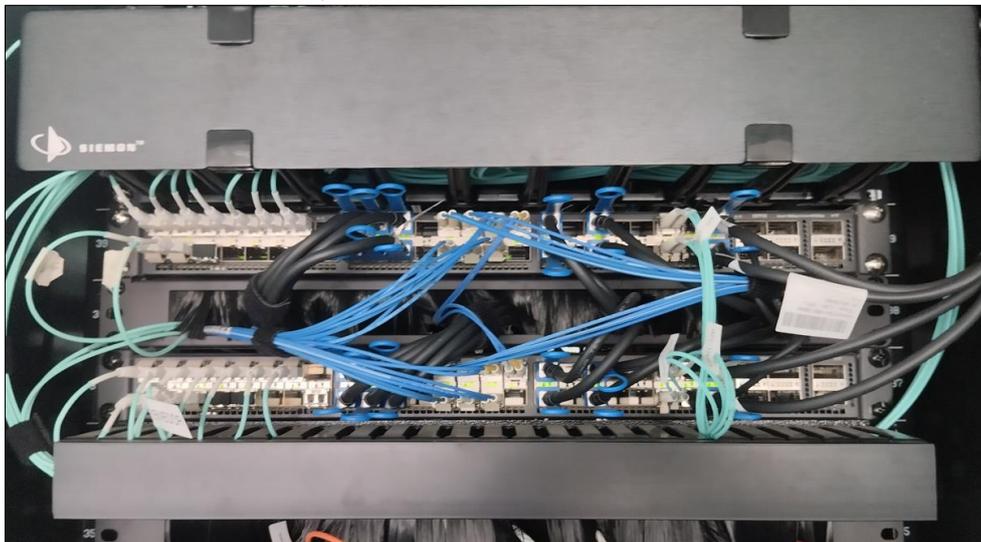
- Soporta 48 puerto SFP+ 10GbE y 6 puertos de 40 Gb

- Ofrece baja latencia (alrededor de 1 μ s por puerto 10GbE)
- Soporta IRF
- Capacidad de *switching* 1440Gbps
- Capacidad de *throughput* hasta 1071 Mpps (millones de paquetes por segundo)
- Soportar *jumbo frames*. El tamaño máximo soportado por puerto es de 10000 bytes
- Soporta configuraciones de VXLAN
- Soporta IEEE 802.3x Flow Control
- Fuentes de poder y ventiladores redundantes

Estos equipos ofrecen un buen rendimiento en toda red, por ello, se elige compartir tráfico LAN y SAN iSCSI. Esta separación de tráfico se realizará con VLANs.

Figura 73

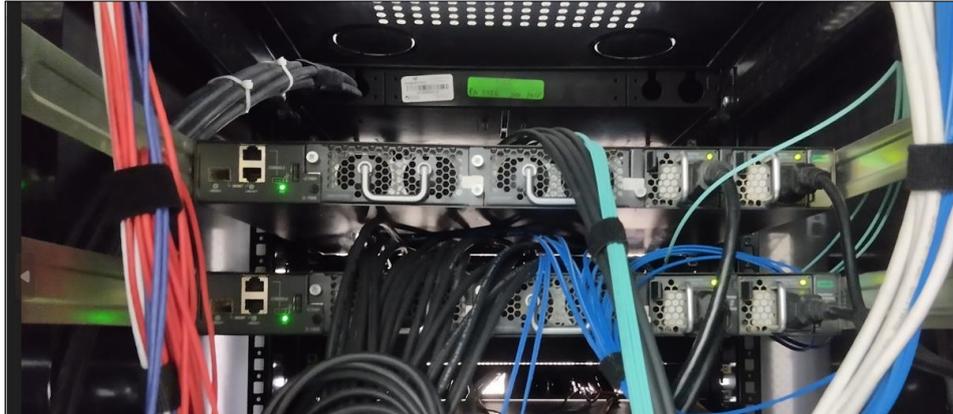
Switches HPe Flex Fabric 5940, vista frontal



En la figura 74, se muestra la parte trasera de los dos switches HPe Flex Fabric 5940.

Figura 74

Switches HPe Flex Fabric 5940, vista trasera



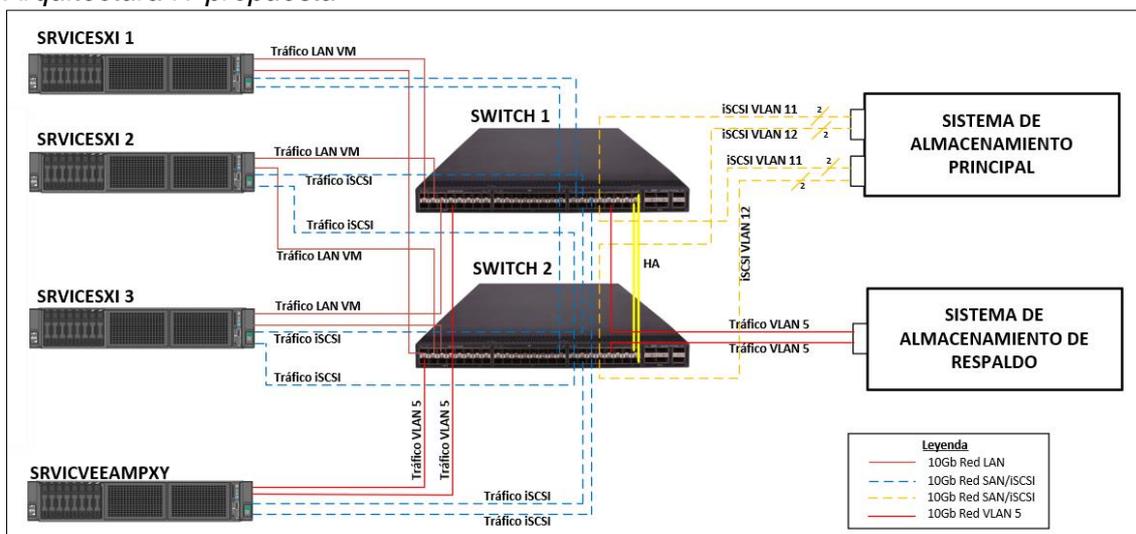
3.2.4. Diseño de la arquitectura IT de la solución

Para el diseño de la arquitectura IT de la solución tomaremos en cuenta el espacio del sistema de almacenamiento principal y de respaldo, así como el cálculo del consumo de IOPS de las máquinas virtuales y la validación de los equipos de comunicaciones existentes.

La figura 75 muestra el diseño de la arquitectura IT del sistema de almacenamiento en alta disponibilidad propuesto para la empresa Agrícola Challapampa S.A.C.

Figura 75

Arquitectura IT propuesta



Con la arquitectura IT propuesta se tendrá los siguientes beneficios:

- *Switches* TOR (Top of Rack) redundantes
- Tráfico LAN y SAN independientes
- Redundancia de puertos tráfico LAN para los servidores con *VMware vSphere ESXi*
- Redundancia de puertos tráfico SAN iSCSI para los servidores con *VMware vSphere ESXi*
- Sistema de almacenamiento principal con controladoras redundantes
- Redundancia de *path* a nivel de tarjetas PCIe en el sistema de almacenamiento principal
- Redundancia de *path* del sistema de almacenamiento de *backup*
- *Backup* por la red dedicada SAN iSCSI para mejorar los tiempos de respaldo

3.2.5. Elaboración de especificaciones técnicas

En base al dimensionamiento realizado y arquitectura IT propuesta se elaboró la tabla 11 y 12, donde se especifica las características técnicas para la solicitud de adquisición de los dos sistemas de almacenamiento.

Tabla 11

Especificaciones técnicas para el sistema de almacenamiento de alta disponibilidad

Característica	Descripción
Cantidad	Una (1)
Factor de forma	Rack
Arquitectura	El sistema de almacenamiento puede híbrido o all flashed (AFA).
Storage Controller o Storage Processor	Controladoras redundantes Puede ser Activo/Activo o Activo/Pasivo.
Fuentes de poder y ventiladores	Redundantes (configuración N+1)
Sistema operativo	El sistema de almacenamiento debe admitir plataformas y agrupaciones de sistemas operativos líderes en la industria, incluidos: Windows Server 2012, Windows Server 2016, VMware, Linux y Unix, etc.
CPU y memoria	Procesador de tecnología Intel Xeon Skylake como mínimo y 12 cores como mínimo por sistema. Incluir mínimo dos memorias espejadas DDR4 NVRAM o NVDIMM.
Caché	El sistema de almacenamiento deberá entregar por lo menos 64 GB de memoria cache nativa por sistema para las operaciones de lectura y escritura. La memoria cache de escritura deberá estar completamente protegida y no se permitirá pérdida de datos en caso falle las fuentes de poder. La cache deberá ser usada únicamente para información y control de Datos.
Discos	Soporte discos SAS, SATA, FLASH.
Capacidad instalada y soportada	El sistema de almacenamiento deberá entregar 16 TB binarios de capacidad efectiva.
IOPS	Cantidad mínima ofertada es de 19000 IOPS
Conectividad HBA	Soporta conectividad Fibre Channel (8/16 Gbps) and iSCSI (10/25 GbE) Los puertos iSCSI pueden ser tipo base-T, SFP+ y fiber channel. La solución ofertada debe venir mínimo con 4 tarjetas dual port de 10GbE fiber channel.
Nivel de protección de discos	El Sistema de Almacenamiento deberá soportar la falla de hasta tres discos en simultaneo sin pérdida de datos.
Integración	Debe soportar vVol, VASA e integración con software de respaldo Veeam backup
Mantenimiento y crecimiento de controladoras	El almacenamiento ofertado deberá permitir crecimientos sin interrupciones a series de almacenamiento de mayor generación dentro de la familia dada sin necesidad de reemplazar todo el equipo

	<p>No deberá de existir tiempo de inactividad mientras se actualiza el almacenamiento al modelo de próxima generación dentro de la serie dada.</p>
Características necesarias	<p>Deduplicación, compresión, snapshot, calidad de servicio.</p> <p>Las actualizaciones de software, firmware, parches/fixes deben ser certificadas y entregadas por el fabricante, considerando todos los componentes de red, cómputo, almacenamiento y virtualización. El proveedor deberá contar con una aplicación de gestión por parte del fabricante que unifique la descarga automática de parches/fixes, así como detalles de parches/fixes soportados y su procedimiento de aplicación. No podrán ser aplicadas actualizaciones y/o parches que no hayan sido pre-validados y liberados por el fabricante.</p>
Replicación	<p>La solución deberá contar con funcionalidades de replicación nativa sin requerir de software de terceros o de hardware adicional, así mismo deberá contar con mecanismos de optimización de la transferencia de datos para minimizar el uso de ancho de banda requerido para replicar.</p>
Cable de poder	<p>HPE C19 – C20 WW 250V 10Amp 3.0m Jumper Cord</p>
Plataforma de gestión y monitoreo	<ul style="list-style-type: none"> • Contar con un panel de control operativo que permita una vista detallada y acceso a hipervínculos de componentes de la infraestructura. • Contar con estadísticas de recursos que permitan vistas detalladas que muestren estadísticas de componentes de infraestructura como CPU, memoria, capacidad de almacenamiento. • Contar con visualizaciones de rendimiento que entreguen gráficos y cronogramas codificados por colores que indican latencia, IOPS de lectura / escritura, rendimiento, uso de capacidad, saturación de rendimiento e impacto potencial del almacenamiento. • Contar con alertas de bienestar (detección basada en reglas) que entregue alertas de bienestar basadas en reglas o umbrales. • Contar con un panel de control ejecutivo que entregue una vista consolidada de todos los componentes del almacenamiento, incluida la eficiencia de la capacidad total, los casos de soporte cerrados automática y manualmente, el estado de protección de datos desglosado por carga de trabajo y/o aplicación y recomendaciones de actualización de hardware. • Debe entregar recomendaciones preventivas para reducir las conjeturas sobre la administración de la infraestructura y la confiabilidad de la aplicación
Garantía y soporte	<p>4 años Soporte 24x7 con tiempo de respuesta de 4 horas El cual deberá ser brindado por el fabricante del hardware ofertado. Monitoreo Permanente de la Infraestructura</p>

Tabla 12

Especificaciones técnicas para el sistema de almacenamiento de respaldo

Característica	Descripción
Cantidad	Un (1) sistema de almacenamiento de respaldo en disco.
Formato	Rack El sistema de almacenamiento debe permitir hacer respaldo y recuperación de información basado en discos duros, mediante un mecanismo de optimización de deduplicación; dicha deduplicación deberá ser en línea, durante la ingesta de datos.
Tipo de disco	Soporte de discos SAS y SATA.
Interfaz De Host	Debe soportar puertos de 1GbE, 10GbE, 10 GbE SFP+, 10GbE-T, 16 Gb FC o 32 Gb FC. El equipo ofertado tiene que venir con 2 puertos de 10GbSFP+ y 4 puertos de 1 GbE.
Cantidad de TB	Capacidad de 170 TB como mínimo
Rendimiento	La librería virtual debe llegar a un rendimiento de escritura de 18TB/hr.
Crecimiento	Debe soportar crecimiento en TB sin deduplicación y compresión. El mismo se debe realizar mediante la adición de nuevos cajones, permitiendo un crecimiento modular de la solución.
Protección	La solución propuesta debe contar con un nivel de protección RAID6. Dicho RAID se deberá realizar a nivel de hardware y no vía software.
Compatibilidad	El dispositivo debe ser compatible con los softwares de backup Microfocus Data Protector, EMC NetWorker, IBM TSM y Veeam Backup.
Deduplicación	La solución propuesta debe incluir la funcionalidad de Deduplicación, el proceso debe correr en la solución y en ninguna circunstancia debe tener agentes o manejadores instalados en los servidores de respaldo o los clientes del Software de respaldo. La deduplicación deberá efectuarse en línea, durante la ingesta de datos. Debiendo estar licenciado para la capacidad de la solución propuesta/ofertada.
Administración	El sistema de almacenamiento debe contar con un software de gestión propio que vía GUI o Web para su administración. Debe tener la capacidad de generar y enviar correos electrónicos o alarmas a una consola de gestión y soporte de SNMP traps. Debe Permitir exportar información de monitoreo, log de errores, etc. hacia "fuera" del dispositivo.
Disponibilidad	El dispositivo debe tener fuentes de poder y ventiladores redundantes, con capacidad de ser reemplazados en caliente.
Soporte De Réplicas	Debe soportar replicación entre dispositivos de la misma familia.

Grabación	<p>Debe contar la capacidad de emular y escribir en formato de tecnologías LTO.</p> <p>Debe soportar los protocolos CIFS y NFS para presentar volúmenes.</p> <p>Debe incluir protocolo de aceleración de respaldo, el cual permita deduplicar el rendimiento de escritura de los datos.</p>
Soporte y garantía	<p>4 años de soporte con nivel de atención 24x7 con un máximo de 4 horas de tiempo de respuesta el cual debe ser brindado por el fabricante del hardware ofertado.</p>
Gestión unificada	<p>Contar con una plataforma de análisis predictivo que brinde inteligencia con capacidad de predecir y prevenir problemas de infraestructura antes de que sucedan, a través de herramientas de predicción inteligentes como machine <i>learning</i> y/o inteligencia artificial.</p> <p>Análisis del equipo conectada globalmente y utilizar estos datos para predecir y evitar problemas.</p> <p>Contar con capacidad de visualizar de forma remota tendencias detalladas de rendimiento, ratios de eficiencia, predicciones de capacidad, controles de estado e información de mejores prácticas.</p>

3.3. Selección de la solución a implementar

En base a las especificaciones técnicas elaboradas, se invitó a participar a dos marcas reconocidas en el mercado: HPe y DellEMC, para que puedan ofrecer soluciones a lo requerido.

En la tabla 13 se muestra el comparativo técnico para la adquisición del sistema de almacenamiento principal.

Tabla 13

Comparación entre sistemas de almacenamiento principal HPe y DellEMC

Características	HPE	DellEMC
	HPE Nimble HF20	Storage DellEMC XT380
Storage Processor	2 controladoras Activo – Stand by	2 controladoras Redundantes: Activo – Activo
IOPS	Desempeño 19K IOPS (50/50)	Desempeño 31 883 IOPS (50/50)
Procesador del storage processor	Procesador Intel Xeon de 6 cores y un total de 12 para todo el sistema.	Cada controladora tiene 1 Procesadores Intel Xeon de 1.7 GHz de 6 cores, en total 12 para todo el sistema.
Memoria del storage processor	No especifica cantidad de memoria RAM, pero tiene NVRAM.	64 GB De memoria RAM por controladora
Disponibilidad	99.9999%	99.999%
Cantidad de discos	2 Discos de 480 SSD y 21x1 TB NLSAS, capacidad aprox. 16 TB. Configuración Triple paridad con spare integrado.	11 TB Aprox. con 2 arreglos (RAID5 4+1) de discos flash de 1.6 TB + 2 hot spare
Puertos iSCSI	4 tarjetas dual port fiber channel de 10GbE.	2 tarjetas dual port <i>fiber channel</i> de 10GbE.
Discos para cache	Dispone de 6 discos de 480 SSD para cache	3 Discos de 400GB <i>Fast Cache</i>
Virtualización del sistema de almacenamiento	Almacenamiento en bloque, vvols	Almacenamiento bloque/archivo/vvols.
Características de software del sistema de almacenamiento	Snapshot, deduplicacion en línea, compresión en línea, think provisioning, clones de copia. Gestión de categorías de aplicaciones para los discos lógicos creados. Ofrece compresión y deduplicacion.	Snapshot, deduplicacion en línea, compresión en línea, think provisioning, clones de copia. Gestión de categorías de aplicaciones para los discos lógicos creados. Ofrece compresión y deduplicacion.
Consola de monitoreo Cloud	Infosight (consola web donde indica las recomendaciones del fabricante sobre los servidores físicos, virtuales y sistema de almacenamiento) y ofrece un monitoreo permanente.	Cloud IQ (Analíticas de storage y buenas prácticas).
Integración con software de virtualización	Integración con vcenter server.	Integración con vcenter server.
Integración con software de respaldo	Integración con Veeam para optimizar los respaldos basados en Snapshots.	Integración con Veeam para optimizar los respaldos basados en Snapshots.

