

**UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E
INFORMÁTICA**



TESIS

“Implementación de una plataforma segura de aplicaciones y escritorios virtuales para mejorar el trabajo remoto en el Ministerio de Defensa, 2023”

AUTOR(ES):

Bach. Castillo Yarlequé, Javier Francisco

Bach. Pineda Becerra, Jorge Guillermo

**PARA OPTAR EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas e Informática**

ASESOR:

Mg. Corilla Baquerizo, Eduardo Cancio

ORCID: 0000-0003-3472-2696

DNI N°: 20037930

**LIMA - PERÚ
2024**

INFORME DE SIMILITUD



UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

Facultad de Ciencias e Ingeniería

INFORME DE SIMILITUD N° 067-2024-FCI-UPCI-T-ECCB

A : **MG. JHONY RECHER JARA CABALLERO**
Decano (e) de la Facultad de Ciencias e Ingeniería

DE : **MG. EDUARDO CANCIO CORILLA BAQUERIZO**

ASUNTO : Informe de Evaluación de Similitud de Tesis

FECHA : Jesús María, 15 de noviembre del 2024

Tengo el agrado de dirigirme a Ud. a fin de informar lo siguiente:

1. Mediante el uso del programa informático TURNITIN (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 15 palabras) se ha analizado la tesis titulada: **"Implementación de una plataforma segura de aplicaciones y escritorios virtuales para mejorar el trabajo remoto en el Ministerio de Defensa, 2023"**, presentado por el (los) Br (es):

Bach. Castillo Yarlequé, Javier Francisco

Bach. Pineda Becerra, Jorge Guillermo

2. El resultado de la evaluación indica que la tesis en mención tiene un INDICE DE SIMILITUD DE 8% (cumpliendo con el art. 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019)
3. Al término del análisis, se concluye que PUEDE(N) CONTINUAR su trámite.

Sin otro particular quedo de usted.

Atentamente

Mg. Eduardo Cancio Corilla Baquerizo
DOCENTE UPCI

PD:

Se adjunta:

- Recibo digital Turnitin
- Resultado de similitud

DEDICATORIA

A ti, mamá, por tu amor incondicional, tu apoyo y tu fortaleza. Gracias por ser mi pilar y por siempre creer en mí. Este logro es en gran parte gracias a ti, a tu sacrificio y dedicación. A ti, papá, aunque ya no estés físicamente a mi lado, siento tu presencia en cada paso que doy. Siempre me enseñaste la importancia del esfuerzo, la disciplina y la honestidad.

A ti, abuelo, que también ya no estás con nosotros, pero cuya sabiduría y amor siguen vivos en mi corazón. Gracias por las lecciones de vida que me diste y por siempre apoyarme.

A mi esposa, mi compañera de vida, por tu amor, paciencia y comprensión. A mi hija, mi razón de ser y de seguir adelante. Tu sonrisa y alegría son el faro que ilumina mi camino. Este logro es también para ti, con la convicción de que sigas persiguiendo tus sueños con la misma pasión.

Bach. Castillo Yarlequé, Javier Francisco.

A ti, mamá, quien con tu amor y sacrificio me enseñaste a ser fuerte y a nunca rendirme. A ti, papá, quien, aunque ya no me acompañas en este camino, tu legado sigue siendo mi mayor motivación. Gracias a ustedes por todas las enseñanzas que me dejaron, por el amor y la disciplina con que formaron mi vida. Este título también es un tributo a ustedes, por todo lo que hicieron por mí y por todo lo que me enseñaron.

Bach. Pineda Becerra, Jorge Guillermo

AGRADECIMIENTO

Quiero expresar mi más sincero y profundo agradecimiento a todas las personas que me han acompañado y apoyado a lo largo de este proceso, sin cuyo respaldo esta tesis no habría sido posible.

A mi madre, por su amor incondicional, su paciencia y su fortaleza. Su ejemplo de vida y su apoyo constante me han dado la fuerza necesaria para seguir adelante, incluso en los momentos más difíciles. A ella le dedico este logro, pues sin su guía, este camino no hubiera sido el mismo.

A mi padre, quien ya no está entre nosotros, pero cuya presencia sigue viva en cada uno de mis pensamientos y decisiones. A mi amado abuelo, quien también nos dejó, pero cuya influencia sigue guiando mi vida.

Finalmente, a mi asesor, el Mg. Corilla Baquerizo Eduardo Cancio, por su orientación, apoyo académico y profesional durante todo este proceso.

Bach. Castillo Yarlequé, Javier Francisco.

A mi madre, quien lamentablemente ya no está entre nosotros, pero cuyo amor y sabiduría siguen guiando mis pasos cada día. Ella fue mi mayor fuente de fortaleza, y su ejemplo de sacrificio, dedicación y amor incondicional ha sido mi mayor motor. A mi padre, también fallecido, a quien agradezco por su apoyo inquebrantable a lo largo de mi vida. Aunque su ausencia física es dolorosa, su legado de esfuerzo, responsabilidad y principios sigue siendo una constante en mi camino.

A mi asesor, el Mg. Corilla Baquerizo Eduardo Cancio, por su valioso apoyo académico y humano durante todo este proceso.

Bach. Pineda Becerra, Jorge Guillermo

PRESENTACIÓN

Señores miembros del jurado, en cumplimiento del “Reglamento de Grado de Bachiller y Título Profesional de la Universidad Peruana de Ciencias e Informática, aprobado por Resolución N° 373-2019-UPCI-R; y en estricto cumplimiento del requisito establecido por el “Artículo N° 45, ley N° 30220”; donde se indica los requisitos para la obtención de grados y títulos, es de acuerdo a las exigencias académicas que cada universidad establezca, presentamos ante ustedes nuestra tesis titulada “Implementación de una plataforma segura de aplicaciones y escritorios virtuales para mejorar el trabajo remoto en el Ministerio de Defensa, 2023”, la cual será puesto a vuestra consideración, evaluación y juicio profesional; para su aprobación y esta nos conlleve a ostentar el título profesional de Ingeniero de Sistemas e Informática.

Bach. Castillo Yarlequé, Javier Francisco

Bach. Pineda Becerra, Jorge Guillermo

ÍNDICE

CARÁTULA.....	i
INFORME DE SIMILITUD	ii
DEDICATORIA	iii
AGRADECIMIENTO	iv
PRESENTACIÓN	v
ÍNDICE	vi
ÍNDICE DE TABLAS	viii
ÍNDICE DE FIGURAS.....	ix
RESUMEN.....	x
ABSTRACT	xi
I. INTRODUCCION	12
1.1. Realidad problemática.....	12
1.2. Planteamiento del problema	22
1.3. Hipótesis de la investigación	22
1.4. Objetivos de la investigación	23
1.5. Variables, dimensiones e indicadores	23
1.6. Justificación del estudio	25
1.7. Antecedentes nacionales e internacionales	30
1.7.1. Antecedentes internacionales	30
1.7.2. Antecedentes nacionales	32
1.8. Marco teórico.....	34
1.8.1. Sistema de información	34
1.8.2. Trabajo remoto	38
1.9. Definición de términos básicos.....	40
II. METODO	43
2.1. Tipo y diseño de la investigación.....	43
2.2. Población y muestra	44
2.3. Técnicas para la recolección de datos	45
2.4. Validez y confiabilidad de instrumentos.....	46
2.5. Procesamiento y análisis de datos	47
2.6. Aspectos éticos.....	48
III. RESULTADOS.....	49
3.1. Resultados descriptivos	49
3.2. Prueba de normalidad.....	57
3.3. Contrastación de las hipótesis.....	58

IV. DISCUSION	62
V. CONCLUSIONES	64
VI. RECOMENDACIONES	65
IV. REFERENCIAS BIBLIOGRÁFICAS	66
ANEXOS.....	70
Anexo 01: Matriz de Consistencia	70
Anexo 02: Instrumento de recolección de datos.....	71
Anexo 03: Base de datos	75
Anexo 04: Evidencia de similitud digital	96
Anexo 05: Autorización de publicación en repositorio.....	98
Anexo 06: Implementación de la solución	100
Procedimiento de instalación de CITRIX ADC (NETSCALER).....	133
Procedimiento configuración de CITRIX ADC (NETSCALER)	136
Procedimiento instalación de Citrix delivery controller	151
Procedimiento configuración de Citrix delivery controller.....	161
Procedimiento de instalación de Citrix applications server	190
Procedimiento configuración de rsa authentication manager.....	216
Procedimiento de asignación de Token RSA al usuario autorizado	224
Procedimiento de acceso al entorno virtual de teletrabajo	232

ÍNDICE DE TABLAS

Tabla 1. Incidentes de seguridad año 2022	20
Tabla 2. Incidentes incidentes año 2023	20
Tabla 3. Tipos de eventos de seguridad	21
Tabla 4. Operacionalización de variables	24
Tabla 5. <i>Juicio de Expertos</i>	46
Tabla 6. <i>Análisis de fiabilidad</i>	47
Tabla 7. <i>Frecuencia de la variable plataforma de aplicaciones seguras y escritorios virtuales</i>	49
Tabla 8. <i>Frecuencia de la dimensión tecnología y herramientas de comunicación</i>	50
Tabla 9. <i>Frecuencia de la dimensión seguridad y acceso a la información</i>	51
Tabla 10. <i>Frecuencia de la dimensión infraestructura de trabajo remoto</i>	52
Tabla 11. <i>Frecuencia de la variable plataforma de aplicaciones seguras y escritorios virtuales</i>	53
Tabla 12. <i>Frecuencia de la dimensión tecnología y herramientas de comunicación</i>	54
Tabla 13. <i>Frecuencia de la dimensión seguridad y acceso a la información</i>	55
Tabla 14. <i>Frecuencia de la dimensión infraestructura de trabajo remoto</i>	56
Tabla 15. <i>Prueba de normalidad</i>	57
Tabla 16. <i>Contrastación de la hipótesis general</i>	58
Tabla 17. <i>Contrastación hipótesis específica 1</i>	59
Tabla 18. <i>Contrastación hipótesis específica 2</i>	60
Tabla 19. <i>Contrastación de la hipótesis específica 3</i>	61
Tabla 20. Matriz de consistencia	70

ÍNDICE DE FIGURAS

Figura 1. Diagrama de una Red Privada Virtual, del tipo Client-to-Site	18
Figura 2. Diagrama de pareto de los incidentes de seguridad	21
Figura 3. Frecuencia de la variable plataforma de aplicaciones seguras y escritorios virtuales	49
Figura 4. <i>Frecuencia de la dimensión tecnología y herramientas de comunicación.</i>	50
Figura 5. <i>Frecuencia de la dimensión seguridad y acceso a la información.</i>	51
Figura 6: <i>Frecuencia de la dimensión infraestructura de trabajo remoto.</i>	52
Figura 7. <i>Frecuencia de la variable plataforma de aplicaciones seguras y escritorios virtuales.</i>	53
Figura 8. <i>Frecuencia de la dimensión tecnología y herramientas de comunicación</i>	54
Figura 9. <i>Frecuencia de la dimensión seguridad y acceso a la información.</i>	55
Figura 10: <i>Frecuencia de la dimensión infraestructura de trabajo remoto.</i>	56

RESUMEN

El trabajo de investigación tuvo como objetivo principal “Explicar la implementación de una plataforma segura de aplicaciones y escritorios virtuales en la mejora del trabajo remoto en el MINDEF, 2023”.

Para lo cual se aplicó la siguiente metodología, el tipo de investigación fue aplicada, el diseño experimental, pre experimental, el nivel descriptivo explicativa y finalmente el enfoque de la investigación cuantitativo, ya que se utilizó la prueba de los rangos con signo de Wilcoxon para la prueba de hipótesis; Así mismo se utilizó la técnica de la encuesta y su instrumento de recolección de datos fue el cuestionario. La población estuvo constituida por 400 usuarios y la muestra fue la misma de la población.

Se aplicó el coeficiente de alfa de Cronbach para el análisis de fiabilidad, donde se tuvo en resultado de 0,723, superior al mínimo aceptable de 0.7.

En los resultados obtenidos, se puede observar de la prueba de los rangos con signo de Wilcoxon, de los totales del pre-test y post-test el $P = 0.000$ es $< a 0.05$, entonces se rechaza la H_0 y aceptamos la H_1 . Si, se implementa una plataforma segura de aplicaciones y escritorios virtuales entonces mejora del trabajo remoto en el MINDEF, 2023.

Palabras clave: Acceso a la información, Aplicaciones, Escritorios virtuales, Infraestructura, Plataforma segura, Software, Trabajo remoto, Virtualización.

ABSTRACT

The main objective of the research work was “To explain the implementation of a secure platform for virtual applications and desktops in improving remote work at MINDEF, 2023”.

For this, the following methodology was applied, the type of research was applied, the experimental, pre experimental design, the descriptive explanatory level and finally the quantitative research approach, since the Wilcoxon signed rank test was used for the hypothesis test; Likewise, the survey technique and its data collection instrument, the questionnaire, were used. The population consisted of 400 users and the sample was the same as the population.

The Cronbach's alpha coefficient was applied for the reliability analysis, where the result was 0.723, higher than the minimum acceptable value of 0.7.

In the results obtained, it can be observed from the Wilcoxon signed rank test, of the pre-test and post-test totals that $P = 0.000$ is < 0.05 , then H_0 is rejected and H_1 is accepted. If a secure platform for virtual applications and desktops is implemented, then remote work will improve at MINDEF, 2023.

Keywords: Access to information, Applications, Virtual desktops, Infrastructure, Secure platform, Software, Remote work, Virtualization.

I. INTRODUCCION

1.1. Realidad problemática

La adopción masiva del trabajo remoto, impulsada en gran medida por la pandemia de COVID-19, ha puesto de manifiesto la importancia crítica de las plataformas seguras de aplicaciones y escritorios virtuales. Sin embargo, su implementación a gran escala ha generado una serie de desafíos y problemáticas que requieren atención.

Seguridad

Ataques cibernéticos: El aumento del perímetro de seguridad debido al trabajo remoto ha incrementado la vulnerabilidad a ciberataques, como phishing, ransomware y malware.

Pérdida de dispositivos: La pérdida o robo de dispositivos personales utilizados para acceder a redes corporativas representa un riesgo significativo para la seguridad de los datos.

Acceso no autorizado: La dificultad de controlar el acceso a los recursos de la empresa desde múltiples ubicaciones y dispositivos aumenta el riesgo de acceso no autorizado.

Desempeño

Latencia: La distancia entre el usuario y el servidor puede causar latencia, lo que afecta la experiencia del usuario y la productividad.

Ancho de banda: La demanda de ancho de banda puede superar la capacidad de las redes domésticas, especialmente en áreas con infraestructura de red limitada.

Calidad de servicio: La calidad de la conexión a Internet puede variar significativamente, lo que afecta la estabilidad y el rendimiento de las aplicaciones.

Gestión

Complejidad: La gestión de un gran número de dispositivos y usuarios remotos puede ser compleja y requiere de herramientas y procesos especializados.

Actualizaciones: Mantener actualizadas las aplicaciones y sistemas operativos en múltiples dispositivos puede ser un desafío logístico.

Soporte técnico: Brindar soporte técnico a usuarios remotos puede ser más difícil y costoso que en un entorno de oficina tradicional.

Experiencia del usuario

Usabilidad: La interfaz de usuario de las plataformas de escritorio virtual puede no ser tan intuitiva como la de una computadora local, lo que puede afectar la productividad.

Integración de aplicaciones: La integración de diferentes aplicaciones y servicios puede ser compleja y requerir de configuraciones específicas.

Implicaciones a nivel mundial

Desigualdad digital: El acceso a internet de alta velocidad y dispositivos adecuados no es equitativo en todo el mundo, lo que limita la capacidad de muchos trabajadores para participar en el trabajo remoto.

Impacto en la economía: Los problemas de seguridad y desempeño pueden generar pérdidas financieras significativas para las empresas.

Riesgos para la privacidad: La gestión inadecuada de los datos personales puede dar lugar a violaciones de la privacidad y a sanciones legales.

Cambios en los modelos de trabajo: El trabajo remoto está transformando fundamentalmente la forma en que las empresas operan, lo que requiere una adaptación de las políticas y las prácticas laborales.

La adopción masiva del trabajo remoto en América ha puesto de manifiesto una serie de desafíos y oportunidades relacionadas con las plataformas seguras de aplicaciones y escritorios virtuales. A continuación, se detallan las principales problemáticas y sus implicaciones para las empresas y los trabajadores en la región:

Desafíos específicos de américa latina

Brecha digital: La desigualdad en el acceso a internet de alta velocidad y dispositivos adecuados es más pronunciada en América Latina, lo que limita la capacidad de muchos trabajadores para utilizar eficazmente las plataformas de trabajo remoto.

Infraestructura tecnológica: La infraestructura tecnológica en muchas regiones de América Latina puede ser insuficiente para soportar el aumento de la demanda de servicios en la nube y el acceso remoto.

Cultura organizacional: La transición al trabajo remoto puede ser más desafiante en culturas organizacionales más jerárquicas y menos acostumbradas a la flexibilidad laboral.

Seguridad cibernética: Las amenazas cibernéticas son cada vez más sofisticadas y las empresas latinoamericanas pueden carecer de los recursos necesarios para proteger sus sistemas y datos.

Problemáticas comunes a nivel mundial

Seguridad de la información

Ataques cibernéticos: El aumento del perímetro de seguridad debido al trabajo remoto ha incrementado la vulnerabilidad a ciberataques.

Pérdida de dispositivos: La pérdida o robo de dispositivos personales utilizados para acceder a redes corporativas representa un riesgo significativo.

Acceso no autorizado: La dificultad de controlar el acceso a los recursos de la empresa desde múltiples ubicaciones aumenta el riesgo de acceso no autorizado.

Desempeño

Latencia: La distancia entre el usuario y el servidor puede causar latencia, lo que afecta la experiencia del usuario y la productividad.

Ancho de banda: La demanda de ancho de banda puede superar la capacidad de las redes domésticas, especialmente en áreas con infraestructura de red limitada.

Gestión

Complejidad: La gestión de un gran número de dispositivos y usuarios remotos puede ser compleja y requiere de herramientas y procesos especializados.

Actualizaciones: Mantener actualizadas las aplicaciones y sistemas operativos en múltiples dispositivos puede ser un desafío logístico.

Soporte técnico: Brindar soporte técnico a usuarios remotos puede ser más difícil y costoso que en un entorno de oficina tradicional.

Experiencia del usuario

Usabilidad: La interfaz de usuario de las plataformas de escritorio virtual puede no ser tan intuitiva como la de una computadora local, lo que puede afectar la productividad.

Integración de aplicaciones: La integración de diferentes aplicaciones y servicios puede ser compleja y requerir de configuraciones específicas.

