UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERIA

PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y

COMUNICACIONES

DISEÑO DE UN PLATAFORMA DE VIRTUALIZACIÓN DE

APLICACIONES PARA LA COOPERATIVA LOS ANDES

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR(ES)

Silva Arias, José David (0000-0002-0990-1089)

ASESOR

Rodriguez Gutiérrez, Alfredo Efraín (0000-0001-6246-049X)

Lima, 17 de febrero de 2020

DEDICATORIA:

A mis queridos padres, mi tía Olimpia y mi incansable tío Ángel.

AGRADECIMIENTOS

El presente trabajo tiene la misión de ayudarme a concluir el ciclo universitario iniciado el año 2013, asimismo ha logrado el poder tomar la problemática de una empresa y con ella elaborar un diseño factible y sustentable para la solución del mismo, esto conlleva horas de investigación y trabajo por mi persona, las cuales me han podido ayudar a crecer como persona y profesional.

El agradecimiento en esta parte se lo otorgare a mi padre que aun estando lejos de mi persona a sido la fuerza que me acompaña a seguir en el día a día y que lejos de atosigarme o criticarme por las decisiones que uno toma, ha sido el apoyo que uno necesitaba desde muy joven.

Por último, unas gracias a mi madre y enamorada que fueron de aquellas personas que, han sido siempre de las mas juiciosas durante el periodo del desarrollo de mi tesis, han sabido darme la mano en los momentos de flaqueza.

RESUMEN

El presente trabajo de tesis desarrolla el diseño de una plataforma de virtualización de aplicaciones que pueda atender usuarios locales, externos y móviles de una organización. Esta plataforma de virtualización será diseñada bajo el modelo de disposición en capas y siguiendo los estándares, recomendaciones y buenas prácticas de cada uno de los fabricantes que componen la solución, así como también de metodologías de trabajo como la Gestión de puntos finales unificados (UEM- Unified endpoint management).

En el primer capítulo del presente diseño, hablaremos a grandes rasgos de la organización objetivo en el cual se desea plasmar dicho proyecto, así como la situación problemática en el campo de acción de la organización, luego definiremos el objetivo general y sus respectivos objetivos específicos e indicadores.

En el segundo capítulo, se presentará el marco teórico, el cual incluirá toda la información referente a las definiciones, normativa y metodología a utilizar.

En el tercer capítulo, se realizará el análisis del problema a solucionar con el diseño a proponer, además se identificarán los problemas con la información recabada de la organización, con ello se elaborará el análisis del alcance, impacto y soluciones posibles.

En el cuarto capítulo, se mencionan a detalle las especificaciones del diseño multicapas de la plataforma de virtualización de aplicaciones. Y finalmente, se mostrarán los resultados y validaciones, los cuales servirán para demostrar el cumplimiento de los objetivos específicos planteados en el capítulo uno.

Palabras clave: Virtualización; Aplicaciones; Proxy Ica; HDX; Citrix Gateway.

ABSTRACT

This thesis work develops the design of an application virtualization platform that can serve local, external and mobile users of an organization. This virtualization platform will be designed under the layered layout model and following the standards, recommendations and good practices of each of the manufacturers that make up the solution, as well as work methodologies such as EMM (EMM - Enterprise Mobility Management) .

In the first chapter of the present design, we will speak in broad strokes of the objective organization in which it is desired to capture said project, as well as the problematic situation in the field of action of the organization, then we will define the general objective and its respective specific objectives and indicators.

In the second chapter, the theoretical framework will be presented, which will include all the information regarding the definitions, regulations and methodology to be used.

In the third chapter, the analysis of the problem to be solved with the design to be proposed will be carried out, in addition the problems will be identified with the information collected from the organization, with this the analysis of the scope, impact and possible solutions will be elaborated.

In the fourth chapter, the multilayer design specifications of the application virtualization platform will be mentioned in detail. And finally, the results will be displayed and validations, which will serve to demonstrate compliance with the objectives specific ones raised in chapter one.

Keywords: Virtualization; Applications; Ica proxy; HDX; Citrix Gateway

TABLA DE CONTENIDOS

1. INTRODUCCIÓN	1
1.1 Motivación del tema	1
1.2 Organización Objetivo.....	2
1.3 Campo de Acción en la Organización Objetivo	3
1.4 Situación Problemática y Problemas en el Campo de Acción	6
1.4.1 Situación Problemática	6
1.4.2 Problemas a Resolver	7
1.5 Objetivos del Proyecto General y Específicos	8
1.5.1 Objetivo General.....	8
1.5.2 Objetivos Específicos	8
1.6 Indicadores o Mecanismos del Logro de los Objetivos.....	8
1.7 Justificación del Proyecto.....	9
1.7.1 Funcional	9
1.7.2 Tecnológico	9
1.7.3 Económico	10
1.8 Estado del Arte	10
1.8.1 Conceptos Básicos de una Infraestructura de Virtualización de Aplicaciones	10
1.8.2 Virtualización de Aplicaciones en la Actualidad	12
CAPÍTULO 2. MARCO TEÓRICO	20
2.1 ¿Cómo Funciona la Virtualización?	21
2.2 Tipos de Virtualización	21
CAPÍTULO 3. DEFINICIÓN DEL PROBLEMA Y TOMA DE REQUERIMIENTOS	26
3.1 Análisis del problema	26
3.2 Identificación del problema	26
3.2.1 Modelo carente de un sistema de administración y supervisión centralizado.....	27
3.2.2 Gastos en infraestructura local desplegada en sucursales	29
3.2.3 Bajo desempeño de la aplicación en uso	30
3.2.4 Servidores de acceso a aplicaciones saturados en su capacidad de trabajo.....	33
3.2.5 Acceso externo inseguro.....	34

3.2.6 Diseño carente de alta disponibilidad	35
3.3 Relación entre el problema y las causas que lo originan	37
3.4 Evaluación de impacto en la organización	38
3.5 Soluciones Posibles	45
3.6 Toma de Requerimientos.....	47
3.7 Registro De Interesados.....	49
3.8 Estructura de descomposición del trabajo (EDT).....	51
CAPÍTULO 4. DISEÑO DE PROPUESTA DE SOLUCIÓN.....	52
4.1 Análisis de tecnología de virtualización de aplicaciones	52
4.2. Infraestructura Actual	54
4.2.1 Configuración Clúster Vmware Vsphere	54
4.2.2 Configuración de almacenamiento	56
4.3 Diseño de Infraestructura Citrix Virtual Apps	57
4.4 Metodología del diseño: Arquitectura Conceptual.....	58
4.4.1 Modelo de Entrega.....	59
4.4.2 Topología de sitio	59
4.4.3 Estrategia de gestión de imágenes	60
4.4.4 Definición de grupos de usuarios	60
4.5 Metodología del diseño: Capa de usuarios	62
4.5.1 Propiedad de los dispositivos de punto final	63
4.5.2 Administración unificada de dispositivos de punto final (UEM).....	63
4.5.3 Selección de Workspace	64
4.6 Metodología del diseño: Capa De Acceso.....	65
4.6.1 Autenticación.....	66
4.6.1.1 Proveedor de autenticación.....	66
4.6.1.2 Punto de autenticación.....	67
4.6.1.3 Directiva de autenticación	68
4.6.2 StoreFront	70
4.6.2.1 Alta disponibilidad	70
4.6.2.2 Referencia del Delivery Controller.....	71
4.6.2.3 Balizas	71
4.6.2.4 Presentación de los recursos	72
4.6.2.5 Grupos de agregación	72

4.6.2.6 Escalabilidad.....	74
4.6.3 Citrix Gateway.....	75
4.6.3.1 Topología.....	75
4.6.3.2 Alta disponibilidad	76
4.6.3.3 Plataforma.....	77
4.6.3.4 Directiva de pre-autenticación.....	79
4.6.3.5 Directiva de sesión.....	81
4.6.3.6 Perfil de sesión	81
4.7 Metodología del diseño: Capa de recursos	82
4.7.1 Experiencia de usuario.....	83
4.7.1.1 Protocolo de visualización.....	83
4.7.1.2 Protocolo de transporte.....	84
4.7.1.3 Optimización de inicios de sesión	85
4.7.1.4 Configuraciones de directiva de presentación visual	86
4.7.1.5 Configuraciones del método criptográfico	87
4.7.2 Datos del usuario	88
4.7.3 Directivas.....	89
4.7.4 Impresión	90
4.7.5 Aplicaciones	91
4.7.6 Máquinas virtuales.....	92
4.8 Metodología de diseño: Capa de control	98
4.8.1 Active Directory	98
4.8.2 Base de datos	99
4.8.2.1 Edición.....	99
4.8.2.2 Tamaño del servidor de la base de datos	99
4.8.2.3 Tamaño de las instancias	101
4.8.5 Citrix Licensing Server.....	103
4.8.6 Delivery Controllers	104
4.9 Metodología del diseño: Capa de hardware	107
4.9.1 Separación de la carga de trabajo	107
4.9.2 Tamaño del almacenamiento	110
4.10 Metodología de recuperación VMware a Azure	113
4.10.1 Componentes de la arquitectura	113

4.10.2 Proceso de replicación	115
4.10.3 Proceso de conmutación por error y conmutación por recuperación	117
4.11 Dimensionamiento para el diseño de plataforma	118
4.11.1 Requerimientos Capa Cliente	119
4.11.2 Requerimientos Capa Acceso	119
4.11.3 Requerimientos Capa Control	121
4.11.4 Requerimientos Capa Recursos	122
4.11.5 Requerimientos Capa Hardware	124
4.11.6 Requerimiento Servicios Corporativos para la plataforma de acceso a las aplicaciones	124
4.11.6.1 Base de Datos	125
4.11.6.2 Active Directory	126
4.11.6.3 Licencias Terminal Server	128
4.11.6.4 Antivirus	128
4.11.7 Requerimientos de Infraestructura de Red	128
4.11.8 Requerimientos de Infraestructura de Licenciamiento	129
4.11.9 Requerimientos de Infraestructura de Backup.....	130
4.11.10 Representación gráfica	131
4.12 Análisis económico en CAPEX de la solución propuesta.....	132
4.12.1 Estimación de costes hardware.....	132
4.12.2 Estimación de costes de licencias	132
4.12.3 Estimación de costes de certificados digitales.....	133
4.12.4 Estimación de costes de infraestructura de Backup.....	133
4.12.5 Resumen de costes.....	135
CAPÍTULO 5. PRUEBAS, RESULTADOS Y VALIDACIÓN	136
5.1 Evaluación de los resultados del diseño considerando el cumplimiento de la administración y supervisión centralizada según las buenas prácticas de virtualización...	136
5.1.1 Propósito de evaluación.....	136
5.1.2 Alcance de evaluación	136
5.2 Evaluación de los resultados de la optimización del desempeño de la aplicación considerando la mejora del rendimiento y un óptimo consumo de ancho de banda según las buenas prácticas de virtualización.	140
5.2.1 Propósito de evaluación.....	140

5.2.2 Alcance de evaluación	140
5.2.3 Tipos de pruebas	141
5.2.3.1 Pruebas retardo en el uso de la aplicación	141
5.2.3.2 Pruebas consumo ancho de banda	141
5.2.4 Recursos para las pruebas	142
5.2.4.1 Software	143
5.2.4.2 Hardware	143
5.2.5 Configuraciones de ambiente de pruebas	143
5.2.6 Casos de prueba	144
5.2.6.1 Retardo en el uso de la aplicación	144
5.2.6.2 Evaluación consumo ancho de banda	148
5.3 Evaluación de los resultados de la continuidad de acceso a la aplicación considerando la alta disponibilidad y seguridad a la solución según las buenas prácticas de virtualización	156
5.3.1 Propósito de evaluación	156
5.3.2 Alcance de evaluación	157
5.3.3 Tipos de pruebas	157
5.3.3.1 Pruebas de seguridad y continuidad de acceso	157
5.3.4 Recursos para las pruebas	158
5.3.4.1 Software	158
5.3.4.2 Hardware	158
5.3.5 Configuraciones de ambiente de pruebas	159
5.3.6 Casos de prueba	159
- CONCLUSIONES	178
- RECOMENDACIONES	180
- BIBLIOGRAFÍA	181
- GLOSARIO	187
- SIGLARIO	189
- ANEXOS	190

ÍNDICE DE TABLAS

Tabla 1	<i>Áreas beneficiadas con el proyecto</i>	4
Tabla 2	<i>Objetivo e indicadores del proyecto</i>	8
Tabla 3	<i>Tabla Objetivo Específico por Problema</i>	26
Tabla 4	<i>Resumen de tipo de acceso a aplicaciones</i>	27
Tabla 5	<i>Lista de sistemas operativos de host por sede</i>	28
Tabla 6	<i>Lista de principales tareas de TI</i>	29
Tabla 7	<i>Infraestructura local por sede</i>	30
Tabla 8	<i>Aplicaciones utilizadas</i>	31
Tabla 9	<i>Categorización de aplicaciones</i>	32
Tabla 10	<i>Matriz de causa e impacto del problema</i>	37
Tabla 11	<i>Consumo Total Aproximado por sede</i>	41
Tabla 12	<i>Latencia Aproximada por sede</i>	42
Tabla 13	<i>Gastos ocasionados por tipo de línea</i>	43
Tabla 14	<i>Gastos ocasionados en optimizadores de BW</i>	44
Tabla 15	<i>Gastos ocasionados en UTM</i>	45
Tabla 16	<i>Soluciones seleccionadas</i>	46
Tabla 17	<i>Resumen de objetivos específicos y requerimientos</i>	48
Tabla 18	<i>Registro de interesados</i>	49
Tabla 19	<i>Comparativa de tecnologías de virtualización</i>	52
Tabla 20	<i>Servidores presentes en la organización</i>	54
Tabla 21	<i>Resumen de problemas y capas del diseño</i>	58
Tabla 22	<i>Usuarios por sucursal</i>	58
Tabla 23	<i>Segmentación de usuarios por nivel de seguridad</i>	60
Tabla 24	<i>Segmentación de usuarios por movilidad</i>	61
Tabla 25	<i>Segmentación de usuarios tipo de usuario</i>	62
Tabla 26	<i>Puntos de autenticación según tipo de usuario</i>	67
Tabla 27	<i>Puntos de autenticación según nivel de seguridad</i>	69
Tabla 28	<i>Puntos de autenticación según tipo de usuario</i>	74
Tabla 29	<i>Características diseño Storefront</i>	74
Tabla 30	<i>Asignación CPU virtual según carga de trabajo</i>	94
Tabla 31	<i>Asignación CPU virtual según carga de trabajo</i>	95
Tabla 32	<i>Asignación Cache disco según carga de trabajo</i>	96
Tabla 33	<i>Asignación caché en RAM según carga de trabajo</i>	96
Tabla 34	<i>Asignación IOPS disco según carga de trabajo</i>	97
Tabla 35	<i>Asignación espacio base de datos de sitio</i>	101
Tabla 36	<i>Asignación espacio base de datos de supervisión</i>	102
Tabla 37	<i>Asignación espacio base de datos de Povisioning Services</i>	102
Tabla 38	<i>Usuarios por núcleo según carga de trabajo</i>	107
Tabla 39	<i>Directriz de densidad por servidor</i>	108
Tabla 40	<i>Propiedades de las opciones de almacenamiento</i>	110
Tabla 41	<i>Atributos por tipo de RAID</i>	111
Tabla 42	<i>Ejercicio de cálculo de procesamiento de red</i>	112
Tabla 43	<i>Componentes de Arquitectura Azure Site Recovery</i>	113

Tabla 44	<i>Roles de XenApp</i>	118
Tabla 45	<i>Especificaciones Citrix Gateway VPX Requeridos</i>	120
Tabla 46	<i>Citrix Storefront Requeridos</i>	121
Tabla 47	<i>Citrix Delivery Controller Requeridos</i>	121
Tabla 48	<i>Citrix License Server Requerido</i>	122
Tabla 49	<i>Consumo de aplicaciones</i>	123
Tabla 50	<i>Dimensionamiento catálogo Citrix Apps</i>	124
Tabla 51	<i>Recuento global recursos</i>	124
Tabla 52	<i>Dimensionamiento BBDD Citrix</i>	126
Tabla 53	<i>Dimensionamiento estructura AD Citrix</i>	127
Tabla 54	<i>Dimensionamiento Perfiles Citrix</i>	127
Tabla 55	<i>Requerimientos de licenciamiento</i>	129
Tabla 56	<i>Dimensionamiento ASR.</i>	131
Tabla 57	<i>Costes de licencias.</i>	132
Tabla 58	<i>Costes de certificados digitales.</i>	133
Tabla 59	<i>Costes de uso de plataforma ASR.</i>	134
Tabla 60	<i>Resumen de costes diseño de plataforma</i>	135
Tabla 61	<i>Matriz para el objetivo específico nro. 1</i>	136
Tabla 62	<i>Recuento global recursos plataforma Citrix y Azure</i>	137
Tabla 63	<i>Recuento recursos disponibles en la organizacion</i>	137
Tabla 64	<i>Matriz de recursos a nivel de hardware y software.</i>	138
Tabla 65	<i>Tabla de compatibilidad de aplicaciones</i>	139
Tabla 66	<i>Matriz para el objetivo específico nro. 2</i>	140
Tabla 67	<i>Software utilizado para los planes de Pruebas del Objetivo Específico 2.</i>	143
Tabla 68	<i>Hardware utilizado para el plan de pruebas del Objetivo Especifico 2.</i>	143
Tabla 69	<i>Configuración de ambiente para Objetivo Especifico 2.</i>	143
Tabla 70	<i>Consumo Recursos Aplicaciones ERP</i>	149
Tabla 71	<i>Consumo Recursos Aplicaciones Multimedia</i>	149
Tabla 72	<i>Consumo Recursos Aplicaciones ERP con EDT</i>	151
Tabla 73	<i>Consumo Recursos Aplicaciones ERP con MDRLE</i>	152
Tabla 74	<i>Consumo Recursos Aplicaciones ERP con EDT y MDRLE</i>	153
Tabla 75	<i>Consumo Recursos Aplicaciones ERP con ECC</i>	153
Tabla 76	<i>Consumo Recursos Aplicaciones ERP con Profundidad de color preferida</i>	154
Tabla 77	<i>Consumo Recursos Aplicaciones ERP con Profundidad de color preferida</i>	154
Tabla 78	<i>Consumo Recursos Aplicaciones ERP con Calidad Visual</i>	155
Tabla 79	<i>Consumo Recursos Aplicaciones ERP optimizado</i>	155
Tabla 80	<i>Matriz para el objetivo específico nro. 3</i>	156
Tabla 81	<i>Software utilizado para Pruebas del objetivo específico 3.</i>	158
Tabla 82	<i>Hardware utilizado para Pruebas del objetivo específico 3.</i>	158
Tabla 83	<i>Configuración de ambiente para el objetivo específico 3.</i>	159
Tabla 84	<i>Caso de uso 1 para el plan de pruebas de seguridad de acceso.</i>	159
Tabla 85	<i>Caso de uso 2 para el plan de pruebas de continuidad de acceso.</i>	161
Tabla 86	<i>Caso de uso 3 para el plan de pruebas de continuidad de acceso</i>	162
Tabla 87	<i>Caso de uso 4 para el plan de pruebas de continuidad de acceso.</i>	163
Tabla 88	<i>Caso de uso 5 para el plan de pruebas de continuidad de acceso.</i>	163
Tabla 89	<i>Caso de uso 6 para el plan de pruebas de continuidad de acceso</i>	164
Tabla 90	<i>Caso de uso 7 para el plan de pruebas de continuidad de acceso</i>	165
Tabla 91	<i>Caso de uso 8 para el plan de pruebas de continuidad de acceso</i>	166
Tabla 92	<i>Caso de uso 9 para el plan de pruebas de continuidad de acceso</i>	167

Tabla 93	<i>Caso de uso 10 para el plan de pruebas de continuidad de acceso.....</i>	167
Tabla 94	<i>Ejecución de pruebas de caso de uso nro. 1 para el O.E. 3.....</i>	168
Tabla 95	<i>Ejecución de pruebas de caso de uso nro. 2 para el O.E. 3.....</i>	169
Tabla 96	<i>Ejecución de pruebas de caso de uso nro. 3 para el O.E. 3.....</i>	169
Tabla 97	<i>Ejecución de pruebas de caso de uso nro. 4 para el O.E. 3.....</i>	169
Tabla 98	<i>Ejecución de pruebas de caso de uso nro. 5 para el O.E. 3.....</i>	170
Tabla 99	<i>Ejecución de pruebas de caso de uso nro. 6 para el O.E. 3.....</i>	170
Tabla 100	<i>Ejecución de pruebas de caso de uso nro. 7 para el O.E. 3.....</i>	170
Tabla 101	<i>Ejecución de pruebas de caso de uso nro. 8 para el O.E. 3.....</i>	171
Tabla 102	<i>Ejecución de pruebas de caso de uso nro. 9 para el O.E. 3.....</i>	171
Tabla 103	<i>Ejecución de pruebas de caso de uso nro. 10 para el O.E. 3.....</i>	171
Tabla 104	<i>Resultados para el caso de uso nro. 1 del O.E. 3.....</i>	172
Tabla 105	<i>Resultados para el caso de uso nro. 2 al 9 del O.E. 3</i>	176

ÍNDICE DE FIGURAS

<i>Figura 1.</i> Infraestructura de red de la data center en donde se implementará el proyecto, elaboración propia. Adaptado de “Plano general de red de la sede Central de Cooperativa Los Andes”, elaboración propia.	5
<i>Figura 2.</i> Infraestructura de red de la organización en donde se implementará el proyecto, elaboración propia. Adaptado de “Plano general de red sedes Cooperativa Los Andes”, elaboración propia.	5
<i>Figura 3.</i> Diagrama de componentes principales de una implementación típica, que se denomina “sitio”. Adaptado de “XENAPP Y XENDESKTOP 7.15 LTSR Información técnica general”, por Citrix, 2020.....	10
<i>Figura 4.</i> Representación de la arquitectura docker. Adaptado de “Docker: let’s ship your application” por Medium, 2018.....	17
<i>Figura 5.</i> Representación de un esquema MSIX. Adaptado de “What is MSIX?” por Microsoft, 2019.	18
<i>Figura 6.</i> Representación de la nueva arquitectura de Docker después de compilarla en runC y containerd. Adaptado de “Docker vs CRI-O vs Containerd” por Computing for Geeks, 2019.	19
<i>Figura 7.</i> Diagrama de servicios tradicionales. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.....	20
<i>Figura 8.</i> Representación de un esquema de máquina virtual e hipervisor. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.....	21
<i>Figura 9.</i> Representación de un esquema de virtualización de datos. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.	22
<i>Figura 10.</i> Representación de un esquema de virtualización de escritorios. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.....	23
<i>Figura 11.</i> Representación de un esquema de virtualización de servidores. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.....	23
<i>Figura 12.</i> Representación de un esquema de virtualización de sistemas operativos. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.	24
<i>Figura 13.</i> Representación gráfica del tráfico de canal de bajada saturado. Adaptado de “Informe Métricas”, por Portal Axesat, 2020.....	32
<i>Figura 14.</i> Representación gráfica del reporte Latencia Enlaces Satelitales. Adaptado de “Informe Métricas”, por Portal Axesat, 2020.....	33
<i>Figura 15.</i> Representación de la red de producción Cooperativa Los Andes. Adaptado de “Plano general de red de la sede Central de Cooperativa Los Andes”, elaboración propia.	35
<i>Figura 16.</i> Representación del esquema de acceso a las apps. Adaptado de “Plano general de red de la sede Central de Cooperativa Los Andes”, elaboración propia.....	36
<i>Figura 17.</i> Representación del diagrama de conexión externa para el acceso a recursos. Adaptado de “Esquema de servicios publicados de Cooperativa Los Andes”, elaboración propia.	37
<i>Figura 18.</i> Representación del mapa de procesos de Cooperativa Los Andes. Adaptado de “Cooperación Entre Cooperativas”, por Cooperativa Los Andes, 2018.	39

<i>Figura 19.</i> Cuadrante mágico que representa la competencia entre los fabricantes Cuadrante mágico para herramientas de gestión de puntos finales unificados en el año 2019. Adaptado de “Magic Quadrant for Unified Endpoint Management”, por Gartner, 2019.....	47
<i>Figura 20.</i> Representación del EDT que se utilizara para el presente proyecto. Adaptado de “EDT del proyecto”, elaboración propia.	51
<i>Figura 21.</i> Infraestructura virtual, formada por un cluster de VMWare conformado por tres hosts. Adaptado de “Cluster VMWare vSphere”, elaboración propia.	55
<i>Figura 22.</i> Distribución de la infraestructura de storage HP en la organización. Adaptado de “Storage Producción”, elaboración propia.	56
<i>Figura 23.</i> Representación del modelo de diseño de cinco capas. Adaptado de “Citrix Provisioning 1912 Arquitectura”, por Citrix, 2019	57
<i>Figura 24.</i> Representación del modelo de entrega local. Adaptado de “Xenapp y XenDesktop 7.15 LTSR: Diseño”, por Citrix, 2020.	59
<i>Figura 25.</i> Representación de la vista sin grupos de agregación en el Citrix Storefront. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	73
<i>Figura 26.</i> Representación de la vista sin grupos de agregación en el Citrix Storefront. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	73
<i>Figura 27.</i> Representación de la topología de dos brazos con dos zonas desmilitarizadas (DMZ) separadas para aislar los flujos del tráfico front-end y back-end. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.....	76
<i>Figura 28.</i> Representación de las especificaciones de los modelos de Citrix VPX. Adaptado de “NetScaler VPX: Virtualizing the power of advanced web and application delivery and	79
<i>Figura 29.</i> Representación del diagrama de flujo de directivas de pre-autenticación para el cumplimiento de directrices de seguridad implementadas. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	80
<i>Figura 30.</i> Representación de la directiva de sesión del tipo HDX Proxy. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.....	82
<i>Figura 31.</i> Representación del Inicio Sesión Clásico en Citrix Apps. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	85
<i>Figura 32.</i> Representación del Inicio Sesión con el agente WEM. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	86
<i>Figura 33.</i> Tabla de recomendaciones de tamaños de clave por la NIST (Instituto Nacional de Estándares y Tecnología) Adaptado de “Recommendation for Key Management”, por NIST, 2016.	88
<i>Figura 34.</i> Representación del enrutamiento del servidor de impresión de Windows (con el servidor de impresión universal). Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	91
<i>Figura 35.</i> Representación del esquema de interconexión NUMA. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	93
<i>Figura 36.</i> Representación del modelo de unidad organizativa recomendado por Citrix. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.....	98

<i>Figura 37.</i> Fórmula para determinar cantidad de Delivery Controllers Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.....	105
<i>Figura 38.</i> Fórmula de la carga de trabajo. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	108
<i>Figura 39.</i> Fórmula de la carga de trabajo. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.	109
<i>Figura 40.</i> Representación que muestra los componentes principales de la Arquitectura de recuperación ante desastres de VMware a Azure. Adaptado de “Arquitectura de recuperación ante desastres de VMware a Azure”, por Microsoft Azure, 2019.	115
<i>Figura 41.</i> Representación que muestra el proceso de replicación entre las VM de VMware al portal de Azure. Adaptado de “Arquitectura de recuperación ante desastres de VMware a Azure”, por Microsoft Azure, 2019.....	116
<i>Figura 42.</i> Representación que muestra el proceso de Conmutación por recuperación VMware desde Azure. Adaptado de “Arquitectura de recuperación ante desastres de VMware a Azure”, por Microsoft Azure, 2019.....	118
<i>Figura 43.</i> Representación que muestra los componentes principales de una implementación típica de Citrix Virtual Apps. Adaptado de “CITRIX VIRTUAL APPS AND DESKTOPS	118
<i>Figura 44.</i> Dimensionamiento Sitio Database. Adaptado de “XenDesktop 7 Database Sizing Tool”, elaboración propia.	125
<i>Figura 45.</i> Dimensionamiento Monitor Database. Adaptado de “XenDesktop 7 Database Sizing Tool”, elaboración propia.	126
<i>Figura 46.</i> Representación gráfica de la infraestructura de red propuesta en la sede Central en Lima, elaboración propia.	129
<i>Figura 47.</i> Componentes arquitectónicos del Azure Migrate Server Migration. Adaptado de “Arquitectura de migración basada en agente”, Microsoft Azure,2019.....	130
<i>Figura 48.</i> Requerimientos para el dimensionamiento de contingencia de plataforma virtual de aplicaciones. Adaptado de “Arquitectura de migración basada en agente”, Microsoft Azure,2019.	131
<i>Figura 49.</i> Representación gráfica de la infraestructura completa de virtualización de aplicaciones propuesta en la sede Central en Lima, elaboración propia.	132
<i>Figura 50.</i> Resumen de factibilidad económica del Azure Site Recovery tomando el costo por hora de uso. Adaptado de “Arquitectura de migración basada en agente”, Microsoft Azure,2019.	134
<i>Figura 51.</i> Línea de comandos WMI para el acceso a información RTT. Adaptado de “Habilitación de recursos WMI”, elaboración propia.	145
<i>Figura 52.</i> Resultado de consulta WMI para información RTT. Adaptado de “Habilitación de recursos WMI”, elaboración propia.	145
<i>Figura 53.</i> Simulación latencia con herramienta Clumsy. Adaptado de “Configuración de simulador de red Clumsy”, elaboración propia.	146
<i>Figura 54.</i> Código de consulta los valores ICA RTT y NetworkLatency. Adaptado de “Configuración de script vía Powershell”, elaboración propia.	146
<i>Figura 55.</i> Elaboración de script para la consulta secuencial. Adaptado de “Configuración de script vía Powershell”, elaboración propia.	146
<i>Figura 56.</i> Resultados de ejecución de script de tiempo de demora. Adaptado de “Configuración de script vía Powershell”, elaboración propia.	147

<i>Figura 57.</i> Verificación de RTT desde módulo Citrix Gateway. Adaptado de “Comprehensive Citrix HDX visibility powered by NetScaler Management and Analytics System”, por Citrix, 2017.	147
<i>Figura 58.</i> Pantalla de contadores del performance monitor en el servidor VDA a ser medido. Adaptado de “Evaluación Consumo Ancho de Banda”, elaboración propia.	148
<i>Figura 59.</i> Pestaña Configuración en la GUI Citrix ADC para habilitación de EDT. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia.	150
<i>Figura 60.</i> Pestaña Configuración básica para el servidor virtual VPN y habilitación de DTLS. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia.	151
<i>Figura 61.</i> Pestaña Configuración HDX Thinwire para habilitación de MDRLE. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia.	152
<i>Figura 62.</i> Claves de registro según la configuración de compresión con pérdida actual. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia.	153
<i>Figura 63.</i> Muestra de tabla con profundidad de color a 24 y 16 bits. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia.	154
<i>Figura 64.</i> Uso de certificado interno para acceder localmente a la plataforma de aplicaciones. Adaptado de “Acceso interno a la plataforma”, elaboración prueba.	173
<i>Figura 65.</i> Uso de certificado externo para acceder desde internet a la plataforma de aplicaciones. Adaptado de “Acceso externo a la plataforma”, elaboración prueba.	174
<i>Figura 66.</i> Uso de certificado externo para acceder desde un dispositivo móvil a la plataforma de aplicaciones. Adaptado de “Acceso móvil a la plataforma”, elaboración prueba.	175
<i>Figura 67.</i> Captura de tráfico de red en la comunicación entre cliente y el portal de aplicaciones. Adaptado de “Captura análisis de red”, elaboración prueba.	175

1. INTRODUCCIÓN

El presente proyecto tiene como tema principal la virtualización de aplicaciones core que utilizan en la Cooperativa Los Andes, esta tecnología nos permitirá aislar la aplicación del sistema operativo subyacente y con ello conseguir una mayor compatibilidad y movilidad.

Para conseguir esto se utilizan varias técnicas y software de diferentes fabricantes del mercado; aportando con ello a la organización mayor seguridad, disponibilidad y menores costos.

1.1 Motivación del tema

“En la actualidad, aunque las empresas están apostando por la nube, la virtualización tradicional es la infraestructura más común no sólo para las cargas de trabajo existentes, sino también para la implementación de nuevas aplicaciones” (Dawson, 2018). La tendencia de las empresas se orienta a simplificar el acceso a la información para lograr mayor eficiencia por parte del usuario final, ello de la mano con el acceso seguro a dicha información.

Para ello la virtualización de aplicaciones tiene la capacidad de ayudar al equipo de TI con las actualizaciones del sistema operativo y de la aplicación. Los usuarios pueden seguir accediendo a sus aplicaciones de la forma habitual cuando obtienen un dispositivo nuevo o cuando migran de sistema operativo. Anteriormente, el área de TI tenía que reconfigurar y reasignar las aplicaciones a cada máquina nueva o repotenciada, con ello la forma de funcionar de una aplicación tradicional vendría a ser menos atractiva en escenarios en los cuales el procesamiento local no es necesario. Los usuarios pueden seguir accediendo a sus aplicaciones de la forma habitual cuando obtienen un nuevo dispositivo o migran de sistema operativo. Anteriormente, el área de TI tenía que reconfigurar y reasignar las aplicaciones a cada máquina nueva o repotenciada, con ello la forma de funcionar de una aplicación tradicional vendría a ser menos atractiva en escenarios en los cuales el procesamiento local no es necesario.

Esto último se justifica en el caso de compañías pequeñas a medianas que posean sedes remotas con anchos de banda no estables y requieren servicios de TI que permitan la transaccionalidad de sus operaciones en tiempo real, por lo que funcionalidades que poseen actualmente la virtualización de aplicaciones garantizan que los empleados tengan una experiencia nativa dondequiera que se encuentren, incluso cuando las conexiones de red no sean las ideales y no se necesite de una infraestructura local.

“En efecto, la virtualización de aplicaciones proveen una reducción de esfuerzo administrativo, además de un aprovechamiento de la infraestructura actual de servidores y dispositivos finales, siendo esta una solución rentable, segura y confiable que permite administrar de manera eficiente la plataforma tecnológica con la que cuentan las organizaciones, mejorando la gestión, el desempeño de los recursos, la movilidad, la disponibilidad del servicio y aplicaciones, como su manejo dentro de tiempos más eficientes.” (Julian, 2016)

El resultado final de esta infraestructura es que los usuarios pueden acceder a sus datos y aplicaciones desde casi cualquier dispositivo, en cualquier lugar y a cualquier hora. Asimismo, proporciona mayor seguridad de datos, una migración de plataforma más sencilla, una mejor recuperación ante desastres y un nuevo aprovisionamiento de las aplicaciones en minutos en lugar de horas.

1.2 Organización Objetivo

Cooperativa Los Andes es una institución financiera fundada el 12 de febrero de 1994 como Caja Rural de Ahorro y Crédito, con el fin de brindar productos y servicios financieros accesibles, competitivos y confiables, dirigidos preferentemente al sector rural, y así mejorar la calidad de vida de los pobladores y contribuyendo con el desarrollo de la economía regional y nacional.

Forma parte de Los Andes Grupo Financiero, un importante conglomerado económico que opera en el mercado financiero y de capitales a través de empresas como Los Andes, Los Andes Fondos y Los Andes Bolsa, y opera en la Bolsa de Valores de Lima con el nemónico DIVIC1 y ha recibido el reconocimiento de esa organización por sus altos estándares de buena gobernanza en los concursos de Buen Gobierno Corporativo del 2008 y 2013.

La Fenacrep así como el Banco Central de Reserva del Perú regulan y supervisan el trabajo de Los Andes, que es miembro del Fondo de Seguros de Depósitos y de la Asociación de Instituciones de Microfinanzas del Perú.

Entre 2015 y 2019, Los Andes expandió sus operaciones de 7 a 15 sucursales en la región de Apurímac, contando con más de 310 colaboradores y presencia en 4 regiones del Perú a través de 15 puntos de atención.

Su fortaleza financiera le permitió obtener notas positivas con las calificadoras de riesgo especializadas, lo que ha convertido a Los Andes en una de las cooperativas más grandes del Perú.

En la actualidad, Los andes es una entidad líder, consolidada y especializada en el otorgamiento de créditos para microempresas, Pymes, banca personal y reinserción de comunidades andinas al sistema financiero.

a) Misión:

Garantizar la educación cooperativa, servicios financieros y complementarios adecuados a las necesidades de sus socios con una organización solidaria y autogestionaria.

b) Visión:

Ser una de las principales instituciones financieras líder en microfinanzas en el Perú, por su autenticidad cooperativa y solidez financiera.

c) Objetivo estratégico:

Contamos con notas positivas con clasificadoras de riesgo especializadas que nos ratifican como una empresa solvente y estable, lo que nos ha convertido en una de las instituciones microfinancieras más grandes del Perú, regulada y supervisada por la Superintendencia de Banca, Seguros y AFP – SBS, así como por el Banco Central de Reserva del Perú.

El 2016, Cooperativa Los Andes ha sido reconocida con un premio a sus buenas prácticas corporativas. Este galardón nos impulsa a seguir fortaleciendo nuestra cultura de buena gobernanza. En esta primera postulación han sido evaluados nuestros estándares de gestión corporativa entre los que se destacan: nuestro nivel de transparencia al ser una empresa privada y supervisada por los organismos reguladores del mercado financiero y de capitales, la sostenibilidad de nuestra clasificación de riesgo, la aplicación de auditorías altamente rigurosas, el fortalecimiento de nuestro ambiente de control y gestión de riesgos. Todo ello con la mira de ser una empresa bien gestionada para dar un mejor servicio a nuestros clientes, seguridad a nuestros depositantes, sostenibilidad a nuestros acreedores y valor para nuestros accionistas. Trabajamos para el bienestar de nuestros grupos de interés.

1.3 Campo de Acción en la Organización Objetivo

El campo de acción de este diseño de plataforma de virtualización de aplicaciones se desarrolla en el área de TI (Tecnologías de la Información) de la cooperativa Los Andes, el

cual se encarga de brindar todo el soporte tecnológico a la organización. El proyecto a diseñar será implementado en el centro de datos de la misma empresa ubicada en Lima.

Asimismo, las áreas involucradas en dicho proyecto serán las áreas interconectadas en sucursales, desde las cuales accederán desde sus terminales u otro dispositivo móvil que tengan acceso a internet.

En la siguiente tabla se muestra las diversas áreas según sucursales que se verán beneficiadas de acuerdo la sede en la cual se ubiquen.

Tabla 1
Áreas beneficiadas con el proyecto

Ítem	Sucursal	Áreas
1	OEP Lima (Datacenter)	Caja, Auditoria, Administración, Contabilidad, RRHH, TI, Finanzas
2	Agencia Aymaraes	Caja, Administración, Contabilidad, Finanzas
3	Agencia Abancay	Caja, Administración, Contabilidad, Finanzas
4	Agencia Andahuaylas	Caja, Administración, Contabilidad, Finanzas
5	Agencia Uripa	Caja, Administración, Contabilidad, Finanzas
6	Agencia Chuquibambilla	Caja, Administración, Contabilidad, Finanzas
7	Agencia Cotabambas	Caja, Administración, Contabilidad, Finanzas
8	Agencia Huancarama	Caja, Administración, Contabilidad, Finanzas
9	Agencia Huaccana	Caja, Administración, Contabilidad, Finanzas
10	Agencia Tintay	Caja, Administración, Contabilidad, Finanzas
11	Agencia Antabamba	Caja, Administración, Contabilidad, Finanzas
12	Agencia Curahuasi	Caja, Administración, Contabilidad, Finanzas
13	Agencia Cusco	Caja, Administración, Contabilidad, Finanzas
14	Agencia Huancavelica	Caja, Administración, Contabilidad, Finanzas
15	Agencia Santo Tomás	Caja, Administración, Contabilidad, Finanzas

Nota: Se presentan las agencias de la organización en todo el Perú, elaboración propia.

Asimismo, la base de datos para el acceso a servicios, servidores de autenticación de usuarios y equipos para usuarios finales se mantendrán en la sede principal, ya que actualmente cuenta con los recursos que dan abasto para el correcto funcionamiento de dicho entorno.

En la siguiente figura, se presenta la infraestructura de hardware actual con el que cuenta la organización en el centro de datos de la sede principal y sucursales en las cuales aún se dispone de recursos locales para el acceso y almacenamiento a la información.

Figura 1. Infraestructura de red de la data center en donde se implementará el proyecto, elaboración propia. Adaptado de “Plano general de red de la sede Central de Cooperativa Los Andes”, elaboración propia.

En la siguiente figura, se presenta la infraestructura de red actual entre sucursales y oficina principal.

Figura 2. Infraestructura de red de la organización en donde se implementará el proyecto, elaboración propia. Adaptado de “Plano general de red sedes Cooperativa Los Andes”, elaboración propia.

1.4 Situación Problemática y Problemas en el Campo de Acción

1.4.1 Situación Problemática

El plan de expansión territorial de cooperativa Los Andes obedece a una estrategia de ampliación del negocio cuya base es el mundo de las microfinanzas, hacia una entidad bancaria que pueda operar en todo el territorio.