Garantía y soporte	Garantía y soporte proactivo por 4 años.	Garantía y soporte proactivo por 4 años.
Costo USD \$ (No incluye IGV)	\$45,500.00	\$42,526.00

De la tabla 13, se puede concluir que la solución de HPe calza con las especificaciones técnicas solicitadas para el sistema de almacenamiento principal, porque se requiere una solución integral con los equipos existentes, alta disponibilidad, redundancia de componentes, capacidad, monitoreo permanente y que el fabricante brinde recomendaciones para el sistema de almacenamiento y máquinas virtuales.

La figura 76 y 77 son capturas del diseño de la solución ofertada por el fabricante HPe haciendo uso de la herramienta *HPe NinjaStars*.

Figura 76

Diseño de sistema de almacenamiento HPe Nimble HF20

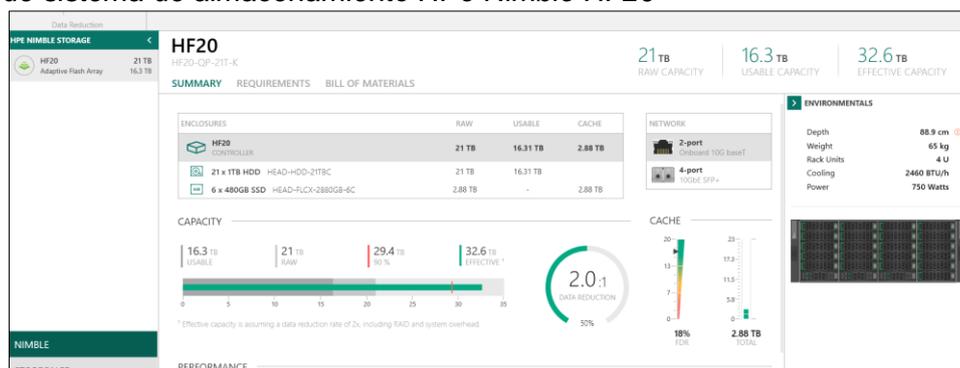
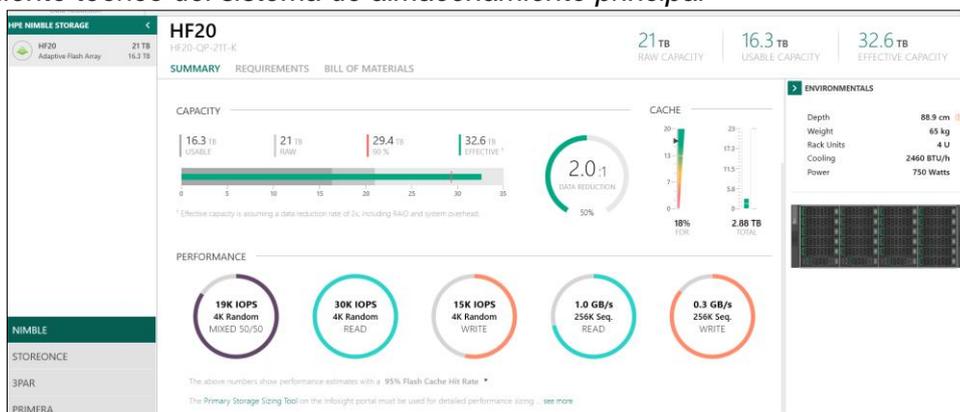


Figura 77

Rendimiento teórico del sistema de almacenamiento principal



La tabla 14 es el comparativo técnico para la adquisición del sistema de almacenamiento de respaldo.

Tabla 14

Comparativo entre sistemas de almacenamiento de respaldo HPE y DellEMC

Características	HPE	DellEMC
	HPe StoreOnce 3640 48 TB	DellEMC PowerProtect 3300 16TB
Formato	Rack Sistema de almacenamiento de respaldo en disco (<i>appliance</i> de respaldo a disco)	Rack Sistema de almacenamiento de respaldo en disco (<i>appliance</i> de respaldo a disco)
Tipo de disco	Soporta SAS	Soporta SAS
Interfaz de host	El equipo viene con 2 puertos de 10GbE fiber channel y 4 puertos de 1GbE	El equipo viene con 2 puertos de 10GbE fiber channel y 4 puertos de 1GbE
Cantidad de TB	El sistema de almacenamiento viene con capacidad de 48 TB RAW y capacidad efectiva de 36 TB.	El sistema de almacenamiento viene con capacidad de 16 TB RAW y capacidad efectiva de 12 TB.
Velocidad de ingesta de datos	Hasta 18.0 TB/h (usando HPe StoreOnce Catalyst).	Hasta 7.0 TB/h (usando DellEmc DD Boost).
Crecimiento	El equipo soporta crecimiento agregando expansiones de caja de discos.	El equipo soporta crecimiento agregando expansiones de caja de discos.
Protección	El sistema de almacenamiento viene con dos discos SAS en RAID1 para el sistema operativo y 12 discos de 4TB NLSAS en RAID6 para almacenar backups.	El sistema de almacenamiento viene con dos discos SAS en RAID1 para el sistema operativo y 8 discos de 2TB NLSAS en RAID6 para almacenar backups.
Compatibilidad	El sistema de almacenamiento es compatible con los softwares de backup Microfocus Data Protector, EMC Networker, IBM TSM y Veeam Backup.	El sistema de almacenamiento es compatible con los softwares de backup Microfocus Data Protector, EMC Networker, IBM TSM y Veeam Backup.
Deduplicación	El sistema de almacenamiento viene con software deduplicacion y trabaja sin agentes. El proceso de deduplicacion lo realiza en línea durante la ingesta de datos.	El sistema de almacenamiento viene con software deduplicacion y trabaja sin agentes. El proceso de deduplicacion lo realiza en línea durante la ingesta de datos.

Administración	El sistema de almacenamiento tiene un software de gestión web o GUI para su administración. Soporta configuración de notificaciones.	El sistema de almacenamiento tiene un software de gestión web o GUI para su administración. Soporta configuración de notificaciones.
Disponibilidad	El sistema de almacenamiento tiene fuentes de poder y ventiladores redundantes, y tienen la capacidad de ser cambiados en caliente.	El sistema de almacenamiento tiene fuentes de poder y ventiladores redundantes, y tienen la capacidad de ser cambiados en caliente.
Grabación	El sistema de almacenamiento soporta emulación de tecnología LTO. Soporta protocolo NFS y CIFS. Incluye protocolo Catalyst para aceleración de copias de respaldo.	El sistema de almacenamiento soporta emulación de tecnología LTO. Soporta protocolo NFS y CIFS. Incluye protocolo DD Boost para aceleración de copias de respaldo.
Soporta y garantía.	Incluye 4 años de soporte 24x7 con un tiempo de atención máxima de 4 horas y el soporte lo brinda el fabricante.	Incluye 4 años de soporte 24x7 con un tiempo de atención máxima de 4 horas y el soporte lo brinda el fabricante.
Gestión unificada	El equipo se integra a la consola cloud HPe Infosight, que permite predecir y prevenir posibles fallas en el equipo a través de la inteligencia artificial y brinda métricas de análisis de rendimiento del equipo.	El equipo se integra a la consola Cloud IQ, que permite predecir y prevenir posibles fallas en el equipo a través de la inteligencia artificial y brinda métricas de análisis de rendimiento del equipo
Costo USD \$ (No incluye IGV)	\$14,120.00	\$15,191.00

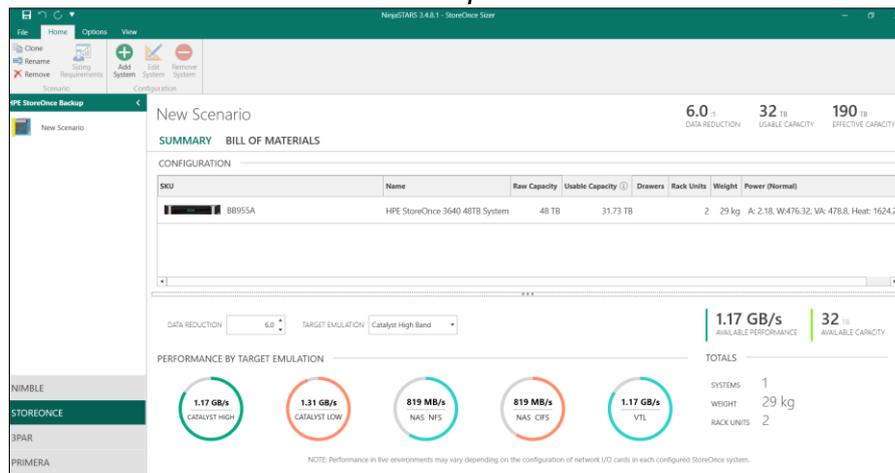
Según la tabla 14, se concluye que la mejor oferta es la solución HPe, ya que ofrece más capacidad en disco, mayor capacidad de ingesta de datos, integración con el hardware existente y el nuevo sistema de almacenamiento principal.

Adquiriendo estos dos sistemas de almacenamiento del mismo fabricante y configurando todo el equipamiento a la consola *cloud* de *infosight*, se podría tener visibilidad de toda la arquitectura de IT. Con ello se tendría una consola unificada donde se vería el estado de salud del equipamiento y recomendaciones sobre las configuraciones existentes.

En la figura 78, se muestra el diseño del sistema de almacenamiento *HPe StoreOnce 3640 48TB* haciendo uso de la herramienta de *HPe NinjaStars*.

Figura 78

Diseño de sistema de almacenamiento de respaldo



3.4. Instalación, implementación, configuración y puesta a punto de la solución

A continuación, se describe el proceso de implementación del sistema de almacenamiento en alta disponibilidad. Para ello, se seguirá el siguiente procedimiento para la puesta en marcha de la solución:

- Instalación física de los sistemas de almacenamiento
- Cableado de red de los sistemas de almacenamiento
- Configuración lógica de los puertos de los *switches* HPe
- Configuración de los servidores ESXi
- Implementación de sistemas de almacenamientos HPe
- Migración de máquinas virtuales
- Implementación y configuración de servidor de respaldo

3.4.1. Instalación física de los sistemas de almacenamiento

La empresa Agrícola Challapampa S.A.C tiene 4 servidores HPe DL380 GEN10 que se encuentran instalados de manera física en el primer gabinete de su *datacenter*. Los nombres para los servidores que usaremos en el presente proyecto se muestran en la figura 79 y 80.

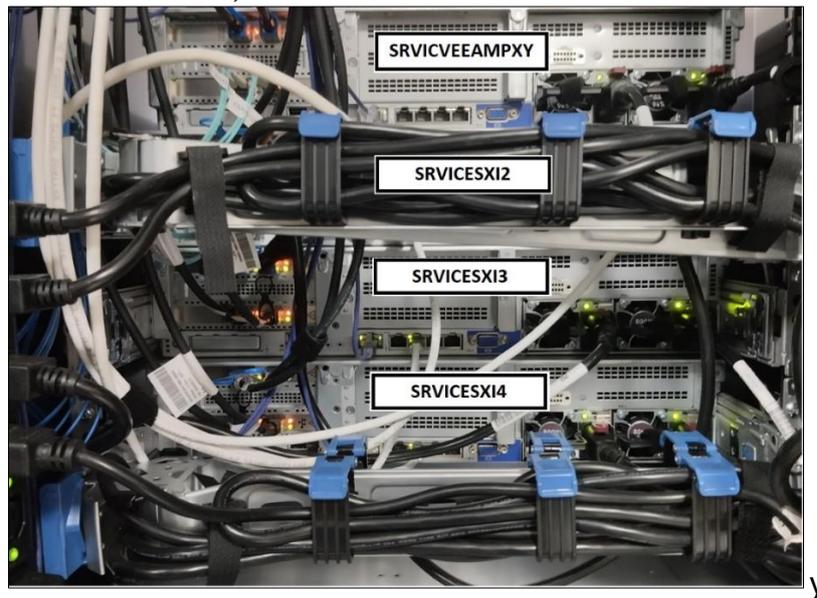
Figura 79

Servidores HPe DL380 Gen 10, vista frontal



Figura 80

Servidores HPe DL380 Gen 10, vista trasera

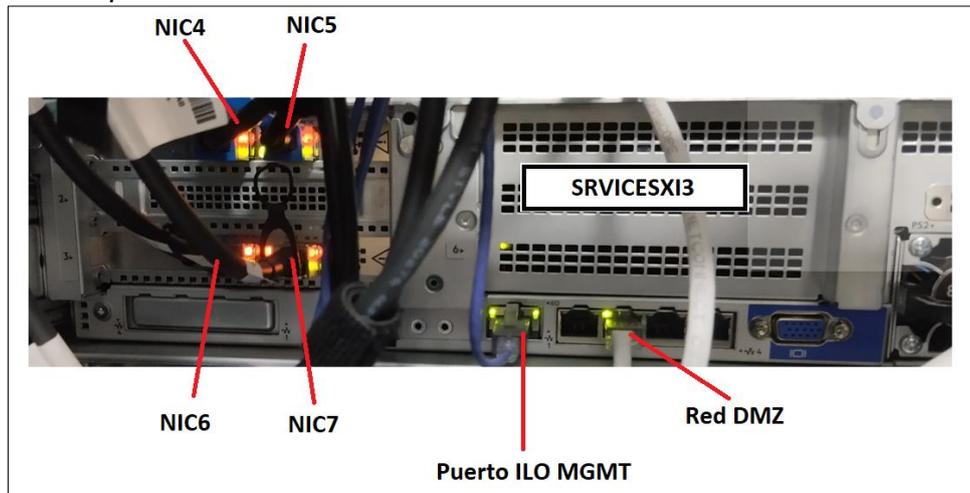


El cableado de las tarjetas *dual port* de 10Gb hacia los switches HPe se realizó con cables DAC SFP+ y *fiber channel* con conector LC-LC OM4.

En la figura 81, se muestra la nomenclatura de puertos del servidor SRVICESX13 y es la misma para todos los servidores físicos:

Figura 81

Descripción de puertos de servidor SRVICESX13



El sistema de almacenamiento Nimble se instaló en el RU 10 -13, tal como se muestra en la figura 82 y 83.

Figura 82

Sistema de almacenamiento Nimble HF20, vista frontal sin tapa



Figura 83

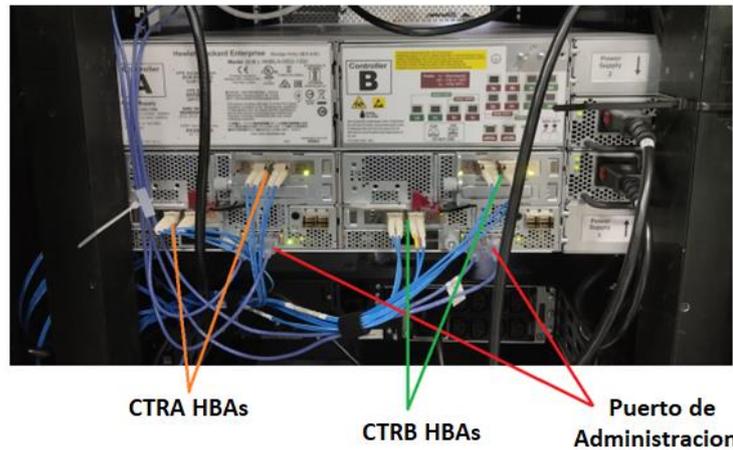
Sistema de almacenamiento Nimble HF20, vista frontal con tapa



En la figura 84, se muestra la parte trasera del sistema de almacenamiento *HPe Nimble HF20* y la descripción de puertos.

Figura 84

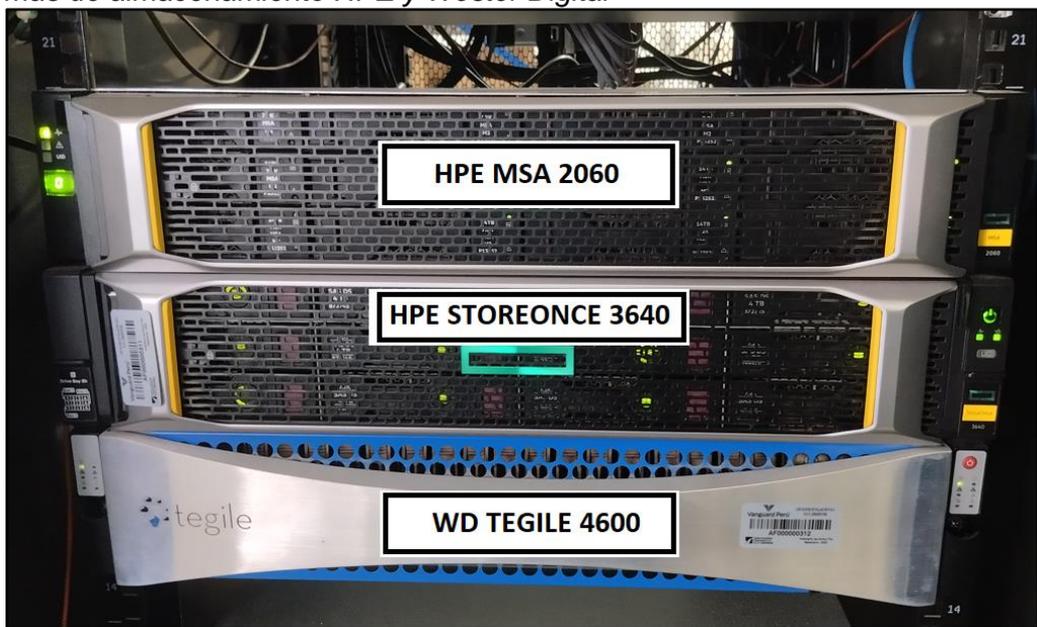
Descripción de puertos del sistema de almacenamiento Nimble



El sistema de almacenamiento *HPe Storeonce* se instaló en el segundo gabinete del *datacenter* y se muestra en la figura 85.