Implicancias para las empresas

Costos: La inversión en infraestructura, software y capacitación puede ser significativa.

Productividad: Los problemas de conectividad y seguridad pueden afectar la productividad de los empleados.

Riesgo reputacional: Una violación de datos puede dañar la reputación de la empresa y generar pérdidas financieras.

Adaptación cultural: Las empresas deben adaptarse a una nueva cultura de trabajo y gestionar los desafíos de la colaboración remota.

La implementación de plataformas seguras de aplicaciones y escritorios virtuales en el contexto del trabajo remoto en Perú presenta una serie de desafíos únicos, interrelacionados con factores tecnológicos, sociales y económicos. A continuación, se detallan algunas de las problemáticas más relevantes:

Desafíos específicos de Perú

Brecha digital: Existe una brecha digital significativa en el país, con acceso limitado a internet de alta velocidad en muchas regiones, especialmente en zonas rurales. Esto dificulta la adopción de soluciones basadas en la nube y el trabajo remoto.

Infraestructura tecnológica: La infraestructura tecnológica en general, incluyendo la red eléctrica y la conectividad, puede ser inestable o insuficiente en algunas áreas, lo que afecta el rendimiento de las plataformas virtuales.

Conocimiento técnico: La falta de conocimientos técnicos en el manejo de herramientas digitales y plataformas virtuales puede ser un obstáculo para los trabajadores y las empresas.

Costos: La inversión en infraestructura tecnológica y software puede ser un desafío para las pequeñas y medianas empresas peruanas.

Seguridad cibernética: Los ciberataques son una amenaza constante, y las empresas peruanas pueden carecer de los recursos necesarios para implementar medidas de seguridad robustas.

Problemáticas comunes a nivel mundial (adaptadas al contexto peruano)

Calidad de la conexión a internet: La inestabilidad de la conexión a internet en algunas zonas del país puede generar latencia, interrupciones en el servicio y afectar la productividad.

Seguridad de los datos: La protección de los datos sensibles de las empresas y los empleados es un desafío constante, especialmente en un entorno de trabajo remoto donde los dispositivos personales pueden ser utilizados para acceder a información confidencial.

Gestión de dispositivos: La gestión de una gran cantidad de dispositivos remotos puede ser compleja y requiere de herramientas especializadas.

Experiencia del usuario: La falta de familiaridad con las herramientas de colaboración virtual puede afectar la productividad y la satisfacción de los empleados.

Implicaciones para las empresas peruanas

Pérdida de productividad: Los problemas de conectividad, la falta de capacitación y las dificultades técnicas pueden reducir la productividad de los empleados.

Riesgos de seguridad: Los ciberataques pueden causar pérdidas financieras significativas y dañar la reputación de la empresa.

Dificultad para atraer y retener talento: Las empresas que no ofrecen opciones de trabajo remoto pueden tener dificultades para atraer y retener a los mejores talentos.

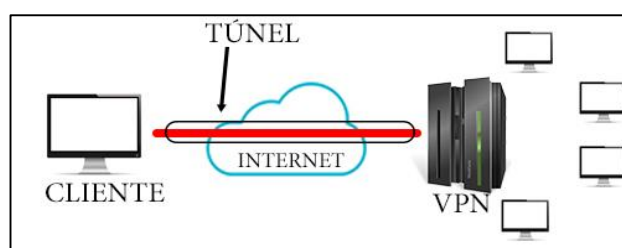
Costos operativos: La implementación y mantenimiento de una plataforma de trabajo remoto puede generar costos adicionales.

La coyuntura actual presentada a nivel mundial y que afecta con mucha incidencia en nuestro país es la pandemia del nuevo coronavirus COVID-19, generando gran impacto principalmente en los sectores de salud y economía. Cabe resaltar que, esta enfermedad actualmente no cuenta con tratamiento alguno para combatirlo y tiene altos índices de personas contagiadas, con una tasa de mortalidad preocupante; sin embargo, existen medidas y controles de bioseguridad que pueden ayudar a minimizar el riesgo de contraer esta enfermedad, ya que es muy fácil su propagación entre las personas. Ante esta situación, el gobierno peruano ha adoptado varios controles para nuestra población, siendo uno de ellos el distanciamiento social obligatorio. Referente a ello, se han aplicado diversas medidas como el distanciamiento físico de metro y medio entre las personas y el trabajo remoto, el cual permite a los empleados realizar sus actividades o funciones laborales desde su hogar, a través del uso de las tecnologías de la información, previniendo el contacto con otras personas (contagio).

Actualmente muchas empresas públicas y privadas están utilizando herramientas tecnológicas como la Red Privada Virtual (VPN), del tipo Client-to-Site, con la finalidad de poder cumplir con el trabajo remoto. Existen muchas marcas en el mercado tecnológico que proporcionan este tipo de servicio; sin embargo, no es el mecanismo más adecuado debido al alto riesgo de seguridad que implica su operación. Por ejemplo, existe la probabilidad de contraer un virus informático (por ejemplo, malware) que pueda afectar a la infraestructura tecnológica de la empresa. En ese sentido, es importante mencionar que el Ministerio de Defensa no es ajeno a este tipo de configuraciones.

En este caso, el Ministerio de Defensa utiliza una red privada virtual que, si bien es cierto que está configurada a través de un protocolo denominado IPsec (Internet Protocol security) el cual brinda mayor seguridad al túnel VPN, no se puede descartar que el riesgo de sufrir un contagio por un software malicioso (malware) sigue siendo alto. Esto se debe a que las computadoras de los usuarios finales son equipos personales, los cuales generalmente son empleados por más de un integrante de la familia, en algunos casos. En ese sentido, podemos mencionar que las redes virtuales, en general, cuando tienen un buen protocolo de cifrado pueden hacer que un túnel sea seguro, pero ello no minimiza el riesgo de que los equipos informáticos como el de los emisores (usuarios finales en casa) puedan estar comprometidos con algún tipo de software malicioso, lo cual representaría una situación perjudicial para la infraestructura tecnológica del Ministerio de Defensa del Perú.

Figura 1.
Diagrama de una Red Privada Virtual, del tipo Client-to-Site



Fuente: <https://wikis.fdi.ucm.es/ELP/VPN>, el 24 ene 2017

Tipos de ataques

Se prevé al menos tres modalidades de ciberataques que enfrentarán los usuarios finales:

- **Phishing.** Normalmente utilizan el correo como medio para enviar información o enlaces falsos, con el propósito de robar credenciales de red, infección de malware, etc.
- **Ingeniería social.** Por medio de esta técnica los ciberdelincuentes, a través de la psicología llegan a robar información de los usuarios finales con el objetivo de realizar intrusiones no autorizadas.
- **Robo de dispositivos.** Los usuarios dejan pegadas las contraseñas en sus respectivos dispositivos, lo cual genera es un riesgo alto, si el equipo llega a manos de un ciberdelincuente.
- **Keylogger.** Ejecuta un seguimiento y registra cada pulso de tecla a través de un software o hardware, con la intención de capturar información, esta actividad puede ser ilícita, ponen en riesgo la protección de datos.
- **Ransomware.** Es un software malicioso que tiene como propósito infectar equipos de cómputo (servidores, PCs), con una finalidad secuestrar las bases de datos o los archivos del tipo documento, para solicitar un rescate económico, es usado en su mayoría por ciberdelincuentes.
- **Malware.** Es un software malicioso que tiene como propósito infectar equipos de cómputo, con una finalidad mal intencionada, es usado en su mayoría por ciberdelincuentes.

Incidentes de seguridad 2022 – 2023

A continuación, se muestra el registro de incidentes de seguridad reportados en el Ministerio de Defensa, durante los años 2022 y 2023:

Tabla 1.
Incidentes de seguridad año 2022

Evento de seguridad	Cantidad de incidentes de seguridad												Total de incidentes de seguridad por evento
	Ene-22	Feb-22	Mar-22	Abr-22	May-22	Jun-22	Jul-22	Ago-22	Set-22	Oct-22	Nov-22	Dic-22	
Software malicioso del tipo keylogger	0	0	1	0	0	0	1	0	0	0	0	1	3
Descargar un Ransomware	2	2	1	1	1	2	1	2	2	1	2	2	19
Propagar un malware	0	0	0	0	0	0	1	0	0	0	0	1	2
Ingeniería social / Phishing	1	2	0	2	1	1	1	2	1	2	1	2	16
Ejecución del malware	2	2	1	2	1	1	1	2	1	2	2	2	19
Robo de información	0	0	0	0	0	0	0	0	0	0	0	0	0
Total de Incidentes Mensual	5	6	3	5	3	4	5	6	4	5	5	8	59

Fuente: Elaboración propia

Tabla 2.
Incidentes incidentes año 2023

Evento de seguridad	Cantidad de incidentes de seguridad									Total de incidentes de seguridad por evento
	Ene-23	Feb-23	Mar-23	Abr-23	May-23	Jun-23	Jul-23	Ago-23	Set-23	
Software malicioso del tipo keylogger	0	0	1	2	1	1	2	1	1	9
Descargar un Ransomware	1	1	2	3	4	3	4	4	3	25
Propagar un malware	0	0	1	0	3	5	3	3	4	19
Ingeniería social / Phishing	2	3	9	6	4	8	6	5	9	52
Ejecución del malware	0	1	2	1	1	2	2	1	1	11
Robo de información	0	0	0	0	0	0	0	0	0	0
Total de incidentes mensual	3	5	15	12	13	19	17	14	18	116

Fuente: Elaboración propia

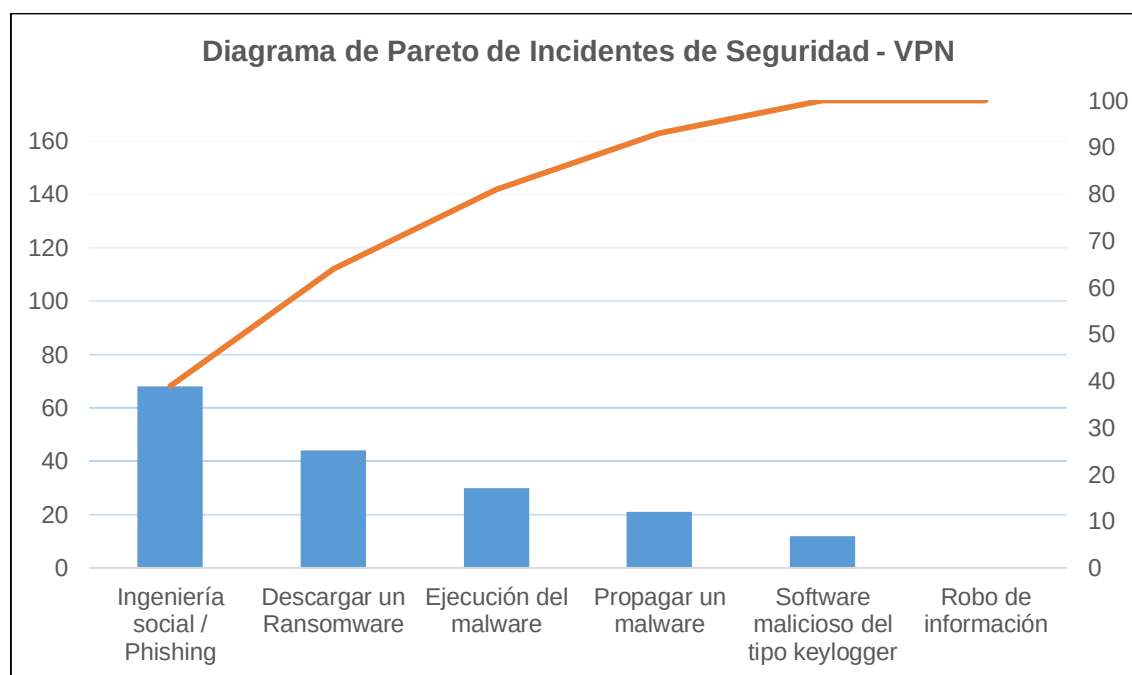
Con dicha información, se procede a consolidar la misma para la elaboración del Diagrama de Pareto correspondiente:

Tabla 3.
Tipos de eventos de seguridad

Evento de seguridad	Cantidad de incidentes de seguridad	Porcentaje de incidentes de seguridad	Porcentaje de incidentes de seguridad acumulado
Ingeniería social / Phishing	68	39	39
Descargar un Ransomware	44	25	64
Ejecución del malware	30	17	81
Propagar un malware	21	12	93
Software malicioso del tipo keylogger	12	7	100
Robo de información	0	0	100
TOTAL	175		

Fuente: Elaboración propia

Figura 2.
Diagrama de pareto de los incidentes de seguridad



Fuente: Elaboración propia

Del diagrama de Pareto realizado y su correspondiente análisis ejecutado, podemos decir que, si atendemos los tres primeros eventos, identificando sus causas y tomando las acciones pertinentes, se habrá logrado solucionar el 81% de los incidentes de seguridad suscitados en el Ministerio de Defensa.

1.2. Planteamiento del problema

Delimitación del problema

Espacial

El presente trabajo de investigación fue desarrollado en la sede principal del Ministerio de Defensa, Lima - Perú.

Temporal

Para el análisis del presente trabajo de investigación se obtuvo información de los incidentes de seguridad en el Ministerio de Defensa sede Principal, Jesús María, Lima.

1.2.1. Problema general

¿Cómo la implementación de una plataforma segura de aplicaciones y escritorios virtuales mejora del trabajo remoto en el MINDEF, 2023?

1.2.2. Problemas específicos

- a) ¿Cómo la infraestructura de virtualización mejora las tecnología y herramientas de comunicación en el MINDEF, 2023?
- b) ¿Cómo el software de virtualización de escritorio y aplicaciones mejora la seguridad y acceso a la información en el MINDEF, 2023?
- c) ¿Cómo el gestor de conexión mejora la infraestructura de trabajo remoto en el MINDEF, 2023?

1.3. Hipótesis de la investigación

1.3.1. Hipótesis general

Si, se implementa una plataforma segura de aplicaciones y escritorios virtuales entonces mejora el trabajo remoto en el MINDEF, 2023.

1.3.2. Hipótesis específicas

- a) Si, se implementa una infraestructura de virtualización entonces mejora las tecnología y herramientas de comunicación en el MINDEF, 2023.

- b) Si, se implementa un software de virtualización de escritorio y aplicaciones entonces mejora la seguridad y acceso a la información en el MINDEF.
- c) Si, se implementa el gestor de conexión entonces mejora la infraestructura de trabajo remoto en el MINDEF, 2023.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Explicar la implementación de una plataforma segura de aplicaciones y escritorios virtuales en la mejora del trabajo remoto en el MINDEF, 2023.

1.4.2. Objetivos específicos

- a) Explicar la infraestructura de virtualización en la mejora de las tecnología y herramientas de comunicación en el MINDEF, 2023.
- b) Explicar el software de virtualización de escritorio y aplicaciones en la mejora de la seguridad y acceso a la información en el MINDEF.
- c) Explicar el gestor de conexión en la mejora de la infraestructura de trabajo remoto en el MINDEF, 2023.

1.5. Variables, dimensiones e indicadores

1.5.1. Variable independiente

- ✓ Plataformas seguras de aplicaciones y escritorios virtuales

1.5.2. Variable dependiente

- ✓ Trabajo remoto

1.5.3. Dimensiones

- ✓ Infraestructura de virtualización
- ✓ Software de virtualización de escritorio y aplicaciones
- ✓ Gestor de conexión
- ✓ Tecnología y herramientas de comunicación

- ✓ Seguridad y acceso a la información
- ✓ Infraestructura de trabajo remoto

1.5.4. Indicadores de la variable dependiente

- ✓ Numero de dispositivos conectados
- ✓ Nivel de compatibilidad
- ✓ Soporte de múltiples aplicaciones
- ✓ Nivel de autonomía
- ✓ Nivel de disponibilidad ante fallos
- ✓ Tasa de Incidentes de Seguridad
- ✓ Nivel de autenticación
- ✓ Algoritmo de autenticación

1.5.5. Operacionalización de variables

Tabla 4.
Operacionalización de variables

Variable	Dimensión	Indicador	Técnica/Instrumentos
Plataforma de aplicaciones seguras y escritorios virtuales	Infraestructura de Virtualización	Si / No	--
	Software de Virtualización de Escritorio y Aplicaciones		
Trabajo remoto	Gestor de Conexión	Numero de dispositivos conectados	Encuesta/ Cuestionario
	Tecnología y herramientas de comunicación	Nivel de compatibilidad	
	Seguridad y acceso a la información	Soporte de múltiples aplicaciones	
		Nivel de autonomía	
		Nivel de disponibilidad ante fallos	
		Tasa de incidentes de seguridad	
	Infraestructura de trabajo remoto	Nivel de autenticación	
		Algoritmo de autenticación	

Fuente: Elaboración propia

1.6. Justificación del estudio

Justificación teórica

Justificación teórica de una plataforma de aplicaciones seguras y escritorios virtuales para la mejora del trabajo remoto se basa en varios aspectos clave relacionados con la tecnología, la seguridad de la información y la productividad. Se presentan los fundamentos que explican por qué estas plataformas son esenciales para mejorar el trabajo remoto:

1. Acceso remoto seguro. - El trabajo remoto implica el acceso a información y recursos corporativos desde ubicaciones diversas, lo que incrementa los riesgos de seguridad. Las plataformas de escritorios virtuales (VDI, por sus siglas en inglés) y aplicaciones seguras ofrecen conexiones cifradas y medidas de seguridad avanzadas, como la autenticación multifactorial, lo que permite que los empleados accedan a los recursos empresariales de manera segura desde cualquier lugar. Desde un enfoque teórico, esto se apoya en los principios de seguridad informática, como el modelo CIA (Confidencialidad, Integridad y Disponibilidad).

Confidencialidad: El acceso a los datos se realiza a través de túneles cifrados, reduciendo el riesgo de filtraciones.

Integridad: Las medidas de control aseguran que los datos no sean manipulados por terceros no autorizados.

Disponibilidad: Los empleados tienen acceso continuo a sus entornos de trabajo sin necesidad de trasladarse físicamente.

2. Aumento de la productividad y la eficiencia. - El uso de escritorios virtuales permite a los empleados tener un entorno de trabajo homogéneo, independientemente del dispositivo o la ubicación. Esto facilita la continuidad del trabajo, ya que no hay diferencias en el acceso a software, aplicaciones o configuraciones. Desde el punto de vista teórico,

esto se sustenta en modelos de eficiencia organizacional y el trabajo ubicuo (ubiquitous work), donde el entorno digital permite una mayor flexibilidad y adaptación sin perder el control centralizado.