Este proceso fue acompañado con la ampliación del número de sucursales en zonas clave como Cusco, Huancavelica y Apurímac, los problemas presentados en este proceso expansión han sido los siguientes:

1. Los accesos a las aplicaciones no son eficientes fuera de la red principal, el acceso remoto a dichos sistemas no se realiza de manera fluida y constante, lo cual genera inconsistencias con la data ingresada en los cierres de caja diarios. Esto obliga a que el responsable de cada sucursal tenga que enviar la data de forma manual a través de un disco externo con la información para poder consolidar la información.
2. Actualmente el área de TI mantiene el acceso externo provisionando infraestructura local en la sucursal, optimizadores de ancho de banda y cortafuegos para el acceso a los servicios es a través de una VPN por IPsec para el acceso y en las sedes con enlaces de internet satelitales se realiza vía escritorio remoto a la IP pública del servidor de aplicaciones, la cual demanda gastos en los costos de mantenimiento, licenciamiento y aprovisionamiento ante nuevos requerimientos.
3. La atención de incidencias se realiza desde la sede principal, donde el área de TI se encarga de revisar los problemas por pérdida de conexión al servidor de aplicaciones, asignar recursos a los nuevos hosts, actualizarla de manera manual luego del lanzamiento de nuevas versiones, verificar la compatibilidad de los componentes de las nuevas versiones con los hosts de su red local, todo ello genera un exceso de horas hombre al área de TI.
4. Las operaciones no pueden ser realizadas por la totalidad de equipos en simultáneo por la lentitud en el acceso a las mismas y se reparten las actividades hasta el cierre de caja diario, lo que en ocasiones genera un incremento de horas trabajadas por el personal de las sucursales.
5. Las aplicaciones se encuentran vulnerables a ataques por *ransomware* o *bitlockers* al encontrarse instaladas dentro de los hosts y no contar con políticas de concientización al usuario en el uso de recursos TI, asimismo debido a la alta rotación de personal en sucursales se han ubicado casos en los cuales se compromete el acceso y la integridad de la información.

Por último, tendríamos que agregar incidentes que corresponden a la pérdida o robo de algún dispositivo de la red empresarial.

6. Debido al crecimiento en su base de clientes tanto en nuestras localidades como fuera de ella, el personal se encuentra limitado al no poder acceder a sus aplicaciones desde sus dispositivos móviles, lo que los limita a solo trabajar desde la red empresarial.

7. Los servidores desde donde acceden actualmente se encuentran situados en la sede principal constando de un solo nodo desde el cual se despliega a la totalidad de usuarios, sin una solución de alta disponibilidad orientada a la aplicación implementada, asimismo las capacidades de dicho servidor han sido creadas para un dimensionamiento realizado hace 4 años.

8. El área de TI no realiza monitorizaciones e informes relacionados con la disponibilidad de las aplicaciones y sus componentes, lo que le impide establecer y comparar logros de disponibilidad según metas establecidas con las áreas que utilizan dichos recursos, para poder tomar medidas correctivas en lo que se requiere mejorar.

1.4.2 Problemas a Resolver

El presente diseño buscará resolver los siguientes problemas:

1. El área de TI carece de una plataforma de gestión centralizada desde la cual permita a todos los usuarios un único punto de entrada para mejorar las capacidades de control y supervisión, que a su vez reduzca los costes operacionales y de infraestructura.
2. El modelo de trabajo actual está expuesto a pérdida, fuga o corrupción de la información ya que carece de una visibilidad y de los controles de acceso necesarios para responder a las nuevas formas de trabajo de los usuarios.
3. Existen dificultades para identificar y solucionar problemas de acceso a las aplicaciones reportados por los usuarios. Esto debido a la proliferación de protocolos de red y productos que dificultan tener una visibilidad integral del tráfico de las aplicaciones, dilatando el tiempo de solución de problemas referidos con el rendimiento.
4. La actual plataforma utilizada cuenta con problemas de movilidad debido al crecimiento y la falta de recursos en sedes no les permite acceder a las aplicaciones corporativas críticas desde lugares diversos (redes de oficinas, redes de agentes, instalaciones del cliente).
5. El diseño actual no puede proporcionar un funcionamiento ininterrumpido de las aplicaciones, ya que cuenta con un solo nodo ante cualquier incidencia, asimismo carece de

una planificación de capacidades para asegurar que los recursos están en su lugar a medida que crecen las demandas de la red y de los dispositivos.

1.5 Objetivos del Proyecto General y Específicos

1.5.1 Objetivo General

Diseñar una solución de virtualización de aplicaciones desplegadas por el área de TI para el acceso a los usuarios tanto dentro como fuera del ámbito de la red empresarial de la cooperativa Los Andes. Para este diseño se está considerando las buenas prácticas de los fabricantes Citrix, Microsoft y VMWare.

1.5.2 Objetivos Específicos

1. OE1: Diseñar una plataforma de virtualización que permita la administración y supervisión centralizada según las buenas prácticas de virtualización.
2. OE2: Optimizar el desempeño de la aplicación, direccionando hacia un mejor rendimiento y un óptimo consumo de ancho de banda según las buenas prácticas de virtualización.
3. OE3: Proponer un diseño que brinde continuidad y seguridad de acceso a la plataforma según las buenas prácticas de virtualización.

1.6 Indicadores o Mecanismos del Logro de los Objetivos

En base a los objetivos específicos detallados en el capítulo anterior se plantean los siguientes indicadores de logro por objetivo específico.

Tabla 2

Objetivo e indicadores del proyecto

Objetivo Específico	Indicador de Logro	Métrica
Diseñar una plataforma de virtualización que permita la administración y supervisión centralizada según las buenas prácticas de virtualización.	Matriz de recursos a nivel de hardware y software requeridos para la centralización de aplicaciones.	Porcentaje de aplicaciones virtualizadas.
Optimizar el desempeño de la aplicación, direccionando hacia un mejor rendimiento y un óptimo consumo de ancho de banda según las buenas prácticas de virtualización.	Tiempos de acceso a la aplicación, obtención de reportes e impresión.	Ms
	Comparativas de saturación de los enlaces de ancho de banda en sedes.	Bits/s

Proponer un diseño que brinde continuidad y seguridad de acceso a la plataforma según las buenas prácticas de virtualización.	Capacidad de acceso externo de manera segura a la plataforma centralizada de aplicaciones.	Número de conexiones satisfactorias desde una red interna y externa.
	Cantidad máxima permitida de datos perdidos medidos en el tiempo y tiempo que tarda la restauración desde el incidente hasta que las operaciones normales estén disponibles (RPO y RTO)	Minutos

Nota: Se presentan los objetivos del proyecto con sus respectivos indicadores de logro y las métricas utilizadas para la medición de los mismos, elaboración propia.

1.7 Justificación del Proyecto

El entorno empresarial actual es muy dinámico y cambiante. Esto crea mayor presión en las empresas, puesto que tienen que buscar constantemente alternativas que ofrezcan al usuario una mejor experiencia que le permitan explotar al máximo el recurso humano y con ello lograr altos índices de eficiencia en el desarrollo de sus labores y que estas se vean reflejadas en mayores réditos económicos.

Por lo cual podríamos justificar dicha propuesta en tres aspectos:

1.7.1 Funcional

Esto debido a que el diseño le otorga un mayor control operacional al área de TI, permitiéndole simplificar las tareas de mantenimiento y administración al no necesitar una infraestructura TI adicional para dicha tarea. Todo ello permitirá la optimización de horas hombre para la gestión de los recursos.

Asimismo, el diseño busca brindarles accesos de forma segura y rápida a los usuarios externos a través de una plataforma correctamente dimensionada, los cuales impactarán en una mejora la productividad, ya que el usuario accederá a los recursos que necesite según el perfil que tenga asignado, y desde cualquier lugar.

1.7.2 Tecnológico

La virtualización de aplicaciones ofrece un sistema de entrega de aplicaciones de extremo a extremo para todas las aplicaciones de la organización, la centraliza a un entorno de aislamiento en el dispositivo de destino donde se ejecutarán, ayudando así, a optimizar la

productividad de tu empresa con acceso universal a información desde cualquier dispositivo, garantizando que la infraestructura de sistemas pueda acompañar el ritmo rápido de los cambios de la empresa. Asimismo, otorga interfaces más intuitivas, y menor coste de la infraestructura requerida.

1.7.3 Económico

Este aspecto se visualiza un menor costo para la entrega de aplicaciones ya que se van a optimizar los recursos con los que se cuenta tanto en hardware como licenciamiento, asimismo reducirá otros gastos indirectos que son el de energía eléctrica, refrigeración y mantenimiento, en sucursales se reducirá los gastos de planes de ancho de banda, infraestructura local y los gastos que estos conllevan.

Figura 3. Diagrama de componentes principales de una implementación típica, que se denomina “sitio”. Adaptado de “XENAPP Y XENDESKTOP 7.15 LTSR Información técnica general”, por Citrix, 2020.

1.8 Estado del Arte

1.8.1 Conceptos Básicos de una Infraestructura de Virtualización de Aplicaciones

La mayoría de las empresas planifican dentro de sus estrategias de mejoramiento de negocio, la adquisición de nuevos recursos computacionales, así como la administración de ellos, lo que permite evidenciar su crecimiento y desarrollo en el ámbito en el que se desenvuelven. Los avances innovadores relacionados con el hardware, como es la reducción del espacio que este ocupa, en comparación con las máquinas que se fabricaban años atrás y el incremento

de las capacidades de procesamiento de datos, de memoria y de almacenamiento. Estos factores son claves al momento de tomar decisiones por parte de la dirección y, por el otro, temas relacionados con la administración de las plataformas, la seguridad de la información, la escalabilidad y la normatividad regente.

Teniendo en cuenta los últimos puntos mencionados, además de la computación centralizada, la virtualización de aplicaciones soluciona en gran parte los inconvenientes que se presentan con respecto a ellos, ya que se administran las plataformas desde una única ubicación, de forma más segura y eficiente, teniendo bajo control temas como el del licenciamiento y el de las versiones del software, al contrario de la tendencia que hasta hace un par de años se veía en el mercado, donde lo que se pretendía era darle preferencia a la computación distribuida. Además, con la virtualización se tiene la posibilidad de tener sistemas limpios, con tiempos de despliegue superiores a los tradicionales; se pueden ejecutar varios sistemas operativos sobre el mismo hardware, mejorar la disponibilidad y el rendimiento de las aplicaciones y los servicios, tener una mejor respuesta ante incidentes de seguridad y desastres, mejorar los planes de continuidad del negocio, reducir costos a largo plazo, incrementar el periodo de vida de los recursos tecnológicos y, de paso, la eficacia energética y optimizar el esquema de administración de servidores.

Mencionaremos brevemente los beneficios más representativos que conllevan un esquema de virtualización de aplicaciones:

- Consolidación de servicios: para las organizaciones, la reducción de costos es un tema primordial que siempre se debe tener en primer plano. Mediante la virtualización, las empresas se encuentran llevando a cabo tareas de centralización de servicios en hardware de menor costo, pero del cual se obtiene máximo provecho de sus capacidades al tener un solo servidor en el que corren múltiples instancias.
- Optimización de cargas de trabajo: la virtualización favorece la eficiencia de los sistemas al entregar dinámicamente los recursos solicitados por las aplicaciones, esto gracias a que todos los recursos se encuentran compartidos y son administrados por el hipervisor quien determina los niveles de exigencia del hardware y su asignación.
- Facilidad de administración: al reducir la complejidad en la administración de los sistemas debido al incremento en la compatibilidad, genera una gran repercusión en el entorno, siendo mucho más simple la recuperación de los servicios ante desastres o la preparación de nuevos servicios.

1.8.2 Virtualización de Aplicaciones en la Actualidad

“Hoy en día, la virtualización de aplicaciones es una solución madura con sus propios beneficios y desventajas. En el mundo actual, la virtualización de aplicaciones en la empresa está dominada por Microsoft (App-V), VMWare ThinApp y Citrix Xenapp. Asimismo, de un tiempo acá otras soluciones como Spoon y Numecent han venido ganando terreno, eso sí enfocándose en áreas como BYOD y SaaS, resumiendolo en siete soluciones de virtualización de aplicaciones diferentes las cuales están vivas y activas en este segmento de la industria.

Enterprise Mobility, BYOD, Consumerización de TI, Big Data, Cloud Computing, Cloud Management Solutions, Dynamic Datacenter y Software Defined Datacenter son las principales tendencias en la industria de TI actual. La virtualización se incorpora en varias de estas tendencias.

Application and Desktop Delivery es un proceso que tiene el objetivo de ofrecer aplicaciones independientes de la ubicación y el dispositivo, para que los usuarios puedan trabajar en el sitio, en línea, fuera del sitio, fuera de línea, en cualquier lugar, con cualquier dispositivo de la empresa o propio y en cualquier momento. La entrega dinámica de aplicaciones es una funcionalidad esencial y parte de una estrategia más amplia de un escritorio optimizado.

Empoderar al usuario final al dar acceso a las aplicaciones de Windows, Web y Mobile para que pueda acceder a los datos y sistemas de información desde los centros de datos públicos y privados, independientemente del dispositivo o la ubicación, es el objetivo estratégico final para las empresas de hoy.

En la mayoría de las infraestructuras empresariales, la mayoría de las aplicaciones son de arquitectura web o basadas en Windows. La proporción de aplicaciones Web vs. Windows está cambiando y depende de la vertical (se usa la palabra vertical para describir el proceso de conversión de cifras monetarias a porcentajes), el cliente, el historial, el legado, la innovación y el control del desarrollo de aplicaciones. Las aplicaciones clásicas de Windows son el nuevo tipo de aplicaciones heredadas y durarán los próximos 20 años. Las aplicaciones de Windows se instalan (de forma manual, automática o integradas en la imagen base) o se virtualizan.” (Spruijt, 2013)

1.8.3 SOLUCIONES PARA LA VIRTUALIZACIÓN DE APLICACIONES

- Stream to Client, este tipo de escenario se utiliza cuando se tiene gran cantidad de usuarios y no se cuenta con el hardware requerido, este consiste en colocar las aplicaciones en perfiles y almacenarlas en un servidor de archivos de forma que cuando se inicia, este utiliza recursos del cliente, los archivos necesarios para ejecutar la aplicación se transmiten al dispositivo del usuario. Como por ejemplo el software App-V de Microsoft.

- Stream to Server, consiste en la entrega de aplicaciones virtuales a demanda, que se trata de conectar a los usuarios con las aplicaciones que están en servidores para que hagan uso de ellas de forma remota. Como por ejemplo XenApp, de Citrix, o Horizon Apps, de VMware. (Fernández, 2017)

A continuación, se va a detallar lo que interesa para este diseño de cada uno para poder determinar cuál es el más adecuado, no solo por el coste sino por los beneficios técnicos y funcionales que aportará al diseño.

1.8.3.1 STREAMED TO CLIENT

Microsoft App-V

“Se trata de una plataforma propia, compuesta por las funciones Cliente-Servidor-Secuenciador, que forma parte de “Microsoft Desktop Optimization Pack (MDOP)” y permite que las aplicaciones estén disponibles para los usuarios finales sin instalarlas directamente en sus equipos. Su funcionamiento se basa en transformar, mediante un proceso de grabación, las aplicaciones en servicios administrados centralmente, que se publican en un servidor Central, y se distribuye a los clientes de forma que nunca se instalan en sus equipos y no entran en conflicto con otras aplicaciones.

Lo significativo del producto se encuentra en su sencillez, a pesar de requerir un despliegue de una plataforma propia constituida por 3 componentes:

- Cliente; software que es necesario instalar en los equipos de los usuarios para que se realice la sincronización con el servidor.
- Secuenciador; equipo en donde se graba la secuencia de instalación para que genere el paquete que contendrá todas las librerías y ficheros necesarios para su instalación.
- Management and Publishing; servidor que contiene la consola en donde se registran los paquetes que se han creado y se distribuyen a los clientes.

Ahora bien, el gran problema, en cuanto al funcionamiento, que presenta este producto para las necesidades que se buscan es lo que lo hacen bueno, su sencillez y, por lo tanto, sus limitaciones de secuenciación. La gestión del entorno se limita en publicar una serie de paquetes, en formato “*.appv”, para que estos se descarguen en todos los clientes configurados, no permitiendo realizar un control ni ninguna otra acción. Además, todo el peso y funcionamiento recae sobre el PC del cliente de forma que estos equipos son indispensables, de manera que se pueden producir errores puntuales lo que obligaría a realizar una asistencia técnica presencial.” (Fernández, 2017)

Por otro lado, como ya se ha dicho, el producto se basa en la distribución de unos paquetes que hay que secuenciar cada vez que haya que aplicar un cambio, con el trabajo añadido que ello implica, y que su limitación en dicho proceso impide secuenciar o empaquetar cualquier aplicación o requisito. Esto obligaría, como mínimo, a que las máquinas de los clientes cumplan con una serie de requisitos mínimos en cuanto a software para que este método funcione correctamente.

Por último, otro gran inconveniente, a parte del funcionar ya comentado, es su adquisición o licenciamiento, ya que a pesar de ser un producto “aparentemente” gratuito, se requiere ser un cliente con licenciamiento por volumen de acuerdo al sistema operativo sobre el cual esté montado.

1.8.3.2 STREAM TO SERVER

Citrix XenApp

“El producto XenApp ha venido ofreciendo una de las mejores experiencias de entrega de aplicaciones para los usuarios, con 25 años de experiencia en el sector, adaptándose a las necesidades de cada uno de ellos. Ofrece una solución completa para el acceso, administración y despliegue de aplicaciones integrándose con los productos y plataformas de otros fabricantes: VMware; con su plataforma de virtualización vSphere y/o App Volumes y Microsoft; con su producto App-V.” (Fernández, 2017)

De este modo, se puede aumentar de forma nativa, sus capacidades para ofrecer un entorno más completo para las organizaciones más exigentes. Además, trae integrado la funcionalidad de AppDisk que es, en cuanto a funcionamiento y expectativas, la característica con la que quiere plantar cara a App Volumes de VMware, que se verá a continuación.

Este producto proporciona 4 de los requisitos que satisfacen las necesidades del diseño que se quiere plantear:

- Centralizar todas las aplicaciones en unos servidores, donde están instaladas, para posteriormente ofrecerles a los usuarios para que las inicien como si se tratara de sus equipos personales.
- Las aplicaciones, a pesar de ejecutarse en remoto, se integrarán en los equipos locales de tal modo que todos los dispositivos de los clientes como las impresoras o discos duros serán accesibles sin ningún problema.
- Ofrece la posibilidad de acceder a las aplicaciones a través de un portal web para que los usuarios remotos puedan acceder a sus aplicaciones desde cualquier lugar y dispositivo.
- Gracias a su tecnología HDX y políticas de visualización la experiencia del usuario, en cuanto a refresco, velocidad de respuesta y profundidad de color, será la óptima y adecuada teniendo en cuenta los anchos de banda de cada ubicación remota. De esta forma, el tráfico de red empleado para el acceso a las aplicaciones no entorpece a otras actividades.

En cuanto a la administración y control, ofrece diferentes herramientas y consolas de gestión, Citrix Studio, y control, Citrix Director, que facilita y simplifica el trabajo al equipo de TI.

Ahora bien, su adquisición se limita a la compra de las licencias por usuario concurrente que se requieran. Es decir, para poder hacer uso de esta aplicación se tendrá que adquirir un bloque de licencias igual o superior al número de usuarios que trabajen de forma simultánea contra la plataforma. De igual modo, al necesitar de servicio de escritorio remoto de Microsoft (RDS) se tendrán que adquirir licencias de este tipo para autenticar el acceso a los usuarios o máquinas dependiendo del modelo seleccionado y requerido para el cliente. (Montenegro, Gallego, & Jaramillo, 2017)

Horizon Apps

“Es uno de los productos que ofrece VMware dentro de su paquete de aplicaciones empresariales y está diseñada para brindarle a los usuarios un sistema seguro y un espacio de trabajo virtual fácil de administrar, que les ofrece una experiencia consistente y convincente en todos los dispositivos.” (Fernández, 2017)

Según las necesidades que hay y que se buscan, Horizon Apps, que pertenece al paquete de VMware Horizon, ofrece a los usuarios finales el acceso rápido y fácil a todas sus aplicaciones, publicadas en los servidores, a través de un espacio de trabajo unificado.

En esta tipología de productos VMware posee la aplicación App Volumes la cual permite crear particiones en las que están instalados los programas y presentarlos a los servidores

para que sea accesible para los usuarios. Este producto salió antes al mercado y con un funcionamiento mucho más depurado que el que ofrece AppDisk de XenApp en sus comienzos. No obstante, este componente no es exclusivo, es decir, el propio fabricante lo vende y promociona para su implantación con el producto de XenApp y de este modo dar una nueva disponibilidad de aprovisionamiento de aplicaciones para los servidores que luego utilizaran los usuarios. Este gancho comercial que realiza VMware puede dar una idea del liderazgo que tiene el producto de XenApp en relación con esta demanda de servicio.

Igual que se ha visto en el anterior apartado, soluciones para la infraestructura, este fabricante ofrece una formación específica para este tipo de producto para todos los profesionales de TI que necesiten adquirir los conocimientos necesarios para desplegar y gestionar esta plataforma. (VMware, 2017)

El gran problema que se presenta en este producto, sin tener en cuenta que XenApp es el líder de esta gama de productos, con una tecnología más que validada en miles de clientes de todo el mundo con grandes necesidades y exigencias, es el precio.

VMware presenta el mismo modelo de licenciamiento que Citrix, siendo necesaria la adquisición de licencias por usuario concurrente y de las licencias RDS para el acceso por usuarios o máquinas. No obstante, este producto no se caracteriza por ser económico y ante una necesidad de unos 150 usuarios concurrentes actuales el coste de licencias Horizon es muy elevado.

1.8.4 NUEVAS TENDENCIAS PARA LA ENTREGA DE VIRTUALIZACIÓN DE APLICACIONES

1.8.4.1 DOCKERS

Un contenedor es una unidad de software estándar que empaqueta una aplicación con todas sus dependencias y bibliotecas. Esto facilita la implementación de aplicaciones en contenedores, independientemente de la configuración del hardware o del sistema operativo. A diferencia de las máquinas virtuales, los contenedores utilizan el sistema operativo host en lugar de agrupar un sistema operativo con la aplicación.

Docker es una plataforma de contenedores el cual proporciona un ecosistema completo de herramientas para construir imágenes de contenedores, extraer estas imágenes de registros

conocidos, implementar contenedores y administrar u orquestar contenedores en ejecución en un grupo de máquinas.

Figura 4. Representación de la arquitectura docker. Adaptado de “Docker: let’s ship your application” por Medium, 2018.

1.8.4.2 MSIX

MSIX combina las mejores características de MSI y AppX. Es un formato de empaquetado directo que los administradores de sistemas pueden incluso programar para instalaciones «sin supervisión». Desde la perspectiva del usuario, un MSIX se instala como un archivo MSI, pero por dentro funciona como un archivo AppX. (Microsoft, 2019)

Figura 5. Representación de un esquema MSIX. Adaptado de “What is MSIX?” por Microsoft, 2019.

Basado en la tecnología de contenedores este formato queda aislado del resto del sistema y permite realizar desinstalaciones y actualizaciones sin problemas. Cuando instalas un programa usando MSI o EXE, el programa puede hacer cambios en el registro y crear archivos y carpetas en todo su sistema. Cuando los desinstalas, a menudo hay archivos y claves de registro que permanecen, dejando desorden en el sistema.

Con MSIX, los programas se instalan en un contenedor y todos los archivos necesarios permanecen dentro de ese contenedor o siguen reglas precisas y predecibles sobre dónde pueden estar esos archivos (en la carpeta AppData, por ejemplo). Cuando los desinstalas, todos los datos se van con el programa, no deja ningún desorden. Eso significa que tu sistema estará más limpio en el futuro.

Otro punto importante es que es posible la distribución de MSIX fuera de la Microsoft Store. Con ello es mucho más sencillo coger programas antiguos y volver a empaquetarlos bajo MSIX. Y lo más importante. Microsoft lanzó un SDK para mejorar la compatibilidad multiplataforma. Como vemos en su página de GitHub, el soporte es posible para iOS,

MacOS, Android, Linux e incluso versiones más antiguas de Windows. El proceso es simple. Los desarrolladores colocan instrucciones especiales en los archivos MSIX para permitirle identificar el sistema operativo y los pasos a seguir. (Ranchal, 2019)

1.8.4.3 CONTAINERD

Originalmente se construyó como un punto de integración para tiempos de ejecución de OCI (Open Container Initiative) como *runc*, pero de un tiempo acá ha agregado muchas funcionalidades para equiparlo con las necesidades de las plataformas de contenedores modernas como Docker y Kubernetes. Docker abrió su funcionalidad de tiempo de ejecución de contenedor principal en un componente independiente llamado containerd, la cual es básicamente uno de los componentes del ecosistema Docker, es un tiempo de ejecución de contenedor que puede administrar un ciclo de vida completo del contenedor, desde la transferencia y/o almacenamiento de imágenes hasta la ejecución, supervisión y conexión en red del contenedor. (Docker, 2019)

Figura 6. Representación de la nueva arquitectura de Docker después de compilarla en *runc* y *containerd*. Adaptado de “Docker vs CRI-O vs Containerd” por Computing for Geeks, 2019.

CAPÍTULO 2. MARCO TEÓRICO

“La virtualización es una tecnología que permite crear servicios de TI útiles mediante recursos que están ligados tradicionalmente al hardware. Además, distribuye sus funcionalidades entre diversos usuarios o entornos, lo que permite utilizar toda la capacidad de una máquina física.” (RedHat, 2018)

En términos prácticos, imagínese que tiene tres servidores físicos con propósitos específicos individuales. El primero es un servidor de correo, el segundo un servidor web y el tercero ejecuta aplicaciones heredadas internas. Cada servidor utiliza cerca del 30 % de su capacidad; es decir, solo una parte de su potencial de ejecución. Pero como las aplicaciones heredadas siguen siendo importantes para sus operaciones internas, tiene que conservarlas junto con el tercer servidor que las hospeda.

*Figura 7.*Diagrama de servicios tradicionales. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.

Generalmente, era más fácil y confiable ejecutar tareas individuales en servidores individuales: un servidor, un sistema operativo y una tarea. No era sencillo asignar múltiples tareas a un servidor. Pero la virtualización permite dividir el servidor de correo en dos servidores únicos que pueden administrar tareas independientes, para poder migrar las aplicaciones heredadas. Se utiliza el mismo hardware, pero de manera más eficiente.

Si pensamos en la seguridad, es posible volver a dividir el primer servidor para que administre otra tarea y aumentar su uso de un 30 % a un 60 %, y luego a un 90 %. Una vez realizada esta división, los servidores que quedan vacíos pueden volver a utilizarse para otras tareas o dejar de utilizarse por completo para reducir los costos de refrigeración y mantenimiento.

2.1 ¿Cómo Funciona la Virtualización?

“El software denominado hipervisores separa los recursos físicos de los entornos virtuales, es decir, todo lo que necesitan los recursos. Los hipervisores pueden conformarse como elementos principales de un sistema operativo (como una computadora portátil) o se pueden instalar directamente en el hardware (como un servidor), que es la forma en que la mayoría de las empresas virtualiza los hipervisores toman los recursos físicos y los dividen de manera tal que los entornos virtuales puedan usarlos.” (RedHat, 2018)

*Figura 8.*Representación de un esquema de máquina virtual e hipervisor. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.

Los recursos se dividen según las necesidades, desde el entorno físico hasta los numerosos entornos virtuales. Los usuarios interactúan con los servicios publicados y los ejecutan dentro de las máquinas virtuales. La máquina virtual funciona como un archivo de datos único. Al igual que con cualquier archivo digital, se puede mover de una computadora a otra, abrir en cualquiera de ellas y esperar que funcione de la misma manera.

Cuando el entorno virtual se está ejecutando y un usuario o programa emite una instrucción que requiere recursos adicionales del entorno físico, el hipervisor transmite la solicitud al sistema físico y guarda los cambios en la caché. Todo esto sucede prácticamente a la misma velocidad que habría si este proceso se realizará dentro de la máquina física.

2.2 Tipos de Virtualización

Virtualización de los datos

Los datos que se encuentran repartidos por todas partes se pueden consolidar en una fuente única. La virtualización de los datos permite que las empresas los traten como si fueran una cadena de suministro dinámica; de esta manera, se obtiene la capacidad de procesamiento que permitirá reunir los datos de varias fuentes, integrar otras fuentes nuevas con facilidad y transformar los datos en función de las necesidades de los usuarios.

Figura 9. Representación de un esquema de virtualización de datos. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.

Las herramientas de virtualización de los datos se enfrentan a varias fuentes de datos y permiten tratarlas como una sola. De este modo, es posible proporcionar a cualquier aplicación o usuario los datos necesarios, en la forma requerida y en el momento justo.

Virtualización de los escritorios

La virtualización de los escritorios suele confundirse fácilmente con la virtualización de los sistemas operativos, que permite implementar varios sistemas operativos en una sola máquina. Sin embargo, con la virtualización de los escritorios, un administrador central (o una herramienta de administración automatizada) puede implementar entornos simulados de escritorio en cientos de máquinas físicas al mismo tiempo.

*Figura 10.*Representación de un esquema de virtualización de escritorios. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.

A diferencia de los entornos de escritorio tradicionales que se instalan, configuran y actualizan físicamente en cada máquina, la virtualización de los escritorios permite que los administradores realicen ajustes de configuración, actualizaciones y controles de seguridad de forma masiva en todos los escritorios virtuales.

Virtualización de los servidores

Los servidores son computadoras diseñadas para procesar un gran volumen de tareas específicas de forma muy efectiva, para que otras computadoras, como las portátiles o de escritorio, puedan ejecutar otras tareas. La virtualización de un servidor le permite ejecutar más funciones específicas e implica dividirlo para que los elementos se puedan utilizar para realizar varias funciones.

*Figura 11.*Representación de un esquema de virtualización de servidores. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.

Virtualización del sistema operativo

La virtualización del sistema operativo se realiza en el kernel, es decir, los administradores de tareas centrales de los sistemas operativos. Es una forma útil de ejecutar los entornos Linux y Windows de manera paralela.

Figura 12. Representación de un esquema de virtualización de sistemas operativos. Adaptado de “¿Qué es la virtualización?” por Red Hat, 2018.

Las empresas también pueden instalar sistemas operativos virtuales en las computadoras, lo cual:

- Reduce el costo del hardware en masa, ya que las computadoras no requieren capacidades tan inmediatas.
- Aumenta la seguridad porque todas las instancias virtuales se pueden supervisar y aislar.
- Limita el tiempo que se destina a los servicios de TI, como las actualizaciones de software.

Virtualización de aplicaciones

La virtualización de aplicaciones sigue un método diferente. No virtualiza el entorno operativo, sino que solo virtualiza la capa de aplicación. De este modo cada aplicación se puede ejecutar de forma aislada, es decir, independientemente del entorno.

Hay dos enfoques para la problemática de aplicaciones:

- Terminal Services: Esta tecnología consiste básicamente en servidores centralizados en los cuales están instalados los aplicativos y sirven sesiones múltiples a los usuarios para ejecutar las aplicaciones servidas. Este tipo de tecnología la utilizan fabricantes como Citrix.

- Streaming de aplicaciones: Esta tecnología de virtualización de aplicaciones permite que las aplicaciones se transmitan desde una ubicación centralizada a un entorno de aislamiento en el dispositivo de destino donde se van a ejecutar. Este tipo de tecnología la utilizan fabricantes como Microsoft.

CAPÍTULO 3. DEFINICIÓN DEL PROBLEMA Y TOMA DE REQUERIMIENTOS

3.1 Análisis del problema

Actualmente garantizar el acceso a las aplicaciones de negocio es de vital importancia para las distintas áreas de la organización, con ello estas podrán desarrollar eficientemente sus funciones. El despliegue de estas se convierte en un servicio crítico tomando como referencia que se desarrollan en el sector micro financiero y que hay que cumplir normativas de seguridad en sistemas informáticos, de red y datos. El rápido crecimiento en este sector ha traído consigo que la organización y sus sistemas de información demanden soluciones que permitan ahorrar tiempo, aumentar la eficiencia del personal y disminuir los costos operativos, del cual el área de TI es responsable.

En la Cooperativa Los Andes se ha venido presentando inconvenientes con el acceso a las aplicaciones de negocio, es por ello que se formulan los siguientes problemas relacionados con dichas incidencias.

3.2 Identificación del problema

A continuación, brindaremos una tabla en la cual verificaremos que los objetivos específicos identificados en capítulos anteriores tengan una relación directa con los problemas identificados.

Tabla 3

Tabla Objetivo Específico por Problema

Objetivos Específicos	Problema
Diseñar una plataforma de virtualización que permita la administración y supervisión centralizada según las buenas prácticas de virtualización.	Modelo carente de un sistema de administración y supervisión centralizado. Gastos en infraestructura local desplegada en sucursales
Optimizar el desempeño de la aplicación, direccionando hacia un mejor rendimiento y un óptimo consumo de ancho de banda según las buenas prácticas de virtualización.	Bajo desempeño de la aplicación en uso Servidores de acceso a aplicaciones saturados en su capacidad de trabajo
Proponer un diseño que brinde continuidad y seguridad de acceso a la	Acceso externo inseguro Diseño carente de alta disponibilidad

plataforma según las buenas prácticas de virtualización.

Solución carente de movilidad para el acceso desde dispositivos móviles a las aplicaciones

Nota: Se presentan los objetivos del proyecto con los problemas identificados en cada uno de ellos, elaboración propia.

3.2.1 Modelo carente de un sistema de administración y supervisión centralizado.

En la actualidad, el modelo de administración está orientado al dispositivo, el acceso a la aplicación se realiza instalando la aplicación en el host cliente en caso de que el enlace no sea satelital, caso contrario se configura el acceso directo al terminal server tal y como se detalla en la siguiente tabla:

Tabla 4

Resumen de tipo de acceso a aplicaciones

Ítem	Sucursal	Ancho de banda(I/O)	Medio de acceso	Tipo de Acceso
1	OEP Lima	30 Mbps/30 Mbps	Fibra Óptica	Cliente servidor
2	Agencia Aymaraes	2 Mbps/1 Mbps	ADSL	RDP
3	Agencia Abancay	5 Mbps/5 Mbps	Radio Enlace	Cliente servidor
4	Agencia Andahuaylas	5 Mbps/5 Mbps	Radio Enlace	Cliente servidor
5	Agencia Uripa	1 Mbps/512 Kbps	Satelital	RDP
6	Agencia Chuquibalmbilla	1 Mbps/512 Kbps	Satelital	RDP
7	Agencia Cotabambas	1 Mbps/512 Kbps	Satelital	RDP
8	Agencia Huancarama	1 Mbps/512 Kbps	Satelital	RDP
9	Agencia Huaccana	1 Mbps/512 Kbps	Satelital	RDP
10	Agencia Tintay	1 Mbps/512 Kbps	Satelital	RDP
11	Agencia Antabamba	1 Mbps/512 Kbps	Satelital	RDP
12	Agencia Curahuasi	1 Mbps/512 Kbps	Satelital	RDP
13	Agencia Cusco	10 Mbps/10 Mbps	Fibra Óptica	Cliente servidor
14	Agencia Huancavelica	10 Mbps/10 Mbps	Fibra Óptica	Cliente servidor
15	Agencia Santo Tomás	1 Mbps/512 Kbps	Satelital	RDP

Nota: Se presentan las sucursales de la organización, así como el ancho de banda asignado, medio y tipo de acceso respectivo, elaboración propia.

En los hosts en los que se acceden a la aplicación se pueden verificar conflictos asociados con el sistema operativo u otras aplicaciones ya instaladas, debido a que se tiene que verificar

que las APIs sean compatibles con el sistema operativo del equipo huésped, asimismo verificar que tengan instalados versiones de *framework* actualizadas para su correcto funcionamiento de las DLL compartida con otros programas, a su vez corroborar que las funcionalidades de la aplicación trabajen de manera correcta sea una arquitectura de 32 o 64 bits.

En la tabla 5 listamos la cantidad de equipos en la red empresarial, así como los sistemas operativos que poseen y con los que la aplicación debe ser testeado por TI para su funcionamiento.

Tabla 5

Lista de sistemas operativos de host por sede

Ítem	Sucursal	Hosts	SO w7	SO w8	SO w8.1	SO w10
1	OEP Lima	21	3	0	0	18
2	Agencia Aymaraes	5	2	2	0	0
3	Agencia Abancay	5	2	2	0	1
4	Agencia Andahuaylas	5	2	3	0	0
5	Agencia Uripa	5	2	0	0	3
6	Agencia Chuquibalmbilla	5	2	0	0	3
7	Agencia Cotabambas	5	2	0	3	0
8	Agencia Huancarama	5	2	0	3	0
9	Agencia Huaccana	5	2	0	0	3
10	Agencia Tintay	5	2	0	0	3
11	Agencia Antabamba	5	2	3	0	0
12	Agencia Curahuasi	5	2	3	0	0
13	Agencia Cusco	5	2	2	0	1
14	Agencia Huancavelica	5	2	2	0	1
15	Agencia Santo Tomás	5	2	3	0	0

Nota: Se presentan las sucursales de la organización, la cantidad de equipos que le corresponde y la distribución que poseen, elaboración propia.

Debido al volumen de usuarios con los que la plataforma cuenta actualmente, genera que la administración y supervisión del entorno dependen de la capacidad del usuario de TI de poder acceder al equipo del usuario y el de poder atender de manera empírica dicha incidencia, ya que no se cuenta con un sistema que registro de eventos multicapa en la plataforma actual, lo cual limita la capacidad de TI de poder atender las incidencias y brindar el acceso a las aplicaciones de la manera idónea. En ese sentido, la solución planteada deberá simplificar de

manera eficiente las tareas de mantenimiento tanto desde la parte frontal del portal web al cual ingresan los usuarios como de la parte lógica del sitio el cual permite que todo funcione correctamente.

Tabla 6

Lista de principales tareas de TI.

Ítem	Tareas TI	Cantidad de casos por semana	Tiempo dedicado por host	Sedes Afectadas	Cantidad de Equipos
1	Actualización de la versión de la aplicación	1 a 2	5 m - 10 m	14	70
2	Creación o modificación de perfiles de usuario	1 a 2	5 m - 10 m	15	1 a 2
3	Monitoreo pérdidas de conexión con el servicio.	5 a 10	10m - 15m	12	5 a 10
4	Atender fallas de acceso portapapeles o servicio de impresión	5 a 10	10m - 15m	12	5 a 10
5	Atender fallas de acceso externo a la aplicación	5 a 10	15m - 20m	14	5 a 10

Nota: Se presentan las tareas de TI, así como la cantidad de casos por semana, tiempo sedes y cantidad de equipos correspondiente, elaboración propia.

La tabla 6 lista la cantidad de tareas relacionadas con el soporte que se da para que los usuarios puedan acceder a las aplicaciones, así como la cantidad de tiempo que sugiere al área de TI atenderla, la misma que significa la cantidad de tiempo la cual el usuario no puede realizar sus labores.

Además, en las tareas mencionadas en la tabla anterior se requiere que los clientes tengan parte de los requisitos de las aplicaciones y en el caso de producirse algún problema con alguna descarga de los paquetes sigue siendo necesario desplazarse hasta el cliente para revisar su problema, por lo que se mantiene una dependencia de ejecución, rendimiento y funcionamiento con los equipos locales.

3.2.2 Gastos en infraestructura local desplegada en sucursales

El escenario actual contempla que en sucursales se cuente con un UTM para poder conectarse vía VPN IPSEC a los recursos y/o un directorio activo en sitio para poder validar los permisos

de acceso a la información, lo que genera un gasto anual fijo en infraestructura local y licenciamiento.

Asimismo, el área de TI ha optado por solucionar los problemas de conectividad incrementando los anchos de banda en sedes que utilizan plataformas satelitales acompañado de optimizadores WAN en ambos extremos, todo ello con el propósito de mejorar la experiencia del usuario, lo cual ha generado el aumento de los gastos referidos a los servicios que ofrece TI, sin que ello vaya de la mano con la mejora del desempeño de la plataforma.

Tabla 7
Infraestructura local por sede

Ítem	Sucursal	UTM	Optimizadores BW
1	OEP Lima (Datacenter)	FGT200E	1555 Series
2	Agencia Aymaraes	FGT60E	555 Series
3	Agencia Abancay	FGT60E	-
4	Agencia Andahuaylas	FGT60E	-
5	Agencia Uripa	FGT60E	555 Series
6	Agencia Chuquibambilla	FGT60E	555 Series
7	Agencia Cotabambas	FGT60E	555 Series
8	Agencia Huancarama	FGT60E	555 Series
9	Agencia Huaccana	FGT60E	555 Series
10	Agencia Tintay	FGT60E	555 Series
11	Agencia Antabamba	FGT60E	555 Series
12	Agencia Curahuasi	FGT60E	555 Series
13	Agencia Cusco	FGT60E	-
14	Agencia Huancavelica	FGT60E	-
15	Agencia Santo Tomás	FGT60E	555 Series

Nota: Se presentan las sucursales de la organización, así como la infraestructura asignada respectivamente, elaboración propia.

En la tabla 7 mencionamos el equipamiento por sucursal, adicional a ello están los gastos operativos y costos asociados a la capacitación del personal de TI para la administración de la infraestructura adquirida.

3.2.3 Bajo desempeño de la aplicación en uso

Debido a que las sucursales se encuentran en zonas donde no se pueden encontrar servicios de ancho de banda óptimos para el buen desempeño en el uso de las aplicaciones, se recurre a no usar simultáneamente todos los equipos a la red con el fin de no saturar los enlaces y aminorar los retardos en los ingresos de información a las aplicaciones, ello genera retrasos en las labores del personal, a su vez dificulta la consolidación de la información, para ello sería óptimo que podamos utilizar protocolos de acceso para enviar y recibir datos que incorporen capacidades avanzadas de optimización y aceleración para conseguir el mejor rendimiento sobre cualquier tipo de red, incluidas las conexiones WAN con poco ancho de banda y alta latencia, asimismo aminorar en lo posible los retardos en el uso de los sistemas. Para el caso práctico mencionaremos las aplicaciones y los dividiremos por los tipos de consumo que estos generan, en la tabla 6 veremos que en el caso de las oficinas que cuenten con líneas satelitales el uso de aplicaciones del tipo medio a alto es inviable más aún cuando el tráfico se desplaza sin ningún tipo de prioridad sobre el mismo canal sobre el cual pasan datos para otros usos.

Por otro lado, los usuarios reportan que, al consumir sus aplicaciones de los servidores de escritorio remoto, perciben lentitud en el procesamiento de estas, ya sea ingresado datos, obteniendo reportes, etc. Esta percepción empeora en las horas de alta demanda de consumo de las aplicaciones de negocio.