Figura 85

Sistemas de almacenamiento HPE y Wester Digital



En la figura 86, se muestra la parte trasera del sistema de almacenamiento *HPe Storeonce 3640* y se describe los puertos de comunicación.

Figura 86

Descripción de puertos HPe StoreOnce 3640

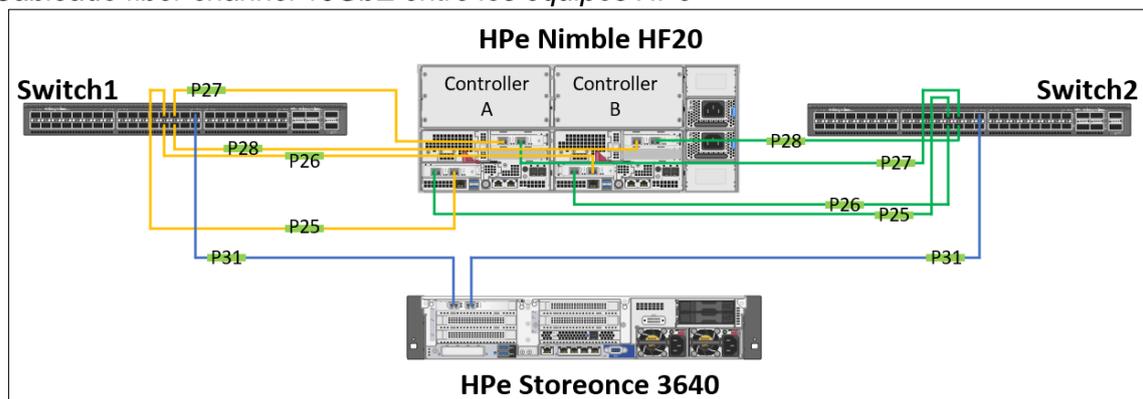


3.4.2. Cableado de red de los sistemas de almacenamiento

El cableado *fiber channel* 10 GbE entre los sistemas de almacenamientos y los *switches* HPe se realizó según la figura 87.

Figura 87

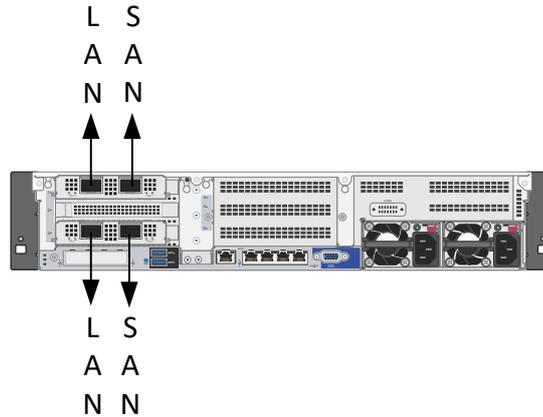
Cableado fiber channel 10GbE entre los equipos HPe



Desde los puertos físicos de cada servidor con *vmware vSphere ESXi* se cableó un puerto de cada tarjeta PCIe a cada switch y se configuró el tráfico según la figura 88, de tal manera que se mantenga la conectividad en caso falle alguna tarjeta PCIe física.

Figura 88

Tráfico LAN y SAN en el servidor HPe DL380 Gen10



3.4.3. Configuración lógica de los puertos físicos de los switches HPe

En este subcapítulo se configuró los puertos físicos de los switches HPe que hacen la arquitectura IT propuesta. Para iniciar la configuración, se establece una conexión por SSH a los switches y se agregó una descripción a cada conexión de los equipos que forman parte de la arquitectura IT de alta disponibilidad al switch para facilitar la configuración lógica de los puertos.

Figura 89

Descripción de puertos Switch HPe 1

```
10.13.5.3 - PuTTY
XGB1/0/13    UP    10G(a)  F(a)  T    1
XGB1/0/14    DOWN auto  A      T    1
XGB1/0/15    DOWN auto  A      T    1
XGB1/0/16    DOWN auto  A      T    1
XGB1/0/17    DOWN auto  A      T    1    PP-Synology-Backups 10.13.5
XGB1/0/18    UP    10G(a)  F(a)  A    17
XGB1/0/19    UP    10G(a)  F(a)  A    11    VEEAM_PROXY_ISCSI_11
XGB1/0/20    UP    10G(a)  F(a)  T    1    SRVICESXI2_NIC5
XGB1/0/21    UP    10G(a)  F(a)  T    1    SRVICESXI3_NIC5
XGB1/0/22    UP    10G(a)  F(a)  T    1    SRVICESXI4_NIC5
XGB1/0/23    DOWN auto  A      A    1
XGB1/0/24    DOWN auto  A      T    1    10.13.5.19/172.16.105.9 ESX
XGB1/0/25    UP    10G(a)  F(a)  A    11    NIMBLE_HBA1
XGB1/0/26    UP    10G(a)  F(a)  A    11    NIMBLE_HBA2
XGB1/0/27    UP    10G(a)  F(a)  A    11    NIMBLE_HBA3
XGB1/0/28    UP    10G(a)  F(a)  A    11    NIMBLE_HBA4
XGB1/0/29    UP    10G(a)  F(a)  A    31    MSA_CTRLA
XGB1/0/30    UP    10G(a)  F(a)  A    31    MSA_CTRLB
XGB1/0/31    UP    10G(a)  F(a)  A    5    HP_STOREONCE
XGB1/0/32    DOWN auto  A      A    1
XGB1/0/33    UP    10G(a)  F(a)  T    1    Sophos XG330 Master A1
XGB1/0/34    UP    10G(a)  F(a)  T    1    Sophos XG330 Slave A1
XGB1/0/35    DOWN auto  A      A    1
XGB1/0/36    DOWN auto  A      A    1
XGB1/0/37    UP    10G(a)  F(a)  T    1
XGB1/0/38    UP    10G(a)  F(a)  T    1    Ten-GigabitEthernet1/0/37 I
XGB1/0/39    DOWN auto  A      A    1
XGB1/0/40    DOWN auto  A      A    1
XGB1/0/41    DOWN auto  A      A    1
XGB1/0/42    DOWN auto  A      T    1
XGB1/0/43    DOWN auto  A      A    5    VEEAM_PROXY_BACKUP_HP_STORE
XGB1/0/44    UP    10G(a)  F(a)  T    1    SRVICESXI2_NIC6
XGB1/0/45    UP    10G(a)  F(a)  T    1    SRVICESXI3_NIC6
XGB1/0/46    UP    10G(a)  F(a)  T    1    SRVICESXI4_NIC6
XGB1/0/47    UP    10G(a)  F(a)  --   --
XGB1/0/48    UP    10G(a)  F(a)  --   --
```

Figura 90

Descripción de puertos Switch HPe 2

```
10.13.5.3 - PuTTY
XGB2/0/15 DOWN auto A T 1
XGB2/0/16 DOWN auto A T 1
XGB2/0/17 DOWN auto A T 1 PP-Synology-Backups 10.13.5
XGB2/0/18 UP 10G(a) F(a) A 17
XGB2/0/19 UP 10G(a) F(a) A 12 VEEAM_PROXY_ISCSI_12
XGB2/0/20 UP 10G(a) F(a) T 1 SRVICESX12_NIC4
XGB2/0/21 UP 10G(a) F(a) T 1 SRVICESX13_NIC4
XGB2/0/22 UP 10G(a) F(a) T 1 SRVICESX14_NIC4
XGB2/0/23 DOWN auto A A 1
XGB2/0/24 DOWN auto A T 1 10.13.5.19/172.16.105.9 ESX
XGB2/0/25 UP 10G(a) F(a) A 12 NIMBLE_CTRL1
XGB2/0/26 UP 10G(a) F(a) A 12 NIMBLE_CTRL2
XGB2/0/27 UP 10G(a) F(a) A 12 NIMBLE_CTRL3
XGB2/0/28 UP 10G(a) F(a) A 12 NIMBLE_CTRL4
XGB2/0/29 UP 10G(a) F(a) A 32 MSA_CTRLA
XGB2/0/30 UP 10G(a) F(a) A 32 MSA_CTRLB
XGB2/0/31 UP 10G(a) F(a) A 5 HP_STOREONCE
XGB2/0/32 DOWN auto A A 1
XGB2/0/33 UP 10G(a) F(a) T 1 Sophos XG330 Master A2
XGB2/0/34 UP 10G(a) F(a) T 1 Sophos XG330 Slave A2
XGB2/0/35 DOWN auto A A 1
XGB2/0/36 DOWN auto A A 1
XGB2/0/37 UP 10G(a) F(a) T 1
XGB2/0/38 UP 10G(a) F(a) T 1 Ten-GigabitEthernet2/0/37 I
XGB2/0/39 DOWN auto A A 1
XGB2/0/40 DOWN auto A A 1
XGB2/0/41 DOWN auto A A 1
XGB2/0/42 DOWN auto A A 1
XGB2/0/43 UP 10G(a) F(a) A 5 VEEAM_PROXY_BACKUP_HP_STORE
XGB2/0/44 UP 10G(a) F(a) T 1 SRVICESX12_NIC7
XGB2/0/45 UP 10G(a) F(a) T 1 SRVICESX13_NIC7
XGB2/0/46 UP 10G(a) F(a) T 1 SRVICESX14_NIC7
XGB2/0/47 UP 10G(a) F(a) -- --
XGB2/0/48 UP 10G(a) F(a) -- --

[Ica-5940]
[Ica-5940]
[Ica-5940]
```

La tabla 15 describe la configuración que se aplicó a cada puerto en los switches HPe según el siguiente detalle: ID de puerto, descripción o nomenclatura, tipo de puerto y que VLAN(s) se transmiten.

Tabla 15*Configuración de puertos físicos en los switches HPe*

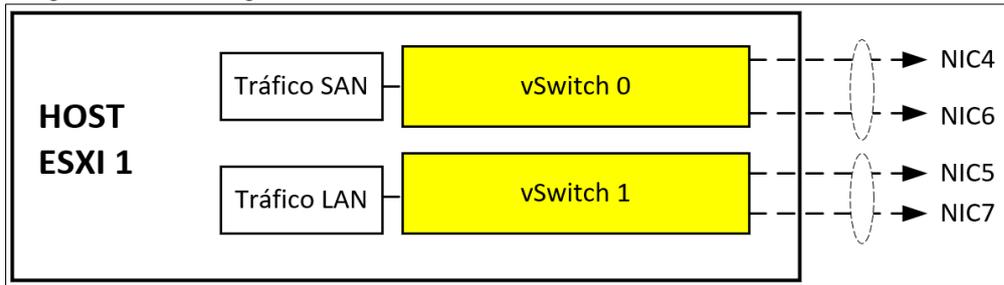
ID de Puerto	Descripción de puerto	Tipo de puerto	VLAN(s)
XGE1/0/19	VEEAM PROXY (Backup for SAN)	Acceso	11
XGE1/0/20	SRVICESXI2_NIC5	Troncal	6,8,11,12,31,32
XGE1/0/21	SRVICESXI3_NIC5	Troncal	6,8,11,12,31,32
XGE1/0/22	SRVICESXI4_NIC5	Troncal	6,8,11,12,31,32
XGE1/0/25	NIMBLE_HBA1	Acceso	11
XGE1/0/26	NIMBLE_HBA2	Acceso	11
XGE1/0/27	NIMBLE_HBA3	Acceso	11
XGE1/0/28	NIMBLE_HBA4	Acceso	11
XGE1/0/31	HPE STOREONCE	Acceso	5
XGE1/0/43	VEEAM PROXY LAN	Acceso	5
XGE1/0/44	SRVICESXI2_NIC6	Troncal	1,5,10,17
XGE1/0/45	SRVICESXI3_NIC6	Troncal	1,5,10,17
XGE1/0/46	SRVICESXI4_NIC6	Troncal	1,5,10,17
XGE2/0/19	VEEAM PROXY (Backup for SAN)	Acceso	12
XGE2/0/20	SRVICESXI2_NIC4	Troncal	1,5,10,17
XGE2/0/21	SRVICESXI3_NIC4	Troncal	1,5,10,17
XGE2/0/22	SRVICESXI4_NIC4	Troncal	1,5,10,17
XGE2/0/25	NIMBLE_HBA1	Acceso	12
XGE2/0/26	NIMBLE_HBA2	Acceso	12
XGE2/0/27	NIMBLE_HBA3	Acceso	12
XGE2/0/28	NIMBLE_HBA4	Acceso	12
XGE2/0/31	HPE STOREONCE	Acceso	5
XGE2/0/43	VEEAM PROXY LAN	Acceso	5
XGE2/0/44	SRVICESXI2_NIC7	Troncal	6,8,11,12,31,32
XGE2/0/45	SRVICESXI3_NIC7	Troncal	6,8,11,12,31,32
XGE2/0/46	SRVICESXI4_NIC7	Troncal	6,8,11,12,31,32

3.4.4. Configuración lógica de los servidores ESXi

En cada servidor ESXi se creó dos virtual switch y se configuró las tarjetas de red físicas según la figura 91. Esta configuración se da con el fin de mantener la alta disponibilidad en caso alguna tarjeta PCIe falle, y se separe el tráfico LAN y SAN.

Figura 91

Diagrama de configuración de los vSwitch en el host ESXi 2



La nueva distribución de VLAN quedó según la figura 92 y 93.

Figura 92

VLAN que pasan por la troncal NIC4

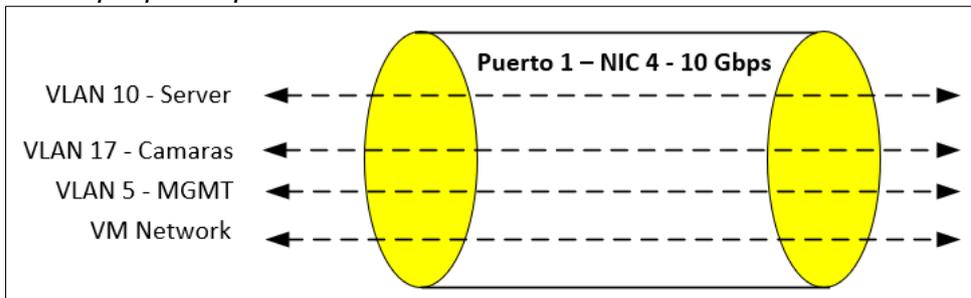
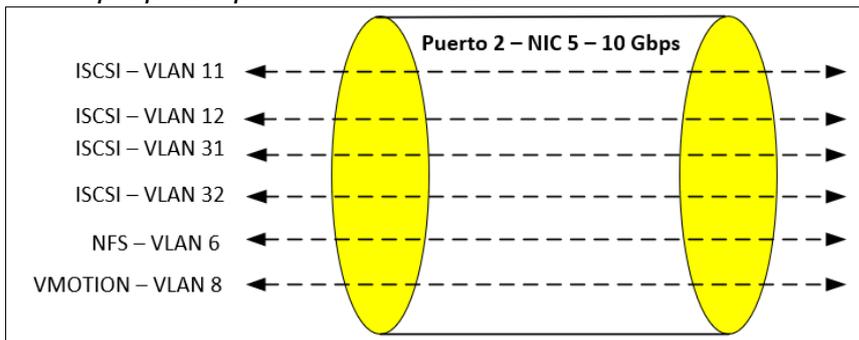


Figura 93

VLAN que pasan por la troncal NIC5



Los virtual switch para el servidor SRVICESXI2 quedó según la figura 94 y 95.

Figura 94

Grupo de puertos en vSwitch1 en ESXi2

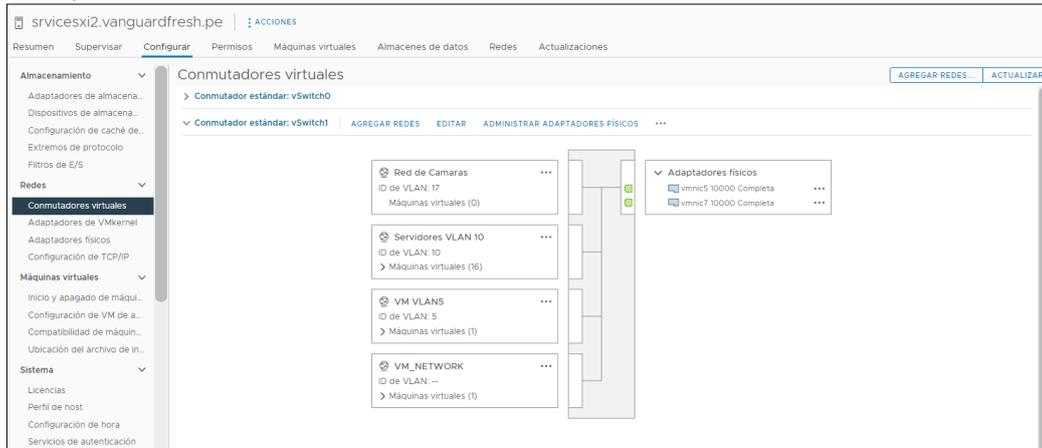
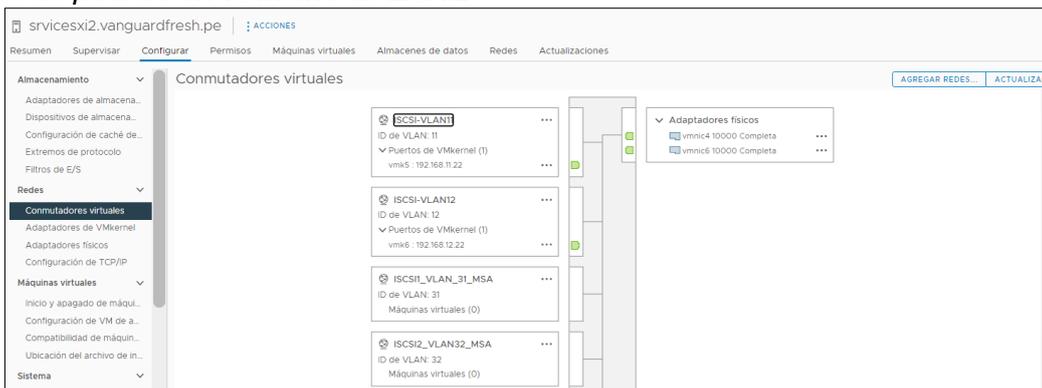


Figura 95

Grupo de puertos en vSwitch1 en ESXi2



En cada servidor ESXi se configuro se creó las agrupaciones de puerto ISCSI-VLAN11 y ISCSI-VLAN12, y dirección IP de *VMkernel* para que puedan tener conectividad a la subred iSCSI. El detalle de configuración se muestra en la tabla 16.