3. Reducción de costos y gestión centralizada. - Las empresas que adoptan plataformas de escritorios virtuales y aplicaciones seguras pueden optimizar los costos relacionados con hardware, mantenimiento y gestión de infraestructuras físicas. Teóricamente, esto se alinea con el modelo de computación en la nube y la virtualización, que permiten la consolidación de recursos, la elasticidad en el uso de infraestructura y la disminución de los costos operativos. La gestión centralizada también permite a los administradores TI controlar y actualizar el entorno de trabajo remoto de manera más eficiente, aplicando políticas de seguridad y actualizaciones de forma remota.

4. Flexibilidad y adaptabilidad. - Las plataformas de aplicaciones seguras y escritorios virtuales ofrecen una gran flexibilidad tanto para los empleados como para las empresas. Los empleados pueden trabajar desde cualquier dispositivo, ya que las aplicaciones no dependen del hardware local. Esto reduce la necesidad de soporte técnico in situ y permite que las organizaciones respondan rápidamente a los cambios en las condiciones laborales, como la necesidad de implementar el trabajo remoto de forma masiva, tal como ocurrió durante la pandemia de COVID-19. Desde el punto de vista teórico, esto se relaciona con la teoría de la adaptabilidad organizacional, que sugiere que las organizaciones flexibles y con capacidad de respuesta rápida pueden mantenerse competitivas en entornos cambiantes.

5. Seguridad de datos y cumplimiento normativo. - En un entorno de trabajo remoto, el manejo seguro de los datos es crucial. Las plataformas de escritorios virtuales y aplicaciones seguras facilitan el cumplimiento de normativas como el RGPD (Reglamento General de Protección de Datos) y otras regulaciones de protección de la información. Esto

se debe a que los datos permanecen en servidores controlados y no se almacenan localmente en los dispositivos de los empleados. Teóricamente, esto se apoya en los principios de ciberseguridad y gobernanza de datos, asegurando que la información corporativa sea gestionada bajo marcos legales estrictos y minimizando los riesgos de vulnerabilidades.

6. Resiliencia ante ciberataques. - El trabajo remoto expone a las organizaciones a un mayor número de ataques cibernéticos, como el phishing y el ransomware. Las plataformas de escritorios virtuales reducen estos riesgos al minimizar el acceso directo a los sistemas corporativos y proporcionar un entorno controlado que puede ser monitoreado y protegido de manera más eficiente. Desde una perspectiva teórica, esto está respaldado por el modelo de defensa en profundidad, que propone múltiples capas de seguridad para proteger los activos digitales críticos.

7. Colaboración y comunicación efectiva. - El uso de plataformas de aplicaciones seguras permite una mayor integración de herramientas colaborativas, como mensajería instantánea, videollamadas y sistemas de gestión de proyectos. Estas herramientas facilitan una colaboración más fluida entre equipos remotos, reduciendo la barrera de la distancia. Teóricamente, esto está relacionado con los conceptos de trabajo colaborativo asistido por computadora (CSCW, por sus siglas en inglés) y la teoría de la comunicación organizacional, que sostienen que las tecnologías colaborativas permiten una interacción más efectiva en entornos de trabajo distribuidos.

Justificación práctica

Se basa en la manera en que estas tecnologías resuelven problemas concretos y mejoran la experiencia de empleados y empresas en entornos de trabajo distribuidos. A continuación, se detallan los beneficios tangibles y aplicaciones prácticas:

1. Mejora en la seguridad de los datos. - En la práctica, una de las principales preocupaciones del trabajo remoto es la seguridad de la información. Al utilizar escritorios virtuales y aplicaciones seguras, las empresas pueden proteger sus datos críticos, ya que estos permanecen en servidores corporativos en lugar de en los dispositivos personales de los empleados. Esto minimiza el riesgo de pérdida o robo de información en caso de que el dispositivo sea comprometido o robado.

2. Accesibilidad desde cualquier dispositivo. - Un escritorio virtual permite a los empleados acceder a sus aplicaciones y documentos desde cualquier dispositivo, ya sea una computadora portátil, una tablet o incluso un smartphone, sin depender de la configuración específica del hardware. Esto facilita enormemente el trabajo remoto y elimina las barreras tecnológicas relacionadas con la compatibilidad de software.

3. Ahorro de costos en hardware. - Las empresas que adoptan plataformas de escritorios virtuales no necesitan proporcionar hardware de alto rendimiento a sus empleados, ya que la mayor parte del procesamiento se realiza en los servidores. Los empleados pueden trabajar desde dispositivos más sencillos, lo que reduce los costos de adquisición y mantenimiento de equipos.

4. Mantenimiento centralizado y actualización simplificada. - En lugar de tener que realizar actualizaciones y mantenimiento en cada dispositivo individual, los administradores de TI pueden gestionar el entorno de trabajo desde un punto central. Los escritorios virtuales permiten desplegar actualizaciones, parches de seguridad y nuevas aplicaciones a todos los usuarios de manera simultánea y sin interrupciones.

5. Facilita la continuidad del negocio. - En situaciones inesperadas, como desastres naturales o pandemias, donde los empleados no pueden acceder a las oficinas físicas, los escritorios virtuales aseguran que puedan continuar trabajando desde cualquier lugar. Esto garantiza la continuidad del negocio sin interrupciones significativas.

6. Aumento de la productividad. - El acceso constante y fluido a las aplicaciones y datos empresariales, sin importar el lugar o el dispositivo, contribuye a una mayor productividad. Además, las plataformas de escritorios virtuales suelen incluir herramientas de colaboración integradas que facilitan la comunicación y la coordinación entre equipos remotos.

7. Control y visibilidad centralizados. - Las plataformas de escritorios virtuales permiten a los administradores de TI tener un control total sobre el entorno de trabajo remoto. Pueden monitorear la actividad de los usuarios, aplicar políticas de seguridad de manera uniforme y responder rápidamente a incidentes, lo que mejora la gestión del riesgo.

8. Cumplimiento normativo. - En sectores donde la regulación y el cumplimiento de normas de seguridad son estrictos (como el sector financiero, salud o legal), las plataformas de escritorios virtuales facilitan la adherencia a normativas al proporcionar un entorno seguro donde se gestionan los datos de acuerdo con los estándares exigidos.

9. Reducción del riesgo de ataques cibernéticos. - El trabajo remoto aumenta el riesgo de ataques cibernéticos, especialmente cuando los empleados acceden a la red corporativa desde diferentes puntos y dispositivos. Las plataformas de escritorios virtuales reducen estos riesgos al centralizar las medidas de seguridad, asegurando que los dispositivos externos no tengan acceso directo a la red interna.

Importancia del estudio

El estudio de las plataformas de aplicaciones seguras y escritorios virtuales es esencial para comprender cómo mejorar el trabajo remoto de manera eficiente, segura y flexible. La importancia de este estudio radica en su capacidad para abordar desafíos prácticos como la seguridad de los datos, la productividad, la reducción de costos y el cumplimiento normativo, mientras que también permite a las empresas adaptarse a un entorno laboral cambiante y mantenerse competitivas.

1.7. Antecedentes nacionales e internacionales

1.7.1. Antecedentes internacionales

(Zai, y otros, 2024) Elaboraron el artículo “Implementación de escritorios virtuales para investigación clínica en un centro de salud académico: reporte de un caso, Oxford University Press on behalf of the American Medical Informatics Association, Worcester, United States”.

Tuvo como objetivos, abordar los desafíos de compartir datos de investigación clínica mediante la implementación de escritorios virtuales basados en la nube, mejorando colaboración entre investigadores manteniendo la seguridad de los datos.

Materiales y métodos: este estudio de caso detalla la implementación de escritorios virtuales en la Facultad de Medicina de UMass Chan (UMass Chan). el proceso implicó la formación de un grupo de trabajo ejecutivo de dirección de informática de investigación, la identificación de requisitos clave, la implementación de Amazon WorkSpaces, y establecer una gestión de datos configurable para el apoyo a la investigación.

Resultados: Las lecciones clave incluyen la importancia de la colaboración, el equilibrio entre la facilidad de uso y la funcionalidad, la flexibilidad en la gestión de datos, la maximización eficiencia del escritorio virtual dentro de las limitaciones presupuestarias y comentarios continuos de los usuarios. La implementación de escritorios virtuales soporta asegurar la investigación colaborativa, avanzar en el conocimiento médico y mejorar los resultados de la atención médica.

Discusión: El enfoque estructurado para implementar escritorios virtuales aborda la seguridad de los datos, el cumplimiento normativo y la colaboración en tiempo real de la retroalimentación continua y las mejoras iterativas han mejorado la eficacia del sistema.

Conclusión: La implementación exitosa de escritorios virtuales en UMass Chan demuestra el potencial de dichos sistemas para soportar sistemas seguros y investigación colaborativa, que ofrece ideas para iniciativas similares en otros centros de salud académicos.

(Sachintha, 2024) desarrollo el artículo “El futuro del trabajo: escritorios virtuales en la nube y su impacto en la eficiencia y seguridad del lugar de trabajo, Researchgate, Colombo, Sri Lanka”.

Este informe de investigación forma parte de la evaluación de SIT233 Cloud Computing. Explora la creciente tendencia de Virtual Cloud Desktops (VCD), un servicio de nube administrado que ofrece entornos completos de estaciones de trabajo a los dispositivos de los usuarios. Conocido también como escritorio como servicio (DaaS), VCD ofrece soluciones escalables, seguras y rentables, lo que reduce la necesidad de actualizaciones de hardware. Impulsados por el aumento del trabajo remoto, los avances tecnológicos y la rentabilidad, grandes proveedores como Amazon, Microsoft y Google lideran esta innovación. El informe examina las tecnologías habilitadoras clave, las motivaciones, las aplicaciones y el impacto en los grandes proveedores de servicios en la nube. También evalúa los beneficios y desventajas, predice avances futuros y ofrece estrategias para promover la conciencia. En general, VCD está preparado.

(Díaz & Avendaño, 2022) elaboro la tesis “Diseño de una plataforma virtual para la optimización de recursos tecnológicos en la empresa Maint, Trabajo de titulación previo a la obtención del título de Magister en Telecomunicaciones, Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador”.

La empresa MAINT durante el año 2020 durante la pandemia COVID-19 detectó un aumento en el consumo de energía eléctrica dentro de sus oficinas en la sucursal

Guayaquil. Un informe técnico detectó que este aumento se produce porque varios equipos de escritorio permanecen encendidos. Las 24 horas del día, los siete días de la semana.

El objetivo de este trabajo es analizar la implementación de un entorno de escritorio virtual con VMware Horizon y realizar una proyección a cinco años de los gastos operativos dentro de la empresa.

El objetivo es contrastar el ahorro que supone apagar los ordenadores de sobremesa con la instalación de escritorios virtuales y concluir con una conclusión de ventajas y beneficios.

1.7.2. Antecedentes nacionales

(Isidro, 2023) elaboro la tesis “Diseñar una plataforma de virtualización de aplicaciones utilizando terminales de acceso para escritorios virtuales y con alta disponibilidad híbrida para el sistema integrado de administración financiera (SIAF) en la (Dirección de sanidad policial), Universidad Peruana de Ciencias Aplicadas (UPC), Para optar el título profesional de Ingeniero de Redes y Comunicaciones. Lima, Perú”.

Dado que la virtualización se ha convertido en los últimos años en una pieza fundamental para avance y desarrollo tecnológico, esto gracias a que puede con su nivel de abstracción de la Ayuda de hardware a todos los niveles para utilizar eficientemente los recursos computacionales. Esta tesis analiza las diferentes variables de virtualización que son tanto la software y hardware teniendo en cuenta para ello desde servidores hasta terminales acceso a plataformas de virtualización de aplicaciones, desarrollando una investigación exhaustiva tanto a nivel teórico como técnico con pruebas de rendimiento en el equipo en cuestión. La piedra angular para que la virtualización prospere de manera efectiva de aplicaciones es optimizar configuraciones y estimar de forma escalable y fiable tanto hardware como software, ya que se obtienen diferentes resultados según el convergencia de estas tecnologías, tal como se obtiene en las pruebas de rendimiento, todo

esto centrándose en la carga de usuarios y el nivel de concurrencia ejemplificándolo durante el desarrollo de la investigación, aspectos como el tratado de seguridad para la virtualización de la CSA (Cloud Security Alliance) que proporciona una fortaleza a nivel del ecosistema de virtualización de aplicaciones que se está creando para albergar toda la plataforma tecnológica.

(Jara, 2021) desarrollo la tesis “Implementación de una plataforma de virtualización usando amazon web services, para soportar las aplicaciones de la empresa Programate SAC, Para obtener el título de Ingeniero de Sistemas, Universidad Autónoma del Perú. Lima, Perú”

Esta investigación se desarrolló en la empresa Programate S.A.C., en la cual se realizó la implementación de una plataforma de virtualización utilizando Amazon Web Services para las diferentes aplicaciones con las que cuenta la empresa. La plataforma Amazon Web Services cuenta con diferentes servicios los cuales nos facilitan la creación de una plataforma virtual con diferentes tipos de soluciones. El propósito es crear una plataforma virtual para migrar diferentes aplicaciones que tiene la empresa Programate S.A.C. utilizando la plataforma Amazon Web Services. A destacar, utilizar Amazon Web Services estaría en línea con las grandes empresas que están utilizando plataformas en la nube ya que una de las ventajas de estas plataformas es utilizar los últimos desarrollos del siglo XXI. Al finalizar nuestra investigación los resultados que nos dieron fueron favorables para la presente investigación.

(Llesquen, 2020) desarrollo la tesis “Implementación de la plataforma virtual Microsoft Teams en la gestión educativa de la Institución Educativa Privada Nuestro Maravilloso Mundo, Lima, 2020, Para optar el grado de Maestra en Administración de la Educación, Universidad Cesar Vallejo. Lima, Perú”.

El propósito de este estudio fue evaluar el impacto de la aplicación de la Plataforma Microsoft Team en la Administración Educativa de la Institución Educativa Privada Nuestro Maravilloso Mundo Lima, 2020. El método utilizado en esta tesis estuvo vinculado a un enfoque cuantitativo, explicativo, y a un diseño experimental preexperimental de longitud longitudinal. El grupo de estudio estuvo compuesto por 108 profesores de la institución educativa citada previamente. Antes de su aplicación, el instrumento fue evaluado por especialistas. Para confirmar la confiabilidad del instrumento, se analizaron los datos del cuestionario empleado en el pretest y el post test, logrando un nivel de fiabilidad de 0,000 para la variable Plataforma Microsoft Teams en la Gestión Educativa.

La fiabilidad de los instrumentos posee una correlación magnífica con la confiabilidad. Entre los hallazgos más destacados de la población analizada, en la variable Gestión Educativa se destaca que, de los 108 participantes en el pre Test, el 90,7% se situó en el nivel medio y en el Postest, el 100% se situó en el nivel alto. Podemos deducir que la Plataforma Microsoft Team ejerce un impacto beneficioso en la gestión Educativa, dado que ha facilitado la organización, planificación y dirección de los procesos de la Institución Educativa de forma eficiente.

1.8. Marco teórico

1.8.1. Sistema de información

Según (Laudon & Laudon, 2022) define:

Los sistemas de información gerenciales (SIG) “son conjuntos de hardware, software, datos, personas, procesos y redes que trabajan juntos para recopilar, procesar, almacenar, analizar y distribuir información para apoyar la toma de decisiones, la planificación, el control y las operaciones de una organización en todos sus niveles y funciones”. (p. 6).

Sistema informático

“Es un conjunto de entidades interrelacionadas que emplea un ordenador, el mismo que posee dispositivos y secciones programables para utilizarlos en la extracción, almacenamiento y procesamiento de datos. El usuario, los periféricos y el ordenador en sí, conforman un Sistema Informático”. (Raya, Raya, & Zurdo, 2014)

Plataforma de aplicaciones informáticas

Según (Apple, 2023) “Una plataforma de aplicaciones informáticas se refiere al entorno que permite el desarrollo, ejecución y gestión de aplicaciones de software, proporcionando las herramientas, los servicios y los recursos necesarios para facilitar estos procesos”. Estas plataformas actúan como una base sobre la cual las aplicaciones pueden ser diseñadas, probadas y desplegadas, facilitando la integración con otros sistemas y la optimización de recursos tecnológicos

Elementos de una plataforma de aplicaciones

Infraestructura: Hardware, software base y servicios en la nube que soportan la ejecución de las aplicaciones.

Herramientas de desarrollo: Editores de código, depuradores, emuladores y frameworks que facilitan la creación de aplicaciones.

Servicios: Bases de datos, almacenamiento, autenticación, notificaciones y otras funcionalidades que pueden ser reutilizadas por las aplicaciones.

APIs (Interfaces de Programación de Aplicaciones): Permiten la integración de diferentes componentes y servicios.

Modelos de distribución: Definen cómo se distribuyen y consumen las aplicaciones (por ejemplo, app stores, marketplaces).

Escritorios virtuales

Un escritorio virtual es una representación digital de un espacio de trabajo que simula un escritorio físico, pero existe y se ejecuta en un entorno informático. Permite a los usuarios organizar sus aplicaciones, archivos y ventanas de manera independiente, creando múltiples espacios de trabajo virtuales dentro de un mismo sistema operativo.

Características de un escritorio virtual:

Espacios de trabajo independientes: Cada escritorio virtual funciona como un espacio de trabajo aislado, permitiendo a los usuarios organizar diferentes tareas o proyectos sin interferencias.

Gestión de ventanas: Los usuarios pueden mover ventanas entre escritorios virtuales, creando diferentes layouts y flujos de trabajo.

Personalización: Los escritorios virtuales suelen ser altamente personalizables, permitiendo a los usuarios cambiar fondos, temas y configuraciones.

Acceso remoto: En muchos casos, los escritorios virtuales se pueden acceder de forma remota, lo que permite a los usuarios trabajar desde cualquier dispositivo con conexión a internet.

Infraestructura de virtualización

La infraestructura de virtualización es un conjunto de tecnologías y componentes que permiten crear, gestionar y operar entornos virtuales que emulan hardware físico, permitiendo que múltiples sistemas operativos y aplicaciones compartan los mismos recursos de hardware. Esto incluye hipervisores, servidores, redes y almacenamiento que están diseñados para soportar cargas de trabajo virtualizadas, optimizando así el uso de recursos y la escalabilidad de las infraestructuras tecnológicas (Stallings, 2015).

Una infraestructura de virtualización es un entorno tecnológico que permite crear múltiples sistemas operativos y aplicaciones virtuales sobre un único hardware físico. Es

decir, se trata de una capa de software que abstrae los recursos físicos de un servidor (CPU, memoria, almacenamiento) para crear múltiples máquinas virtuales que funcionan de manera independiente.

