Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Escuela Profesional de Ingeniería de Sistemas

La emergencia sanitaria y la continuidad operativa en el sector regulatorio nacional: implementación de una plataforma de trabajo remoto en el marco de la pandemia por COVID-19

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Ignacio KOIKE JARA ALMONTE

ASESOR

Rosa MENÉNDEZ MUERAS

Lima, Perú

2021

Referencia bibliográfica

Koike, I. (2021). *La emergencia sanitaria y la continuidad operativa en el sector regulatorio nacional: implementación de una plataforma de trabajo remoto en el marco de la pandemia por COVID-19*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	IGNACIO KOIKE JARA ALMONTE
Tipo de documento de identidad	DNI
Número de documento de identidad	46472877
URL de ORCID	https://orcid.org/0000-0002-6004-6372
Datos de asesor	
Nombres y apellidos	ROSA MENÉNDEZ MUERAS
Tipo de documento de identidad	DNI
Número de documento de identidad	10246770
URL de ORCID	https://orcid.org/0000-0003-2403-7679
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	JOHN LEDGARD TRUJILLO TREJO
Tipo de documento	DNI
Número de documento de identidad	06187585
Miembro del jurado 1	
Nombres y apellidos	JAVIER CABRERA DIAZ
Tipo de documento	DNI
Número de documento de identidad	08692591
Datos de investigación	
Línea de investigación	No aplica
Grupo de investigación	No aplica
Agencia de financiamiento	Propio

Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Cercado de Lima Jr. Carlos Amezaga No. 375 Universidad Nacional Mayor de San Marcos Latitud: -12.0564232 Longitud: -77.0843327
Año o rango de años en que se realizó la investigación	2021
URL de disciplinas OCDE	2.02.04 - Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 20:00 horas del día 28 de diciembre del año 2021, se reunieron virtualmente los docentes designados como Miembros del Jurado del Trabajo de Suficiencia Profesional, presidido por el Lic. Trujillo Trejo John Ledgard (Presidente), Mg. Cabrera Diaz Javier (Miembro) y la Mg. Menéndez Mueras Rosa (Miembro Asesor), usando la plataforma Meet (https://meet.google.com/gfv-qdyi-szt), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: ***"LA EMERGENCIA SANITARIA Y LA CONTINUIDAD OPERATIVA EN EL SECTOR REGULATORIO NACIONAL: IMPLEMENTACIÓN DE UNA PLATAFORMA DE TRABAJO REMOTO EN EL MARCO DE LA PANDEMIA POR COVID-19",*** *por el Bachiller* ***Koike Jara Almonte Ignacio;*** *para obtener el Título Profesional de Ingeniero de Sistemas.*

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de ***19 DIECINUEVE.***

A continuación el Presidente de Jurados el Lic. Trujillo Trejo John Ledgard, declara al Bachiller ***Ingeniero de Sistemas****.*

Siendo las 20:55 horas, se levantó la sesión.

Presidente
Lic. Trujillo Trejo John Ledgard

Miembro
Mg. Cabrera Diaz Javier

Miembro Asesor
Mg. Menéndez Mueras Rosa

DEDICATORIA

A mi madre, por su paciencia infinita.

A Tyler, estés donde estés.

AGRADECIMIENTOS

Agradezco, ante todo, a mi familia por todo su apoyo durante mis años de vida universitaria.

Agradezco a los superiores que he tenido a lo largo de mi vida profesional, por su confianza en mi talento y habilidades. Sin su apoyo, el proyecto que inspiró este trabajo no hubiese sido posible.

Agradezco a mi asesora, por su apoyo a pesar de las complicaciones y contratiempos y, sobre todo, por confiar en la calidad de mi proyecto y ayudarme a materializarlo en el presente trabajo.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMATICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

LA EMERGENCIA SANITARIA Y LA CONTINUIDAD OPERATIVA EN EL SECTOR REGULATORIO NACIONAL: IMPLEMENTACIÓN DE UNA PLATAFORMA DE TRABAJO REMOTO EN EL MARCO DE LA PANDEMIA POR COVID-19

Autor: Koike Jara Almonte, Ignacio

Asesor: Mg. Menéndez Mueras, Rosa

Título: Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniero de Sistemas

Fecha: **2021**

RESUMEN

El presente trabajo de suficiencia profesional aborda la implementación, y todas las actividades previas y posteriores, de una plataforma que permitiese a los colaboradores del Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL continuar con sus labores desde sus hogares en el contexto de la emergencia sanitaria por COVID-19.

El proyecto se basó en la arquitectura de Servicios de Escritorio Remoto del fabricante/desarrollador Microsoft y tuvo como producto final una plataforma de trabajo remoto que permitió al organismo regulador de telecomunicaciones retomar operaciones en un breve plazo de tiempo luego de la declaratoria de estado de emergencia nacional, pudiendo así continuar con su labor de servir al ciudadano.

Palabras Claves*: Infraestructura Tecnológica, Trabajo Remoto.*

NATIONAL UNIVERSITY OF SAN MARCOS

FACULTY OF SYSTEMS ENGINEERING AND INFORMATICS

PROFESSIONAL SCHOOL OF SYSTEMS ENGINEERING

HEALTH EMERGENCY AND OPERATIONAL CONTINUITY IN THE NATIONAL REGULATORY SECTOR: IMPLEMENTATION OF A REMOTE WORK PLATFORM IN THE CONTEXT OF THE PANDEMIC BY COVID-19

Author: Koike Jara Almonte, Ignacio

Advisor: Mg. Menéndez Mueras, Rosa

Title: Professional Sufficiency Work Report for opt for the Professional title of System Engineer

Date: **2021**

ABSTRACT

The present work of professional sufficiency addresses the implementation, and all previous and subsequent activities, of a platform that allowed the employees of the Supervisory Agency for Private Investment in Telecommunications (OSIPTEL by its Spanish Acronym) to continue their work from their homes in the context of the COVID-19 health emergency.

The project was based on Microsoft's Remote Desktop Services architecture and its final product was a remote work platform that allowed the telecommunications regulatory agency to resume operations in a short period of time after the declaration of a state of national emergency, thus being able to continue with its work of serving citizens.

Key words: Technological Infrastructure, Remote Work.

ÍNDICE GENERAL

DEDICATORIA IV
AGRADECIMIENTOS V
RESUMEN VI
ABSTRACT VII
ÍNDICE GENERAL VIII
ÍNDICE DE TABLAS X
ÍNDICE DE FIGURAS XI
INTRODUCCIÓN 1
CAPÍTULO I TRAYECTORIA PROFESIONAL 2
1.1. Presentación profesional 2
1.2. Experiencia profesional 2
1.2.1 Organismo Supervisor de Inversión Privada en Telecomunicaciones 2
CAPÍTULO II CONTEXTO EN EL QUE SE DESARROLLÓ LA EXPERIENCIA 4
2.1. Empresa – actividad que realiza 4
2.2. Misión 6
2.3. Visión 6
2.4. Organización de la empresa 6
2.5. Área, cargo y funciones desempeñadas 8
2.6. Experiencia profesional realizada en la organización 9
CAPÍTULO III ACTIVIDADES DESARROLLADAS 11
3.1. Situación Problemática 11
3.1.1 Definición del problema 11
3.2. Solución 13
3.2.1 Objetivos 14
3.2.1.1 Objetivo General 14
3.2.1.2 Objetivos Específicos 14
3.2.2 Alcance 14
3.2.3 Etapas y metodología 15
3.2.4 Fundamentos utilizados 16
3.2.4.1 Servidor de red 16

3.2.5 Implementación de las áreas de procesos y sus buenas prácticas 23
3.2.5.1 Fase 1: Planeación 23
3.2.5.2 Fase 2: Análisis 26
3.2.5.3 Fase 3: Diseño 33
3.2.5.4 Fase 4: Construcción 39
3.2.5.5 Fase 5: Seguimiento y Optimización 61
CAPÍTULO IV REFLEXIÓN CRÍTICA DE LA EXPERIENCIA 63
CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES 64
5.1 Conclusiones 64
5.2 Recomendaciones 64
Bibliografía 66

ÍNDICE DE TABLAS

No se encuentran elementos de tabla de ilustraciones.

ÍNDICE DE FIGURAS

Figura 1: Organigrama del OSIPTEL 7
Figura 2: Organigrama Interno de la OTI 8
Figura 3: Diagrama de conexión y operación de la solución 33
Figura 4: Diagrama de arquitectura de la solución 34
Figura 5: Diagrama de arquitectura lógico 38
Figura 6: Panel de Administración del Servidor 41
Figura 7: Asistente de Configuración - Pantalla 1 41
Figura 8: Asistente de Configuración - Pantalla 2 41
Figura 9: Asistente de Configuración - Pantalla 3 42
Figura 10: Asistente de Configuración - Pantalla 4 42
Figura 11: Asistente de Configuración - Pantalla 5 43
Figura 12: Asistente de Configuración - Pantalla 6 43
Figura 13: Asistente de Configuración - Pantalla 7 44
Figura 14: Asistente de Configuración - Pantalla 8 44
Figura 15: Asistente de Configuración - Pantalla 9 45
Figura 16: Asistente de Configuración - Pantalla 10 45
Figura 17: Componentes RDS configurados 46
Figura 18: Creación de una colección 46
Figura 19: Asistente de Configuración de Colecciones - Pantalla 1 47
Figura 20: Asistente de Configuración de Colecciones - Pantalla 2 47
Figura 21: Asistente de Configuración de Colecciones - Pantalla 3 48
Figura 22: Asistente de Configuración de Colecciones - Pantalla 4 48
Figura 23: Asistente de Configuración de Colecciones - Pantalla 5 49
Figura 24: Asistente de Configuración de Colecciones - Pantalla 6 49
Figura 25: Asistente de Configuración de Colecciones - Pantalla 7 50
Figura 26: Componentes RDS configurados 50
Figura 27: Propiedades de la Colección 51
Figura 28: Propiedades de la colección - Pantalla 1 51
Figura 29: Propiedades de la colección - Pantalla 2 52
Figura 30: Propiedades de la colección - Pantalla 3 53
Figura 31: Propiedades de la colección - Pantalla 4 54
Figura 32: Propiedades de la colección - Pantalla 5 55
Figura 33: Propiedades de la colección - Pantalla 6 56
Figura 34: Propiedades de la colección - Pantalla 7 57
Figura 35: Componentes RDS configurados 58
Figura 36: Asistente de Configuración de Licenciamiento - Pantalla 1 58
Figura 37: Asistente de Configuración de Licenciamiento - Pantalla 2 59
Figura 38: Componentes RDS configurados 59
Figura 39: Asistente de Configuración de Puerta de Enlace - Pantalla 1 60
Figura 40: Asistente de Configuración de Puerta de Enlace - Pantalla 2 60
Figura 41: Asistente de Configuración de Puerta de Enlace - Pantalla 3 61

INTRODUCCIÓN

El presente trabajo de suficiencia profesional describe la formulación, análisis, diseño, implementación y optimización de una plataforma de trabajo remoto basada en la arquitectura de la solución *Microsoft Remote Desktop Services*. Este trabajo se divide en cinco capítulos:

En el CAPÍTULO I, se describe la trayectoria profesional del autor y las funciones que desempeñó en cada organización en la que laboró.

En el CAPÍTULO II, se realiza una breve descripción de la empresa donde el autor trabajó durante la implementación del proyecto descrito en el presente.

En el CAPÍTULO III, se detalla el problema principal, la solución, los objetivos, el alcance de la solución, la metodología aplicada, los fundamentos utilizados y la implementación de la solución.

En el CAPÍTULO IV, se indica la reflexión crítica de la experiencia obtenida luego de la ejecución del proyecto.

En el CAPÍTULO V, se listan las conclusiones y recomendaciones del trabajo de suficiencia.

CAPÍTULO I
TRAYECTORIA PROFESIONAL

1.1. Presentación profesional

El autor del presente trabajo es bachiller en Ingeniería de Sistemas de la Universidad Nacional Mayor de San Marcos con amplia experiencia en Infraestructura Tecnológica, Redes de Datos y Seguridad Digital. Actualmente se desempeña como *Analista de seguridad y servicios de infraestructura tecnológica* en el *Organismo Supervisor de Inversión Privada en Telecomunicaciones* – OSIPTEL.

En cada proyecto en el que ha participado ha propuesto ideas innovadoras y soluciones factibles para la organización, siempre demostrando su capacidad de trabajo en equipo y con personas a su cargo, en la propuesta, análisis, diseño e implementación de soluciones tecnológicas.

1.2. Experiencia profesional

A continuación, se detalla la experiencia profesional del autor del presente trabajo:

1.2.1 Organismo Supervisor de Inversión Privada en Telecomunicaciones

Noviembre, 2019 – Actualidad

Cargo: Analista de seguridad y servicios de infraestructura tecnológica

Funciones:

- Establecer mecanismos apropiados para la operación de servicios de la plataforma de la infraestructura tecnológica, así como la seguridad de esta, con el objetivo de lograr un óptimo desempeño de los servicios de tecnologías de la información que son soportados por la mencionada plataforma y dar cumplimiento al marco normativo vigente.

Mayo 2018 – octubre 2019

Cargo: Asistente de Infraestructura Tecnológica

Funciones:

- Participación en labores como la elaboración de términos de referencia y especificaciones técnicas, la gestión de servicios tercerizados, el monitoreo y operación del centro de datos institucional, la gestión de la red de datos institucional, el seguimiento al cumplimiento de los controles de la Norma ISO/IEC 27001:2013 entre otras.

Septiembre 2017 – mayo 2018

Cargo: Practicante Profesional en la Jefatura de Infraestructura Tecnológica

Funciones:

- Apoyo en operaciones de la Jefatura de Infraestructura Tecnológica tales como el monitoreo del centro de datos institucional, la gestión de la red de datos a nivel nacional, el seguimiento a las contrataciones y la gestión de servidores Linux/Windows entre otras actividades.

CAPÍTULO II
CONTEXTO EN EL QUE SE DESARROLLÓ LA EXPERIENCIA

2.1. Empresa – actividad que realiza

El Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL (Portal Web Institucional del OSIPTEL, 2021), es un organismo público especializado, regulador y descentralizado adscrito a la Presidencia del Consejo de ministros, que cuenta con autonomía técnica, administrativa, económica y financiera.

Fue creado el 11 de julio de 1991 mediante Decreto Legislativo Nº 702, e inició sus actividades con la instalación de su primer Consejo Directivo el 26 de enero de 1994. Su Reglamento General (Decreto Supremo Nº 008-2001-PCM) fue publicado en el diario El Peruano el 2 de febrero de 2001.

El Organismo Supervisor cuenta con 6 funciones:

- Función Reguladora

Puede fijar las tarifas de los servicios públicos de telecomunicaciones, establecer sistemas tarifarios en sus diferentes modalidades y dictar las disposiciones que sean necesarias para esto. Esta facultad se ejerce previa evaluación de las condiciones del mercado que justifiquen su intervención, garantizando la calidad y eficiencia económica en la prestación de los servicios públicos de telecomunicaciones.

- Función Normativa

Dicta los reglamentos o normas que regulan los procedimientos a su cargo, otras de carácter general y mandatos u otras normas de carácter particular referidas a intereses, obligaciones o derechos de las entidades o actividades supervisadas o de sus usuarios. Adicionalmente, tiene la facultad de tipificar las infracciones por incumplimiento de obligaciones establecidas por normas legales, normas técnicas y aquellas derivadas de los contratos de concesión, así como por

el incumplimiento de las disposiciones reguladora y normativa. Esto comprende la potestad de aprobar su propia escala de sanciones.

- Función Fiscalizadora Y Sancionadora

Califica infracciones e impone medidas correctivas según corresponda a las empresas operadoras y demás empresas o personas que realizan actividades sujetas a su competencia, por el incumplimiento de obligaciones derivadas de normas legales o técnicas, así como de las obligaciones contraídas por los concesionarios en los respectivos contratos de concesión.

- Función De Solución De Controversias

Debe conocer y resolver toda controversia que afecte o pueda afectar el mercado de los servicios públicos de telecomunicaciones, aunque solo una de las partes tenga la condición de empresa operadora. Concilia y resuelve, en vía administrativa, los intereses entre entidades o empresas bajo su ámbito de competencia, entre entidades o empresas y sus usuarios, así como los conflictos y controversias entre estos. Asimismo, resuelve controversias en la vía arbitral cuando las partes hayan acordado someter sus discrepancias a arbitraje administrativo.

- Función De Solución De Reclamos

Resuelve los reclamos de los usuarios en segunda instancia, siempre que estas se encuentren en las materias señaladas en la normativa correspondiente.

- Función Supervisora

Verifica el cumplimiento de las obligaciones legales por parte de las empresas operadoras y demás empresas o personas que realizan actividades sujetas a su competencia; así como el cumplimiento de cualquier mandato, resolución o norma emitida por el Osiptel.

2.2. Misión

Promover la competencia del mercado de telecomunicaciones, calidad de los servicios de telecomunicaciones y el empoderamiento del usuario; de manera continua, eficiente y oportuna.

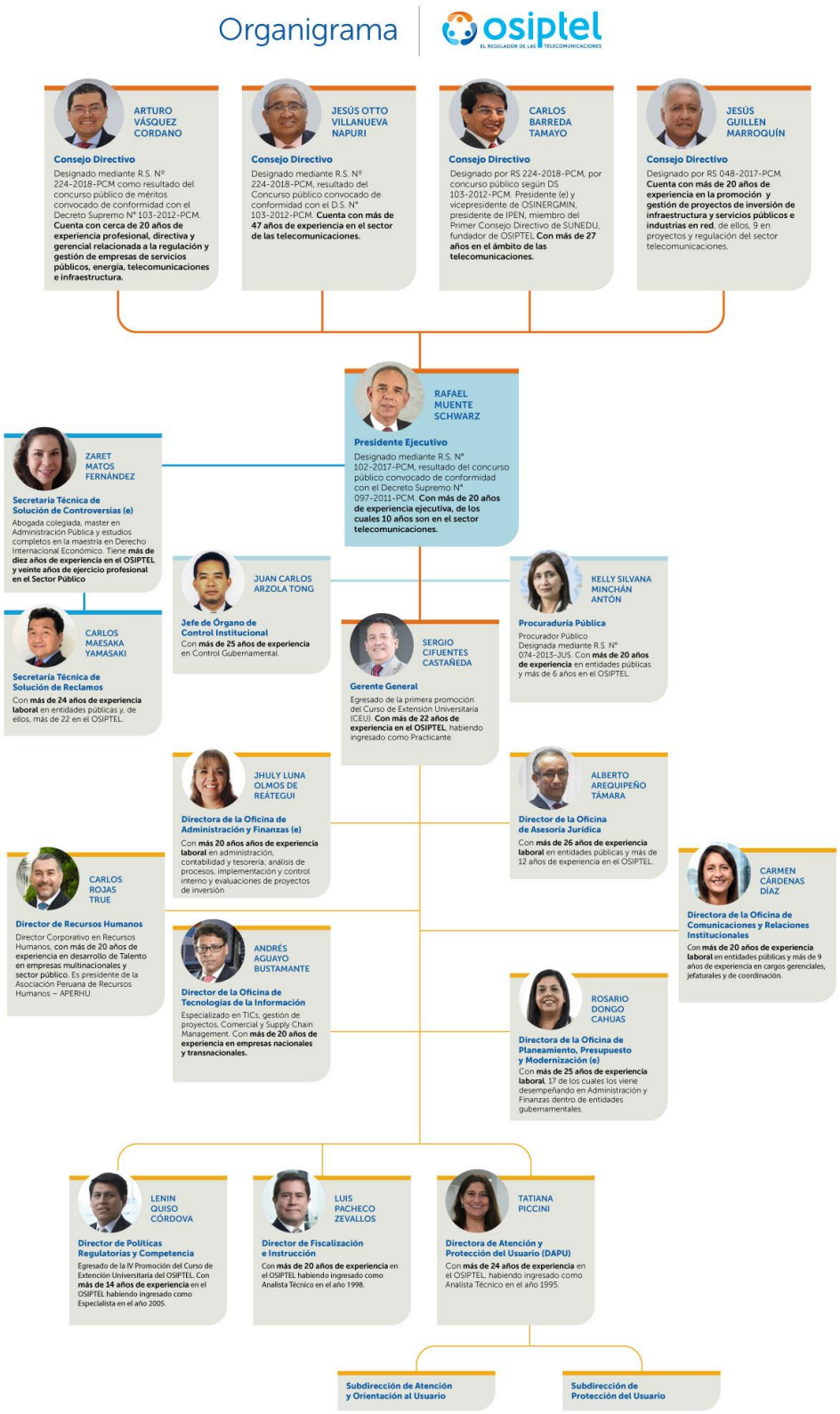
2.3. Visión

Lograr que los servicios de telecomunicaciones sean accesibles y de calidad, en un marco de competencia efectiva, y ser reconocidos por la población como una institución autónoma, técnica e innovadora.