El acceso descentralizado a las aplicaciones de negocio, el manejo de múltiples credenciales y la percepción de bajo rendimiento en los servidores de escritorio remoto, afectan directamente a la experiencia de uso por parte de los usuarios, el cual es identificado como un problema en la organización.

Tabla 8

Aplicaciones utilizadas

Ítem	Aplicación	Áreas	Tipo Consumo
1	Flujo NET®	Caja, Finanzas, Contabilidad	Alto
2	CONCAR® SQL	Finanzas, Contabilidad, Auditoría	Alto
3	RS CRM®	Administración	Ligero
4	PLACAR® CB	Administración, RRHH	Medio
5	SISPAG®	Finanzas, Contabilidad, Auditoría	Alto
6	IVMS	Auditoría, TI	Alto

Nota: Se presentan las aplicaciones sobre las cuales se plasmará el diseño, las áreas que consumen dichas aplicaciones y el tipo de consumo que se le da, elaboración propia.

Tabla 9
Categorización de aplicaciones

Ítem	Tipo Consumo	Media Consumo de BW
1	Ligero	0.45 Mbps
2	Medio	0.59 Mbps
3	Alto	3.00 Mbps

Nota: Se presentan el tipo de consumo y el ancho de banda consumido según cada uno, elaboración propia.

Las mediciones en la tabla 9 han sido realizadas a través del Sinefa, el cual es un administrador de ancho de banda que nos permite desglosar de manera granular cada servicio detectado en la red wan y mostrarnos el uso de ancho de banda consumido, puertos utilizados e ip de usuario que accede.

En las gráficas 5 y 6 visualizamos la saturación sobre los enlaces de 1Mbps, así como los niveles de latencia superando los umbrales mínimos recomendados para el uso sin retrasos en la red de servicios, estos fueron sacados del portal de monitoreo del proveedor satelital, que para el caso práctico es Axesat Perú.

Figura 13. Representación gráfica del tráfico de canal de bajada saturado. Adaptado de “Informe Métricas”, por Portal Axesat, 2020.

Figura 14. Representación gráfica del reporte Latencia Enlaces Satelitales. Adaptado de “Informe Métricas”, por Portal Axesat, 2020.

3.2.4 Servidores de acceso a aplicaciones saturados en su capacidad de trabajo

La plataforma actual fue creada cuando las aplicaciones eran accedidas solo desde la oficina principal en Lima, estando el datacenter en la red local era sostenible la interacción de los usuarios con las aplicaciones accediendo a través del escritorio remoto o instalados localmente los que no necesitaban de una licencia.

Conforme la organización ha ido creciendo los recursos para los 21 usuarios que un comienzo fue contemplado han tenido que soportar las 91 conexiones que actualmente poseen incluyendo sucursales, y a la espera del acceso de usuarios móviles proyectados en los próximos 5 años.

Asimismo, la escalabilidad de la cual esta plataforma carece se da tanto a nivel horizontal como vertical, ya que además de carecer de recursos para el acceso por escritorio remoto, también es un solo servidor desde el cual se acceden a todas las aplicaciones que no pueden ser instalados localmente en los dispositivos finales.

Por otro lado, los usuarios son susceptibles a fluctuaciones en el uso de recursos, por ejemplo: aplicaciones con distintos niveles de consumo de recursos de hardware, ya que reportan que, al consumir sus aplicaciones remotamente, perciben lentitud en el procesamiento de las mismas, al momento de ingresar datos, obtención de reportes, impresión de cierres de caja.

A esto le sumamos que no hay un límite de veces que las aplicaciones puedan ser abiertas, generando que tareas en segundo plano incrementen el consumo de recursos, además no hay un tiempo de expiración para que la aplicación se encuentre abierta y dejen de consumir recursos para la comunicación con los servidores de base de datos. Esta percepción empeora en las horas de alta demanda de consumo de las aplicaciones de negocio y cuando se actualizan las versiones de las aplicaciones las cuales solicitan mayores recursos en memoria y cpu.

3.2.5 Acceso externo inseguro

El acceso a la aplicación desde las sucursales se viene ejecutando a través del protocolo RDP como se indica en la tabla 2, son los lugares en los que se cuentan con menos ancho de banda, estas apuntan a la dirección IP pública la cual es traducida hacia una IP privada asignada al terminal server, protocolo el cual es utilizado por “los ciberdelincuentes que utilizan ataques de fuerza bruta, que consisten en probar múltiples credenciales de acceso, es decir usuario y contraseña, de forma automatizada contra los objetivos. En caso de conseguir acceso, pasan al siguiente objetivo, que generalmente será instalar malware, esto con el objetivo de una vez tener acceso en el equipo de la víctima, tienen como principal fin la instalación de malware, pudiendo ser este de varios tipos:

- Ransomware, el malware que cifra la información y pide un rescate. Este tipo de amenaza ha pasado de propagarse por medio del correo electrónico con ingeniería social, a hacerlo a través de servicios RDP vulnerables.
- Cryptojacking que consiste en utilizar los recursos del sistema para minar criptomonedas. El minado de criptomonedas ha desplazado al ransomware como amenaza más común y rentable.
- Malware que roba información y datos confidenciales, como contraseñas de acceso a otros servicios.
- Infecciones que convierten a tu equipo en un zombi, controlado remotamente por ciberdelincuentes, formando parte de una botnet.” (INCIBE, 2019)

Asimismo, los servidores en los que se acceden tanto interna como externamente comparten el mismo rango de subred, sin ninguna red DMZ de por medio como se muestra en la figura 16, lo cual permitiría a cualquier intruso que haya llegado a nuestro terminal pueda tener acceso a los demás servidores de red de producción, esto acompañado a que en el diseño

actual no existe ningún dispositivo que monitoree o genere alarmas por si se producen alguna alerta de seguridad.

Figura 15. Representación de la red de producción Cooperativa Los Andes. Adaptado de “Plano general de red de la sede Central de Cooperativa Los Andes”, elaboración propia.

3.2.6 Diseño carente de alta disponibilidad

El acceso en sedes en las cuales no gozan de buen ancho de banda consta del acceso a un terminal server el cual se ubica en un único site sobre dos centros de datos ESXi los cuales trabajan en HA, asimismo el servidor de base de datos cuenta con un *failover cluster* todo almacenado sobre una datastore con arreglo de disco RAID 10, dicho esto si bien cuentan con los servicios de alta disponibilidad ya implementados, el servicio sólo cuenta con un terminal server y un directorio activo local, los cuales de corromperse el sistema operativo o alguna falla en los servicios que estos ofrecen, comprometería el acceso a los servicios.

Asimismo, verificamos que el acceso en sucursales es escritorio remoto o vía cliente servidor, en uno publicando el puerto 3389 y el otro el 1494, pero en ambos casos apuntando a una sola dirección IP pública del enlace primario de internet, en caso de que el servicio de este se degrade, las oficinas remotas no podrían acceder al servicio.

Según lo mencionado podríamos concluir que la actual plataforma como se visualiza en la figura 5 no cuenta con servicios redundantes en lo que concierne a directorio activo, terminal server y base de datos, lo cual no ofrece un servicio de alta disponibilidad ante las incidencias ya mencionadas, por lo que sería ideal trabajar con un diseño que pueda otorgar una dirección de acceso que sea transparente para el usuario, aparte de contar con un servidor adicional que no solo ayude para la disponibilidad sino también para el control de carga. Asimismo, sería idóneo poder contar con una solución en la nube que nos pueda ofrecer un site adicional.

*Figura 16.*Representación del esquema de acceso a las apps. Adaptado de “Plano general de red de la sede Central de Cooperativa Los Andes”, elaboración propia.

3.2.1 Solución carente de movilidad para el acceso externo a las aplicaciones

En cuanto a los entornos que se han visto, se pueden indicar que no llegan a satisfacer las necesidades del cliente, entre otros motivos porque no da la posibilidad de ejecutar las aplicaciones desde dispositivos móviles y sistemas operativos con Android, iOS y Windows Phone.

Actualmente, las conexiones externas se vienen realizando tal y como se muestra en la figura 18, usuarios de áreas administrativas que consumen aplicaciones de negocio fuera de la red empresarial, estos pueden conectarse vía RDP desde conexiones de internet externas, el cual no le brinda una experiencia de usuario ideal para el trabajo fluido, en casos dicho protocolo se bloquea en los firewalls de entidades bancarias o gubernamentales por temas de seguridad denegando el acceso a la aplicación.

La otra forma es utilizando un cliente VPN, esta forma otorga un limitado ancho de banda no gestionado para la conexión hacia la sede Central. Asimismo, las conexiones que se trate de realizar desde sistemas operativos como Andorid, IOS o Windows Phone no se podrán realizar ya que actualmente no soporta dichas plataformas.

Figura 17. Representación del diagrama de conexión externa para el acceso a recursos. Adaptado de “Esquema de servicios publicados de Cooperativa Los Andes”, elaboración propia.

3.3 Relación entre el problema y las causas que lo originan

Tabla 10
Matriz de causa e impacto del problema

Problema	Causa
Modelo carente de un sistema centralizado de administración y supervisión	No cuenta con una plataforma centralizada de administración de aplicaciones.
	No cuenta con una plataforma centralizada de administración de la arquitectura virtualizada.
	El soporte es vía programas de acceso remoto los cuales dificultan la atención de los tickets generados y realizadas en los dispositivos del usuario final.
	No se cuenta con un diseño que permita monitorear y brinde información del estado de servicio de la solución la cual nos permita tomar acciones proactivas ante alguna incidencia.
	Los servicios dependen de la integridad del dispositivo para poder acceder a la aplicación.
Gastos en infraestructura	No se lleva el control adecuado de los recursos debido a la cantidad de sedes y recursos desplegados.

local desplegada en sucursales	La plataforma actual requiere que exista infraestructura local para poder acceder y validar las aplicaciones a los distintos usuarios en sucursales.
Bajo performance en el uso de la aplicación	Ancho de bandas limitados en sucursales. Uso de protocolos no optimizados para el acceso a aplicaciones. Se utiliza escenario cliente servidor para el acceso a la aplicación. No se utiliza de forma óptima el ancho de banda de sucursales.
Servidores de acceso a aplicaciones saturados en su capacidad de trabajo	Mal dimensionamiento de plataforma de acceso a las aplicaciones. Plataforma carente de escalabilidad para mayor cantidad de usuarios y aplicaciones.
Acceso externo inseguro	Los servicios no están publicados de manera segura para el acceso externo. Servidores con acceso externo no se encuentran dentro de una DMZ. El acceso es a través de protocolos inseguros y vulnerables a ataques DDOS o de fuerza bruta. No se cuenta con una solución la cual tenga redundancia de los servicios críticos como lo son el terminal server ni el directorio activo o algún recurso alternativo para restaurar inmediatamente los servicios cuando ocurran problemas.
Diseño carente de alta disponibilidad	Se cuenta con un solo nodo de infraestructura a disposición de la organización. El acceso en sucursales depende de una IP pública asignada por nuestro ISP, la cual en caso de estar con el servicio degradado impediría su acceso fuera de la sede Lima.
Solución carente de movilidad para el acceso externo a las aplicaciones	No se tiene control sobre la totalidad de los dispositivos finales desde donde se accede a los servicios. El diseño actual no es compatible con sistemas operativos de dispositivos móviles.

Nota: Se presenta una matriz en donde se muestra la problemática de la organización y las causas que las originan, elaboración propia.

3.4 Evaluación de impacto en la organización

El impacto del problema engloba tres niveles en la empresa:

- Nivel organizacional: Los socios califican a la cooperativa Los Andes como una entidad rural poco proactiva con los diferentes servicios que brinda.
- Nivel técnico: Los procesos transaccionales de caja, consultas y afiliaciones de socios son muy lentos debido a la baja velocidad de los enlaces contratados en las sucursales. Estos problemas son ocasionados por la dificultad de acceder a servicios de ancho de banda dedicados y la falta de una infraestructura no optimizada para este tipo de escenarios.

- Nivel económico. Los gastos en los que se invierten para mejorar el desempeño en el acceso a las aplicaciones ya sea en líneas dedicadas en cada oficina, en infraestructura local, etc.

Las líneas mencionadas las explicaremos a detalle a continuación:

• Nivel organizacional

Para definir el alcance organizacional del problema, se deben conocer las funciones de la Cooperativa Los Andes. A finales de los años 90 fue creada como una institución de microfinanzas que pueda cumplir la labor de fortalecimiento de los servicios de defensa financiera, asesoramiento, procesamiento y comercialización para agricultura familiar sostenible. Las acciones se concentran particularmente en el sur del país (Sierra), en los departamentos de Apurímac, Cusco y Puno, áreas caracterizadas por una tasa de pobreza muy alta (entre 50 y 97%). Según el mapa de proceso de la imagen siguiente podríamos elaborar la siguiente lista de labores dentro de la cooperativa:

Figura 18. Representación del mapa de procesos de Cooperativa Los Andes. Adaptado de “Cooperación Entre Cooperativas”, por Cooperativa Los Andes, 2018.

Subproceso de solicitud de crédito

Es el primer proceso que inicia el proceso de negocio de la Cooperativa

- Recopilación de información del cliente e ingreso a base de datos.
- Ubicación del cliente en mercado objetivo.
- Ubicación de promociones crediticias al cliente.
- Verificación de la existencia del cliente.
- Desarrollo del análisis (crédito administrativo, ordinario y plazos).
- Realizar los procesos de Instrumentación y Desembolso.
- Observación y seguimiento de los acreditados
- Gestión de cobranzas.

Subproceso de solicitud de ahorros

Es el segundo proceso que inicia el proceso de negocio de la Cooperativa

- Recopilación de información del cliente e ingreso a base de datos.
- Verificación de la existencia del cliente.
- Desarrollo del análisis (tipos de cuentas, tasas de intereses, vigencia del depósito).
- Notificaciones de cláusulas del contrato.
- Observación y seguimiento de los abonados.
- Gestión de devoluciones.

Subproceso de servicios

Es el tercer proceso que desarrolla la cooperativa y más enfocada en cubrir aspectos relacionados con el cumplimiento de los procesos relacionados al funcionamiento.

- Análisis y evaluación mensual, de los indicadores, verificando la adecuada estructura financiera de la cooperativa.
- Revisión y análisis mensual de la ejecución del Plan Empresarial, verificando el cumplimiento de metas financieras y administrativas.
- Mensualmente se analizan y evalúan los estados financieros parciales, así como del cierre contable del año anterior, verificando la racionalidad de los mismos y sus resultados.
- Se conoce y analiza mensualmente, la calificación de riesgos emitida por el Fondo de Garantías Fenacrep, para verificar la adecuada administración financiera de la cooperativa.

- Trimestralmente se verifica y analiza el Informe de la Unidad de Cumplimiento de la Cooperativa.
- Revisión y análisis de Morosidad, emitiéndose las recomendaciones necesarias para su adecuada gestión y control.
- Análisis de expedientes de crédito, verificando que cada crédito se haya otorgado de acuerdo a la política crediticia de la cooperativa.
- Verificación y análisis del plan de trabajo de la Auditoría Interna.
- Evaluación y análisis de forma mensual, de los informes de auditoría interna, verificando las revisiones y operaciones de la cooperativa.
- Supervisión del cumplimiento de la Ley contra el Lavado de Dinero y Otros Activos y la Ley para Prevenir y Reprimir el Financiamiento al Terrorismo.
- Análisis y revisión de la aplicación de los procedimientos de cobro por préstamos, emitiendo las recomendaciones necesarias para una gestión eficiente de los mismos.

● **Nivel técnico**

Las sucursales se congestionan debido a la cantidad de transacciones diarias que realizan. Esto además se encuentra limitada por las bajas velocidades de transmisión con las que cuentan algunos enlaces de banda ancha o satelital. Asimismo, es crítico que en las sucursales el acceso a las aplicaciones no sea de manera uniforme y centralizada. Toda la información que se genera en cada sucursal se almacena localmente generando potenciales brechas de seguridad.

Los usuarios en las sucursales cuentan con un acceso a internet en planes ADSL 2 Mbps al 25% efectivo de la velocidad, o en su defecto con enlaces satelitales de 1Mbps de bajada y 512 Kbps de subida al 100% con latencias de aproximadamente 600 ms a 700 ms.

Considerando la cantidad de usuarios con acceso a internet por cada sucursal y el *throughput* requerido, se puede obtener el tráfico total, el cual se presenta en la siguiente tabla.

Tabla 11

Consumo Total Aproximado por sede

Ítem	Sucursal	Bajo	Consumo BW	Medio	Consumo BW	Alto	Consumo BW	Consumo Total
1	OEP Lima	1	64 Kbps	5	1.0 Mbps	15	9.0 Mbps	9.96 Mbps
2	Agencia Aymaraes	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
3	Agencia Abancay	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps

4	Agencia Andahuaylas	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
5	Agencia Uripa	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
6	Agencia Chuquibalmbilla	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
7	Agencia Cotabambas	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
8	Agencia Huancarama	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
9	Agencia Huaccana	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
10	Agencia Tintay	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
11	Agencia Antabamba	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
12	Agencia Curahuasi	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
13	Agencia Cusco	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
14	Agencia Huancavelica	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps
15	Agencia Santo Tomás	1	64 Kbps	1	250 Kbps	3	1.8 Mbps	2.10 Mbps

Nota: Se presenta la lista de sucursales, el consumo total que realizan según la cantidad de usuarios y el tipo de tráfico realizado, elaboración propia.

Según los resultados de la tabla 11, sólo en 5 de las 15 sucursales podríamos cumplir con los mínimos requeridos en lo que respecta a ancho de banda requerido.

Por otro lado, al momento de revisar los requerimientos de red para las sucursales de la organización solo se considera el soporte de carga de ancho de banda que requieren para acceder al portal de aplicaciones según la cantidad de usuarios que se utilice en cada sucursal, sin embargo, se obvia detalles como la latencia y el tiempo de resolución DNS que tenga la línea al interactuar con las aplicaciones, más aun cuando se visualiza que los tipos de tecnología que se utilizan no son uniformes y manejan latencias variables, asimismo los casos de uso que se están describiendo son altamente susceptibles a la latencia y no se ajustan dentro de los umbrales anteriormente mencionados.

En la siguiente tabla se detalla la latencia promedio capturada según el tipo de líneas de internet contratadas.

Tabla 12
Latencia Aproximada por sede

Ítem	Sucursal	Medio de acceso	Latencia Promedio
------	----------	-----------------	-------------------

1	OEP Lima (Datacenter)	Fibra Óptica	50 ms - 150 ms
2	Agencia Aymaraes	ADSL	120 ms - 200 ms
3	Agencia Abancay	Radio Enlace	150 ms - 250 ms
4	Agencia Andahuaylas	Radio Enlace	150 ms - 250 ms
5	Agencia Uripa	Satelital	600 ms - 800 ms
6	Agencia Chuquibambilla	Satelital	600 ms - 800 ms
7	Agencia Cotabambas	Satelital	600 ms - 800 ms
8	Agencia Huancarama	Satelital	600 ms - 800 ms
9	Agencia Huaccana	Satelital	600 ms - 800 ms
10	Agencia Tintay	Satelital	600 ms - 800 ms
11	Agencia Antabamba	Satelital	600 ms - 800 ms
12	Agencia Curahuasi	Satelital	600 ms - 800 ms
13	Agencia Cusco	Radio Enlace	150 ms - 250 ms
14	Agencia Huancavelica	Radio Enlace	150 ms - 250 ms
15	Agencia Santo Tomás	Satelital	600 ms - 800 ms

Nota: Se presenta la lista de sucursales, el medio de acceso y la latencia promedio en cada enlace, elaboración propia.

● Nivel económico

En la siguiente tabla, se presentan los gastos generados por cada sucursal, considerando su ancho de banda y tipo de acceso. Como se puede observar, las sedes cuentan con líneas ADSL, radio enlace, fibra óptica y satelital. Debido al alto costo por mega en líneas como las satelitales, y que actualmente se opta por incrementar los anchos de bandas para mejorar el desempeño; es que el presente diseño busca ayudar a utilizar el ancho de banda de manera óptima y reducir los costos asociados a incrementos en las velocidades contratadas.

Tabla 13

Gastos ocasionados por tipo de línea

Ítem	Sucursal	Ancho de banda(I/O)	Medio de acceso	Costo Mensual sin IGV
1	OEP Lima (Datacenter)	30 Mbps/30 Mbps	Fibra Óptica	\$ 850.00
2	Agencia Aymaraes	2 Mbps/1 Mbps	ADSL	\$120.00
3	Agencia Abancay	5 Mbps/5 Mbps	Radio Enlace	\$ 1200.00
4	Agencia Andahuaylas	5 Mbps/5 Mbps	Radio Enlace	\$ 1200.00
5	Agencia Uripa	1 Mbps/512 Kbps	Satelital	\$1200.00
6	Agencia Chuquibambilla	1 Mbps/512 Kbps	Satelital	\$1200.00
7	Agencia Cotabambas	1 Mbps/512 Kbps	Satelital	\$1200.00

8	Agencia Huancarama	1 Mbps/512 Kbps	Satelital	\$1200.00
9	Agencia Huaccana	1 Mbps/512 Kbps	Satelital	\$1200.00
10	Agencia Tintay	1 Mbps/512 Kbps	Satelital	\$1200.00
11	Agencia Antabamba	1 Mbps/512 Kbps	Satelital	\$1200.00
12	Agencia Curahuasi	1 Mbps/512 Kbps	Satelital	\$1200.00
13	Agencia Cusco	10 Mbps/10 Mbps	Fibra Óptica	\$ 800.00
14	Agencia Huancavelica	10 Mbps/10 Mbps	Fibra Óptica	\$ 900.00
15	Agencia Santo Tomás	1 Mbps/512 Kbps	Satelital	\$1200.00

Nota: Se presenta la lista de sucursales, el ancho de banda contratado, el medio de acceso y el costo actual de dicho servicio, elaboración propia.

Tabla 14

Gastos ocasionados en optimizadores de BW.

Ítem	Sucursal	Optimizadores BW	Costo Anual sin IGV
1	OEP Lima (Datacenter)	1555 Series	\$ 7500.00
2	Agencia Aymaraes	555 Series	\$1250.00
3	Agencia Abancay	-	-
4	Agencia Andahuaylas	-	-
5	Agencia Uripa	555 Series	\$1250.00
6	Agencia Chuquibalmbilla	555 Series	\$1250.00
7	Agencia Cotabambas	555 Series	\$1250.00
8	Agencia Huancarama	555 Series	\$1250.00
9	Agencia Huaccana	555 Series	\$1250.00
10	Agencia Tintay	555 Series	\$1250.00
11	Agencia Antabamba	555 Series	\$1250.00
12	Agencia Curahuasi	555 Series	\$1250.00
13	Agencia Cusco	-	-
14	Agencia Huancavelica	-	-
15	Agencia Santo Tomas	555 Series	\$1250.00

Nota: Se presenta la lista de sucursales, el modelo de optimizador de ancho de banda y el valor de mercado respectivo, elaboración propia.

Tabla 15
Gastos ocasionados en UTM

Ítem	Sucursal	UTM	Costo Anual sin IGV
1	OEP Lima (Datacenter)	FGT200E	\$ 2000.00
2	Agencia Aymaraes	FGT60E	\$480.00
3	Agencia Abancay	FGT60E	\$480.00
4	Agencia Andahuaylas	FGT60E	\$480.00
5	Agencia Uripa	FGT60E	\$480.00
6	Agencia Chuquibalmbilla	FGT60E	\$480.00
7	Agencia Cotabambas	FGT60E	\$480.00
8	Agencia Huancarama	FGT60E	\$480.00
9	Agencia Huaccana	FGT60E	\$480.00
10	Agencia Tintay	FGT60E	\$480.00
11	Agencia Antabamba	FGT60E	\$480.00
12	Agencia Curahuasi	FGT60E	\$480.00
13	Agencia Cusco	FGT60E	\$480.00
14	Agencia Huancavelica	FGT60E	\$480.00
15	Agencia Santo Tomás	FGT60E	\$480.00

Nota: Se presenta la lista de sucursales, el modelo UTM que poseen y el valor de mercado respectivo, elaboración propia.

3.5 Soluciones Posibles

Las soluciones posibles como diseño a utilizar han sido descritas en la parte teórica y estado del arte, por lo cual acá mencionaremos la selección de la solución a desarrollar, así como los problemas que atenderemos con cada una de ellas.

En lo que se refiere al modelo de virtualización de infraestructura, actualmente la cooperativa posee un modelo de hipervisor de tipo 1 o nativo (VMware vSphere), el cual le ofrece una mayor eficiencia de todos los recursos, gestión única y compartida, el cual cumplirá con todas las exigencias que sean planteado de una forma más sencilla y simplificando las tareas para los profesionales del servicio de TI, y a la vez que también podrá alinearse a la solución que elijamos para virtualizar las aplicaciones. Asimismo, las actuales aplicaciones requieren de una llave usb colocada dentro del equipo que las alberga, esta permite validar la licencia e ingresar a los servicios.

En cuanto a los entornos de soluciones de aplicaciones que se han mencionado, hemos optado por la de entrega a demanda, entre otros motivos porque es el producto que mejor satisface y complementa todas las necesidades que tiene el cliente, en cuanto al proceso de consolidación, y que junto con VMware vSphere ofrece la mejor alternativa, posibilidad y a un precio, considerablemente más bajo, este es el Citrix XenApp 7.x, esta solución se desplegará en los servidores de la cooperativa Los Andes y no en nube ya que el licenciamiento por concurrencias solo está disponible en escenarios locales, por lo que este será el producto que se emplea para el diseño de centralización y distribución de las aplicaciones a los usuarios finales.

Tabla 16
Soluciones seleccionadas

Lista de Problemas Identificados	Solución Planteada	Funcionalidad a utilizar
Acceso externo inseguro	Citrix XenApp	Citrix Gateway, Storefront
Modelo carente de un sistema centralizado de administración y supervisión	Citrix XenApp	Director
Bajo performance en el uso de la aplicación	Citrix XenApp	ICA Protocol, HDX Pro
Solución carente de movilidad para el acceso externo a las aplicaciones	Citrix XenApp	Citrix Gateway
Diseño carente de alta disponibilidad	Citrix XenApp	Delivery Controller HA
Gastos en infraestructura local en sucursales	Citrix XenApp	Storefront

Nota: Se presenta un cuadro con la lista de problemas identificados y el tipo de solución planteada con su funcionalidad respectiva. Adaptado de “Citrix Virtual Apps and Desktops”, por Citrix, 2019.

Asimismo, podemos verificar que se encuentra bien posicionado en el cuadrante de Gartner junto a otras soluciones en el mercado.

Figura 19. Cuadrante mágico que representa la competencia entre los fabricantes Cuadrante mágico para herramientas de gestión de puntos finales unificados en el año 2019. Adaptado de “Magic Quadrant for Unified Endpoint Management”, por Gartner, 2019.

3.6 Toma de Requerimientos

- Definir el modelo de entrega, la topología de sitio y la estrategia de gestión de imágenes a utilizar según los objetivos comerciales de la organización.
- Verificar que la solución se integre con el directorio activo, la base de datos SQL y el datastore existentes en la organización. Asimismo, que los servicios a añadir sean virtualizables por el VMware Vsphere 6.5.

- Evaluar tecnologías de virtualización de aplicaciones que cumplan con estándares de seguridad a través de la centralización de datos y el control de acceso.
- Cada uno de los servidores debe contar con la cantidad de recursos de hardware necesarios para satisfacer la carga de usuarios actual y del crecimiento anual de los próximos 5 años.
- Verificar los tiempos de inicio de sesión al cargar el entorno de usuario en el portal de aplicaciones, y tiempos de retardo al registrar entradas.
- Calcular el ancho de banda utilizado por aplicación considerando protocolos de visualización y transporte.
- Realizar un análisis de tráfico de los diferentes enlaces en sucursales que se considerarán en la topología de red, teniendo en cuenta el número de usuarios, la cantidad de dispositivos y las tasas de transferencia efectivas requeridos por aplicación.
- Definir los grupos de usuarios y segmentarlos según los requisitos de seguridad, movilidad y carga de trabajo.
- Diseñar una solución que cuente con un portal web para el acceso a las aplicaciones local y externo y una plataforma que soporte el acceso desde dispositivos móviles.
- Realizar un análisis sobre la estrategia de autenticación indicando los puntos y directivas a utilizar para establecer una conexión segura a la aplicación virtual.
- Proponer una solución en la que los recursos que la compongan puedan configurarse en alta disponibilidad para evitar puntos únicos de fallo.

Tabla 17

Resumen de objetivos específicos y requerimientos

Objetivo Específico	Requerimiento
Diseñar una plataforma de virtualización que permita la administración y supervisión centralizada según las buenas prácticas de virtualización.	<p>Definir el modelo de entrega, la topología de sitio y la estrategia de gestión de imágenes a utilizar en la plataforma.</p> <p>Verificar que la solución se integre con el directorio activo, la base de datos SQL y el datastore existentes en la organización. Asimismo, que los servicios a añadir sean virtualizables por el VMware Vsphere 6.5.</p> <p>Evaluar tecnologías de virtualización de aplicaciones que cumplan con estándares de seguridad a través de la centralización de datos y el control de acceso.</p>

	Cada uno de los servidores debe contar con la cantidad de recursos de hardware necesarios para satisfacer la carga de usuarios actual y del crecimiento anual de los próximos 5 años
Optimizar el desempeño de la aplicación, direccionando hacia un mejor rendimiento y un óptimo consumo de ancho de banda según las buenas prácticas de virtualización.	<p>Verificar los tiempos de inicio de sesión al cargar el entorno de usuario en el portal de aplicaciones, y tiempos de retardo al registrar entradas.</p> <p>Calcular el ancho de banda utilizado por aplicación considerando protocolos de visualización y transporte.</p> <p>Realizar un análisis de tráfico de los diferentes enlaces en sucursales que se considerarán en la topología de red, teniendo en cuenta el número de usuarios, la cantidad de dispositivos y las tasas de transferencia efectivas requeridos por aplicación.</p> <p>Definir los grupos de usuarios y segmentarlos según los requisitos de seguridad, movilidad y carga de trabajo</p>
Proponer un diseño que brinde continuidad y seguridad de acceso a la plataforma según las buenas prácticas de virtualización.	<p>Diseñar una solución que cuente con un portal web para el acceso a las aplicaciones local y externo y una plataforma que soporte el acceso desde dispositivos móviles.</p> <p>Realizar un análisis sobre la estrategia de autenticación indicando los puntos y directivas a utilizar para establecer una conexión segura a la aplicación virtual</p> <p>Proponer una solución en la que los recursos que la compongan puedan configurarse en alta disponibilidad para evitar puntos únicos de fallo.</p>

Nota: Se presentan los objetivos específicos del proyecto con sus respectivos requerimientos, elaboración propia.

3.7 Registro De Interesados

Tabla 18
Registro de interesados

Cargo	Organización a que pertenece	Rol en el Proyecto	Nivel interés (Bajo, Medio, Alto)	Nivel influencia (Bajo, Medio, Alto)
Gerente General	Cooperativa Los Andes	Patrocinador	Bajo	Bajo

Gerente de TI	Cooperativa Los Andes	Cliente	Alto	Alto
Jefe de Operaciones	Cooperativa Los Andes	Alta Dirección	Bajo	Alto
Jefe de Contabilidad	Cooperativa Los Andes	Alta Dirección	Medio	Bajo
Usuario sucursal	Cooperativa Los Andes	Cliente	Bajo	Alto
Partner	Partner	Partner	Bajo	Bajo
Administrador TI	Cooperativa Los Andes	Director proyecto	Alto	Alto
Jefe de Proyecto (David Silva)	Externo	Jefe Proyecto	Alto	Alto
Analista QA (Dandy Rosales)	Externo	Analista	Medio	Medio
Tester (Daniel Espinoza)	Externo	Tester	Medio	Medio

Nota: Se presenta el registro de interesados para el presente proyecto, elaboración propia.

3.8 Estructura de descomposición del trabajo (EDT)

Figura 20. Representación del EDT que se utilizara para el presente proyecto. Adaptado de “EDT del proyecto”, elaboración propia.

CAPÍTULO 4. DISEÑO DE PROPUESTA DE SOLUCIÓN

En el presente capítulo, se mencionarán los criterios que se han tenido en cuenta para la selección del fabricante y modelo de virtualización de aplicaciones a utilizar entre las diversas soluciones que hay actualmente en el mercado. Una vez seleccionado listaremos los recursos actuales con el cual cuenta la organización, luego se presentará el análisis de infraestructura requerida por cada servicio que conformará el diseño, teniendo en cuenta los requerimientos indicados en el capítulo anterior. Asimismo, se indican los criterios de diseño a considerar aplicando las buenas prácticas de los fabricantes a nivel físico, lógico, consideraciones de seguridad definidas por el cliente y los costos asociados al despliegue de dicha solución. Esto tomado según las necesidades plasmadas en cada uno de los objetivos específicos planteados.

4.1 Análisis de tecnología de virtualización de aplicaciones

Para la selección de la tecnología a utilizar en el presente diseño haremos las comparativas entre las principales soluciones en el mercado como RDS de Microsoft, Vmware Horizon y Citrix Virtual Apps y verificando cual de estas se alinea mejor a los objetivos planteados en el capítulo anterior.

La comparación la haremos basándonos en la integración, simplicidad y rendimiento, nos centraremos en aspectos claves para descubrir cómo cada solución se diferencia con la otra. En la siguiente tabla se realiza una comparativa de los puntos más importantes de las tres tecnologías citadas anteriormente:

Tabla 19

Comparativa de tecnologías de virtualización.

Características	Citrix	VMWare	Microsoft
Acceso a escritorios VDI de Windows y Linux	✓	Windows únicamente	Windows únicamente
Estabilidad del entorno y sencillez de implantación	✓	-	-
Gestión centralizada de la plataforma en una única consola	✓	Limitado	-
Acceso a aplicaciones virtuales de Windows y Linux virtual (publicadas)	✓	Windows únicamente	Windows únicamente
Integración			

Inicio instantáneo de aplicaciones con lanzamiento previo y permanencia de sesión	✓	-	-
Integración de aplicaciones Windows virtualizadas, así como aplicaciones SaaS/Web en el menú Inicio	✓	-	✓
Compatibilidad con funciones de Windows Aero	✓	-	✓
Acceso sin inconvenientes a aplicaciones locales desde VDI o sesiones de escritorio compartido alojadas	✓	-	-
Simplicidad			
Desbloqueo y reinicio de contraseña autoservicio del usuario	✓	-	✓
Configuración de clientes automatizada basada en usuario de dominio o cuenta de correo electrónico	✓	-	-
Selección automática de la mejor ruta de conexión al portal vía StoreFront o enrutamiento óptimo a través de Citrix Gateway	✓	-	-
Experiencia de usuario sencilla y coherente en cualquier dispositivo	✓	Limitado	Limitado
Implementación automatizada de los cambios de interfaz de usuario a todos los clientes de Citrix Workspace	✓	-	-
Facilidad de despliegue e instalación de la plataforma	✓	Limitado	-
Amplia compatibilidad para escritorios y aplicaciones	✓	Limitado	-
Rendimiento			
Rendimiento de sesión optimizado incluso en conexiones de larga distancia, ancho de banda limitada y alta latencia	✓	Limitado	-
Fiabilidad de la sesión y reconexión automática de clientes	✓	Limitado	-
Rendimiento de aplicaciones casi nativo en redes con una alta latencia y alta pérdida de paquetes con HDX	✓	-	-
Guardado de personalizaciones, perfiles de usuario entre sesiones	✓	-	Limitado
Admite la aceleración de gráficos con GPUs suministrados por Intel, AMD y NVIDIA.	✓	Limitado	-
Impresión sin controladores desde cualquier dispositivo y con un consumo mínimo de ancho de banda	✓	Limitado	✓

Nota: Se presentan las tres principales soluciones en virtualización de aplicaciones en el mercado, indicando las características de cada una de ellas, elaboración propia.

Como se puede observar en la tabla comparativa Citrix es superior en diversos aspectos, en consecuencia, al análisis y comparativa anterior, se ha considerado Citrix Virtual Apps como la opción más adecuada para la realización del diseño.

4.2. Infraestructura Actual

En esta parte se revisará a los recursos actualmente con los que dispone la organización, así como los disponibles para ver la factibilidad del diseño de la plataforma de aplicaciones.

Los servidores con los cuales ya se cuentan en para la presente solución, se listan a continuación.

Tabla 20

Servidores presentes en la organización

Ítem	HOST	vCPU	vRAM (GB)	Almacenamiento (GB)	Rol
1	AD01	4	6	SO: 80	Directorio Activo Principal
2	AD02	4	6	SO: 80	Directorio Activo Respaldo
				SO: 150	
3	DB01	16	32	DATA FILES: 100 LOG: 100 BACKUP: 100	Base de Datos Principal
4	FSV01	4	6	SO: 80 DATA FILES: 900	Fileserver Principal
5	FSV02	4	6	SO: 80 DATA FILES: 900	Fileserver Secundario
6	VC01	4	4	SO: 80	Servidor Administración Vcenter

Nota: Se presentan los cuatro servidores presentes en la organización, indicando el nombre de host y los roles que cumplen, elaboración propia.

4.2.1 Configuración Clúster VMware Vsphere

Actualmente la organización cuenta con una infraestructura virtual en alta disponibilidad basada en el software de virtualización de servidores VMWare vSphere. Por lo tanto, a partir del levantamiento de información actual revisaremos si los requerimientos de hardware para el diseño podrán ser cubiertos. Para ello mencionaremos la infraestructura actual de Cooperativa Los Andes.

Figura 21. Infraestructura virtual, formada por un cluster de VMWare conformado por tres hosts. Adaptado de “Cluster VMWare vSphere”, elaboración propia.

En la figura 21, se observa los componentes del *cluster* en *VMware vSphere*, esta cuenta de 03 servidores HP Blade 460C de décima generación los cuales son utilizados como host de virtualización. Gracias al *cluster* se obtiene una infraestructura de alta disponibilidad, pudiendo tolerar el fallo de un servidor caído.

El resultado de la sumarización de hardware de los 03 host que forman parte del *cluster* nos resultarán los siguientes datos:

- Cantidad total de procesadores: 108 (36 procesadores x 3 hosts)
- Cantidad total de recursos de CPU: 248.4 GHz (2.3 GHz x 36 procesadores x 3 hosts)
- Cantidad total de memoria RAM: 386.62 GB (128GB por 3 hosts)
- Número de host protegidos: 2 hosts.

Concluimos que gracias al *cluster* con el que actualmente cuenta la organización, la infraestructura de maquinas virtuales de Citrix Apps que se provisionarán estarán protegidos tanto por la estructura física del blade HP C7000 como por la funcionalidad de Vsphere HA

que nos otorgará alta disponibilidad para las maquinas virtuales agrupando en un *clúster* las máquinas virtuales y los *hosts* en los que residen y en caso de un error, las máquinas virtuales en un *host* con errores se reinician en *hosts* alternativos.

4.2.2 Configuración de almacenamiento

La presenta organización cuenta, como parte de su infraestructura, un equipo de almacenamiento SAN HP MSA 2050, compuesto por 1 *enclosure* que contiene 24 discos de 900 GB de capacidad de alta velocidad, resultando en un total de 21.09 TB de almacenamiento, este equipo está conectado directamente al equipo HP Blade C7000.

Actualmente, toda esta capacidad de almacenamiento está distribuido y administrado por el *cluster* de virtualización VMWare. La infraestructura de almacenamiento de la organización tiene una configuración de arreglo de discos, los cuales se encuentran en produccion. La imagen 22 indica la distribución actual que se viene utilizando.

Figura 22.Distribución de la infraestructura de storage HP en la organización. Adaptado de “Storage Producción”, elaboración propia.

4.3 Diseño de Infraestructura Citrix Virtual Apps

Para diseñar la solución de virtualización de aplicaciones se alinearán decisiones técnicas con requisitos organizativos y de usuario. El enfoque recomendado se centra en trabajar a través de cinco capas distintas:

Figura 23. Representación del modelo de diseño de cinco capas. Adaptado de “Citrix Provisioning 1912 Arquitectura”, por Citrix, 2019

En un nivel superior, la solución se basa en un modelo unificado y estandarizado de 5 capas.

1. Capa de usuario: Define los grupos de usuarios únicos, puntos finales y ubicaciones.
2. Capa de acceso: Define como un grupo de usuarios obtienen acceso a sus recursos. Se centra en seguro políticas de acceso y tiendas de aplicaciones.
3. Capa de recursos: Define las aplicaciones y los datos proporcionados a cada grupo de usuarios.
4. Capa de control: Define la infraestructura subyacente necesaria para admitir que los usuarios accedan a sus recursos.
5. Capa de hardware: Define la implementación física de la solución general.

El poder de este modelo es que es extremadamente flexible ya que cada grupo de usuarios puede tener su propio conjunto de políticas de acceso y recursos o el de poder compartirse, pero independientemente de cómo el usuario, el acceso y los recursos estén definidas, todas son administradas por una única capa de control integrada, como se muestra a en la figura 21. Las problemáticas plasmadas en el capítulo anterior podrán ser solucinadas a través de este tipo de modelo, en la tabla 19 indicaremos el problema y que capa ocupa.

Tabla 21
Resumen de problemas y capas del diseño.

Problema	Capa
Modelo carente de un sistema de administración y supervisión centralizado.	Control
Gastos en infraestructura local desplegada en sucursales	Control
Bajo desempeño de la aplicación en uso	Recursos
Servidores de acceso a aplicaciones saturados en su capacidad de trabajo	Hardware
Acceso externo inseguro	Acceso
Diseño carente de alta disponibilidad	Hardware
Solución carente de movilidad para el acceso desde dispositivos móviles a las aplicaciones	Usuario

Nota: Se presenta la lista de problemas y la capa que, enfocada a atender su solución, elaboración propia.