Componentes de una infraestructura de virtualización:

Hipervisor: Es el software que gestiona la virtualización, asignando recursos a las máquinas virtuales y aislando cada una de ellas.

Máquinas virtuales: Son instancias de sistemas operativos que se ejecutan sobre el hipervisor, cada una con sus propios recursos asignados.

Almacenamiento virtual: Permite crear volúmenes de almacenamiento virtuales que pueden ser asignados a las máquinas virtuales.

Redes virtuales: Permiten crear redes lógicas aisladas para cada máquina virtual o grupo de máquinas virtuales.

Software de virtualización de escritorio y aplicaciones

El software de virtualización de escritorio y aplicaciones permite ejecutar entornos de trabajo virtuales y aplicaciones en servidores remotos, facilitando el acceso desde múltiples dispositivos y ubicaciones. Esta tecnología separa los entornos de trabajo o aplicaciones de los dispositivos físicos en los que se utilizan, proporcionando flexibilidad, seguridad y gestión centralizada de los recursos (Silberschatz, Galvin, & Gagne, 2018).

Gestor de conexión

Un gestor de conexión es una herramienta de software que permite gestionar y supervisar las conexiones de red, facilitando la configuración, administración y mantenimiento de la conectividad de dispositivos y redes. Este tipo de software es fundamental para administrar los recursos de red, asegurar la disponibilidad de conexiones y optimizar la calidad del servicio. (Tanenbaum & Wetherall, 2011)

1.8.2. Trabajo remoto

Según (Davenport & Prusak, 2000), El trabajo remoto se define como una modalidad laboral en la que los empleados pueden realizar sus tareas desde un lugar fuera de la oficina, utilizando tecnologías de la información para comunicarse y colaborar con sus colegas. Esta modalidad promueve la flexibilidad en la ubicación del trabajador y puede mejorar tanto la productividad como el equilibrio entre la vida laboral y personal.

El trabajo remoto, también conocido como teletrabajo, es una modalidad laboral que permite a los empleados realizar sus tareas laborales desde una ubicación diferente a la oficina tradicional, generalmente desde su hogar. Esta modalidad se ha vuelto cada vez más popular en los últimos años, gracias al avance de las tecnologías de la información y la comunicación, y se ha visto impulsada aún más por la pandemia de COVID-19.

El trabajo remoto se basa en el uso de herramientas tecnológicas como:

Computadoras: Para acceder a los sistemas y aplicaciones de la empresa.

Internet: Para conectarse a la red de la empresa y comunicarse con compañeros.

Software de colaboración: Para trabajar en equipo, compartir archivos y realizar videoconferencias.

Estas herramientas permiten a los empleados realizar sus tareas de manera eficiente y colaborativa, sin importar dónde se encuentren.

Ventajas del trabajo remoto

Flexibilidad: Los empleados pueden adaptar su horario de trabajo a sus necesidades personales y familiares.

Mayor productividad: Al eliminar el tiempo de traslado y las interrupciones en la oficina, muchos empleados reportan un aumento en su productividad.

Reducción de costos: Las empresas pueden reducir costos al necesitar menos espacio de oficina y al ahorrar en gastos relacionados con el transporte.

Ampliación del talento: Las empresas pueden contratar a empleados de cualquier parte del mundo.

Reducción del impacto ambiental: Al reducir los desplazamientos, se disminuye la huella de carbono.

Desafíos del trabajo remoto

Aislamiento social: Los empleados pueden sentirse aislados y desconectados de sus compañeros de trabajo.

Dificultad para separar la vida laboral y personal: El trabajo y la vida personal pueden mezclarse, lo que puede generar estrés y dificultades para desconectar.

Requiere disciplina y autogestión: Los empleados deben ser capaces de organizarse y trabajar de forma independiente.

Necesidad de contar con un espacio de trabajo adecuado: Es importante contar con un espacio tranquilo y equipado para trabajar de forma eficiente.

Tecnología y herramientas de comunicación

La tecnología y las herramientas de comunicación se refieren a los dispositivos, plataformas y aplicaciones que permiten la transmisión de información y facilitan la interacción entre personas o grupos, sin importar su ubicación geográfica. Estas herramientas incluyen desde el correo electrónico y la mensajería instantánea hasta plataformas de videoconferencia y redes sociales, que han transformado la forma en que las personas comparten conocimientos y colaboran (Castells, 2009).

Las tecnologías y herramientas de comunicación son sistemas y dispositivos que facilitan la transmisión, recepción y procesamiento de información entre individuos o grupos. Estas herramientas pueden ser analógicas o digitales, y abarcan desde medios tradicionales como el teléfono y la radio hasta plataformas digitales más recientes como internet, redes sociales y aplicaciones de mensajería instantánea.

Elementos las tecnologías y herramientas de comunicación

Transmisión: Proceso de envío de información a través de un canal.

Recepción: Proceso de captura y decodificación de la información transmitida.

Procesamiento: Manipulación de la información para adaptarla a las necesidades del usuario.

Interacción: Permite la comunicación bidireccional entre los usuarios.

Convergencia: Tendencia a integrar diferentes medios y tecnologías en un solo dispositivo o plataforma.

Seguridad y el acceso a la información

La seguridad y el acceso a la información abarcan las políticas, prácticas y tecnologías diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información. Estos sistemas de seguridad establecen controles de acceso para asegurar que solo los usuarios autorizados puedan obtener, modificar o utilizar los datos, protegiendo así a las organizaciones de amenazas internas y (Whitman & Mattord, 2017).

Infraestructura de trabajo remoto

La infraestructura de trabajo remoto se refiere al conjunto de tecnologías, herramientas y servicios que permiten a los empleados trabajar de manera efectiva desde fuera de las oficinas tradicionales. Esta infraestructura incluye redes seguras, plataformas de colaboración en línea, acceso remoto a sistemas y políticas de ciberseguridad, lo que permite a los equipos mantener la productividad y comunicación en un entorno distribuido (Olson & Olson, 2014)

1.9. Definición de términos básicos

1.9.1.- Acceso remoto

La capacidad de acceder a una red o sistema informático desde una ubicación diferente a la oficina física.

1.9.2.- Aplicaciones virtuales

Programas que se ejecutan en un entorno virtual, permitiendo a los usuarios acceder a ellos a través de la nube, sin necesidad de instalarlos localmente.

1.9.3.- Autenticación

Proceso de verificación de la identidad de un usuario que intenta acceder a un sistema o recurso.

1.9.4.- Ciberseguridad

Conjunto de medidas y prácticas diseñadas para proteger sistemas, redes y datos de ataques digitales y accesos no autorizados.

1.9.5.- Escritorio virtual

Entorno de trabajo que simula un escritorio físico, al que los usuarios pueden acceder a través de la red, permitiendo un acceso seguro a aplicaciones y datos.

1.9.6.- Gestor de conexión

Software que facilita la gestión y supervisión de las conexiones de red, permitiendo configuraciones seguras y eficientes.

1.9.7.- Infraestructura de virtualización

Conjunto de tecnologías que permiten crear y gestionar entornos virtuales que emulan hardware físico, optimizando el uso de recursos.

1.9.8.- Red Privada virtual (VPN)

Tecnología que crea una conexión segura y cifrada a través de una red pública, permitiendo a los usuarios acceder a recursos de forma segura.

1.9.9.- Seguridad de la Información

Prácticas y políticas destinadas a proteger la integridad, confidencialidad y disponibilidad de la información.

1.9.10.- Teletrabajo

Modalidad laboral en la que los empleados realizan sus tareas desde una ubicación diferente a la oficina, utilizando tecnologías digitales.

1.9.11.- Plataforma de trabajo colaborativo

Herramienta que permite a los equipos trabajar juntos en tiempo real, independientemente de su ubicación geográfica, mediante funciones de comunicación y gestión de proyectos.

1.9.12.- Autenticación de dos factores (2FA)

Método de seguridad que requiere dos formas de verificación antes de otorgar acceso a un sistema.

1.9.13.- Nube (Cloud)

Infraestructura que permite el almacenamiento y acceso a datos y aplicaciones a través de Internet, sin necesidad de gestionar hardware físico localmente.

1.9.14.- Control de acceso

Conjunto de políticas y tecnologías que determinan quién puede acceder a ciertos recursos dentro de una red o sistema.

1.9.15.- Gestión de dispositivos móviles (MDM)

Estrategias y herramientas utilizadas para gestionar y asegurar dispositivos móviles utilizados en el trabajo remoto.

II. METODO

2.1. Tipo y diseño de la investigación

2.1.1. Tipo de investigación

El proyecto es una investigación del tipo aplicada.

La investigación aplicada se enfoca en resolver problemas concretos y prácticos mediante la aplicación de conocimientos científicos. Según (Hernández, Fernández, & Baptista, 2014) la investigación aplicada "se caracteriza por su orientación hacia la solución de problemas específicos, en la que los resultados obtenidos son de utilidad inmediata para la toma de decisiones o la mejora de procesos en contextos específicos" (p. 8).

2.1.2. Diseño de la investigación

Esta investigación es de tipo Pre-Experimental. (Pedhazur & Schmelkin, 2013) afirma que: Es una investigación que posee todos los elementos de un experimento, excepto que los sujetos no se asignan aleatoriamente a los grupos. En ausencia de aleatorización, el investigador se enfrenta con la tarea de identificar y separar los efectos de los tratamientos del resto de factores que afectan a la variable dependiente (p. 277)

2.1.3. Nivel de la investigación

La investigación tiene nivel descriptivo explicativa.

El nivel de investigación descriptivo-explicativo combina características de los estudios descriptivos y explicativos, con el propósito de identificar y detallar las características de

un fenómeno o situación y luego explicar las relaciones y causas que lo producen. Este tipo de investigación no solo describe las variables de estudio, sino que también profundiza en el entendimiento de por qué y cómo ocurren ciertos eventos (Hernández, Fernández, & Baptista, 2014)

El nivel de esta investigación es de tipo descriptiva. (Rodríguez, 2005) afirma:

La investigación descriptiva “comprende la descripción, registro, análisis e interpretación de la naturaleza actual, composición o procesos de los fenómenos. El enfoque se hace sobre conclusiones dominantes, o sobre cómo una persona, grupo o cosa, se conduce o funciona en el presente. La investigación descriptiva trabaja sobre realidades y su característica fundamental es la de presentarnos una interpretación correcta”. (p. 24)

El nivel de investigación explicativo busca identificar las causas o factores que determinan ciertos fenómenos, tratando de comprender el "por qué" y el "cómo" de los mismos. Este tipo de investigación intenta establecer relaciones de causa-efecto entre las variables para ofrecer una comprensión profunda de los procesos involucrados (Hernández, Fernández, & Baptista, 2014)

2.1.4. Enfoque de la investigación

Según (Sabino, 2019) "El enfoque cuantitativo se orienta a la medición y análisis de datos numéricos para describir, explicar y predecir fenómenos. Se basa en la lógica deductiva y el uso de métodos estadísticos para generar conocimiento objetivo y generalizable" (p. 187).

El enfoque de la investigación será cuantitativo, ya que se planteará un problema general con problemas específicos y luego se delimitará por medio de la comprobación del marco teórico por medio de diferentes fuentes mediante las hipótesis planteadas.

2.2. Población y muestra

Población

Según (Tamayo, 2004) afirma que:

Población: “totalidad de un fenómeno de estudio, incluye la totalidad de unidades de análisis o entidades de población que integran dicho fenómeno y que debe cuantificarse para un determinado estudio integrando un conjunto N de entidades que participan de una determinada característica, y se le denomina población por constituir la totalidad del fenómeno adscrito a un estudio o investigación” (p. 176)

La población estará conformada por 400 usuarios con distintos roles aplicados en la empresa.

Muestra

El presente trabajo de investigación tuvo una población de 400 usuarios, en tal sentido se estima conveniente analizar y trabajar el 100] % de la población no es necesario el cálculo de la muestra.

Según (Tamayo, 2004) indica partir de la población cuantificada para una investigación se determina la muestra, cuando no es posible medir cada una de las entidades de población; esta muestra, se considera, es representativa de la población.

Según (Palella & Martins, 2006), una muestra “es una parte o un subconjunto de una población que debe tener características lo más replicadas posible”. (p. 93).

2.3. Técnicas para la recolección de datos

Técnicas

Para este trabajo se utilizará como técnica general un formato de encuestas.

Según (Tamayo, 2004), Siguiendo un diseño previamente establecido para garantizar la veracidad de la información recopilada, la encuesta es aquella que permite dar respuestas a problemas en términos descriptivos como de relación de variables.

Instrumentos

El formato de recojo de información será cuestionario.

“Es un instrumento que agrupa una serie de preguntas relativas a un evento, situación o temática particular, sobre el cual el investigador desea obtener información”. (Hurtado de Barrera, 2012)

2.4 . Validez y confiabilidad de instrumentos

Validez del instrumento

Para validar la encuesta, se aplicará el coeficiente Kappa

$$K = P_o - P_e / (1 - P_e)$$

Donde:

P_e = Porcentaje esperado por puro azar

P_o = Porcentaje observado

Para poder validar el contenido se utilizó el Juicio de tres expertos, expertos en asesoramiento de tesis y el ámbito temático.

Tabla 5.
Juicio de Expertos

N°	Expertos	Promedio de ponderación
1	Mg. Corilla Baquerizo, Eduardo Cancio	88 %
2	Ing. Cubas Lozano, Flor Yanina	85 %
3	Mg. Gonzales Calderón, José Ramos	89 %
Ponderado		87%

Fuente: Elaboración propia

De la evaluación del juicio de 03 expertos se ha obtenido una ponderación excelente.

Criterio de confiabilidad de instrumento

Para que las encuestas sean confiables, se usará el coeficiente Alpha de Cronbach

$$\alpha = \frac{k}{(k-1)} \left(1 - \frac{\sum \sigma_i^2}{\sigma_x^2} \right)$$

Donde

k = es el número de ítems

$(\sigma_i)^2$ = varianza de cada ítem

$(\sigma_x)^2$ = varianza del cuestionario total

Según (Ñaupas, Mejía, & Novoa, 2014) cuando las mediciones no difieren significativamente en el tiempo o en la aplicación a diferentes personas, es fiable. La confiabilidad es la prueba que genera confianza cuando los resultados siempre son iguales al aplicarse en condiciones iguales o similares. Para evaluar los coeficientes de alfa de Cronbach, se proponen los siguientes criterios:

- ✓ Coeficiente alfa > 0.9 es excelente
- ✓ Coeficiente alfa > 0.8 es bueno
- ✓ Coeficiente alfa > 0.7 es aceptable
- ✓ Coeficiente alfa > 0.6 es cuestionable
- ✓ Coeficiente alfa > 0.5 es pobre
- ✓ Coeficiente alfa < 0.5 es inaceptable

Tabla 6.
Análisis de fiabilidad

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,723	12

Fuente: Elaboración propia

De acuerdo a la aplicación del alfa de Cronbach el resultado fue igual a 0.723 podemos decir que el instrumento de recojo de información es Aceptable.

2.5. Procesamiento y análisis de datos

Según (Sánchez-Vega, 2017) Es fiable cuando las mediciones no difieren significativamente entre diferentes personas o en el tiempo. La confiabilidad es la prueba que genera confianza cuando se aplica en condiciones iguales o similares y los resultados siempre son iguales. Se proponen los siguientes criterios para medir los coeficientes de alfa de Cronbach (p. 23).

El análisis de información se realizará usando el software estadístico informático SPSS versión 26, algunos gráficos provienen del software SPSS para las revisiones de normalidad y constratación de hipótesis con el respectivo estadígrafo, y otros con diferentes detalles serán diseñados con el software MS Excel.

2.6. Aspectos éticos

Tenemos el compromiso de respetar estilos de normas APA, reglamentos de grados, principios y títulos de la Universidad Peruana de Ciencias e Informática, además, respetar el derecho de autor citando adecuadamente para respetar la propiedad intelectual.

III. RESULTADOS

3.1. Resultados descriptivos

Resultado descriptivo del Pre-Test

Tabla 7.

Frecuencia de la variable *plataforma de aplicaciones seguras y escritorios virtuales*.

PRE_Plataforma de aplicaciones seguras y escritorios virtuales

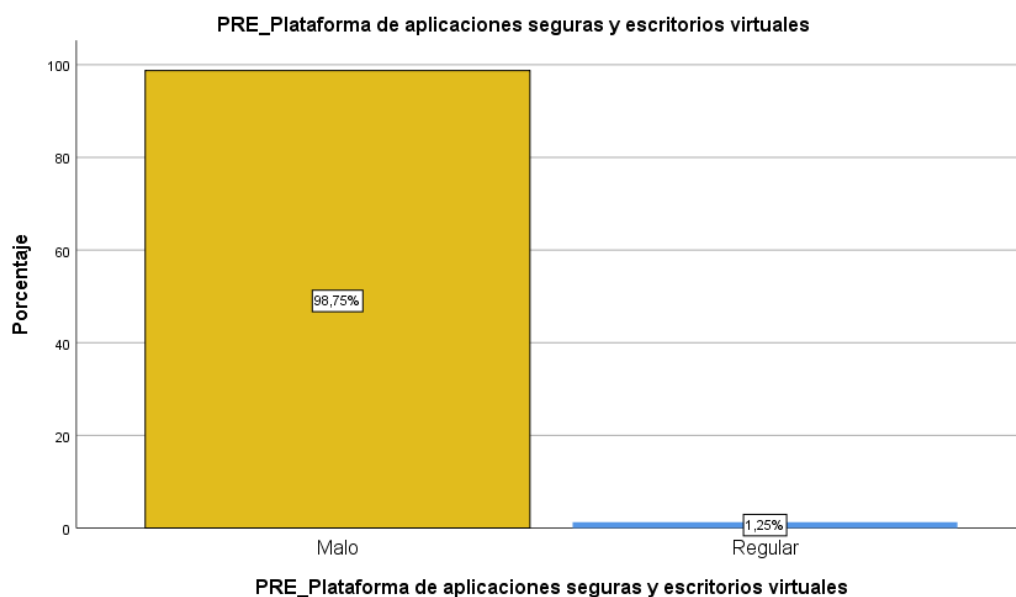
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	395	98,8	98,8	98,8
	Regular	5	1,3	1,3	100,0
	Total	400	100,0	100,0	

Fuente: Elaboración propia

Grafico

Figura 3.

Frecuencia de la variable *plataforma de aplicaciones seguras y escritorios virtuales*



Fuente: Elaboración propia.

Interpretación. Se observa del total de los usuarios encuestados el 98.75 % perciben como malo y el 1.25% perciben como regular el nivel de la variable plataforma de aplicaciones seguras y escritorios virtuales.

Tabla 8.
Frecuencia de la dimensión tecnología y herramientas de comunicación.