2.4. Organización de la empresa

En la imagen a continuación se puede apreciar el organigrama oficial del Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL, las unidades orgánicas que lo componen y los miembros de la alta dirección a cargo de cada una de ellas.

Figura 1: Organigrama del OSIPTEL

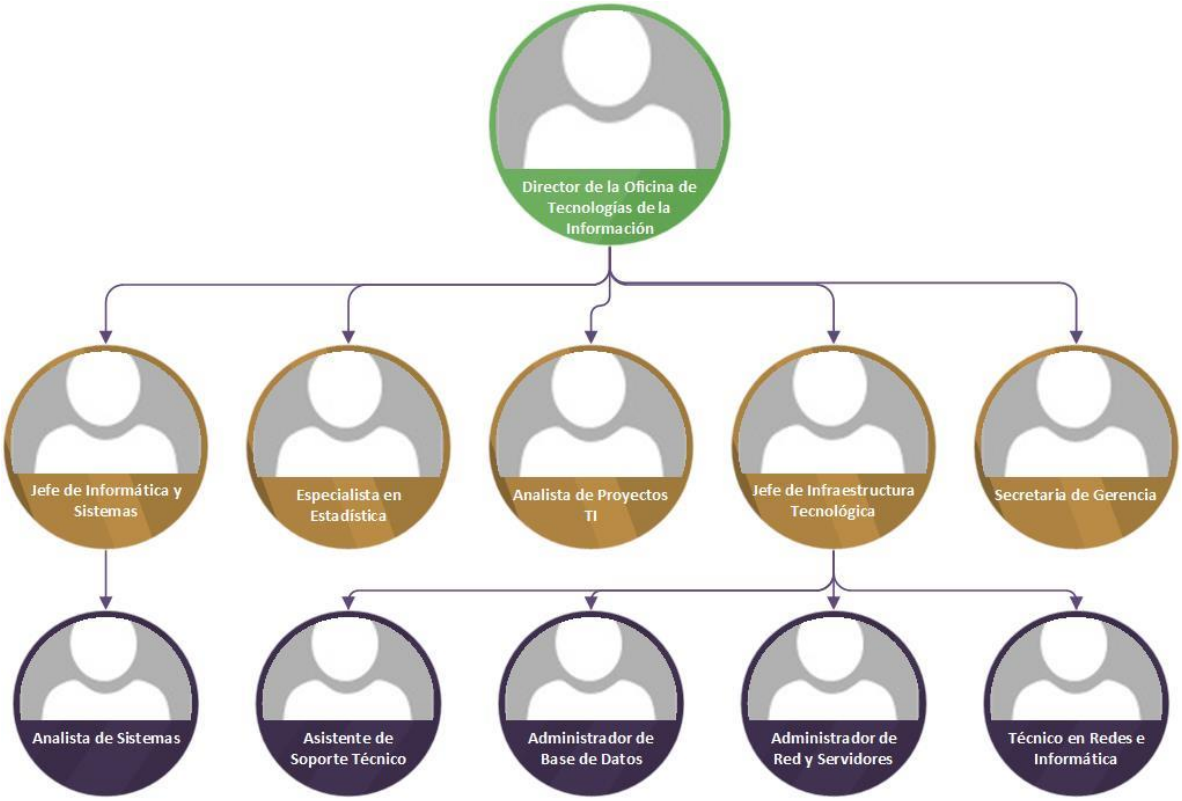


Fuente: (Portal Web Institucional del OSIPTEL, 2021)

2.5. Área, cargo y funciones desempeñadas

El autor de este trabajo de suficiencia profesional se desempeñó como *Analista de seguridad y servicios de infraestructura tecnológica* en la *Oficina de Tecnologías de la Información* del *Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL*, el área en mención se encuentra representada en el siguiente gráfico:

Figura 2: Organigrama Interno de la OTI



Funciones:

- Participar en actividades de su competencia durante las etapas de análisis, implementación, operación y mejora de los servicios de TI gestionados por la Jefatura de Infraestructura Tecnológica, para que se consideren los aspectos de seguridad informática pertinentes.
- Analizar los componentes de la infraestructura de servicios de TI para proponer e implementar soluciones de optimización, convergencia y/o migración a entornos de virtualización y computación en nube.

- Analizar los componentes de la plataforma de seguridad de infraestructura tecnológica, para proponer e implementar mejoras, controles y realizar monitores.
- Apoyar en la supervisión de servicios tercerizados, para abordar los temas relacionados a la seguridad informática de infraestructura tecnológica.
- Apoyar en la elaboración de especificaciones técnicas y términos de referencia para la contratación de bienes y servicios que soporten las operaciones o estén relacionados a la seguridad de la infraestructura tecnológica institucional.
- Apoyar en las operaciones de la Jefatura de Infraestructura Tecnológica en referencia a redes de datos y voz, comunicaciones de servicios de TI, seguridad y monitoreo de infraestructura tecnológica; para cumplir con los procedimientos y normas establecidas por la entidad y el área.
- Proponer a la Gerencia las políticas, controles, sistemas y procedimientos para la óptima administración y mejor aprovechamiento de los recursos informáticos del OSIPTEL.

2.6. Experiencia profesional realizada en la organización

Durante la experiencia profesional en el equipo de Infraestructura Tecnológica del OSIPTEL, el autor ha tenido la oportunidad de ampliar y poner en práctica sus conocimientos sobre el análisis, diseño, implementación y operación de diversas soluciones y plataformas de infraestructura tecnológica y seguridad digital colaborando en el cumplimiento de los objetivos estratégicos institucionales apoyados en soluciones de TI y, a la vez, garantizando el cumplimiento normativo vigente en el sector público nacional y el alineamiento a estándares internacionales como la Norma ISO/IEC 27001.

El haberse formado en la institución desde tempranas etapas de su vida profesional le ha permitido obtener un profundo conocimiento sobre el funcionamiento de la institución, sus procesos, sus prioridades, sus procedimientos para la toma de decisiones, priorización de actividades y asignación de recursos,

así como también conocer al detalle la operación y composición de la plataforma tecnológica que soporta las actividades institucionales. Todo esto, le permite ser capaz de proponer y ejecutar proyectos con una visión completa sobre el impacto que los mismos tendrán no solo en la operación diaria de la institución sino también en los diferentes elementos técnicos, tecnológicos y humanos con los que interactuará dicho proyecto.

En el año 2020, en el contexto de la emergencia sanitaria nacional por COVID-19, se le encargó la labor de proponer, analizar, diseñar, probar e implementar una plataforma que permitiese a los funcionarios de la institución continuar desempeñando sus funciones de manera remota; es en el marco de dicho encargo que se desarrolla el presente trabajo de suficiencia profesional.

CAPÍTULO III
ACTIVIDADES DESARROLLADAS

3.1. Situación Problemática

3.1.1 Definición del problema

A fin de entender la real situación problemática a la que se enfrentaba la organización que aborda el presente documento es necesario entender la coyuntura que se desencadenó en el país, y en especial en las organizaciones del sector público, a causa de la pandemia por COVID-19.

El sector público peruano llevaba varios años construyendo bases legales, programas de desarrollo e instituciones especializadas, todos ellos abocados a la tarea de incorporar las tecnologías de la información y comunicaciones en el quehacer diario de las instituciones públicas para así lograr hacer más eficientes los procesos del sector y, como consecuencia, lograr un mejor uso de los recursos del tesoro público a fin de acortar las brechas de desarrollo entre los diversos sectores socioeconómicos del país.

Como claros ejemplos de ello podemos mencionar la "*Ley de Gobierno Digital*" (aprobada mediante Decreto Legislativo Nº 1412 del año 2018) que busca instituir un marco de gobernanza para todo lo relacionado a gobierno digital y la correcta gestión de la identidad, los servicios, la arquitectura, la seguridad, los datos y la interoperabilidad digitales; así como también establecer un régimen legal de aplicación al uso transversal de las tecnologías digitales. Podemos, además, mencionar también la creación de la Secretaría de Gobierno y Transformación Digital – SeGDI, órgano que forma parte de la Presidencia del Consejo de ministros – PCM y que tiene por finalidad liderar todas las iniciativas nacionales en materia de servicios digitales, o la promulgación de la "Ley de Ciberdefensa", que establece un marco normativo para las actividades militares en el ciberespacio. Muchos años de labor normativa, de difusión, de concientización y demás, con el objetivo de tener instituciones públicas que se soporten en servicios digitales sólidos y así mejoren los servicios que le brindan a la ciudadanía.

Sin embargo, muchas de estas iniciativas o políticas se encontraban en etapas muy tempranas de su implementación, con un desarrollo muy incipiente o incluso, en algunos casos, sin haber comenzado siquiera su adopción en muchas instituciones. Esta serie de falencias se dejaron en evidencia cuando, el 15 de marzo de 2020, se declaró el estado de emergencia nacional y la cuarentena obligatoria; súbitamente un enorme número de instituciones públicas dejaron de operar y, lo que es peor, no tenían planes de acción que les fuesen a permitir retomar operaciones en el corto o mediano plazo. De hecho, evaluando los datos en retrospectiva, un estudio del Banco Interamericano de Desarrollo – BID (Roseth, Reyes, & Amé, 2021) indicó que más del 50% de funcionarios públicos peruanos encuestados reportó no haber podido llevar a cabo alguna tarea critica durante el periodo de emergencia sanitaria, casi el 30% reportó no tener acceso a algún archivo o aplicativo necesario para el desarrollo de sus funciones y, lo que es peor, el 45% de ellos se vieron en la necesidad de asistir de forma presencial a sus oficinas al menos una vez por semana para lograr el cumplimiento de sus tareas. Este estudio deja en evidencia que el impacto por la coyuntura sanitaria no fue, ni muchos menos, de corta duración en lo concerniente a la adaptación al trabajo remoto en las instituciones públicas peruanas y con ello se evidencia también la pobre adopción de tecnologías de la información en estas.

Ya en la coyuntura de la emergencia sanitaria, y habiéndose mencionado previamente la situación en que se encontraban muchas entidades publicas en materia de servicios digitales, se presentó un nuevo reto para estas: la imposibilidad de continuar con las contrataciones en trámite o de realizar nuevos procesos de contratación durante el periodo que durase el estado de emergencia sanitaria. Con esta medida muchas instituciones quedaron totalmente impedidas de acceder a los recursos para retomar sus operaciones al no ser capaces de brindarle a sus colaboradores los elementos para realizar sus labores de forma remota. Aunque esta medida fue corregida tiempo después, lo cierto es que ya se habían perdido meses de trabajo en los organismos públicos afectados, fueron muy pocas las instituciones publicas que lograron implementar condiciones de trabajo remoto

en los primeros días de la emergencia sanitaria, las demás simplemente detuvieron operaciones.

Luego de este breve preámbulo, que ha servido para poner al lector en autos del contexto en el cual se llevó a cabo la ejecución del trabajo descrito en el presente documento, ya es posible comenzar a plasmar las mismas interrogantes que surgieron en los profesionales de TI del sector público peruano a inicios del estado de emergencia sanitaria: ¿Cómo lograr que los servicios digitales internos de la institución estén disponibles para los colaboradores desde sus hogares? ¿Cómo lograrlo haciendo uso únicamente de los recursos tecnológicos disponibles? ¿Cómo lograrlo en un periodo de tiempo que asegure retomar las operaciones y, por ende, la atención al ciudadano a la brevedad?

Esta es la coyuntura en la cual se plantea el desarrollo del presente trabajo: intentar dotar a una institución pública de una plataforma de trabajo remoto que le permita mantener operaciones, y por ende continuar atendiendo a la ciudadanía, en el marco de la emergencia sanitaria por COVID-19.

Problemas Específicos:

- Necesidad de hacer disponibles para los colaboradores en sus hogares todos los servicios informáticos internos de la institución.
- Necesidad de contar con una solución en plazos breves de tiempo (horas o, como máximo, días).
- Imposibilidad de realizar contrataciones para la obtención de nuevas capacidades operativas (Software, Hardware, recurso humano, entre otros).
- Escalabilidad de la solución propuesta: todos los colaboradores deben poder trabajar en simultáneo a lo largo de la jornada.

3.2. Solución

Implementación de una plataforma de trabajo remoto para los colaboradores del Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL.

3.2.1 Objetivos

3.2.1.1 Objetivo General

Dotar al Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL de una plataforma de trabajo remoto en el marco de la emergencia sanitaria por COVID-19.

3.2.1.2 Objetivos Específicos

- Analizar la infraestructura de hardware y software de la que dispone la institución para la implementación deseada.
- Analizar las alternativas de plataformas de trabajo remoto que podrían satisfacer las necesidades de la institución.
- Formular una arquitectura de solución de trabajo remoto que satisfaga las necesidades institucionales.
- Diseñar la arquitectura con los componentes y relaciones que la constituirían.
- Implementar la arquitectura de plataforma de trabajo remoto seleccionada.
- Optimizar el rendimiento de la plataforma implementada.

3.2.2 Alcance

El alcance del presente trabajo es la formulación, diseño, implementación y optimización de una plataforma de trabajo remoto que permita a los colaboradores del OSIPTEL mantener operaciones durante la emergencia sanitaria por COVID-19.

El alcance está limitado hasta la optimización, o afinamiento, de la plataforma y, la operación y monitoreo de esta se encuentran fuera de dicho limite, asimismo, la validación del funcionamiento de los softwares o aplicativos personalizados de uso institucional se encuentra también fuera del mencionado alcance.

3.2.3 Etapas y metodología

La implementación de la plataforma de trabajo remoto, actividad neurálgica para la construcción del presente documento, se ejecutó siguiendo una metodología lineal (también llamada cascada), es decir, una actividad a continuación de la otra y cada una con uno o varios objetivos puntuales; en ese sentido, las fases planteadas para el proyecto fueron las mencionadas a continuación:

3.2.3.1 Planificación

Se recabó toda la información referente a la infraestructura tecnológica disponible, a las alternativas de solución viables y, principalmente, a las necesidades específicas a satisfacer con la solución que se propusiese.

3.2.3.2 Análisis

Se evaluaron las alternativas de solución técnicamente viables con la infraestructura tecnológica disponible y que sean capaces de satisfacer las necesidades de los colaboradores. Como producto de esta etapa se seleccionó la arquitectura de solución a implementar.

3.2.3.3 Diseño

Se diseñó la solución a implementar adaptando la arquitectura de plataforma escogida a las condiciones de la institución. Se establecieron los componentes necesarios para la implementación y sus relaciones con los componentes preexistentes en la plataforma tecnológica de la entidad.

3.2.3.4 Construcción

Se implementó la arquitectura de solución elegida, se integró con los componentes preexistentes en la plataforma tecnológica de la entidad y se validó la correcta operación de todas relaciones.

3.2.3.5 Seguimiento y Optimización

Se validó el cumplimiento de las necesidades de los colaboradores y, se identificaron y aplicaron oportunidades de perfeccionamiento en las configuraciones de la plataforma.

3.2.4 Fundamentos utilizados

3.2.4.1 Servidor de red

Se puede definir un “servidor de red”, también llamado “equipo servidor”, como un sistema que brinda, a través de una red de datos, recursos (sean estos datos, servicios, aplicativos, programas o algún otro tipo de recurso) a otro conjunto de quipos, usualmente denominados “clientes”; en general, es posible denominar “servidor” a todo equipo de cómputo que comparte algún tipo de recurso con otros equipos de cómputo haciendo uso de una red de datos. Llegados a este punto es preciso aclarar que un equipo en particular puede comportarse como servidor y como cliente al mismo tiempo, es decir, brindar recursos a un grupo de equipos y consumir recursos de otro grupo de equipos al mismo tiempo.

Básicamente, para que un equipo actúe como un servidor el único requisito indispensable es que se encuentre adecuadamente configurado para escuchar las peticiones de los equipos clientes en su red de datos. Esta característica, la de escuchar las peticiones de otros equipos, puede ser parte del conjunto de funcionalidades del propio sistema operativo instalado (como en el caso de los sistemas operativos Windows Server, que cuentan con un amplio abanico de configuraciones para escuchar y atender diversidad de peticiones de equipos cliente) o puede ser implementada en el servidor a través de la instalación de software especializado para tal fin (como en el caso del software de servidor web Apache, que permite que el equipo escuche y atienda solicitudes de navegadores de internet; es este caso, el software Apache es una capa adicional de software a la ya existente con el sistema operativo del equipo).

Entre los principales tipos de servidor, realizando una clasificación según su funcionalidad, podemos mencionar los siguientes:

- Servidores de archivos: uno de los usos más antiguos para un equipo es el de emplearlo como servidor de archivos, es decir, un equipo centralizado que se encarga de almacenar y compartir ficheros entre los clientes de la red de datos. Estos ficheros pueden ser de todo tipo (dependiendo de la configuración del servidor), desde fotografías y documentos de texto hasta instaladores de software y archivos de código fuente. Una de las grandes ventajas que ofrece el almacenamiento centralizado de archivos es la simplificación de tareas asociadas al mismo: como la ejecución de respaldos de información, la validación de la identidad de los clientes solicitantes o la implementación de mecanismos de tolerancia a fallos. Una de las cualidades de dedicar un equipo servidor a labores exclusivamente de servidor de archivos es que se pueden configurar sus características de hardware para potenciar las tareas de lectura y escritura de información, así como también la capacidad de transferir grandes volúmenes de información en corto tiempo.
- Servidores de impresión: disponer de una gran cantidad de equipos de impresión distribuidos a través de una serie de oficinas y tener que atender a un elevado número de usuarios realizando constantes peticiones de impresión es un escenario que podría resultar desalentador, sin embargo, la implementación de un servidor de impresión puede aligerar sustantivamente la carga de trabajo en estos casos. Un servidor de impresión se encarga de atender, de forma centralizada, las peticiones de impresión de los distintos equipos cliente de la red de datos y gestionar dicha petición para que sea ejecutada por un equipo de impresión en específico de acuerdo con ciertas características que pueda cumplir el solicitante. Con este tipo de implementaciones ya no es necesario que todos los clientes de la red de datos se encuentren directamente conectados a los equipos de impresión, basta con que tengan acceso al servidor de impresión.