4.4 Metodología del diseño: Arquitectura Conceptual

Para el caso del diseño conceptual de la arquitectura de cómputo, la cual incluye modelo de entrega, topología y estrategia en la gestión de imágenes, para la plataforma de virtualización de aplicaciones, se va a tener en cuenta los requerimientos identificados en los puntos 3.2.1 y 3.2.2; así como también para el caso de la restricción se tomará en cuenta los identificados en los puntos 3.2.4.

A continuación, se realizará un análisis para determinar las características del equipamiento requerido para la capa de procesamiento y memoria RAM de la plataforma de virtualización de servidores.

Teniendo en cuenta las buenas prácticas ya mencionadas y la cantidad de usuarios y sucursales desde donde se conectan señalado en la tabla 05 es que indicaremos las características elegidas según el caso de uso en estudio.

Tabla 22
Usuarios por sucursal.

Ítem	Sucursal	Usuarios
1	OEP Lima	21
2	Agencia Aymaraes	5
3	Agencia Abancay	5
4	Agencia Andahuaylas	5
5	Agencia Uripa	5
6	Agencia Chuquibambilla	5
7	Agencia Cotabambas	5

8	Agencia Huancarama	5
9	Agencia Huaccana	5
10	Agencia Tintay	5
11	Agencia Antabamba	5
12	Agencia Curahuasi	5
13	Agencia Cusco	5
14	Agencia Huancavelica	5
15	Agencia Santo Tomás	5
Total		91

Nota: Se presentan la cantidad usuarios por sucursal de la organización, elaboración propia.

4.4.1 Modelo de Entrega

Para el diseño se tendrán en cuenta que los componentes estén alojados en el centro de datos local (On-Premises) de la organización. Es así que se requerirá que el equipo local de TI administre todos los aspectos de la solución.

Figura 24. Representación del modelo de entrega local. Adaptado de “Xenapp y Xendesktop 7.15 LTSR: Diseño”, por Citrix, 2020.

4.4.2 Topología de sitio

Para el diseño se contará con un solo sitio, en el cual se agruparán los servidores y aplicaciones para formar un solo entidad arquitectónica y de gestión. Todos los datos persistentes y dinámicos del sitio, incluido el sitio la configuración, las tareas de escritorio y el estado de sesión se almacenarán dentro de la base de datos centralizada con la que actualmente cuentan y la misma que cuenta con un clúster SQL ya implementado.

Además, este único sitio va tener que soportar las 91 sesiones concurrentes que se han solicitado en los requerimientos.

4.4.3 Estrategia de gestión de imágenes

Para la creación y administración de imágenes maestras se optará por la estrategia de imágenes en capas con la cual podremos crear imágenes maestras que son la fusión de una capa de sistema operativo, una plataforma y muchas aplicaciones.

Con ello reduciremos los esfuerzos asociados con el despliegue y actualización, cuando el administrador necesite actualizar el VDA de la versión 7.14 a 7.15 en diez imágenes, el administrador sólo actualiza una capa de plataforma única y el resto ya contará con la actualización.

Inicialmente, el enfoque de la imagen en capas requiere más tiempo para implementarse porque el administrador debe construir la biblioteca de capas de la organización. Sin embargo, una vez que las capas están disponibles, el tiempo para mantener las imágenes se reduce drásticamente.

4.4.4 Definición de grupos de usuarios

En este punto se alinearán los grupos de usuarios con las áreas a las cuales pertenecen, ya que la mayoría de los usuarios de una misma área consume el mismo conjunto de aplicaciones.

- Segmentación de usuarios

- **Seguridad:** En este punto indicaremos las directivas apropiadas para cada grupo de usuarios. Por ejemplo, si un usuario requiere un alto nivel de seguridad, como solución óptima para él se recomendará entregarle un token. Utilizaremos tres clasificaciones posibles:

Tabla 23

Segmentación de usuarios por nivel de seguridad

Nivel de seguridad	Descripción
Bajo	Los usuarios están autorizados para transferir datos desde y hacia el entorno virtualizado, el acceso es con usuario y contraseña vía pastrought.
Medio	Todo el tráfico de autenticación y de sesión debe estar protegido; no debe permitirse a los usuarios instalar ni modificar sus entornos virtualizados.
Alto	Para el acceso se tendrá que agregar un token de seguridad, además, se cifrará el tráfico de datos y este no podrá salir del centro de datos; todo el acceso de usuarios debe ser sometido a auditoría.

Nota: Se presentan la segmentación de usuarios según el nivel de seguridad. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- **Movilidad:** Para el caso de estudio hemos encontrado cuatro clasificaciones posibles:

Tabla 24
Segmentación de usuarios por movilidad

Movilidad	Requisito
Locales	Siempre utiliza el mismo dispositivo, conectado a una red interna, segura y de alta velocidad.
Local itinerante	Se conecta desde diferentes ubicaciones, pero siempre dentro de la red interna, segura y de alta velocidad.
Remota	A veces se conecta desde redes externas, que no son seguras y tienen una velocidad variable.
Móvil	A menudo necesita tener acceso cuando la conexión de red es intermitente o no está disponible.

Nota: Se presentan la segmentación de usuarios según el nivel de movilidad. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- **Carga de trabajo:** El tipo y la cantidad de aplicaciones a las que accede el usuario tiene un impacto en la densidad global. Para los usuarios que necesiten usar aplicaciones multimedia se tendrá que utilizar códec para optimizar su experiencia de usuario. Existen tres clasificaciones posibles:

Tabla 25
Segmentación de usuarios tipo de usuario

Tipo de usuario	Características
Ligero	1-2 aplicaciones de productividad de oficina.
Medio	2-10 aplicaciones de productividad de oficina y/o con uso ligero de multimedia.
Intensivo	Alto procesamiento de datos y uso intensivo de multimedia.

Nota: Se presentan la segmentación de usuarios según la carga de trabajo. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.5 Metodología del diseño: Capa de usuarios

En este punto desarrollaremos la capa superior del modelo de cinco capas de Citrix Virtual Apps, según la metodología de diseño del fabricante es la capa de usuarios, para la cual definiremos por cada grupo de usuarios que tengamos en la organización.

En este punto estableceremos la dirección general del entorno de cada grupo de usuarios, a su vez incorporaremos criterios de evaluación que vayan de la mano con las prioridades de la organización y los requisitos de cada grupo de usuarios con el objetivo de definir estrategias eficaces, las cuales impactarán sobre la flexibilidad y la funcionalidad de la plataforma, que son parte de la solución de los problemas definidos en los puntos 3.2.1 y 3.2.6.

Empezaremos por definir los dispositivos de punto final que se conectaran a la plataforma de virtualización de aplicaciones, entre ellos se cuentan:

- PC de escritorio
- Cliente ligero
- Smartphone
- Tableta
- Laptop

4.5.1 Propiedad de los dispositivos de punto final

Los dispositivos de punto final son propiedad de la organización y la administración es por cuenta de su área de TI. Sin embargo, la idea de poseer este tipo de plataformas ayudará a impulsar políticas empresariales para que los usuarios utilicen dispositivos personales en el trabajo (BYOD), con ello mejoramos en la satisfacción de los empleados, reducimos costes y simplificamos las labores de administración por parte del área de TI. El hecho de que BYOD sea una iniciativa que pueda retribuir grandes beneficios empresariales, no significa que se deba permitir a todos los usuarios usar dispositivos personales en el entorno corporativo.

Es por ello que definiremos los requisitos que deben cumplir los usuarios para que se le permita el uso de un dispositivo personal, estos se identificaron durante la segmentación de usuarios:

- **Seguridad:** Los usuarios que posean perfiles con información sensible no podrán acceder a través de dispositivos personales, con ello se evitara riesgos de robo de datos.
- **Movilidad:** Es usuarios que requieran siempre utilizar el mismo dispositivo, conectado a una red interna, segura y de alta velocidad, es posible que no puedan utilizar dispositivos personales.
- **Cargas de Trabajo:** Si el trabajo del usuario involucre el uso de aplicaciones instaladas localmente, es posible que el individuo tenga una mejor experiencia desde dispositivos propiedad de la organización.

4.5.2 Administración unificada de dispositivos de punto final (UEM)

Las soluciones UEM son un enfoque que nos permite asegurar y controlar computadoras de escritorio, laptops y dispositivos móviles de manera integral desde una sola consola, permitiendo al administrador de a través de los recursos de red poder tener visibilidad y control de los *endpoints*. Sin embargo, UEM es mucho más que solamente permitir o denegar el acceso a esos recursos, implica también la gestión del SSO (Single Sign On), administración de usuarios, revisión y actualización de dispositivos, administración de recursos, seguridad, control de acceso y entrega de aplicaciones.

El uso de este tipo de soluciones se vuelve en un aliado estratégico al permitir que los recursos de red y sus activos estén seguros, mientras se sigue otorgando al usuario final los medios para poder acceder a la información con la menor cantidad de obstáculos.

El termino UEM proviene de la evolución de tecnologías predecesoras como lo eran MDM (Mobile Device Management), el cual actuaba sobre dispositivos propiedad de la organización, este poseía una seguridad rígida que normalmente llevaba a los usuarios a saltarse las normas de seguridad o utilizar dispositivos propios para poder realizar su trabajo de forma eficiente. Luego la evolución nos llevo al BYOD (Bring Your Own Device), en la cual las *suites* de MDM evolucionaron hacia EMM (Enterprise Mobility Management) para reemplazar dispositivos propiedad de la empresa a la de los empleados, pero utilizados para hacer tareas de la empresa, en el EMM se enfocó en la visibilidad del dispositivo y su control para maximizar la productividad mientras se preservaba la seguridad de la información; a la vez que empezó a soportar una gran variedad de dispositivos móviles.

Las *suites* de UEM vienen a ser la última generación de este tipo de soluciones que gestiona y monitorea cada dispositivo de usuario, a través de todo el ciclo de vida (device deployment, configuración, seguridad, monitoreo y soporte). Los usuarios tienen la libertad de utilizar sus dispositivos y las organizaciones vigilan que se mantenga el acceso seguro a la información. (Hess, 2017)

4.5.3 Selección de Workspace

El acceso a la plataforma de aplicaciones requiere tener instalado el Citrix Workspace, el cual posee cliente de software fácil de instalar y que proporcionará el acceso a aplicaciones y datos de manera sencilla y segura desde cualquier dispositivo, incluidos smartphones, tabletas, PC y Mac.

Este utilizará el protocolo HDX construido sobre el protocolo ICA el cual se encarga de enviar solo las entradas de teclado y mouse al servidor remoto y recibir actualizaciones de capturas de pantalla en el dispositivo cliente y con ello optimizando el uso ancho de banda solicitado en el punto 3.2.3.

- Implementación inicial

En esta sección indicaremos los mecanismos a utilizarse para implementar y actualizar Citrix Workspace:

- **Directiva de grupo:** Para los clientes que se encuentren dentro de la red local, la implementación y configuración del Citrix Receiver se realizará mediante una directiva de grupo del directorio activo. Esta directiva funcionará a través de una plantilla ADMX descargada desde la página web del fabricante, desde ella se podrá elaborar la GPO. En el editor de directivas de grupo local, en la plantilla añadida, se realizará la siguiente configuración:

Citrix Workspace and Plugins\Windows\Workspace\Startup_Logon_Scripts

- **StoreFront:** Para los equipos que se encuentren fuera de la red local, el despliegue del Receiver se realizará a través del acceso a los almacenes de StoreFront vía su portal web. Este portal detecta si el usuario no cuenta o posee una versión desactualizada del Citrix Receiver, luego automáticamente descarga el paquete requerido para el sistema operativo cliente.
- **Instalación manual:** Para los equipos móviles y de propiedad de los usuarios el procedimiento se realizará manualmente ya sea a través de la descarga desde el sitio de descargas de Citrix Receiver o la búsqueda en las tiendas de Windows, Android y iOS. Al llegar a este sitio, se realiza la detección de clientes y se descargará el paquete específico en función de la plataforma y el sistema operativo. Cabe señalar que para el primer uso que realicen los usuarios se deberá introducir la URL del servidor. Esta opción se utiliza en un entorno BYOD.

Para mantener los dispositivos de punto final actualizados en su versión de Citrix Workspace más reciente, bastará con poseer como mínimo la versión 4.8 de Workspace para Windows y la versión 12.6 de Workspace en el caso de Mac, para que este lo detecte automáticamente y solicite al usuario auto instalar la versión más reciente. En el caso de dispositivos móviles, el Workspace para iOS y Android se actualizan automáticamente a través de su tienda correspondiente. (Citrix, 2020a)

4.6 Metodología del diseño: Capa De Acceso

La segunda capa de la metodología del diseño es la capa de acceso, que se define para cada grupo de usuarios. La creación de un diseño adecuado para la capa de acceso es una parte

importante del proceso de virtualización de aplicaciones. Esta capa gestiona la validación de usuarios mediante la autenticación y organiza el acceso a todos los componentes necesarios para establecer una conexión segura a la aplicación virtual, por lo que los requerimientos planteados en el punto 3.2.4 podrán ser atendidos.

Las decisiones para diseñar la capa de acceso se basan en los requisitos de movilidad de cada grupo de usuarios, así como en los dispositivos de punto final utilizados.

4.6.1 Autenticación

El acceso a los recursos se basa en la identidad del usuario. Al definir la estrategia de autenticación, se tiene en cuenta el punto de entrada del usuario en el entorno, así como la forma en que se autenticará el usuario, para ello tendremos que evaluar los siguientes puntos y decidir la que más se ajusta a nuestro escenario y requerimientos actuales.

4.6.1.1 Proveedor de autenticación

El modelo tradicional ha venido siendo a través de un usuario y una contraseña generado en el directorio activo, para obtener acceso a los recursos asignados al perfil. Como la mayoría de las organizaciones solían tener una implementación local de Active Directory, por lo que este requisito concreto era fácil de cumplir.

En esta nueva plataforma nos permitirá no solamente satisfacer a nuestros usuarios internos sino también cuando se requiera dar acceso a usuarios que no pertenezcan a nuestra organización, por lo que se requiere una cuenta para poder acceder a los recursos de nuestro diseño de Citrix Virtual Apps. Por eso, podríamos optar por el uso de un proveedor de identidades (IdP) de terceros (como Azure Active Directory, Google, etc.), en lugar de mantener un solo punto de autenticación local, el cual nos ayudaría en mantener la disponibilidad de este recurso.

Con la implementación del Servicio de autenticación federada de Citrix, en Citrix Virtual Apps se puede usar un IdP de terceros. Es así que el área de TI daría acceso a un tercero que utilizando las credenciales de su propia cuenta de Google u otro, podrá acceder a las aplicaciones, sin la necesidad de crear un usuario en nuestro dominio, lo que facilitará la incorporación de usuarios externos.

4.6.1.2 Punto de autenticación

Antes de que un usuario se conecte a un recurso virtual, primero debe autenticarse. El lugar de autenticación suele estar determinado por los requisitos de movilidad del grupo de usuarios, los cuales los detallamos en la tabla 22 con la segmentación de usuarios que se ha realizado dentro de la organización.

Asimismo, según la información anterior dispondremos para este diseño de dos puntos de autenticación en nuestra plataforma de Citrix Virtual Apps:

StoreFront: Citrix StoreFront ofrece servicios de autenticación y entrega de recursos para Citrix Receiver, lo que permite a los almacenes empresariales centralizados entregar las aplicaciones, este recurso lo utilizaremos para la autenticación tanto de usuarios locales como de los locales itinerantes.

Citrix Gateway: El servicio de Citrix Gateway será el recurso que proporcione el acceso seguro a las aplicaciones y los datos, y ofrece controles mediante directivas precisas que se pueden aplicar a aplicaciones y datos, a la vez que permite a los usuarios trabajar desde cualquier lugar y con ello cumplir el requerimiento planteado en la problemática del punto 3.2.6.

En la siguiente tabla, se indican los puntos de autenticación preferidos según los requisitos de movilidad del grupo de usuarios:

Tabla 26

Puntos de autenticación según tipo de usuario.

Requisitos de movilidad del grupo de usuarios	Punto de autenticación preferido
Locales	StoreFront
Local itinerante	StoreFront
Remota	Citrix Gateway
Móviles	Citrix Gateway

Nota: Se presentan puntos de autenticación preferidos según los requisitos de movilidad del grupo de usuarios. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

La autenticación para grupos de usuarios con un requisito de movilidad remota o móvil puede ocurrir directamente en StoreFront cuando sea necesario. Por ejemplo, puede que las directivas de seguridad DMZ prohíban el acceso desde NetScaler Gateway al dominio, acceso necesario para la autenticación de certificados del cliente con tarjetas inteligentes. En ese caso, el acceso a StoreFront para la autenticación se puede entregar a través de un servidor virtual SSL_BRIDGE de NetScaler, que ofrece un conducto para el tráfico HTTPS. Por regla general, el servidor virtual se alojaría junto a NetScaler Gateway en el mismo NetScaler configurado para proporcionar el acceso HDX Proxy al entorno del escritorio virtual. Aunque tal caso de uso pueda ser necesario a veces, se recomienda autenticar a los usuarios externos a través de NetScaler Gateway.

4.6.1.3 Directiva de autenticación

Ya habiendo identificado los puntos de autenticación, mencionaremos los tipos de autenticación a utilizar.

StoreFront: Este será utilizado para autenticar a usuarios dentro de nuestra red local. El StoreFront autentica a los usuarios directamente con Active Directory. A su vez tendremos varios métodos de autenticación, estos variarán de acuerdo al método de acceso del usuario, los requisitos de seguridad y la ubicación de la red. Para el diseño utilizaremos los siguientes.

- **Nombre de usuario y contraseña:** Requiere que los usuarios inicien sesión directamente en el sitio introduciendo un nombre de usuario y una contraseña.
- **PassThrough de dominio:** Nos permitirá realizar la transferencia de credenciales de dominio desde los dispositivos de los usuarios. Los usuarios realizarán la autenticación en los equipos unidos a un dominio de Windows y su sesión se inicia automáticamente cuando acceden a los almacenes de aplicaciones.
- **PassThrough de Citrix Gateway:** Nos permitirá la autenticación *PassThrough* desde Citrix Gateway. Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceda a sus almacenes de aplicaciones.

Citrix Gateway: Este será utilizado para autenticar a usuarios dentro de nuestra red externa. Citrix Gateway admite varios métodos de autenticación. Los métodos mencionados son los que se utilizarán para ofrecer la autenticación de varios factores.

- **LDAP:** A través de este protocolo ligero de acceso a directorios (LDAP) se podrá acceder a servicios de información de directorios como Microsoft Active Directory y podrá autenticar a los usuarios y extraer la información de pertenencia a grupos de esos usuarios.
- **RADIUS (token):** La opción de RADIUS se utilizará cuando el nivel de acceso a la aplicación sea alto, ya que esta consta de un protocolo de seguridad de red basado en UDP, el cual nos proporcionará autenticación, autorización y contabilidad. El servidor de acceso a la red (Citrix Gateway en este caso) reenviará las credenciales a un servidor de RADIUS el cual comprobará las credenciales localmente o comprobarlas en un servicio de directorio (IdP). Tras la comprobación, el servidor RADIUS según la validación que realice podrá aceptar la conexión, rechazarla o desafiarla y solicitar una segunda forma de autenticación, como un token.

En nuestro caso siendo una empresa mediana dedicada a las finanzas el cual ofrece a sus usuarios el acceso a aplicaciones virtuales con acceso a datos confidenciales, como registros de transacciones bancarias. Se rigen por normas de seguridad como la SSAE 16 y nos obliga a utilizar autenticación de varios factores para los usuarios de acceso remoto. La autenticación LDAP se ha implementado en función del nombre de usuario y la contraseña, junto con la autenticación RADIUS mediante tokens podremos cubrir los requerimientos del punto 3.2.4.

El tipo de autenticación de un grupo de usuarios suele determinarse en función de los requisitos de seguridad y el punto de autenticación utilizado. La siguiente tabla ayuda a definir la solución adecuada para cada grupo de usuarios en función del nivel de seguridad requerido:

Tabla 27
Puntos de autenticación según nivel de seguridad.

Punto de autenticación	Requisito de seguridad	Tipo de autenticación
StoreFront	Bajo, medio, alto	Bajo: Nombre de usuario y contraseña de LDAP; PassThrough. Medio: Nombre de usuario y contraseña de LDAP; PassThrough. Alto: LDAP y/o tarjeta inteligente Bajo: Nombre de usuario y contraseña de LDAP.

Citrix Gateway	Bajo, medio, alto	Medio: Nombre de usuario y contraseña de LDAP. Alto: LDAP y token; LDAP y tarjeta inteligente; token y tarjeta inteligente
----------------	-------------------	---

Nota: Se presentan solución adecuada para cada grupo de usuarios en función del nivel de seguridad requerido. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.6.2 StoreFront

Para nuestro diseño recurriremos al uso del servicio de Citrix StoreFront para poder autenticar a los usuarios en los recursos de Citrix Virtual Apps. El StoreFront nos permitirá indicar y agregar las aplicaciones disponibles en una única interfaz para que los usuarios accedan a través del Citrix Receiver para Windows, iOS o Android, o bien desde el portal web asignado por la organización.

4.6.2.1 Alta disponibilidad

Para cumplir con los requerimientos del punto 3.2.5 en cuanto a la disponibilidad de los recursos que forman parte del diseño, los cuales ante una caída permitirían que los usuarios no puedan iniciar nuevas aplicaciones publicadas ni administrar sus suscripciones. Es por ello, que se requiere implementar al menos dos servidores de StoreFront para evitar que este componente se convierta en un único punto de fallo. Al implementar una solución de equilibrio de carga, los usuarios no sufrirán interrupciones del servicio. Las opciones de alta disponibilidad con las cuales se cuentan son las siguientes:

- **Equilibrio de carga de hardware:** En esta opción el Citrix Gateway es el que se encarga de verificar la disponibilidad del servicio de StoreFront y equilibrar de forma activa la carga de las solicitudes de los usuarios. Citrix Gateway cumpliría la función de equilibrador de carga de hardware, este vendría a ser el modelo ideal de alta disponibilidad, ya que cumple con la función de equilibrador de carga, y asimismo viene preconfigurado con comprobaciones de estado de StoreFront, reenviando las solicitudes al segundo Storefront en caso el principal no se encuentre disponible.

- **Round robin de DNS:** Esta opción nos permite un equilibrio de carga básico en varios servidores sin realizar comprobaciones de disponibilidad. Sin embargo, si un servidor de

StoreFront deja de estar disponible, el round robin de DNS seguirá redirigiendo a los usuarios al servidor que ha fallado. Para el caso práctico no se utilizará round robin de DNS.

- **Equilibrio de carga de red de Windows:** Este servicio de Windows es capaz de realizar comprobaciones básicas para verificar la disponibilidad de nuestro servidor, pero a su vez no nos ayuda a determinar el estado de cada servicio. Esto podría provocar que se siga reenviando a los usuarios a los servidores de StoreFront que no estén en capacidad de procesar nuevas solicitudes. Los usuarios no podrían acceder a aplicaciones como resultado.

Viendo las bondades de las tres opciones de alta disponibilidad, es que optaremos por trabajar con el modelo de equilibrio de carga por hardware.

4.6.2.2 Referencia del Delivery Controller

Para poder proporcionar de aplicaciones a los usuarios, la plataforma deberá configurar el Storefront con la dirección IP o el nombre DNS de, al menos, un Controller en cada sitio de Citrix Virtual Apps. Asimismo, para la tolerancia a errores, se deberá indicar varios controladores para cada sitio. De forma predeterminada, StoreFront trata una lista de servidores en orden de conmutación por error (activa/pasiva).

A medida que se vaya creciendo la cantidad de usuarios que se conecten a la plataforma o haya una elevada carga de inicios de sesión, es que se optará por una distribución activa en la carga de usuarios (activa/activa). Esto se realizaría mediante un equilibrador de carga con monitores XML integrados, como Citrix Gateway, o mediante la configuración de StoreFront para equilibrar la carga de la lista de Controllers en lugar de tratarlos como una lista ordenada.

4.6.2.3 Balizas

Conforme a los requerimientos del punto 3.2.6 es que el Citrix Receiver utiliza balizas (sitios web) para identificar si un usuario se ha conectado a una red interna o externa. Los usuarios internos se conectarán directamente al StoreFront para autenticarse, mientras que los usuarios externos se conectarán a través del Citrix Gateway. Es posible controlar las aplicaciones que un usuario visualiza en su perfil, esto en función de la baliza a la que tienen acceso sea local o externa.

Para la baliza interna se configurará un sitio que no se pueda resolver externamente. De forma predeterminada, la baliza interna es la URL base que apunte al StoreFront. Para la baliza externa utilizaremos cualquier sitio externo que produzca una respuesta HTTP. El Citrix Receiver se encargará de supervisar continuamente el estado de las conexiones de red tales como enlaces activos, enlaces inactivos o cambios de la puerta de enlace predeterminada. En caso se detecte un cambio de estado, el Citrix Receiver en primera instancia verificará que se pueda acceder a los puntos de la baliza interna antes de pasar a comprobar la accesibilidad de los puntos de la baliza externa. StoreFront proporcionará al Citrix Receiver las direcciones HTTP(s) de los puntos de la baliza durante el proceso inicial de descarga de la conexión/configuración y ofrecerá las actualizaciones en casa se realice alguna modificación. Para poder otorgarle de alta disponibilidad es que se especificara de al menos dos balizas externas que puedan resolverse desde redes externas.

4.6.2.4 Presentación de los recursos

En este punto el área de TI deberá determinar las aplicaciones que deben mostrarse siempre a los usuarios en su pantalla de inicio o en la ficha destacada. En general, estas aplicaciones serán desplegadas según al área al que pertenezcan y/o cualquier otra aplicación que puedan necesitar todos los usuarios de un entorno. StoreFront puede filtrar o presentar estos recursos mediante palabras clave definidas en el campo descripción de las propiedades de las aplicaciones publicadas para así facilitar la tarea de despliegue

4.6.2.5 Grupos de agregación

Para el caso práctico la solución Citrix Virtual Apps incluirá varios sitios de entrega debido a la cantidad de usuarios con los cuales se cuenta, por lo que el StoreFront deberá combinar los recursos disponibles para que el usuario disponga de una única interfaz para todos los recursos publicados. Sin embargo, si varios sitios publican los mismos recursos, en la vista de aplicaciones el usuario puede que se muestre una sola aplicación varias veces como en la figura siguiente.

*Figura 25.*Representación de la vista sin grupos de agregación en el Citrix Storefront. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Para evitar ello es que se definirá grupos de agregación de StoreFront los cuales permitirán combinar los recursos de varios sitios para proporcionar al usuario una vista única e intuitiva. Con ello StoreFront agrupará los recursos publicados duplicados en un solo icono como se muestra en la siguiente imagen.

*Figura 26.*Representación de la vista sin grupos de agregación en el Citrix Storefront. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Una vez configurado los grupos de agregación determinaremos la forma de cómo equilibrar la carga de los usuarios en los diferentes sitios de Citrix Virtual Apps cuando es un icono de agregación. Las opciones que manejaremos son las siguientes:

- **Equilibrio de carga:** Debido a que vamos a utilizar varios sitios de acceso a las aplicaciones, utilizaremos umbrales de acuerdo a las recomendaciones sobre la capacidad de cada sitio. El StoreFront se encargará de distribuir cada una de las solicitudes de los usuarios por todos los sitios configurados.
- **Conmutación por error:** Para poder utilizar este tipo de funcionalidad se tendrá que contar un site adicional ya sea local o en la nube, esto nos permitirá disponer de recursos en caso

ocurra una interrupción del servicio para el traslado de usuarios de un sitio a otro. Para este diseño se ha considerado contar con una plataforma en espera en caso el site principal tenga una interrupción.

A continuación, brindaremos la lista de usuarios, los almacenes con los que se cuentan y los métodos de agregación durante la fase de diseño.

Tabla 28

Puntos de autenticación según tipo de usuario.

Grupo de usuarios	Almacenes disponibles	Almacenes de equilibrio de carga	Almacenes de conmutación por error
Intensivo	XAPP_01, XAPP_02, XAPP_03, ASR01	XAPP_01, XAPP_02, XAPP_03	ASR01
Ligero	XAPP_01, XAPP_02, ASR01	XAPP_01, XAPP_02	ASR01

Nota: Se presentan los usuarios, los almacenes y los métodos de agregación durante la fase de diseño. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.6.2.6 Escalabilidad

Dentro de las problemáticas planteadas en el punto 3.2.3, se menciona un modelo carente de escalabilidad, esto debido a la expansión de la organización y la falta de flexibilidad por parte de la plataforma para conectar la cantidad de usuarios adicionales.

Es por ello que para diagramar la cantidad de usuarios de Citrix Workspace que admite un único servidor de StoreFront tendremos que tener en cuenta los recursos que se van asignar y el nivel de actividad de los usuarios en la plataforma. Asimismo, tener en cuenta que los usuarios de Receiver para Web consumirán más RAM que los usuarios nativos de Receiver, por lo que se recomienda un mínimo de 4 GB de RAM por servidor de StoreFront en todos los casos como base. Además, si hay más sitios o usuarios por almacén, esto incrementará la utilización de la CPU y el tiempo de respuesta del servidor. Para el caso práctico se tendrá un clúster de 2 nodos para el Storefront, los recursos y la cantidad de actividades que soportará se indicará en la siguiente tabla.

Tabla 29

Características diseño Storefront.

Implementación de StoreFront	Uso de CPU	Actividades simultáneas
Implementación independiente: 4 CPU, 4 GB de RAM, uso intensivo (inicio de sesión, enumeración, suscripción, cancelación de suscripción, cierre de sesión)	75%	291 por segundo
Implementación independiente: 4 CPU, 4 GB de RAM, uso intensivo (inicio de sesión, enumeración, suscripción, cancelación de suscripción, cierre de sesión)	90%	375 por segundo
Implementación de StoreFront en clúster: 2 nodos, cada uno con 4 unidades CPU, 4 GB de RAM, uso intensivo (inicio de sesión, enumeración, suscripción, cancelación de suscripción, cierre de sesión)	75%	529 por segundo
Implementación de StoreFront en clúster: 2 nodos, cada uno con 4 unidades CPU, 4 GB de RAM, uso intensivo (inicio de sesión, enumeración, suscripción, cancelación de suscripción, cierre de sesión)	90%	681 por segundo

Nota: Se presentan las especificaciones técnicas asignadas al Storefront, el porcentaje de CPU utilizado y la cantidad de actividades en simultáneo que soporta. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Viendo la cantidad de actividades que podemos realizar en simultaneidad podremos indicar que para la cantidad actual de usuarios se daría abasto y nos permitirá crecer en la capacidad de inicio de sesión hasta 529 usuarios al 75% de la capacidad del Storefront.

Por último, cabe indicar que las pruebas del fabricante indican una disminución del rendimiento cuando una sola implementación de StoreFront crece más de 3 o 4 nodos de StoreFront con un máximo de 5 o 6 servidores admitidos en un único grupo de servidores, por lo que en caso se requiera aumentar rendimiento sería suficiente con incrementar el CPU asignado a las máquinas virtuales al sistema

4.6.3 Citrix Gateway

Para el grupo de usuarios que utilizan Citrix Gateway como punto de autenticación indicaremos un conjunto de decisiones de diseño adicionales. Estas decisiones de diseño no serán aplicadas a puntos de autenticación que no sean Citrix Gateway.

4.6.3.1 Topología

Para la selección de la topología de red se ha tenido que planificar que la arquitectura de acceso remoto pueda garantizar la funcionalidad, el rendimiento y la seguridad necesarios y además que vayan de la mano con los problemas planteados con los puntos 3.2.4, 3.2.5 y 3.2.6. Es por ello que el diseño de la arquitectura de acceso remoto debe completarse en colaboración con el equipo de seguridad de la organización para así poder garantizar el cumplimiento de los requisitos de seguridad corporativos. Para nuestro caso en estudio utilizaremos la topología de dos brazos que detallaremos a continuación.

- **Dos brazos (alta seguridad):** Con la topología de 2 brazos, el Citrix Gateway utilizará dos o más interfaces enlazadas física o lógicamente, con las redes LAN virtuales y sus subredes IP asociadas. El transporte del tráfico front-end para los usuarios se dirigirá a una de estas interfaces. El tráfico front-end está aislado del tráfico back-end que se realizan entre los servicios y los servidores de la infraestructura de escritorios virtuales, que se dirige a una segunda interfaz. Eso permite el uso de zonas desmilitarizadas (DMZ) separadas para aislar los flujos del tráfico front-end y back-end, junto con un control y una supervisión granulares de los dos firewalls con los que actualmente la organización posee.

Figura 27. Representación de la topología de dos brazos con dos zonas desmilitarizadas (DMZ) separadas para aislar los flujos del tráfico front-end y back-end. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.6.3.2 Alta disponibilidad

Si el Citrix Gateway no está disponible, los usuarios remotos no podrán acceder al entorno. Por lo tanto, se deben de tener en cuenta en el diseño al menos dos hosts Citrix Gateway para evitar que este componente se convierta en un único punto de fallo.

Al configurar Citrix Gateway en un par de alta disponibilidad (activo/pasivo), el Citrix Gateway secundario supervisará el primer dispositivo enviándole mensajes periódicos, también denominados mensajes de latido o comprobaciones de estado, para determinar si el dispositivo principal acepta conexiones. En caso se produzca un error en la comprobación del estado, el Citrix Gateway secundario volverá a intentar la conexión durante un período de tiempo que especifiquemos hasta que determine que el dispositivo principal no funciona. Si el dispositivo secundario confirma el error de comprobación del estado, el Citrix Gateway secundario toma el lugar del Citrix Gateway principal.

4.6.3.3 Plataforma

Para identificar la plataforma Citrix Gateway idóneo para cumplir los requisitos del proyecto, se deben identificar las restricciones clave de los recursos. Dado que todo el tráfico de acceso remoto se protegerá mediante la capa de sockets seguros (SSL), transportada por el protocolo de transferencia de hipertexto (HTTP), se tendrán que tener en cuenta dos métricas de recursos:

- **Procesamiento de SSL:** El procesamiento de SSL son los gigabits del tráfico SSL que se pueden procesar por segundo (Gbps).
- **Transacciones SSL por segundo (TPS):** La métrica TPS identifica cuántas transacciones por segundo Application Delivery Controller (ADC) puede ejecutar una transacción SSL. La capacidad variará principalmente en función de la longitud de clave requerida, para este diseño consideraremos llaves de 2048 bits. La capacidad de TPS es una consideración útil principalmente durante la fase de negociación, cuando SSL se configura por primera vez, y es menos un factor en la fase de cifrado y descifrado por lotes, que es la mayor parte de la sesión.

Si bien la métrica del TPS es importante que supervisar, las buenas prácticas sugieren que el procesamiento de SSL sea el factor más importante para identificar el Citrix Gateway apropiado.

La sobrecarga media del ancho de banda de un certificado SSL se considerará insignificante en relación con el volumen de tráfico de una aplicación virtual utilizada y no se suele tener en cuenta como parte del procesamiento de SSL requerido. Sin embargo, hacer provisiones para el ancho de banda de SSL garantizará que el procesamiento total estimado sea suficiente. Este ancho de banda variará según los algoritmos de cifrado que se utilicen, así como con los tamaños de paquetes. Según las recomendaciones lo idóneo es considerar en el ancho de banda de la carga de trabajo en un 2%, por lo que, para determinar el procesamiento de SSL requerido para nuestra plataforma de Citrix Gateway, multiplicaremos por 1,02 el máximo de ancho de banda simultáneo para un centro de datos:

Procesamiento de SSL = Máximo de ancho de banda simultáneo x 1,02

Por ejemplo, para nuestro caso práctico en el cual contamos con 55 usuarios y la media del consumo de usuario por aplicación es de aproximadamente de 0.59 Mbps, el modelo de Citrix Gateway apropiado se puede determinar de la siguiente manera:

$55 \text{ usuarios} \times 0.59 \text{ Mbps} = 32.45 \text{ Mbps}$

$\sim 34 \text{ Mbps} = 32.45 \text{ Mbps} \times 1,02$

Este valor del procesamiento de SSL lo compararemos con las prestaciones de rendimiento de las plataformas de Citrix Gateway disponibles con el objetivo de determinar la más adecuada para nuestro entorno. Para nuestro caso práctico se optará por el tipo VPX.

- **VPX:** El dispositivo Citrix Gateway VPX es un servidor virtual el cual nos proporcionará las mismas funcionalidades completa que un Citrix Gateway en hardware. Sin embargo, los dispositivos NetScaler VPX nos ayudará a aprovechar los recursos de hardware con los que cuenta actualmente la organización, y son adecuados para entornos de tamaño pequeño y mediano en el cual nos ubicamos. Normalmente, este tipo de recursos nos permite un crecimiento de hasta 500 usuarios para las instancias de VPX.

Verificando la lista de prestaciones del procesamiento de SSL de nuestro escenario y las hojas de datos de la plataforma de Citrix Gateway VPX, podríamos indicar que el modelo

VPX 200 sería suficiente para manejar la carga requerida, ya que cumple con los parámetros de desempeño diagramados como se detalla en la siguiente imagen.

	VPX 3000	VPX 1000	VPX 200	VPX 10
NetScaler VPX system requirements ^{1,2}				
Processor ³	2-4 vCPUs Intel VTx or AMD-V	2-4 vCPUs Intel VTx or AMD-V	2 vCPUs Intel VTx or AMD-V	2 vCPUs Intel VTx or AMD-V
Memory ⁴	2 GB	2 GB	2 GB	2 GB
Hard drive	20 GB	20 GB	20 GB	20 GB
Hypervisor			XenServer 6.0, 6.1 and 6.2 VMware ESXi 4.x, 5.1, 5.5 Microsoft Hyper-V 2008 R2, 2012 R1 KVM	
Pay as you grow license upgrade	N/A	Upgrade option to VPX 3000	Upgrade options to VPX 1000 and VPX 3000	Upgrade options to VPX 200, VPX 1000 and VPX 3000
NetScaler VPX performance ⁵				
System throughput	3000 Mbps	1000 Mbps	200 Mbps	10 Mbps
SSL transaction/sec (2K key certificates)			Up to 750	
SSL throughput, Gpbs			Up to 1.0	
Compression throughput, Gbps			Up to 0.75	
SSL VPN/ICA proxy concurrent users			Up to 1500	

*Figura 28.*Representación de las especificaciones de los modelos de Citrix VPX. Adaptado de “NetScaler VPX: Virtualizing the power of advanced web and application delivery and remote access services” por Citrix, 2015.

Sin embargo, la escalabilidad dependerá, en realidad, de los requisitos de seguridad, ya que el procesamiento de SSL de NetScaler disminuye con el uso de algoritmos de cifrado cada vez más complejos y longitudes de clave más largas, en nuestro caso tenemos un exceso del 588% en lo que respecta al procesamiento SSL lo que nos permitirá tener un buffer necesario podrá dar carta libre a desarrollar nuestras políticas de seguridad. Cabe recalcar, que este cálculo representa un único dispositivo Citrix Gateway principal. Por lo que para poder tener redundancia de N+1 se requeriría un dispositivo Citrix Gateway adicional de la misma plataforma y en el mismo modelo.

4.6.3.4 Directiva de pre-autenticación

Esta directiva nos permitirá sumar funcionalidades de seguridad que nos ayudarán a cumplir los requerimientos del punto 3.2.4, estas directivas de pre-autenticación serán aplicados a los grupos de usuarios que tienen al Citrix Gateway como punto de autenticación. La función de las directivas de pre-autenticación es la de limitar el acceso al entorno en función de si el dispositivo de punto final cumple determinados criterios mediante un análisis de Endpoint Analysis (EPA).

Las directivas de acceso de pre-autenticación se pueden configurar para probar antivirus, firewalls, sistemas operativos o incluso la configuración del Registro. Estas directivas se pueden utilizar para impedir el acceso por completo al portal o las puede usar Citrix Virtual Apps para controlar la disponibilidad de aplicaciones, la asignación de portapapeles e incluso la asignación de impresoras. Por ejemplo, si un dispositivo de usuario no tiene antivirus instalado, se puede establecer un filtro para ocultar aplicaciones que tengan un alto nivel de criticidad.

La siguiente imagen ofrece una descripción general de cómo se pueden utilizar varias directivas para personalizar las funciones de un recurso de virtualización:

Figura 29. Representación del diagrama de flujo de directivas de pre-autenticación para el cumplimiento de directrices de seguridad implementadas. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Para el caso de nuestra organización sería ideal utilizar EPA para escanear dispositivos de punto final y comprobar que tienen instalados los certificados necesarios en el dispositivo que les permita el acceso a las aplicaciones.

4.6.3.5 Directiva de sesión

Los usuarios que tengan al Citrix Gateway como punto de autenticación deberán tener definidas directivas de sesión que les corresponda. Estas serán las que definan la experiencia general de usuario posterior a la autenticación.

Para el caso práctico crearemos directivas de acuerdo con el tipo de dispositivo Citrix Receiver utilizado, estos se agruparán en no móviles (Windows, Mac y Linux OS) y móviles (iOS, Android y Windows Phone). En nuestro escenario aceptaremos la compatibilidad con dispositivos móviles, dispositivos no móviles en función de los requisitos de los dispositivos cliente identificados durante la fase de evaluación.

Para identificar las directivas de sesión de dispositivos, se incluirán las siguientes expresiones.

- **Dispositivos móviles:** La expresión se establece en REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver, que tiene una prioridad más alta que la directiva de dispositivos no móviles para garantizar que los dispositivos móviles se detecten.

- **Dispositivos no móviles:** La expresión se establece en ns_true, lo que significa que debe aplicarse a todo el tráfico que se le envíe.