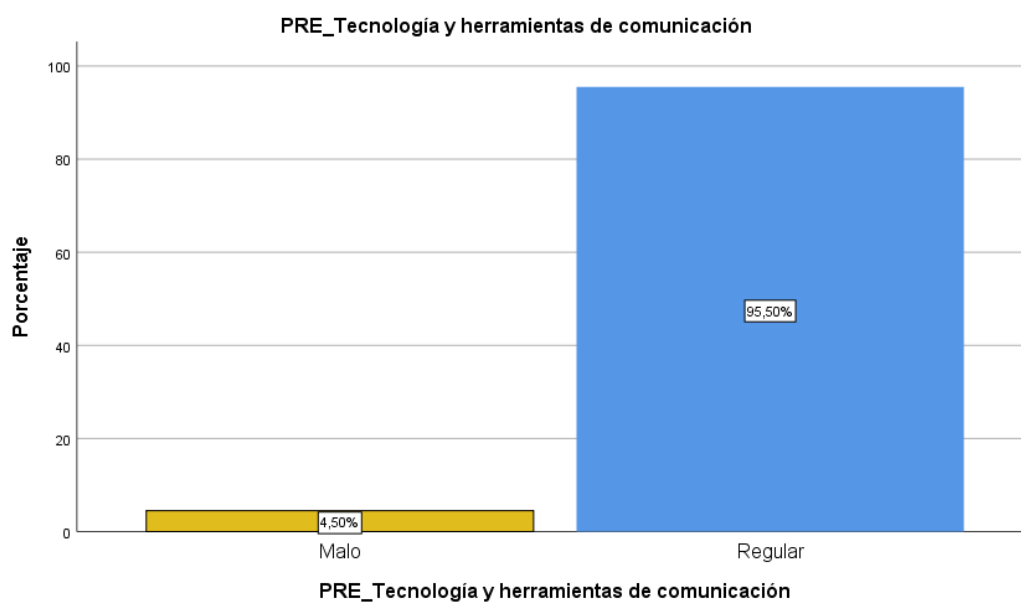
PRE_Tecnología y herramientas de comunicación

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	18	4,5	4,5	4,5
	Regular	382	95,5	95,5	100,0
	Total	400	100,0	100,0	

Fuente: Elaboración propia

Grafico

Figura 4.
Frecuencia de la dimensión tecnología y herramientas de comunicación.



Fuente: Elaboración propia

Interpretación. Se observa del total de usuarios encuestados manifiestan que el 95.50 % consideran como regular y el 4.50% consideran como malo el nivel de la dimensión tecnología y herramientas de comunicación.

Tabla 9.
Frecuencia de la dimensión seguridad y acceso a la información

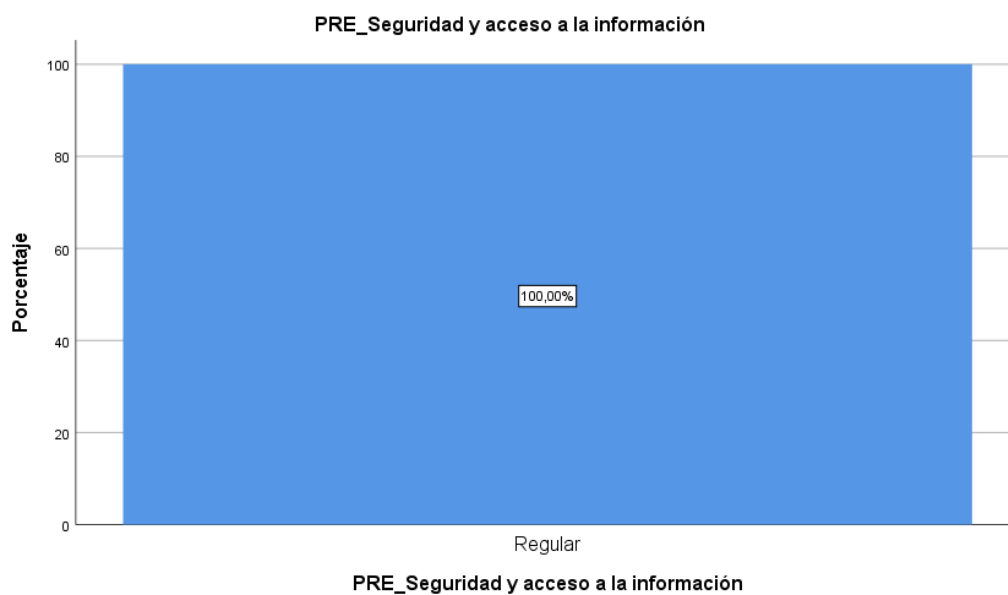
PRE_Seguridad y acceso a la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	400	100,0	100,0	100,0

Fuente: Elaboración propia

Grafico

Figura 5.
Frecuencia de la dimensión seguridad y acceso a la información



Fuente: Elaboración propia.

Interpretación. Se observa del total de usuarios encuestados manifiestan que el 100% consideran como regular el nivel de la dimensión seguridad y acceso a la información.

Tabla 10.
Frecuencia de la dimensión infraestructura de trabajo remoto

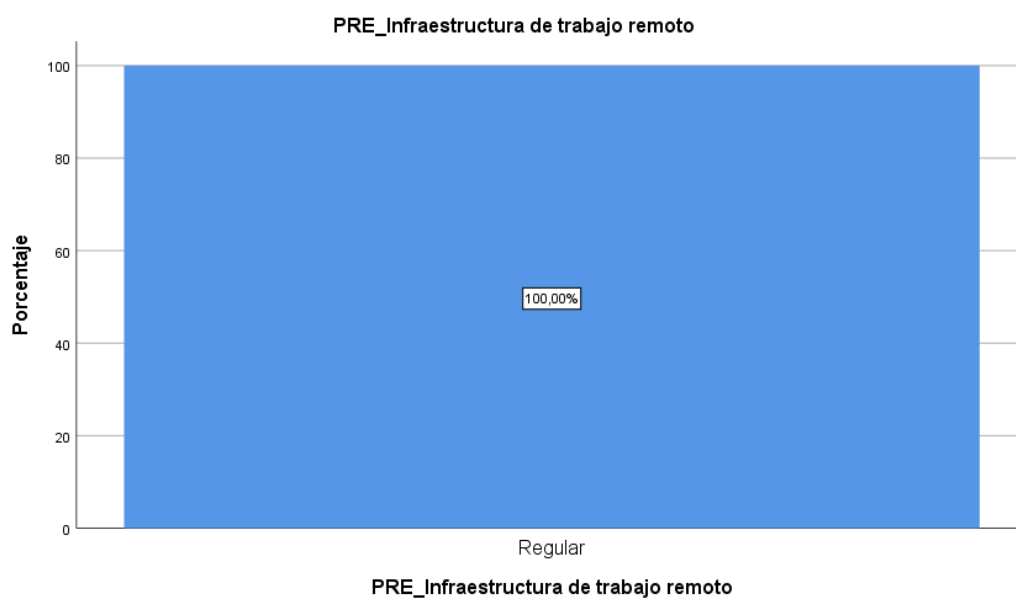
PRE_Infraestructura de trabajo remoto

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	400	100,0	100,0	100,0

Fuente: Elaboración propia

Grafico

Figura 6:
Frecuencia de la dimensión infraestructura de trabajo remoto.



Fuente: Elaboración propia.

Interpretación. Se observa del total de usuarios encuestados manifiestan que el 100% consideran como regular el nivel de la dimensión infraestructura de trabajo remoto.

Resultados descriptivos Pos-Test

Tabla 11.

Frecuencia de la variable *plataforma de aplicaciones seguras y escritorios virtuales*

POS_Plataforma de aplicaciones seguras y escritorios virtuales

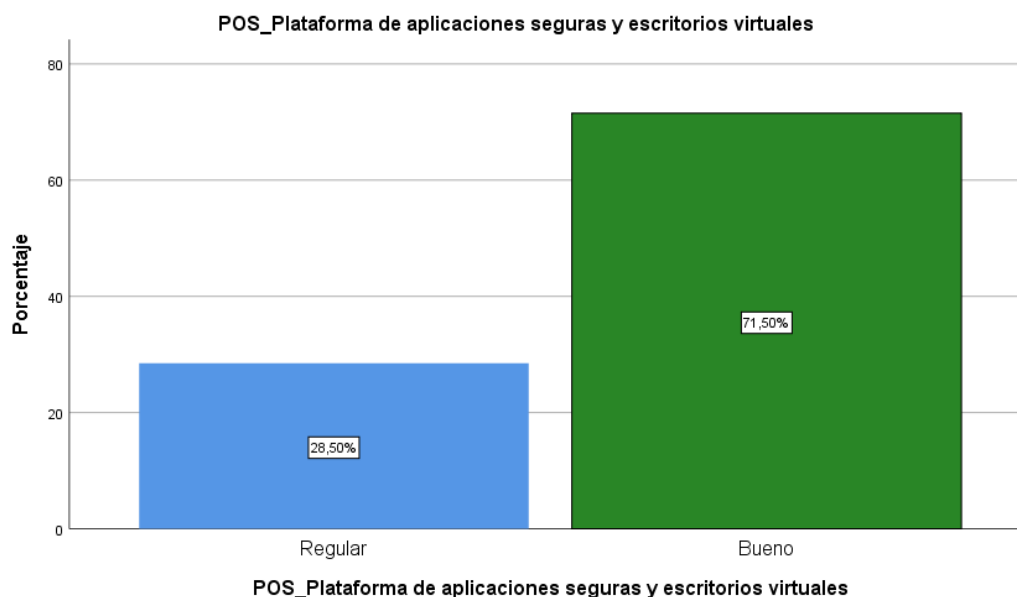
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	114	28,5	28,5	28,5
	Bueno	286	71,5	71,5	100,0
	Total	400	100,0	100,0	

Fuente: Elaboración propia

Grafico

Figura 7.

Frecuencia de la variable *plataforma de aplicaciones seguras y escritorios virtuales*



Fuente: Elaboración propia.

Interpretación. Se observa del total de los usuarios encuestados manifiestan que el 71.50 % es consideran como bueno y el 28.50% consideran como regular el nivel de la variable plataforma de aplicaciones seguras y escritorios virtuales.

Tabla 12.
Frecuencia de la dimensión tecnología y herramientas de comunicación

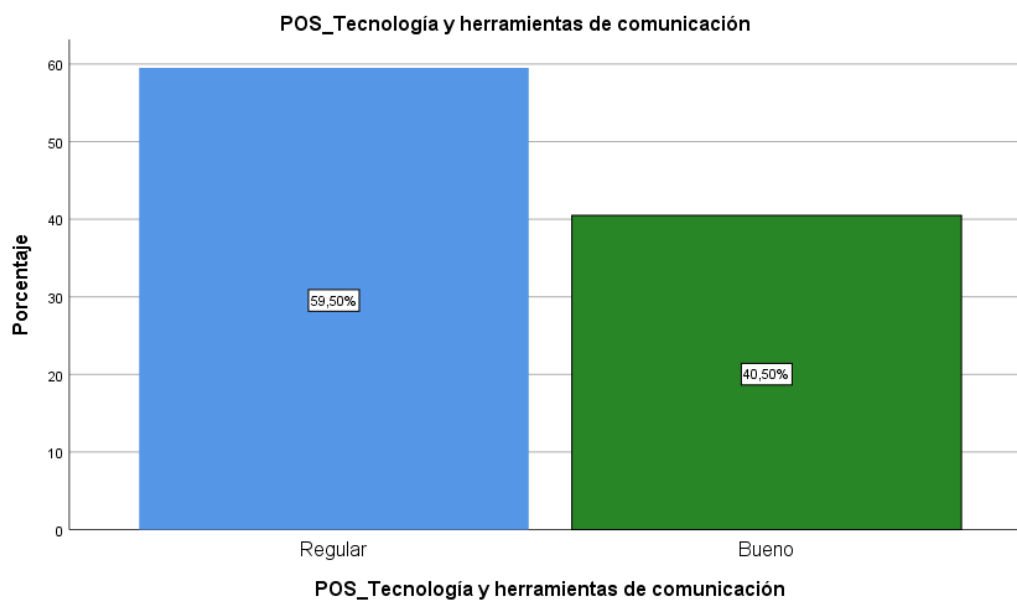
POS_Tecnología y herramientas de comunicación

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	238	59,5	59,5	59,5
	Bueno	162	40,5	40,5	100,0
	Total	400	100,0	100,0	

Fuente: Elaboración propia

Grafico

Figura 8.
Frecuencia de la dimensión tecnología y herramientas de comunicación



Fuente: Elaboración propia

Interpretación. Se observa del total de usuarios encuestados manifiestan que el 59.50 % consideran como regular y el 40.50% consideran como bueno el nivel de la dimensión tecnología y herramientas de comunicación.

Tabla 13.
Frecuencia de la dimensión seguridad y acceso a la información

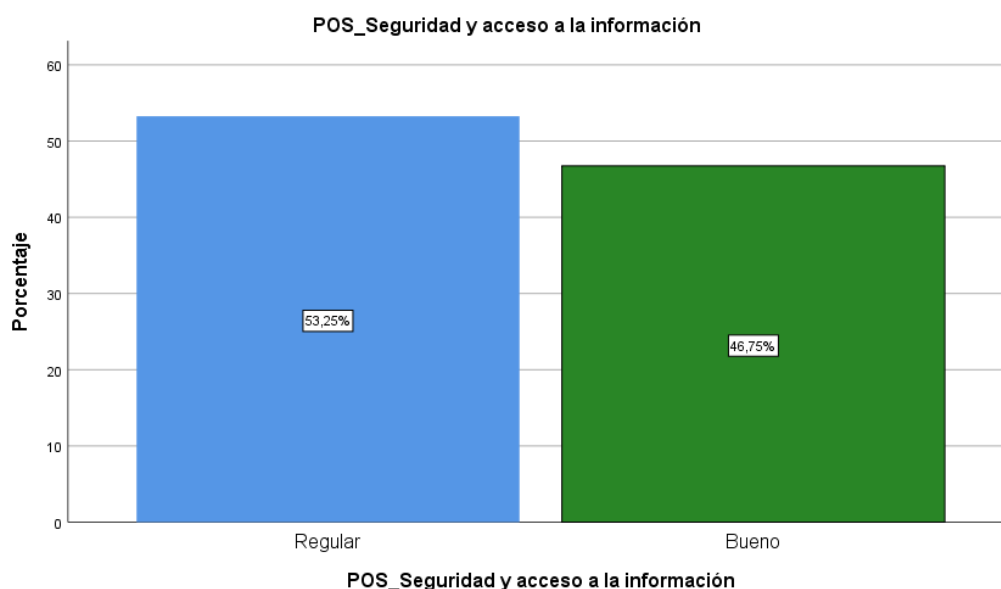
POS_Seguridad y acceso a la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	213	53,3	53,3	53,3
	Bueno	187	46,8	46,8	100,0
	Total	400	100,0	100,0	

Fuente: Elaboración propia

Grafico

Figura 9.
Frecuencia de la dimensión seguridad y acceso a la información



Fuente: Elaboración propia.

Interpretación. Se observa del total de usuarios encuestados manifiestan que el 53.25% consideran como regular y el 46.75% consideran como bueno el nivel de la dimensión Seguridad y acceso a la información.

Tabla 14.
Frecuencia de la dimensión infraestructura de trabajo remoto

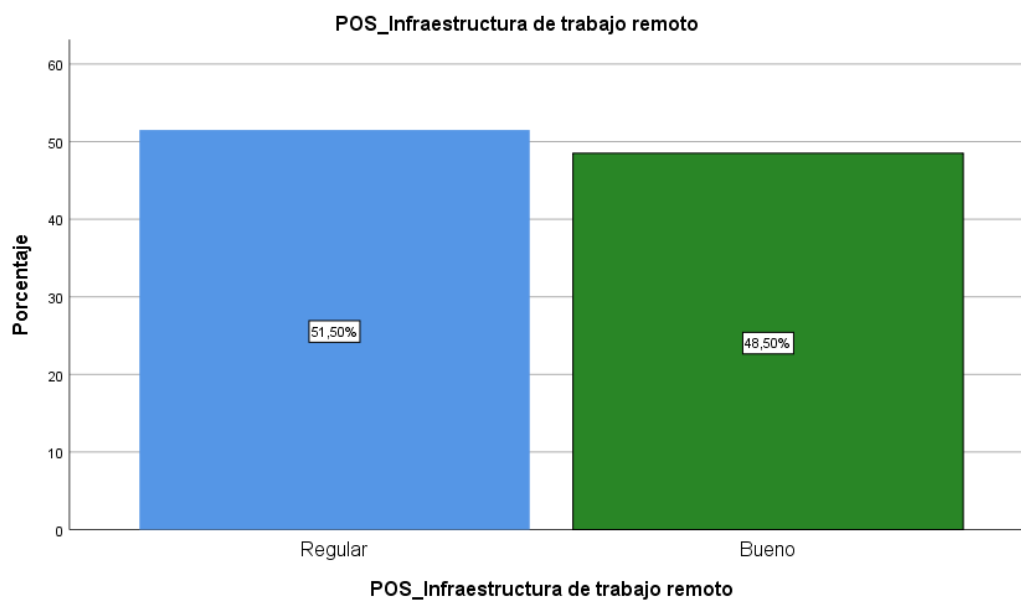
POS_Infraestructura de trabajo remoto

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Regular	206	51,5	51,5	51,5
	Bueno	194	48,5	48,5	100,0
	Total	400	100,0	100,0	

Fuente: Elaboración propia

Grafico

Figura 10:
Frecuencia de la dimensión infraestructura de trabajo remoto



Fuente: Elaboración propia.

Interpretación. Se observa del total de usuarios encuestados manifiestan que el 51.50% consideran como regular y el 48.50% consideran como bueno el nivel de la dimensión infraestructura de trabajo remoto.

3.2. Prueba de normalidad

La prueba de normalidad aplicada fue con el método estadístico de Kolmogorov-Smirnov, debido a que la muestra es mayor a 50. Para la investigación la muestra fue de 400 usuarios encuestados.

$$D = \max |F_n(x) - F_0(x)|$$

Siendo $F_n(x)$ la función de distribución muestral y $F_0(x)$ la función teórica o correspondiente a la población normal especificada en la hipótesis nula.

Hipótesis:

H0: Los datos provienen de una distribución normal

H1: Los datos no provienen de una distribución normal

Decisión: Es significativa si $p > \alpha$, entonces se acepta H0. ($\alpha = 0.05$)

Tabla 15.
Prueba de normalidad

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRE_Plataforma de aplicaciones seguras y escritorios virtuales	,532	400	,000	,085	400	,000
POS_Plataforma de aplicaciones seguras y escritorios virtuales	,451	400	,000	,565	400	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Interpretación:

Se observa que la significancia bilateral de $P = 0.000 < 0.05$, por lo tanto, se rechaza la H0, se infiere que la muestra proviene de una distribución no paramétrica. En tal sentido, para la prueba de hipótesis se utilizó la prueba de los rangos con signo de Wilcoxon.