Tabla 16*Configuración de puertos VMkernel de cada servidor ESXi*

Servidor	Grupo de Puertos	VLAN	Dirección IP de VMkernel	Tarjetas de red
SRVICESXI2	ISCSI-VLAN11	VLAN 11	192.168.11.22 / 24	VMNIC 4 - ACTIVO
	ISCSI-VLAN11			VMNIC 6 - STAND BY
SRVICESXI2	ISCSI-VLAN12	VLAN 12	192.168.12.22 / 24	VMNIC 4 - STAND BY
	ISCSI-VLAN12			VMNIC 6 - ACTIVO
SRVICESXI3	ISCSI-VLAN11	VLAN 11	192.168.11.23 / 24	VMNIC 4 - ACTIVO
	ISCSI-VLAN11			VMNIC 6 - STAND BY
SRVICESXI3	ISCSI-VLAN12	VLAN 12	192.168.12.23 / 24	VMNIC 4 - STAND BY
	ISCSI-VLAN12			VMNIC 6 – ACTIVO
SRVICESXI4	ISCSI-VLAN11	VLAN 11	192.168.11.24 / 24	VMNIC 4 – ACTIVO
	ISCSI-VLAN11			VMNIC 6 - STAND BY
SRVICESXI4	ISCSI-VLAN12	VLAN 12	192.168.12.24 / 24	VMNIC 4 - STAND BY
	ISCSI-VLAN12			VMNIC 6 – ACTIVO

Se habilitó el *iSCSI software adapter* en cada servidor ESXi y se configuró los *iSCSI initiator* según la tabla 17.

Tabla 17*iSCSI initiator de cada servidor ESXi*

Servidor	ISCSI initiator	Servidor iSCSI - Nimble HF20
SRVICESXI2	iqn.1998-01.com.vmware:svicesxi2-4924d056	192.168.11.10:3260
		192.168.12.10:3260
SRVICESXI3	iqn.1998-01.com.vmware:svicesxi3-74b7e9db	192.168.11.10:3260
		192.168.12.10:3260
SRVICESXI4	iqn.1998-01.com.vmware:svicesxi4-72415000	192.168.11.10:3260
		192.168.12.10:3260

En cada servidor *ESXi*, se configuró los *VMkernel* para que soporten tráfico *iSCSI* y se incrementó el *jumbo frames* de 1500 a 9000.

Con la configuración realizada, los *iSCSI initiator* de cada servidor *ESXi* se va a poder visualizar en el sistema de almacenamiento *Nimble*.

Posterior a esa labor, se actualizó la versión de *VMware vSphere ESXi* de la versión 6.7U3 a la versión 7 U3 de los tres servidores: SRVICESXI2, SRVICESXI3 y SRVICESXI4, porque la versión actual ya no tenía soporte con el fabricante.

Las nuevas versiones se muestran en las figuras 96, 97 y 98.

Figura 96

Servidor SRVICESXI2



Figura 97

Servidor SRVICESXI3



Figura 98

Servidor SRVICESXI4



3.4.5. Implementación y configuración de los sistemas de almacenamiento

A continuación se describe el procedimiento de implementación y configuración de los dos sistemas de almacenamiento HPe.

- Sistema de almacenamiento principal *HPe Nimble HF20*
- Sistema de almacenamiento de respaldo *HPe StoreOnce 3640*

A. Implementación y configuración de sistema de almacenamiento principal.

Se enciende el sistema de almacenamiento principal HPe Nimble HF20 y se aplica las siguientes direcciones IP para el sistema:

- IP Flotante : 10.13.5.141 / 255.255.255.0 /10.13.5.1
- IP Controladora A : 10.13.5.142 / 255.255.255.0 /10.13.5.1
- IP Controladora B : 10.13.5.143 / 255.255.255.0 /10.13.5.1

Donde, la IP flotante es una IP virtual que permite la alta disponibilidad de las dos controladoras.

Las redes iSCSI con las que va a trabajar los nuevos sistemas de almacenamiento son las siguientes:

- ISCSI1 VLAN 11 : subnet1 192.168.11.0
- ISCSI2 VLAN 12 : subnet2 192.168.12.0

Los puertos de las tarjetas PCIe de ambas controladoras se configuró con las siguientes direcciones IP:

- Tg1a VLAN11 192.168.11.12 / 255.255.255.0
- Tg1b VLAN12 192.168.12.12 / 255.255.255.0
- Tg3a VLAN11 192.168.11.13 / 255.255.255.0
- Tg3b VLAN12 192.168.12.13 / 255.255.255.0

Figura 99

Configuración de tarjetas de red HPe Nimble HF20

INTERFACE	ARRAY NAME	LINK STATUS	SUBNET LABEL	DATA IP ADDRESS	UNCONFIGURED	VLAN ID	TAGGED
eth0a	nimblevanguardfresh	🟢🟢	management				
eth0b	nimblevanguardfresh	🟢🟢	management				
tg1a	nimblevanguardfresh	🟢🟢	Subnet-1	192.168.11.12			
tg1b	nimblevanguardfresh	🟢🟢	Subnet-2	192.168.12.12			
tg3a	nimblevanguardfresh	🟢🟢	Subnet-1	192.168.11.13			
tg3b	nimblevanguardfresh	🟢🟢	Subnet-2	192.168.12.13			

Con los 21 discos existentes se configuró un arreglo RAID de triple paridad y nos brindó una capacidad efectiva de 14.83 TiB.

Figura 100

Capacidad efectiva del sistema de almacenamiento Nimble HF20

Array: nimblevanguardfresh
TOTAL USAGE: 4.96 TiB of 14.83 TiB

FRONT PANEL: HDD: 14.8 TB Usable (19.1 TB / 21 TB Raw) | CACHE: 2.6 TB Usable (2.6 TB / 2.9 TB Raw)

HDD	21	HDD	22	HDD	23	HDD	24
HDD	17	HDD	18	HDD	19	HDD	20
HDD	13	HDD	14	HDD	15	HDD	16
HDD	9	HDD	10	HDD	11	HDD	12
HDD	5	HDD	6	HDD	7	HDD	8
SSD	1 A	SSD	2 A	SSD	3 A	HDD	4
	1 B		2 B		3 B		

En la consola web del sistema de almacenamiento Nimble se crea los servidores host con cada *iSCSI* iniciator de cada servidor ESXi.

Figura 101

Host SRVICESXI2.VANGUARDFRESH.PE

Initiator Group: SRVICESXI2.VANGUARDFRESH.PE

Connections: 84 | Initiators: 2 | Volumes: 6

NAME	IQN	IP ADDRESS
ISCSI-1-ESXI2	iqn.1998-01.com.vmware.servicesxi2-49244056	192.168.11.22
ISCSI-2-ESXI2	iqn.1998-01.com.vmware.servicesxi2-49244056	192.168.12.22

Figura 102

Host SRVICESXI3.VANGUARDFRESH.PE

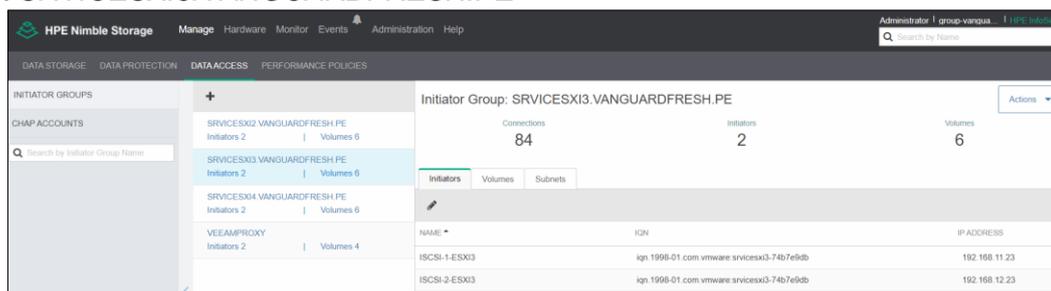
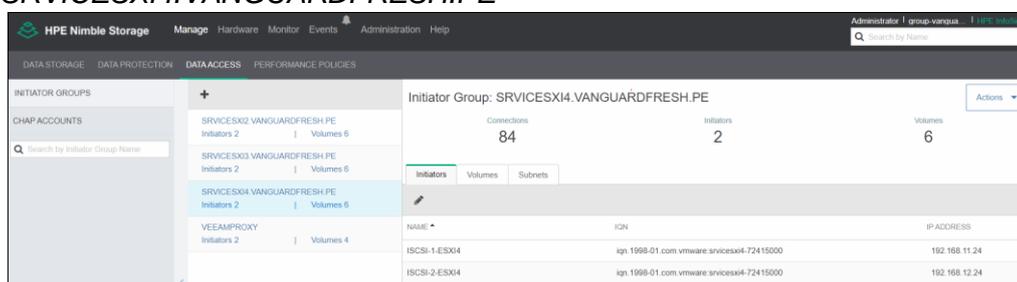


Figura 103

Host SRVICESXI4.VANGUARDFRESH.PE



En el sistema de almacenamiento principal se creó 3 discos lógicos y se asignó a cada servidor físico según la tabla 18.

Tabla 18

Asignación de LUN a servidores físicos ESXi.

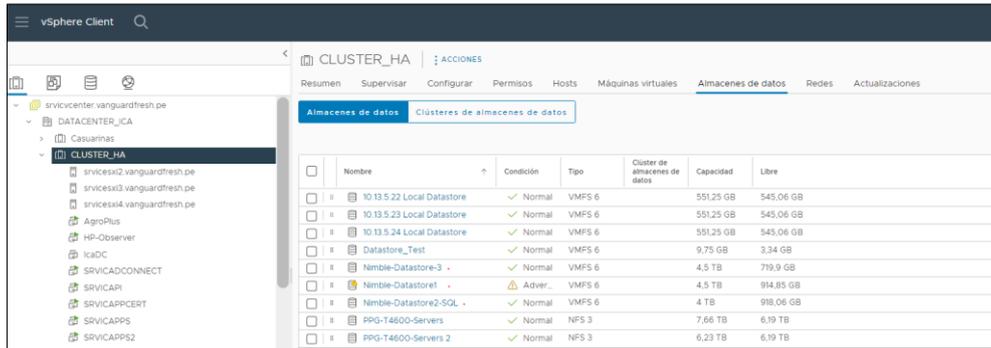
LUN	Cap.	Asignación	Permisos
Nimble-LUN01	4.5 TiB	SRVICESXI2, SRVICESXI3, SRVICESXI4	Lectura/Escritura
Nimble-LUN02	4 TiB	SRVICESXI2, SRVICESXI3, SRVICESXI4	Lectura/Escritura
Nimble-LUN03	4.5 TiB	SRVICESXI2, SRVICESXI3, SRVICESXI4	Lectura/Escritura

Luego de asignar las LUN a los servidores con ESXi, se creó los tres *datstores* con formato VMFS y se visualizó en el clúster de VMware.

- Nimble-LUN01 : Nimble-Datastore1
- Nimble-LUN02 : Nimble-Datastore2-SQL
- Nimble-LUN03 : Nimble-Datastore-3

Figura 104

Listado de datastores

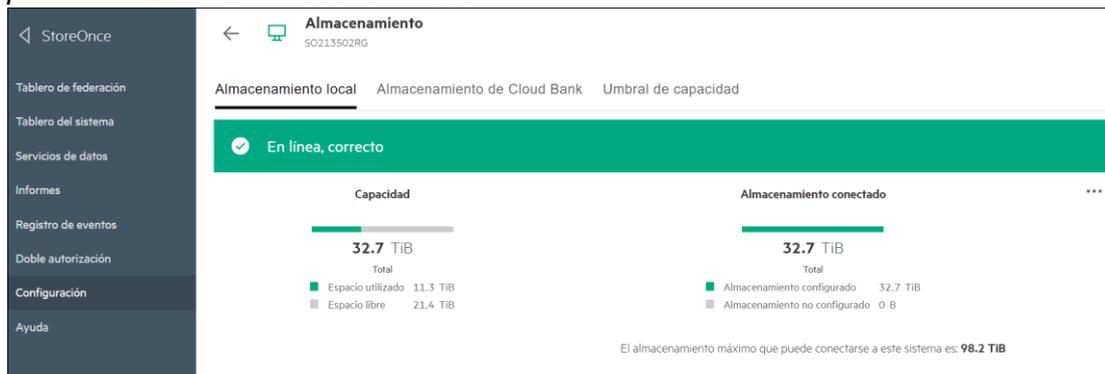


B. Implementación y configuración del sistema de almacenamiento de respaldo. Se enciende el sistema de almacenamiento de respaldo *HPe Storeonce 3640* y se aplicó la siguiente configuración:

- Las dos tarjetas de red (tráfico de respaldo) de 10Gb se configuró en *teaming* para que tenga alta disponibilidad de conectividad a nivel de los switches.
- Se configuró la dirección IP de administración web: 10.13.10.139 / 255.255.255.0 / 10.13.10.1.
- Se configuró la dirección IP para tareas de respaldo: 10.13.5.139 / 255.255.255.0 / 10.13.5.1.
- Se configuró un arreglo RAID6 de los 12 discos de 4TB, que nos brinda una capacidad aproximada de 36 TB o 32.7 TiB.

Figura 105

Espacio eficaz de HPe StoreOnce 3640



- Creación de usuario local para que los clientes puedan conectarse a los almacenes tipo *Catalyst*.
- Se creó dos almacenes del tipo *Catalyst*.
 - Repositorio_Veeam_1 : 9TiB
 - Repositorio_2_Veeam_Mensual : 9TiB

Figura 106

Almacenes de tipo *Catalyst*

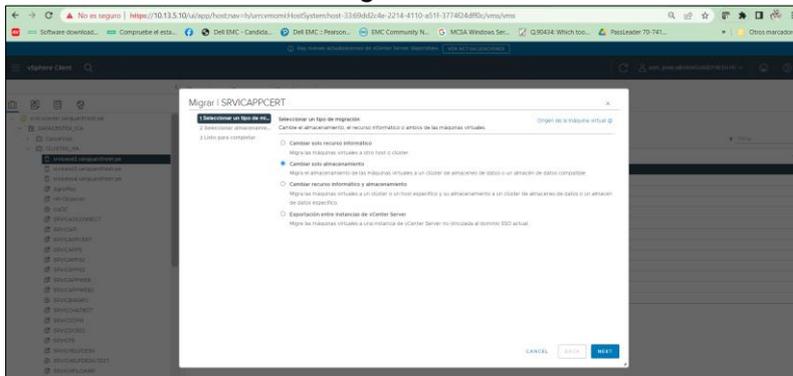


3.4.6. Migración de máquinas virtuales

Luego de crear los *datastore* en el clúster de *VMware*, se procede con la migración de las máquinas virtuales haciendo uso de la herramienta *VMware storage vmotion*. Esta herramienta nos permite hacer migraciones en caliente sin afectar la operatividad de las máquinas virtuales.

Figura 107

Herramienta *VMware Storage vMotion*



Datastores origen: PPG-T4600-Server y PPG-T4600-Server 2.

Datastores destino: Nimble-Datastore1, Nimble-Datastore2 y Nimble-Datastore3.

Con esa herramienta, se deja libre los *datastores* antiguos y estos, no se eliminan del clúster porque a futuro se planea usar como almacenamiento para la réplica de los servidores virtuales.

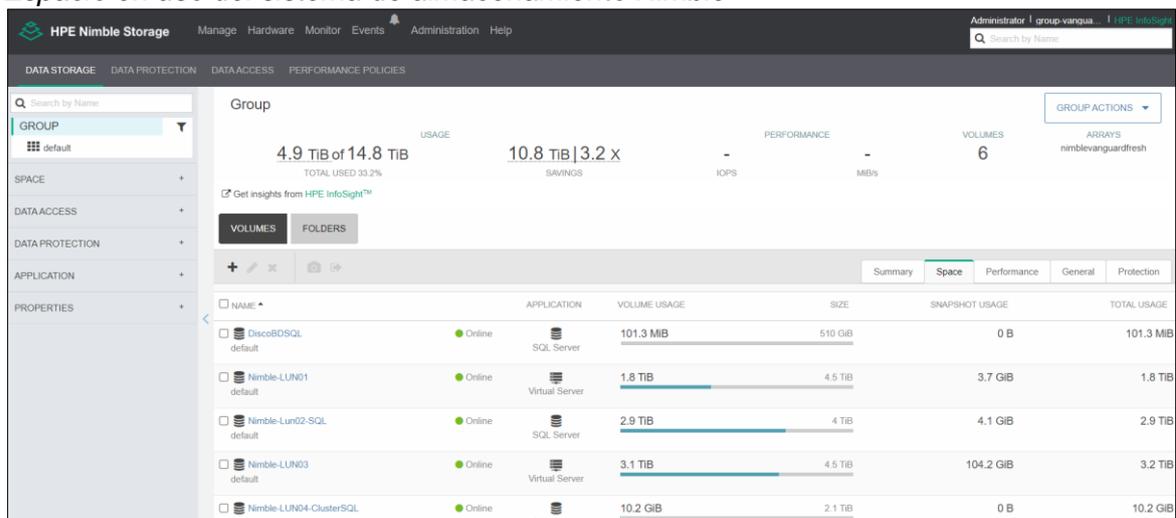
Luego de la migración de servidores virtuales, el sistema de almacenamiento Nimble empieza a deduplicar/comprimir los datos almacenados y en base ello podemos hacer los siguientes cálculos:

- El espacio provisionado del sistema de almacenamiento es de 15.7 TiB, del cual, el espacio real ocupado es de 4.9TiB.
- Espacio en uso de las LUN: 1.8 TiB + 2.9 TiB + 3.1 TiB = 7.8 TiB

Se concluye que el porcentaje de compresión/deduplicación es de un 62.82% aprox. del espacio lógico ocupado.