Estas directivas de sesión también se pueden usar para aplicar expresiones de análisis de dispositivos de punto final. Estas directivas de sesión se aplican después de la autenticación, pero imitan las directivas de pre-autenticación mencionadas anteriormente. El uso de directivas de sesión es una opción para ofrecer un plan B a los dispositivos de punto final que no cumplen todos los requisitos de seguridad, como el acceso de solo lectura a aplicaciones específicas. (Citrix, 2020b)

4.6.3.6 Perfil de sesión

Las directivas de sesión definidas anteriormente tendrán asignadas un perfil de sesión correspondiente. El perfil de sesión define los detalles necesarios para que el grupo de usuarios obtengan acceso al entorno. Existen dos formas principales de perfiles de sesión que determinan el método de acceso al entorno de las aplicaciones virtuales tanto el VPN SSL como el HDX Proxy, para este caso utilizaremos el segundo tipo de acceso y lo detallaremos a continuación.

- **HDX Proxy:** Con HDX Proxy, los usuarios se conectarán a sus aplicaciones virtuales a través de Citrix Gateway sin exponer direcciones internas externamente. En esta configuración, Citrix Gateway utilizará una micro VPN y sólo enviará el tráfico HDX tal y como se muestra en la figura 30. Otros tipos de tráfico en el dispositivo de punto final del cliente, como tráfico personal hacia Internet, no serán utilizados por el Citrix Gateway.

En función del dispositivo de punto final y el dispositivo Citrix Receiver que se utiliza en la organización, este método será el que se utilizará en cada grupo de usuarios, además la mayoría de los dispositivos Citrix Receiver admiten HDX Proxy. El uso de HDX Proxy otorgará de acceso seguro para el ingreso a las aplicaciones virtuales desde sedes remotas, ya que solamente el tráfico específico de la sesión de la aplicación tiene permiso para atravesar la infraestructura corporativa.

Figura 30. Representación de la directiva de sesión del tipo HDX Proxy. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.7 Metodología del diseño: Capa de recursos

La aceptación general de la solución por parte del usuario depende en gran medida de las decisiones tomadas en esta capa, ya que nos enfocaremos específicamente en los grupos de usuarios. Dicho esto, en esta parte diagramamos las características que deberán tener los perfiles, la impresión, las aplicaciones y el desempeño que esta debe mostrar, todos estos puntos desempeñarán un papel fundamental a la hora de que las aplicaciones se ajusten a los requisitos del grupo de usuarios, requisitos identificados en los puntos 3.2.1, 3.2.2 y 3.2.3.

4.7.1 Experiencia de usuario

En esta sección definiremos los códec, los protocolos de transporte y las capacidades de autoservicio a utilizar en la plataforma, los cuales afectarán en la experiencia general y a su vez se esperará poder asemejar o mejorar a la experiencia de una aplicación instalada localmente en nuestro centro de datos. En esta parte procuraremos darle el diseño adecuado para que la experiencia de usuario puede solventar los problemas de red que tenemos localizados en sucursales.

4.7.1.1 Protocolo de visualización

El protocolo de visualización determinará la calidad de las imágenes estáticas, el vídeo y el texto dentro de la sesión del usuario, así como el impacto en la escalabilidad del servidor en el cual se encuentra instalada la aplicación. Para este punto se elegirán las siguientes opciones:

- **H.264:** Protocolo orientado al uso predominantemente de aplicaciones multimedia. Este ofrece velocidades de fotogramas más altas necesarias para vídeos de alta calidad, al mismo tiempo que ahorra ancho de banda de red. Estos beneficios se producen a expensas del tiempo de procesamiento de la CPU, lo que reduce la escalabilidad y densidad del servidor de aplicaciones.

- **Thinwire:** El principio de este protocolo se basa en la transferencia de datos sin ocupar mucho ancho de banda. Es utilizado en la mayoría de los casos de uso, ya que ofrece una buena experiencia de usuario con costes mínimos de recursos. A su vez existen dos variaciones de Thinwire:

 - Antiguo:* Optimizado para motores gráficos Windows 7 y Windows 2008

 - Thinwire+:* Optimizado para el motor de gráficos de Windows 10, Windows 2012 y Windows 2016

- **Selective H.264 (pantalla adaptable):** El protocolo a utilizar en la plataforma es este, y consiste en el uso en simultáneo de los códec H.264 y Thinwire+ para partes de la pantalla. A su vez se subdivide según la casuística que tengamos.

 - Do not use:* Sólo se usa Thinwire+, no H.264. Ideal para usuarios sin vídeos ni otras aplicaciones que necesitan gráficos generados por el servidor.

Para la pantalla entera: Solo se usa H.264. Ideal para usuarios con un uso intensivo de vídeos y gráficos 3D generados por el servidor, especialmente en situaciones de bajo ancho de banda.

Para áreas en cambio constante: Este utiliza H.264 para las partes de la pantalla que cambian constantemente, mientras que el resto de la pantalla usa Thinwire+. (Citrix, 2020c)

- **Códec de compresión sin pérdida (MDRLE):** El codificador MDRLE posee una razón de compresión más alta y con menor consumo de ancho de banda que el códec 2DRLE en sesiones de escritorio estándar. Este codec trabaja de la mano con Thinwire y lo utiliza para descomponer texto e imágenes simples, que a menudo formará gran parte de lo que el usuario verá en su labor diaria, es así que los mapas de bits serán comprimidos por este códec sin pérdida de Citrix. El uso del códec MDRLE otorga aproximadamente, entre un 10 y un 15 % de reducción en el consumo del ancho de banda brindando una interactividad de sesión mejorada y costes reducidos. (Citrix, 2016a)

Esta última variante mencionada es la mejor opción para la mayoría de los usuarios que van a acceder a nuestra plataforma, ya que no solo no solo nos beneficiará en el impacto en la experiencia general del usuario, sino también en la escalabilidad del servidor según los requerimientos definidos en el punto 3.2.3.

4.7.1.2 Protocolo de transporte

Para definir el protocolo a usar en este diseño definiremos a grandes rasgos las tres formas de transportar el protocolo HDX a través de la red:

- **TCP:** Protocolo de transporte común por LAN y conexiones WAN de latencia baja, pero sufre cuando las distancias de conexión aumentan, lo que aumenta la latencia y conlleva más retransmisiones.
- **EDT:** Protocolo de transporte propietario de Citrix, basado en UDP. Para redes de latencia alta o pérdida de paquetes, más comunes en enlaces WAN de larga distancia. Ofrece una experiencia más interactiva para el usuario, sin aumentar por ello la carga de CPU en el servidor, aunque consume más ancho de banda de red que TCP.
- **Transporte adaptativo:** Utiliza los protocolos de transporte TCP y EDT. En redes que no admiten el transporte de EDT por la red hace el cambio automático a TCP.

El protocolo elegido para la presente plataforma va ser el de transporte adaptativo como la opción estándar de transporte, con ello tanto EDT y TCP intentarán en paralelo durante la conexión inicial, la reconexión de fiabilidad de la sesión y la reconexión automática de clientes. Esta mejora reduce el tiempo de conexión cuando se prefiere EDT, pero en caso el transporte UDP subyacente necesario no esté disponible recurre a TCP.

De forma predeterminada, después de recurrir a TCP, el transporte adaptable sigue buscando EDT cada 5 minutos.

Para que pueda trabajar bajo este protocolo se tendrán que habilitar los siguientes requisitos:

- Tener instalado en el servidor de aplicaciones sólo agentes VDA IPv4. No se admiten configuraciones de IPv6 ni mixtas
- Agregar reglas de firewall para permitir el tráfico entrante en los puertos UDP 1494 y 2598 del VDA.

4.7.1.3 Optimización de inicios de sesión

Cuando un usuario ingresa sus credenciales en Windows a la plataforma de Citrix Virtual Apps, ocurren una serie de pasos para configurar completamente su entorno de usuario, ya que al inicializar la sesión se comienza a aplicar el perfil del usuario, las preferencias de la política de grupo, ejecutar scripts de inicio de sesión, unidades de mapeo e impresoras de mapeo. Tal y como se muestra en la siguiente imagen.

Figura 31. Representación del Inicio Sesión Clásico en Citrix Apps. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Una vez que todos estos procesos se completan, el shell se inicializa, el usuario podrá recién interactuar con su interfaz de aplicaciones.

Es por ello que para evitar este tipo de retrasos la solución más fácil es simplemente eliminar estas operaciones que requieren mucho tiempo de nuestro inicio de sesión, esto a través del servicio llamado Workspace Environment Management podremos lograr dicho cometido.

*Figura 32.*Representación del Inicio Sesión con el agente WEM. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Tal y como se muestra en la imagen, el Workspace Environment Management elimina todas estas operaciones y aplica las asignaciones, los scripts y los perfiles en segundo plano, después de inicializar la sesión y las aplicaciones. El usuario recibe el mismo entorno, pero recibe su interfaz de forma más rápida, y con ello colaborando con los requerimientos del punto 3.2.3.

4.7.1.4 Configuraciones de directiva de presentación visual

Estas son un conjunto de configuraciones en las directivas que nos ayudaran a establecer la calidad de las imágenes enviadas desde los escritorios virtuales a los dispositivo finales de nuestros usuarios.

- Profundidad de color preferida para gráficos simples

Al habilitar esta funcionalidad nos permitira reducir la profundidad de color en los graficos que se envian a través de la red, las opciones a elegir estan entre 8 a 16 bits por pixel (el valor predeterminado es la profundidad de color es de 24 bits por píxel) los cuales nos ofrecerán una mejora potencial en el desempeño en conexiones con escaso ancho de banda, el costo de

ello será una leve degradación en la calidad de la imagen. Estas opciones se utilizan siempre y cuando no se utilice el códec de vídeo para compresión definida para la pantalla entera.

- **Velocidad de fotogramas de destino**

Esta configuración nos servirá para especificar la cantidad máxima de fotogramas por segundo (fps) que se envían desde el escritorio virtual al dispositivo final del usuario. De forma predeterminada, el valor máximo es 30 fotogramas por segundo, la cual permite una mejor experiencia del usuario, pero a cambio de mayor consumo de ancho de banda.

Por lo que reducir la cantidad de fotogramas por segundo a 10 nos permitirá maximizar la escalabilidad del servidor y obtener menores consumos de ancho de banda, esto a costa de una mejor experiencia de usuario.

- **Calidad visual**

En esta parte podremos elegir el tipo de configuración de calidad visual de las imágenes que se mostrarán en el dispositivo del usuario, de forma predeterminada se establece en Media.

Las opciones disponibles para especificar la calidad de imagen son las siguientes:

- **Baja:** Su uso se da en red de ancho de banda limitado donde el coste de calidad visual puede ser sacrificado por una mayor interactividad.
- **Media:** Esta opción es la que nos ofrece la mejor eficiencia de rendimiento y ancho de banda para los casos de uso que podamos tener.
- **Alta:** Opción utilizada cuando se requiere calidad de imagen sin pérdida y se dispone de un buen ancho de banda.

Para el diseño planteado optaremos entre las opciones Media y Baja según el ancho de banda que se disponga en el lugar desde donde se trate de acceder a las aplicaciones.

4.7.1.5 Configuraciones del método criptográfico

Para el diseño elaborado utilizaremos un método de criptografía de clave pública asimétrico de curva elíptica (ECC) el cual se basa en curvas elípticas sobre campos finitos. Entre las características que esta otorgará al diseño indicaremos:

- **Tamaño de clave más pequeño:** ECC posee el mismo nivel de fuerza criptográfica que sus contrapartes pero con tamaños de clave considerablemente más pequeños. Esto da como resultado en un menor consumo de recursos computacionales y de ancho de banda.

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Figura 33. Tabla de recomendaciones de tamaños de clave por la NIST (Instituto Nacional de Estándares y Tecnología) Adaptado de “Recommendation for Key Management”, por NIST, 2016.

Como se puede ver en la tabla anterior, la comparacion de tamaños de clave entre la RSA y el ECC indican que la diferencia de tamaño sigue aumentando a medida que crecen la cantidad de bits utilizados.

- **Mayor velocidad:** Al poseer un tamaño de clave mas pequeño, permite que el procesamiento sea más agil y con ello un tiempo de carga del portal de acceso más rápido con lo cual se mejora la experiencia del usuario final. (Citrix, 2016b)

4.7.2 Datos del usuario

Para poder reducir los tiempos de acceso a la información diseñaremos un modelo en el cual los datos estén lo más cerca de la aplicación y con ello el usuario tenga una buena experiencia. Ya que a medida que aumenta la distancia entre la aplicación y los datos, la latencia también aumenta, lo que ralentiza cualquier operación de archivo (abrir, guardar, modificar).

- Ubicación de los datos del usuario

El almacenamiento requerido para el uso de las aplicaciones se encontrará almacenadas localmente ya que a los servidores los cuales brindaran el acceso a las aplicaciones se conectan al servidor de base de datos actual que ya está en producción, la cual cuenta con sus volúmenes almacenados en el datastore de la organización.

Por otro lado, la data generada por la creación de perfiles de los usuarios que se conectan a la plataforma tiende a ser despreciable, ya que los archivos que generan de la interacción con las aplicaciones se pueden almacenar en el dispositivo final desde el cual se accede.

- Recuperación de datos

La data generada por la interacción con las aplicaciones se almacena en el servidor de base de datos, el cual posee un volumen perteneciente a una LUN con arreglo de disco RAID 10, asimismo la organización cuenta con un servidor Veeam Backup el cual genera copias de seguridad de a base de datos del tipo incrementales sacadas diariamente y almacenadas en cintas. (Citrix, 2019b)

4.7.3 Directivas

En esta parte se definirán las directivas con las que debe contar el diseño, los cuales ofrecerán la base para configurar y ajustar los entornos de nuestra plataforma de virtualización, y con ello controlar la configuración de la conexión, la seguridad y el ancho de banda en función de diversas combinaciones de usuarios, dispositivos o tipos de conexión.

Para lograr este propósito tendremos que tener en cuenta tanto las directivas de Microsoft como las de Citrix para englobar todas las configuraciones de optimización, seguridad y experiencia del usuario.

- Motor preferido para las directivas

Para nuestro escenario utilizaremos las directivas de grupo de Active Directory a través de archivos ADMX de Citrix, los cuales nos permitirán ampliar las directivas de grupo y realizar mecanismos avanzados de filtrado. A través del uso de estas directivas de grupo de Active Directory nos permitirá administrar directivas de Windows y directivas de Citrix en la misma ubicación, y así minimizar las herramientas administrativas necesarias para la administración de directivas.

Estas directivas de grupo se replicarán automáticamente en los controladores de dominio, por lo que la información estará protegida y la aplicación de las directivas se verán simplificadas.

- Integración de las directivas

Para el escenario diseñado se van a requerir configurar directivas tanto de Active Directory como de Citrix para crear así un entorno completamente configurado. En casos con el de estudio en el cual se cuentan con Servicios de Escritorio remoto (RDS) de Windows y recursos de Citrix, se puede configurar funcionalidades similares en dos ubicaciones diferentes. Para evitar estas confusiones, las directivas de RDS sólo se configurarán donde sea necesario y verificando que no haya ninguna directiva correspondiente en la configuración de Citrix Virtual Apps, o que la configuración sea necesaria específicamente para el uso de RDS dentro de la organización. La configuración de directivas de manera granular simplificará el proceso de comprensión del conjunto resultante de directivas y facilitará asimismo la solución de problemas en las configuraciones de directivas.

4.7.4 Impresión

En este punto se planificará e indicará la solución de impresión adecuada de acuerdo a nuestro escenario, para ello comprenderemos las tecnologías disponibles, así como sus ventajas y limitaciones.

- Aprovisionamiento de impresoras

El proceso de creación de impresoras al inicio de una sesión de Citrix Virtual Apps, para nuestro diseño el enfoque a utilizar es el siguiente:

- Impresoras basadas en la sesión

A través de este método el conjunto de impresoras de red será asignadas a los usuarios mediante una directiva de Citrix al inicio de cada sesión. Estas serán asignadas basadas en la proximidad de la dirección IP de la subred desde la cual accede a sus aplicaciones. Las impresoras de red creadas con esta directiva variarán en función de la ubicación del dispositivo de punto final del usuario. La impresión de proximidad nos servirá en situaciones en las que los usuarios se conectan desde diferentes ubicaciones utilizando el mismo dispositivo de punto final (es decir, portátil, tableta).

- Enrutamiento de impresoras

Al estar las impresoras aprovisionadas como impresoras de sesión, el enrutamiento de los trabajos de impresión ya no se realiza a través del dispositivo de punto final del usuario sino

se basarán en la ubicación de red del dispositivo de punto final, la sesión del usuario y el servidor de impresión.

Por lo que la recomendación es la de montar al menos un servidor donde se encuentre desplegado Citrix Universal Print Server, el cual puede estar montado sobre un servidor de impresiones de Windows. Esto nos ayudará en las tareas de instalar drivers de impresoras en las máquinas VDA, ya que al instalar el agente VDA se instalará el driver universal de Citrix, y en el cual a través de una directiva podremos indicar que a la hora de crear la impresora si no existiese el driver nativo, use el universal.

Así como se muestra en la imagen el punto final ya no tendrá que interactuar con la impresora sino delegara ese trabajo a nuestro servidor de impresiones.

*Figura 34.*Representación del enrutamiento del servidor de impresión de Windows (con el servidor de impresión universal). Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.7.5 Aplicaciones

En este punto revisaremos la compatibilidad de las aplicaciones con la plataforma que pensamos desplegar y a su vez los requisitos del usuario y del negocio indicados en los capítulos 3.2.1 y 3.2.2 para la selección del método de entrega apropiado.

- **Compatibilidad**

Para lograr la compatibilidad de las aplicaciones en el siguiente diseño utilizaremos una combinación de pruebas manuales de usuario, para ello dispondremos de los siguientes requisitos de compatibilidad importantes a verificarse:

- **Sistema operativo:** La aplicación debe ser compatible con el sistema operativo del host en que se va a desplegar la solución.
- **Multiusuario:** En este punto validaremos la compatibilidad de la aplicación y sus capacidades para trabajar en modo multiusuario en un sistema operativo de servidor como Windows Server 2016.
- **Arquitectura de la aplicación:** Es importante saber si la aplicación contiene código de 16 bits, 32 bits o 64 bits para poder seleccionar un sistema operativo adecuado.
- **Interoperabilidad:** En este punto determinaremos los problemas de interoperabilidad de las aplicaciones para que puedan tomarse las medidas adecuadas de corrección o seleccionar un modelo de entrega alternativo.
- **Dependencia:** Puede que las aplicaciones necesiten interactuar entre sí para proporcionar a los usuarios una experiencia perfecta.

- **Método de entrega de aplicaciones**

El método de entrega de las aplicaciones a usar en este diseño será el de aplicación alojada en Windows, este nos permitirá que las aplicaciones se instalen en un host multi usuario de Citrix Apps y se implemente como una aplicación, no como un escritorio. Los usuarios accederán a la aplicación Windows alojada en servidores directamente desde el dispositivo de punto final, con lo que se oculta el hecho de que la aplicación se ejecuten de forma remota.

4.7.6 Máquinas virtuales

En esta parte indicaremos los recursos virtuales que se requieren para así obtener la asignación adecuada de procesador, la memoria y el disco. Esto tendrá un impacto directo en la cantidad de hardware necesario, así como en la experiencia del usuario.

Es por ello que debemos de garantizar que los escritorios virtuales y las aplicaciones brinden niveles de rendimiento similares a los escritorios físicos, pero sin llegar al punto de asignar recursos a las máquinas virtuales por encima de sus requisitos.

Los recursos asignados se basarán en la carga de trabajo de cada grupo de usuarios, determinada durante la fase de evaluación.

- Procesador virtual (CPU virtual)

Para el modelo de virtualización basados en aplicaciones alojados, la asignación adecuada de CPU virtuales se basa en la arquitectura de acceso no uniforme a la memoria (NUMA) de los procesadores.

Figura 35. Representación del esquema de interconexión NUMA. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Cuando la placa base del servidor tiene varios procesadores, todos acceden a la memoria través del mismo bus de memoria. Esto produce un cuello de botella en la arquitectura de los procesadores debido a las esperas para utilizar el bus de memoria.

Mediante el uso de NUMA cada procesador tiene acceso directo mediante un bus privado a unos bancos de memoria, mitigando las esperas en el bus general ya que se utiliza solamente

para acceder a espacios de memoria de otro procesador. La cantidad asignada las colocaremos según a carga de trabajo y si apuntamos a un objetivo de escalabilidad o el de mejor la experiencia al usuario. (Gonzalez, 2012)

Tabla 30
Asignación CPU virtual según carga de trabajo.

Carga de Trabajo	Sistema operativo	CPU virtual configurada para la escalabilidad	CPU virtual configurada para la experiencia
Ligera	Windows 2016	NUMA o ½ de NUMA	NUMA o ½ de NUMA
Media	Windows 2016	NUMA o ½ de NUMA	NUMA o ½ de NUMA
Alta	Windows 2016	NUMA o ½ de NUMA	NUMA o ½ de NUMA

Nota: Se presentan las cargas de trabajo existentes en el servidor VDA y la cantidad de NUMAs recomendado. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- Optimización de CPU

En el entorno compartido y virtualizado el cual diseñamos, un solo usuario puede monopolizar los recursos de la CPU debido a un proceso fuera de control o a una operación intensa de procesamiento de datos en Excel. Si se sobrepasa la capacidad del procesador, no podremos satisfacer las solicitudes de los demás usuarios, lo que dará lugar a una sesión bloqueada.

Es por ello que utilizaremos un componente de Citrix Virtual Apps, el Citrix Workspace Environment Management que anteriormente lo habíamos utilizado en la parte de experiencia de usuario para agilizar los tiempos de inicio de sesión, en este caso nos brindara optimización de la CPU. Esta funcionalidad ubica los procesos que utilizan un determinado porcentaje de la CPU durante un período de tiempo definido, la prioridad del proceso disminuye de normal a baja o muy baja, todos los procesos restantes reciben una mayor prioridad y se superará el riesgo de tener un proceso fuera de control. La optimización de la CPU también recordará los procesos que activaron la protección de la CPU e iniciará automáticamente el proceso con una prioridad menor en inicios futuros.

- Memoria virtual (RAM virtual)

La cantidad de memoria asignada a cada recurso se realizará en función de la carga de trabajo esperada del usuario y la aplicación. La asignación de memoria insuficiente a las máquinas virtuales provocará una paginación excesiva en el disco, lo que resultará en una mala experiencia de usuario; la asignación de demasiada memoria RAM aumentará el coste general de la solución.

La siguiente tabla contiene instrucciones sobre la RAM virtual que debe asignarse en función de la carga de trabajo.

Tabla 31

Asignación CPU virtual según carga de trabajo.

Carga de Trabajo	Sistema operativo	RAM virtual configurada para la escalabilidad	RAM virtual configurada para la experiencia
Ligera	Windows 2016	320 MB por usuario	320 MB por usuario
Media	Windows 2016	640 MB por usuario	640 MB por usuario
Alta	Windows 2016	1280 MB por usuario	1280 MB por usuario

Nota: Se presentan las cargas de trabajo existentes en el servidor VDA y la cantidad de vCPUs recomendado. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- Optimización de RAM

En la plataforma actual los usuarios trabajan en una sola aplicación a la vez, aunque la mayoría tiene cinco o más aplicaciones en ejecución, pero inactivas. Cuando un proceso pasa de activo a inactivo, la aplicación y el sistema operativo liberan una parte del espacio de trabajo activo de la memoria del proceso para liberar recursos del sistema. Sin embargo, se trata de solo un pequeño porcentaje del espacio de trabajo de la aplicación. El resto permanece bloqueado para la aplicación, lo que limita gravemente los recursos del sistema disponibles.

Es por ello que para la plataforma a diseñar se utilizará la optimización de RAM a través del Citrix Workspace Environment Management, con lo cual se obliga a las aplicaciones que están inactivas durante un tiempo determinado a liberar el exceso de memoria hasta que dejen de estar inactivas. Cuando la aplicación vuelve a un estado activo, la memoria liberada se

carga de nuevo en el espacio de trabajo activo. Asimismo, esta optimización está sujeta a una lista de exclusión para la optimización de RAM en caso ciertos procesos presenten problemas con la optimización.

- **Caché de disco**

La cantidad de almacenamiento que requiere cada VM variará según la carga de trabajo y el tipo de imagen. Los requisitos de espacio en disco para la caché de escritura y el disco de diferenciación dependerán del uso de la aplicación y del comportamiento del usuario. Aun así, la tabla siguiente contiene un punto de partida para estimar los requisitos de espacio en disco según el tamaño de la máquina con CPU y RAM virtuales según las siguientes pautas:

Tabla 32
Asignación Cache disco según carga de trabajo.

Carga de Trabajo	Sistema operativo	Espacio de almacenamiento
Ligera	Windows 2016	60 GB
Media	Windows 2016	60 GB
Alta	Windows 2016	60 GB

Nota: Se presentan las cargas de trabajo existentes en el servidor VDA y la cantidad de cache en disco recomendada. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- **Memoria caché de la RAM**

La memoria caché de la RAM se utiliza para mejorar el rendimiento del almacenamiento tradicional al compartir la memoria agrupada no paginada de la máquina virtual.

En la tabla siguiente se ofrece una orientación sobre la cantidad de cache de la RAM de que se generan por usuario en función de la carga de trabajo y del sistema operativo.

Tabla 33
Asignación caché en RAM según carga de trabajo.

Carga de Trabajo	Sistema operativo	Memoria caché RAM configurada para la escalabilidad	Memoria caché RAM configurada para la experiencia
Ligera	Windows 2016	4 GB	4 GB
Media	Windows 2016	8 GB	8 GB
Alta	Windows 2016	10 GB	10 GB

Nota: Se presentan las cargas de trabajo existentes en el servidor VDA y la cantidad de memoria RAM recomendada. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- IOPS de almacenamiento

El rendimiento del almacenamiento está limitado por la cantidad de operaciones que puede gestionar por segundo, denominada IOPS (operaciones de entrada y salida por segundo). Asignar pocas IOPS de almacenamiento resulta en un escritorio VDI donde las aplicaciones, las páginas web y los datos se cargan con lentitud.

En la tabla siguiente se ofrece una orientación sobre la cantidad de IOPS de almacenamiento que se generan por usuario en función de la carga de trabajo y del sistema operativo.

Tabla 34
Asignación IOPS disco según carga de trabajo.

Carga de Trabajo	Sistema operativo	IOPS de almacenamiento (sin caché basada en RAM)	IOPS de almacenamiento (con caché basada en RAM)
Ligera	Windows 2016	4 IOPS	1 IOPS
Media	Windows 2016	6 IOPS	1 IOPS
Alta	Windows 2016	8 IOPS	1 IOPS

Nota: Se presentan las cargas de trabajo existentes en el servidor VDA y la cantidad IOPS de almacenamiento recomendado. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.8 Metodología de diseño: Capa de control

En este punto se definirá la infraestructura subyacente necesaria para admitir el acceso de los usuarios a sus recursos, asimismo describiremos los detalles que rodean a los componentes utilizados para admitir el resto del entorno, y que le otorgará a la plataforma de la administración centralizada requerida en los puntos 3.2.1 y 3.2.2.

4.8.1 Active Directory

- Estructura de unidades organizativas

Lo recomendable es que los componentes de infraestructura de una implementación de Citrix Virtual Apps tengan su propia unidad organizativas (OU) dedicada, esto ayudara a para separar trabajadores y controladores con fines administrativos. Al tener sus propias unidades organizativas, los objetos que hay dentro tendrán una mayor flexibilidad con su administración, al tiempo que permitirán al área de TI obtener un control delegado.

A continuación, mostraremos un ejemplo de estructura de unidad organizativa de Citrix.

*Figura 36.*Representación del modelo de unidad organizativa recomendado por Citrix. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- Grupos de usuarios

Lo recomendable para administrar la plataforma Citrix Virtual Apps es la de asignar permisos y autorizaciones a grupos de usuarios en lugar de hacerlo a usuarios individuales, con ello evitamos estar cambiando permisos para recursos y derechos de usuario al crear, modificar o eliminar cuentas de usuario.

4.8.2 Base de datos

La mayoría de los recursos a utilizarse en la plataforma de Citrix Virtual Apps requieren de una base de datos, en estos se almacenarán toda la configuración del sitio Citrix Virtual Apps; así como los registros de este, sean históricos de conexiones de los usuarios o acciones realizadas por los administradores quedan almacenados en bases de datos. Las bases de datos se almacenarán en un servidor Microsoft SQL Server, en entornos muy pequeños un SQL Express sobre el Delivery Controller sería suficiente. Pero queda clara la importancia de la disponibilidad de las BBDD, por tanto, una solución de alta disponibilidad será importante, algo como SQL Database Mirroring puede ayudarnos y permitir que Delivery Controller siempre tenga conectividad. También es recomendable habilitar y configurar LHC o Local Host Caché en el broker para seguir dando servicio sin conectividad a la base de datos. De manera predeterminada, estas tres bases de datos se instalan en la misma ubicación que la BD del sitio; aunque esto se podría modificar. (Citrix Systems, High Availability for Citrix XenDesktop and XenApp, 2012)

4.8.2.1 Edición

Lo recomendable en función de las prestaciones de las diversas ediciones de SQL Server disponibles poder trabajarlo con la versión Standard para poder alojar las bases de datos de Citrix Virtual Apps en entornos de producción. La edición Standard ofrece una cantidad adecuada de funciones para satisfacer las necesidades de la mayoría de los entornos a utilizar.

4.8.2.2 Tamaño del servidor de la base de datos

Para garantizar el rendimiento y la estabilidad de nuestro entorno SQL Server se debe de tener el tamaño correcto. No se puede generalizar un tamaño que sirva para la plataforma en su totalidad, es por ello que se indicará lo recomendable para el tamaño de SQL Server por producto.

- **Citrix Virtual Apps**

Los brokers de Citrix Virtual Apps utilizan la base de datos como un bus de mensajes para las comunicaciones del broker, el almacenamiento de datos de configuración y el almacenamiento de datos de supervisión y de registros de configuración. Las bases de datos se utilizan constantemente, y el impacto en el rendimiento de SQL Server puede considerarse alto.

Lo recomendable según las pruebas de escalabilidad interna de Citrix, es cumplir con las siguientes especificaciones de SQL Server para un servidor que aloje todas las bases de datos de Citrix Virtual Apps:

2 núcleos/4 GB de RAM para entornos de hasta 5000 usuarios

4 núcleos/8 GB de RAM para entornos de hasta 15 000 usuarios

8 núcleos/16 GB de RAM para entornos con más de 15 000 usuarios

Asimismo, los archivos de bases de datos y los registros de transacciones deben estar alojados en subsistemas de almacenamiento separados para poder hacer frente a una gran cantidad de transacciones. Para el caso de estudio se tiene estimado trabajar con 55 usuarios, donde la primera especificación permitirá trabajar de manera fluida.

De manera predeterminada, Citrix Virtual Apps utiliza tres bases de datos distintas en la misma ubicación que la base de datos del sitio; estas normalmente cumplen las siguientes funciones:

- **Base de datos de configuración del sitio:** Contiene datos de runtime dinámico y de configuración estática.
 - **Base de datos de supervisión:** Contiene datos de supervisión como información de conexión y sesión los cuales pueden ser visualizados a través de Citrix Director.
 - **Base de datos de registros de configuración:** Contiene un registro para cada cambio administrativo realizado en el sitio, este es visualizable a través de Citrix Studio.
- (Citrix, 2019)

- **Provisioning Services**

Este producto nos permitirá almacenar los datos de configuración estática, los servidores de aprovisionamiento, información de runtime y auditorías en la base de datos. En función del patrón de arranque y de administración, el impacto en el rendimiento de la base de datos se puede considerar entre bajo y medio.

Lo recomendable en lo que respecta a especificaciones de su servidor de SQL Server es trabajarlo con 4 núcleos y 4 GB de RAM.

4.8.2.3 Tamaño de las instancias

Al dimensionar una base de datos SQL, se consideran dos aspectos importantes:

- Archivo de base de datos: contiene los datos y objetos, como tablas, índices, procedimientos y vistas almacenados en la base de datos.
- Archivo de registro de transacciones: contiene un registro de todas las transacciones y modificaciones de la base de datos realizadas por cada transacción.

- Base de datos del sitio

El tamaño de esta instancia de base de datos depende no solo del tamaño físico del entorno, sino también de los patrones de usuario, entre los que podemos mencionar:

- La cantidad de sesiones conectadas
- La cantidad de agentes VDA configurados y registrados
- La cantidad de transacciones que se producen durante el inicio de sesión
- Transacciones de latidos de VDA (Servicio que se encarga de la alta disponibilidad de una VDA)

El tamaño de la base de datos del sitio se basa en la cantidad de agentes VDA y de sesiones activas. En la tabla siguiente se muestra el tamaño recomendado según cantidad de usuarios y aplicaciones a publicar.

Tabla 35
Asignación espacio base de datos de sitio.

Usuarios	Aplicaciones	Tamaño máximo esperado (MB)
1000	50	30
10 000	100	60
100 000	200	330

Nota: Se presentan el tamaño máximo esperado según cantidad de usuarios y aplicaciones. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- Base de datos de supervisión

Esta base de datos al contener información de supervisión es la que mas espacio va a ocupar ya que contienen información histórica del sitio. El tamaño va a depender de los siguientes factores:

- La cantidad de usuarios
- La cantidad de sesiones y conexiones
- Configuración del período de retención
- Cantidad de transacciones por segundo

Tabla 36
Asignación espacio base de datos de supervisión.

Usuarios	Tipo	1 semana (MB)	1 mes (MB)	3 meses (MB)	1 año (MB)
1000	HSD	20	70	230	900
10 000	HSD	160	600	1950	7700
100 000	HSD	1500	5900	19 000	76 000

Nota: Se presentan el tamaño máximo esperado según cantidad de usuarios y aplicaciones. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Base de datos de registros de configuración

Esta base de datos suele ser la más pequeña y varía en función de la cantidad de actividades administrativas diarias que se inician desde scripts de Studio, Director o PowerShell, por lo que su tamaño es difícil de estimar. Cuantos más cambios realizamos en las herramientas mencionadas, más grande será la base de datos. (Citrix, 2020d)

Provisioning Services

Esta base de datos contiene datos de configuración estática y de registros de configuración de servicios ya preestablecidos, queda mencionarlos para conocer el tamaño a darle.

Tabla 37
Asignación espacio base de datos de Povisioning Services.

Elemento de configuración	Espacio en la base de datos necesario (KB)	Cantidad de elementos (ejemplo)	Total (KB)
Configuración de la comunidad de servidores base	112	-	112
Grupo de usuarios con acceso a la comunidad	50	10	250
Sitio	4	5	20
Colección de dispositivos	10	50	500
Vista de la comunidad	4	10	40
Relación entre la vista de la comunidad y el dispositivo	5	1	5000

Vista del sitio	4	5	20
Relación entre la vista del sitio y el dispositivo	5	1	5000
Dispositivo	2	5000	10 000
Programa de arranque del dispositivo	10	-	-
Relación entre el dispositivo y el disco	35	1	175 000
Relación de la impresora del dispositivo	1	-	-
Datos de personalidad del dispositivo	1	-	-
Estado del dispositivo (cuando se inicia)	1	5000	5000
Propiedad personalizada del dispositivo	2	-	-
Disco virtual	1	20	20
Versión del disco virtual	3	5	300
Localizador de discos	10	1	200
Propiedad personalizada del localizador de discos	2	-	-
Servidor	5	10	50
IP de servidor	2	1	20
Estado del servidor (cuando se inicia)	1	20	20
Propiedad personalizada del servidor	2	-	-
Almacén de discos virtuales	8	5	40
Relación entre el almacén de discos virtuales y el servidor	4	1	40
Conexión con XenServer (VirtualHostingPool)	4	-	-
Tarea de actualización de discos virtuales	10	10	100
Cambio administrativo (auditoría habilitada)	1	10 000	10 000
Total			211 732 KB (~212 MB)

Nota: Se presentan el tamaño máximo recomendado según el listado de elementos de configuración que posee dicha base de datos. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.8.5 Citrix Licensing Server

Este servicio administra las licencias del entorno Citrix, desde MyCitrix.com se descargarán los archivos con formato. LIC para luego ser importado. El Delivery Controller se comunica con él para administrar la licencia de cada usuario o dispositivo que se conecte, mediante un licenciamiento nominal (asociada al usuario) o concurrente (carga simultánea). Para el diseño en estudio se licenciarán tres productos, los dos primeros recursos mencionados utilizan el

servidor de licencias, mientras que el restante requerirá una licencia para instalarse en el propio producto. (Citrix, 2019a)

- Citrix Virtual Apps
- Provisioning Services
- Citrix Gateway

- Tamaño

Lo recomendable es trabajar con un único servidor virtual de licencias con dos núcleos y 2 GB de RAM puede emitir aproximadamente 170 licencias por segundo o 306 000 licencias cada media hora, con esas cantidades sería suficiente para nuestro escenario.

- Alta disponibilidad

Para escenarios como el nuestro basta con un único servidor de licencias. En caso de que el servidor de licencias no esté disponible, los servicios dependientes de este recurso entrarán en un período de gracia de 30 días, lo que ofrece tiempo más que suficiente para resolver problemas de conectividad o bien restaurar o reconstruir el servidor de licencias.

4.8.6 Delivery Controllers

- Tamaño del servidor

La escalabilidad de los Delivery Controllers se basa en el uso de la CPU. A mayor cantidad de núcleos de procesador haya disponibles, más usuarios podrán conectarse y ser admitidos por el controlador. Cada solicitud de inicio, registro, enumeración y lanzamiento de aplicaciones afecta al procesador del controlador. A medida que la avalancha de solicitudes se intensifica, la utilización de la CPU del controlador aumenta. La CPU de este recurso alcanza su umbral crítico aproximadamente al 80% del consumo, por lo que requerirá ampliarse vertical u horizontalmente.

La incorporación de núcleos de CPU adicionales a un Delivery Controller reducirá la utilización general de la CPU, lo que permitirá a un solo controlador admitir más sesiones. La otra opción es agregar otro controlador a la configuración del sitio. El controlador tendría la misma configuración que otros controladores, y la carga se distribuiría de manera uniforme entre todos los controladores, lo que ayudaría a reducir la carga global en cada controlador.

Las recomendaciones del fabricante indican que el Delivery Controller, mediante la siguiente configuración, puede admitir más de 5000 escritorios.

La siguiente fórmula se puede utilizar para calcular la cantidad de Delivery Controllers necesarios para nuestra plataforma.

$$\text{Number of Delivery Controllers} = \frac{\text{Number of Active Sessions per Site}}{5,000} + 1$$

*Figura 37.*Fórmula para determinar cantidad de Delivery Controllers Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- Alta disponibilidad

Si el servidor que aloja el Delivery Controller no está disponible, los usuarios no podrán acceder a sus escritorios virtuales o aplicaciones publicadas. Por lo tanto, se deben implementar al menos dos Delivery Controllers (redundancia N+1) por zona en diferentes servidores físicos para evitar que este componente se convierta en un punto de fallo único. De este modo, si falla un controlador, los demás pueden gestionar las conexiones y administrar el sitio.

Las ubicaciones de todos los Delivery Controllers se especifican en el VDA, lo que le permite recurrir a la conmutación por error automática si la comunicación con un Delivery Controller no está disponible. El VDA comprueba las siguientes ubicaciones por orden y se detiene en el primer lugar en el que encuentre el Delivery Controller:

El fabricante recomienda utilizar la función de actualización automática (habilitada de forma predeterminada). Esta función simplificará la administración del entorno porque mantiene actualizados los VDA al agregar y quitar Delivery Controllers.

- Cifrado de XML Service

En una sesión habitual, el servidor de StoreFront pasa credenciales a Citrix XML Service en un Delivery Controller. El protocolo XML de Citrix utiliza texto no cifrado para intercambiar todos los datos, a excepción de las contraseñas, que se transmiten mediante ofuscación.

Si se puede interceptar el tráfico entre los servidores de StoreFront y los Controllers de XenDesktop, este será vulnerable a los ataques siguientes:

- Los atacantes pueden interceptar el tráfico XML y robar información del conjunto de recursos que la plataforma posee.
- Los atacantes capaces de descifrar la ofuscación pueden obtener credenciales de los usuarios.
- Los atacantes pueden suplantar el Controller de Citrix Virtual Apps e interceptar solicitudes de autenticación.

Según lo mencionado se recomienda que el tráfico XML de Citrix se aisle en la red dedicada física o virtual del centro de datos, reduciendo la probabilidad de una interceptación. Otra forma sería utilizando cifrado SSL para enviar datos de StoreFront a través de una conexión HTTP segura.

- Administración de carga de SO de servidor

Las directivas de administración de carga predeterminadas se aplican a todos los grupos de entrega de SO de servidor. La configuración predeterminada establece en 250 el máximo de sesiones que un servidor puede alojar y no tiene en cuenta el uso de CPU ni de la memoria, esta política predeterminada es una limitante ya que no indica carga verdadera, lo que podría ocasionar una sobrecarga del servidor, así como uso ineficiente de los recursos.

Debido a ello el fabricante recomienda elaborar directivas de administración de carga personalizadas, que se puede aplicar a todos los servidores como referencia, un ejemplo de ellas podría ser las siguientes:

- **Uso de CPU:** Carga completa = 80%.
- **Prioridad de procesos excluidos para el uso de CPU:** Por debajo de lo normal o Bajo.
- **Uso de memoria:** Carga completa = 80%.

- **Carga base de uso de memoria:** Notificar carga cero (MB) = 786.
- **Número máximo de sesiones:** 250 (Valor Inicial).

Lo ideal es que los valores se personalicen en función de los resultados de las pruebas de escalabilidad que se hagan en laboratorio.

4.9 Metodología del diseño: Capa de hardware

En esta sección, se describirán los ajustes a nivel de hardware para los servidores de la infraestructura virtual y los hosts de aplicaciones virtuales. Para este caso práctico se utilizará hardware ya existente por lo que se hará la mejor configuración para cumplir los diferentes requisitos de carga de trabajo. Con esta información podremos atender requerimientos planteados en el punto 3.2.2 respecto a la eliminación de hardware fuera de nuestro de datos y el 3.2.5 sobre la alta disponibilidad.