3.3. Contrastación de las hipótesis

3.3.1. Contrastación de la hipótesis general

Para la prueba de hipótesis se utilizó la prueba de los rangos con signo de Wilcoxon.

H0: Si no se implementa una plataforma segura de aplicaciones y escritorios virtuales entonces no mejora el trabajo remoto en el MINDEF, 2023.

H1: Si, se implementa una plataforma segura de aplicaciones y escritorios virtuales entonces mejora el trabajo remoto en el MINDEF, 2023.

Tabla 16.

Contrastación de la hipótesis general

Rangos				
		N	Rango promedio	Suma de rangos
POS_Plataforma de aplicaciones seguras y escritorios virtuales - PRE_Plataforma de aplicaciones seguras y escritorios virtuales	Rangos negativos	0 ^a	,00	,00
	Rangos positivos	400 ^b	200,50	80200,00
	Empates	0 ^c		
	Total	400		

a. POS_Plataforma de aplicaciones seguras y escritorios virtuales < PRE_Plataforma de aplicaciones seguras y escritorios virtuales

b. POS_Plataforma de aplicaciones seguras y escritorios virtuales > PRE_Plataforma de aplicaciones seguras y escritorios virtuales

c. POS_Plataforma de aplicaciones seguras y escritorios virtuales = PRE_Plataforma de aplicaciones seguras y escritorios virtuales

Estadísticos de prueba^a

	POS_Plataforma de aplicaciones seguras y escritorios virtuales - PRE_Plataforma de aplicaciones seguras y escritorios virtuales
	-18,197 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

Interpretación

Se puede observar de la prueba de los rangos con signo de Wilcoxon, de los totales del pre-test y post-test el $P = 0.000$ es < 0.05 , entonces se rechaza la H0 y aceptamos la H1. Si, se implementa una plataforma segura de aplicaciones y escritorios virtuales entonces mejora el trabajo remoto en el MINDEF, 2023.

Contrastación hipótesis específica 1

H0: Si, no se implementa una infraestructura de virtualización entonces no mejora las tecnología y herramientas de comunicación en el MINDEF, 2023.

H1: Si, se implementa una infraestructura de virtualización entonces mejora las tecnología y herramientas de comunicación en el MINDEF, 2023.

Tabla 17.

Contrastación hipótesis específica 1

Rangos		N	Rango promedio	Suma de rangos
POS_Tecnología y herramientas de comunicación - PRE_Tecnología y herramientas de comunicación	Rangos negativos	0 ^a	,00	,00
	Rangos positivos	171 ^b	86,00	14706,00
	Empates	229 ^c		
	Total	400		

a. POS_Tecnología y herramientas de comunicación < PRE_Tecnología y herramientas de comunicación

b. POS_Tecnología y herramientas de comunicación > PRE_Tecnología y herramientas de comunicación

c. POS_Tecnología y herramientas de comunicación = PRE_Tecnología y herramientas de comunicación

Estadísticos de prueba^a

POS_Tecnología y herramientas de comunicación - PRE_Tecnología y herramientas de comunicación	
Z	-12,766 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

Interpretación: Se puede observar de la prueba de los rangos con signo de Wilcoxon, de los totales del pre-test y post-test el $P = 0.000$ es < 0.05 , entonces se rechaza la H0 y aceptamos la H1. Si, se implementa una infraestructura de virtualización entonces mejora las tecnología y herramientas de comunicación en el MINDEF, 2023.

Contrastación hipótesis específica 2

H0: Si, no se implementa un software de virtualización de escritorio y aplicaciones entonces no mejora la seguridad y acceso a la información en el MINDEF.

H1: Si, se implementa un software de virtualización de escritorio y aplicaciones entonces mejora la seguridad y acceso a la información en el MINDEF.

Tabla 18.
Contrastación hipótesis específica 2

Rangos		N	Rango promedio	Suma de rangos
POS_Seguridad y acceso a la información - PRE_Seguridad y acceso a la información	Rangos negativos	0 ^a	,00	,00
	Rangos positivos	187 ^b	94,00	17578,00
	Empates	213 ^c		
	Total	400		

a. POS_Seguridad y acceso a la información < PRE_Seguridad y acceso a la información

b. POS_Seguridad y acceso a la información > PRE_Seguridad y acceso a la información

c. POS_Seguridad y acceso a la información = PRE_Seguridad y acceso a la información

Estadísticos de prueba^a

	POS_Seguridad y acceso a la información - PRE_Seguridad y acceso a la información
Z	-13,675 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

Interpretación. Se puede observar que se realizó la prueba de los rangos con signo de Wilcoxon, de los totales del pre-test y post-test el $P = 0.000$ es < a 0.05, entonces se rechaza la hipótesis nula y aceptamos la hipótesis alterna. Si, se implementa un software de virtualización de escritorio y aplicaciones entonces mejora la seguridad y acceso a la información en el MINDEF.

Contrastación de la hipótesis específica 3

H0: Si, no se implementa el gestor de conexión entonces no mejora la infraestructura de trabajo remoto en el MINDEF, 2023.

H1: Si, se implementa el gestor de conexión entonces mejora la infraestructura de trabajo remoto en el MINDEF, 2023.

Tabla 19.

Contrastación de la hipótesis específica 3

Rangos			
		N	Rango promedio
POS_Seguridad y acceso a la información - PRE_Infraestructura de trabajo remoto	Rangos negativos	0 ^a	,00
	Rangos positivos	187 ^b	94,00
	Empates	213 ^c	
	Total	400	

a. POS_Seguridad y acceso a la información < PRE_Infraestructura de trabajo remoto

b. POS_Seguridad y acceso a la información > PRE_Infraestructura de trabajo remoto

c. POS_Seguridad y acceso a la información = PRE_Infraestructura de trabajo remoto

Estadísticos de prueba^a

	POS_Seguridad y acceso a la información - PRE_Infraestructura de trabajo remoto
Z	-13,675 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

Interpretación. Se puede observar que se realizó la prueba de los rangos con signo de Wilcoxon, de los totales del pre-test y post-test el $P = 0.000$ es < a 0.05, entonces se rechaza la hipótesis nula y aceptamos la hipótesis alterna. Si, se implementa el gestor de conexión entonces mejora la infraestructura de trabajo remoto en el MINDEF, 2023.

IV. DISCUSION

La investigación tuvo como objetivo principal “Explicar la implementación de una plataforma segura de aplicaciones y escritorios virtuales en la mejora del trabajo remoto en el MINDEF, 2023”. Se puede observar de la prueba de los rangos con signo de Wilcoxon, de los totales del pre-test y post-test el $P = 0.000$ es $< a 0.05$, entonces se rechaza la H_0 y aceptamos la H_1 . Si, se implementa una plataforma segura de aplicaciones y escritorios virtuales entonces mejora del trabajo remoto en el MINDEF, 2023.

De acuerdo al autor (Isidro, 2023) elaboro la tesis “Diseñar una plataforma de virtualización de aplicaciones utilizando terminales de acceso para escritorios virtuales y con alta disponibilidad híbrida para el sistema integrado de administración financiera (SIAF) en la (Dirección de sanidad policial), Universidad Peruana de Ciencias Aplicadas (UPC)”.

Dado que la virtualización se ha convertido en los últimos años en una pieza fundamental para avance y desarrollo tecnológico, esto gracias a que puede con su nivel de abstracción de la Ayuda de hardware a todos los niveles para utilizar eficientemente los recursos computacionales. Esta tesis analiza las diferentes variables de virtualización que son tanto la software y hardware teniendo en cuenta para ello desde servidores hasta terminales acceso a plataformas de virtualización de aplicaciones, desarrollando una investigación exhaustiva tanto a nivel teórico como técnico con pruebas de rendimiento en el equipo en cuestión. La piedra angular para que la virtualización prospere de manera efectiva de aplicaciones es optimizar configuraciones y estimar de forma escalable y fiable tanto hardware como software, ya que se obtienen diferentes resultados según el convergencia de estas tecnologías, tal como se obtiene en las pruebas de rendimiento, todo esto centrándose en la carga de usuarios y el nivel de concurrencia ejemplificándolo

durante el desarrollo de la investigación, aspectos como el tratado de seguridad para la virtualización de la CSA (Cloud Security Alliance) que proporciona una fortaleza a nivel del ecosistema de virtualización de aplicaciones que se está creando para albergar toda la plataforma tecnológica.

Asimismo, el autor (Jara, 2021) desarrollo la tesis “Implementación de una plataforma de virtualización usando amazon web services, para soportar las aplicaciones de la empresa Programate SAC, Para obtener el título de Ingeniero de Sistemas, Universidad Autónoma del Perú. Lima, Perú”

Esta investigación se desarrolló en la empresa Programate S.A.C., en la cual se realizó la implementación de una plataforma de virtualización utilizando Amazon Web Services para las diferentes aplicaciones con las que cuenta la empresa. La plataforma Amazon Web Services cuenta con diferentes servicios los cuales nos facilitan la creación de una plataforma virtual con diferentes tipos de soluciones. El propósito es crear una plataforma virtual para migrar diferentes aplicaciones que tiene la empresa Programate S.A.C. utilizando la plataforma Amazon Web Services. A destacar, utilizar Amazon Web Services estaría en línea con las grandes empresas que están utilizando plataformas en la nube ya que una de las ventajas de estas plataformas es utilizar los últimos desarrollos del siglo XXI. Al finalizar nuestra investigación los resultados que nos dieron fueron favorables para la presente investigación.

.

V. CONCLUSIONES

La presente investigación tiene las siguientes conclusiones:

1. Observamos que el $P = 0.000$ es $< a 0.05$, entonces se rechaza la H_0 y aceptamos la H_1 .
Si, se implementa una plataforma segura de aplicaciones y escritorios virtuales entonces mejora del trabajo remoto en el MINDEF, 2023.
2. Observamos el $P = 0.000$ es $< a 0.05$, entonces se rechaza la H_0 y aceptamos la H_1 . Si, se implementa una infraestructura de virtualización entonces mejora las tecnología y herramientas de comunicación en el MINDEF, 2023.
3. Observamos que el $P = 0.000$ es $< a 0.05$, entonces se rechaza la hipótesis nula y aceptamos la hipótesis alterna. Si, se implementa un software de virtualización de escritorio y aplicaciones entonces mejora la seguridad y acceso a la información en el MINDEF.
4. Observamos el $P = 0.000$ es $< a 0.05$, entonces se rechaza la hipótesis nula y aceptamos la hipótesis alterna. Si, se implementa el gestor de conexión entonces mejora la infraestructura de trabajo remoto en el MINDEF, 2023.

VI. RECOMENDACIONES

En función a los resultados obtenidos en la presente investigación, se han realizado las siguientes recomendaciones de la implementación de una plataforma segura de aplicaciones y escritorios virtuales entonces mejora el trabajo remoto en el MINDEF, 2023

1. Hacer seguimiento a la implementación de la plataforma segura de aplicaciones y escritorios virtuales para mejorar el trabajo remoto en el MINDEF, 2023.
2. Monitorear la implementación de la infraestructura de virtualización para mejorar las tecnología y herramientas de comunicación en el MINDEF, 2023.
3. Elaborar un plan de seguimiento y monitoreo de la implementación del software de virtualización de escritorio y aplicaciones para mejorar la seguridad y acceso a la información en el MINDEF.
4. Implementar controles del proceso implementación del gestor de conexión para mejorar la infraestructura de trabajo remoto en el MINDEF, 2023.

IV. REFERENCIAS BIBLIOGRÁFICAS

- Ander-Egg, E., & Aguilar, M. (2018). *Investigación acción participativa: Paradigmas y metodologías (9a ed.)*. Indoamericana.
- Apple. (2023). *Plataforma de aplicaciones*. Apple Inc.
- Arias, F. G. (2012). *El Proyecto de Investigación, Introducción a la metodología científica, 6ª Edición*. Editorial Episteme.
- Davenport, T. H., & Prusak, L. (2000). *Working knowledge: How organizations manage what they know (2.ª ed.)*. Harvard Business School Press.
- Díaz, G. R., & Avendaño, A. J. (2022). Diseño de una plataforma virtual para la optimización de recursos tecnológicos en la empresa Maint. *Trabajo de titulación previo a la obtención del título de Magister en Telecomunicaciones*. Escuela Superior Politecnica del Litoral, Guayaquil, Ecuador.
- Hernández, S. R., Fernández, C. C., & Baptista, L. P. (12 de 09 de 2014). *Metodología de la investigación (Quinta ed.)*. (M. G. S.A., Ed.) Mexico, Mexico: McGraw Hill.
- Hurtado de Barrera, J. (2012). *El proyecto de investigación Comprensión holística de la metodología y la investigación*. Caracas, Venezuela: Ediciones Quirón .
- Isidro, C. F. (2023). Diseñar una plataforma de virtualización de aplicaciones utilizando terminales de acceso para escritorios virtuales y con alta disponibilidad híbrida para el sistema integrado de administración financiera (SIAF) en la (Dirección de sanidad policial). *Para optar el título profesional de Ingeniero de Redes y Comunicaciones*. Universidad Peruana de Ciencias Aplicadas (UPC), Lima , Perú.
- Jara, C. T. (2021). Implementación de una plataforma de virtualización usando amazon web services, para soportar las aplicaciones de la empresa Programate SAC. *Para obtener el título de Ingeniero de Sistemas*. Universidad Autónoma del Perú, Lima, Perú.

- Laudon, K. M., & Laudon, J. P. (2022). *Sistemas de información gerenciales (15a ed.)*. Pearson Educación.
- Llesquen, C. R. (2020). “Implementación de la plataforma virtual Microsoft Teams en la gestión educativa de la Institución Educativa Privada Nuestro Maravilloso Mundo, Lima, 2020”. *Para optar el grado de Maestra en Administración de la Educación*. Universidad Cesar Vallejo, Lima , Perú.
- Martínez, J. A., & Rodríguez, M. C. (2016). *Sistemas de información gerencial: Un enfoque práctico (5a ed.)*. Pearson Educación.
- Ñaupas, H., Mejía, E., Novoa, E., & Villagómez, A. (2014). *Metodología de la Investigación*. Colombia: Ediciones de la U.
- Ñaupas, P. H., Mejía, M. E., & Novoa, R. E. (2014). *Metodología de la investigación Cuantitativa - Cualitativa y Redacción de la Tesis*. Bogotá, Colombia: Ediciones de la U -.
- Olson, G. M., & Olson, J. S. (2014). *Working together apart: Collaboration over the internet. Synthesis Lectures on Human-Centered Informatics*. Morgan & Claypool Publishers.
- Palella, S. S., & Martins, P. F. (2006). *Metodologia de la investigacion cuantitativa*. Caracas: FEDUPEL.
- Pedhazur, E. J., & Schmelkin, L. P. (2013). *Measurement, design, and analysis: An integrated approach*. psychology press.
- Raya, C. J., Raya, G. L., & Zurdo, j. (2014). *Sistemas informáticos*. Ra-Ma Editorial.
- Rodríguez, M. E. (2005). *Metodología de la Investigación*. (U. J. Tabasco, Ed.) Tabasco, México. Obtenido de https://books.google.com.pe/books?id=r4yrEW9Jhe0C&pg=PA25&dq=investigacion++tipo+descriptiva&hl=es&sa=X&ved=2ahUKEwigx_blu7nyAhWqEbkGHVH

3C1wQ6AEwAHoECAQQAg#v=onepage&q=investigacion%20%20tipo%20descrip
 ptiva&f=false

Sabino, C. (2019). *Investigación cualitativa en salud: Nuevos paradigmas, conceptos y métodos (3a ed.)*. Eco Ediciones.

Sachintha, F. (2024). El futuro del trabajo: escritorios virtuales en la nube y su impacto en la eficiencia y seguridad del lugar de trabajo. *Researchgate*, 1-9.

Sánchez-Vega, L. (2017). *Procesamiento de datos: Conceptos, herramientas y aplicaciones (2a ed.)*. Editorial Pirámide.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating system concepts (10.ª ed.)*. Wiley.

Stallings, W. (2015). *Foundations of modern networking: SDN, NFV, QoE, IoT, and cloud*. Pearson.

Tamayo y Tamayo, M. (2008). *El proceso de la investigacion cientifica*. México D.F.: EDITORIAL LIMUSA. S.A. DE C.v.

Tamayo, T. M. (2004). *El proceso de la investigación científica* (Cuarta edición ed.). (2. Editorial Limusa, Ed.) Balderas, México: EDITORIAL LIMUSA, S.A. DE C.V.

Obtenido de

https://books.google.com.pe/books?id=BhymmEqkkJwC&pg=PA176&dq=poblacion+y+muestra+de+una+investigacion&hl=es&sa=X&ved=2ahUKEwi_oMmdx_PyAhWAGLkGHdVNDsYQ6AF6BAGJEAI#v=onepage&q=poblacion%20y%20muestra%20de%20una%20investigacion&f=false

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks (5.ª ed.)*. Pearson.

Whitman, M. E., & Mattord, H. J. (2017). *Principles of information security (6.ª ed.)*. Cengage Learning.

- Zai, A. H., Wong, S., Guilarte-Walker, Y., Langlois, P., Apurv, S. C., McManus, D. D., & Luzuriaga, K. (2024). Implementación de escritorios virtuales para investigación clínica en un centro de salud académico: reporte de un caso. *Oxford University Press on behalf of the American Medical Informatics Association*, 1 - 7.
doi:<https://doi.org/10.1093/jamiaopen/ooae083>
- Zurdo, M. A., Raya, G. J., Raya, & M., C. L. (2014). *Sistemas de información: Teoría y práctica (2a ed.)*. McGraw-Hill Education.