Figura 108

Espacio en uso del sistema de almacenamiento Nimble

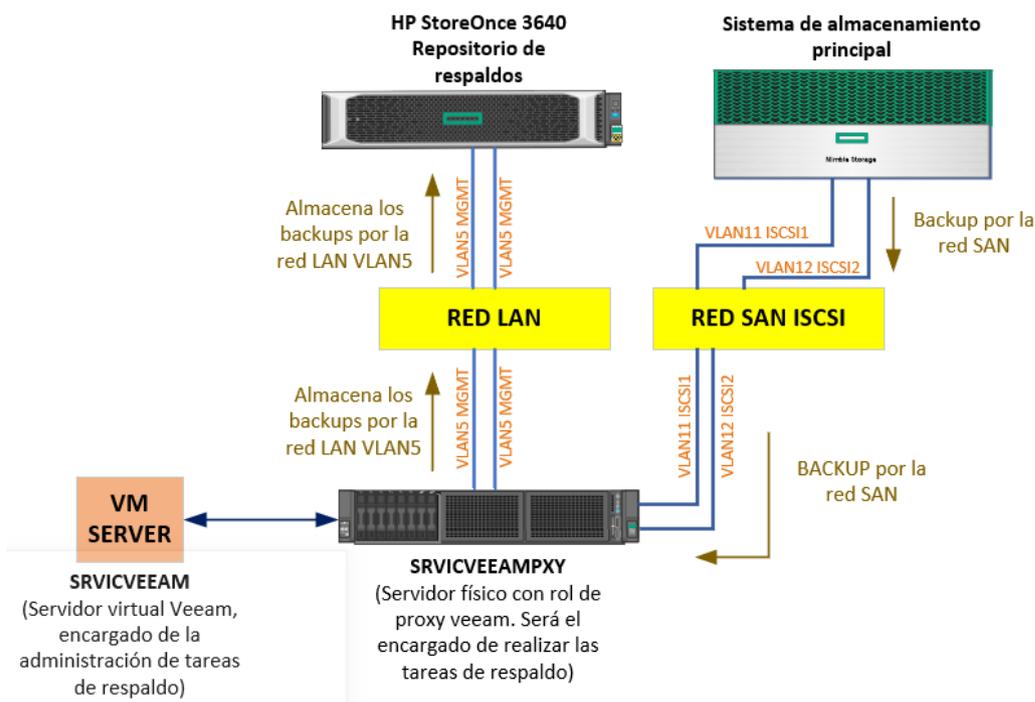


3.4.7. Implementación y configuración de servidor de respaldo

A partir de la arquitectura IT propuesta, en la figura 109, se muestra la implementación del servidor de respaldo.

Figura 109

Arquitectura IT de sistema de respaldo



El servidor **SRVICVEEAMPXY** será el encargado de hacer los respaldos vía SAN y los almacenará por la red LAN VLAN 5 en los almacenes *catalyst* del sistema de almacenamiento *HPe StoreOnce 3640*.

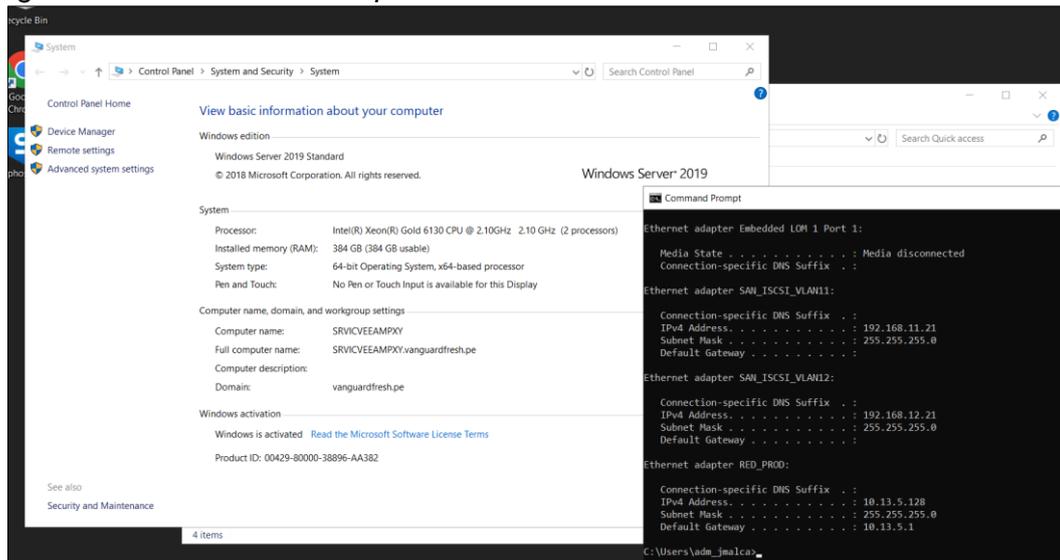
Primero, se formateó el servidor **SRVICESXI1** y se instaló el sistema operativo *Windows Server Standard 2019*. A este servidor se le configuro los siguientes parámetros:

- Hostname : Srvicveeampxy.vanguardfresh.pe
- IP Red Prod. : 10.13.5.128 / 255.255.255.0 / 10.13.10.1
- IP iSCSI1 : 192.168.11.21 / 255.255.255.0
- IP iSCSI2 : 192.168.12.21 / 255.255.255.0

La figura 110 muestra el resumen de la configuración del servidor **SRVICVEEAMPXY**.

Figura 110

Configuración de servidor de respaldo

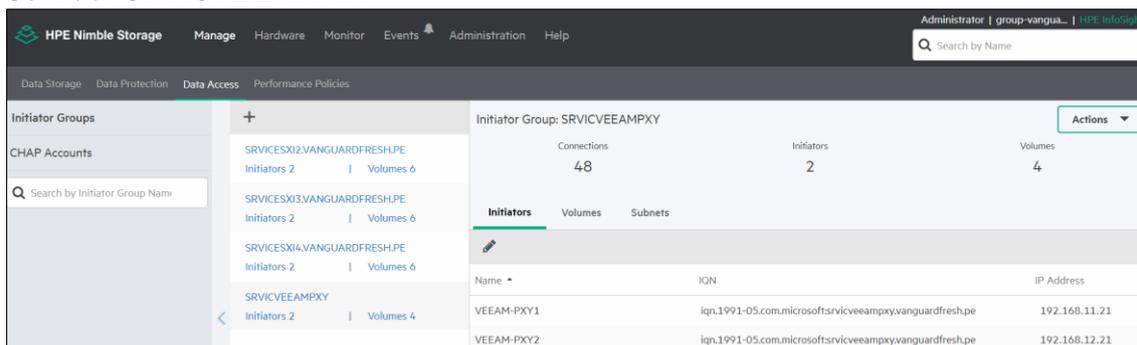


Se realizó una configuración de *teaming* de las 2 tarjetas de red que están en la VLAN 5. Esto se da con el motivo de mantener la alta disponibilidad y aumentar ancho de banda; y en el caso de la red SAN, una tarjeta se configuró en la VLAN11 y la otra en la VLAN 12.

Se inició el servicio iSCSI a nivel de Windows y se agregó el servidor iSCSI destino (sistema de almacenamiento) para que el sistema de almacenamiento principal pueda reconocer el *iSCSI initiator*. Luego, se ingresó a la interfaz web del sistema de almacenamiento principal, y se creó el host a partir del *iSCSI initiator* que ya figura en la interfaz web.

Figura 111

Servidor SRVICVEAMPXY



Luego de configurar el host *SRVICVEEAMPXY*, se asignó las tres LUN en modo lectura desde la interfaz web del sistema de almacenamiento *HPe Nimble*. El resumen de asignación se muestra en la tabla 19.

Tabla 19

Asignación de LUN a servidor SRVICVEEAMPXY.

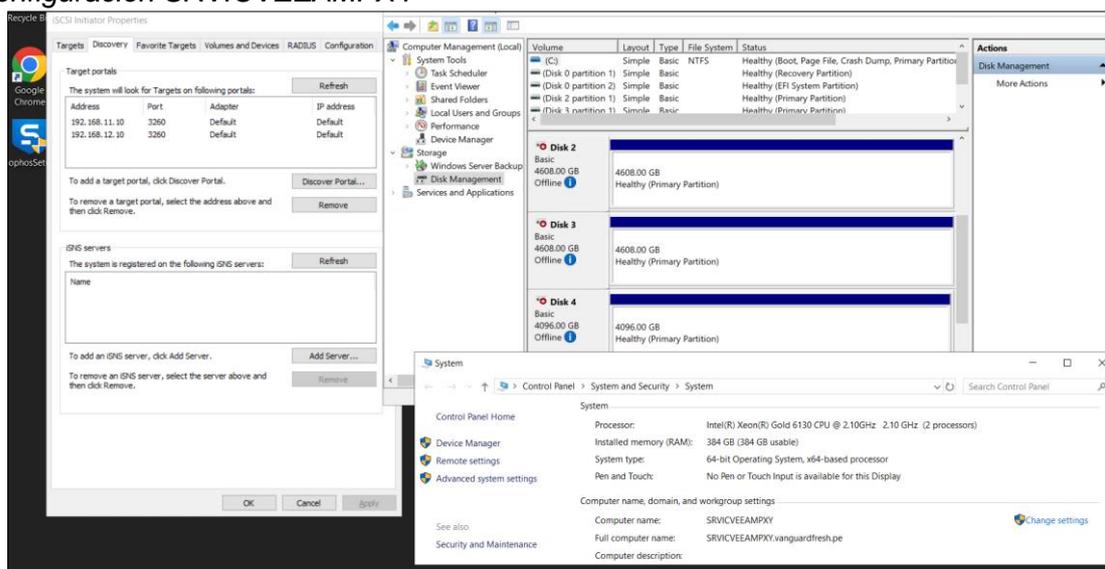
LUN	Capacidad	Asignación	Permisos
Nimble-LUN01	4.5 TiB	SRVICVEEAMPXY	Lectura
Nimble-LUN02	4 TiB	SRVICVEEAMPXY	Lectura
Nimble-LUN03	4.5 TiB	SRVICVEEAMPXY	Lectura

El motivo de asignar los discos al servidor proxy Veeam es para que se pueda realizar respaldos vía SAN.

Al tener varios *path* desde el servidor físico al sistema de almacenamiento principal, se habilita y configura el rol de *multipath IO (MPIO)* para que el servidor físico pueda reconocer la misma LUN desde varios *path* o caminos (ver figura 112), es decir, no figure discos repetidos.

Figura 112

Configuración SRVICVEEAMPXY

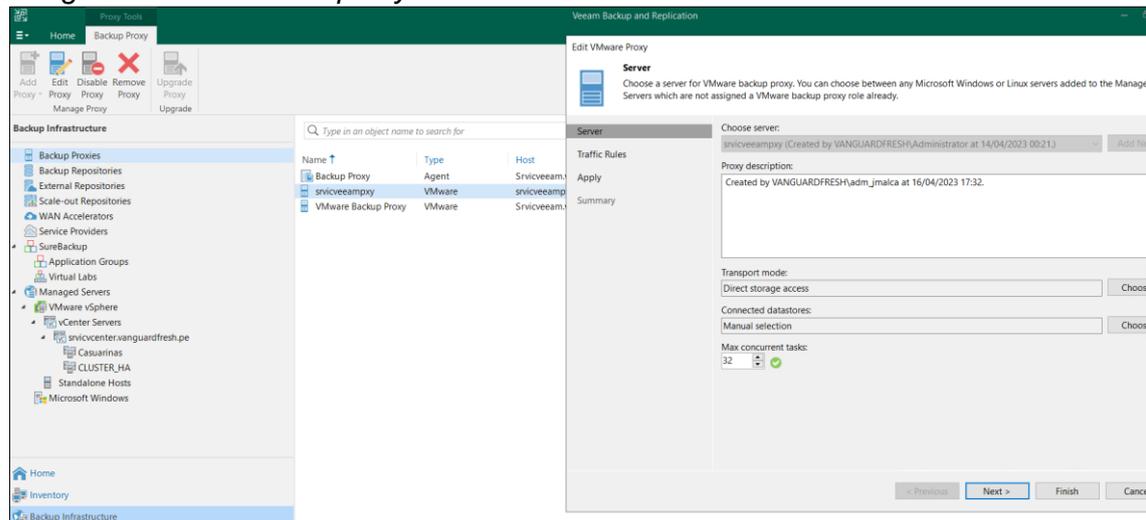


En la consola de administración *Veeam*, se agregó el servidor físico *SRVICVEEAMPXY* y se instaló el rol de proxy. El servidor *proxy Veeam* se configuró el

modo de transporte *direct storage access* para que pueda realizar respaldos vía SAN y se agregó los 3 *datastores* de manera manual.

Figura 113

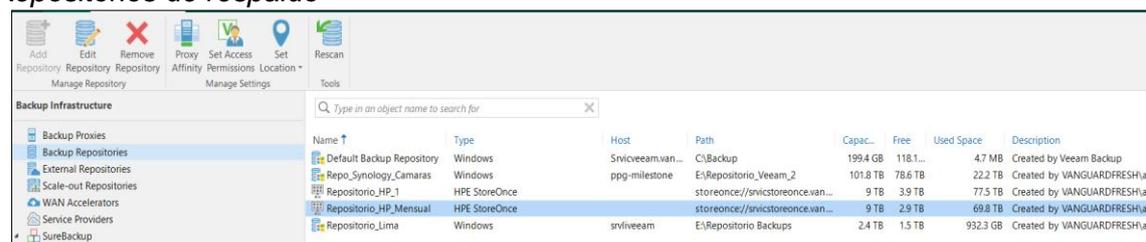
Configuración de servidor proxy Veeam



En la interfaz web del Veeam se agregó los dos almacenes del tipo *Catalyst* para que puedan ser usados como repositorio de respaldos, ver figura 114.

Figura 114

Repositorios de respaldo



Teniendo los repositorios configurados, se procede a configurar las tareas de respaldo diarias según la tabla 20.

Tabla 20*Tareas de respaldo tipo diario.*

Tareas de respaldo	Servidores	Tipo de respaldo	Horario	Repositorio
BK_Diario_VMs_Grupo1	SRVICADCONNECT,SRVICDCPRI,SRVICDCSEC,SRVICFS,SRVICMAMUT,SRVICRDG, SRVICRDS,SRVICWSUS,SRVICMILESTONE,SRVICPARECORD,SRVICPRINT,SRVICAPPS	Diario	11:00 p. m.	Repositorio_HP_1
BK_Diario_VMs_Grupo2	SRVICAPPPROD,SRVICNISWEB,SRVICNISTAREO,SRVICNISCAMPO,SRVICNISPACK-QA	Diario	3:30 a. m.	Repositorio_HP_1
BK_Diario_VMs_Grupo3	SRVICNISIRA,SRVICPLANIF	Diario	Después de BK_Diario_VMs_Grupo 2	Repositorio_HP_1
BK_Diario_VMs_Grupo4	SRVICVEEAM	Diario	1:00 p. m.	Repositorio_HP_1
BK_Diario_VMs_Grupo5	SRVICSERVICEDESK_P ROD	Diario	6:00 p. m.	Repositorio_HP_1
BK_Diario_VMs_Grupo6	SRVICAPPWEB,SRVICHELPDESK,SRVICAPPWEB2,SRVICAPPCERT,SRVICAPPS2,SRVICAPPS3,SRVICWEBCONSULTA	Diario	7:00 a. m.	Repositorio_HP_1

Luego de configurar las tareas diarias, se procede a configurar las tareas de respaldo mensuales según la tabla 21.

Tabla 21

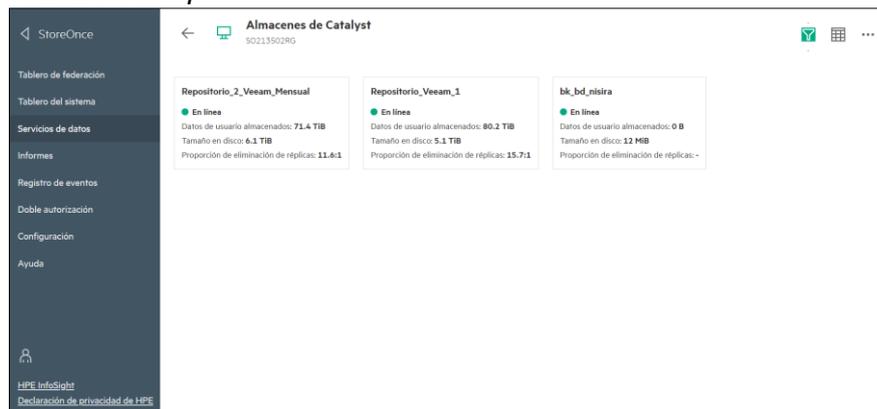
Tareas de respaldo de tipo mensual.