- Servidores de aplicaciones: este tipo de servidores permiten que los clientes ejecuten aplicativos de forma remota en lugar de que cada equipo cliente tenga que hacerlo de forma local. Usualmente se recurre al uso de servidores de aplicaciones cuando el aplicativo en cuestión demanda la utilización de muchos recursos de hardware para su explotación y, por ello se haría onerosa la utilización de este aplicativo en cada uno de los equipos cliente (puesto que cada equipo cliente debería contar con robustas capacidades de hardware); en lugar de ello se centraliza la instalación y explotación del aplicativo y se brinda acceso a los clientes a dicha ubicación centralizada. Asimismo, centralizar la explotación de un aplicativo en un servidor de aplicaciones permite aligerar cargas de trabajo operativo asociadas al mantenimiento del propio aplicativo o a la gestión de los accesos al mismo. Muchos de los tipos de servidores que se detallarán más adelante en el presente pueden ser considerados como implementaciones altamente especializadas de servidores de aplicaciones.
- Servidores de resolución de nombres de dominio: también conocidos como “servidores DNS”, son equipos encargados de la resolución de nombres dentro de una red de datos. La resolución de nombres consiste en convertir los nombres de fácil entendimiento para los usuarios humanos en direcciones IP interpretables por los equipos de cómputo. El sistema DNS consiste en una base de datos ampliamente distribuida de nombres de dominio y servidores DNS a los que los equipos cliente pueden consultar por un nombre de equipo desconocido. Cuando un equipo cliente necesita conocer la dirección IP de un determinado sistema, envía una petición al servidor DNS indicando el nombre del recurso en cuestión y el servidor DNS le responde indicándole la dirección IP correspondiente a dicho recurso. Los servidores DNS pueden considerarse un tipo muy especializado de servidor de aplicaciones.

- Servidores de correo: los servidores de correo electrónico son uno de los tipos de servidor más común en los entornos empresariales actuales. Estos servidores se encargan de recibir los mensajes de correo electrónico dirigidos hacia un usuario especifico y almacenar dichos mensajes hasta que dicho usuario, a través de un equipo cliente en la red de datos, valide satisfactoriamente su identidad y reclame como suyos dichos mensajes. Disponer de un servidor de correo electrónico aligera enormemente la carga operativa que representaría que cada equipo cliente de la red de datos tuviese su propio sistema de gestión de mensajes de correo. Al igual que en el caso de los servidores DNS, los servidores de correo electrónico también pueden ser considerados servidores de aplicaciones especializados.
- Servidores web: una implementación específica más de un servidor de aplicaciones y, quizás, la implementación más abundante en el marcado actual. Un servidor web es un tipo particular de servidor que hospeda programas y conjuntos de datos que serán solicitados por los equipos cliente a través de la internet o de una intranet en particular. Los servidores web atienden las peticiones de entrega de sitios web, u otros servicios web, que llegan a través de los navegadores que se ejecutan en los equipos cliente. Los softwares de servidor web ampliamente más difundidos son *Apache*, *Microsoft Internet Information Services – IIS* y *Nginx*.

- Servidores de base de datos: por todos es sabido que la cantidad de datos que las organizaciones e individuos consumen es abrumadora en estos días, sin embargo, la gestión de dichos volúmenes inmensos de datos sería inviable sin la utilización de bases de datos, softwares altamente especializados que permiten gestionar los datos de los individuos y las organizaciones y aligerar la carga operativa de su tratamiento y explotación. Como es de suponer, la exigencia de recursos informáticos que demanda el tratamiento de enormes volúmenes de datos es muy elevada como para poder ser satisfecha por equipos convencionales. Todo lo anterior nos sirve como justificación para ubicar esos grandes repositorios, las bases de datos, en equipos servidores centralizados desde los cuales se les pueda proveer de hardware especializado a la vez que se simplifica la labor de gestión de acceso a la información por parte de los equipos cliente. Los softwares de gestión de bases de datos más comúnmente utilizados son *Oracle* y *Microsoft SQL*.

- Servidores proxy: también llamados servidores intermediarios, son los que actúan como mediadores entre un cliente y un servidor. Comúnmente son utilizados por motivos de seguridad cuando se busca aislar al cliente o al servidor a fin de protegerlo de amenazas externas.

  El modo de operación más común de un servidor proxy es el siguiente: Un servidor proxy recibirá la petición del equipo cliente, pero no la trasladará al equipo servidor deseado por el cliente, en su lugar trasladará dicha petición a otro equipo servidor y, cuando este segundo equipo servidor haya emitido una respuesta, el servidor proxy comunicará dicha respuesta al equipo cliente de forma transparente a este último. De esa forma, el cliente y el equipo servidor deseado nunca se llegan a comunicar realmente entre si.

- Servidores de virtualización: una de las tecnologías más utilizadas en los entornos empresariales es la virtualización, la posibilidad de ejecutar diversos entornos (usualmente sistemas operativos) completamente independiente unos de otros sobre el mismo equipo físico (sobre el mismo hardware). A diferencia de los equipos servidores tradicionales, en los que la dupla equipo hardware y sistema operativo es el estándar de implementación, en los servidores de virtualización se hace uso de una capa de software especializado llamado hipervisor, el cual se encargará de interactuar directamente con el hardware y de brindar al usuario interfaces para que gestione (cree, modifique, administre o elimine) entornos virtuales (también llamados máquinas virtuales). De esta forma el usuario administrador no solo puede gestionar de forma centralizada diversos equipos, sino que, además, puede exigir al máximo las capacidades de hardware de su equipamiento.
- Servidores de gestión: uno de los tipos más especializados de servidor es el de los servidores de gestión, administración o monitoreo. Este tipo de equipos no tienen por finalidad atender de forma directa las peticiones de un conjunto de equipos clientes, en su lugar realizan labores como analizar todo lo que circula por la red, proveer interfaces para controlar otros equipos o consultar constantemente los niveles de utilización de los recursos de hardware de un equipo y luego brindan acceso a la información consolidada a los usuarios administradores de la red de datos. Los subtipos de servidores que podríamos detallar en esta categoría son muchos y escapan a los propósitos del presente documento.
- Servidores de directorio: otro de los tipos de servidores más abundantes en las redes corporativas actuales, suelen recibir diferentes nombres como Controlador de Dominio, *Active Directory*, *LDAP*, entre otros; y aunque técnicamente cada uno de esos nombres no es del todo correcto (puesto que cada uno hace referencia a un elemento distinto) lo cierto es que la superposición de funciones de cada uno de los elementos mencionados y la estrecha relación que guardan entre si, hacen que entrar en el detalle de su especificación particular escape al alcance del presente documento.

Para efectos del presente documento es importante conocer una característica particular de los servidores de directorio: son grandes repositorios centralizados de bases de datos y servicios que permiten a los usuarios interactuar con los diversos componentes que conforman la red de datos. Para efectos del presente documento se utilizará la denominación "*Directorio Activo*" cuando se pretenda hacer alusión a la plataforma de servidores de directorio de una organización.

Por otra parte, entre los principales tipos de servidor, realizando una clasificación según su plataforma operativa, podemos mencionar los siguientes:

- Servidores *GNU/Linux*: aquí podemos hallar a todos los equipos que hacen uso de una versión de servidor de algún sistema operativo que use como *kernel* el popular núcleo de código abierto desarrollado por Linus Torvalds. Al ser de código abierto, este tipo de servidores se plantean no solo como alternativas de bajo coste de implementación para un innumerable número de entornos empresariales y educativos, sino que además es posible modificar su composición más profunda (su código fuente) para obtener versiones adaptadas a entornos muy particulares, haciéndolos, por esta última característica mencionada, perfectos para labores de investigación y desarrollo en equipamiento muy específico o desarrollado a la medida de cierta organización particular.
- Servidores *Microsoft Windows Server*: aquí encontramos a todos los equipos que ejecutan la versión de servidor del famoso sistema operativo de *Microsoft*. Este tipo de implementaciones suelen ser comunes en entornos empresariales debido la gran cantidad de empresas especializadas en dar soporte a estas soluciones y a la simplicidad que plantea implementar muchos tipos de funcionalidades en estos sistemas operativos: están diseñados para brindar, a través de una interfaz gráfica sencilla, la posibilidad de desplegar un gran número de servicios y roles sin necesidad de recurrir a interfaces de línea de comandos como es usual en GNU/Linux.

Existen diversos criterios para clasificar los equipos servidores, sin embargo, las 2 clasificaciones previamente planteadas y detalladas en el presente documento son las de mayor relevancia para los fines del presente.

3.2.5 Implementación de las áreas de procesos y sus buenas prácticas

A continuación, se detallan las fases constituyentes del proyecto y las actividades que se ejecutaron en cada una de ellas

3.2.5.1 Fase 1: Planeación

En esta fase, se procedió a recabar toda la información disponible sobre la infraestructura tecnológica aprovechable, las alternativas de solución viables y las necesidades por satisfacer de cara a los colaboradores de la institución.

En lo referente a la infraestructura tecnológica aprovechable, la institución contaba con lo siguiente:

- A nivel de hardware:
    - 5 equipos marca *IBM* modelo *System x3550 M2*.
        - Doble socket Intel® Xeon® CPU E5530 2.40 GHz 4 núcleos.
        - 128 GB de memoria RAM.
        - 408 GB de almacenamiento
            - 6 HDD de tecnología SAS y 10K RPM configurados en un arreglo RAID 1E (una forma propietaria, de la marca IBM, de implementación de un RAID 10 tradicional).
- A nivel de software:
    - Contrato empresarial vigente *Microsoft Enterprise Agreement*, lo que permite acceder y explotar el abanico de soluciones empresariales del fabricante/desarrollador Microsoft; entre las soluciones utilizables se encuentra la plataforma *Microsoft Windows Server*.
- Componentes preexistentes y explotables:

- Conexión a internet empresarial simétrico de 300 mbps con conexión alterna de 150 mbps.
- Centro de datos equipado y acondicionado con todo lo necesario para la correcta operación de la infraestructura de servicios (sistema de respaldo eléctrico, sistema de refrigeración, cableado estructurado administrable, sistema biométrico de control de acceso, gabinetes de servidores equipados, entre otros).
- Red de comunicaciones de centro de datos moderna, robusta y con soporte por parte de un contratista especializado.
- Plataforma Microsoft debidamente estandarizada y gestionada de forma centralizada por un clúster de entornos Controlador de Dominio.
- Plataforma de virtualización *VMware* implementada, optimizada y con soporte por parte de un contratista especializado.
- Certificado digital del tipo *wildcard* (un tipo de certificado digital que permite explotar el dominio registrado, así como todos sus subdominios respectivos) registrado a nombre de la institución.

En lo referente a las alternativas de solución viables, se consideraron las siguientes:

- *Microsoft Remote Desktop Services*: los Servicios de Escritorio Remoto (comúnmente abreviados como RDS por sus siglas en inglés) son una particular forma de virtualización que consiste en brindarle a cada usuario una sesión independiente en un entorno de trabajo común, es decir, sobre una misma plataforma (un mismo equipo físico, por ejemplo) trabajan diversos usuarios cada uno con una sesión independiente pero compartiendo todos los mismos recursos subyacentes (procesador, memoria, almacenamiento, entre otros.). Es preciso aclarar que los servicios de escritorio remoto de Microsoft también permiten la creación de VDI, sin embargo, no es una alternativa comúnmente explotada y no fue considerada para efectos del presente análisis.

- Infraestructura de Escritorios Virtuales: comúnmente llamados VDI (por sus siglas en inglés "*Virtual Desktop Infraestructure*"), son una particular forma de virtualización en la cual se crean instancias totalmente independientes unas de otras para que cada una sea explotada por un usuario en particular, es decir, cada usuario dispone de una máquina virtual para su uso individual e independiente de las maquinas en las que trabajen sus colegas.
- Redes privadas virtuales: comúnmente llamadas VPN (por sus siglas en inglés "*Virtual Private Network*"), son implementaciones que permiten conectar 2 o más redes de datos diferentes o, en la mayoría de los casos, unir a un usuario remoto a una red en específico; en el caso que nos compete, por ejemplo, la implementación de una VPN implicaría que el colaborador (desde su domicilio) podría conectar su equipo a la red de datos de la institución y trabajar como si estuviese físicamente dentro de las oficinas del OSIPTEL.

Finalmente, respecto a los requerimientos funcionales o exigencias mínimas a satisfacer de cara a los colaboradores, se identificaron las siguientes:

- Disponer de una plataforma de trabajo remoto en el menor tiempo posible, horas o días luego de declarado el estado de emergencia sanitaria a nivel nacional.
- Acceso a los repositorios de documentación digital institucional (repositorios centralizados en los cuales cada unidad orgánica del OSIPTEL almacena los documentos digitales que le corresponden).
- Acceso a los aplicativos y plataformas de uso imperativo en el sector público (como por ejemplo los sistemas gestionados por el Ministerio de Economía y Finanzas: Sistema Integrado de Administración Financiera – SIAF y Sistema Integrado de Gestión Administrativa – SIGA).
- Acceso a los aplicativos y plataformas de uso interno en la institución (como por ejemplo el Sistema de Gestión Documental – SISDOC, el Sistema de Seguimiento a Contratos – SICTO o el Sistema de Administración Integrado – SAI).

- Acceso a la Plataforma Nacional de Interoperabilidad – PIDE y los servicios que pone a disposición de las instituciones públicas.
- Posibilidad de que todos los colaboradores trabajen en simultaneo y que puedan trabajar en el horario del día que consideren más adecuado.

Es preciso mencionar que, además de los requerimientos funcionales exigidos por los colaboradores, para la implementación de la solución planteada fue preciso respetar requerimientos no funcionales tales como normativa vigente (directivas de uso de software legal, lineamientos y políticas del Sistema de Gestión de Seguridad de la Información – SGSI, imposibilidad de realizar contrataciones durante el estado de emergencia, entre otras) o condiciones técnicas de seguridad (la comunicación entre el usuario y la institución debe ser cifrada, los usuarios no deben poder retirar la información de los equipos de la institución, entre otras).

Con toda la información antes mencionada ya puesta sobre el tablero de trabajo se procedió a realizar el análisis de la viabilidad de cada alternativa de solución, sus niveles de exigencia respecto a los recursos disponibles y su grado de satisfacción respecto a las exigencias de los colaboradores.

3.2.5.2 Fase 2: Análisis

En esta segunda fase del proyecto se buscó determinar la alternativa de solución que fuese capaz de satisfacer las necesidades de los usuarios internos y que, además, fuese técnicamente viable de implementar con los recursos tecnológicos disponibles por parte de la entidad. Para ello se analizó a detalle toda la información colectada durante la fase previa y se centró la discusión en torno a las ventajas y desventajas de cada alternativa de solución.

A continuación, se detalla el análisis de fortalezas y debilidades identificadas para cada una de las alternativas de solución planteadas:

- Redes privadas virtuales
    - Ventajas

- Permite a los colaboradores trabajar desde sus hogares y acceder a la red de datos institucional.
- Los equipos con los que se trabaja pasan a formar parte de la red de datos institucional, por lo cual pueden hacer uso de todos los servicios de red ofrecidos al interior de las oficinas: acceso a repositorios documentales, acceso a aplicativos de uso en el sector público, acceso a aplicativos de uso interno en la institución, acceso a los servicios de la PIDE, entre otros.
- Todos los colaboradores pueden hacer uso del servicio de conexión VPN en simultaneo o durante el periodo horario que consideren más adecuado.
- Esta alternativa, al basarse únicamente en el establecimiento de enlaces o conexiones de red, no implica mayor utilización de infraestructura tecnológica a excepción de la conexión institucional a internet.

- Desventajas
  - Depende de la calidad de conexión (estabilidad, velocidad, ancho de banda, latencia, entre otros) a internet de la que disponga el colaborador en su domicilio y de las condiciones del equipo de cómputo desde el que realice la conexión.
  - La institución no cuenta con una plataforma para la implementación de una solución masiva del tipo VPN por lo cual las alternativas para viabilizar esta propuesta serian: la contratación de una solución del tipo VPN a una empresa especialista o la implementación de una plataforma VPN con elementos disponibles (software libre o alternativas similares) y gestión por parte del personal especialista de la entidad.

La primera opción no era viable en el contexto del presente proyecto puesto que, como ya se ha mencionado antes, las contrataciones en el sector público se encontraban suspendidas; mientras que la segunda alternativa planteaba una limitación del tipo temporal puesto que implicaba que el personal técnico especialista de la entidad se entrenase en el uso de este tipo de herramientas antes de que pudiesen comenzar si quiera con las labores de implementación.

- Se requiere que cada colaborador haga uso de un equipo desde su domicilio, esto se podría lograr únicamente de 2 maneras: permitiendo que el colaborador conecte su equipo personal a la red de datos institucional o brindándole al colaborador un equipo propiedad de la organización para que realice sus labores desde su hogar.

  Permitir que el colaborador conecte su equipo personal a la red de datos institucional supondría generar una gran brecha de seguridad puesto que, al no ser un equipo gestionado por el área técnica de la organización, dicho equipo podría contener una serie de amenazas (en la forma de software malicioso o de configuraciones inadecuadas) que podrían trasladarse al resto de la red de datos de la organización y poner en riesgo la seguridad de la información institucional.

Por otra parte, otorgar equipos propiedad de la institución a los colaboradores para que hagan uso de ellos desde sus hogares era una alternativa que planteaba serios retos en el contexto en que se desarrolló el presente proyecto. El primero de los retos identificados fue que esta alternativa planteaba la entrega a domicilio de los equipos a los colaboradores o, que los colaboradores recogiesen los equipos de las oficinas del OSIPTEL, en ambos casos se estaría actuando en contra de las restricciones y recomendaciones instauradas durante el estado de emergencia sanitaria; el segundo, y quizás el mas importante, era que, al momento de la implementación de la solución, aun no existía normativa específica que autorizase el uso de equipos de la institución de forma permanente en los hogares de los colaboradores.

- Aun si no existiese la condicionante anteriormente mencionada, esta alternativa de solución aun plantea otro reto, esta vez del tipo temporal: para poder preparar los equipos, sean estos propiedad de la institución o del colaborador, con los software y configuraciones necesarias se iba a requerir una gran cantidad de tiempo; adicionalmente al tiempo que supondría el traslado de dichos equipos hasta los hogares de los usuarios (en caso se usasen equipos de la institución) o el traslado del personal especialista hasta las ubicaciones de los equipos (en caso se optase por conectar a la red de datos los equipos propiedad de los colaboradores); respecto a este último punto, se tiene el agravante de que muchos de los colabores residen fuera de Lima (la única ciudad en la que se cuenta con personal técnico especialista) y, en el contexto de la emergencia sanitaria, los viajes entre provincias o regiones del país se encontraban prohibidos.

- Conclusión: esta alternativa de solución no resulta técnicamente viable puesto que, entre otros, implica el traslado de equipos o de personas y podría suponer una violación a las condiciones impuestas en el contexto de la emergencia sanitaria nacional.