ANEXOS

Anexo 01: Matriz de Consistencia

Tabla 20.
Matriz de consistencia

Problemas General	Objetivos General	Hipótesis General	Variables Independiente	Indicador V.I.	Variables Dependiente	Indicador V.D.
¿Cómo influye la implementación de una plataforma de aplicaciones seguras y escritorios virtuales en la mejora del trabajo remoto en el MINDEF, 2023?	Explicar la influencia de la implementación de una plataforma de aplicaciones seguras y escritorios virtuales en la mejora del trabajo remoto en el MINDEF, 2023.	Si, existe influencia de la implementación de una plataforma de aplicaciones seguras y escritorios virtuales entonces mejora del trabajo remoto en el MINDEF, 2023.	Plataforma de aplicaciones seguras y escritorios virtuales	----	Trabajo remoto	----
Problemas Especifico	Objetivos Específicos	Hipótesis Especificas				
a) ¿Cómo influye infraestructura de virtualización en la mejora de las tecnología y herramientas de comunicación en el MINDEF, 2023?	a) Explicar la influencia de la infraestructura de virtualización en la mejora de las tecnología y herramientas de comunicación en el MINDEF, 2023.	a) Si, existe influencia de la infraestructura de virtualización entonces mejora las tecnología y herramientas de comunicación en el MINDEF, 2023.	Infraestructura de virtualización	Si / No	Tecnología y herramientas de comunicación	Numero de dispositivos conectados Nivel de compatibilidad Soporte de múltiples aplicaciones
b) ¿Cómo influye el software de virtualización de escritorio y aplicaciones en la mejora de la seguridad y acceso a la información en el MINDEF, 2023?	b) Explicar la influencia del software de virtualización de escritorio y aplicaciones en la mejora de la seguridad y acceso a la información en el MINDEF.	b) Si, existe influencia del software de virtualización de escritorio y aplicaciones entonces mejora la seguridad y acceso a la información en el MINDEF.	Software de virtualización de escritorio y aplicaciones	Si / No	Seguridad y acceso a la información	Nivel de autonomía Nivel de disponibilidad ante fallos Tasa de Incidentes de Seguridad
c) ¿Cómo influye el gestor de conexión en la mejora de la infraestructura de trabajo remoto en el MINDEF, 2023?	c) Explicar la influencia del gestor de conexión en la mejora de la infraestructura de trabajo remoto en el MINDEF, 2023.	c) Si, existe influencia del gestor de conexión entonces mejora la infraestructura de trabajo remoto en el MINDEF, 2023.	Gestor de conexión	Si / No	Infraestructura de trabajo remoto	Nivel de autenticación Algoritmo de autenticación

Anexo 02: Instrumento de recolección de datos

CUESTIONARIO DE PREGUNTAS

El objetivo general fue “Explicar la influencia de la implementación de una plataforma de aplicaciones seguras y escritorios virtuales en la mejora del trabajo remoto en el MINDEF, 2023.”. Marque con X en el casillero de acuerdo a la siguiente escala valorativa.

Escala Valorativa

Muy malo	Malo	Regular	Bueno	Muy bueno
1	2	3	4	5

Nº	VD: TRABAJO REMOTO	ESCALA				
		1	2	3	4	5
D1: Tecnología y herramientas de comunicación						
# dispositivos conectados						
1	¿Los dispositivos con conexión de escritorio virtual funcionan adecuadamente?					
2	Nivel de compatibilidad ¿Todos los dispositivos de cómputo tienen un nivel de compatibilidad para el trabajo remoto?					
3	Soporte de múltiples aplicaciones ¿Cómo considera, el software de aplicaciones que se utiliza para la conexión remota?					
4	¿Cree Ud. ¿Que la plataforma de escritorio virtuales soportara para trabajar con diversos softwares en el trabajo remoto?					
D2: Seguridad y acceso a la información						
Nivel de autonomía						
5	¿Cree Ud. que el acceso a la intranet a través de la plataforma de aplicaciones y escritorios virtuales es confiable?					
6	Nivel de disponibilidad ante fallos ¿Cómo calificas tener el servicio de una plataforma de aplicaciones seguras y escritorios virtuales para garantizar la continuidad de los servicios?					
7	Tasa de incidentes de seguridad ¿La implementación de una plataforma de aplicaciones seguras y escritorios virtuales reduce la tasa de incidentes de seguridad?					
8	¿Cómo califica las herramientas de protección de seguridad informática que tiene los escritorios virtuales?					
D3: Infraestructura de trabajo remoto						
Nivel de autenticación						
9	¿Cómo califica el nivel de autenticación de la plataforma de aplicaciones y escritorios virtuales del Ministerio?					
10	¿Cómo califica Ud. el nivel de acceso a la plataforma?					
11	Algoritmo de autenticación ¿Cómo califica el nivel de dificultad de los usuarios y contraseñas?					
12	¿Consideras adecuado la infraestructura actual para que el trabajo remoto sea seguro?					

Juicio de expertos


UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
INGENIERÍA DE SISTEMAS E INFORMÁTICA
VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "Implementación de una plataforma segura de aplicaciones y escritorios virtuales para mejorar el trabajo remoto en el Ministerio de Defensa, 2023"

PRESENTADO POR (Tesistas): Bach. Castillo Yarlequé, Javier Francisco
 Bach. Pineda Becerra, Jorge Guillermo

I. DATOS GENERALES DEL EXPERTO N°: 01

- 1.1. Apellidos y Nombres: Corlila Baquerizo, Eduardo Cancio
 1.2. Grado Académico : Mg. Investigación y Docencia Universitaria
 1.3. Cargo e Institución donde Labora: Docente Univesitario, Investigador y Jefe de Proyectos de TIC - INEI
 1.4. Tipo de Instrumento de Evaluación: ENCUESTA

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Está expresado en conducta observable				X	
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Existe organización Lógica					X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					X
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología				X	
8. COHERENCIA	Entre índices, indicadores y dimensiones					X
9. METODOLOGÍA	Responde al propósito del trabajo bajo los objetivos a lograr.				X	

II. OPCION DE APLICABILIDAD : Se puede aplicar el Instrumento.....

III. PROMEDIO DE VALORACIÓN: 88%.....

IV. RECOMENDACIONES : Ninguno

Firma del experto:

Fecha: 28/10/2024

DNI : 20037930



UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
INGENIERÍA DE SISTEMAS E INFORMÁTICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "Implementación de una plataforma segura de aplicaciones y escritorios virtuales para mejorar el trabajo remoto en el Ministerio de Defensa, 2023"

PRESENTADO POR (Tesisistas): Bach. Castillo Yarlequé, Javier Francisco
 Bach. Pineda Becerra, Jorge Guillermo

I. DATOS GENERALES DEL EXPERTO N°: 02

- 1.1. Apellidos y Nombres: Cubas Lozano, Flor Yanina
 1.2. Grado Académico : Ingeniero de Sistemas y Computo
 1.3. Cargo e Institución donde Labora: Consultor Senior de Desarrollo de Sistemas - Freelance
 1.4. Tipo de Instrumento de Evaluación: **ENCUESTA**

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Está expresado en conducta observable				X	
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Existe organización Lógica					X
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					X
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología				X	
8. COHERENCIA	Entre índices, indicadores y dimensiones				X	
x	Responde al propósito del trabajo bajo los objetivos a lograr.					X

II. OPCION DE APLICABILIDAD : Que se aplique

III. PROMEDIO DE VALORACIÓN: 85%.....

IV. RECOMENDACIONES : Ninguno

Firma del experto:

FLOR YANINA CUBAS LOZANO
 Ingeniera de Sistemas y Computo
 CIP N° 381220

Fecha: 25/10/2024

DNI : 71702871



UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE CIENCIAS E INGENIERÍA
INGENIERÍA DE SISTEMAS E INFORMÁTICA

VALIDACIÓN DE INSTRUMENTO

TÍTULO DE LA TESIS: "Implementación de una plataforma segura de aplicaciones y escritorios virtuales para mejorar el trabajo remoto en el Ministerio de Defensa, 2023"

PRESENTADO POR (Tesis): Bach. Castillo Yarlequé, Javier Francisco
 Bach. Pineda Becerra, Jorge Guillermo

I. DATOS GENERALES DEL EXPERTO N°: 03

- 1.1. Apellidos y Nombres : Gonzales Calderón, José Ramos
 1.2. Grado Académico : Maestro en Gestión de Tecnologías de la Información
 1.3. Cargo e Institución donde Labora: Docente, Consultor de Proyectos - RENIEC
 1.4. Tipo de Instrumento de Evaluación: ENCUESTA

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 40%	BUENO 41 – 60%	MUY BUENO 61 – 80%	EXCELENTE 81 – 100%
1. CLARIDAD	Está formulado con lenguaje apropiado					X
2. OBJETIVIDAD	Está expresado en conducta observable					X
3. ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					X
4. ORGANIZACIÓN	Existe organización Lógica				X	
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad					X
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					X
7. CONSISTENCIA	Se basa en aspectos teóricos, científicos acordes a la tecnología				X	
8. COHERENCIA	Entre índices, indicadores y dimensiones					X
9. METODOLOGÍA	Responde al propósito del trabajo bajo los objetivos a lograr				X	

II. OPCIÓN DE APLICABILIDAD : Se puede aplicar el cuestionario.....

III. PROMEDIO DE VALORACIÓN : 89%.....

IV. RECOMENDACIONES : Ninguno.....

Firma del experto:

Fecha: 31/10/2024

DNI : 17541317

Anexo 03: Base de datos

Pre test

	Tecnología y herramientas de comunicación				Seguridad y acceso a la información				Infraestructura de trabajo remoto											
N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	TOTAL	N_V2	D1	ND1	D2	ND2	D3	ND3
1	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	12	2	16	2
2	3	2	2	2	1	2	2	2	2	4	4	2	28	1	9	2	7	2	12	2
3	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
4	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
5	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
6	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
7	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
8	1	2	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
9	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
10	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
11	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
12	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
13	2	1	2	2	1	2	1	2	2	2	1	1	19	1	7	2	6	2	6	2
14	1	2	2	2	2	2	2	2	2	1	1	1	20	1	7	2	8	2	5	2
15	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
16	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
17	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
18	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
19	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
20	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
21	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
22	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
23	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
24	1	2	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
25	2	2	2	2	2	2	2	2	2	2	1	1	22	1	8	2	8	2	6	2
26	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
27	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
28	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
29	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
30	1	2	2	2	2	2	2	2	2	1	1	1	20	1	7	2	8	2	5	2
31	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
32	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
33	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
34	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
35	2	1	2	2	1	2	1	2	2	1	1	1	18	1	7	2	6	2	5	2
36	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
37	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
38	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
39	3	1	2	1	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2

40	2	2	2	1	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
41	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
42	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
43	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
44	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
45	1	1	2	2	1	2	1	2	2	2	1	1	18	1	6	2	6	2	6	2
46	3	2	2	2	2	2	2	2	2	1	1	1	22	1	9	2	8	2	5	2
47	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
48	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
49	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
50	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
51	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
52	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
53	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
54	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
55	1	1	2	1	1	2	2	2	2	1	1	1	17	1	5	2	7	2	5	2
56	3	2	2	1	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
57	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
58	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
59	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
60	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
61	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
62	2	2	2	2	2	2	2	2	2	1	1	1	21	1	8	2	8	2	5	2
63	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
64	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
65	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
66	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
67	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
68	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
69	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
70	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
71	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
72	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
73	4	2	2	2	2	2	2	2	2	2	1	1	24	1	10	2	8	2	6	2
74	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
75	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
76	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
77	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
78	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
79	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
80	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
81	2	2	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
82	1	1	1	1	1	2	2	2	2	1	1	1	16	1	4	1	7	2	5	2
83	2	2	2	2	1	2	2	3	2	1	1	1	21	1	8	2	8	2	5	2
84	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2

85	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
86	4	2	2	2	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
87	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
88	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
89	1	1	2	2	1	2	2	2	2	1	1	2	19	1	6	2	7	2	6	2
90	3	2	2	2	1	2	1	2	2	1	1	1	20	1	9	2	6	2	5	2
91	2	1	1	1	1	2	2	2	2	1	1	1	17	1	5	2	7	2	5	2
92	3	2	2	2	1	2	2	3	2	1	1	1	22	1	9	2	8	2	5	2
93	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	12	2	16	2
94	3	2	2	2	1	2	2	2	2	4	4	2	28	1	9	2	7	2	12	2
95	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
96	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
97	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
98	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
99	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	12	2	16	2
100	3	2	2	2	1	2	2	2	2	4	4	2	28	1	9	2	7	2	12	2
101	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
102	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
103	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
104	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
105	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
106	1	2	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
107	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
108	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
109	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
110	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
111	2	1	2	2	1	2	1	2	2	2	1	1	19	1	7	2	6	2	6	2
112	1	2	2	2	2	2	2	2	2	1	1	1	20	1	7	2	8	2	5	2
113	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
114	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
115	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
116	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
117	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
118	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
119	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
120	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
121	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
122	1	2	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
123	2	2	2	2	2	2	2	2	2	2	1	1	22	1	8	2	8	2	6	2
124	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
125	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
126	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
127	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
128	1	2	2	2	2	2	2	2	2	1	1	1	20	1	7	2	8	2	5	2
129	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2

130	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
131	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
132	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
133	2	1	2	2	1	2	1	2	2	1	1	1	18	1	7	2	6	2	5	2
134	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
135	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
136	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
137	3	1	2	1	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
138	2	2	2	1	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
139	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
140	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
141	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
142	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
143	1	1	2	2	1	2	1	2	2	2	1	1	18	1	6	2	6	2	6	2
144	3	2	2	2	2	2	2	2	2	1	1	1	22	1	9	2	8	2	5	2
145	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
146	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
147	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
148	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
149	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
150	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
151	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
152	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
153	1	1	2	1	1	2	2	2	2	1	1	1	17	1	5	2	7	2	5	2
154	3	2	2	1	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
155	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
156	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
157	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
158	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
159	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
160	2	2	2	2	2	2	2	2	2	1	1	1	21	1	8	2	8	2	5	2
161	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
162	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
163	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
164	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
165	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
166	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
167	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
168	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
169	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
170	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
171	4	2	2	2	2	2	2	2	2	2	1	1	24	1	10	2	8	2	6	2
172	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
173	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
174	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2

175	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
176	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
177	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
178	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
179	2	2	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
180	1	1	1	1	1	2	2	2	2	1	1	1	16	1	4	1	7	2	5	2
181	2	2	2	2	1	2	2	3	2	1	1	1	21	1	8	2	8	2	5	2
182	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
183	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
184	4	2	2	2	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
185	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
186	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
187	1	1	2	2	1	2	2	2	2	1	1	2	19	1	6	2	7	2	6	2
188	3	2	2	2	1	2	1	2	2	1	1	1	20	1	9	2	6	2	5	2
189	2	1	1	1	1	2	2	2	2	1	1	1	17	1	5	2	7	2	5	2
190	3	2	2	2	1	2	2	3	2	1	1	1	22	1	9	2	8	2	5	2
191	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
192	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
193	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
194	2	2	2	2	2	2	2	2	2	1	1	1	21	1	8	2	8	2	5	2
195	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
196	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
197	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
198	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
199	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
200	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
201	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
202	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
203	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
204	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
205	4	2	2	2	2	2	2	2	2	2	1	1	24	1	10	2	8	2	6	2
206	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
207	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
208	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
209	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
210	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
211	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
212	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
213	2	2	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
214	1	1	1	1	1	2	2	2	2	1	1	1	16	1	4	1	7	2	5	2
215	2	2	2	2	1	2	2	3	2	1	1	1	21	1	8	2	8	2	5	2
216	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
217	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
218	4	2	2	2	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
219	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2

220	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
221	1	1	2	2	1	2	2	2	2	1	1	2	19	1	6	2	7	2	6	2
222	3	2	2	2	1	2	1	2	2	1	1	1	20	1	9	2	6	2	5	2
223	2	1	1	1	1	2	2	2	2	1	1	1	17	1	5	2	7	2	5	2
224	3	2	2	2	1	2	2	3	2	1	1	1	22	1	9	2	8	2	5	2
225	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
226	4	2	2	2	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
227	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
228	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
229	1	1	2	2	1	2	2	2	2	1	1	2	19	1	6	2	7	2	6	2
230	3	2	2	2	1	2	1	2	2	1	1	1	20	1	9	2	6	2	5	2
231	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	12	2	16	2
232	3	2	2	2	1	2	2	2	2	4	4	2	28	1	9	2	7	2	12	2
233	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
234	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
235	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
236	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
237	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
238	1	2	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
239	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
240	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
241	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
242	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
243	2	1	2	2	1	2	1	2	2	2	1	1	19	1	7	2	6	2	6	2
244	1	2	2	2	2	2	2	2	2	1	1	1	20	1	7	2	8	2	5	2
245	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
246	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
247	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
248	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
249	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
250	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
251	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
252	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
253	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
254	1	2	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
255	2	2	2	2	2	2	2	2	2	2	1	1	22	1	8	2	8	2	6	2
256	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
257	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
258	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
259	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
260	1	2	2	2	2	2	2	2	2	1	1	1	20	1	7	2	8	2	5	2
261	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
262	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
263	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
264	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2

265	2	1	2	2	1	2	1	2	2	1	1	1	18	1	7	2	6	2	5	2
266	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
267	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
268	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
269	3	1	2	1	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
270	2	2	2	1	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
271	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
272	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
273	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
274	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
275	1	1	2	2	1	2	1	2	2	2	1	1	18	1	6	2	6	2	6	2
276	3	2	2	2	2	2	2	2	2	1	1	1	22	1	9	2	8	2	5	2
277	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
278	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
279	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
280	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
281	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
282	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
283	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
284	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
285	1	1	2	1	1	2	2	2	2	1	1	1	17	1	5	2	7	2	5	2
286	3	2	2	1	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
287	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
288	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
289	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
290	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
291	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
292	2	2	2	2	2	2	2	2	2	1	1	1	21	1	8	2	8	2	5	2
293	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
294	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
295	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
296	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
297	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
298	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
299	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
300	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
301	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
302	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
303	4	2	2	2	2	2	2	2	2	2	1	1	24	1	10	2	8	2	6	2
304	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
305	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
306	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
307	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
308	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
309	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2

310	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
311	2	2	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
312	1	1	1	1	1	2	2	2	2	1	1	1	16	1	4	1	7	2	5	2
313	2	2	2	2	1	2	2	3	2	1	1	1	21	1	8	2	8	2	5	2
314	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
315	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
316	4	2	2	2	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
317	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
318	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
319	1	1	2	2	1	2	2	2	2	1	1	2	19	1	6	2	7	2	6	2
320	3	2	2	2	1	2	1	2	2	1	1	1	20	1	9	2	6	2	5	2
321	2	1	1	1	1	2	2	2	2	1	1	1	17	1	5	2	7	2	5	2
322	3	2	2	2	1	2	2	3	2	1	1	1	22	1	9	2	8	2	5	2
323	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	12	2	16	2
324	3	2	2	2	1	2	2	2	2	4	4	2	28	1	9	2	7	2	12	2
325	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
326	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
327	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
328	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
329	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
330	1	2	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
331	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
332	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
333	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
334	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
335	2	1	2	2	1	2	1	2	2	2	1	1	19	1	7	2	6	2	6	2
336	1	2	2	2	2	2	2	2	2	1	1	1	20	1	7	2	8	2	5	2
337	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
338	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
339	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
340	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
341	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
342	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
343	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
344	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
345	2	1	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
346	1	2	2	1	1	2	2	2	2	1	1	1	18	1	6	2	7	2	5	2
347	2	2	2	2	2	2	2	2	2	2	1	1	22	1	8	2	8	2	6	2
348	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
349	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
350	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
351	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
352	1	2	2	2	2	2	2	2	2	1	1	1	20	1	7	2	8	2	5	2
353	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
354	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2