4.9.1 Separación de la carga de trabajo

Para el diseño de Citrix Virtual Apps se creará un clúster de recursos dedicados separado de otros servicios que se puedan contar en la organización. Citrix recomienda utilizar clústeres de recursos para separar las cargas de trabajo y con ello ajustar mejor el tamaño del host, ya que cada carga de trabajo presenta requisitos únicos, como ratios de sobreasignación y uso de memoria.

- Procesador físico (pCPU)

En la tabla siguiente se ofrece una guía de la cantidad de sesiones de usuario que se pueden admitir para cargas de trabajo bajas, medianas y altas por núcleo físico.

Tabla 38
Usuarios por núcleo según carga de trabajo.

Carga de Trabajo	Sistema operativo	Usuarios por núcleo físico
Ligera	Windows 2016	21
Media	Windows 2016	14
Alta	Windows 2016	7

Nota: Se presentan las cargas de trabajo existentes y la cantidad de usuarios por núcleo recomendado. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

La estimación de usuarios por núcleo físico es un número de referencia de usuarios tomando como referencia la aplicación CONCAR SQL. El número de referencia debe ajustarse en función de las necesidades específicas de la infraestructura. Asimismo, en la siguiente tabla indicaremos factores que provocan un cambio en la referencia de la densidad del servidor.

Tabla 39
Directriz de densidad por servidor.

Característica	Impacto en la densidad del servidor
Antivirus (no optimizado)	Disminución del 25%
Supervisión en tiempo real	Disminución del 15%
Adobe PDF	Disminución del 20%
Office 2016	Disminución del 25%
Hyper-Threading	Aumento del 20%

Nota: Se presentan factores que afectan la densidad de usuarios en nuestro servidor de aplicaciones Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Para calcular la cantidad total de núcleos físicos necesarios para la carga de trabajo de Citrix Virtual Apps, utilizaremos la siguiente fórmula para cada grupo de usuarios:

$$\text{Total XenApp pCPU} = \sum Users_i / UsersPerCore_i * (1 + (AV + Mon + Off13 + Off16 - HV))$$

Figura 38.Fórmula de la carga de trabajo. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

$\sum$ representa la suma de todas las combinaciones de grupos de usuarios “i”.

$Users_i$ = Cantidad de usuarios simultáneos por grupos de usuarios

$UsersPerCore_i$ = Cantidad de usuarios por núcleo físico

AV = Impacto del antivirus (predeterminado = 0,25)

Mon = Impacto de las herramientas de supervisión (predeterminado = 0,15)

$Adob$ = Impacto de Adobe PDF (predeterminado = 0,2)

$Off16$ = Impacto de Office 2016 (predeterminado = 0,25)

HT = Impacto de Hyper-Threading (predeterminado = 0,2)

- Memoria física (pRAM)

El método recomendado para ajustar el tamaño de la memoria de un host físico es decidir el tamaño en función de la memoria total necesaria para admitir las máquinas virtuales y la capacidad de la CPU del host. Para calcular la memoria total necesaria para Citrix Virtual Apps bastará con multiplicar la cantidad de máquinas virtuales por la cantidad de memoria asignada a las máquinas virtuales. La suma de todos los catálogos de máquinas será la RAM total necesaria para los hosts de Citrix Virtual Apps se muestra en la siguiente fórmula.

$$Total\ XenApp\ pRAM = \sum_i VM_i * vRAM_i$$

*Figura 39.*Fórmula de la carga de trabajo. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

$\sum$ representa la suma de todas las combinaciones de grupos de usuarios “i”.

VM_i = Cantidad de usuarios simultáneos por grupos de usuarios

$vRAM_i$ = Cantidad de RAM asignada a cada máquina virtual

- Host físico (pHost)

La cantidad de hosts físicos que admitan las cargas de trabajo de Citrix Virtual Apps estará limitada por la cantidad de núcleos de procesador disponibles. En la siguiente fórmula se ofrece una estimación de la cantidad de hosts necesarios para las cargas de trabajo del usuario.

Citrix Apps pHosts = (Total de unidades CPU físicas de Citrix Apps / Núcleos por host físico +1)

Una vez que se ha determinado la cantidad de hosts físicos en función de los núcleos del procesador, se calcula la cantidad de RAM necesaria para cada host.

Citrix Apps pRAM per pHost = HypervisorRAM + (Total de RAM física de Citrix Apps / Hosts físicos de Citrix Apps -1)

4.9.2 Tamaño del almacenamiento

- Arquitectura del almacenamiento

Las principales arquitecturas de almacenamiento son las siguientes:

- Almacenamiento local
- Almacenamiento de conexión directa (DAS)
- Almacenamiento conectado a la red (NAS)
- Red de área de almacenamiento (SAN)
- Híbrido

Para el caso práctico y según el hardware existente en la organización la plataforma estará usando la SAN que actualmente existe en la topología de red de la organización.

Este tipo de red de almacenamiento permitirá a los equipos conectarse a diferentes dispositivos de almacenamiento, por lo que los servidores no tienen la propiedad del subsistema de almacenamiento, lo que permite compartir los datos en varios equipos. Normalmente, una red SAN tendrá su propia red dedicada de dispositivos de almacenamiento a los que generalmente no se puede acceder a través de la red por los medios comunes por lo que se necesita un adaptador especializado: el adaptador de bus de host o HBA.

Este tipo de arquitecturas nos permitirá ser altamente escalables, sin afectar en el rendimiento conforme se conectan más dispositivos y almacenamiento.

En la siguiente tabla se resumen las opciones de almacenamiento disponibles y se clasifican según lo idóneas que sean para las implementaciones de Citrix Virtual Apps. (Citrix, 2020e)

Tabla 40

Propiedades de las opciones de almacenamiento.

Propiedades de almacenamiento	Local	DAS	NAS	SAN
Coste de implementación	Bajo	Medio	Medio	Alto
Administración	Baja	Media	Media	Alta
Rendimiento	Alto	Medio/alto	Medio/alto	Alto
Redundancia	Baja/media	Media/alta	Media/alta	Alta
Escalabilidad	Baja	Media/alta	Media/alta	Alta

Caso de uso corriente	Entornos de producción pequeños y medianos	Entornos de producción pequeños y medianos	Entornos de producción pequeños y medianos	Entornos de producción medianos y grandes
Nota: Se presentan los tipos de almacenamiento disponibles y sus propiedades de almacenamiento. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.				

- Nivel de RAID

Para elegir el mejor nivel de RAID para la plataforma y sus distintos recursos, se tendrá que tener en cuenta la relación entre IOPS y la lectura/escritura generada por una aplicación o una carga de trabajo determinadas, junto con las prestaciones individuales de un nivel de RAID. Para cargas de trabajo de alojamiento que consumen muchos recursos de lectura, los niveles de RAID optimizados para operaciones de lectura como RAID 1, 5, 6 o 10 son ideales ya que permiten que las operaciones de lectura se distribuyen por todos los discos del conjunto RAID simultáneamente.

Para cargas de trabajo de alojamiento que consumen muchos recursos de escritura, niveles de RAID como RAID 1 o 10 son ideales, ya que están optimizados para la escritura y cuentan con una penalización baja de escritura.

En la siguiente tabla se describen los atributos cuantitativos esenciales de los niveles de RAID más utilizados:

Tabla 41
Atributos por tipo de RAID.

RAID	Capacidad (%)	Tolerancia de fallos	Rendimiento de lectura	Rendimiento de escritura	Cantidad mínima de discos
0	100	Ninguna	Muy alto	Alto (penalización de escritura 1)	2
1	50	Fallo de una sola unidad	Muy alto	Medio (penalización de escritura 2)	2
5	67 - 94	Fallo de una sola unidad	Alto	Bajo (penalización de escritura 4)	3

6	50 - 88	Fallo de unidad dual	Alto	Bajo (penalización de escritura 6)	4
10	50	Fallo de una sola unidad en cada submatriz de discos	Muy alto	Medio (penalización de escritura 2)	4

Nota: Se presentan los tipos de arreglo RAID y los atributos y funciones que pueden otorgar al diseño. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

- Cantidad de discos

Para determinar la cantidad necesaria de discos, es importante comprender las características de rendimiento de cada disco, las características del nivel de RAID y los requisitos de rendimiento de la carga de trabajo existente. Para ello dispondremos de la siguiente fórmula para el cálculo básico para determinar la cantidad total de discos necesarios:

Cantidad total de discos = Cantidad total de IOPS de lectura + (Total de IOPS de escritura x Penalización de RAID) / IOPS de velocidad de disco

- Ancho de banda del almacenamiento

El ancho de banda del almacenamiento es la conectividad entre los servidores y el subsistema de almacenamiento. Comprender los requisitos de ancho de banda puede ayudar a determinar el hardware idóneo para entregar datos y aplicaciones a una velocidad que permita ofrecer una experiencia positiva al usuario final.

Para planificar el ancho de banda requerido, es necesario determinar el procesamiento de cada sistema individualmente presente dentro de la plataforma y que utilice algún componente de red.

Para nuestro caso práctico haremos el ejemplo con un entorno con 5 máquinas virtuales similares (alojadas en 2 hosts de virtualización y conectadas a una puerta de enlace NAS).

Tabla 42
Ejercicio de cálculo de procesamiento de red.

	Promedio	Pico
Procesamiento por VM	0.5 Mbps	1.5 Mbps

Procesamiento por host	2.5 Mbps (5 VM x 0.5 Mbps)	7.5 Mbps (5 VM x 1.5 Mbps)
Procesamiento por almacenamiento	5 Mbps (2 hosts x 2.5 Mbps)	15 Mbps (2 hosts x 7.5 Mbps)

Nota: Se presentan los promedios de uso de ancho de banda tomando en cuenta 5 máquinas virtuales y dos hosts de virtualización. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Con una tarjeta NIC en las comunicaciones de almacenamiento de 100 Mbps para podrá admitir la carga máxima de todos los sistemas dentro de la plataforma.

4.10 Metodología de recuperación VMware a Azure

En esta parte indicaremos la arquitectura a utilizar y los procesos a requerir para que el diseño pueda replicarse, conmutar por error y recuperar las máquinas virtuales de VMware entre nuestro sitio de VMware local y Azure, mediante el servicio Azure Site Recovery.

4.10.1 Componentes de la arquitectura

Para la recuperación ante desastres de VMware en Azure se requerirán de los siguientes componentes.

Tabla 43

Componentes de Arquitectura Azure Site Recovery

Componente	Requisito	Detalles
Azure	Una suscripción a Azure, una cuenta de Azure Storage para almacenamiento en caché, un disco administrado y una red de Azure.	Los datos replicados desde las máquinas virtuales locales se almacenan en Azure Storage. Las máquinas virtuales de Azure se crean con los datos replicados cuando se ejecuta una conmutación por error desde el entorno local en Azure. Las máquinas virtuales de Azure se conectan a la red virtual de Azure cuando se crean.
Servidor de configuración	Se tendrá que crear una máquina virtual de VMware	Servidor de configuración: coordina las comunicaciones entre el entorno local y Azure, además de administrar la replicación de datos.

	para ejecutar los componentes locales de Site Recovery, incluido el servidor de configuración, el servidor de procesos y el servidor de destino maestro, cabe indicar que de forma predeterminada se instalan todos los servicios juntos.	Servidor de proceso: Este se encarga de recibir los datos de la replicación; los optimiza mediante almacenamiento en caché, compresión y cifrado, y los envía a Azure Storage. Además, instala el Azure Site Recovery Mobility Service en las máquinas virtuales que se van a replicar y realiza la detección automática de las máquinas locales
		Servidor de destino principal: Este se encarga de controlar los datos de replicación durante la conmutación por recuperación desde Azure.
Servidores de VMware	Se recomienda un servidor vCenter para administrar las máquinas virtuales VMware que se hospedan en los servidores ESXi de vSphere local.	Durante la implementación de Site Recovery, se agregan servidores VMware al almacén de <i>Recovery Services</i> .
Máquinas replicadas	Mobility Service está instalado en cada una de las máquinas virtuales de VMware que se van a replicar.	Se requiere tener instalado, ya sea automatizado via <i>Configuration Manager</i> del servidor de procesos o manualmente.

Nota: Se presentan los componentes, requisitos y funciones del esquema de arquitectura de Azure Site Recovery. Adaptado de “Arquitectura de recuperación ante desastres de VMware a Azure”, por Microsoft Azure, 2019.

A continuación, mostraremos el digrama con el resumen de componentes mencionados en la tabla 41.

Figura 40. Representación que muestra los componentes principales de la Arquitectura de recuperación ante desastres de VMware a Azure. Adaptado de “Arquitectura de recuperación ante desastres de VMware a Azure”, por Microsoft Azure, 2019.

4.10.2 Proceso de replicación

Para habilitar la replicación de una VM en el almacenamiento de Azure según la directiva de replicación que se haya especificado se debe tener en cuenta lo siguiente:

- Para nuestro caso en el que contamos con VM de VMware, la replicación es a nivel de bloque, mediante el agente *Mobility Service* que se ejecuta en la VM.

- Las directivas de replicación disponibles son las siguientes:

- **Umbral de RPO.** Este valor especifica con qué frecuencia se crean los puntos de recuperación de datos. Se genera una alerta si la replicación continua excede este límite.
- **Retención de punto de recuperación.** Aca se especifica el tiempo que *Site Recovery* conserva los puntos de recuperación, por defecto son 24 horas.
- **Instantáneas coherentes con la aplicación.** Indica la frecuencia con la que *Site Recovery* toma una instantánea coherente con la aplicación., el valo predeterminado es de cada cuatro horas.

- El tráfico por donde se va a replicar la información entre los servidores locales y el *Site Recovery* será a través de los puntos de conexión públicos de *Azure Storage* a través de Internet o través del *Azure ExpressRoute*, que es una conexión privada entre nuestro entorno local y el centro de datos de Azure.

- Una vez terminada la replicación inicial, el servidor de procesos se encarga de enviar los cambios del tipo incremental a Azure.
- La comunicación se realiza según como se muestra en la figura 38 y consta de los siguientes pasos:
 - Las máquinas virtuales se comunican con el servidor de configuración local en el puerto HTTPS 443 entrante para la administración de la replicación.
 - El servidor de configuración organiza la replicación con Azure a través del puerto HTTPS 443 saliente.
 - Las máquinas virtuales envían datos de replicación al servidor de procesos en el puerto HTTPS 9443 entrante.
 - El servidor de procesos recibe datos de replicación, los optimiza y los cifra para enviarlos después a Azure Storage a través del puerto 443 de salida. (Azure, 2019)
- Una vez concluida la transferencia de la información, estos aterrizan en la cache de Azure para luego ser procesados y almacenados en un disco administrado por Azure (denominado disco ASR), en este sitio es donde se crean los puntos de recuperación y donde se almacenan las instantáneas.

Figura 41. Representación que muestra el proceso de replicación entre las VM de VMware al portal de Azure. Adaptado de “Arquitectura de recuperación ante desastres de VMware a Azure”, por Microsoft Azure, 2019.

4.10.3 Proceso de conmutación por error y conmutación por recuperación

Estando a replicación configurada y trabajando la replicación incremental, se realiza una conmutación por error de prueba para verificar que funcione correctamente. La conmutación por error y la conmutación por recuperación, según sea necesario.

- Una vez iniciada la conmutación por error inicial, se confirma su inicio accediendo a la carga de trabajo desde la máquina virtual de Azure.

- Cuando nuestro sitio local principal esté disponible de nuevo, se podrá preparar el escenario para la conmutación por recuperación. Para ello se deberá tener lista la infraestructura de conmutación por recuperación, la cual consta de:

- Servidor de procesos temporal de Azure: Esta asumirá su rol como servidor de procesos y se encargará de controlar la replicación desde Azure.
- Conexión VPN: Se necesitará de una conexión VPN o *ExpressRoute* (utilizada para la replicación) desde la red de Azure a la infraestructura local.
- Servidor de destino maestro independiente: El servidor con el rol de destino principal se encargará de controlar la conmutación por recuperación.
- Directiva de conmutación por recuperación: Esta directiva se crea automáticamente cuando creamos la directiva de replicación entre el entorno local y Azure.

- Teniendo los cuatro componentes mencionados la conmutación por recuperación constará de tres fases:

Fase 1 Inicia la replicación desde Azure de vuelta a las máquinas virtuales locales.

Fase 2: Ejecuta la tarea de conmutación por error en el sitio local.

Fase 3: Terminada la tarea de conmutación, se debe habilitar de nuevo la replicación de las máquinas virtuales locales con Azure. (Azure, 2019)

Figura 42. Representación que muestra el proceso de Conmutación por recuperación VMware desde Azure. Adaptado de “Arquitectura de recuperación ante desastres de VMware a Azure”, por Microsoft Azure, 2019.

4.11 Dimensionamiento para el diseño de plataforma

Las cinco capas revisadas anteriormente nos dan como resultado la siguiente arquitectura:

Figura 43. Representación que muestra los componentes principales de una implementación típica de Citrix Virtual Apps. Adaptado de “CITRIX VIRTUAL APPS AND DESKTOPS Información técnica general”, por Citrix, 2020.

Ahora que se ha detallado los principales componentes detallaremos la funcionalidad de cada elemento en la siguiente tabla:

Tabla 44
Roles de XenApp

Rol	Descripción	Función
DC	Delivery Controller	Componente de administración central de un sitio
DB	Base de datos	Componente para almacenar la información de configuración y sesiones.
VDA	Virtual Delivery Agent (VDA)	Componentes que entregan aplicaciones o escritorios.
CSF	Citrix StoreFront	Aloja la tienda de las aplicaciones de su empresa
CS	Citrix Studio	Consola de administración desde la que configurar y administrar la implementación de Citrix Virtual Apps
CD	Citrix Director	Herramienta Web que permite a los equipos de asistencia técnica y TI supervisar un entorno
CLS	Citrix License Server	Administra las licencias de los productos Citrix

Para poder explicar a detalle los requerimientos necesarios para el diseño los dividiremos en capas tal y como se hizo con su diseño:

4.11.1 Requerimientos Capa Cliente

A nivel de dispositivo de usuario, la plataforma se basa en el uso de un cliente Citrix Workspace para el acceso a los recursos en los servidores. La recomendación es tener instalada la última versión de dicho cliente en el dispositivo a conectar.

Los requisitos a nivel de sistema operativo de cliente y servidor son los siguientes:

- PC clientes: Windows 7, 8, 8.1. 10
- Servidores: Windows Server 2012, 2012R2 y 2016

Para nuestro caso no tendría problemas de compatibilidad con los equipos ya que los sistemas operativos existentes se encuentran dentro de la lista mencionada.

En nuestro diseño vamos a agrupar dispositivos según ubicación y funcionalidad, este quedaría de la siguiente manera:

- Equipos Corporativos dentro de la red local

La configuración será realizada a través de una directiva de grupo a todos los equipos que estén unidos al dominio.

- Equipos Corporativos y no corporativos fuera de la red local

La configuración y los accesos serán desplegados de forma manual, los clientes Workspace descargados desde la dirección de acceso a la plataforma de aplicaciones.

- Dispositivos móviles

El cliente Workspace permite acceder desde los principales sistemas operativos incluidos en estos dispositivos (Android, IOS).

4.11.2 Requerimientos Capa Acceso

En este punto atenderemos requerimientos que se necesitan para el Citrix Gateway y el StoreFront, que servirán para la autenticación de los usuarios locales como externos, los cuales serán detallados a continuación:

Citrix Gateway

En este servicio se configurará el acceso externo consolidado, así como el monitoreo y visibilidad de las aplicaciones, por otra parte, también se realizará el balanceo de los StoreFront. Este par de Citrix Gateway permitirá habilitar la alta disponibilidad trabajando uno en modo activo y otro pasivo. En caso de caída de uno de ellos, el secundario actuaría como primario y asumiría todos los servicios desplegados.

Esta primera capa del entorno de acceso tiene como cometido:

- Gestionar las sesiones SSL-HDX contra la granja de servidores Citrix. De forma que todas las conexiones hacia el exterior sean sólo conexiones SSL.
- Proporcionar balanceos de conexiones en el acceso al entorno frontal web.
- Proporcionar funcionalidades de cambio de contraseñas para los usuarios que accedan al portal.
- Balancear el acceso a servicios corporativos como DNS y LDAP para la resolución y autenticación.

Tabla 45

Especificaciones Citrix Gateway VPX Requeridos

SERVIDOR	ROL	SISTEMA OPERATIVO	CPU	MEMORIA (GB)	DISCO (GB)
CG01	Citrix Gateway VPX 200	CentOS	2	2	20
CG02	Citrix Gateway VPX 200	CentOS	2	2	20

Nota: Se presenta el resultado total del cálculo de procesador y memoria ram necesario para el Citrix Gateway VPX. Adaptado de “NetScaler VPX: Virtualizing the power of advanced web and application delivery and remote access services”, por Citrix, 2015.

StoreFront

La segunda capa del entorno de acceso tiene como cometido:

- Soportar el entorno de acceso Web
- Proporcionar escritorios y aplicaciones a los equipos clientes y a los dispositivos móviles haciendo uso del servicio services sites de PNAgent
- Proporcionar un portal de acceso personalizado y dedicado para Clínica Abril

Para ello configuraremos dos servidores virtuales sobre los que instalaremos Citrix StoreFront 3.0.4, las cuales van a estar a cargo de soportar las conexiones internas, por lo que estarán configurados en la red LAN de producción, estas a través del Citrix Gateway serán balanceadas, para dotarlos de alta disponibilidad y equilibrio de carga.

Las características de estos equipos serán:

Tabla 46

Citrix Storefront Requeridos

SERVIDOR	ROL	SISTEMA OPERATIVO	CPU	MEMORIA (GB)	DISCO (GB)
CSF01	Citrix StoreFront Interno	Windows Server 2016	2	8	40
CSF02	Citrix StoreFront Interno	Windows Server 2016	2	8	40

Nota: Se presenta el resultado total del cálculo de procesador y memoria ram necesario para los dos servidores Citrix Storefront. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.11.3 Requerimientos Capa Control

En esta capa se encuentran todos aquellos recursos que manejan y enlazan los diferentes componentes que permitirá ganar tanto la administración centralizada como la alta disponibilidad en cada parte que el diseño posea.

Delivery Controller

En el diseño que planteamos constará de dos servidores que cumplirán la función de Delivery Controller en alta disponibilidad. Adicionalmente se instalarán la consola de administración (Citrix Studio), la consola de monitorización/soporte (Citrix Director).

Por lo tanto, el dimensionamiento quedaría de la siguiente manera:

Tabla 47

Citrix Delivery Controller Requeridos

SERVIDOR	ROL	SISTEMA OPERATIVO	CPU	MEMORIA (GB)	DISCO (GB)
DC01	Delivery Controller 7.15	Windows Server 2016	2	8	40
DC02	Delivery Controller 7.15	Windows Server 2016	2	8	40

Nota: Se presenta el resultado total del cálculo de procesador y memoria ram necesario para los dos servidores Delivery Controller. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

Servidor licencias Citrix

Para el servicio de licenciamiento de la plataforma Citrix, las buenas prácticas no considera necesario la creación de un sistema que dote de alta disponibilidad, ya que este entorno tiene

la posibilidad de funcionar entregar un plazo adicional de 30 días, por lo tanto, en caso de caída el servicio no se vería interrumpido.

El servidor de licencias Citrix va a requerir de las siguientes características:

Tabla 48

Citrix License Server Requerido

SERVIDOR	ROL	SISTEMA OPERATIVO	CPU	MEMORIA (GB)	DISCO (GB)
CLS01	License Server	Windows Server 2016	2	4	40

Nota: Se presenta el resultado total del cálculo de procesador y memoria ram necesario para el Servidor de Licencias. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.11.4 Requerimientos Capa Recursos

En esta capa definiremos el sistema operativo sobre el cual se desplegarán las aplicaciones, así como los cálculos de los recursos asignados a este según la cantidad de usuarios y los recursos necesarios para el correcto desempeño de las aplicaciones.

Para este caso las aplicaciones serán desplegadas sobre un servidor Windows server 2016 en el cual se encontrarán las aplicaciones instaladas, este será destinado tanto para el acceso local y externo.

Estos grupos de recursos se crean y se agrupan en cuatro catálogos, atendiendo al tipo de recurso y se asignan a los usuarios de acuerdo con los grupos de entrega.

Para dimensionar los servidores de aplicaciones Citrix Virtual Apps, hemos tomado los siguientes parámetros como sesión de usuario de referencia:

- La sesión del usuario sobre el servidor (sin aplicaciones) consume alrededor de unos 70MB de RAM.
- El uso del antivirus sobre el servidor consume alrededor de unos 250 MB de RAM, así como las aplicaciones de Office 150 MB de RAM y Adobe PDF 2 MB respectivamente.
- Flujo NET®, CONCAR® SQL, SISPAG® genera un consumo de unos 150MB RAM.
- RS CRM® y PLACAR® CB genera un consumo de 80-100MB RAM.
- IVMS Aplicación corporativa un consumo de 250MB RAM

Los consumos de CPU de estas aplicaciones suelen ser bajos salvo la visualización de vídeos y multimedia que puede generar el IVMS. Por lo que el cálculo de CPU en este caso es despreciable.

Tabla 49

Consumo de aplicaciones

Aplicación	Consumo Estimado
Sesión	70 MB
Antivirus	250 MB
Office	150 MB
Flujo NET®	150 MB
CONCAR® SQL	150 MB
RS CRM®	100 MB
PLACAR® CB	100 MB
SISPAG®	150 MB
IVMS	250 MB
Adobe PDF	2 MB
Total	1.5 GB

Nota: Se presenta el listado de aplicaciones que se va a encontrar en los servidores de aplicaciones y el consumo estimado de memoria ram, elaboración propia.

En base a esta cifra y al número final de usuarios, salen las siguientes estimaciones:

En principio la cifra de usuarios que se contempla que van a hacer uso de aplicaciones publicadas por Citrix Apps es de 90. Para un máximo de 90 usuarios con una concurrencia del 100% generarían unos consumos de RAM aproximados de:

$$90 \text{ usuarios} \times 1.5 \text{ GB} = 135 \text{ GB}$$

$$135 \text{ GB} / 1,024 = 131,83 \text{ GB}$$

Se debe estimar al menos 2 GB de RAM por VM como reserva para la gestión del sistema operativo. Por otro lado, aunque la virtualización del entorno maximiza el uso de los servidores físicos, la capa de gestión del hypervisor siempre penaliza en parte el rendimiento de las VM, por lo que el número de usuario final por VM se ve levemente penalizado.

Partiendo de que vamos a contar con máquinas virtuales Citrix Apps con unos 64 GB RAM: 64 GB (Por Máquina Virtual) - 2GB (S.O.) / 1.5 GB por sesión = 41.33 sesiones por VM server

Teniendo en cuenta que se tiene que soportar un máximo de 90 sesiones simultáneas, harían falta 3 servidores virtuales de aplicaciones Citrix Apps lo cual nos brindaría asimismo una escalabilidad de un 30 % en la cantidad de usuarios que puedan conectarse.

Tabla 50
Dimensionamiento catálogo Citrix Apps

SERVIDOR	ROL	SISTEMA OPERATIVO	UNIDADES	CPU	MEMORIA (GB)	DISCO (GB)	USO DISCO
XAPP_0#	XenAPP	Windows Server 2016	3	8	64	C:\ 50 D:\ 10 E:\ 20	S.O. DATOS PAGEFILE

Nota: Se presenta el resultado total del cálculo de procesador, memoria ram y espacio en disco necesario para el Servidores de aplicaciones. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.11.5 Requerimientos Capa Hardware

Realizando un recuento global de los recursos necesarios para desplegar la plataforma Citrix proyectada, es estima lo siguiente:

Tabla 51
Recuento global recursos

ENTORNO	vCPU	vRAM (GB)	ALMACENAMIENTO (GB)
Citrix Apps	24	192	240
Servidores infraestructura Citrix	10	36	200
Citrix Gateway	4	4	40
Perfiles Citrix UPM			10
BBDD Citrix			20
Totales	37	232	510

Nota: Se presenta el recuento de recursos necesarios para los diversos servicios de la infraestructura Citrix Virtual Apps, elaboración propia.

4.11.6 Requerimiento Servicios Corporativos para la plataforma de acceso a las aplicaciones

Denominamos servicios corporativos a todos aquellos recursos que se van a utilizar sobre servicios ya existentes en la plataforma actual, de las cuales la plataforma de Citrix se apoyará para realizar diversas operaciones.

4.11.6.1 Base de Datos

Dimensionamiento

Un sitio Citrix Apps utiliza tres bases de datos de SQL Server:

- Sitio: (también conocido como Configuración del sitio) Almacena la configuración del sitio en ejecución, más el estado actual de la sesión y la información de conexión.
- Registro de configuración: (también conocido como Registro) Almacena información sobre los cambios de configuración del sitio y las actividades administrativas. Esta base de datos se usa cuando la función Configuración de registro está habilitada.
- Monitoreo: Almacena datos utilizados por el Director, como información de sesión y conexión.

Para el cálculo se utilizará la herramienta Database Sizing Tool:

Sitio:

XenDesktop 7 Database Sizing Tool

Data from this tool should be used for guidance only, as index maintenance and fragmentation will impact database size.

Users	Sessions Per User	Connections Per Session	HSD Workers	VDI Workers	Machine Catalogs	Delivery Groups	Applications	Applications Per User	Applications Per Session	Failure Rate (%)	Hotfixes
90	1	1	90	1	3	1	10	10	5	1	3

Site Database (7.6)

Database Sizing

Calculation	Day 0 (MB)	Day 1 (MB)	Week (MB)	Month (MB)	Quarter (MB)	Year (MB)
1	22	22	22	22	22	22

Figura 44.Dimensionamiento Sitio Database. Adaptado de “XenDesktop 7 Database Sizing Tool”, elaboración propia.

Monitoreo:

Figura 45. Dimensionamiento Monitor Database. Adaptado de “XenDesktop 7 Database Sizing Tool”, elaboración propia.

Por lo cual resumiremos las 3 bases de datos según la siguiente tabla.

Tabla 52

Dimensionamiento BBDD Citrix

SERVICIO	UBICACIÓN	TAMAÑO (GB)
Sitio	DB01	1
Registro de configuración	DB01	1
Monitoreo	DB01	15

Nota: Se presenta el recuento de recursos necesarios para la base de datos de la infraestructura Citrix Virtual Apps, elaboración propia.

4.11.6.2 Active Directory

La plataforma utilizará dos recursos del directorio activo para poder utilizar servicios adicionales para asignar políticas, derechos y propiedades de un conjunto de objetos en una forma sencilla y estructurada.

Para el caso práctico listaremos los recursos a utilizar para este diseño:

- Estructura de OU: Para la plataforma requerirá de una estructura de unidades organizativas dentro del árbol de directorio del dominio de producción de la Cooperativa Los Andes. La estructura recomendada se basa en una OU principal que contendrá varias sub-unidades organizativas para cada uno de los roles de servicio. De esta manera se podrá aplicar

diferentes niveles de las políticas de seguridad y configuraciones para cada elemento de la plataforma.

En la siguiente tabla indicaremos las ubicaciones de los diversos componentes de la plataforma en cada una de sus unidades organizativas (OU):

Tabla 53

Dimensionamiento estructura AD Citrix

Nombre de OU	Ubicación de OU	Descripción
Citrix	Root\	OU principal
Cuentas de Gestión	Citrix\	Cuentas de los administradores de la plataforma y de las cuentas de servicio
Grupos	Citrix\	OU para separar los diferentes tipos de grupos de seguridad
Administración	Citrix\Grupos	Grupos de administración de la plataforma
Seguridad	Citrix\Grupos	Grupos de seguridad para dar acceso a los diferentes recursos
Infraestructura	Citrix\	OU para agrupar los componentes de infraestructura
SrvInf	Citrix\Infraestructura	Servidores de Infraestructura
ServXenApp	Citrix\Infraestructura	Servidores de XenApp

Nota: Se presenta las unidades organizativas a crear y su respectiva ubicación dentro del directorio activo. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

• **Políticas de grupo (GPO):** Las políticas de grupo deben ser aplicadas sobre las OU’s donde se alojan los servidores de aplicaciones Citrix Apps (ServXenApp). Citrix recomienda disponer de las siguientes configuraciones (Citrix, 2014):

- **Loopback Mode:** Permitirá remplazar las políticas de usuario por las establecidas para la máquina.
- **Inheritance Blocking:** Permitirá bloquear las herencias para proporcionar un mayor control sobre lo que pasa en el entorno.

Para el dimensionamiento del repositorio donde se almacenarán los perfiles hemos realizado el siguiente cálculo:

Tabla 54

Dimensionamiento Perfiles Citrix

USUARIOS	ESPACIO POR USUARIO (MB)	NUMERO DE USUARIOS	DISCO (GB)
----------	--------------------------	--------------------	------------

Perfiles Citrix	100	90	8.78
-----------------	-----	----	------

Nota: Se presenta el resultado total del cálculo de espacio en disco necesario para los perfiles de usuario en el directorio activo. Adaptado de “Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR”, por Citrix, 2020.

4.11.6.3 Licencias Terminal Server

Para el diseño se debe de disponer de un servidor de licencias Microsoft Remote Desktop Services, de modo que se agregarán la cantidad de licencias que se tiene contemplado en el diseño que para este caso son 91 usuarios.

4.11.6.4 Antivirus

Se debe de realizar la configuración en cada uno de los servidores Citrix, desde los cuales van a acceder los usuarios tanto local como externamente.

4.11.7 Requerimientos de Infraestructura de Red

La disposición de las redes que tienen configuradas es la siguiente:

- Red de DMZ: En esta red están conectados los dos Citrix Gateway con lo que se propone el diseño este en la subred 10.10.10.x/28.
- Red de Producción: Red en la que están conectados tanto los servidores de la infraestructura como los equipos de los usuarios: 172.16.10.x/24
- Firewall: El esquema actual cuenta con un Fortigate 200E el cual va a ser utilizado como equipo de seguridad el cual estará encargado de resolver las consultas DNS referidos a la dirección web del portal de aplicaciones, así como realizar el nateo de la dirección pública asignada a la privada del servidor de producción.

La siguiente figura representa el diagrama de red propuesto:

Figura 46. Representación gráfica de la infraestructura de red propuesta en la sede Central en Lima, elaboración propia.

4.11.8 Requerimientos de Infraestructura de Licenciamiento

De acuerdo a la cantidad de servidores, procesadores asignados para el diseño de la plataforma y la cantidad de usuarios, es que se presentan las siguientes tablas de licenciamiento de Microsoft y Citrix necesarias para la solución.

Tabla 55

Requerimientos de licenciamiento

Ítem	Cantidad	Versión	Fabricante
1	33	Windows Server 2016 Standard por Core	Microsoft
2	90	CAL de Remote Desktop Services por dispositivo	Microsoft
3	90	CAL de Windows Server 2016 por dispositivo	Microsoft
4	90	Citrix Virtual Apps and Desktops Advanced Edition - x1 User/Device	Citrix
5	2	Citrix ADC VPX 200 Standard Edition	Citrix

Nota: Se presenta el requerimiento de licenciamiento Citrix y Microsoft necesario para la solución para tres servidores VPX y noventa usuarios, elaboración propia.

4.11.9 Requerimientos de Infraestructura de Backup

A continuación, describiremos los requerimientos a nivel de arquitectura y procesos usados al implementar la replicación, la conmutación por error y la recuperación de máquinas virtuales (VM) de VMware entre un sitio de VMware local y Azure para la recuperación ante desastres, mediante el servicio Azure Site Recovery.

El servicio de por si requiere de los siguientes componentes:

- Dispositivo de replicación: Es un equipo local que sirve de puente entre el entorno local y la herramienta Azure Migrate Server Migration.
- Servicio de Movilidad: Es un agente que se instala en cada máquina que quiera replicar y migrar.

*Figura 47.*Componentes arquitectónicos del Azure Migrate Server Migration. Adaptado de “Arquitectura de migración basada en agente”, Microsoft Azure,2019.

Según los datos publicados en la página del fabricante y la cantidad de VM que vamos a desplegar en el diseño presentamos la siguiente imagen con los datos a elegir para el dimensionamiento del ASR.

CPU	Memoria	Espacio libre para el almacenamiento de datos en caché	Tasa de renovación	Límites de replicación
8 vCPU (2 sockets * 4 núcleos @ 2,5 GHz)	16 GB	< 300 GB	500 GB o menos	< 100 máquinas
12 vCPU (2 sockets * 6 núcleos @ 2,5 GHz)	18 GB	600 GB	De 501 GB a 1 TB	100-150 máquinas.
16 vCPU (2 sockets * 8 núcleos @ 2,5 GHz)	32 GB	1 TB	1 TB a 2 TB	151-200 máquinas.

Figura 48.Requerimientos para el dimensionamiento de contingencia de plataforma virtual de aplicaciones. Adaptado de “Arquitectura de migración basada en agente”, Microsoft Azure,2019.

Los valores mostrados en la imagen se pueden usar para averiguar si necesita un servidor de procesos adicional en la implementación.

En nuestro caso, la tasa de cambio diaria (tasa de renovación) es inferior a 2 TB, y la cantidad de máquinas menor a 100, por lo que la primera configuración de especificaciones se ajustaría a nuestro diseño.

Tabla 56
Dimensionamiento ASR.

SERVIDOR	ROL	SISTEMA OPERATIVO	UNIDADES	CPU	MEMORIA (GB)	DISCO (GB)	USO DISCO
						C:\ 50	S.O.
ASR01	CONFIGURACION/PROCESS SERVER	Windows Server 2016	1	8	16	D:\600	SERVER CACHE
						E:\600	RETENCION DISK

Nota: Se presenta el recuento de recursos necesarios el servicio de contingencia Azure Site Recovery, elaboración propia.

4.11.10 Representación gráfica

El esquema final con del diseño que se ha planteado, tanto para el acceso externo como interno será según la figura 44.

Figura 49. Representación gráfica de la infraestructura completa de virtualización de aplicaciones propuesta en la sede Central en Lima, elaboración propia.

4.12 Análisis económico en CAPEX de la solución propuesta

4.12.1 Estimación de costes hardware

La cooperativa Los Andes dispone de todo el hardware necesario para alojar los recursos solicitados en las cinco capas anteriores para este diseño, por lo que en este aspecto no se requiere presupuesto.

4.12.2 Estimación de costes de licencias

En este apartado realizamos un resumen del licenciamiento que es necesario adquirir. Como hemos comentado en capítulos anteriores además del licenciamiento Citrix es necesario adquirir licencias Terminal Server.

Tabla 57
Costes de licencias.

Concepto	Cantidad	Coste Unidad (por 3 años)	Importe \$
CAL Windows Server 2016	91	100	9100
CAL Microsoft Terminal Server 2016	91	250	22750

Citrix Virtual Apps	91	300	27300
Citrix Gateway	2	5000	10000
TOTAL			69150

Nota: Se presenta la factibilidad económica que se basa en la cantidad de licencias Microsoft y Citrix a adquirir, elaboración propia.

4.12.3 Estimación de costes de certificados digitales

En este apartado realizamos un resumen de costos referentes a certificados digitales a utilizar para el uso del Citrix Gateway.

Tabla 58

Costes de certificados digitales.

Concepto	Cantidad	Coste Unidad (por 3 años)	Importe \$
Certificado Externo TLS	2	382.5	765
TOTAL			765

Nota: Se presenta la factibilidad económica que se basa en el certificado digital a adquirir, elaboración propia.

4.12.4 Estimación de costes de infraestructura de Backup

En este apartado realizamos un resumen de costos referentes al uso del servicio Azure Site Recovery, estos datos los analizaremos de acuerdo con la calculadora que ofrece el servicio Azure y según la tabla 16, en la cual se muestra la cantidad de recursos a utilizar, en la siguiente figura verificaremos el costo por hora del uso de dicha plataforma.

Virtual Machines 4 E8 v3 (8 vCPU(s), 64 GB RAM) x 1 Hours; Windows – (...)

Virtual Machines

REGION:
West US

OPERATING SYSTEM:
Windows

TYPE:
(OS Only)

TIER:
Standard

INSTANCE:
E8 v3: 8 vCPU(s), 64 GB RAM, 200 GB Temporary storage, \$0.928/hour

Billing Option

Save up to 72% on pay-as-you-go prices with 1-year or 3-year Reserved Virtual Machine Instances. Reserved Instances are great for applications with steady-state usage and applications that require reserved capacity. [Learn more about Reserved VM Instances pricing.](#)

☒ Pay as you go
☐ 1 year reserved (~23% savings)
☐ 3 year reserved (~36% savings)

Save up to 40% with Windows Server Licenses you already own. [Learn more about Azure Hybrid Benefit to save compute costs.](#) ☐

4
Virtual machines

×

1
Hours

=
\$3.71
Per month

*Figura 50.*Resumen de factibilidad económica del Azure Site Recovery tomando el costo por hora de uso. Adaptado de “Arquitectura de migración basada en agente”, Microsoft Azure,2019.

Para el diseño de esta solución consideraremos una disponibilidad de la plataforma del 99.9%, el cual nos daría 719.28 horas de servicios mensual, esto nos arrojaría el uso de la plataforma ASR por una hora al mes.

Tabla 59
Costes de uso de plataforma ASR.

Concepto	Cantidad	Coste Unidad (por hora)	Importe \$
Uso Plataforma ASR	1	3.71	3.71
TOTAL			3.71

Nota: Se presenta la factibilidad económica que se basa en el uso de la plataforma Azure Site Recovery, elaboración propia.