- Infraestructura de Escritorios Virtuales
  - Ventajas
    - Permite a los colaboradores trabajar desde sus hogares y acceder a la red de datos institucional.
    - Los entornos en los que se trabaja se encuentran hospedados en el centro de datos institucional, por lo cual ya forman parte de la red de datos local y pueden hacer uso de todos los servicios de red ofrecidos al interior de las oficinas: acceso a repositorios documentales, acceso a aplicativos de uso en el sector público, acceso a aplicativos de uso interno en la institución, acceso a los servicios de la PIDE, entre otros.
    - Todos los colaboradores pueden hacer uso del servicio de VDI en simultaneo o durante el periodo horario que consideren más adecuado.
    - Al ser un esquema de trabajo de conexión a un entorno remoto, las labores de implementación requieren únicamente esfuerzo del lado del área técnica y ningún esfuerzo por parte del colaborador.
    - Se dispone de los elementos básicos para su construcción: hardware (el conjunto de servidores mencionados en la fase de Planificación) y software (licenciamiento empresarial Microsoft en caso se optase por una solución VDI de este fabricante), certificados digitales y, al ser una implementación que se realizaría dentro de las instalaciones del centro de datos institucional, se explotarían todas las condiciones que este ofrece, así como también su red de datos local.
  - Desventajas

        - Depende de la calidad de conexión (estabilidad, velocidad, ancho de banda, latencia, entre otros) a internet de la que disponga el colaborador en su domicilio y de las condiciones del equipo de cómputo desde el que realice la conexión.
        - Al ser una alternativa que construye un entorno de trabajo independiente para cada usuario es una opción que podría demandar muchos recursos de hardware para su implementación, para realizar esta validación se requeriría una fase de pruebas de desempeño y cargas de trabajo que podría tomar varios días antes de poderse dictaminar si se dispone de los recursos suficientes para satisfacer la demanda de todos los colaboradores.
    - Conclusión: esta alternativa de solución es técnicamente viable, sin embargo, en el contexto de desarrollo del presente proyecto podría significar la necesidad de utilizar tiempos de pruebas de desempeño mayores a los que la institución podría tolerar ante la inmediatez para retomar operaciones internas y, en consecuencia, de cara al ciudadano.
- *Microsoft Remote Desktop Services*
    - Ventajas
        - Permite a los colaboradores trabajar desde sus hogares y acceder a la red de datos institucional.
        - Los entornos en los que se trabaja se encuentran hospedados en el centro de datos institucional, por lo cual ya forman parte de la red de datos local y pueden hacer uso de todos los servicios de red ofrecidos al interior de las oficinas: acceso a repositorios documentales, acceso a aplicativos de uso en el sector público, acceso a aplicativos de uso interno en la institución, acceso a los servicios de la PIDE, entre otros.

- Todos los colaboradores pueden hacer uso del servicio de escritorio remoto en simultaneo o durante el periodo horario que consideren más adecuado.
- Al ser un esquema de trabajo de conexión a un entorno remoto, labores de implementación requieren únicamente esfuerzo del lado del área técnica y ningún esfuerzo por parte del colaborador.
- Se dispone de los elementos básicos para su construcción: hardware (el conjunto de servidores mencionados en la fase de Planificación) y software (licenciamiento empresarial Microsoft), certificados digitales y, al ser una implementación que se realizaría dentro de las instalaciones del centro de datos institucional, se explotarían todas las condiciones que este ofrece, así como también su red de datos local.
- El fabricante/desarrollador de la plataforma pone a disposición abundante documentación sobre las diversas alternativas de implementación de esta solución.

- Desventajas
  - Depende de la calidad de conexión (estabilidad, velocidad, ancho de banda, latencia, entre otros) a internet de la que disponga el colaborador en su domicilio y de las condiciones del equipo de cómputo desde el que realice la conexión.
- Conclusión: esta alternativa es técnicamente viable y plantea únicamente una desventaja del lado del cliente que puede considerarse asumible y de menor impacto en comparación con las debilidades que presentan las otras dos alternativas exploradas anteriormente.

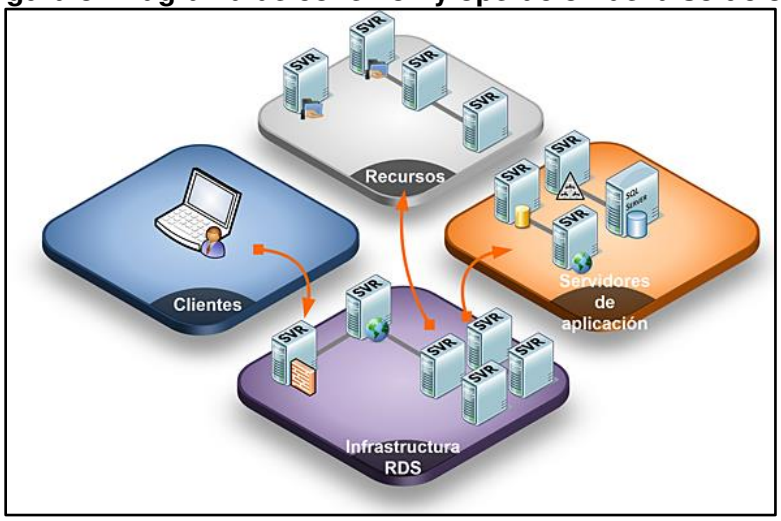
Como se puede apreciar, luego del análisis plasmado líneas arriba, la arquitectura de *Microsoft Remote Desktop Services* es la única alternativa de solución técnicamente viable bajo las condiciones del contexto en que se desarrolló el proyecto (tomando en consideración que la alternativa de los VDI implicaría un periodo de pruebas de desempeño que terminaría impactando en los tiempos de implementación y puesta en producción). Por tal motivo se optó por iniciar las labores pertinentes para su implementación y puesta en producción a la brevedad.

3.2.5.3 Fase 3: Diseño

Habiéndose determinado en la fase anterior la alternativa de solución a construir, era preciso definir la arquitectura de la solución a fin de proceder con las labores de implementación. Para ello se recurrió a la documentación del fabricante (Microsoft, 2021) a fin de determinar la arquitectura a emplear.

En primer lugar, se determinó el diagrama de conexión y operación a alto nivel del que haría uso la solución. Como se puede apreciar el grafico a continuación, los usuarios únicamente interactúan (a través de una conexión a internet) con la plataforma RDS y es esta ultima la encargada de conectarse con los diversos servicios de la red de datos institucional y ponerlos a disposición de los usuarios.

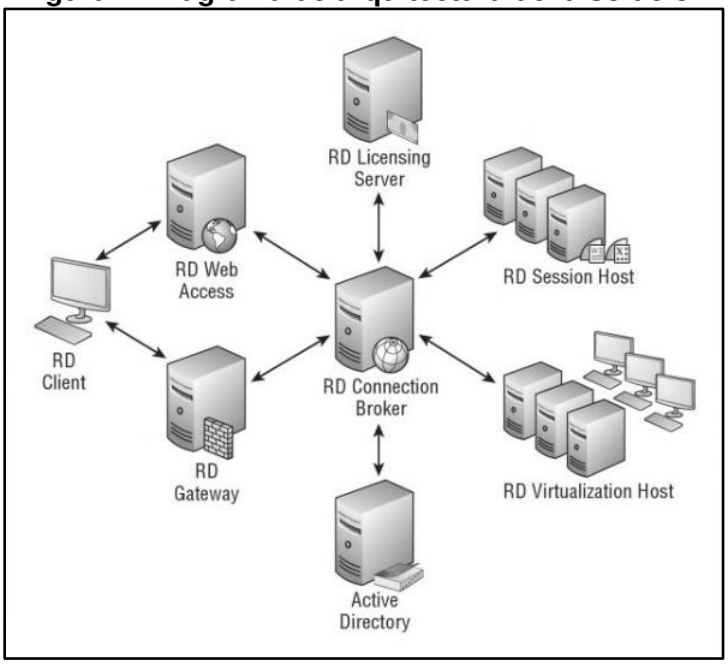
Figura 3: Diagrama de conexión y operación de la solución



Fuente: (Asimane, 2017)

Posteriormente se procedió a determinar la arquitectura de alto nivel de la solución, dicho diagrama se puede apreciar en el grafico a continuación.

Figura 4: Diagrama de arquitectura de la solución



Fuente: (Rath , 2021)

Asimismo, en el grafico precedente, se pueden apreciar referencias a ciertos componentes propios de la Arquitectura RDS y que procederemos a explicar brevemente a continuación:

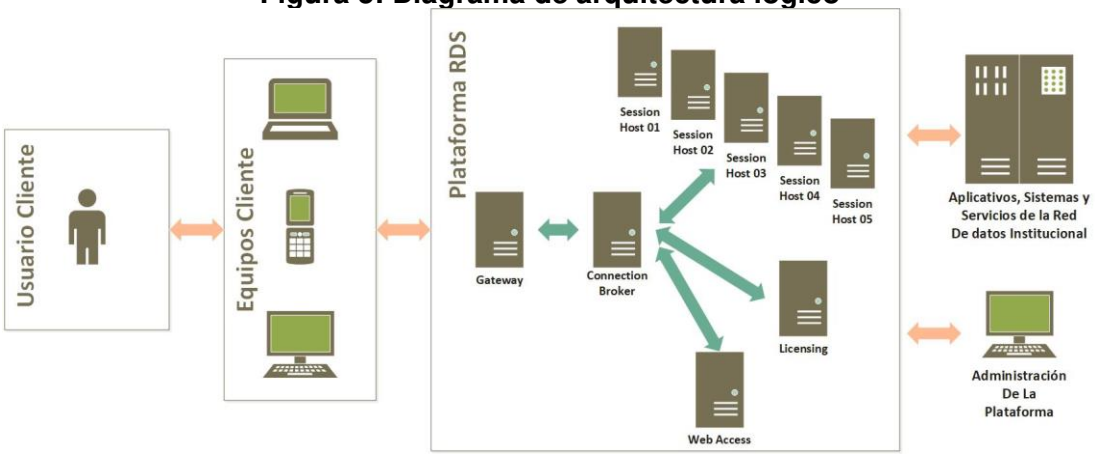
- *Active Directory* (Directorio Activo): como ya se ha establecido previamente, el Directorio Activo es el núcleo de toda arquitectura o plataforma *Microsoft* que se desee implementar. Asimismo, como se mencionó en apartados previos, la organización ya cuenta con una plataforma de entornos que cumplen el rol de Directorio Activo, por lo cual su implementación escapa al alcance del presente.
- *RD Client* (Cliente de Escritorio Remoto): se considera como equipo cliente a todo dispositivo (PC, dispositivo móvil, entre otros) que se conecta a la plataforma RDS para hacer uso de sus servicios.
- *RD Gateway* (Puerta de Enlace de Escritorio Remoto): componente necesario cuando la plataforma RDS se encontrará conectada a redes públicas (como la internet) pues es la encargada de ser quien responda ante la dirección IP pública publicada hacia la internet y, por ende, es la primera instancia en atender las peticiones de los clientes. Entre sus funciones podemos mencionar:
    - Opera como Proxy o intermediario pues recibe las solicitudes de conexión de los clientes desde las redes públicas y gestiona su atención con los elementos de la plataforma RDS.
    - Encripta el canal de comunicaciones entre el cliente y la plataforma RDS.
    - Es la primera capa de validación de seguridad: valida que el cliente tiene permisos para conectarse al recurso solicitado y, además, valida que el recurso solicitado está autorizado para brindar servicios al cliente.

- *RD Session Host* (Anfitrión de Sesión de Escritorio Remoto): componente que se encarga de ejecutar los procesos requeridos por los clientes, es en este componente donde se generan las sesiones de usuario y, por ende, donde se ejecutan todos los programas y aplicativos que el usuario requiera utilizar, es, por ende, el componente más exigido en términos de recursos hardware de toda la plataforma RDS.
- *RD Connection Broker* (Agente de Conexión de Escritorio Remoto): componente encargado de gestionar las conexiones entre los equipos clientes y los *Session Host* de la plataforma RDS. Si bien es cierto que el *Gateway* actúa como un primer filtro de conexión, esto lo realiza como una labor de seguridad y no de gestión de la conexión; es el *Connection Broker* el encargado de administrar a donde se conectará cada cliente y esto es particularmente útil cuando se trata de implementaciones RDS en las cuales se requiere distribuir la carga de trabajo entre varios *Session Host*, como es el caso del presente proyecto. Entre sus funciones podemos mencionar:
    - Revalidar las credenciales del cliente.
    - Asignar a los clientes a los entornos en los que trabajaran (*Session Host*).
    - Habilitar o deshabilitar las conexiones hacia determinados entornos (*Session Host*).
    - Distribuir la carga de trabajo entre los diferentes *Session Host*.
    - Gestionar el consumo multimedia entre los *Session Host* y los clientes (entrada y salida de audio).
    - Gestionar el uso de recursos compartidos entre los *Session Host* y los clientes (compartición de archivos, portapapeles, equipos de impresión, entre otros).
    - Gestionar las condiciones de la conexión del cliente (cuanto tiempo puede permanecer conectado, cuando tiempo puede permanecer inactivo, luego de cuánto tiempo se cerrará su sesión de trabajo, entre otras).

- *RD Web Access* (Acceso Web a Escritorio Remoto): componente que se encarga de hacer disponibles, a través de un portal web, para los clientes las aplicaciones instaladas en los *Session Host* de la plataforma RDS. Es particularmente útil cuando se busca poner a disposición de los usuarios ciertos aplicativos en particular sin necesidad de recurrir a crearles una sesión de trabajo completa; este no es el caso del presente proyecto, sin embargo, este componente fue implementado puesto que es imperativo para la construcción de la arquitectura RDS de *Microsoft*.
- *RD Licensing* (Servicio de Licenciamiento de Escritorio Remoto): componente encargado de administrar la asignación de licencias de uso de conexión de escritorio remoto. En la Arquitectura RDS de Microsoft es necesario contar con un tipo especial de licenciamiento para que los clientes puedan conectarse a la plataforma, por ende, la implementación de este componente es imperativa para la construcción de la Arquitectura RDS.
- *RD Virtualization Host* (Anfitrión de Virtualización de Escritorio Remoto): componente encargado de gestionar los entornos virtuales cuando se implementan servicios de VDI con la plataforma Microsoft. Este componente es parte de la Arquitectura RDS de *Microsoft*, pero no es de uso imperativo para su operación y, por ende, no ha sido parte de la presente implementación.

Finalmente, luego de haber determinado el esquema de conexión de la solución y la arquitectura a alto nivel de esta, se procedió a construir el diagrama de arquitectura lógico de la solución adaptado a la implementación esperada. Dicho diagrama se expresa en el grafico a continuación y supone la guía a seguir durante la fase posterior.

Figura 5: Diagrama de arquitectura lógico



Respecto al diagrama precedente es oportuno mencionar algunos puntos:

- Al ser un diagrama lógico, se han abstraído diversos elementos como la complejidad de las conexiones en redes públicas (ubicadas entre los equipos cliente y la plataforma RDS) y los servicios de red necesarios para la operación de la plataforma (como los servicios de Directorio Activo o de Controlador de Dominio).
- Se ha considerado implementar los *Session Host* en los equipos servidores disponibles como parte de la infraestructura; esto debido a que el componente *Session Host* es el más demandante en recursos hardware y, por ello, se ha considerado adecuado que se implemente sobre equipamiento físico dedicado.
- Se ha considerado implementar los componentes *Gateway*, *Web Access*, *Licensing* y *Connection Broker* dentro de la plataforma de virtualización VMware, mencionada previamente como parte de los componentes disponibles, esto debido a que son componentes de bajo consumo de recursos hardware.

Por último, teniendo en claro los esquemas bajo los cuales se implementará y operará la solución, es oportuno realizar una breve explicación del flujo de trabajo que se sigue ante el requerimiento de conexión de un cliente a la plataforma RDS:

1. El usuario, a través de algún software cliente de RDS, solicita acceso a la plataforma RDS.
2. El Gateway valida que el usuario solicitante dispone de acceso para conectarse a la plataforma y valida que los elementos de la plataforma están autorizados a brindarle servicios al usuario solicitante. Posteriormente traslada la petición al *Connection Broker*.
3. El *Connection Broker* evalúa si el usuario solicitante tiene permiso para conectarse a algún *Session Host* en específico y las condiciones para dicha conexión. Posteriormente traslada la petición al *Session Host* elegido.
4. El *Session Host* crea una nueva sesión para el usuario solicitante y le da la bienvenida a su escritorio de trabajo y a todos los servicios que tenga habilitados.

3.2.5.4 Fase 4: Construcción

En esta fase se utilizó el diagrama lógico de construcción diseñado en la etapa anterior para iniciar las labores que materializasen la solución elegida.

En primer lugar, se determinaron los entornos de implementación para cada componente de la solución, así como también sus características.

- *RD Gateway*
    - Se implementará en un entorno virtual en la plataforma *VMware* institucional. Se busca aislar el componente puesto que es un elemento que tendrá contacto directo con redes públicas.
    - Se implementará sobre un entorno *Microsoft Windows Server 2012 R2 Standard*. Se busca lograr la mayor compatibilidad posible con el resto de la plataforma institucional de servidores y herramientas de seguridad.
    - Al servidor se le asignará el nombre *SRVGATEWAY*.

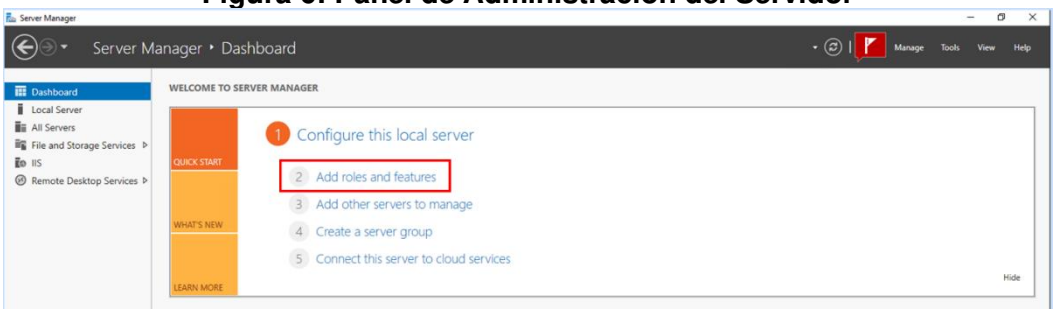
- *RD Connection Broker*, *RD Web Access* y *RD Licensing*
    - Serán implementados en un mismo entorno virtual en la plataforma *VMware*. Se busca optimizar el uso de recursos al centralizar estos componentes de bajo consumo en un único entorno.
    - Se implementarán sobre un entorno *Microsoft Windows Server 2019 Standard*. Se busca lograr simplificar el procedimiento de implementación al contar con una versión más reciente del software.
    - Al servidor se le asignará el nombre *SRVRDS-CB01*.
- *RD Session Host*
    - Serán implementados en los servidores físicos disponibles con los que cuenta la institución, es decir, se implementarán cinco servidores con la funcionalidad de *Session Host*. Se busca distribuir la carga entre el mayor número posible de servidores físicos dedicados al ser el componente *Session Host* el más demandante en recursos hardware.
    - Se implementarán sobre entornos *Microsoft Windows Server 2019 Standard*. Se busca lograr contar con las actualizaciones de compatibilidad y seguridad más recientes puesto que serán los entornos en los que los usuarios ejecutarán sus tareas diariamente.
    - A los equipos se le asignarán los nombres: *SRVRDS-SH01*, *SRVRDS-SH02*, *SRVRDS-SH03*, *SRVRDS-SH04* y *SRVRDS-SH05*.

Antes de proseguir con los detalles de la implementación, es oportuno mencionar que diversos datos (nombres de dominio, direcciones IP, entre otros) serán obviados del contenido del texto, deliberadamente alterados o censurados en las imágenes que los contengan por razones obvias de seguridad y confidencialidad para con la organización analizada.

Posteriormente, se procedió a instalar los componentes de la arquitectura (el fabricante *Microsoft* denomina "*Roles*" a estos componentes) en cada uno de los entornos preparados.