Tareas de respaldo	Tarea diaria	Retención	Repositorio
BK_Mensual_VMs_Grupo1	BK_Diario_VMs_Grupo1	90 días 8 full mensual 1 anual	Repositorio_HP_Mensual
BK_Mensual_VMs_Grupo2	BK_Diario_VMs_Grupo2	90 días 8 full mensual 1 anual	Repositorio_HP_Mensual
BK_Mensual_VMs_Grupo4	BK_Diario_VMs_Grupo4	90 días 8 full mensual 1 anual	Repositorio_HP_Mensual
BK_Mensual_VMs_Grupo5	BK_Diario_VMs_Grupo5	90 días 8 full mensual 1 anual	Repositorio_HP_Mensual
BK_Mensual_VMs_Grupo6	BK_Diario_VMs_Grupo6	90 días 8 full mensual 1 Anual	Repositorio_HP_Mensual

Luego de pasar un cierto periodo de tiempo, el sistema de almacenamiento de respaldo nos brindó las siguientes métricas de ahorro de espacio:

Figura 115

Métricas de ahorro de espacio en disco

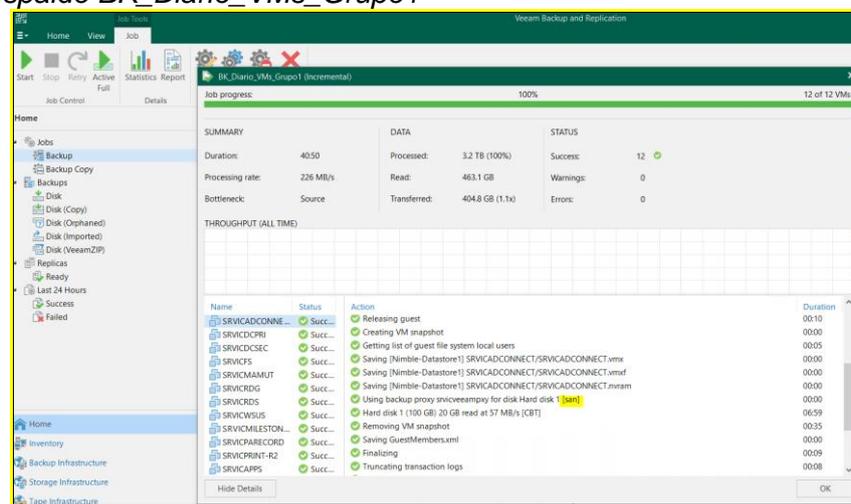


En la figura 115, el repositorio de respaldo diario Repositorio_Veeam_1, muestra un ahorro de espacio de 15.7:1 y el repositorio mensual Respositorio_2_Veeam_Mensual, de 11.6:1. Estos valores describen que el sistema de almacenamiento de respaldo posee un algoritmo eficaz de deduplicacion con el fin de ahorrar espacio en disco.

La figura 116 muestra el proceso de respaldo de la tarea BK_Diario_VMs_Grupo1 y se aprecia que el proceso de respaldo del servidor SRVICADCONNECT se realiza por la red SAN.

Figura 116

Tarea de respaldo BK_Diario_VMs_Grupo1



Las actividades realizadas para la instalación, implementación, configuración y puesto a punto de la solución se resumen en la tabla 22.

Tabla 22*Resumen de actividades de la puesta a punto de la solución.*

Actividades	Descripción
Actividad 01	Instalación física del sistema de almacenamiento principal en el gabinete del datacenter de Agrícola Challapampa S.A.C.
Actividad 02	Instalación física del sistema de almacenamiento de respaldo en el gabinete del datacenter de Agrícola Challapampa S.A.C.
Actividad 03	Cableado de fibra de los dos sistemas de almacenamiento a los switches HPe FF 5940.
Actividad 04	Creación de VLAN iSCSI (VLAN 11 y 12) en los switches HPe FF 5940.
Actividad 05	Configuración lógica de puertos físicos (modo acceso y modo troncal).
Actividad 06	Configuración de tarjetas de red en cada virtual switch de los tres servidores ESXi.
Actividad 07	Configuración de VLANs para separar tráfico LAN/SAN en cada servidor ESXi.
Actividad 08	Configuración de VLANs iSCSI en cada virtual switch de cada servidor ESXi
Actividad 09	Configuración de iSCSI software initiator en cada servidor ESXi
Actividad 10	Actualización de la versión de VMware vSphere ESXi de la 6.7U3 a la 7 U3.
Actividad 11	Inicialización del sistema de almacenamiento principal HPe Nimble HF20.
Actividad 12	Configuración de parámetros de red del sistema de almacenamiento principal Nimble HF20.
Actividad 13	Creación de arreglo de discos con RAID RTP en el sistema de almacenamiento principal.
Actividad 14	Configuración de los hosts en el sistema de almacenamiento principal HPe Nimble HF20 con los softwares iSCSI initiator de cada servidor ESXi
Actividad 15	Creación de tres LUN en el sistema de almacenamiento principal Nimble HF20
Actividad 16	Asignación de LUN a servidores físicos ESXi
Actividad 17	Creación de tres datastores en los servidores ESXi
Actividad 18	Inicialización del sistema de almacenamiento de respaldo HPe StoreOnce 3640.
Actividad 19	Configuración de parámetros de red del sistema de almacenamiento de respaldo HPe StoreOnce 3640
Actividad 20	Configuración de arreglo de discos RAID6
Actividad 21	Creación de dos almacen Catalyst
Actividad 22	Migración de máquinas virtuales
Actividad 23	Configuración de clúster de VMware vSphere en alta disponibilidad.
Actividad 24	Verificación de tasa de deduplicación/compresión en el sistema de almacenamiento HPE Nimble HF20
Actividad 25	Formateo de servidor SRVICESX11 e instalación de Windows server standard 2019.
Actividad 26	Configuración de redes de servidor SRVICVEEAMPXY
Actividad 27	Habilitación de servicio iSCSI y MPIO
Actividad 28	Configuración de iSCSI initiator en el servidor SRVICVEEAMPXY
Actividad 29	Creación de host SRVICVEEAMPXY en la interfaz web del sistema de almacenamiento principal HPe Nimble HF20
Actividad 30	Asignación de discos en modo lectura desde la interfaz web del sistema de almacenamiento principal HPe Nimble al host SRVICVEEAMPXY
Actividad 31	Instalación de servicio proxy Veeam en el servidor SRVICVEEAMPXY

Actividad 32	Creación de dos repositorios de respaldos que hacen referencia a los dos almacenes Catalyst.
Actividad 33	Creación de tareas de respaldo del tipo diario
Actividad 34	Creación de tareas de respaldo del tipo mensual
Actividad 35	Verificación de tasa de deduplicacion en el sistema de almacenamiento de respaldo

3.5. Pruebas de testeo de la solución

A continuación, se describe las diversas pruebas y validaciones de la solución implementada. Se considera los siguientes puntos:

- Pruebas de testeo de la alta disponibilidad de la LAN
- Pruebas de testeo de la alta disponibilidad de la SAN.

3.5.1. Prueba de testeo de la alta disponibilidad de la LAN

Para verificar el correcto funcionamiento de las máquinas virtuales, se hizo pruebas con los puertos LAN del servidor ESXi SRVICESXI2. Para ello, se apagó puerto por puerto y se verificó la continuidad de los servicios.

Figura 117

vSwitch1 del servidor SRVICESXI2

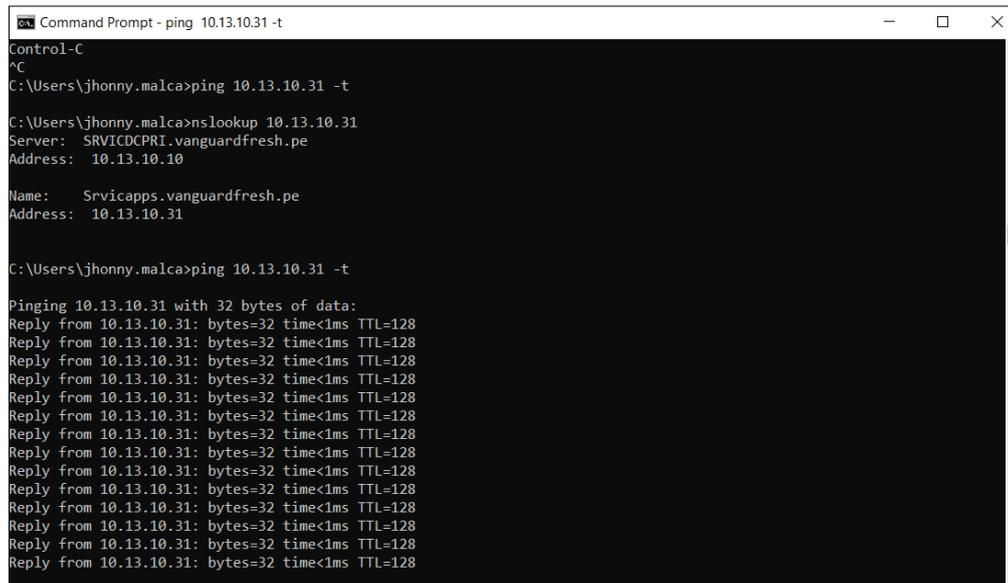


La figura 117 muestra el servidor SRVIESXI2 tiene el vswitch1 con las dos tarjetas vmnic activas.

Se validó conectividad a la máquina virtual SRVICAPPS con dirección IP 10.13.10.31, estando las dos tarjetas activas (ver figura 118).

Figura 118

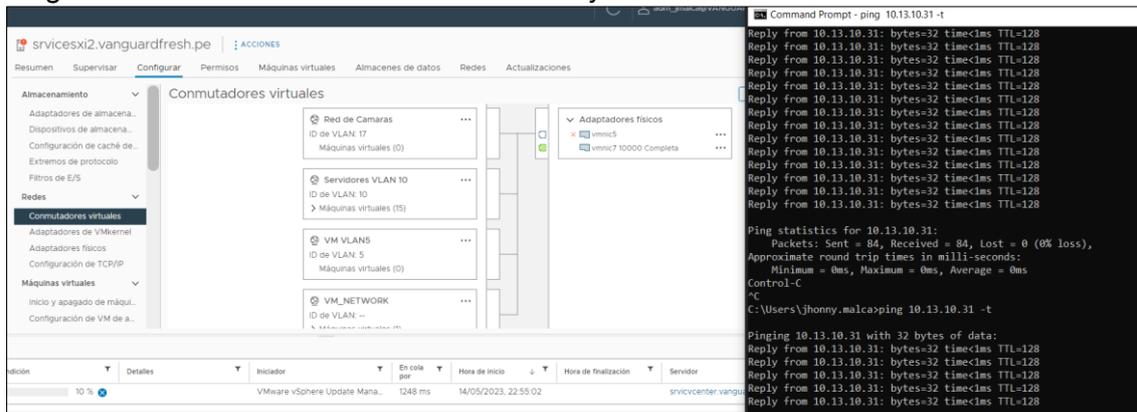
Ping hacia el servidor SRVICAPPS



Se apagó el puerto en el switch (XGE1/0/20) y se validó la continuidad de la conectividad al servidor.

Figura 119

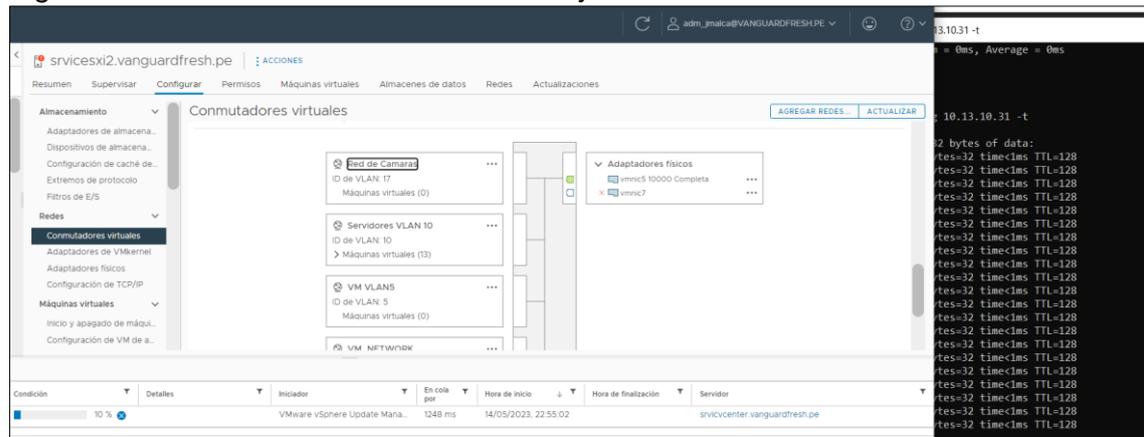
Ping hacia el servidor SRVICAPPS con la tarjeta vmnic 5 desconectada



Se apago el puerto en el switch (XGE2/0/44) y se validó la continuidad de la conectividad a la máquina virtual SRVICAPPS:

Figura 120

Ping hacia el servidor SRVICAPPS con la tarjeta vmnic 7 desconectada



Con esta prueba se concluye que se mantiene la conectividad a las máquinas virtuales a pesar de que una tarjeta de red se malogre o el puerto se desconecte.

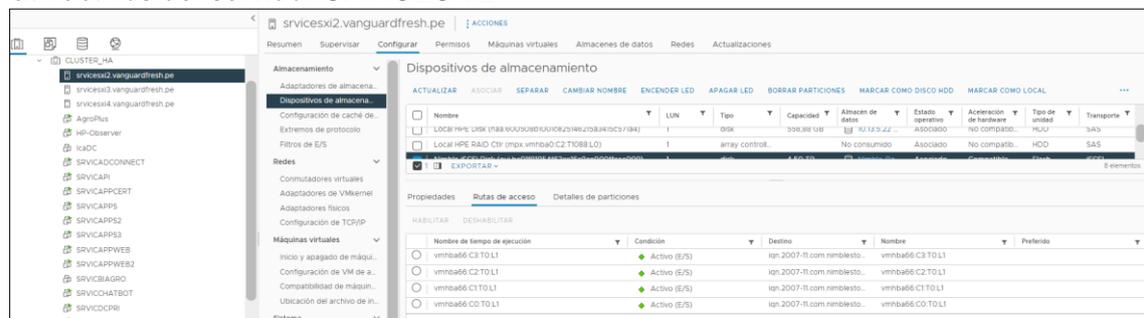
3.5.2. Prueba de testeo de la alta disponibilidad de la SAN

Para validar la alta disponibilidad de conectividad de los servidores al sistema de almacenamiento, se desconecta puerto por puerto y se valida los *path* activos de alguno de los *datastores* que hacen referencia al *Nimble*.

Antes de realizar el procedimiento, se valida los *path* activos existentes del *datastore* con LUN ID 1.

Figura 121

Path activos del servidor SRVICESXI2

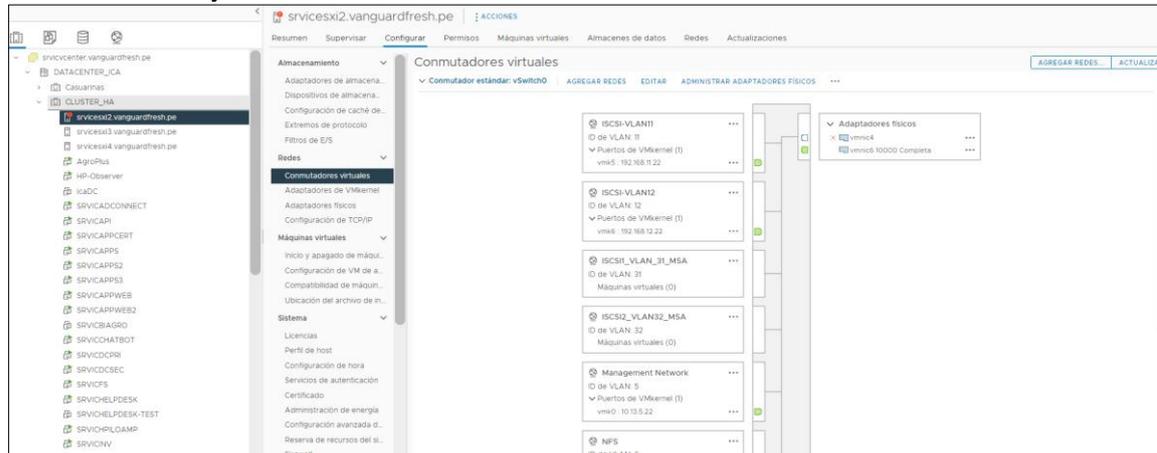


La figura 121 muestra 4 *path* activos porque son 4 conexiones iSCSI destino.

A continuación, se apaga el puerto de XGE1/0/20 y se visualiza como desconectado la vmnic4.

Figura 122

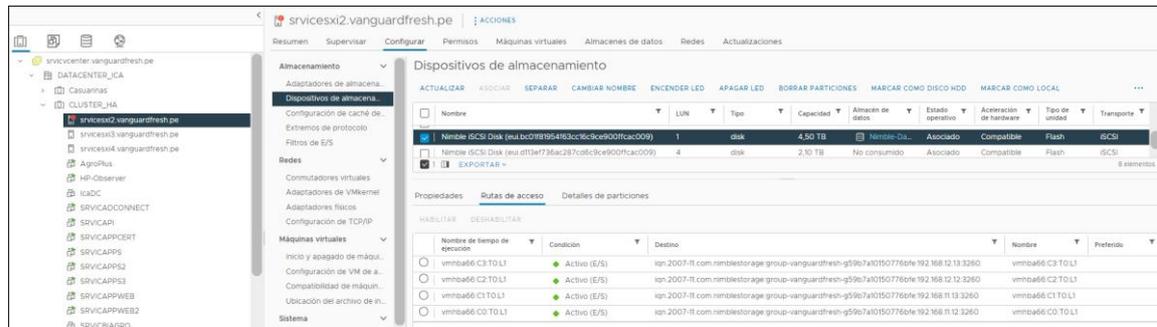
vSwitch0 con tarjeta vmnic4 desconectada



Los path siguen activos y se mantiene la continuidad de los servicios.