4.12.5 Resumen de costes

En este apartado realizamos un análisis global de todos los costes relacionados con la implantación de la solución planteada:

Tabla 60

Resumen de costes diseño de plataforma

Concepto	Cantidad	Coste Unidad (por 3 años)	Importe \$
CAL Windows Server 2016	91	100	9100
CAL Microsoft Terminal Server 2016	91	250	22750
Citrix Virtual Apps	91	300	27300
Citrix Gateway	2	5000	10000
Certificado Externo TLS	2	382.5	765
Uso Plataforma ASR	1	133.56	133.56
TOTAL			70 048.56

Nota: Se presenta la factibilidad económica del diseño de virtualización de aplicaciones, elaboración propia.

CAPÍTULO 5. PRUEBAS, RESULTADOS Y VALIDACIÓN

En este capítulo, se presentan las validaciones de los resultados obtenidos en el diseño de la plataforma de virtualización, considerando el cumplimiento de los objetivos específicos. Las pruebas y la validación de los resultados en el caso de la plataforma se realizaron utilizando los valores teóricos resultantes de las especificaciones tomadas en el capítulo anterior, el cual nos ayudará a comprobar el cumplimiento de los criterios de diseño. Luego de esto se analizarán los resultados obtenidos verificando que se hayan alcanzado los objetivos del proyecto basándose en los indicadores definidos.

5.1 Evaluación de los resultados del diseño considerando el cumplimiento de la administración y supervisión centralizada según las buenas prácticas de virtualización.

Tabla 61

Matriz para el objetivo específico nro. 1

Problema	Objetivos Específicos	Indicador de Logro	Métrica
Modelo carente de un sistema de administración y supervisión centralizado. Gastos en infraestructura local desplegada en sucursales	Diseñar una plataforma de virtualización que permita la administración y supervisión centralizada según las buenas prácticas de virtualización.	Matriz de recursos a nivel de hardware y software requeridos para la centralización de aplicaciones.	Porcentaje de aplicaciones virtualizadas.

Nota: Se presenta una matriz mostrando el problema que resolverá el objetivo específico nro. 1, elaboración propia.

5.1.1 Propósito de evaluación

El propósito de esta evaluación es validar que las aplicaciones de negocio se encuentren disponibles desde un solo portal de acceso, proporcionando al usuario final el acceso fácil y centralizado de las aplicaciones que le corresponda acceder según el perfil que posea, para ello validaremos los requerimientos a nivel de hardware y software para la viabilidad de dicha plataforma, asimismo poder corroborar la cantidad de aplicaciones que van a poder ser publicadas del total que se mencionó en capítulos anteriores.

5.1.2 Alcance de evaluación

El presente plan de pruebas se enfocará en mostrar lo siguiente:

- Matriz de recursos para el portal de aplicaciones.
- Cantidad de aplicaciones disponibles para el usuario.

Para elaborar la matriz de recursos tendremos en cuenta los recursos a requerir para disponer de los servicios que requiere la plataforma de virtualización de aplicaciones.

Tabla 62

Recuento global recursos plataforma Citrix y Azure

ENTORNO	vCPU	vRAM (GB)	ALMACENAMIENTO (GB)
Citrix Apps	24	192	240
Servidores infraestructura Citrix	9	33	200
Citrix Gateway	4	4	40
Perfiles Citrix UPM			10
BBDD Citrix			20
Azure Site Recovery	8	16	1250
Totales	45	245	1760

Nota: Se presenta el recuento de recursos necesarios para abordar la capa hardware y la plataforma de backup en Azure, elaboración propia.

Asimismo, listaremos con los recursos con los que se dispone actualmente en la organización, esta información ha sido tomada del punto 4.1.1 y 4.1.2.

Tabla 63

Recuento recursos disponibles en la organizacion

ENTORNO	vCPU	vRAM (GB)	ALMACENAMIENTO (TB)	TIPO DE ARREGLO
Recursos Totales	108	386.62	7.1	10
			1.75	6
			2.7	5
Recursos Utilizados	36	60	1.2	10
			0.74	6
			1.75	5
Recursos Disponibles	72	326.62	5.9	10
			1	6
			0.95	5

Nota: Se presenta el recuento de recursos disponibles para abordar el proyecto de virtualización de aplicaciones, elaboración propia.

Tabla 64

Matriz de recursos a nivel de hardware y software.

REQUERIMIENTOS DE UNA PLATAFORMA CENTRALIZADA DE APLICACIONES		HARDWARE	SOFTWARE
	ROL	DETALLE	DETALLE
Control	Delivery Controller	02 servidores virtuales, cada uno con 02 vCPU 8GB vram, 40GB de disco duro RAID 10 y tarjeta de red con Throughput de 1 a 10 Gbps	Windows Sever 2016 / Sophos Server Security / XenApp 7.15 LTSR CU4
	Base de Datos	20 GB espacio en disco duro RAID 10	
	Active Directory	10 GB espacio en disco duro RAID 10	
Acceso	Licensing Server	01 servidor virtual, cada uno con 02 vCPU 4GB vram, 40GB de disco duro RAID 6 y tarjeta de red con Throughput de 1 a 10 Gbps	Windows Sever 2016 / Sophos Server Security / XenApp 7.15 LTSR CU4
	Citrix Gateway	02 servidores virtuales, cada uno con 02 vCPU 2GB vram, 20GB de disco duro RAID 10 y tarjeta de red con Throughput de 1 a 10 Gbps	Citrix ADC Release 13.0
	Storefront	02 servidores virtuales, cada uno con 02 vCPU 8GB vram, 40GB de disco duro RAID 10 y tarjeta de red con Throughput de 1 a 10 Gbps	Windows Sever 2016 / Sophos Server Security / XenApp 7.15 LTSR CU4
Recursos	Citrix VDA	03 servidores virtuales, cada uno con 08 vCPU 32GB vram, 80GB de disco duro RAID 10 y tarjeta de red con Throughput de 1 a 10 Gbps	Windows Sever 2016 / Sophos Server Security / XenApp 7.15 LTSR CU4
Servicio Backup	Azure Site Recovery	01 servidor virtual, cada uno con 08 vCPU 16GB vram, 50GB de disco duro RAID 10, 1.1TB de disco duro en RAID 5 y tarjeta de red con Throughput de 1 a 10 Gbps	Windows Sever 2016 / Sophos Server Security / Microsoft ASR Unified Agent

Nota: Se presenta una matriz mostrando los recursos requeridos para cumplir con el dimensionamiento a nivel de hardware y software, elaboración propia.

Luego de corroborar que a nivel de hardware y software estamos en la capacidad de poder albergar la cantidad de usuarios solicitados, asimismo es factibles poder implementar las 5 capas de las cuales consta el diseño; es conveniente validar si dichas aplicaciones son compatibles para el esquema de acceso a aplicaciones propuesto, para ello haremos las validaciones conforme se recomienda en el punto 4.5.1 de la capa de recursos con las aplicaciones mencionadas en el punto 3.2.3. A continuación, dispondremos de los requisitos de compatibilidad más importantes que podrían verificarse, las cuales han sido recabados según la especificaciones del fabricante.

Tabla 65

Tabla de compatibilidad de aplicaciones

	S.O.	Multiu uario	Arquitectura de la aplicación	Interoperabili dad	Dependen cia	Virtualización de aplicaciones
Flujo NET®	Window s 10 Window s 2016	Soport a	x64	Compatible con otros programas	Office, PDF	Streaming, Disposición en capas
CONCA R® SQL	Window s 10 Window s 2016	Soport a	x64	Compatible con otros programas	Office, PDF	Streaming, Disposición en capas
RS CRM®	Window s 10 Window s 2016	Soport a	x64	Compatible con otros programas	Office, PDF	Streaming, Disposición en capas
PLACAR ® CB	Window s 10 Window s 2016	Soport a	x64	Compatible con otros programas	Office, PDF	Streaming, Disposición en capas
SISPAG ®	Window s 10 Window s 2016	Soport a	x64	Compatible con otros programas	Office, PDF	Streaming, Disposición en capas
IVMS	Window s 10 Window s 2016	Soport a	x86, x64	Compatible con otros programas	Reproduc tor de Video	Streaming, Disposición en capas

Nota: Se presenta los requisitos de las aplicaciones para el uso en una plataforma virtual, elaboración propia.

Por los resultados obtenidos en las tablas 45 y 46 podemos concluir que la organización se encuentra en capacidad tanto técnico como de recursos para poder desplegar la solución

multicapas diseñado para la totalidad de aplicaciones, con ello la métrica obtenida por dicho diseño será del 100% según lo mencionado.

5.2 Evaluación de los resultados de la optimización del desempeño de la aplicación considerando la mejora del rendimiento y un óptimo consumo de ancho de banda según las buenas prácticas de virtualización.

Tabla 66

Matriz para el objetivo específico nro. 2

Problema	Objetivos Específicos	Indicador de Logro	Métrica
Bajo desempeño de la aplicación en uso	Optimizar el desempeño de la aplicación, direccionando hacia un mejor rendimiento y un	Tiempos de retardo menores al momento de registrar una entrada en las aplicaciones.	ms
Servidores de acceso a aplicaciones saturados en su capacidad de trabajo	óptimo consumo de ancho de banda según las buenas prácticas de virtualización.	Reducción de la saturación de los enlaces de ancho de banda en sedes.	Bits/s

Nota: Se presenta una matriz mostrando el problema que resolverá el objetivo específico nro. 2, elaboración propia.

5.2.1 Propósito de evaluación

Utilizando las buenas prácticas y los detalles técnicos seleccionados en el diseño realizaremos las comprobaciones de que la plataforma logra obtener tiempos de retardo menores al de la actual plataforma, proporcionando el usuario una mejor experiencia en el registro de entradas en el ERP. Por otro lado, también se validará que se cumplan con los propósitos de poder reducir el consumo de ancho de banda por usuario conectado a una aplicación simulando las características de red que se poseen en sucursales.

5.2.2 Alcance de evaluación

El presente plan de pruebas se enfocará en mostrar lo siguiente:

- Medir los tiempos de retardo de una aplicación al registrar una entrada.
- Verificar el consumo de ancho de banda aplicando los protocolos de envío de paquetes de la solución Citrix Virtual Apps en los enlaces en sucursales.

- Tabla de requerimientos y resultados obtenidos.

5.2.3 Tipos de pruebas

A continuación, listamos los tipos de pruebas a realizar a la plataforma implementada para las pruebas para el presente plan de pruebas.

5.2.3.1 Pruebas retardo en el uso de la aplicación

Esta prueba verifica que la plataforma proporciona al usuario menores tiempos de retardo al interactuar con las aplicaciones de negocio, ya sea cuando consultan una base de datos o se utilice un recurso compartido de archivos.

- **Objetivos:**

- Verificar los tiempos de retardo al utilizar aplicaciones de negocio de los usuarios.
- Contrastar los tiempos de retardo que brinda la actual plataforma con los que se obtienen en las pruebas de la plataforma diseñada.

- **Técnicas:**

- Se utilizará un simulador de red de Windows que nos permita configurar la latencia de red para la conexión entrante y saliente similares con las que se cuentan en sucursales.
- Se elaborará un script en Powershell para la lectura y comparación de los tiempos de retardo en el uso de las aplicaciones.

- **Criterios de finalización:**

- La usabilidad de las aplicaciones cumple a la aceptación estándar del usuario.

- **Consideraciones especiales:**

- Los valores se van a recabar desde la Instrumentación de Administración de Windows (WMI), la cual nos proporcionará la interfaz del sistema operativo host a través del cual sus componentes nos darán la información y distintos tipos de notificaciones que son pertinentes para dichas pruebas.

5.2.3.2 Pruebas consumo ancho de banda

Para esta prueba mediremos el desempeño de las aplicaciones al utilizar Citrix HDX, para poder obtener un mejor rendimiento de red en conexiones de alta latencia como ocurren en varios de los enlaces en sucursales.

La configuración del número correcto de búferes utilizados para enviar los datos nos permitirá que HDX use todo el ancho de banda disponible en conexiones de alta latencia para el acceso a las aplicaciones.

- **Objetivos:**

- Verificar los consumos de ancho de banda para las aplicaciones ERP y multimedia.
- Utilizar las diferentes variantes de Citrix HDX con el fin de ubicar la combinación que nos ofrezca mejor ancho de banda desempeño.
- Contrastar los consumos que brinda la actual plataforma con los que se obtienen en las pruebas de la plataforma diseñada.

- **Técnicas:**

- Se utilizará el PerfMon para rastrear el rendimiento del proceso tanto del ancho de banda como la del CPU.
- Se brindarán los resultados de las mediciones según el uso de los diversos protocolos para los dos tipos de aplicaciones que se manejan.

- **Criterios de finalización:**

- La usabilidad de las aplicaciones cumple el requerimiento de la organización.

- **Consideraciones especiales:**

Para demostrar las validaciones y la diferencia entre diferentes tipos de aplicaciones, vamos a describir dos casos de uso de prueba para obtener resultados reproducibles:

- **Aplicaciones ERP**

En esta parte contemplaremos el trabajar con aplicaciones ya mencionadas en el capítulo 3, como las de Flujo NET, Concar SQL, Sispag y Placar CB. Estas no cuentan con muchos gráficos, ni imágenes o texto sofisticados, solo con menús, tablas e informes en Excel de la información que se maneja.

- **Aplicaciones Multimedia**

Aquí incluiremos a la aplicación IVMS la cual contará con reproducción de video en tiempo real.

5.2.4 Recursos para las pruebas

En este apartado se listan todos los recursos necesarios para realizar las pruebas, tales como los recursos de software, hardware, configuraciones y personal.

5.2.4.1 Software

Tabla 67

Software utilizado para los planes de Pruebas del Objetivo Específico 2.

Ítem	Nombre de software	Versión	Utilidad
1	Google Chrome	78	Navegador para el acceso al portal de aplicaciones.
2	Windows Powershell	5.1	Nos permitirá recopilar información desde el WMI.
3	Clumsy	0.2	Nos permitirá configurar latencia de entrada y salida de red.

Nota: Se presenta el software utilizado para realizar para los planes de pruebas, elaboración propia.

5.2.4.2 Hardware

Tabla 68

Hardware utilizado para el plan de pruebas del Objetivo Especifico 2.

Ítem.	Recurso	Cantidad	Descripción
1	Servidor virtual	1	04 vCPU
2	Disco duro virtual	1	60 GB
3	Memoria virtual	1	8 GB
4	Tarjeta de red	1	1 GBps

Nota: Se presenta el hardware utilizado para realizar los planes de pruebas, elaboración propia.

5.2.5 Configuraciones de ambiente de pruebas

Se presenta en la siguiente tabla, las configuraciones del ambiente de pruebas

Tabla 69

Configuración de ambiente para Objetivo Especifico 2.

Ítem.	Requerimiento	Versión	Fabricante	Implementación y configuración
1	Sistema Operativo para Servidores	Windows Server 2016 Standard	Microsoft	Sistema operativo para servidores donde se configurará la VDA y el Receiver.

2	Citrix ADC BLX	13	Citrix	Módulo en el cual se configurar el códec de video seleccionado según las pruebas.
3	Delivery Controller	7.15	Citrix	Módulo desde donde los usuarios validaran el acceso a las aplicaciones.
4	Citrix VDA	7.15	Citrix	Módulo en donde se encontrarán instaladas las aplicaciones.
4	Módulo de Contabilidad		Realsystems	Software de contabilidad utilizado por los usuarios
5	Google Chrome	78	Google	Navegador de internet por donde se accede a la plataforma de aplicaciones

Nota: Se presenta las configuraciones del ambiente de pruebas utilizado para realizar los planes de pruebas, elaboración propia.

5.2.6 Casos de prueba

5.2.6.1 Retardo en el uso de la aplicación

Una de las métricas útiles disponibles para ICA es una medición de latencia conocida como el tiempo de ida y vuelta (ICA RTT). Este es el intervalo de tiempo medido en el cliente entre el primer paso (acción del usuario) y el último paso (se muestra la respuesta gráfica). Esta métrica puede considerarse como una medida del retraso de la pantalla que experimenta un usuario mientras interactúa con una aplicación alojada en una sesión en un servidor Citrix App.

Los valores de ICA RTT los podremos obtener a través del HDX Insights, pero para el caso práctico los obtendremos a través de un proveedor de WMI para terceros incorporado en nuestro servidor de aplicaciones. Los datos RTT están disponibles en el VDA a través de los proveedores EUEM WMI, como en el diseño utilizaremos RDS (Citrix App) necesitaremos saber la ID de sesión para el cual recabaremos la información.

Dentro de la herramienta de línea de comandos WMIC, ingresamos la siguiente información:

```
C:\Windows\system32\cmd.exe - wmic
C:\Users\dsilva>wmic
wmic:root\cli>/namespace:\\root\citrix\euem
wmic:root\cli>path citrix_euem_roundtrip get /value
```

Figura 51. Línea de comandos WMI para el acceso a información RTT. Adaptado de “Habilitación de recursos WMI”, elaboración propia.

Para el comando ingresado la información de salida sería la siguiente:

```

C:\Windows\system32\cmd.exe - wmic

C:\Users\dsilva>wmic
wmic:root\cli>/namespace:\\root\citrix\euem
wmic:root\cli>path citrix_euem_roundtrip get /value

FirstDrawRoundtripDuration=0
FrameCutRoundtripDuration=0
FrameSendRoundtripDuration=0
InputBandwidthAvailable=0
InputBandwidthUsed=392
InstanceId=3843
NetworkLatency=1
OutputBandwidthAvailable=100702136
OutputBandwidthUsed=33976
ProcessId=f2e02327-acde-4a5d-a4fa-b86746995d8f
RoundtripTime=76
SessionID=2
Timestamp=20191128172542.719000+000
TriggerRoundtripDuration=0
WDTripleRoundtripDuration=0
  
```

Figura 52. Resultado de consulta WMI para información RTT. Adaptado de “Habilitación de recursos WMI”, elaboración propia.

La información enmarcada en rojo nos va a permitir realizar las comparativas de los retardos con la plataforma anterior y la del modelo diseñado. Lo siguiente será utilizar el Clumsy 0.2 para simular la latencia de los enlaces satelitales en sucursales tal y como se muestra en la siguiente imagen.

Figura 53. Simulación latencia con herramienta Clumsy. Adaptado de “Configuración de simulador de red Clumsy”, elaboración propia.

Posteriormente utilizaremos la información que se muestra a través de WMI para ejecutarla vía Powershell. Luego de ello podremos exportarlo a un script para poder consultar los valores ICA RTT e ICA Network Latency, así como un script que mida el tiempo de ping a nuestro punto final.

```
PS C:\Users\dsilva> Get-WmiObject -Namespace root\Citrix\euem -Class Citrix_Euem_RoundTrip | select @{n='Date-Time';e={get-date}}, SessionID, NetworkLatency, RoundTripTime
```

Figura 54. Código de consulta los valores ICA RTT y NetworkLatency. Adaptado de “Configuración de script vía Powershell”, elaboración propia.

Exportaremos el comando de powershell al editor de scripts de Powershell para poder elaborar las comparativas.

Figura 55. Elaboración de script para la consulta secuencial. Adaptado de “Configuración de script vía Powershell”, elaboración propia.

Como se visualiza en la imagen los tiempos de ida y vuelta (ICA RTT) bordean los 664 ms para enlaces simulados con la latencia que se poseen en sucursales, esta información al ser contrastada con la que actualmente se tiene en la plataforma actual podrá darnos valores a favor del modelo en diseño, las cuales permitirán darle al usuario una mejor experiencia de interacción con el portal y aplicaciones.

```

PS C:\Users\dsilva\Documents> .\pruebaRTT.ps1

Date-Time           SessionID NetworkLatency RoundTripTime
-----
27/12/2019 15:51:15         2           625           664
27/12/2019 15:51:15         5           660           700
27/12/2019 15:51:15         3           631           676

```

Figura 56. Resultados de ejecución de script de tiempo de demora. Adaptado de “Configuración de script vía Powershell”, elaboración propia.

Esta información puede ser visualizada de manera gráfica y más detallada en el caso de utilizar el Citrix ADC y su módulo HDX Insight, así como se muestra en la imagen siguiente.

Figura 57. Verificación de RTT desde módulo Citrix Gateway. Adaptado de “Comprehensive Citrix HDX visibility powered by NetScaler Management and Analytics System”, por Citrix, 2017.

El termino ICA RTT representa en el retardo real de aplicación, que incluye: Retardo del sistema operativo cliente, latencia de red, retrasos en el host de la sesión para procesar la solicitud y retrasos en el tiempo de procesamiento de la aplicación en el host de sesión. Si bien los factores mencionados influyen en el valor total, ICA_RTT no es igual a los retrasos sumados anteriormente, esto debido a que la mayoría de estos valores son capa 4 mientras que ICA RTT se calcula en la capa 7.

Por lo tanto, para el caso práctico hemos tenido que simular la topología para obtener los valores de ICA RTT, según lo obtenido en laboratorio por la plataforma diseñada, estos bordearan desde los 60 ms hasta 120 ms de retardo como se muestran en la figura 45, esto sumado a la latencia de red que presente el enlace desde el cual disponemos a conectarnos nos dará el retardo total de interactuar con la plataforma.

5.2.6.2 Evaluación consumo ancho de banda

Para medir el uso del ancho de banda y CPU, definiremos un origen de datos para recopilar a través del Windows Performance Monitor (Perfmon) dentro de las opciones buscaremos la siguiente ruta:

- “\ICA Session\Output ThinWire Bandwidth”

Y para medir el consumo de CPU:

- “\Processor Information\%Processor Utility”

Figura 58. Pantalla de contadores del performance monitor en el servidor VDA a ser medido. Adaptado de “Evaluación Consumo Ancho de Banda”, elaboración propia.

Durante la prueba probaremos los siguientes tres modos:

- Thinwire Plus (Utiliza códec de video para compresión)
- Pantalla completa H.264 (Utiliza códec de video para compresión en toda la pantalla)

- Selectivo H.264 (Utiliza códec de video para compresión: para regiones que cambian activamente).

Los anchos de bandas referenciales fueron tomados de la tabla 9 del punto 3.2.3. Es así que con el uso de los siguientes protocolos de visualización los valores referenciales de consumo de ancho de banda y consumo en cpu serían los siguientes:

Tabla 70

Consumo Recursos Aplicaciones ERP

-	Thinwire Plus	Pantalla completa H.264	Selectivo H.264
Ancho de banda promedio fuera.	0.47 Mbps	0.59 Mbps	0.46 Mbps
Uso procesador promedio.	8,33%	8,46%	7,87%

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con su respectivo códec de visualización, elaboración propia.

Tabla 71

Consumo Recursos Aplicaciones Multimedia

-	Thinwire Plus	Pantalla completa H.264	Selectivo H.264
Ancho de banda promedio fuera.	4.6 Mbps	4.1 Mbps	5.1 Mbps
Uso procesador promedio.	11,64%	14,40%	11,67%

Nota: Se presenta el consumo de recursos de las aplicaciones multimedia con su respectivo códec de visualización, elaboración propia.

Podemos ver que hay una diferencia de alrededor del 6% entre los diferentes modos. Asimismo, podemos notar que, dependiendo el caso de uso, un modo diferente produce la menor cantidad de ancho de banda.

Para usuarios habituales de las aplicaciones ERP, Selectivo H.264 tiene más sentido ya que produce una muy buena experiencia de usuario con el ancho de banda más bajo. Para los usuarios de Aplicaciones Multimedia, se vuelve un poco más complicado. El ancho de banda más bajo se puede lograr con Pantalla Completa H.264, sin embargo, la utilización del procesador es considerablemente mayor que con Thinwire Plus. Este va a depender de las prioridades que uno quiera brindarle según los requisitos del usuario en la sucursal.

De hecho, cuando veamos este caso de uso con nuestros clientes, dependiendo de lo que el cliente quiera lograr, se optaría por diferentes caminos. Si opta por el consumo de ancho de banda más bajo, pantalla completa H.264 puede ser correcto (a un costo considerable en densidad de usuario). O si la densidad de usuarios por servidor es más importante, Thinwire Plus puede ser el adecuado, caso contrario se puede elegir el término medio e ir a Selective H.264, ya que produce una experiencia de usuario igualmente buena que Pantalla Completa H.264 con menos uso del procesador, pero a expensas del ancho de banda.

Una vez elegido el modo que se ajusta al mejor costo beneficio para el uso de la aplicación, podremos recurrir a otras formas de ajustar aún más los diferentes modos y protocolo HDX en general. Para ello demostraremos algunos de estos ajustes en el caso de prueba de Aplicaciones ERP con Selective H.264. Después de todo, es el modo predeterminado y, probablemente, el modo con el que desea ceder si no está claro qué casos de uso encontrará en su entorno.

Para esta parte utilizaremos el transporte adaptativo para vídeo, aplicaciones y datos, y como UDP debería usar el ancho de banda disponible de manera más eficiente ya que no es un protocolo orientado a la conexión, teóricamente podría tener un impacto en el ancho de banda utilizado. Para ello habilitaremos las siguientes opciones dentro de nuestro Citrix Gateway, el cual mantiene comunicación con nuestro StoreFront y autenticar usuarios para nuestro Citrix Virtual Apps, dentro de ella editaremos la opción mostrada para habilitar la configuración DTLS (Datagram Transport Layer Security) que es el protocolo que otorga privacidad cuando se trabaja con el protocolo de transporte UDP.

Figura 59. Pestaña Configuración en la GUI Citrix ADC para habilitación de EDT. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia.

Figura 60. Pestaña Configuración básica para el servidor virtual VPN y habilitación de DTLS. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia.

Una vez habilitada el transporte adaptativo mostraremos los resultados obtenidos a través del Perfmon en la siguiente tabla:

Tabla 72
Consumo Recursos Aplicaciones ERP con EDT

	Selectivo H.264 sin transporte adaptativo	H.264 selectivo con transporte adaptativo
Ancho de banda promedio fuera	0.46 Mbps	0.49 Mbps (+ 7%)
Uso procesador promedio.	7,87%	8,52%

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con el cambio en el protocolo de transporte, elaboración propia.

En este punto vemos un mayor uso del ancho de banda de alrededor del 7%. Hay que tener en cuenta que este empleo viene con una experiencia de usuario mucho mejor en conexiones de alta latencia, las cuales nos permitirá poder utilizar las aplicaciones en sucursales en las cuales los enlaces son satelitales y las latencias bordean de 500 ms a 600 ms.

Siguiendo con la optimización de los recursos para el uso de las aplicaciones, utilizaremos otro código de compresión sin pérdida llamado MDRLE. MDRLE utilizará una mejor compresión para gráficos y texto simples, estos podremos usarlos a partir de la versión de VDA Citrix Apps 7.17 y el receiver para Windows versión 4.11 y bastará con tener habilitada la opción *use video codec for compression*.

Figura 61. Pestaña Configuración HDX Thinwire para habilitación de MDRLE. Adaptado de “Evaluación Consumo Ancho de Banda”, elaboración propia.

Una vez habilitado el codificador MDRLE y validada la versión de VDA y Receiver mostraremos en la tabla 69 los registros entregados en el Perfmon, en la cual visualizaremos una disminución del 7% del ancho de banda utilizado.

Tabla 73
Consumo Recursos Aplicaciones ERP con MDRLE

-	Selectivo H.264 sin MDRLE	Selectivo H.264 con MDRLE
Ancho de banda promedio fuera	0.46 Mbps	0.42 Mbps (-7,1 %)
Uso procesador promedio.	7,87%	8.81%

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con el uso de códec de compresión MDRLE, elaboración propia.

Y si volvemos a habilitar el transporte adaptativo, la disminución es aún mayor:

Tabla 74

Consumo Recursos Aplicaciones ERP con EDT y MDRLE

-	Selectivo H.264 sin MDRLE y transporte adaptativo	Selectivo H.264 con MDRLE y transporte adaptativo
Ancho de banda promedio fuera	0.49 Mbps	0.43 Mbps (-11,4%)
Uso procesador promedio.	8,52%	8,65%

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con el uso de códec de compresión MDRLE y cambio de protocolo de transporte, elaboración propia.

Podremos ver según la tabla 70 que con el MDRLE no solo se compensó el aumento que viene con el Transporte Adaptativo, sino que también disminuyó el ancho de banda requerido, permitiéndole aplicar en sucursales en las cuales sólo tenemos opciones satelitales de conexión.

Otro recurso que utilizaremos será el de la Compresión de color adicional (ECC), esto recomendado para usarlo en escenarios de ancho de banda restringido como el que tenemos en varias sucursales. Para ello tendremos que modificar el registro mostrado en la siguiente imagen al valor de 1.

Figura 62. Claves de registro según la configuración de compresión con pérdida actual. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia.

Las pruebas mostraran que se puede disminuir el ancho de banda en un 3.3%:

Tabla 75

Consumo Recursos Aplicaciones ERP con ECC

-	Selectivo H.264 sin ECC	Selectivo H.264 con ECC
Ancho de banda promedio fuera	0.46 Mbps	0.44 Mbps (-3,3%)
Uso procesador promedio.	7,87%	8,65%

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con el uso del método criptográfico ECC, elaboración propia.

El recurso por utilizar para la siguiente prueba es la de la profundidad de color preferida para gráficos simples, esta nos puede aportar grandes mejoras al ancho de banda requerido, pero a cambio de un costo en la tasa de bits. El valor predeterminado es el de 24 bits y las pruebas las realizaremos con 16 y 8 bits, para varios usos los de 16 bits pueden ser aceptables para un escenario de aplicaciones de oficina, 8 bits probablemente solo serán una opción en circunstancias extraordinarias, como terminales POS. La siguiente imagen muestra una comparación intuitiva entre la profundidad de 24 y 16 bits.

Figura 63. Muestra de tabla con profundidad de color a 24 y 16 bits. Adaptado de “Evaluacion Consumo Ancho de Banda”, elaboración propia

Una vez realizadas las pruebas a través del Perfmon visualizaremos lo siguiente, con 16 bits se puede lograr una buena disminución del 7.1%. mientras que 8 bits ha se puede reflejar una enorme mejora del 44.3%:

Tabla 76
Consumo Recursos Aplicaciones ERP con Profundidad de color preferida

-	Selectivo H.264 con 24 bits	Selectivo H.264 con 16 bits
Ancho de banda promedio fuera	0.46 Mbps	0.42 Mbps (-7,1 %)
Uso procesador promedio.	7,87%	8.81%

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con el uso de profundidad de color preferida a 16 bits, elaboración propia.

Tabla 77
Consumo Recursos Aplicaciones ERP con Profundidad de color preferida

-	Selectivo H.264 con 24 bits	Selectivo H.264 con 8 bits
Ancho de banda promedio fuera	0.46 Mbps	0.25 Mbps (-44.3%)

Uso procesador promedio.	7,87%	9.05%
--------------------------	-------	-------

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con el uso de profundidad de color preferida a 8 bits, elaboración propia.

Finalizando las validaciones utilizaremos el recurso de la calidad visual, la cual al configurarla en calidad baja aumentará aún más la compresión utilizada y producto de ello una disminución adicional del 18.8% en el uso del ancho de banda. A modo de comparación, en la tabla 74 visualizamos en calidad visual alta, media y baja:

Tabla 78

Consumo Recursos Aplicaciones ERP con Calidad Visual

-	Selectivo H.264 con VQ Alta	H.264 selectivo con medio VQ (predeterminado)	Selectivo H.264 con VQ bajo
Ancho de banda promedio fuera	0.67 Mbps (+ 46.8%)	0.46 Mbps	0.37 Mbps (- 18.8 %)
Uso procesador promedio.	9,79%	7,87%	8,51%

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con el uso de calidad visual variable, elaboración propia.

En el caso que habilitáramos todas las configuraciones mencionadas anteriormente (con una profundidad de color de 16 bits), lograríamos los datos mostrados en la tabla 75.

Tabla 79

Consumo Recursos Aplicaciones ERP optimizado

-	Selectivo H.264	H.264 selectivo optimizado
Ancho de banda promedio fuera	0.46 Mbps	0.28 Mbps (-36.3%)
Uso procesador promedio.	7,87%	7,92%

Nota: Se presenta el consumo de recursos de las aplicaciones ERP con el uso de profundidad de color preferida a 16 bits, método criptográfico ECC y códec de compresión MDRLE, elaboración propia.

Eso es una disminución del 36.3% (43.4% en comparación con el Transporte Adaptativo) en un protocolo ya muy optimizado, el cual nos permitiría poder desarrollar el uso fluido de las aplicaciones según los datos de ancho de banda y latencias con los que se cuentan en sucursales.

Con lo cual podríamos concluir que para los enlaces con los que se cuentan en sucursales que bordean los 2 Mbps y contando con una media de 5 usuarios por oficina, podríamos conectar la totalidad de usuarios a dicho enlace, ya que incurriríamos en un uso aproximado del 70% de la capacidad total contratada, siempre y cuando utilicemos la siguiente combinación H.264 selectivo con transporte adaptivo, MDRLE, ECC y a 16 bits.

5.3 Evaluación de los resultados de la continuidad de acceso a la aplicación considerando la alta disponibilidad y seguridad a la solución según las buenas prácticas de virtualización

Tabla 80

Matriz para el objetivo específico nro. 3

Problema	Objetivos Específicos	Indicador de Logro	Métrica
Acceso externo inseguro Solución carente de movilidad para el acceso desde dispositivos móviles a las aplicaciones	Proponer un diseño que brinde continuidad y seguridad de acceso a la plataforma según las buenas prácticas de virtualización.	Capacidad de acceso externo de manera segura a la plataforma centralizada de aplicaciones. Cantidad máxima permitida de datos perdidos medidos en el tiempo y tiempo que tarda la restauración desde el incidente hasta que las operaciones normales estén disponibles (RPO y RTO)	Número de conexiones satisfactorias desde una red interna y externa. Minutos

Nota: Se presenta una matriz mostrando el problema que resolverá el objetivo específico nro. 3, elaboración propia.

5.3.1 Propósito de evaluación

El propósito de esta evaluación es validar que la nueva plataforma de aplicaciones tiene la capacidad de acceso desde una red externa a través de cualquier navegador, asimismo este acceso se realice de forma segura a través de un certificado digital TLS; por otro lado, se deberá constatar la continuidad del acceso a dichas aplicaciones al ir degradando servicios dentro de la plataforma, poniendo en funcionamiento servicios que estaban en modo espera.

5.3.2 Alcance de evaluación

El presente plan de pruebas se enfocará en verificar lo siguiente:

- Acceso externo al portal de aplicaciones.
- Comunicación segura hacia la plataforma utilizando el protocolo TLS.
- Método de conexión del tipo ICA Proxy para el acceso desde los hosts.
- Disponibilidad de acceso a las aplicaciones ante degradación de servicios dentro del diseño de la plataforma.

5.3.3 Tipos de pruebas

Se menciona el tipo de pruebas a realizar a la plataforma implementada para las pruebas para el presente plan de pruebas.

5.3.3.1 Pruebas de seguridad y continuidad de acceso

Las pruebas de seguridad y continuidad de acceso se enfocan en dos aspectos, la seguridad de acceso a la plataforma, en la cual se verifica que el uso de certificados digitales SSL/TLS para el acceso a usuarios locales, externos y móviles, asimismo se verificará que el tipo de conexión del host al servidor sea cifrado; por otro lado, para la continuidad de acceso a las aplicaciones de la plataforma verificaremos que el abordaje multicapa utilizado en el diseño nos permita garantizar la disponibilidad.

• **Objetivos:**

- Verificar que el acceso a la plataforma de aplicaciones sea a través del protocolo HTTPS mediante un navegador web y el protocolo TLS para la comunicación segura.
- Verificar que los usuarios accedan a las aplicaciones mediante el uso del tipo de conexión Proxy ICA.
- Verificar la continuidad del servicio en el diseño multicapa forzando la degradación de servicios en cada una de ellas.

• **Técnicas:**

- Nivel de acceso a la plataforma:

Se comprobará acceder mediante desde cualquier navegador a la plataforma de aplicaciones tanto desde la red interna como externa.

- Nivel de seguridad de la plataforma:

Se comprobará el uso del protocolo TLS en la plataforma de acceso a las aplicaciones.

Se comprobará el uso del tipo de conexión Proxy ICA para el acceso a las aplicaciones.

- Nivel de continuidad de acceso:

Se comprobará la redundancia de servicios por capa en el diseño de la plataforma.

• **Criterios de finalización:**

- El acceso interno como externo mostrara un certificado digital valido en el navegador.

- Para el caso local un certificado digital emitido por un CA local, en el acceso externo por un certificado emitido por un CA externo.

- Se validará que los datos viajan cifrados y que el tipo de conexión es la del Proxy ICA.

- Se validará el acceso al portal ante la degradación de servicios por cada capa diseñada.

5.3.4 Recursos para las pruebas

En este apartado se listan todos los recursos necesarios para realizar las pruebas, tales como los recursos de software, hardware, configuraciones y personal.

5.3.4.1 Software

Tabla 81

Software utilizado para Pruebas del objetivo específico 3.

Ítem	Nombre de software	Versión	Utilidad
1	Google Chrome	78	Navegador para el acceso al portal de aplicaciones.
2	Wireshark	3.0.6	Analizador de tráfico red en tiempo real

Nota: Se presenta el software utilizado para realizar para los planes de pruebas, elaboración propia.

5.3.4.2 Hardware

Tabla 82

Hardware utilizado para Pruebas del objetivo específico 3.

Ítem.	Recurso	Cantidad	Descripción
1	Servidor virtual	1	04 vCPU
2	Disco duro virtual	1	60 GB

3	Memoria virtual	1	8 GB
4	Tarjeta de red	1	1 GBps

Nota: Se presenta el hardware utilizado para realizar los planes de pruebas, elaboración propia.

5.3.5 Configuraciones de ambiente de pruebas

Tabla 83

Configuración de ambiente para el objetivo específico 3.

Ítem.	Requerimiento	Versión	Fabricante	Implementación y configuración
1	Sistema Operativo para Servidores	Windows Server 2016 Standard	Microsoft	Sistema operativo para servidores donde se configurará la VDA y el Receiver.
2	Citrix ADC BLX	13	Citrix	Módulo en el cual se configurará el codec de video seleccionado según las pruebas.
3	Delivery Controller	7.15	Citrix	Modulo desde donde los usuarios validaran el acceso a las aplicaciones.
4	IOS	13.5	Apple	Sistemas Operativo de dispositivo móvil.
5	Google Chrome	78	Google	Navegador de internet por donde se accede a la plataforma de aplicaciones

Nota: Se presenta las configuraciones del ambiente de pruebas utilizado para realizar los planes de pruebas, elaboración propia.

Se presenta en la siguiente tabla, las configuraciones del ambiente de pruebas

5.3.6 Casos de prueba

Se presentan 1 caso de uso diseñado y ejecutado por el equipo de pruebas.

Tabla 84

Caso de uso 1 para el plan de pruebas de seguridad de acceso.

Caso de uso nro. 1	
Tipo de Prueba: Pruebas de seguridad de acceso	
Caso de Prueba: Acceso externo e interno a la plataforma de aplicaciones.	Autor del Caso de Prueba: David Silva.

Versión del Caso de Prueba: 1.0			Fecha de Creación:
Ambiente de prueba: Test.			Fecha de Ejecución:
<p>Objetivo de prueba: Realizar el ingreso al portal a través del navegador y verificar la existencia del certificado digital tanto en el acceso local como externo.</p>			<p>Criterios de éxito y fracaso:</p> <ul style="list-style-type: none"> · Éxito: Existencia de certificados en el navegador. · Fracaso: La página muestra un mensaje de que la conexión con el sitio web no es seguro.
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	Se ingresa la dirección https://citrixapp.adtest.local/Citrix/StoreWeb/ mediante el navegador desde la red interna.	Se muestra el portal de aplicaciones con un certificado digital válido emitido por el CA interno, y así mismo muestra la imagen de ingreso de credenciales del Storefront.	Portal de login de las aplicaciones cargado sin ninguna advertencia de certificado inválido.
2	Se ingresa la dirección https://citrix.adtest.pe/vpn/index.html mediante el navegador desde la red externa.	Se muestra el portal de aplicaciones con un certificado digital válido emitido por el CA externo RapidSSL, en la cual solicita las credenciales de usuario.	Portal de login de las aplicaciones cargado sin ninguna advertencia de certificado inválido.
3	Se ingresa a través de la app Citrix Workspace a los servicios del portal colocando el enlace externo. https://citrix.adtest.pe	Se muestra en la app en los parámetros de seguridad el protocolo de seguridad activado con la versión TLS 1.0, 1.1, 1.2.	Login en la app de acceso a las aplicaciones cargado sin ninguna advertencia de

			certificado inválido
Decisión de Aprobación del Caso de Prueba: Aprobó: <u> x </u> Fallo:			
Nombre y firma del usuario de pruebas		Daniel Espinoza	
Nombre y firma del Analista de pruebas		Dandy Rosales	
Fecha de Aprobación del Caso de Prueba:			

Nota: Se presenta el primer caso de uso para el plan de pruebas de seguridad de acceso, elaboración propia.

Para el uso de los siguientes casos de uso tomaremos como referencia el diseño final obtenido según los puntos mencionados en el capítulo 4 teniendo como resultado la imagen 47.

Tabla 85

Caso de uso 2 para el plan de pruebas de continuidad de acceso.