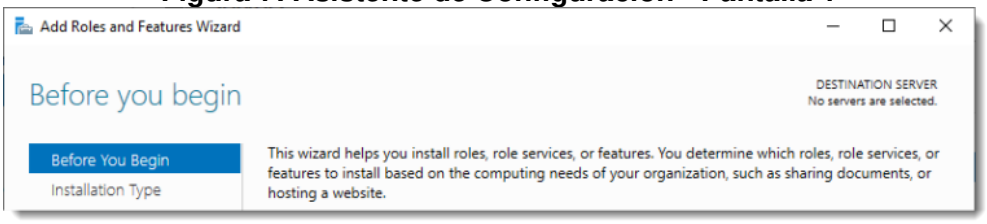
Para iniciar el asistente de configuración de los componentes de la plataforma es necesario, desde el panel de administración del servidor, seleccionar la opción de "*Agregar Roles y Características*" (*Add roles and features*) tal y como se muestra en la imagen a continuación.

Figura 6: Panel de Administración del Servidor



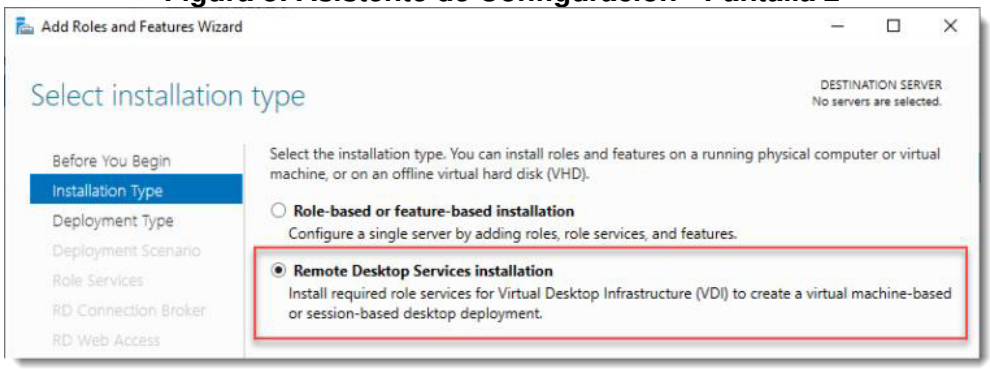
En la primera pantalla del asistente de configuración se nos brinda una breve descripción de las tares que pueden llevarse a cabo desde este asistente.

Figura 7: Asistente de Configuración - Pantalla 1



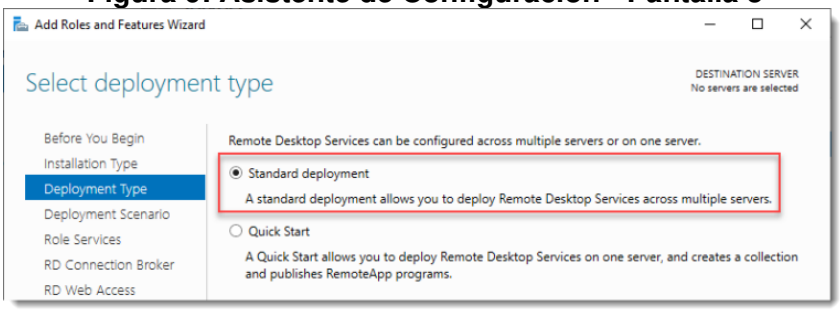
En la segunda pantalla del asistente de configuración se nos permite escoger si deseamos realizar una instalación tradicional de roles o si deseamos configurar una arquitectura de servicios de escritorio remoto. Se elige esta última opción.

Figura 8: Asistente de Configuración - Pantalla 2



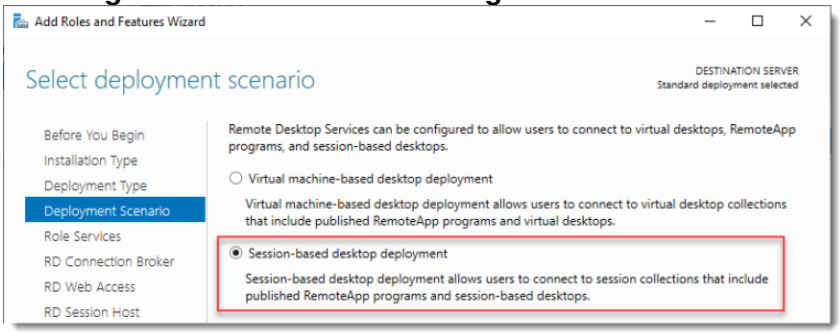
En la tercera pantalla del asistente de configuración se pide escoger el tipo de despliegue que se realizará: un despliegue estándar (*Standard Deployment*) o un despliegue rápido (*Quick Start*). La alternativa de despliegue rápido permite instalar todos los componentes de la plataforma (los roles) en un único equipo o entorno, esto puede resultar útil en escenarios de prueba de concepto o de entornos de trabajo con muy baja exigencia; este no es el caso del presente proyecto, por lo cual se selecciona la alternativa de despliegue estándar, la cual permitirá distribuir la carga de trabajo de los componentes entre diferentes entornos.

Figura 9: Asistente de Configuración - Pantalla 3



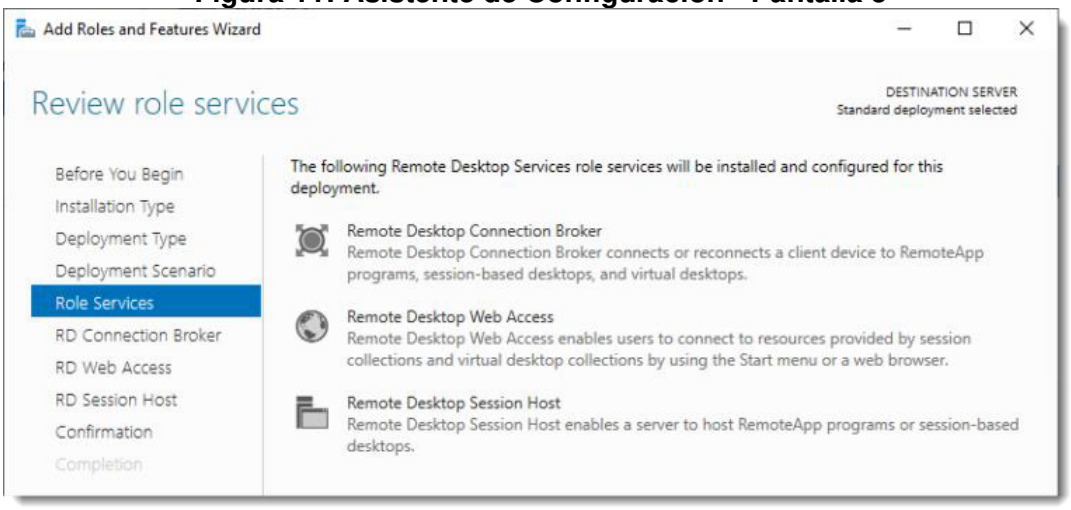
En la cuarta pantalla del asistente de configuración se pide elegir el escenario de operación de la plataforma: un despliegue de escritorios basado en máquinas virtuales o un despliegue de escritorios basado en sesiones. El despliegue de escritorios basado en máquinas virtuales es algo que ya se ha mencionado previamente en el presente documento, se trata de una forma de implementación de *VDI* la cual, como ya se aclaró previamente, no era acorde a las necesidades del contexto del presente proyecto. Se elige la alternativa de despliegue de escritorios basado en sesiones.

Figura 10: Asistente de Configuración - Pantalla 4



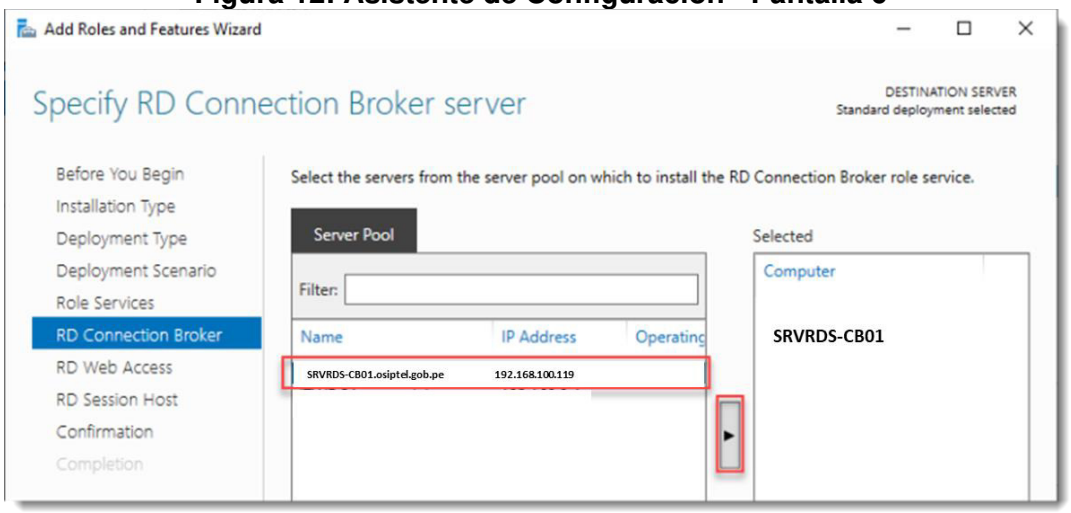
En la quinta pantalla del asistente de configuración se indican los componentes mínimos necesario que el escenario de operación requiere: *Remote Desktop Connection Broker*, *Remote Desktop Web Access* y *Remote Desktop Session Host*, sin embargo, como ya se ha mencionado previamente, la plataforma que se pretende implementar requiere de componentes (roles) adicionales, esto será posible en configuraciones posteriores, por el momento el asistente solo exigirá configurar los 3 componentes mencionados.

Figura 11: Asistente de Configuración - Pantalla 5



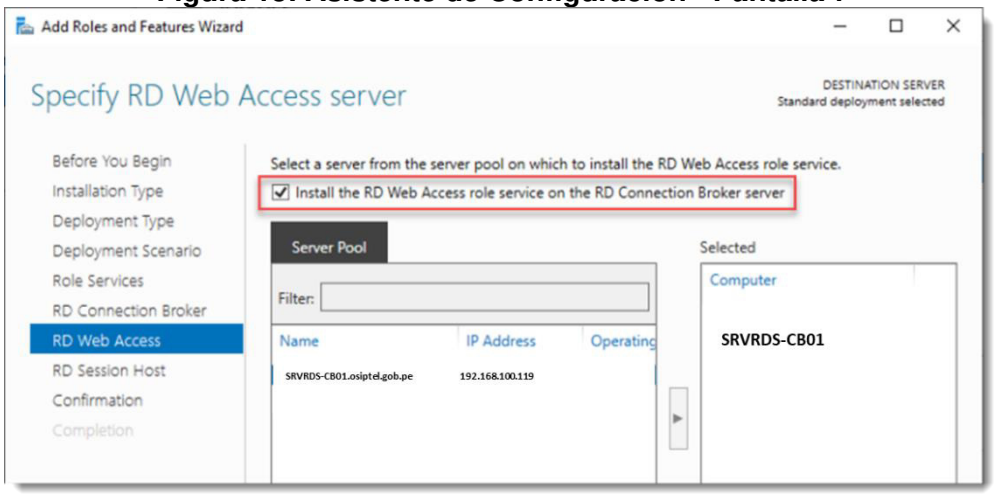
En la sexta pantalla del asistente de configuración se debe seleccionar el entorno en el cual se desplegará el componente *Connection Broker*, en el caso de esta implementación, se selecciona el entorno *SRVRDS-CB01*.

Figura 12: Asistente de Configuración - Pantalla 6



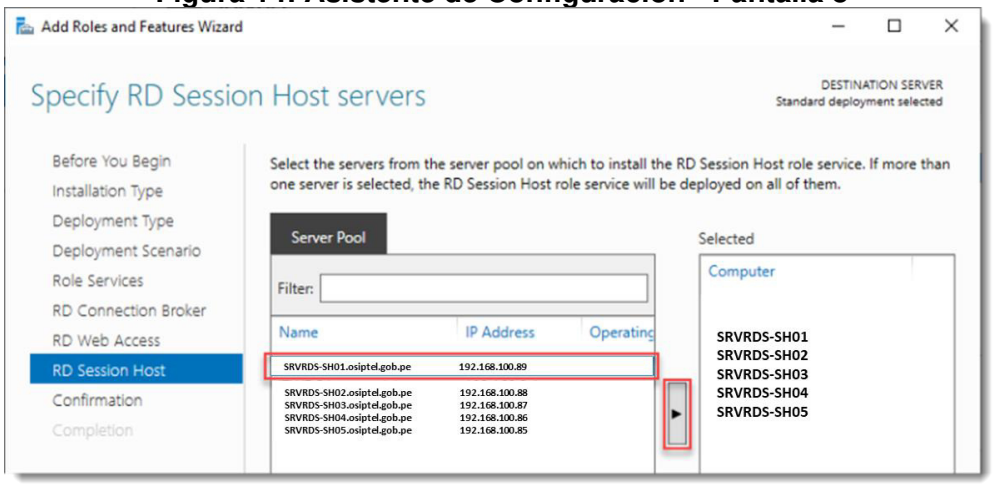
En la séptima pantalla del asistente de configuración se debe seleccionar el entorno en el cual se desplegará el componente *Web Access*, en el caso de esta implementación, como ya se ha mencionado previamente, se utilizará también el entorno *SRVRDS-CB01*, para este caso, el propio asistente de configuración brinda la opción de instalar el componente *Web Access* en el mismo entorno que el componente *Connection Broker* con tan solo marcar una casilla.

Figura 13: Asistente de Configuración - Pantalla 7



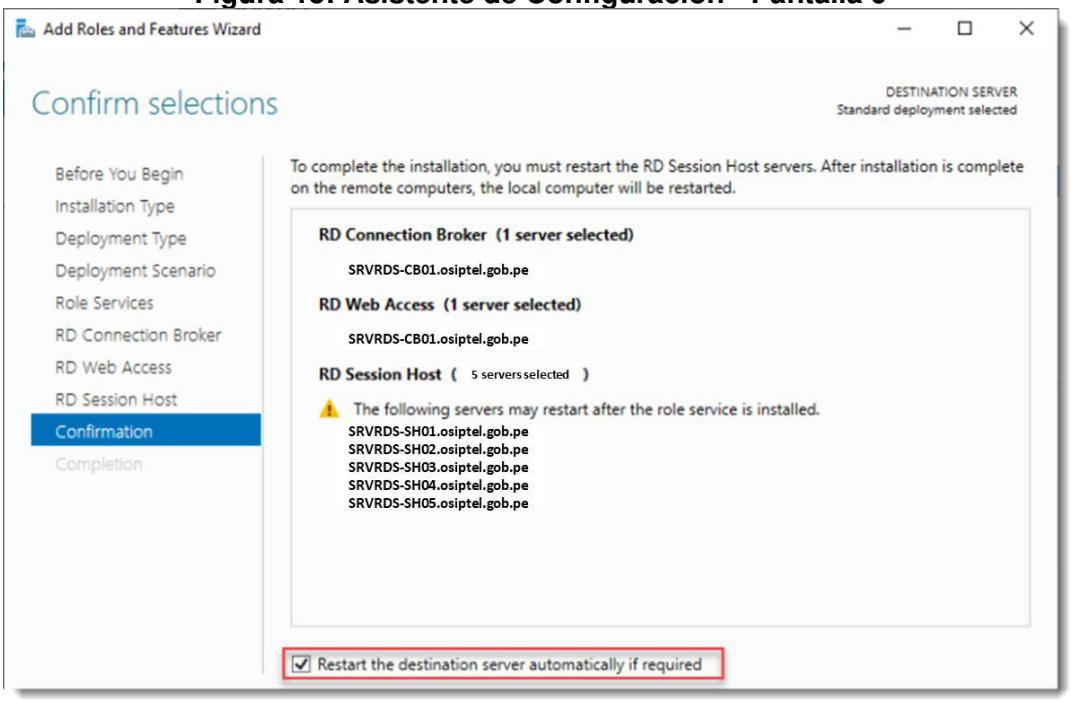
En la octava pantalla del asistente de configuración se deben seleccionar los entornos en los cuales se desplegará el componte *Session Host*, en el caso de esta implementación, se seleccionarán los entornos *SRVRDS-SH01*, *SRVRDS-SH02*, *SRVRDS-SH03*, *SRVRDS-SH04* y *SRVRDS-SH05*.

Figura 14: Asistente de Configuración - Pantalla 8



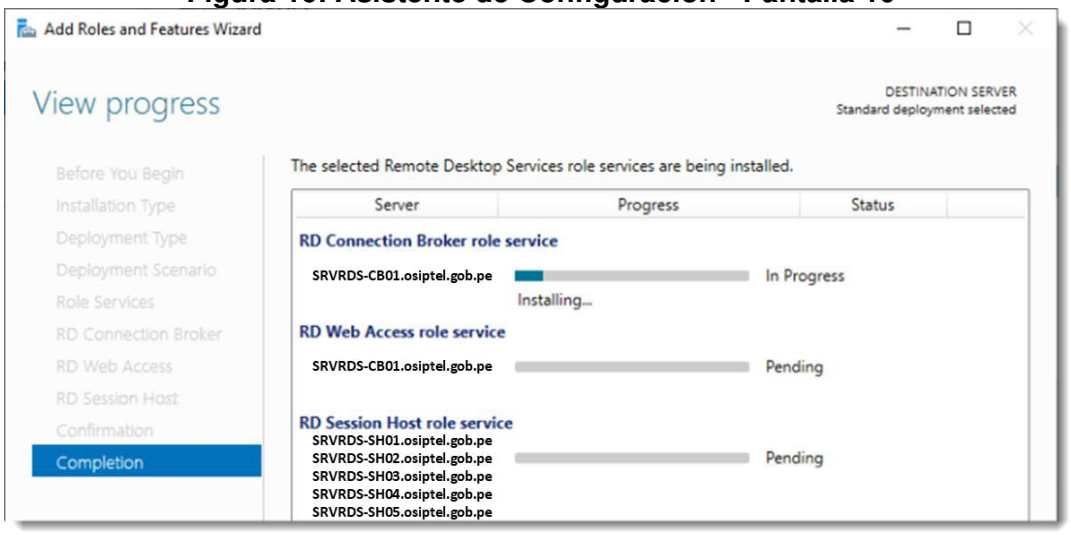
En la novena pantalla del asistente de configuración se brinda un breve resumen de las configuraciones a ejecutar, se advierte que algunos entornos podrían reiniciarse luego de la instalación y finalmente, se solicita autorización para ejecutar dichos reinicios.

Figura 15: Asistente de Configuración - Pantalla 9



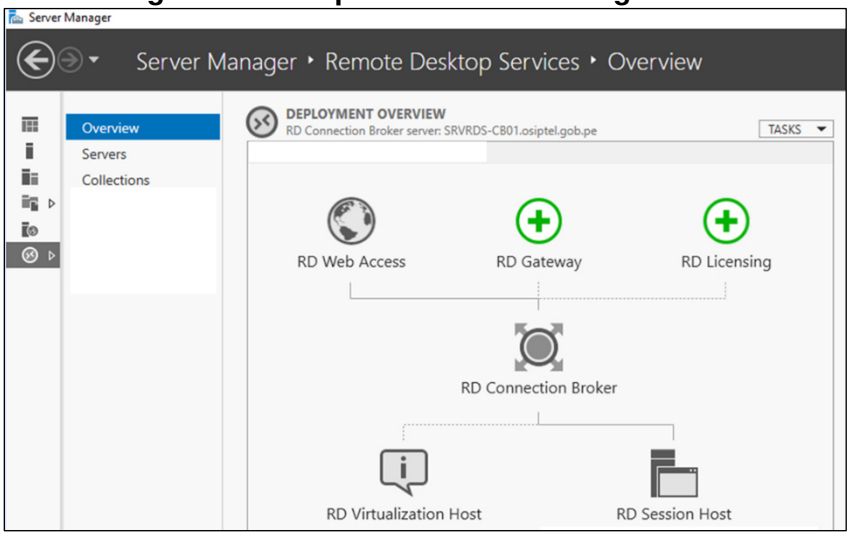
La décima pantalla del asistente de configuración es una pantalla de carga en la cual se muestra el avance de las instalaciones desplegadas.