Figura 123

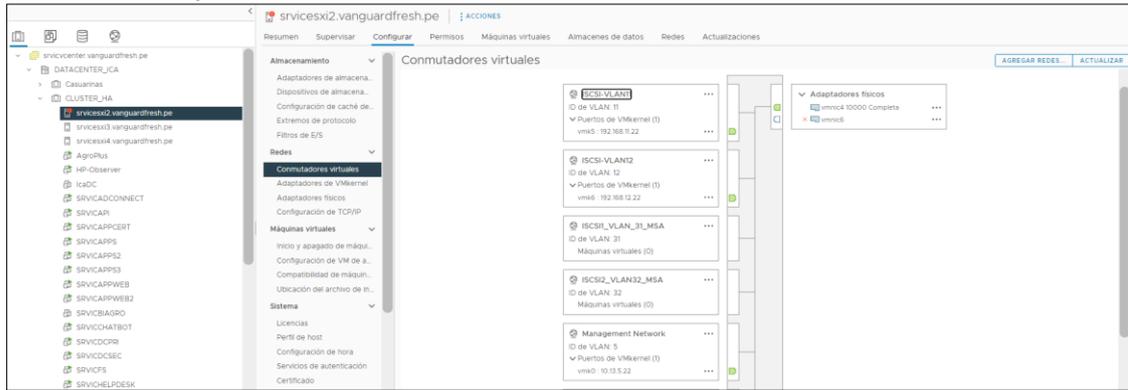
Path activos del servidor SRVICESX12



A continuación se apagó el puerto XG1/0/44 en el switch HPe y se visualiza la tarjeta vmnic6 desconectada en el vswitch0.

Figura 124

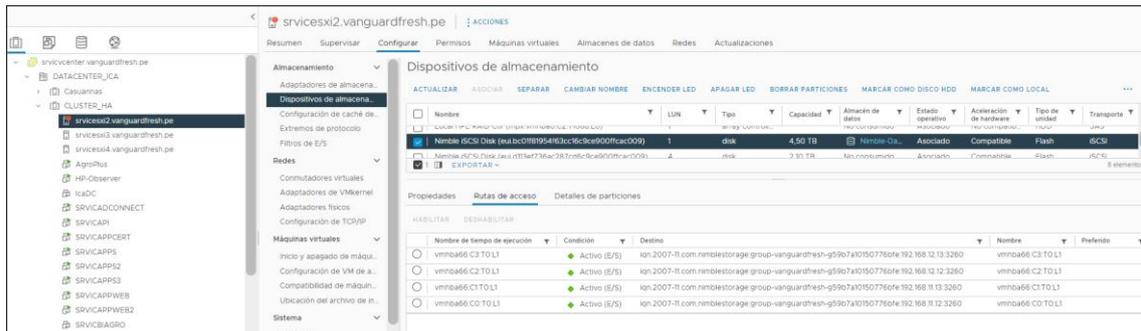
vSwitch0 con tarjeta vmnic6 desconectada



Luego de realizar ambas pruebas, los *path* se mantienen activos, tal como se muestra en la figura 125.

Figura 125

Path activos del servidor SRVICESXI2



Con estas pruebas se concluye lo siguiente: si se desconecta alguna tarjeta del vswitch0 de la red san iSCSI, no se pierde conectividad de los *datastores* donde residen las máquinas virtuales.

Figura 126

Datastores activos en el clúster de VMware

	Nombre	Condición	Tipo	Clúster de almacenes de datos	Capacidad	Libre
<input type="checkbox"/>	10.13.5.22 Local Datastore	✓ Normal	VMFS 6		551,25 GB	545,06 GB
<input type="checkbox"/>	10.13.5.23 Local Datastore	✓ Normal	VMFS 6		551,25 GB	545,06 GB
<input type="checkbox"/>	10.13.5.24 Local Datastore	✓ Normal	VMFS 6		551,25 GB	545,06 GB
<input type="checkbox"/>	datastore	✓ Normal	VMFS 6		8,73 TB	6,77 TB
<input type="checkbox"/>	Datastore_Test	✓ Normal	VMFS 6		9,75 GB	3,34 GB
<input type="checkbox"/>	Nimble-Datastore-3	✓ Normal	VMFS 6		4,5 TB	756,58 GB
<input type="checkbox"/>	Nimble-Datastore1	⚠ Adver...	VMFS 6		4,5 TB	904,73 GB
<input type="checkbox"/>	Nimble-Datastore2-SQL	✓ Normal	VMFS 6		4 TB	912,28 GB
<input type="checkbox"/>	PPG-T4600-Servers	✓ Normal	NFS 3		7,66 TB	6,19 TB
<input type="checkbox"/>	PPG-T4600-Servers 2	✓ Normal	NFS 3		6,23 TB	6,19 TB

La alerta del *datastore Nimble-Datastore01* que se muestra en la figura 126 es por consumo de espacio en disco.

3.6. Validación de la solución

A continuación, se detalla los cálculos que permitan validar la solución implementada.

3.6.1. Cálculo de los tiempos de parada de la solución

Los tiempos de parada de servicios del año 2022 tenían un tiempo considerable debido a que el antiguo sistema de almacenamiento tenía problemas con el software de sus controladoras, provocando que el sistema deje de funcionar afectando la operatividad de las máquinas virtuales que residían en ella. Cada vez que sucedía ello, el administrador de IT tenía que reiniciar el sistema de almacenamiento y servidores ESXi para restablecer los servicios. Este proceso de recuperación demoraba +/- 16 min y los registros figuran en la tabla 23.

Tabla 23

Tiempos de parada de servicio año 2022.

Mes	Tiempo de corte (min)
Enero	15
Febrero	17
Marzo	16
Abril	17

Para el cálculo de los tiempos de parada se toma como muestra los registros de tiempos de corte de servicio del primer cuatrimestre del año 2022 con la arquitectura IT anterior. En base a la tabla 23 se calculó el tiempo promedio de recuperación de servicio MTTR:

$$\text{MTTR} = (15+17+16+17) / 4$$

$$\text{MTTR} = 16.25 \text{ min}$$

En el primer cuatrimestre del año 2023, con la nueva infraestructura de IT, se obtuvo los registros detallados en la tabla 24.

Tabla 24

Tiempos de parada de servicio año 2023.

Mes	Tiempo de corte (min)
Enero	5
Febrero	0
Marzo	4
Abril	0

En base a la tabla 24 se calculó el tiempo promedio de recuperación de servicio MTTR con la nueva infraestructura de IT:

$$\text{MTTR} = 2.25 \text{ min}$$

A continuación, calculamos el porcentaje de disminución de los tiempos de corte de servicio.

$$\% \text{ Disminución} = 100 \$ - (2.25/16.25) \times 100\%$$

$$\% \text{ Disminución} = 86.15 \%$$

3.6.2. Cálculo de los tiempos de respaldo

Para las pruebas de disminución de los tiempos de *backup*, se eligió trabajar con la tarea de respaldo: BK_Diario_VMs_Grupo2.

En la consola *Veeam backup* se sacó el reporte de la tarea de respaldo BK_Diario_VMs_Grupo2, y se extrajo la siguiente información: fecha, día, cantidad de GB respaldados y tiempo de respaldo en formato (MM:SS). Con esta data, se elaboró la tabla

25, y se agregó dos columnas: tiempo en formato minutos (Min) y la cantidad de GB respaldados por minuto.

Tabla 25

Reporte de tarea de respaldo BK_Diario_VMs_Grupo2.

Fecha	Día	GB	Tiempo (MM:SS)	Tiempo(Min)	GB/Min
20.03.2023	Lunes	75.8	18:16	18.27	4.15
21.03.2023	Martes	72.3	10:58	10.97	6.59
22.03.2023	Miércoles	100.3	13:47	13.78	7.28
23.03.2023	Jueves	83.3	11:50	11.83	7.04
24.03.2023	Viernes	75.1	11:15	11.25	6.68
25.03.2023	Sábado	75.9	12:30	12.50	6.07
26.03.2023	Domingo	73.8	23:03	23.05	3.20
27.03.2023	Lunes	87.8	11:38	11.63	7.55
28.03.2023	Martes	92.2	12:26	12.43	7.42
29.03.2023	Miércoles	80.7	12:10	12.17	6.63
30.03.2023	Jueves	82	11:52	11.87	6.91
31.03.2023	Viernes	72.2	10:47	10.78	6.70
01.04.2023	Sábado	63.6	10:41	10.68	5.95
02.04.2023	Domingo	67.5	18:14	18.23	3.70
03.04.2023	Lunes	56.6	09:57	9.95	5.69
04.04.2026	Martes	100.1	13:16	13.27	7.55
05.04.2023	Miércoles	92.8	14:12	14.20	6.54
06.04.2023	Jueves	93.1	13:53	13.89	6.70
07.04.2023	Viernes	77.9	11:11	11.18	6.97
08.04.2023	Sábado	65.5	10:21	10.35	6.33
09.04.2023	Domingo	73.3	18:33	18.55	3.95
10.04.2023	Lunes	75.8	11:42	11.70	6.48
11.04.2023	Martes	113.6	13:43	13.72	8.28
12.04.2023	Miércoles	91.8	12:34	12.57	7.31
13.04.2023	Jueves	98.1	09:33	9.55	10.27
14.04.2023	Viernes	83.2	08:54	8.90	9.35
15.04.2023	Sábado	96.9	09:18	9.30	10.42
16.04.2023	Domingo	98.3	18:46	18.77	5.24
17.04.2023	Lunes	76.5	08:27	8.45	9.05
18.04.2023	Martes	93.4	08:50	8.83	10.57
19.04.2023	Miércoles	91.9	08:59	8.98	10.70
20.04.2023	Jueves	86.4	08:54	8.90	9.71
21.04.2023	Viernes	68.2	08:37	8.62	7.91
22.04.2023	Sábado	94.2	09:21	9.35	10.07
23.04.2023	Domingo	78.3	17:51	17.85	4.39
24.04.2023	Lunes	86.2	08:30	8.50	10.14

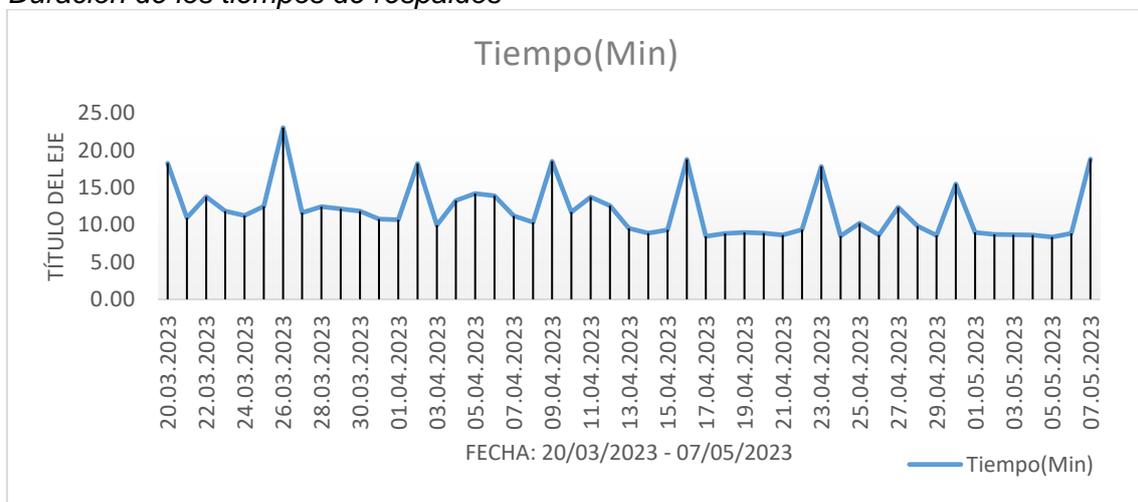
25.04.2023	Martes	117	10:13	10.22	11.45
26.04.2023	Miércoles	92.2	08:38	8.63	10.68
27.04.2023	Jueves	68.1	12:21	12.35	8.10
28.04.2023	Viernes	73.9	09:49	9.82	8.53
29.04.2023	Sábado	70.5	08:34	8.57	8.23
30.04.2023	Domingo	80.7	15:28	15.49	5.21
01.05.2023	Lunes	98.7	08:58	8.97	11.00
02.05.2023	Martes	104.8	08:43	8.72	12.02
03.05.2023	Miércoles	91.7	08:40	8.67	10.58
04.05.2023	Jueves	74.1	08:37	8.62	8.60
05.05.2023	Viernes	80.4	08:22	8.37	9.61
06.05.2023	Sábado	57.2	08:50	8.83	6.48
07.05.2023	Domingo	78.3	18:50	18.83	4.16

De la tabla 25 se nota el comportamiento de la disminución de los tiempos de respaldo y aumento de la cantidad de GB respaldados por minuto. Esto se reflejará en la Fig. 3.58 y 3.59.

En la figura 127, se evidencia que el tiempo que demora los respaldos diarios incrementales disminuye a lo largo del tiempo. Los picos de la figura 127 representan el tiempo de demora de los respaldos full en disco (cada domingo) y no tiene mucha variación porque es un proceso de sintetización de respaldos que se realiza en el mismo sistema de almacenamiento.

Figura 127

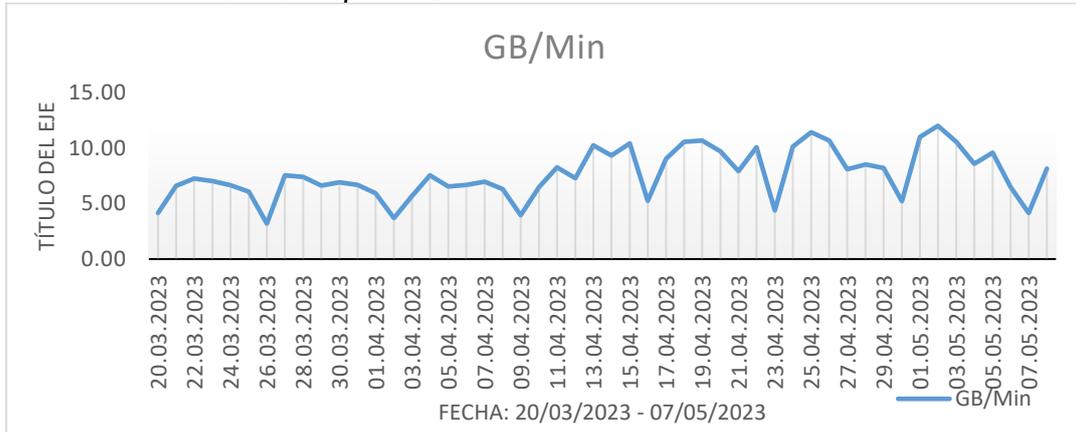
Duración de los tiempos de respaldos



En la figura 128, se evidencia que la cantidad de GB/Min aumenta a lo largo del tiempo, esto es debido a que los respaldos se realizan por la red la SAN.

Figura 128

Variación de velocidad de respaldo GB/Min



La fecha de cambio de la configuración es a partir del 12 de abril del 2023 y a partir de esa fecha se elige el promedio de tiempos de respaldos de 23 antes y 23 días posteriores.

Tiempo promedio de duración de la tarea de respaldo antes de aplicar los cambios.

$$T_{\text{PROM}} = 306.26 / 23 = 13.32 \text{ minutos}$$

Tiempo promedio de duración de la tarea de respaldo luego de aplicar los cambios:

$$T_{\text{PROM}} = 238.61 / 23 = 10.37 \text{ minutos}$$

El porcentaje de disminución promedio de los tiempos de respaldos es:

$$\% \text{ Disminución} = 100\% - (10.37/13.32) \times 100\% \approx 22.15\%$$

$$\% \text{ Disminución} \approx 22.15\%$$

Figura 129

Reporte de respaldo, fecha 03.05.2023, tarea BK_Diario_VMs_Grupo2

Backup job: BK_Diario_VMs_Grupo2								
Created by VANGUARDFRESH\admin_jmalca at 29/11/2021 16:42.								
miércoles, 3 de mayo de 2023 03:30:19								
Success	5	Start time	03:30:19	Total size	750 GB	Backup size	91.8 GB	
Warning	0	End time	03:38:59	Data read	122.8 GB	Dedupe	6.4x	
Error	0	Duration	0:08:40	Transferred	91.7 GB	Compression	1.0x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRVICONISAPPPROD	Success	03:31:51	03:36:52	100 GB	15.1 GB	11.8 GB	0:05:01	
SRVICONISWEB	Success	03:31:51	03:37:30	100 GB	16.1 GB	13.2 GB	0:05:39	
SRVICONISTAREO	Success	03:31:51	03:37:26	200 GB	34 GB	28.2 GB	0:05:35	
SRVICONISCAMPO	Success	03:31:51	03:38:47	150 GB	16.9 GB	11.2 GB	0:06:56	
SRVICONISPACK_QA	Success	03:31:51	03:38:29	200 GB	40.7 GB	27.3 GB	0:06:38	

Figura 130

Reporte de respaldo, fecha 02.05.2023, tarea BK_Diario_VMs_Grupo2

Backup job: BK_Diario_VMs_Grupo2								
Created by VANGUARDFRESH\admin_jmalca at 29/11/2021 16:42.								
martes, 2 de mayo de 2023 03:30:20								
Success	5	Start time	03:30:20	Total size	750 GB	Backup size	104.8 GB	
Warning	0	End time	03:39:03	Data read	135.8 GB	Dedupe	5.6x	
Error	0	Duration	0:08:43	Transferred	104.8 GB	Compression	1.0x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRVICONISAPPPROD	Success	03:32:06	03:37:44	100 GB	22.8 GB	19.4 GB	0:05:38	
SRVICONISWEB	Success	03:32:06	03:37:13	100 GB	15.7 GB	12.9 GB	0:05:07	
SRVICONISTAREO	Success	03:32:06	03:38:29	200 GB	35.4 GB	29.7 GB	0:06:23	
SRVICONISCAMPO	Success	03:32:06	03:38:53	150 GB	16.4 GB	10.7 GB	0:06:47	
SRVICONISPACK_QA	Success	03:32:06	03:38:42	200 GB	45.5 GB	32.1 GB	0:06:36	

Figura 131

Reporte de respaldo, fecha 01.05.2023, tarea BK_Diario_VMs_Grupo2

Backup job: BK_Diario_VMs_Grupo2								
Created by VANGUARDFRESH\admin_jmalca at 29/11/2021 16:42.								
lunes, 1 de mayo de 2023 03:30:05								
Success	5	Start time	03:30:05	Total size	750 GB	Backup size	98.8 GB	
Warning	0	End time	03:39:03	Data read	129.8 GB	Dedupe	5.9x	
Error	0	Duration	0:08:58	Transferred	98.7 GB	Compression	1.0x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRVICONISAPPPROD	Success	03:32:10	03:36:42	100 GB	15.2 GB	11.8 GB	0:04:32	
SRVICONISWEB	Success	03:32:10	03:36:51	100 GB	13.1 GB	10.3 GB	0:04:41	
SRVICONISTAREO	Success	03:32:10	03:38:32	200 GB	40.8 GB	35 GB	0:06:22	
SRVICONISCAMPO	Success	03:32:10	03:38:52	150 GB	16 GB	10.3 GB	0:06:42	
SRVICONISPACK_QA	Success	03:32:10	03:38:50	200 GB	44.7 GB	31.3 GB	0:06:40	

Figura 132

Reporte de respaldo, fecha 04.04.2023, tarea BK_Diario_VMs_Grupo2.