Caso de uso nro. 2			
Tipo de Prueba: Fallo en un servidor de Storefront Interno			
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.		Autor del Caso de Prueba: David Silva.	
Versión del Caso de Prueba: 1.0		Fecha de Creación:	
Ambiente de prueba: Test.		Fecha de Ejecución:	
Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Criterios de éxito y fracaso: <ul style="list-style-type: none">· Éxito:· Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	En este caso se pondrá a prueba los equipos CSF01 y CSF02, los usuarios afectados serán los que trabajan internamente.	Es necesario refrescar el cliente de Citrix para poder ejecutar de nuevo aplicaciones de la plataforma. Las aplicaciones ya iniciadas no se ven afectadas.	Se pierde la conectividad con el StoreFront interno, tanto del acceso web como del cliente de Citrix, las aplicaciones que estuviesen en ejecución funcionan correctamente.
Decisión de Aprobación del Caso de Prueba: Aprobó: <u>x</u> Fallo:			
Nombre y firma del tester		Daniel Espinoza	
Nombre y firma del Analista de pruebas		Dandy Rosales	

Fecha de Aprobación del Caso de Prueba:

Nota: Se presenta el segundo caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

Tabla 86

Caso de uso 3 para el plan de pruebas de continuidad de acceso

Caso de uso nro. 3			
Tipo de Prueba: Fallo en un servidor de Citrix Gateway			
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.		Autor del Caso de Prueba: David Silva.	
Versión del Caso de Prueba: 1.0		Fecha de Creación:	
Ambiente de prueba: Test.		Fecha de Ejecución:	
Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Criterios de éxito y fracaso: <ul style="list-style-type: none">· Éxito:· Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	En este caso se pondrá a prueba los equipos CG01 y CG02, los usuarios afectados serán los que trabajan externamente.	Es necesario refrescar el cliente de Citrix para poder ejecutar de nuevo aplicaciones de la plataforma. Las aplicaciones ya iniciadas no se ven afectadas.	<p>Se pierde la conectividad con Citrix Gateway tanto del acceso web como del cliente de Citrix, las aplicaciones que estuviesen en ejecución funcionan correctamente. El login a través del otro nodo Citrix Gateway funciona correctamente, así como la ejecución de las aplicaciones.</p> <p>Abre las nuevas aplicaciones en un servidor distinto al que, de las aplicaciones abiertas antes de la caída del Citrix Gateway, crea una nueva sesión de usuario en los servidores. En las sesiones creadas con PNAGent abre las aplicaciones en el mismo servidor donde estaban abiertas antes de la parada del servidor.</p>
Decisión de Aprobación del Caso de Prueba: Aprobó: <u> x </u> Fallo:			

Nombre y firma del tester	Daniel Espinoza
Nombre y firma del Analista de pruebas	Dandy Rosales
Fecha de Aprobación del Caso de Prueba:	

Nota: Se presenta el tercer caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

Tabla 87

Caso de uso 4 para el plan de pruebas de continuidad de acceso.

Caso de uso nro. 4			
Tipo de Prueba: Fallo en un servidor de licencias Citrix			
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.		Autor del Caso de Prueba: David Silva.	
Versión del Caso de Prueba: 1.0		Fecha de Creación:	
Ambiente de prueba: Test.		Fecha de Ejecución:	
Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Criterios de éxito y fracaso: <ul style="list-style-type: none">· Éxito:· Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	En este caso se pondrá a prueba el equipo CLS01.	Se pueden iniciar aplicaciones nuevas. Es necesario recuperar el servicio antes de 30 días. A partir de ese momento los usuarios no podrían establecer conexión. No se deben reiniciar equipos dentro del diseño Citrix Apps	Los usuarios inician aplicaciones. Las aplicaciones abiertas no se ven afectadas.
Decisión de Aprobación del Caso de Prueba: Aprobó: <u>x</u> Fallo:			
Nombre y firma del tester		Daniel Espinoza	
Nombre y firma del Analista de pruebas		Dandy Rosales	
Fecha de Aprobación del Caso de Prueba:			

Nota: Se presenta el cuarto caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

Tabla 88

Caso de uso 5 para el plan de pruebas de continuidad de acceso.

Caso de uso nro. 5

Tipo de Prueba: Fallo en un servidor Delivery Controller			
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.		Autor del Caso de Prueba: David Silva.	
Versión del Caso de Prueba: 1.0		Fecha de Creación:	
Ambiente de prueba: Test.		Fecha de Ejecución:	
Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Criterios de éxito y fracaso: · Éxito: · Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	En este caso se pondrá a prueba los equipos DC01 y DC02, esto afecta tanto usuarios internos como externos.	Las aplicaciones ya iniciadas siguen funcionando. Pueden iniciarse aplicaciones nuevas desde cualquiera de los métodos de acceso, web y cliente citrix.	El mismo que el esperado
Decisión de Aprobación del Caso de Prueba: Aprobó: <u> x </u> Fallo:			
Nombre y firma del tester		Daniel Espinoza	
Nombre y firma del Analista de pruebas		Dandy Rosales	
Fecha de Aprobación del Caso de Prueba:			

Nota: Se presenta el quinto caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

Tabla 89

Caso de uso 6 para el plan de pruebas de continuidad de acceso

Caso de uso nro. 6	
Tipo de Prueba: Fallo en un servidor Citrix App	
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.	Autor del Caso de Prueba: David Silva.
Versión del Caso de Prueba: 1.0	Fecha de Creación:
Ambiente de prueba: Test.	Fecha de Ejecución:
	Criterios de éxito y fracaso: <ul style="list-style-type: none"> · Éxito:

Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	En este caso se pondrá a prueba los equipos XAPP_0#, esto afectará a los usuarios que estén ejecutando aplicaciones en el servidor ya sean internos como externos.	Las aplicaciones pierden conexión con el servidor. Es necesario volver a iniciar aplicaciones para que inicien sesión en otro nodo Citrix App activo.	Las aplicaciones se quedan congeladas y es necesario volver a ejecutar la aplicación para que esta se abra en otro servidor. Las sesiones se abren sin problemas en otro servidor.
Decisión de Aprobación del Caso de Prueba: Aprobó: <u>x</u> Fallo:			
Nombre y firma del tester		Daniel Espinoza	
Nombre y firma del Analista de pruebas		Dandy Rosales	
Fecha de Aprobación del Caso de Prueba:			

Nota: Se presenta el sexto caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

Tabla 90

Caso de uso 7 para el plan de pruebas de continuidad de acceso

Caso de uso nro. 7			
Tipo de Prueba: Fallo en el servidor de Base de datos.			
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.		Autor del Caso de Prueba: David Silva.	
Versión del Caso de Prueba: 1.0		Fecha de Creación:	
Ambiente de prueba: Test.		Fecha de Ejecución:	
Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Criterios de éxito y fracaso: <ul style="list-style-type: none">· Éxito:· Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1		Los usuarios pueden trabajar. No se pueden	El mismo que el esperado.

	En este caso se pondrá a prueba el equipo DB01.	realizar cambios de configuración desde la consola Citrix Studio.	
Decisión de Aprobación del Caso de Prueba: Aprobó: <u> x </u> Fallo:			
Nombre y firma del tester		Daniel Espinoza	
Nombre y firma del Analista de pruebas		Dandy Rosales	
Fecha de Aprobación del Caso de Prueba:			

Nota: Se presenta el séptimo caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

Tabla 91

Caso de uso 8 para el plan de pruebas de continuidad de acceso

Caso de uso nro. 8			
Tipo de Prueba: Fallo en el repositorio de perfil de usuarios.			
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.		Autor del Caso de Prueba: David Silva.	
Versión del Caso de Prueba: 1.0		Fecha de Creación:	
Ambiente de prueba: Test.		Fecha de Ejecución:	
Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Criterios de éxito y fracaso: <ul style="list-style-type: none">· Éxito:· Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	En este caso se pondrá a prueba el repositorio \\AD\profiles\$, esto afectará a los usuarios tanto internos como externos.	Los usuarios pueden trabajar con las aplicaciones abiertas, pero fallará la sincronización del inicio y cierre de sesión y no podrán abrir aplicaciones con su perfil (abrirá un perfil temporal).	Se abre un perfil temporal en el que no tenemos nuestra configuración (aparece un mensaje de aviso). Al recuperar el recurso compartido y cerrar sesión el perfil temporal no sobrescribe al original.
Decisión de Aprobación del Caso de Prueba: Aprobó: <u>x</u> Fallo:			
Nombre y firma del tester		Daniel Espinoza	

Nombre y firma del Analista de pruebas	Dandy Rosales
Fecha de Aprobación del Caso de Prueba:	

Nota: Se presenta el octavo caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

Tabla 92

Caso de uso 9 para el plan de pruebas de continuidad de acceso

Caso de uso nro. 9			
Tipo de Prueba: Fallo de un host de infraestructura			
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.		Autor del Caso de Prueba: David Silva.	
Versión del Caso de Prueba: 1.0		Fecha de Creación:	
Ambiente de prueba: Test.		Fecha de Ejecución:	
Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Criterios de éxito y fracaso: · Éxito: · Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	En este caso se pondrá a prueba nuestros hosts de infraestructura ESXI01, ESXI02.	Las aplicaciones y VDI ya iniciadas siguen funcionando. Pueden iniciarse aplicaciones nuevas desde cualquiera de los métodos de acceso, web y cliente citrix.	El mismo que el esperado.
Decisión de Aprobación del Caso de Prueba: Aprobó: <u>x</u> Fallo:			
Nombre y firma del tester		Daniel Espinoza	
Nombre y firma del Analista de pruebas		Dandy Rosales	
Fecha de Aprobación del Caso de Prueba:			

Nota: Se presenta el noveno caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

Tabla 93

Caso de uso 10 para el plan de pruebas de continuidad de acceso

Caso de uso nro. 10	
Tipo de Prueba: Fallo del sitio en el que se aloja la infraestructura	
Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.	Autor del Caso de Prueba: David Silva.

Versión del Caso de Prueba: 1.0		Fecha de Creación:	
Ambiente de prueba: Test.		Fecha de Ejecución:	
Objetivo de prueba: Comprobar la alta disponibilidad de los diferentes elementos que componen el sistema.		Criterios de éxito y fracaso: <ul style="list-style-type: none">· Éxito:· Fracaso:	
Flujo de pasos de la Prueba:			
Nro.	Descripción del paso	Resultado esperado	Resultado obtenido
1	En este caso se desconectará el sitio en el que se encuentra la infraestructura de la red (local y externa)	El agente de conmutacion por error del Azure Site Recovery detectara la Perdida de comunicacion con el sitio local y levantarán las maquinas alojadas en Azure.	El administrador de TI deberá acceder al portal de Azure y confirmar el inicio de las VM en Azure.
Decisión de Aprobación del Caso de Prueba: Aprobó: <u>x</u> Fallo:			
Nombre y firma del tester		Daniel Espinoza	
Nombre y firma del Analista de pruebas		Dandy Rosales	
Fecha de Aprobación del Caso de Prueba:			

Nota: Se presenta el décimo caso de uso para el plan de pruebas de continuidad de acceso, elaboración propia.

5.3.1.4.5 EJECUCIÓN DEL PLAN DE PRUEBAS

A continuación, se presenta en la siguiente tabla, la ejecución del caso de uso nro. 1.

Tabla 94

Ejecución de pruebas de caso de uso nro. 1 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Acceso local, externo y móvil al portal de aplicaciones	1	Se accede al portal de aplicaciones por el enlace interno. Se verifica que no se presente ninguna advertencia de certificado inválido.	Prueba exitosa
	2	Se accede al portal de aplicaciones por el enlace externo. Se verifica que no se presente ninguna advertencia de certificado inválido.	Prueba exitosa

3	Se accede al portal de aplicaciones desde un equipo móvil. Se verifica que no se presente ninguna advertencia de certificado inválido.	Prueba exitosa
---	--	----------------

Nota: Se presenta el plan de pruebas del acceso local, externo y móvil al portal de aplicaciones, elaboración propia.

Tabla 95

Ejecución de pruebas de caso de uso nro. 2 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Fallo en un servidor de Storefront Interno)	1	Se accede al portal de aplicaciones desde el enlace interno. Se verifica que se requiere refrescar el cliente o el navegador para poder ejecutar de nuevo las aplicaciones.	Prueba exitosa

Nota: Se presenta el segundo plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

Tabla 96

Ejecución de pruebas de caso de uso nro. 3 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Fallo en un servidor Citrix Gateway)	1	Se accede al portal de aplicaciones desde el enlace externo. Se verifica que se requiere refrescar el cliente o el navegador para poder utilizar las aplicaciones ya inicializadas.	Prueba exitosa

Nota: Se presenta el tercer plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

Tabla 97

Ejecución de pruebas de caso de uso nro. 4 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Fallo en el servidor de licencias de Citrix)	1	Se accede al portal de aplicaciones desde el enlace externo como interno, los servicios no se ven afectados, se tiene un plazo de 30 días para poder restablecer dicho servicio.	Prueba exitosa

Nota: Se presenta el cuarto plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

Tabla 98

Ejecución de pruebas de caso de uso nro. 5 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Fallo en un servidor Delivery Controller)	1	Se accede al portal de aplicaciones sea interna o desde un enlace externo. Las aplicaciones ya inicializadas trabajan con normalidad.	Prueba exitosa

Nota: Se presenta el quinto plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

Tabla 99

Ejecución de pruebas de caso de uso nro. 6 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Fallo en un servidor Citrix App)	1	Se pierde conexión al servidor en el cual estaba alojado el portal de aplicaciones. Por lo que se requiere volver a iniciar sesión en cualquiera de los otros nodos Citrix App.	Prueba exitosa

Nota: Se presenta el sexto plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

Tabla 100

Ejecución de pruebas de caso de uso nro. 7 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Fallo en un servidor Base de datos)	1	Se accede al portal de aplicaciones sea interna o desde un enlace externo. Sin embargo, no se podrán registrar cambios en la consola de configuración.	Prueba exitosa

Nota: Se presenta el séptimo plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

Tabla 101

Ejecución de pruebas de caso de uso nro. 8 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Fallo en el repositorio de perfil de usuarios)	1	Se accede al portal de aplicaciones sea interna o desde un enlace externo y acceder a las aplicaciones. Sin embargo, se crearán perfiles temporales hasta que se restablezca el repositorio de usuarios.	Prueba exitosa

Nota: Se presenta el octavo plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

Tabla 102

Ejecución de pruebas de caso de uso nro. 9 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Fallo en un host de infraestructura)	1	Se accede al portal de aplicaciones sea interna o desde un enlace externo. Las aplicaciones ya inicializadas trabajan con normalidad.	Prueba exitosa

Nota: Se presenta el noveno plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

Tabla 103

Ejecución de pruebas de caso de uso nro. 10 para el O.E. 3

Prueba	Nro. de prueba	Detalle de prueba	Resultado
Continuidad de acceso a la plataforma de aplicaciones. (Pérdida de conexión del sitio local)	1	Se accede al portal de aplicaciones sea interna o desde un enlace externo. Se deben loguear de nuevo, la información que mostrará sera de acuerdo a lo que se configure en la directive de sincronización.	Prueba exitosa

Nota: Se presenta el noveno plan de pruebas para la continuidad de acceso a la plataforma de aplicaciones, elaboración propia.

5.3.1.4.6 RESULTADOS DEL PLAN DE PRUEBAS

Tabla 104

Resultados para el caso de uso nro. 1 del O.E. 3

Caso de Prueba: Acceso externo e interno a la plataforma de aplicaciones.
Objetivo de prueba: Realizar el ingreso al portal de aplicaciones mediante el uso del navegador y verificar que la página cuente con un certificado válido desde una red interna, externa y móvil.
Resultados de prueba:
1. Se accede al portal de aplicaciones desde la red interna sin ninguna notificación de certificado digital inválido. Se comprueba que el certificado digital emitido proviene de una entidad certificadora local.
2. Se accede al portal de aplicaciones desde la red externa sin ninguna notificación de certificado digital inválido. Se comprueba que el certificado digital emitido proviene de una entidad certificadora externa.
3. Se accede al portal de aplicaciones desde un dispositivo móvil sin ninguna notificación de certificado digital inválido.
4. Se comprueba que el acceso al portal de aplicaciones desde la red interna, externa y móvil está protegido con certificados digitales válidos. Por lo tanto, la comunicación de extremo a extremo se encuentra cifrada.

Nota: Se presenta los resultados del primer caso de uso para el plan de pruebas de acceso externo e interno a la plataforma de aplicaciones, elaboración propia.

Figura 64. Uso de certificado interno para acceder localmente a la plataforma de aplicaciones. Adaptado de “Acceso interno a la plataforma”, elaboración prueba.

En la figura 55, se muestra el uso de un certificado válido accediendo al portal de aplicaciones desde la red interna; dicho certificado fue emitido por una entidad certificadora local perteneciente al directorio activo de prueba que se generó para dicho diseño.

Figura 65. Uso de certificado externo para acceder desde internet a la plataforma de aplicaciones. Adaptado de “Acceso externo a la plataforma”, elaboración prueba.

En la figura 56, se muestra el uso de un certificado válido accediendo al portal de aplicaciones desde la red externa; dicho certificado fue emitido por una entidad certificadora externa, RapidSSL RSA CA.

Figura 66. Uso de certificado externo para acceder desde un dispositivo móvil a la plataforma de aplicaciones. Adaptado de “Acceso móvil a la plataforma”, elaboración prueba.

En la figura 57, se muestra el uso del protocolo de encriptación para el acceso desde un dispositivo móvil al portal de aplicaciones diseñado.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==190.81.46.107

No.	Time	Source	Destination	Protocol	Length	Info
14109	137.076608	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=112486 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14110	137.076609	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=113946 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14111	137.076669	172.16.0.17	190.81.46.107	TCP	54	57897 → 443 [ACK] Seq=1418 Ack=115406 Win=131328 Len=0
14112	137.078933	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=115406 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14113	137.078934	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=116866 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14114	137.078938	190.81.46.107	172.16.0.17	TLSv1.2	1467	Application Data
14115	137.079001	172.16.0.17	190.81.46.107	TCP	54	57897 → 443 [ACK] Seq=1418 Ack=119739 Win=131328 Len=0
14116	137.083216	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=119739 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14117	137.083217	190.81.46.107	172.16.0.17	TLSv1.2	1319	Application Data
14118	137.083308	172.16.0.17	190.81.46.107	TCP	54	57897 → 443 [ACK] Seq=1418 Ack=122464 Win=131328 Len=0
14119	137.084697	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=122464 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14120	137.084729	172.16.0.17	190.81.46.107	TCP	54	57897 → 443 [ACK] Seq=1418 Ack=123924 Win=131328 Len=0
14121	137.085071	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=123924 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14125	137.086680	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=125384 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14126	137.086681	190.81.46.107	172.16.0.17	TCP	1514	443 → 57897 [ACK] Seq=126844 Ack=1418 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
14127	137.086746	172.16.0.17	190.81.46.107	TCP	54	57897 → 443 [ACK] Seq=1418 Ack=128304 Win=131328 Len=0
14128	137.086800	190.81.46.107	172.16.0.17	TLSv1.2	1467	Application Data

Frame 14855: 1467 bytes on wire (11736 bits), 1467 bytes captured (11736 bits) on interface 0

Ethernet II, Src: Fortinet_eb:8b:64 (90:6c:ac:eb:8b:64), Dst: Pegatron_of:df:28 (7c:05:07:0f:df:28)

Internet Protocol Version 4, Src: 190.81.46.107, Dst: 172.16.0.17

Transmission Control Protocol, Src Port: 443, Dst Port: 57897, Seq: 60302, Ack: 1418, Len: 1413

[5 Reassembled TCP Segments (7253 bytes): #14049(1460), #14050(1460), #14051(1460), #14053(1460), #14055(1413)]

Transport Layer Security

TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 7248

Encrypted Application Data: d20a500d67b460462d51b6258997249aabe9a451919d354...

Figura 67. Captura de tráfico de red en la comunicación entre cliente y el portal de aplicaciones. Adaptado de “Captura análisis de red”, elaboración prueba.

En la figura 58, se muestra la captura del tráfico de red utilizando la herramienta *Wireshark*, en él se observa que la comunicación entre el cliente (dirección IP: 172.16.0.17) y el portal de aplicaciones publicado en la red externa (dirección IP: 190.81.46.107) está encriptada bajo el protocolo TLS versión 1.2.

Tabla 105

Resultados para el caso de uso nro. 2 al 9 del O.E. 3

Caso de Prueba: Continuidad de acceso a la plataforma de aplicaciones.
Objetivo de prueba: Realizar el ingreso al portal de aplicaciones mediante el uso del navegador y verificar que la página cuente con un certificado válido desde una red interna, externa y móvil.
Resultados de prueba:
1. Se accede al portal de aplicaciones desde la red interna previa refrescada de la dirección de acceso desde el navegador.
2. Se accede al portal de aplicaciones desde la red externa previa refrescada de la dirección de acceso desde el navegador.
3. El acceso al portal no sufre ninguna incidencia. Las aplicaciones abiertas no se ven afectadas
4. Las aplicaciones ya iniciadas siguen funcionando. Pueden iniciarse aplicaciones nuevas desde el portal web.
5. Las aplicaciones iniciadas en el servidor caído pierden conexión con nodo que alberga sus aplicaciones en ese momento. Es necesario volver a iniciar aplicaciones para que inicien sesión en otro nodo activo.
6. El acceso al portal no sufre ninguna incidencia. Las aplicaciones abiertas no se ven afectadas
7. Las aplicaciones ya iniciadas siguen funcionando. El inicio de sesión se realizará en un perfil temporal hasta el restablecimiento del servicio caído.
8. El acceso al portal no sufre ninguna incidencia. Las aplicaciones abiertas no se ven afectadas
9. Las aplicaciones ya iniciadas siguen funcionando. Pueden iniciarse aplicaciones nuevas desde el portal web.

Nota: Se presenta los resultados del segundo al noveno caso de uso para el plan de pruebas de continuidad de acceso a la plataforma de aplicaciones., elaboración propia.

Según los casos de prueba realizados podemos verificar que por cada recurso que tiene la plataforma posee un servicio adicional redundante, a excepción del License Server el cual nos permite hasta un tiempo de 30 días para poder levantar dicho servicio, tiempo suficiente para poder restaurarlo. Asimismo, en caso de la caída de todo el site en el cual se encuentran

todos los recursos, entraría a trabajar el agente del Azure Site Recovery para poner en modo activo los servicios replicados en la nube y poder continuar con el acceso a las aplicaciones, habrá una pérdida de información que será el tiempo de RPO configurada en la directiva de sincronización de la plataforma local con Azure.

- CONCLUSIONES

A continuación, exponemos las conclusiones, una vez terminado el diseño de la solución propuesta:

- Con la plataforma en mención se podrá reducir los gastos en infraestructura local asignadas en cada sucursal en un 75%, esto incluye optimizadores de ancho de banda, directorios activos y firewalls (según el requerimiento del área de TI) y a su vez en gastos de licenciamiento y gastos operativos que estos generan. Asimismo, los pagos en servicios dedicados de ancho de banda en sucursales no variarán, debido a la optimización que la plataforma realiza sobre el consumo para el uso de aplicaciones y que con los valores actuales que presenta, permitirá el acceso a la cantidad de usuarios mencionado en el diseño.
- Se ha podido diseñar una plataforma que brinda Alta Disponibilidad (HA) ya que los recursos en las 5 capas del diseño cuentan con al menos un servicio redundante, asimismo el RPO que otorgará la solución de Azure Site Recovery será de 4 horas y un RTO de 5 minutos que son los valores por defecto que entregan esa plataforma.
- El diseño propuesto nos asegura una escalabilidad de hasta un 37% en la cantidad de usuarios conectados en simultáneo, permitiéndonos cumplir con el requerimiento inicial de poder sostener el crecimiento del 10% anual durante tres años sin que ello ocasione sobreestimación de costos en la solución.
- El hardware requerido por la solución para cada uno de los recursos que se requiere en cada capa está en la capacidad de ser cubierta al 100% por la infraestructura actual con la que cuenta la organización, asimismo, se podrá integrar con servicios que ya estaban en producción dentro de la plataforma actual, hablamos del directorio activo, el servidor de base de datos basado SQL Server, el datastore corporativo de HP y virtualizables desde el hypervisor Vmware VSphere 6.5 que posee actualmente la cooperativa.
- Las necesidades de movilidad por parte de los usuarios serán cubiertas por el Citrix Gateway, este atenderá a los equipos estacionarios via HTML a través de una URL única y a los usuarios móviles a través del cliente ligero Citrix Workspace.
- En la parte de seguridad la solución cubrirá tres frentes: red, datos y aplicaciones sin tener que implementar y gestionar nuevas y complejas herramientas de seguridad reduciendo las tareas operativas por parte del área de TI en un 75% a comparación del modelo actual.

- El presente modelo otorgará de tres herramientas de administración y análisis tanto a nivel de red, aplicación y recursos. Para la gestión de los recursos se realizará través del Citrix Director, a nivel de red poseerá el NetScaler MAS y para la visibilidad de extremo a extremo de la experiencia del usuario el HDX Insight.
- Las aplicaciones del tipo ERP como las multimedia van a ser trabajadas con el protocolo de visualización H.264 selectivo con pantalla adaptativa, el uso del códec MDRLE, el método de criptografía de clave pública del tipo ECC y a una tasa de 16 bits para poder trabajar de manera fluida en sucursales, según los datos de ancho de banda contratados y latencia que posea.
- Se requieren que el personal de TI posea conocimientos técnicos avanzados en soluciones Citrix, sistemas operativos, virtualización y redes para poder interactuar con la plataforma, ya que a pesar de que la administración y supervisión es intuitiva, se requiere garantizar que los problemas de producción se registren, escalen y resuelvan de manera oportuna.

- RECOMENDACIONES

- Se podría optar por el uso de un proveedor de identidades (IdP) de terceros (como Azure Active Directory, Google, etc.), en lugar de mantener un solo punto de autenticación local, el cual ayudará en mantener la disponibilidad de este recurso. Asimismo, permitirá dar acceso a usuarios que no pertenezcan a nuestra organización, y ya no solicitar una cuenta en nuestro directorio activo.
- Se propone crear un entorno de producción, un entorno de prueba y otro de preproducción. Al disponer de entornos independientes favorecería el poder llevar a cabo las pruebas necesarias.
- Conforme vaya creciendo la cantidad de usuarios y aplicaciones a distribuir, se puede ir delegando servicios de la plataforma de Citrix a la nube, ya sea a su nube propietaria o a los de Azure o AWS, quedando como resultado un escenario híbrido que pueda ofrecernos mejores niveles de disponibilidad y dependiendo del escenario, ahorros en CAPEX y OPEX.
- A mediano plazo poseer una plataforma con autenticación de dos factores para todos los usuarios, con ello otorgar una barrera para la suplantación de usuarios, incluso si la contraseña principal haya sido vulnerada. Este principio consiste en solicitar dos formas diferentes de autenticación: la primera, relacionada con algo que el usuario conozca; y la segunda, relacionada con algo que el usuario utilice, como un token físico.
- Para organizaciones que requieran mayor protección para el acceso a sus redes internas, se puede optar por una implementación de Citrix Gateway en una DMZ de doble salto. Para esta se requiere de tres cortafuegos las cuales dividen la DMZ en dos etapas proporcionando una capa adicional de seguridad a la red interna.
- Habilitar la funcionalidad SmartAccess para aplicaciones HDX, esta funcionalidad permite controlar el acceso a aplicaciones HDX mediante la creación de políticas las cuales poseen filtros que exigen el cumplimiento de propiedades por parte del dispositivo, de no ser cumplirlas de forma automatizada se marca al dispositivo como no conforme y se les deniega el acceso a las aplicaciones.
- Alinearse con normativas como la versión 3.0 de PCI DSS, brindando estándares seguros de tarjetas de pago.

- **BIBLIOGRAFÍA**

42Gears (24 de abril de 2017) ¿Cuál es la diferencia entre MDM, EMM y UEM? [Entrada en blog]. Recuperado de <https://www.42gears.com/blog/difference-between-mdm-emm-uem/> [Consulta: 18 de diciembre de 2019].

Álvarez, J. (2017). *Solución IT Para Virtualización De Puestos De Trabajo Con Citrix* (Tesis de fin de carrera, Universidad Politécnica De Madrid, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, Madrid, España). Recuperado de http://oa.upm.es/48721/1/PFC_JAIME_ALVAREZ_NAVARRO_v1.pdf [Consulta: 11 de octubre de 2019].

Cano, J. J. (s.f.). *Métricas en Seguridad Informática: Una revisión académica* Recuperado de <https://acis.org.co/portal/sites/all/themes/argo/assets/img/Pagina/07-MetricasSeguridadInformaticaUnaRevisionAcademica.pdf> [Consulta: 12 de septiembre de 2019].

Citrix Systems, Inc. (2016) *Citrix VDI Handbook and Best Practices*. Recuperado de <https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/downloads/handbook-715-ltsr.pdf> [Consulta: 15 de septiembre de 2019].

Citrix. (2019a). *Licensing 11.16.3*. Recuperado de <https://docs.citrix.com/en-us/licensing/current-release.html> [Consulta: 10 de enero de 2020].

Citrix. (2019b). *Configuraciones de directiva de Presentación visual*. Recuperado de <https://docs.citrix.com/es-es/citrix-virtual-apps-desktops/policies/reference/ica-policy-settings/visual-display-policy-settings.html> [Consulta: 19 de febrero de 2020].

Citrix. (2020). *Citrix Virtual Apps And Desktops: Información técnica general*. Recuperado de <https://docs.citrix.com/es-es/provisioning/current-release/architecture.html> [Consulta: 13 de enero de 2020].

- Citrix. (2020a). *Capa de usuarios de la metodología de diseño*. Recuperado de <https://docs.citrix.com/es-es/xenapp-and-xendesktop/7-15-ltsr/citrix-vdi-best-practices/design/design-userlayer1.html> [Consulta: 13 de enero de 2020].
- Citrix. (2020b). *Capa de acceso de la metodología de diseño*. Recuperado de <https://docs.citrix.com/es-es/xenapp-and-xendesktop/7-15-ltsr/citrix-vdi-best-practices/design/design-userlayer2.html> [Consulta: 14 de enero de 2020].
- Citrix. (2020c). *Capa de recursos de la metodología de diseño*. Recuperado de <https://docs.citrix.com/es-es/xenapp-and-xendesktop/7-15-ltsr/citrix-vdi-best-practices/design/design-userlayer3.html> [Consulta: 15 de enero de 2020].
- Citrix. (2020d). *Capa de control de la metodología de diseño*. Recuperado de <https://docs.citrix.com/es-es/xenapp-and-xendesktop/7-15-ltsr/citrix-vdi-best-practices/design/design-userlayer4.html> [Consulta: 16 de enero de 2020].
- Citrix. (2020e). *Capa de hardware de la metodología de diseño*. Recuperado de <https://docs.citrix.com/es-es/xenapp-and-xendesktop/7-15-ltsr/citrix-vdi-best-practices/design/design-userlayer5.html> [Consulta: 17 de enero de 2020].
- Citrix Inc. (2019). *Citrix Virtual Apps and Desktops 7 1909*. Recuperado de <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/downloads/citrix-virtual-apps-and-desktops-1909.pdf> [Consulta: 15 de diciembre de 2019].
- Citrix Systems, Inc. (2016) *Las mejores prácticas para la seguridad empresarial*. Recuperado de <https://www.citrix.com/content/dam/citrix/es-es/documents/products-solutions/best-practices-for-enterprise-security.pdf> [Consulta: 11 de octubre de 2019].
- Citrix Systems, Inc. (2016a) *Lossless Compression: Lowering the Cost of Pixel Perfection*. Recuperado de <https://support.citrix.com/article/CTX218314> [Consulta: 20 de febrero de 2020].

Citrix Systems, Inc. (2016b) *How Do I Setup ECC on NetScaler?*. Recuperado de <https://support.citrix.com/article/CTX205289> [Consulta: 20 de febrero de 2020].

Citrix Systems, Inc. (2017) *Comprehensive Citrix HDX visibility powered by NetScaler Management and Analytics System*. Recuperado de https://www.citrix.com/content/dam/citrix/en_us/documents/solution-brief/comprehensive-citrix-hdx-visibility-powered-by-netscaler-mas.pdf [Consulta: 03 de enero de 2020].

Citrix Systems, Inc. (2012). *High Availability for Citrix XenDesktop and XenApp*. Recuperado de https://support.citrix.com/content/dam/supportWS/kA460000000CnsDCAS/HA_for_XD_and_XA_Planning_Guide.pdf [Consulta: 15 de septiembre de 2019].

Citrix Systems, Inc. (2017). *Garantice la entrega segura y fiable de espacios de trabajo digitales*. Recuperado de https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/ensure-the-secure-reliable-delivery-of-digital-workspaces-to-any-user-over-any-network-es.pdf [Consulta: 11 de septiembre de 2019].

Dawson, M. (2018). Red Hat Global Customer Tech Outlook 2019: Automation, cloud, & security lead funding priorities. Recuperado de <https://www.redhat.com/en/blog/red-hat-global-customer-tech-outlook-2019-automation-cloud-security-lead-funding-priorities> [Consulta: 02 de octubre de 2019].

Docker. (2019). *What is containerd?* Recuperado de <https://www.docker.com/blog/what-is-containerd-runtime/> [Consulta: 25 de septiembre de 2019].

Gartner. (2019). *Magic Quadrant for Unified Endpoint Management Tools*. Recuperado de <https://www.gartner.com/doc/reprints?id=1-1ODR3EC0&ct=190812&st=sb> [Consulta: 13 de diciembre de 2019].

González, J. (2 de marzo de 2012) ¿Qué es NUMA? [Entrada en blog]. Recuperado de <https://www.josemariagonzalez.es/manuales-virtualizacion/que-es-numa.html> [Consulta: 1 de diciembre de 2019].

Gonzalez, J. M. (23 de febrero de 2015). Optimización Citrix CloudBridge en Citrix XenApp y XenDesktop (1 de 2) [Entrada en blog] Recuperado de <https://www.josemariagonzalez.es/citrix/optimizacion-citrix-cloudbridge-en-citrix-xenapp-y-xendesktop-1-de-2.html> [Consulta: 15 de octubre de 2019].

Hess, K, *UEM for dummies*. Recuperado de <https://de.cloud.im/Content/docs/IBM-MaaS-UEM-for-Dummies.pdf> [Consulta: 01 de febrero de 2020].

Kibet. J. (16 de diciembre de 2019) Docker vs CRI-O vs Containerd [Entrada en blog]. Recuperado de <https://computingforgeeks.com/docker-vs-cri-o-vs-containerd/> [Consulta: 25 de enero de 2020].

Marañón, J. M. (2013). *Implementación de una plataforma de servidores de aplicaciones* (Tesis de fin de carrera, Universidad Autónoma de Barcelona, Escuela de Ingeniería de Sistemas, Barcelona, España). Recuperado de https://ddd.uab.cat/pub/trerecpro/2014/hdl_2072_231945/MaranonMartinJoseMaria-ETISa2012-13.pdf [Consulta: 10 de octubre de 2019].

Microsoft. (2019). *What is MSIX?* Recuperado de <https://docs.microsoft.com/en-us/windows/msix/overview> [Consulta: 25 de septiembre de 2019].

Microsoft Azure. (2019). *Arquitectura de recuperación ante desastres de VMware a Azure*. Recuperado de <https://docs.microsoft.com/es-es/azure/site-recovery/vmware-azure-architecture> [Consulta: 31 de enero de 2020].

National Institute of Standards and Technology (NIST) (2016). *Recommendation for Key Management Part 1: General*. Recuperado de <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf> [Consulta: 20 de febrero de 2020].

Puricica, C. A. (2018). Desmitificando los Objetivos de Recuperación. Recuperado de <https://www.veeam.com/blog/es-lat/rto-rpo-definitions-values-common-practice.html> [Consulta: 22 de noviembre de 2019].

Ranchal, J. (2 de febrero de 2019) MSIX, el futuro de los instaladores de Windows [Entrada en blog]. Recuperado de <https://www.muycomputer.com/2019/02/12/msix/> [Consulta: 25 de septiembre de 2019].

Sandbu, M. (2017) The Citrix Administrator's Technical Guide to Understanding and Troubleshooting Citrix ICA/HDX Recuperado de <https://goliathtechnologies.com/resources/guides/citrix-ica-hdx/> [Consulta: 22 de diciembre de 2019].

Samuel, J. (2018). How to extend your on premises XenApp XenDesktop environment to Citrix Cloud XA XD Service and Microsoft Azure. Recuperado de <https://www.jasonsamuel.com/2018/01/23/how-to-extend-your-on-premises-xenapp-xendesktop-environment-to-citrix-cloud-xa-xd-service-and-microsoft-azure/> [Consulta: 15 de noviembre de 2019].

Solutions, I. (2019). Citrix Xenapp. Recuperado de <https://inbest.solutions/xen-app/> [Consulta: 05 de diciembre de 2019].

Vásquez, C. (2018). *Plan Metodológico Comparativo entre Invertir en un Data Center vs Infraestructura como Servicio Cloud Computing*. Quito: Universidad Católica de Ecuador. (Tesis de maestría en redes de comunicaciones, Pontificia Universidad Católica del Ecuador, Facultad de Ingeniería, Quito, Ecuador). Recuperado de <http://repositorio.puce.edu.ec/bitstream/handle/22000/15077/Tesis%20Carlos%20Alberto%20V%c3%a1squez%20Benitez.pdf?sequence=1&isAllowed=y> [Consulta: 09 de septiembre de 2019].

VMware, I. (2011). *Citrix XenApp on VMware Best Practices Guide*. Recuperado de <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmware-citrix-xenapp-best-practices-en.pdf> [Consulta: 25 de septiembre de 2019].

Vmware Inc. (2017). *Vmware Horizon 7*. Recuperado de <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/horizon/vmware-horizon-7-datasheet.pdf> [Consulta: 19 de diciembre de 2020].

- **GLOSARIO**

Azure Storage: Solución de almacenamiento en la nube de Microsoft para escenarios modernos de almacenamiento de datos.

Azure ExpressRoute: Servicio que permite crear conexiones privadas entre los centros de datos de Azure y la infraestructura de un entorno local o de colubicación

Backup: Es una copia de los datos originales fuera de la infraestructura que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Bring Your Own Device (BYOD): es una tendencia cada vez más generalizada en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

Configuration Manager: Centro de administración central de Azure

DaaS: Es un servicio en la nube en el cual el back-end de una infraestructura de escritorio virtual (VDI) es hospedado por un proveedor de servicios de nube.

Endpoint: Computadoras de escritorio, Laptops, Tablet, Teléfonos inteligentes y cualquier otro dispositivo utilizado por un empleado o visitante que accese los recursos de la red empresarial.

Firewall: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Infraestructura TI: Hace referencia a un conglomerado de servicios, dispositivos físicos y aplicaciones de software que forman el sostén de los sistemas, funcionamiento de tareas y comunicaciones en cualquier compañía.

ICA RTT: Es el tiempo transcurrido desde que el usuario presiona una tecla hasta que la respuesta se muestra nuevamente en el punto final.

Mobility Service: Servicio de Azure Site Recovery que permite la replicación de una VM a Azure.

On Premise: La empresa instala la solución dentro de sus servidores e infraestructuras

PassThrough: Modo de autenticación que permite validarse en un dominio y usar las aplicaciones y los escritorios entregados por ese dominio sin necesidad de volver a autenticarse para cada aplicación o escritorio.

Recovery Services: Bóvedas de los servicios de recuperación para almacenar datos de copia de seguridad para varios servicios de Azure,

Site Recovery: Solución nativa de recuperación ante desastres como servicio (DRaaS)

SSL: Son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

Thin Client: Es una computadora cliente o un software de cliente en una arquitectura de red cliente-servidor

- SIGLARIO

ADMX: Administrative Templates
ASR: Azure Site Recovery
BYOD: Bring Your Own Device.
CAPEX: Capital Expenditure
CPU: Central Processing Unit.
DaaS: Desktop as a Service.
DLL: Dynamic-Link Library
ECC: Elliptic Curve Cryptography
EPA: Endpoint Analysis
EMM: Enterprise Mobility Management
FENACREP: Federación de Cooperativas de Ahorro y Crédito
GPO: Group Policy Object
IPSEC: Internet Protocol security
LHC: Local Host Cache
MDM: Mobile Device Management
MDRLE: New Lossless Compression Codec
OPEX: Operacional Expenditure
OU: Organizational Unit
QOS: Quality of Service.
POS: Terminal punto de venta.
RAM: Random Access Memory
RLE: Run-length encoding
RPO: Recovery Point Objective
RTO: Recovery Time Objective
TI: Tecnologías de la información.
TLS: Transport Layer Security
VDI: Virtual Desktop Infrastructure.
VM: Virtual Machine
VPN: Virtual Private Network.
IDP: Proveedor de identidades.
UTM: Unified Threat Management
WAN: Wide Area Network

- **ANEXOS**

Anexo 01: Poster de las partes de la Gestión Unificada de punto final.

Fuente: 42Gears (2019)

Anexo 02: Poster de arquitectura de componentes Citrix XenApp y XenDesktop

Fuente: Citrix Blog (2018)

Anexo 03: Poster de riesgos y puntos débiles de la UEM.

Cuatro motivos para adoptar la UEM hoy mismo
PUNTOS DÉBILES	RIESGOS	CÓMO AYUDA LA UEM
1 Herramientas heredadas que no respaldan adecuadamente a los usuarios remotos ni a las fuerzas de trabajo móvil	Dispositivos fuera de la red que no pueden administrarse con facilidad, lo que ocasiona riesgos de seguridad y costos altos de TI	Mantenimiento de todos los terminales (ya sea los de la oficina o los remotos/en el campo) actualizados y en cumplimiento con las políticas corporativas con una intervención mínima del Departamento de TI
2 Administración y herramientas aisladas en dispositivos móviles, de escritorio y duraderos/ diseñados para fines específicos	Administración inconexa que genera costos más altos y una seguridad incoherente en todas las plataformas	Un conjunto unificado de herramientas para administrar con coherencia cualquier terminal o aplicación: móviles y de nube, de escritorio o incluso Internet de las cosas (IoT)
3 Falta de visibilidad en terminales, aplicaciones y usuarios	Administración reactiva y seguridad deficiente	Aprovechamiento de capacidades modernas de administración móvil para operaciones en tiempo real y estados de cumplimiento, independientemente de la ubicación de los dispositivos
4 Dispositivos bloqueados con autoservicio escaso o sin autoservicio	Experiencia de usuario deficiente y costos altos de soporte de TI	Experiencia de usuario coherente en diferentes terminales; admisión de procesos de autoservicio

Fuente: Vmware Blog (2018)

Anexo 04: Evolucion de las ecnologia para dispositivos móviles.

Fuente: MobileWorxs (2015)