Figura 16: Asistente de Configuración - Pantalla 10



Una vez culminada la instalación, los entornos se reinician de forma automática, se valida que han iniciado con el componente (rol) respectivo instalado correctamente y se da por culminado el asistente de configuración. Posteriormente ya es posible ver los componentes instalados desde el panel de gestión del servidor tal y como se puede apreciar en la imagen a continuación, los componentes *RD Connection Broker*, *RD Web Access* y *RD Session Host* ya se pueden apreciar como disponibles.

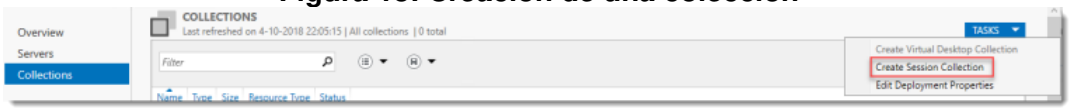
Figura 17: Componentes RDS configurados



A continuación, se procedió a realizar la configuración del componente *Connection Broker* para posibilitar las conexiones hacia los equipos *Session Host*. Para ello, el primer paso es crear una "Colección". En la Arquitectura RDS, una colección no es más que un grupo de equipos que brindarán un determinado servicio, por ejemplo, para efectos del presente proyecto, los cinco equipos servidores que conforman el componente *Session Host* deberán conformar una colección a fin de poner a disposición sus servicios a los usuarios.

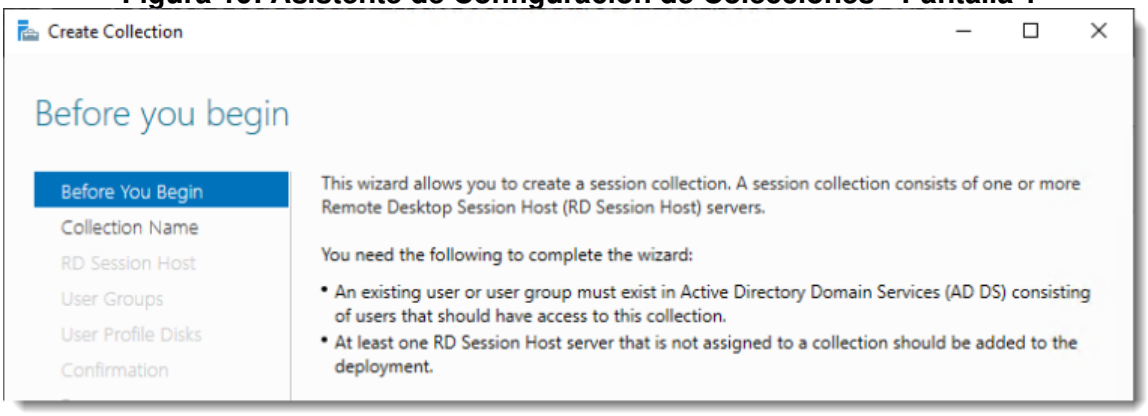
El primer paso es selección la opción "Create Session Collection" desde la interfaz de gestión del servidor como se muestra en la imagen a continuación.

Figura 18: Creación de una colección



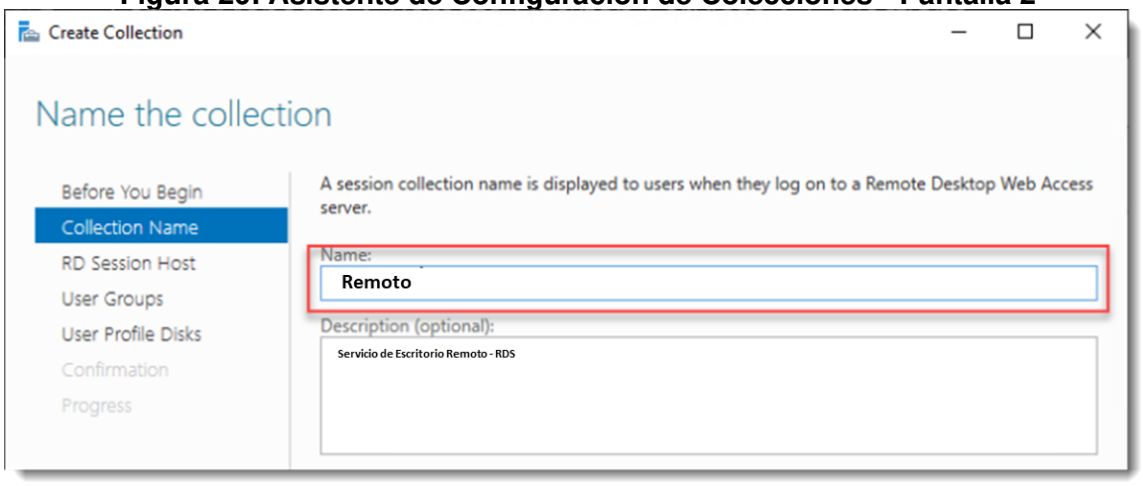
Al igual que cuando se configuró inicialmente la Plataforma RDS, en este caso también se interactúa con un asistente de configuración cuya primera pantalla nos brinda un breve resumen de sus funcionalidades y los requisitos a tomar en cuenta.

Figura 19: Asistente de Configuración de Colecciones - Pantalla 1



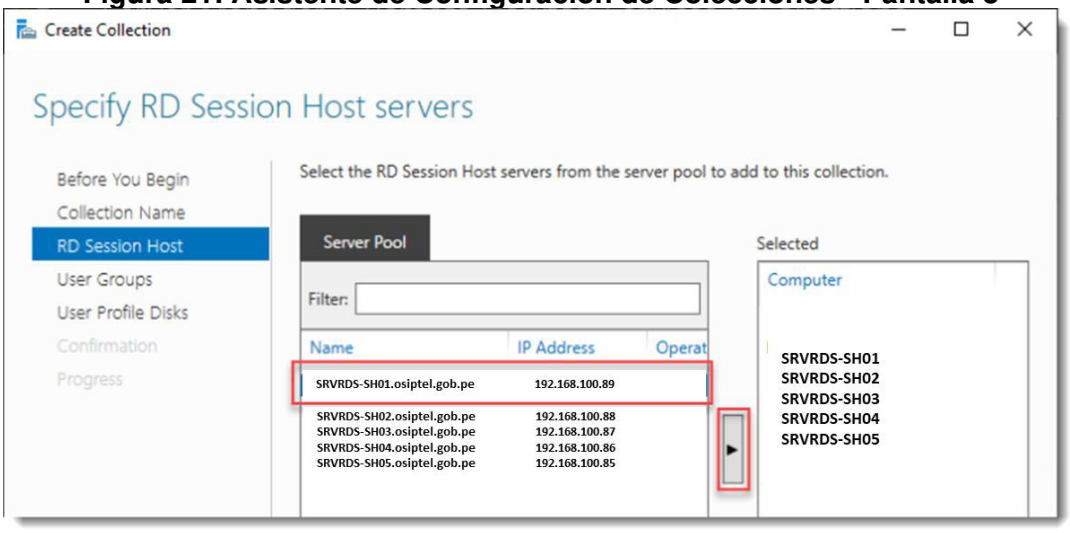
A continuación, solicita que se establezca un nombre para la nueva colección a crear, como se aprecia en la imagen a continuación, en este caso elegiremos de nombre para la colección “Remoto”. Se pide también, de forma opcional, una breve descripción.

Figura 20: Asistente de Configuración de Colecciones - Pantalla 2



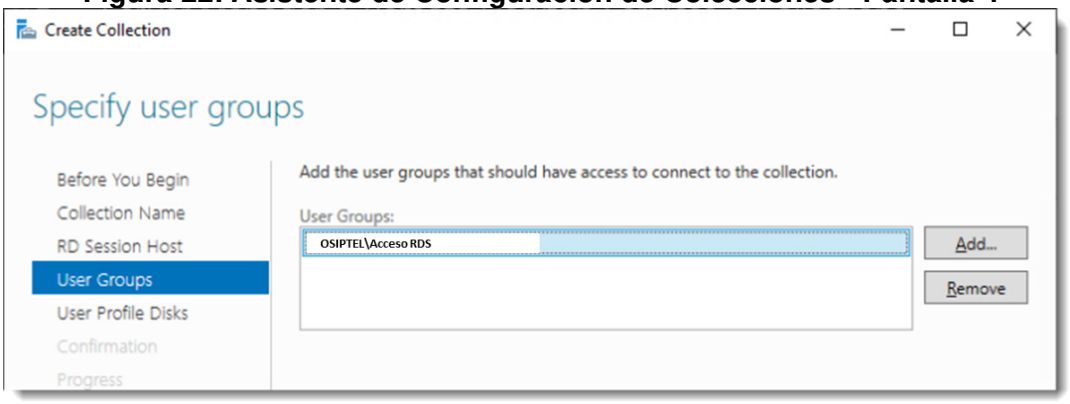
Posteriormente, se debe elegir los equipos *Session Host* que serán parte de la colección a crear. Para este caso, se elegirán todos los *Session Host* configurados hasta el momento: *SRVRDS-SH01*, *SRVRDS-SH02*, *SRVRDS-SH03*, *SRVRDS-SH04* y *SRVRDS-SH05*.

Figura 21: Asistente de Configuración de Colecciones - Pantalla 3



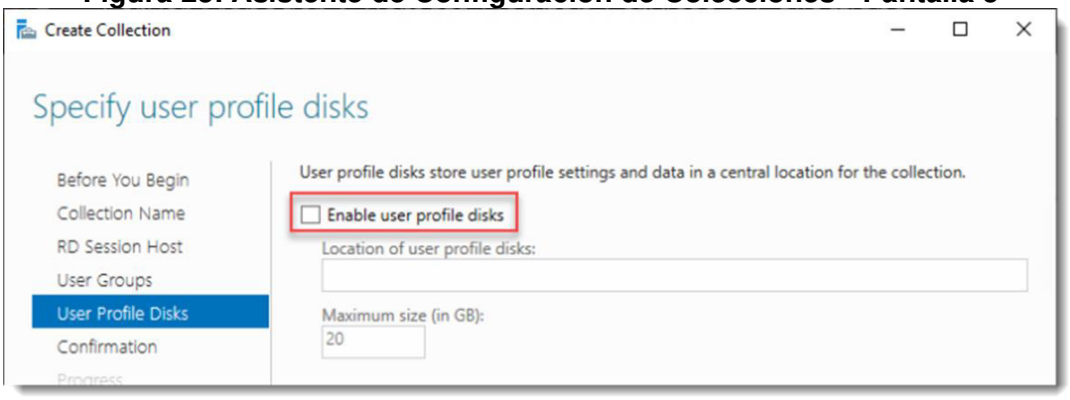
Luego, se pide escoger el grupo de usuarios que tendrán acceso a dicha colección, es decir, el grupo de usuarios que podrán trabajar en los equipos *Session Host*. En este caso, se elige un grupo de *Directorio Activo* previamente existente denominado "*Acceso RDS*".

Figura 22: Asistente de Configuración de Colecciones - Pantalla 4



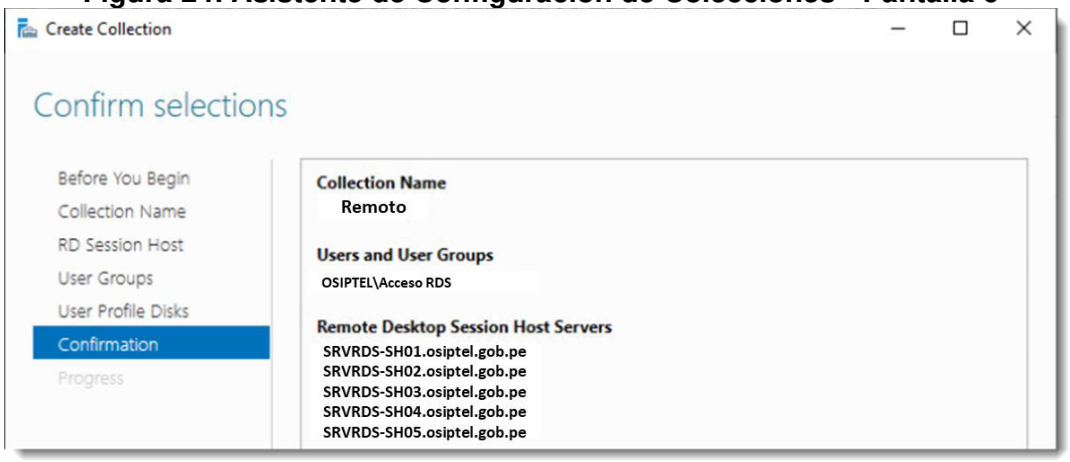
En la quinta pantalla del asistente de configuración de colecciones se nos solicita, de forma opcional, seleccionar una ubicación para el almacenaje de los perfiles de usuario de los colaboradores que trabajaran en la plataforma. En este caso, es pertinente comentar que los sistemas operativos *Microsoft Windows* crean un perfil de usuario (un conjunto de datos y configuraciones particulares para cada usuario) cada vez que un nuevo usuario se conecta a un equipo, esto es útil porque permite al usuario disponer de todos sus ajustes, configuraciones y archivos previamente trabajados cada vez que inicia sesión en el mismo equipo. En este caso, no se seleccionará una ubicación específica para dicho almacenaje.

Figura 23: Asistente de Configuración de Colecciones - Pantalla 5



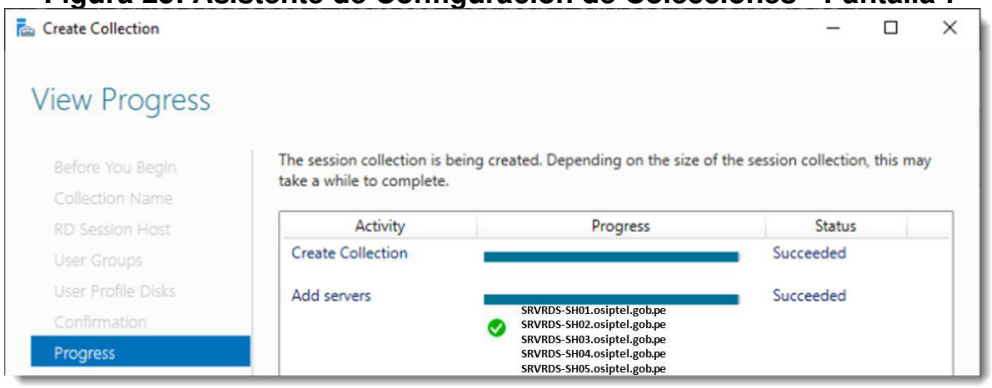
La sexta pantalla del asistente de configuración de colecciones muestra un breve resumen de las configuraciones realizadas hasta el momento.

Figura 24: Asistente de Configuración de Colecciones - Pantalla 6



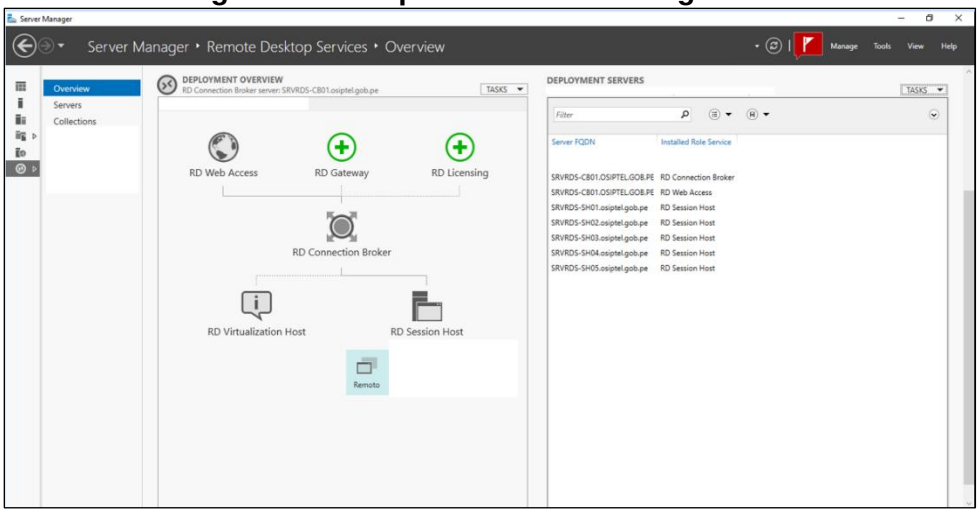
Finalmente, la séptima y última pantalla del asistente muestra el progreso en el despliegue de las configuraciones realizadas y notifica si estas se han realizado con éxito. Luego de esta última pantalla el asistente se cierra y se da por finalizada la labor.

Figura 25: Asistente de Configuración de Colecciones - Pantalla 7



Luego de finalizado el asistente, ya es posible visualizar la colección recién creada en el panel de administración del servidor, tal y como se aprecia en la imagen a continuación. Asimismo, ya es posible apreciar también, en el panel lateral, los servidores que conforman cada componente de la plataforma.

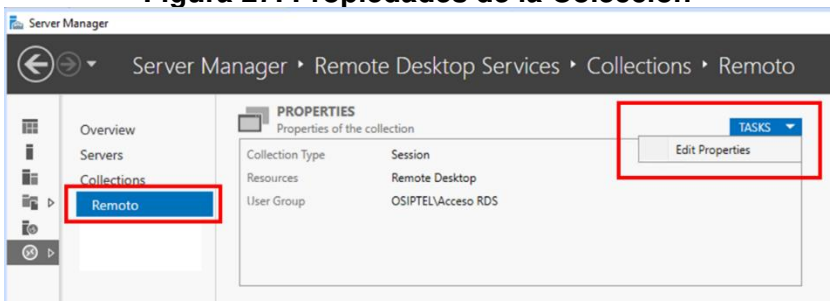
Figura 26: Componentes RDS configurados



Habiendo culminado el asistente, ya se tienen las bases de la Plataforma RDS configuradas: los componentes mínimos necesarios y los equipos que brindarán servicio a los usuarios. Ahora es necesario establecer las condiciones en las que se realizará la conexión de los usuarios, es decir, es necesario establecer los parámetros de las sesiones de trabajo de la colección creada.