Backup job: BK_Diario_VMs_Grupo2								
Created by VANGUARDFRESH\adm_jmalca at 29/11/2021 16:42.								
martes, 4 de abril de 2023 03:30:14								
Success	5	Start time	03:30:14	Total size	750 GB	Backup size	100.2 GB	
Warning	0	End time	03:43:30	Data read	131.3 GB	Dedupe	5.8x	
Error	0	Duration	0:13:16	Transferred	100.1 GB	Compression	1.0x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRVICNISAPPROD	Success	03:32:03	03:38:03	100 GB	23.1 GB	19.8 GB	0:06:00	
SRVICNISWEB	Success	03:32:03	03:37:28	100 GB	17.8 GB	14.9 GB	0:05:25	
SRVICNISTAREO	Success	03:32:03	03:36:57	200 GB	30.5 GB	24.6 GB	0:04:54	
SRVICNISCAMPO	Success	03:32:03	03:38:52	150 GB	15.9 GB	10.1 GB	0:06:49	
SRVICNISPACK_QA	Success	03:36:29	03:43:20	200 GB	44.1 GB	30.7 GB	0:06:51	

Figura 133

Reporte de respaldo, fecha 03.04.2023, tarea BK_Diario_VMs_Grupo2.

Backup job: BK_Diario_VMs_Grupo2								
Created by VANGUARDFRESH\adm_jmalca at 29/11/2021 16:42.								
lunes, 3 de abril de 2023 03:30:16								
Success	5	Start time	03:30:16	Total size	750 GB	Backup size	56.6 GB	
Warning	0	End time	03:40:13	Data read	87.7 GB	Dedupe	9.8x	
Error	0	Duration	0:09:57	Transferred	56.6 GB	Compression	1.0x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRVICNISAPPROD	Success	03:31:52	03:36:56	100 GB	15.5 GB	12.1 GB	0:05:04	
SRVICNISWEB	Success	03:31:52	03:36:29	100 GB	14.1 GB	11.3 GB	0:04:37	
SRVICNISTAREO	Success	03:31:52	03:35:54	200 GB	16 GB	10.2 GB	0:04:02	
SRVICNISCAMPO	Success	03:31:52	03:38:50	150 GB	16.4 GB	10.7 GB	0:06:58	
SRVICNISPACK_QA	Success	03:35:13	03:40:00	200 GB	25.7 GB	12.3 GB	0:04:47	

Figura 134

Reporte de respaldo, fecha 02.04.2023, tarea BK_Diario_VMs_Grupo2.

Backup job: BK_Diario_VMs_Grupo2								
Created by VANGUARDFRESH\adm_jmalca at 29/11/2021 16:42.								
domingo, 2 de abril de 2023 03:30:15								
Success	5	Start time	03:30:15	Total size	750 GB	Backup size	67.5 GB	
Warning	0	End time	03:48:29	Data read	98.5 GB	Dedupe	8.3x	
Error	0	Duration	0:18:14	Transferred	67.5 GB	Compression	1.0x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRVICNISAPPROD	Success	03:32:02	03:37:15	100 GB	16 GB	12.6 GB	0:05:13	
SRVICNISWEB	Success	03:32:02	03:36:58	100 GB	13.5 GB	10.7 GB	0:04:56	
SRVICNISTAREO	Success	03:32:02	03:36:04	200 GB	18.8 GB	13 GB	0:04:02	
SRVICNISCAMPO	Success	03:32:07	03:38:38	150 GB	15.1 GB	9.4 GB	0:06:31	
SRVICNISPACK_QA	Success	03:35:32	03:40:36	200 GB	35.1 GB	21.7 GB	0:05:04	

Capítulo IV. Análisis y discusión de resultados

4.1. Cumplimiento del primer objetivo específico

El primer objetivo específico definido en el presente trabajo es Dimensionar un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa, cuyo indicador de logro es Diagrama de diseño de la arquitectura del sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa.

Para el cumplimiento de este indicador de logro se realizó el cálculo del espacio requerido para el sistema de almacenamiento principal y del almacenamiento de respaldo, tal como se muestra en el subcapítulo 3.2.1. Luego se realizó el cálculo de consumo de IOPS de las máquinas virtuales requeridas para la implementación de la solución, la cual se muestra en el subcapítulo 3.2.2. También se realizó una validación de los equipos de comunicaciones existentes en función de los requerimientos de la solución propuesta tal como se muestra en el subcapítulo 3.2.3.

Finalmente, se elaboró la arquitectura del sistema de almacenamiento de alta disponibilidad tal como se muestra en el subcapítulo 3.2.4 con lo cual cumplimos al 100% con el primer objetivo específico.

4.2. Cumplimiento del segundo objetivo específico

El segundo objetivo específico definido en el presente trabajo es “Implementar un sistema de almacenamiento de alta disponibilidad para la empresa Agrícola Challapampa”, cuyo indicador de logro es: “Implementación del 100% del sistema de almacenamiento para la empresa Agrícola Challapampa”. Para el cumplimiento de este indicador de logro se realizó las especificaciones técnicas generales de la solución a implementar tal como se muestra en el subcapítulo 3.2.5, la cual sirvió de base para realizar la selección de la solución mediante una tabla de comparación técnica entre diversas marcas como se muestra en el subcapítulo 3.3. Luego pasamos a la etapa de la implementación física de

los sistemas de almacenamiento (subcapítulo 3.4.1), cableado de red (subcapítulo 3.4.2), configuración lógica de los puertos físicos de los *switches* HPe (subcapítulo 3.4.3), configuración lógica de los servidores ESXi (subcapítulo 3.4.4), configuración de los sistemas de almacenamiento principal y de respaldo (subcapítulo 3.4.5), migración de las máquinas virtuales (subcapítulo 3.4.6) y finalmente la configuración del servidor de respaldo (subcapítulo 3.4.7).

Por lo tanto, concluimos que se ha cumplido al 100% con el segundo objetivo específico.

4.3. Cumplimiento del tercer objetivo específico

El tercer objetivo específico definido en el presente trabajo es “Disminuir los tiempos de parada de los servicios y los tiempos de respaldos”, cuyos indicadores de logro son Disminuir en 80% los tiempos de parada de los servicios y Disminuir los tiempos de respaldo en 20%.

Para el cumplimiento del primer indicador de logro se realizó los cálculos de los tiempos de parada de la solución mediante una tabla comparativa del primer cuatrimestre del año 2022 (solución antigua) vs el primer cuatrimestre del año 2023 (solución actual), obteniendo una disminución del 86.25%, tal como se muestra en el subcapítulo 3.6.1, con lo cual se cumple el primer indicador de logro.

Para el cumplimiento del segundo indicador de logro se realizó los cálculos de los tiempos de los tiempos de respaldo mediante una tabla comparativa donde se consideró 23 días antes de implementar la solución vs 23 días después de implementar la solución, obteniendo una disminución del 22.15%, tal como se muestra en el subcapítulo 3.6.2, con lo cual se cumple el segundo indicador de logro.

En función a lo descrito se concluye que hemos cumplido al 100% con el tercer objetivo específico propuesto.

Conclusiones

A continuación, se describe las siguientes conclusiones del presente trabajo:

- De las pruebas de testeo de la solución se concluye que toda solución debe tener tarjetas físicas redundantes para mantener la continuidad de los servicios.
- El respaldo vía SAN ayuda a mejorar las ventanas de los tiempos de respaldos.
- La solución de virtualización de *VMware vSphere* es una de las soluciones más completas en el mercado que permite usar de manera eficiente los recursos de un servidor físico y brindar alta disponibilidad.
- Toda red SAN permite tener una arquitectura IT redundante y nos ayuda a minimizar los tiempos de corte de los sistemas.
- Luego de realizar la migración de máquinas virtuales a las LUN del sistema de almacenamiento se concluye que este sistema ofrece tasas de deduplicación / compresión altas, permitiendo ahorrar espacio eficaz en disco.
- El sistema de almacenamiento *HPe StoreOnce* posee un algoritmo eficaz para deduplicar datos tal como se muestra en la interfaz web de administración del sistema de almacenamiento (Fig. 3.46). Gracias a este ahorro de espacio, se podrá almacenar data histórica o alguna otra información relevante para la empresa.

Recomendaciones

Después de desarrollar el presente trabajo, se plantean las siguientes recomendaciones:

- Realizar la automatización de los reportes de tiempos de parada de la solución existente para agilizar la toma de decisiones de la empresa.
- Revisar anual del cableado LAN/SAN. Esto ayudará a detectar posibles errores de comunicación de los servidores con el sistema de almacenamiento principal.
- Disponer de un *dashboard* donde se monitoree el estado de salud de la infraestructura de IT. Esto ayudará a tomar acciones correctivas en el menor tiempo posible en caso se presente algún problema con la solución.
- Realizar un mantenimiento preventivo anual para todos los componentes que forman parte de la infraestructura de IT. Esto ayudará a alargar los tiempos de vida de los equipos y prevenir posibles fallas.
- Actualizar el *firmware* de manera periódica de los dos sistemas de almacenamiento.
- Habilitar los *snapshot* de las LUN a nivel del sistema de almacenamiento principal *HPe Nimble*. Esto es por motivo de tener alguna contingencia en caso exista alguna corrupción de datos en los *datastores* de *VMware*.
- Realizar una segunda copia de los respaldos de las máquinas virtuales en otra sede.

Referencias bibliográficas

- Andréu, J. (2011). *Redes Locales*. Edicion Editex
- Aragón, J. M. (2006). *Almacenamiento Distribuido basado en red (III) Almacenamiento SAN por red TCP/IP*. cuchillac.net. http://cuchillac.net/archivos/pre_ipv6/3_san-nas/lects/lect1_almacenamiento_SAN.pdf
- Blanco, F. (2020). *Diseño de un modelo de virtualización para la implementación de un sistema de servidores en alta disponibilidad* [Tesis de licenciatura, Universidad Cooperativa de Colombia]. Repositorio Institucional UCC.
- Blanco, M. (2023). Sistemas de alta disponibilidad. *Télématique Revista Electrónica de Estudios Telemáticos*, 2(1), 32-41. <https://dialnet.unirioja.es/servlet/articulo?codigo=2968181>
- Brown, M. y Cartwright, H. (2019). *VMware vSphere 6.7 Data Center Design Cookbook*. Packt Publishing.
- Castillo, J. I. (2019). *Redes de datos*. Samsara.
- Childerhose, C. (2022). *Mastering Veeam Backup & Replication*. Packt Publishing.
- Chumbimuni, G. (2018). *Implementación del sistema de recuperación ante desastres de la infraestructura de un Data Center hacia un centro de respaldo*. [Tesis de licenciatura, Universidad Nacional de Ingeniería]. Repositorio Institucional UNI.
- Cisco Networking. (2020). *Introduction to Networks Companion Guide (CCNAv7)*. Pearson.
- Costa Ramos, J. (2019). *Seguridad y Alta disponibilidad*. RA-MA.
- De la Rosa, R (2014). *Virtualización con VMware vSphere*. Doc player. <https://docplayer.es/679778-Virtualizacion-con-vmware-vsphere.html>
- Dordoigne, J. (2015). *Redes Informáticas*. Ediciones ENI.
- European Knowledge Center for Information Technology. (2022, diciembre). *Copias de seguridad (backup): ¿cómo recuperar los datos en caso de pérdida?* TIC Portal. <https://www.ticportal.es/glosario-tic/copia-seguridad-backup>.
- Goel, A. y Corbett, P. (2012), *Paper Netapp RAID Triple Parity*. NetApp. https://www.netapp.com/pdf.html?item=/media/23403-RTP_Goel.pdf
- Hewlett Packard Enterprise. (2021, marzo). *HPE Nimble Storage Deployment Considerations for Networking*. Infosight HPe.

- https://infosight.hpe.com/InfoSight/media/cms/active/public/HPE_Nimble_Storage_Deployment_Considerations_for_Networking.pdf.
- Hewlett Packard Enterprise. (2022, junio). *HPE Nimble Storage Adaptive Flash Arrays*. HPe Docs. <https://www.hpe.com/psnow/doc/a00008274enw?ver=31>
- Hewlett Packard Enterprise. (2020, noviembre). *Deployments considerations for implementing HPe Nimble Storage witch Vmware vSphere 7*. HPe Docs. <https://www.hpe.com/psnow/doc/a00104406enw>
- Hoskings, J. (2005). *Exploring IBM server & storage technology (6ta ed.)*. Maximum Press
- Liberatori, M. (2018). *Redes de Datos y sus Protocolos*. Universidad Nacional de Mar de Plata Argentina. Eudem.
- López, F. (2015). *Sistemas distribuidos*. Universidad Autónoma Metropolitana.
- López, R. (2018). *Enrutamiento y configuración de redes*. Fundación Universitaria del Área Andina Colombia.
- Lowe, D. (2021). *Networking all in one. For Dummies*.
- Morales, A. (2018). *Implementación del sistema de recuperación ante desastres de la infraestructura de un Data Center hacia un centro de respaldo* [Tesis de licenciatura, Universidad Nacional de Ingeniería]. Repositorio UNI.
- Niño, D. (2020). *Diseño de un modelo de virtualización para la implementación de un sistema de servidores en alta disponibilidad*. [Tesis de licenciatura, Universidad Cooperativa de Colombia]. Repositorio Institucional UCC.
- Parziale, L., Britt, D., Davis, C., Forrester, J., Liu, W., Matthewa, C., Rosselot, N. (2006). *TCP/IP Tutorial and Technical Overview*. IBM Redbooks. <https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf>
- Piper, B. (2017), *Learn Cisco Network Administration in a Month of Lunches*. Manning.
- Shakil, T., Jain, V. y Louis, Y. (2019). *LISP Network Deployment and Troubleshooting*. Cisco Press. <https://www.ciscopress.com/store/lisp-network-deployment-and-troubleshooting-the-complete-9780134783161>
- Stallings, W. (2006). *Organización y arquitectura de computadores*. Pearson Educación.
- Stallings, W. (2000). *Comunicaciones y Redes de Computadores*. Pearson Educación.
- Tate, J., Beck, P., Ibarra, H., Kumaravel, S., Miklas, L. (2018). *IBM Reebok Introduction to Storage Area Networks*. IBM Redbooks. <https://www.redbooks.ibm.com/abstracts/sg245470.html>

- Tello, V. (2018). *Diseño de redes de campus utilizando tecnología de virtualización* [Tesis de licenciatura, Universidad Nacional de Ingeniería]. Repositorio Institucional UNI.
- Tintín, V., Caiza, J. y Caicedo, F. (2018). Arquitectura de Redes de Información. *Dominio de las Ciencias*, 4(2), 103-122, https://www.researchgate.net/publication/336003479_Arquitectura_de_redes_de_informacion_Principios_y_conceptos
- Varghese, G. y Xu, J. (2022). *Network Algorithmics*. Morgan Kaufmann.
- Varshney, S. (2020, mayo). *What are Virtual Switches and Standard Switches?*. C#Corner. <https://www.c-sharpcorner.com/article/what-is-virtual-switches-and-standard-switches/>
- Vasquez, S. E. (2015). Tecnologías de almacenamiento de información en el ambiente digital. *e-Ciencias de la Información* 5(2), 1-19, <https://revistas.ucr.ac.cr/index.php/eciencias/article/view/19762/20095>
- Veeam Software. (2023). *User Guide for VMware vSphere ESXi*. Veeam. https://www.veeam.com/veeam_backup_12_user_guide_vsphere_pg.pdf
- VMware. (2010, mayo). *SAN System, Design and Deployment Guide*. VMware Docs. https://www.vmware.com/pdf/vsp_4_san_design_deploy.pdf
- VMware. (2023, julio). *VMware vSphere ESXi 8.0*. VMware Docs. <https://docs.vmware.com/es/VMware-vSphere/8.0/rn/vmware-vsphere-80-release-notes/index.html>
- VMware. (2023, setiembre). *Almacenamiento de vSphere - VMware vSphere ESXi 8.0*. VMware Docs. <https://docs.vmware.com/es/VMware-vSphere/8.0/vsphere-esxi-vcenter-801-storage-guide.pdf>
- Watts, D. (2023, octubre). *Lenovo ThinkSystem SR550 Server (Xeon SP Gen 1/ Gen 2)*. Lenovo Press. <https://lenovopress.lenovo.com/lp1046-thinksystem-sr550-server>
- Xing, L. (2021). *Article Construction of a New Network Information Resource Storage System*. IOPscience. <https://iopscience.iop.org/article/10.1088/1742-6596/2037/1/012073/pdf>