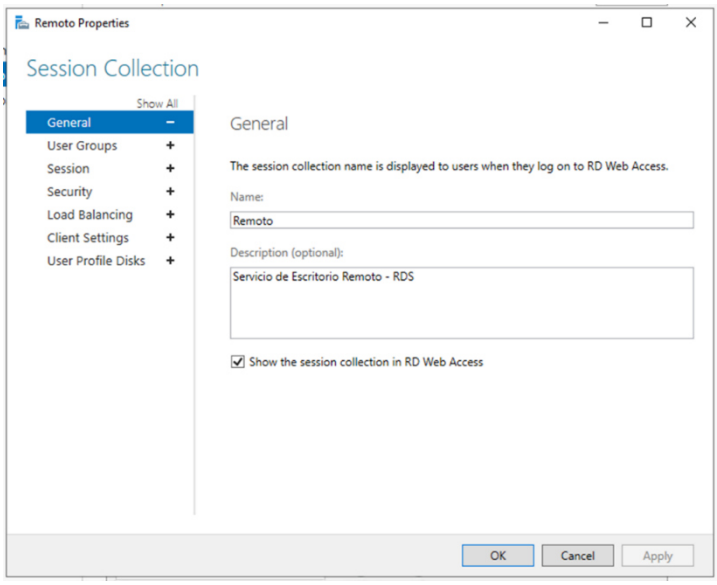
Para realizar la configuración de la colección recientemente creada se debe seleccionar la opción “Editar propiedades” (*Edit Properties*) dentro del menú “Tareas” (*Tasks*) en la interfaz de administración de la colección. La ubicación de los controles mencionados se muestra en la imagen a continuación. Luego de esto se abrirá el asistente de configuración respectivo.

Figura 27: Propiedades de la Colección



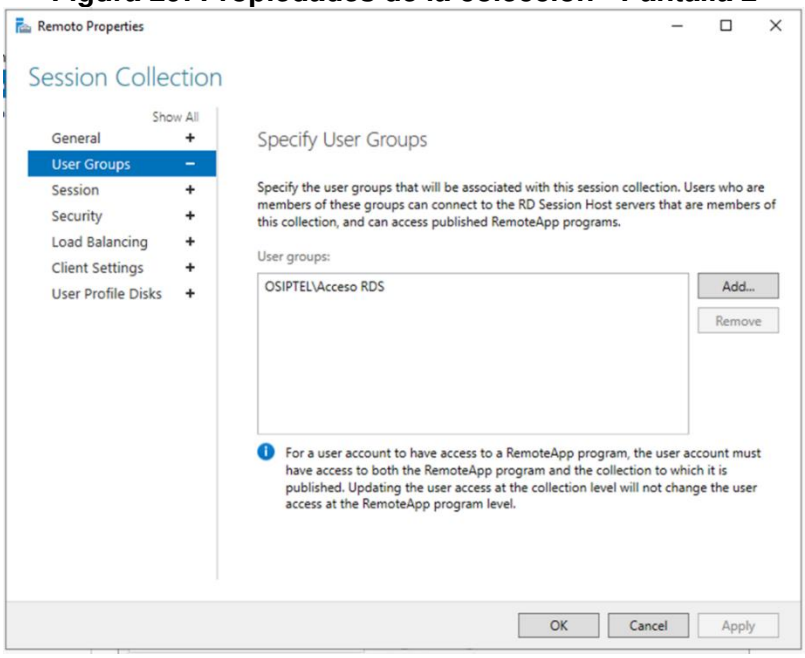
La primera pantalla del asistente de edición de propiedades de la colección muestra información que ya se ha ingresado previamente: el nombre de la colección y una descripción de esta, por lo cual no se harán cambios en esta interfaz.

Figura 28: Propiedades de la colección - Pantalla 1



La segunda pantalla del asistente de edición de propiedades de la colección muestra los grupos de usuarios con permisos de acceso a los recursos de la colección. Este parámetro también ha sido configurado previamente por lo cual tampoco se realizarán cambios en esta interfaz.

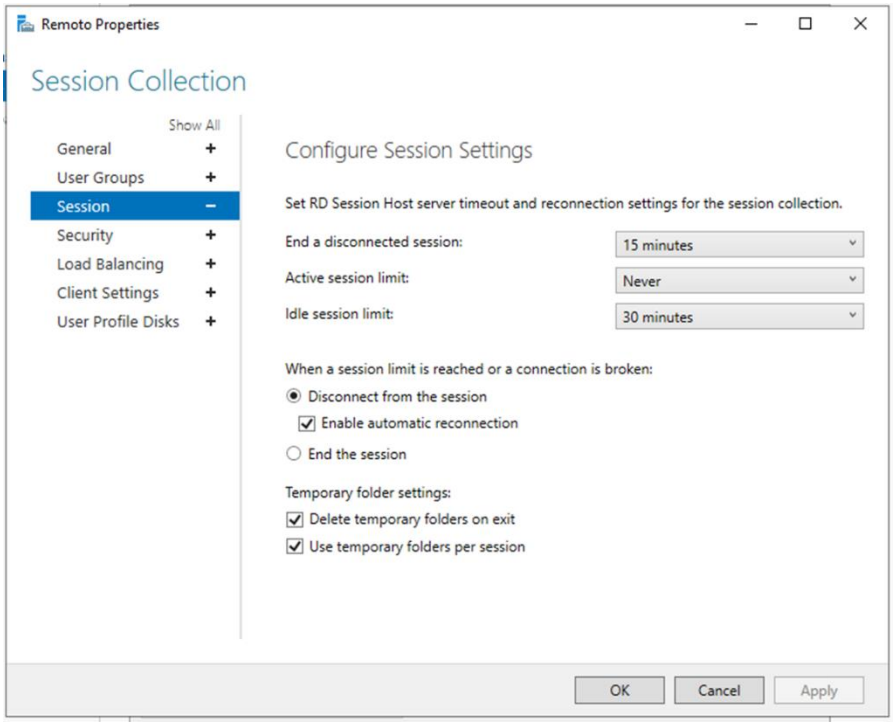
Figura 29: Propiedades de la colección - Pantalla 2



La tercera pantalla del asistente de edición de propiedades de la colección solicita ingresar los parámetros de la sesión de usuario, tal y como se muestra en la imagen a continuación. Al respecto se precisa los siguiente:

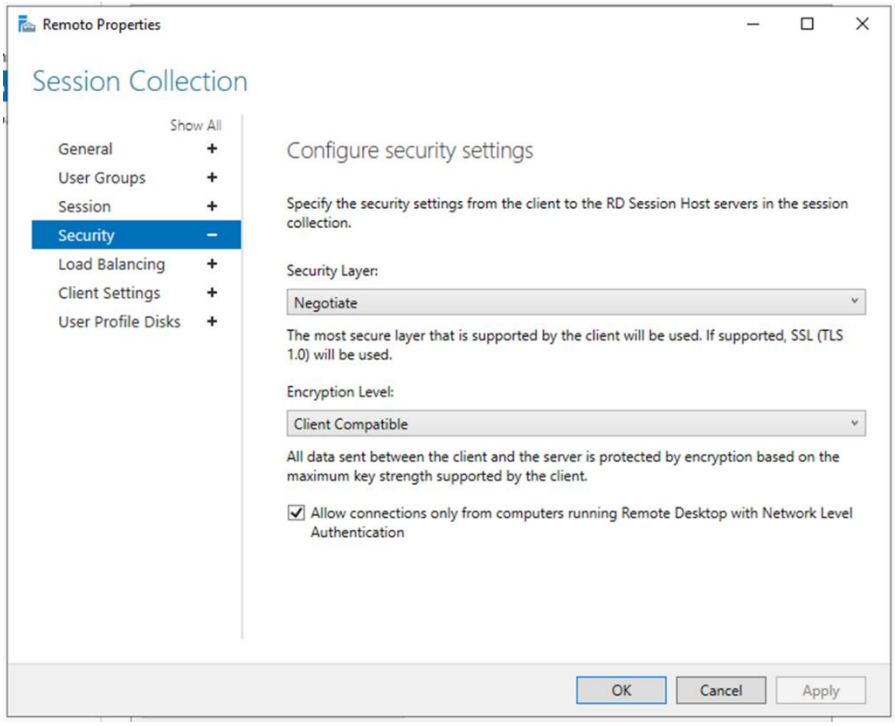
- Finalizar una sesión desconectada (*End a disconnected session*), es el parámetro que indicará después de cuanto tiempo se cerrará la sesión de trabajo del usuario en caso este abandone la conexión sin haber cerrado su sesión. En este caso se configura en 15 minutos. Es importante recalcar la importancia de cerrar las sesiones desconectadas puesto que continúan consumiendo recursos del sistema, aunque el usuario no esté haciendo uso de ellas.
- Límite de sesión activa (*Active session limit*), es el parámetro que indica cuanto tiempo, como máximo, puede durar activa la sesión de un usuario. En este caso no se pretende establecer limite de tiempo para la permanencia de los usuarios en la plataforma.
- Límite de sesión desatendida (*Idle session limit*), es el parámetro que indica cuanto tiempo puede permanecer desatendida (es decir, sin interacción del usuario) una sesión antes de ser cerrada automáticamente. Este parámetro se configura en 30 minutos.
- El siguiente apartado es “Cuando un límite de sesión es alcanzado o una conexión se rompe” (*When a session limit is reached or a connection is broken*) que nos pide indicar como debe responder el sistema en caso cuando se alcancen los limites antes establecidos o se pierda conexión con el usuario. Se habilita la opción “Desconectar de la sesión” (*Disconnect from the session*) y “Habilitar reconexión automática” (*Enable automatic reconnection*), con esto se logra que el usuario pueda retomar su sesión de trabajo en caso sufra una pérdida súbita de conexión.
- Finalmente se solicita indicar las “Propiedades de directorios temporales” (*Temporary folder settings*), en donde se ha habilitado “Eliminar directorios temporales al salir” (*Delete temporary folders on exit*) y “Usar directorios temporales por session” (*Use temporary folders per session*), con esto se logra que, cada vez que el usuario cierre sesión, se liberen los recursos de almacenamiento que estaba utilizando.

Figura 30: Propiedades de la colección - Pantalla 3



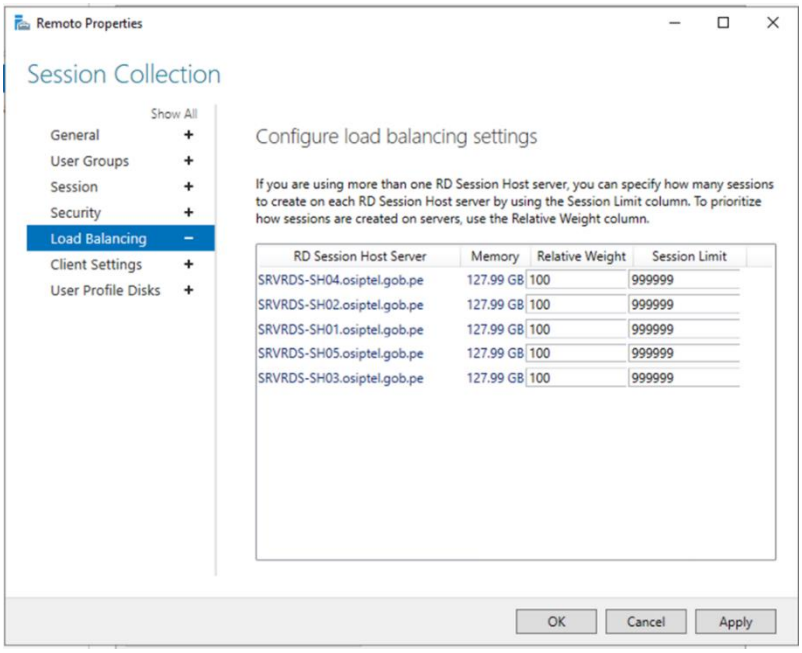
La cuarta pantalla del asistente de edición de propiedades de la colección muestra la configuración de seguridad de la conexión; en este apartado hay que tener en consideración que se busca tener compatibilidad con la mayor cantidad de equipos desde los que los usuarios pudiesen necesitar conectarse, por ello tanto la “Capa de Seguridad” (*Security Layer*) como el “Nivel de Encriptación” (*Encryption Level*) se establecen en condiciones de negociación.

Figura 31: Propiedades de la colección - Pantalla 4



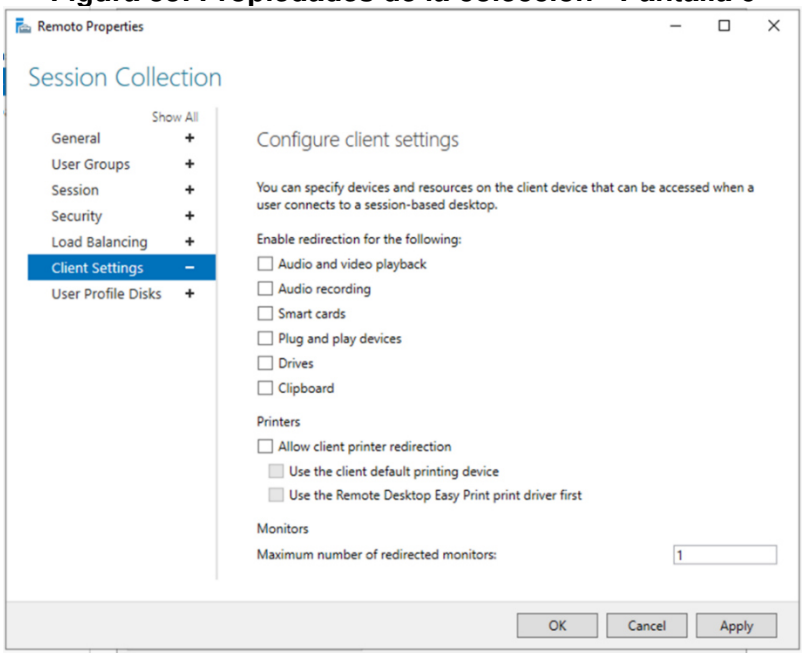
La quinta pantalla del asistente de edición de propiedades de la colección presenta la configuración para distribuir la carga entre los servidores del componente *Session Host*, esto es particularmente útil cuando se tiene infraestructura heterogénea y, por ende, se requiere que unos equipos asuman más o menos carga que otros, sin embargo, este no es el caso en el presente proyecto, por lo cual se configuran todos los equipos con el mismo peso específico, es decir, se distribuirá la carga de trabajo de manera uniforme entre los 5 equipos.

Figura 32: Propiedades de la colección - Pantalla 5



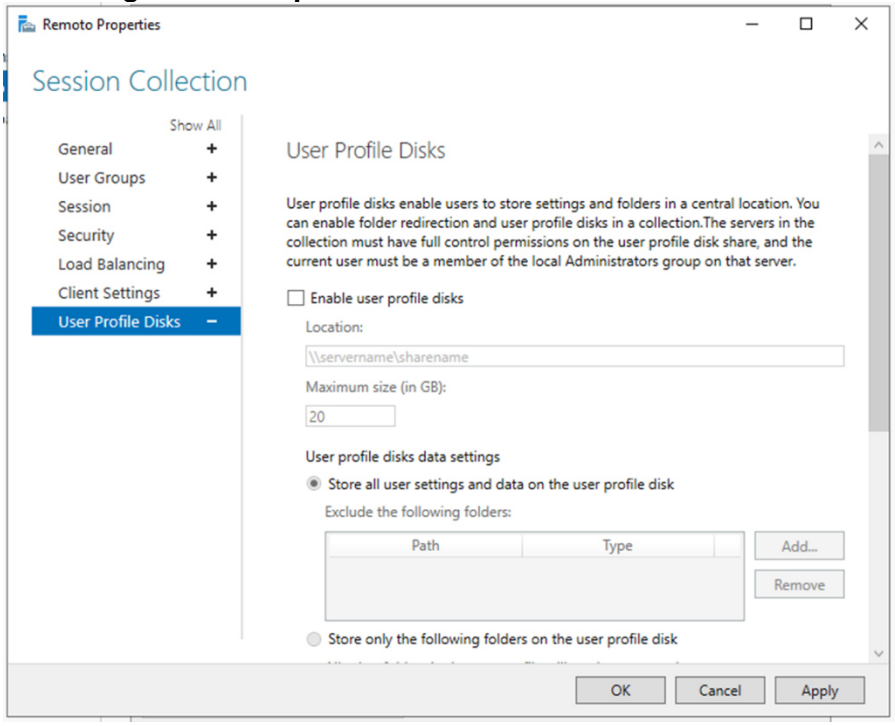
La sexta pantalla del asistente de edición de propiedades de la colección muestra los recursos que el cliente puede compartir con su sesión remota, por ejemplo, se puede permitir que el cliente comparta su equipo de impresión o su equipo de grabación de audio con su sesión de trabajo remoto. En este caso, por motivos de seguridad y desempeño, se restringe cualquier tipo de compartición de recurso entre el equipo cliente y la sesión remota del usuario.

Figura 33: Propiedades de la colección - Pantalla 6



Finalmente, la séptima pantalla del asistente de edición de propiedades de la colección muestra una configuración que ya se ha establecido previamente: la ubicación personalizada donde se guardarán los perfiles de los usuarios. Nuevamente, obviamos esta configuración y damos por terminado el asistente.

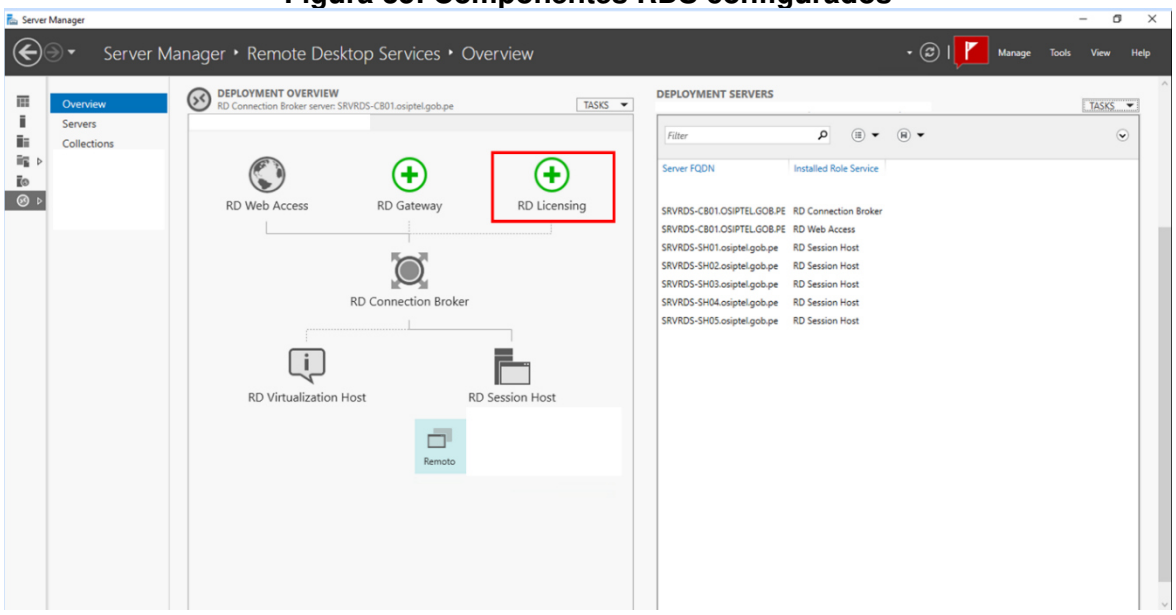
Figura 34: Propiedades de la colección - Pantalla 7



Con la finalización del asistente anterior, todos los componentes hasta ahora instalados están configurados y listos para operar; por lo cual es necesario continuar con la instalación de los dos últimos componentes restantes: *RD Licensing* y *RD Gateway*; el primero permite usar la plataforma de manera legal instalando las licencias de explotación respectivas y el segundo permite a la plataforma estar disponible a través de redes públicas.

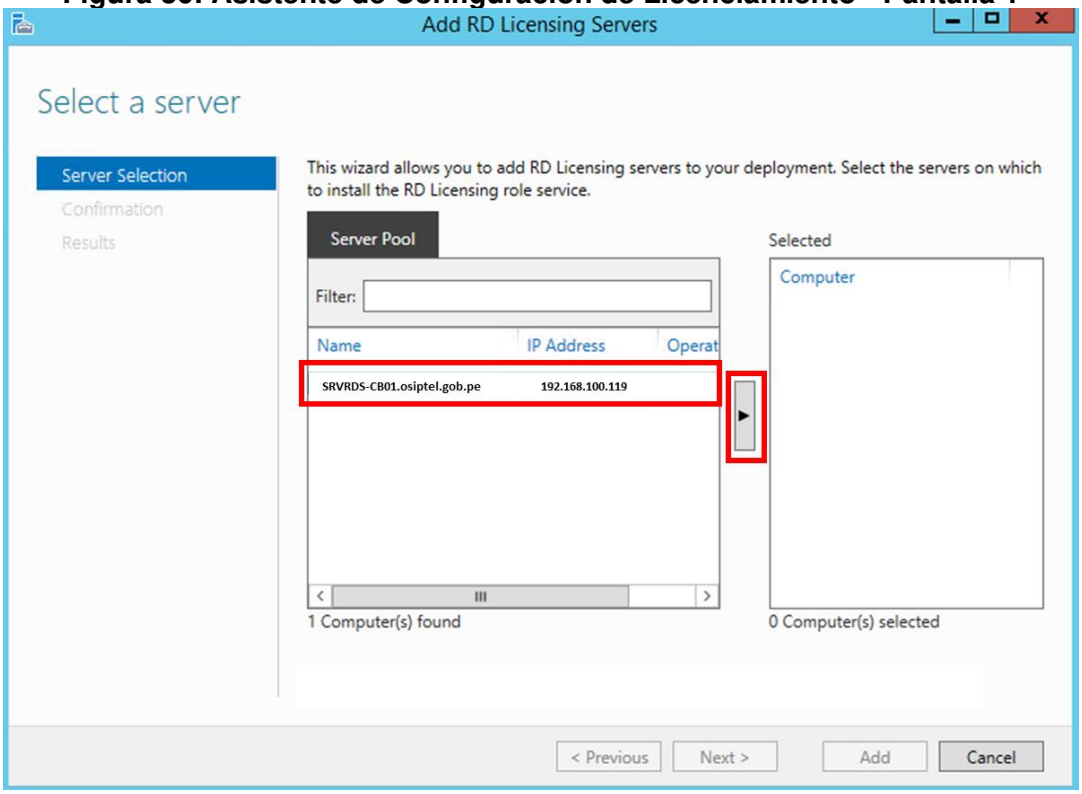
Para iniciar la instalación del componente *RD Licensing* es necesario volver al panel de administración del servidor y selección la alternativa *RD Licensing* en la vista previa del despliegue, tal y como muestra la imagen a continuación.

Figura 35: Componentes RDS configurados



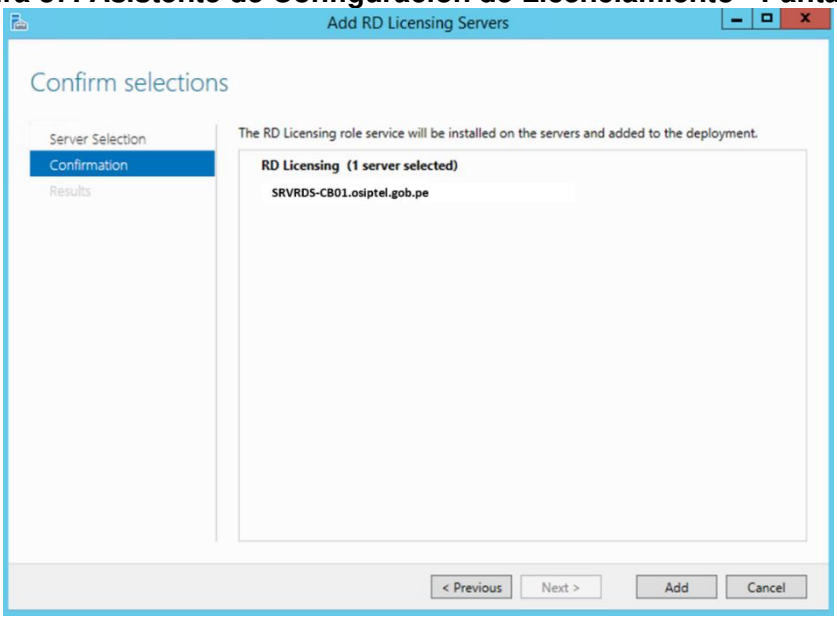
Esta acción abrirá el asistente de configuración del componente *RD Licensing* que se muestra en la imagen a continuación. Únicamente es necesario selecciona el servidor que asumirá el componente de licenciamiento, como ya se ha establecido previamente, será el servidor *SRVRDS-CB01*.

Figura 36: Asistente de Configuración de Licenciamiento - Pantalla 1



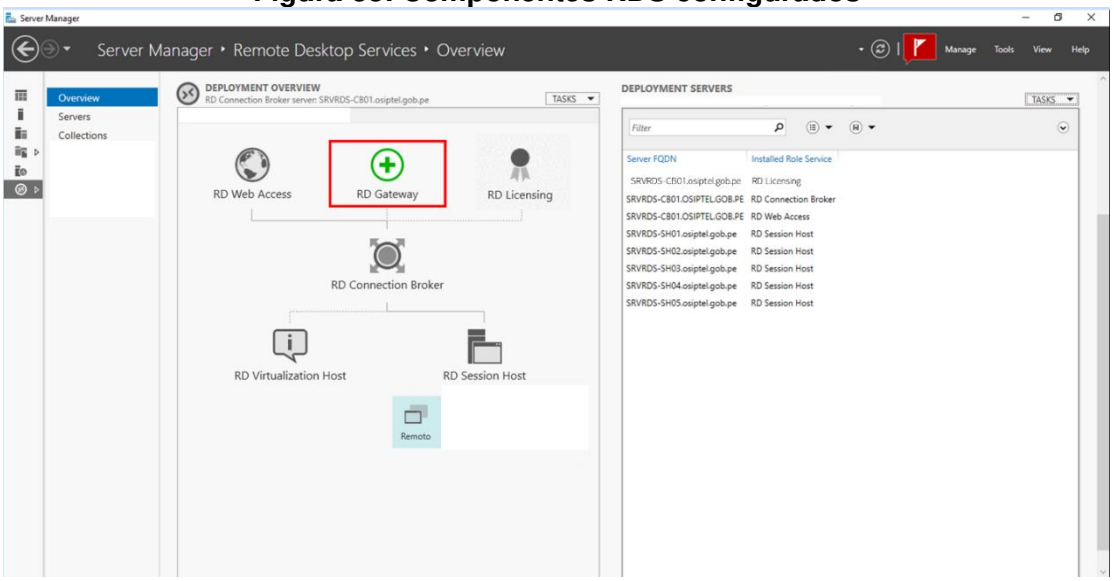
La segunda pantalla del asistente es solo una confirmación antes del despliegue del componente *RD Licensing*, como se muestra en la imagen siguiente. Luego de esto, el asistente finaliza.

Figura 37: Asistente de Configuración de Licenciamiento - Pantalla 2



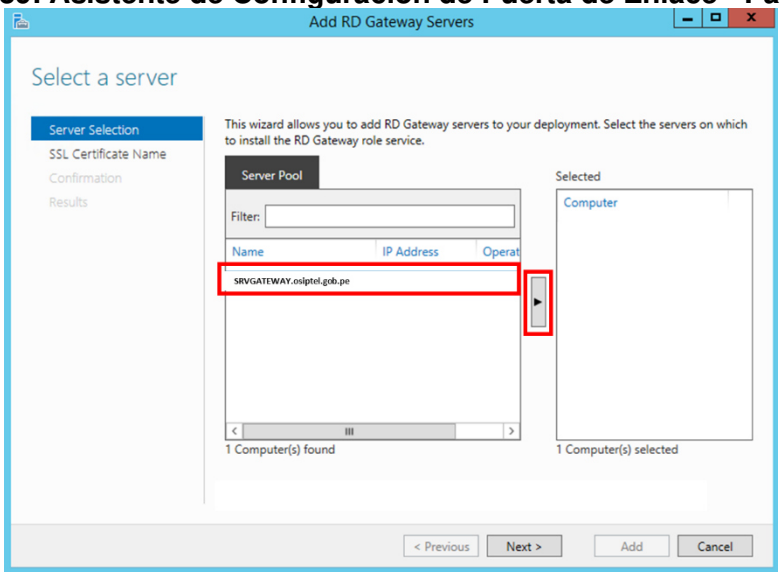
Luego de culminado el asistente, ya es posible visualizar el componente *RD Licensing* en el panel de administración del servidor, tal y como se aprecia en la imagen a continuación. Ahora es necesario selección la opción *RD Gateway* para proceder con la instalación del último componente.

Figura 38: Componentes RDS configurados



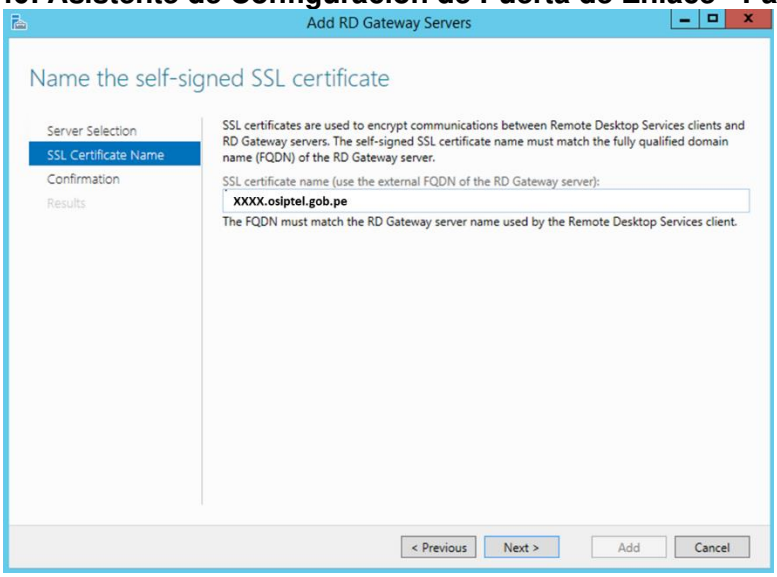
Esto abre un nuevo asistente de configuración, como se aprecia en la imagen siguiente, en el cual debemos selección el servidor que contendrá al componente *RD Gateway*, en este caso, como se ha mencionado antes será el equipo *SRVGATEWAY*.

Figura 39: Asistente de Configuración de Puerta de Enlace - Pantalla 1



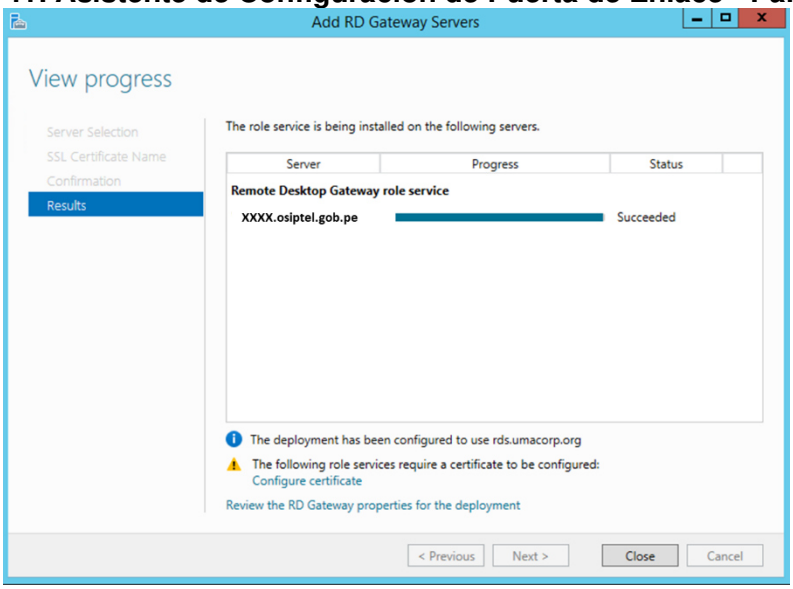
En la segunda pantalla del asistente de configuración se debe introducir el nombre público que tendrá el componente *Gateway*, es decir, el nombre con el que los usuarios en internet podrán encontrarlo; es preciso mencionar que este nombre debe coincidir con el nombre del certificado digital del que se disponga.

Figura 40: Asistente de Configuración de Puerta de Enlace - Pantalla 2



Finalmente, se culmina la instalación en la ultima pantalla del asistente y el componente *RD Gateway* queda instalado en el servidor.

Figura 41: Asistente de Configuración de Puerta de Enlace - Pantalla 3



Con la instalación del componente RD Gateway, y su respectiva configuración, ya se tienen adecuadamente instalados y configurados todos los elementos de la Plataforma RDS planificada en la fase previa. Es ahora necesario evaluar si la implementación satisface las necesidades de los colaboradores.

3.2.5.5 Fase 5: Seguimiento y Optimización

Luego de culminada la fase de implementación de la Plataforma RDS se iniciaron las pruebas de conectividad, desempeño y funcionalidad.

En las pruebas de conectividad se validó que los colaboradores podían conectarse desde sus hogares a la plataforma RDS y que esta los autenticaba correctamente.

En las pruebas de desempeño se validó que las conexiones de los colaboradores se distribuían de manera uniforme entre todos los *Session Host* de la plataforma RDS y que estos eran capaces de soportar la carga de trabajo de todos los colaboradores.

En las pruebas de funcionalidad se validó que la Plataforma RDS fuese capaz de otorgar a los colaboradores todos los servicios digitales que estos necesitaban para el normal desempeño de sus labores (repositorios documentales, aplicativos del sector gobierno, aplicativos institucionales, entre otros).

CAPÍTULO IV
REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

El autor del presente informe tuvo la oportunidad de participar como líder de proyecto en la implementación de la plataforma de trabajo remoto para el OSIPTEL basada en la arquitectura Microsoft RDS en el marco de la emergencia sanitaria por COVID-19.

El inicio del proyecto se dio en una coyuntura bastante convulsa debido a lo desconocido que resultaba para todos los actores el contexto de una emergencia sanitaria y cuarentena obligatoria, es por ello por lo que, desde el primer momento, fue necesaria una toma de decisiones rápida y un marco de trabajo que priorizase el avance en la ejecución por sobre otras actividades como el seguimiento documental o la coordinación entre diversas unidades de negocio.

Al respecto, fue un factor crítico de éxito el dotar al personal a cargo del proyecto de la capacidad de tomar todas las decisiones respecto a la evaluación de alternativas, los mecanismos de implementación, la explotación de los recursos disponibles y demás actividades descritas en el presente; es probable que, de no haber sido así, es decir, de haber seguido un flujo de trabajo más tradicional en una institución pública (con abundante documentación preliminar antes de cada decisión, coordinaciones y validaciones entre unidades de negocio, entre otras actividades que forman parte de la burocracia cotidiana en el sector) no se hubiese logrado el objetivo de contar con la plataforma en operación en un tiempo tan corto: menos de 7 días.

Finalmente, es pertinente mencionar que el objetivo más importante de todos, servir al ciudadano, se pudo seguir cumpliendo durante el periodo de emergencia sanitaria gracias a la puesta en producción de la Plataforma RDS descrita en el presente documento; ese simple hecho ya es suficiente para calificar el proyecto como exitoso pues el bienestar de la ciudadanía es el fin último de todo organismo público incluido, por supuesto, el OSIPTEL.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El proyecto descrito en el presente documento logró que se pusiese a disposición de los colaboradores del OSIPTEL una plataforma que les permitió continuar desarrollando sus labores de forma remota en el contexto de las restricciones de movilidad debido a la emergencia sanitaria por COVID-19 en el Perú.

Mediante la implementación de tecnologías contrastadas y respaldadas en el mercado (como lo es la arquitectura RDS de *Microsoft*) se logró construir una plataforma de trabajo remoto de fácil utilización, segura, escalable y robusta capaz de atender las exigencias de todo el conjunto de colaboradores de la institución.

5.2 Recomendaciones

Se debería enfocar las recomendaciones como oportunidades de mejora a corto-mediano plazo y a mediano- largo plazo.

En el corto-mediano plazo, se debe garantizar la continuidad operativa como objetivo primordial, para ello es necesario realizar revisiones periódicas que abarquen todas las capas técnicas de la plataforma implementada: el hardware, por ejemplo, es pertinente recordar que se utilizó aquel que estaba disponible por estar fuera de operaciones, sin embargo, este componente hardware se encuentra tecnológicamente desfazado y podría presentar inconvenientes en su funcionamiento. Asimismo, el software; si bien se utilizaron versiones modernas de los sistemas operativos instalados, es oportuno recordar que estos se deben actualizar constantemente a fin de evitar crear brechas de seguridad o mermas en el rendimiento. Finalmente, el monitoreo constante de la plataforma es absolutamente necesario toda vez que, mientras se mantengan las medidas sanitarias extraordinarias y el trabajo remoto, los usuarios tienen libertad de elegir los horarios de trabajo que mejor se adapten a su gestión del tiempo.

Por otra parte, para abordar las recomendaciones en el mediano-largo plazo es necesario comprender que la implementación realizada en el presente proyecto se realizó en un contexto muy particular, un contexto de recursos (técnicos, tecnológicos, temporales y humanos) muy limitados y una alta exigencia; por ello, en el largo plazo debiese considerarse 2 factores: nuevas tecnologías y planificación meticulosa. Respecto a las nuevas tecnologías, tenemos ejemplos como el *DaaS* (*Desktop As A Service*) propuesto por el mismo fabricante/desarrollador *Microsoft* y que, sobre simplificándolo, se trata de una implementación RDS con infraestructura totalmente en nube, lo que disminuye drásticamente los tiempos de implementación y gestión a los equipos técnicos, a la vez que brinda a los usuarios un servicio independiente de la conexión a internet de la organización. Respecto a la planificación meticulosa, es necesario recordar que toda migración de tecnología debiese buscar generar el menor impacto posible sobre el usuario, en especial cuando este se encarga de brindar un servicio al ciudadano; por ello, debiese planificarse con antelación, participación de todos los actores y, sobre todo, la debida concientización, las acciones a tomar para migrar la plataforma implementada a un nuevo entorno o una nueva tecnología.

Bibliografía

Asimane, A. (2017). *Servicios RDS de Windows Server 2016.* Éditions ENI.

Microsoft. (01 de Diciembre de 2021). *Microsoft Official Web Site*. Obtenido de Welcome to Remote Desktop Services: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds

Portal Web Institucional del OSIPTEL. (01 de Diciembre de 2021). Obtenido de Portal Web Institucional del OSIPTEL: https://www.osiptel.gob.pe

Rath , M. (01 de Diciembre de 2021). *Marcus Rath's Personal Blog*. Obtenido de SSO Single-Sign-On to your onPremise RDS Remote Desktop Services 2016/2019 Environment: https://blog.matrixpost.net/sso-single-sign-on-to-your-onpremise-rds-remote-desktop-services-2016-2019-environment/

Roseth, B., Reyes, A., & Amé, K. (01 de Diciembre de 2021). *SERVICIOS PÚBLICOS Y GOBIERNO DIGITAL DURANTE LA PANDEMIA.* Obtenido de SERVICIOS PÚBLICOS Y GOBIERNO DIGITAL DURANTE LA PANDEMIA: https://publications.iadb.org/publications/spanish/document/Servicios-publicos-y-gobierno-digital-durante-la-pandemia-Perspectivas-de-los-ciudadanos-los-funcionarios-y-las-instituciones-publicas.pdf