355	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
356	1	2	2	2	1	2	2	2	2	1	1	2	20	1	7	2	7	2	6	2
357	2	1	2	2	1	2	1	2	2	1	1	1	18	1	7	2	6	2	5	2
358	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
359	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
360	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
361	3	1	2	1	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
362	2	2	2	1	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
363	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
364	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
365	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
366	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
367	1	1	2	2	1	2	1	2	2	2	1	1	18	1	6	2	6	2	6	2
368	3	2	2	2	2	2	2	2	2	1	1	1	22	1	9	2	8	2	5	2
369	3	1	1	1	1	2	2	3	2	1	1	1	19	1	6	2	8	2	5	2
370	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
371	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
372	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
373	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
374	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
375	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
376	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
377	1	1	2	1	1	2	2	2	2	1	1	1	17	1	5	2	7	2	5	2
378	3	2	2	1	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
379	3	2	2	2	2	2	2	2	2	2	1	1	23	1	9	2	8	2	6	2
380	2	2	2	2	1	2	2	2	2	2	1	1	21	1	8	2	7	2	6	2
381	1	2	2	2	1	2	2	2	2	2	1	1	20	1	7	2	7	2	6	2
382	2	2	2	2	1	2	2	2	2	1	1	2	21	1	8	2	7	2	6	2
383	3	1	2	2	1	2	1	2	2	2	1	1	20	1	8	2	6	2	6	2
384	2	2	2	2	2	2	2	2	2	1	1	1	21	1	8	2	8	2	5	2
385	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
386	3	2	2	2	1	2	2	2	2	2	1	1	22	1	9	2	7	2	6	2
387	1	2	2	2	1	2	2	2	2	1	1	1	19	1	7	2	7	2	5	2
388	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
389	3	1	2	2	1	2	1	2	2	1	1	1	19	1	8	2	6	2	5	2
390	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
391	1	1	1	1	1	2	2	3	2	1	1	1	17	1	4	1	8	2	5	2
392	2	2	2	2	1	2	2	2	2	1	1	1	20	1	8	2	7	2	5	2
393	5	1	2	1	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
394	5	2	2	1	1	2	2	2	2	1	1	1	22	1	10	2	7	2	5	2
395	4	2	2	2	2	2	2	2	2	2	1	1	24	1	10	2	8	2	6	2
396	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2
397	3	2	2	2	1	2	2	2	2	1	1	2	22	1	9	2	7	2	6	2
398	1	1	2	2	1	2	1	2	2	1	1	1	17	1	6	2	6	2	5	2
399	3	2	2	2	1	2	2	2	2	1	1	1	21	1	9	2	7	2	5	2

400	2	1	1	1	1	2	2	3	2	1	1	1	18	1	5	2	8	2	5	2
-----	---	---	---	---	---	---	---	---	---	---	---	---	----	---	---	---	---	---	---	---

Pos test

	Tecnología y herramientas de comunicación				Seguridad y acceso a la información				Infraestructura de trabajo remoto												
N°	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	POS	N_V2	D1	ND1	D2	ND2	D3	ND3	PRE
1	4	4	4	5	4	4	4	4	5	5	4	4	51	3	17	3	16	2	18	3	40
2	3	4	4	5	5	4	4	4	5	5	4	4	51	3	16	2	17	3	18	3	28
3	4	4	4	5	4	5	5	4	5	4	5	4	53	3	17	3	18	3	18	3	17
4	4	4	4	4	5	4	4	4	4	4	4	4	49	3	16	2	17	3	16	2	21
5	4	4	4	4	4	4	4	4	5	5	5	5	52	3	16	2	16	2	20	3	18
6	4	4	4	5	5	4	4	5	5	5	5	5	55	3	17	3	18	3	20	3	21
7	4	3	4	4	4	4	4	3	4	4	3	4	45	2	15	2	15	2	15	2	18
8	3	3	4	4	3	3	3	3	3	3	4	4	40	2	14	2	12	2	14	2	18
9	4	4	4	5	5	4	4	4	5	5	5	5	54	3	17	3	17	3	20	3	23
10	5	5	4	5	5	4	4	5	5	5	5	4	56	3	19	3	18	3	19	3	20
11	5	5	5	5	4	4	5	4	4	4	5	5	55	3	20	3	17	3	18	3	22
12	4	5	4	5	4	5	5	5	5	5	4	5	56	3	18	3	19	3	19	3	22
13	4	4	4	5	5	4	4	4	5	5	4	4	52	3	17	3	17	3	18	3	19
14	5	4	4	5	4	5	4	3	5	5	5	5	54	3	18	3	16	2	20	3	20
15	4	4	4	3	4	5	4	4	4	4	4	4	48	3	15	2	17	3	16	2	18
16	4	4	5	5	4	5	4	4	4	5	5	3	52	3	18	3	17	3	17	3	22
17	4	4	3	5	4	4	4	3	5	5	4	4	49	3	16	2	15	2	18	3	21
18	4	4	4	5	4	5	5	4	5	5	4	4	53	3	17	3	18	3	18	3	20
19	4	4	3	4	4	4	4	3	4	5	5	5	49	3	15	2	15	2	19	3	19
20	4	3	3	4	4	3	3	3	4	4	4	4	43	2	14	2	13	2	16	2	19
21	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	19
22	3	3	3	4	2	3	3	2	2	2	3	3	33	2	13	2	10	2	10	2	21
23	5	5	5	3	3	3	3	3	3	3	5	4	45	2	18	3	12	2	15	2	18
24	3	3	3	4	3	3	4	4	4	3	4	3	41	2	13	2	14	2	14	2	18
25	4	3	4	3	4	3	4	5	4	4	4	3	45	2	14	2	16	2	15	2	22
26	4	4	3	5	5	4	4	4	5	5	4	3	50	3	16	2	17	3	17	3	22
27	3	3	3	4	4	3	3	3	4	4	4	4	42	2	13	2	13	2	16	2	21
28	3	4	4	3	3	3	4	4	4	4	4	4	44	2	14	2	14	2	16	2	20
29	4	4	3	4	4	4	4	4	4	4	5	5	49	3	15	2	16	2	18	3	20

30	5	5	5	4	4	5	4	5	5	4	5	5	56	3	19	3	18	3	19	3	20
31	4	4	3	4	3	4	4	4	4	4	4	4	46	2	15	2	15	2	16	2	19
32	4	4	4	4	4	3	3	4	4	4	4	4	46	2	16	2	14	2	16	2	22
33	4	5	5	4	4	4	5	5	4	5	4	4	53	3	18	3	18	3	17	3	20
34	4	4	4	4	3	4	4	4	4	5	5	4	49	3	16	2	15	2	18	3	20
35	4	3	4	4	3	3	3	4	3	4	4	4	43	2	15	2	13	2	15	2	18
36	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	12	2	16	2	21
37	5	5	5	4	4	4	4	4	4	4	4	4	51	3	19	3	16	2	16	2	19
38	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	20
39	4	4	3	4	4	4	4	4	4	4	4	4	47	3	15	2	16	2	16	2	19
40	5	5	5	5	5	5	5	5	5	5	5	5	60	3	20	3	20	3	20	3	19
41	5	5	5	5	5	5	5	5	5	5	5	5	60	3	20	3	20	3	20	3	23
42	4	3	4	3	4	4	3	4	3	4	4	3	43	2	14	2	15	2	14	2	21
43	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	20
44	4	4	4	4	4	4	4	4	4	5	4	4	49	3	16	2	16	2	17	3	22
45	4	4	3	3	3	3	4	4	4	3	4	4	43	2	14	2	14	2	15	2	18
46	4	4	4	4	4	3	3	4	4	4	5	4	47	3	16	2	14	2	17	3	22
47	4	4	5	4	3	4	5	5	5	4	3	5	51	3	17	3	17	3	17	3	19
48	5	5	4	5	4	5	4	4	4	4	3	5	52	3	19	3	17	3	16	2	21
49	4	4	4	4	5	4	5	4	5	5	4	3	51	3	16	2	18	3	17	3	19
50	4	4	3	4	3	3	4	5	3	4	3	5	45	2	15	2	15	2	15	2	21
51	3	3	4	3	4	4	4	5	3	4	5	5	47	3	13	2	17	3	17	3	19
52	5	4	4	4	5	4	5	4	3	4	4	4	50	3	17	3	18	3	15	2	21
53	4	4	4	4	4	4	4	5	4	5	5	5	52	3	16	2	17	3	19	3	17
54	5	5	5	4	5	4	4	4	4	4	4	4	52	3	19	3	17	3	16	2	21
55	4	4	4	5	4	5	4	3	4	5	4	3	49	3	17	3	16	2	16	2	17
56	4	4	4	5	4	3	4	5	4	4	4	4	49	3	17	3	16	2	16	2	20
57	5	4	5	5	5	5	4	5	5	4	5	4	56	3	19	3	19	3	18	3	23
58	5	4	4	4	4	4	4	5	4	4	4	5	51	3	17	3	17	3	17	3	21
59	4	4	4	4	4	4	4	4	4	4	5	4	49	3	16	2	16	2	17	3	20
60	3	3	3	4	5	3	4	3	3	3	4	5	43	2	13	2	15	2	15	2	21
61	3	4	3	4	5	4	3	4	3	3	3	3	42	2	14	2	16	2	12	2	20
62	4	4	3	5	4	4	4	4	4	3	4	4	47	3	16	2	16	2	15	2	21
63	4	4	4	4	4	5	4	4	5	4	4	4	50	3	16	2	17	3	17	3	17

64	4	4	4	4	5	4	5	5	4	5	5	5	54	3	16	2	19	3	19	3	22
65	3	3	3	4	3	4	4	4	4	4	4	4	44	2	13	2	15	2	16	2	19
66	4	5	4	4	4	5	5	3	5	4	4	4	51	3	17	3	17	3	17	3	22
67	4	4	4	4	4	4	4	4	5	4	5	5	51	3	16	2	16	2	19	3	19
68	5	4	5	4	5	5	5	5	5	5	4	5	57	3	18	3	20	3	19	3	20
69	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	17
70	4	4	5	3	4	4	5	4	5	4	5	4	51	3	16	2	17	3	18	3	20
71	4	4	4	4	4	4	4	5	4	4	4	4	49	3	16	2	17	3	16	2	21
72	5	5	5	5	5	5	5	4	5	4	4	4	56	3	20	3	19	3	17	3	22
73	3	3	3	4	3	4	3	3	3	4	4	5	42	2	13	2	13	2	16	2	24
74	4	3	4	4	4	3	5	4	3	4	5	4	47	3	15	2	16	2	16	2	21
75	4	4	4	4	4	4	4	4	3	4	3	4	46	2	16	2	16	2	14	2	22
76	4	4	5	4	4	4	4	4	4	4	4	4	49	3	17	3	16	2	16	2	17
77	4	5	4	5	4	4	5	4	5	4	4	4	52	3	18	3	17	3	17	3	21
78	4	4	4	4	4	3	3	3	4	3	4	3	43	2	16	2	13	2	14	2	18
79	4	5	5	4	5	4	5	4	4	4	4	4	52	3	18	3	18	3	16	2	21
80	4	4	4	3	3	3	3	4	3	3	3	4	41	2	15	2	13	2	13	2	18
81	3	3	3	3	3	4	3	4	3	4	4	4	41	2	12	2	14	2	15	2	19
82	5	4	5	4	4	4	4	4	5	4	4	4	51	3	18	3	16	2	17	3	16
83	4	4	4	4	3	4	4	4	4	4	5	4	48	3	16	2	15	2	17	3	21
84	4	4	4	4	4	3	3	4	3	3	3	4	43	2	16	2	14	2	13	2	21
85	4	4	4	4	4	4	5	4	5	4	5	5	52	3	16	2	17	3	19	3	22
86	3	4	3	4	3	4	3	4	3	4	3	4	42	2	14	2	14	2	14	2	22
87	4	5	4	3	4	4	4	4	4	4	4	5	49	3	16	2	16	2	17	3	23
88	4	4	4	4	4	4	4	4	4	3	4	4	47	3	16	2	16	2	15	2	21
89	4	5	4	5	5	5	4	5	4	4	4	4	53	3	18	3	19	3	16	2	19
90	4	4	4	4	4	4	4	4	4	5	4	4	49	3	16	2	16	2	17	3	20
91	3	3	3	3	3	3	3	3	3	3	3	3	36	2	12	2	12	2	12	2	17
92	3	4	4	4	4	4	4	4	4	4	4	4	47	3	15	2	16	2	16	2	22
93	4	4	4	5	4	4	4	4	5	5	4	4	51	3	16	2	18	3	18	3	17
94	3	4	4	5	5	4	4	4	5	5	4	4	51	3	17	3	18	3	18	3	16
95	4	4	4	5	4	5	5	4	5	4	5	4	53	3	18	3	18	3	18	3	17
96	4	4	4	4	5	4	4	4	4	4	4	4	49	3	17	3	16	2	16	2	16
97	4	4	4	4	4	4	4	4	5	5	5	5	52	3	16	2	20	3	20	3	16

98	4	4	4	5	5	4	4	5	5	5	5	5	55	3	18	3	20	3	20	3	17
99	4	4	4	5	4	4	4	4	5	5	4	4	51	3	16	2	18	3	18	3	17
100	3	4	4	5	5	4	4	4	5	5	4	4	51	3	17	3	18	3	18	3	16
101	4	4	4	5	4	5	5	4	5	4	5	4	53	3	18	3	18	3	18	3	17
102	4	4	4	4	5	4	4	4	4	4	4	4	49	3	17	3	16	2	16	2	16
103	4	4	4	4	4	4	4	4	5	5	5	5	52	3	16	2	20	3	20	3	16
104	4	4	4	5	5	4	4	5	5	5	5	5	55	3	18	3	20	3	20	3	17
105	4	3	4	4	4	4	4	3	4	4	3	4	45	2	15	2	15	2	15	2	15
106	3	3	4	4	3	3	3	3	3	3	4	4	40	2	12	2	14	2	14	2	14
107	4	4	4	5	5	4	4	4	5	5	5	5	54	3	17	3	20	3	20	3	17
108	5	5	4	5	5	4	4	5	5	5	5	4	56	3	18	3	19	3	19	3	19
109	5	5	5	5	4	4	5	4	4	4	5	5	55	3	17	3	18	3	18	3	20
110	4	5	4	5	4	5	5	5	5	5	4	5	56	3	19	3	19	3	19	3	18
111	4	4	4	5	5	4	4	4	5	5	4	4	52	3	17	3	18	3	18	3	17
112	5	4	4	5	4	5	4	3	5	5	5	5	54	3	16	2	20	3	20	3	18
113	4	4	4	3	4	5	4	4	4	4	4	4	48	3	17	3	16	2	16	2	15
114	4	4	5	5	4	5	4	4	4	5	5	3	52	3	17	3	17	3	17	3	18
115	4	4	3	5	4	4	4	3	5	5	4	4	49	3	15	2	18	3	18	3	16
116	4	4	4	5	4	5	5	4	5	5	4	4	53	3	18	3	18	3	18	3	17
117	4	4	3	4	4	4	4	3	4	5	5	5	49	3	15	2	19	3	19	3	15
118	4	3	3	4	4	3	3	3	4	4	4	4	43	2	13	2	16	2	16	2	14
119	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
120	3	3	3	4	2	3	3	2	2	2	3	3	33	2	10	2	10	2	10	2	13
121	5	5	5	3	3	3	3	3	3	3	5	4	45	2	12	2	15	2	15	2	18
122	3	3	3	4	3	3	4	4	4	3	4	3	41	2	14	2	14	2	14	2	13
123	4	3	4	3	4	3	4	5	4	4	4	3	45	2	16	2	15	2	15	2	14
124	4	4	3	5	5	4	4	4	5	5	4	3	50	3	17	3	17	3	17	3	16
125	3	3	3	4	4	3	3	3	4	4	4	4	42	2	13	2	16	2	16	2	13
126	3	4	4	3	3	3	4	4	4	4	4	4	44	2	14	2	16	2	16	2	14
127	4	4	3	4	4	4	4	4	4	4	5	5	49	3	16	2	18	3	18	3	15
128	5	5	5	4	4	5	4	5	5	4	5	5	56	3	18	3	19	3	19	3	19
129	4	4	3	4	3	4	4	4	4	4	4	4	46	2	15	2	16	2	16	2	15
130	4	4	4	4	4	3	3	4	4	4	4	4	46	2	14	2	16	2	16	2	16
131	4	5	5	4	4	4	5	5	4	5	4	4	53	3	18	3	17	3	17	3	18

132	4	4	4	4	3	4	4	4	4	5	5	4	49	3	15	2	18	3	18	3	16
133	4	3	4	4	3	3	3	4	3	4	4	4	43	2	13	2	15	2	15	2	15
134	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	16	2	16	2	12
135	5	5	5	4	4	4	4	4	4	4	4	4	51	3	16	2	16	2	16	2	19
136	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
137	4	4	3	4	4	4	4	4	4	4	4	4	47	3	16	2	16	2	16	2	15
138	5	5	5	5	5	5	5	5	5	5	5	5	60	3	20	3	20	3	20	3	20
139	5	5	5	5	5	5	5	5	5	5	5	5	60	3	20	3	20	3	20	3	20
140	4	3	4	3	4	4	3	4	3	4	4	3	43	2	15	2	14	2	14	2	14
141	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
142	4	4	4	4	4	4	4	4	4	5	4	4	49	3	16	2	17	3	17	3	16
143	4	4	3	3	3	3	4	4	4	3	4	4	43	2	14	2	15	2	15	2	14
144	4	4	4	4	4	3	3	4	4	4	5	4	47	3	14	2	17	3	17	3	16
145	4	4	5	4	3	4	5	5	5	4	3	5	51	3	17	3	17	3	17	3	17
146	5	5	4	5	4	5	4	4	4	4	3	5	52	3	17	3	16	2	16	2	19
147	4	4	4	4	5	4	5	4	5	5	4	3	51	3	18	3	17	3	17	3	16
148	4	4	3	4	3	3	4	5	3	4	3	5	45	2	15	2	15	2	15	2	15
149	3	3	4	3	4	4	4	5	3	4	5	5	47	3	17	3	17	3	17	3	13
150	5	4	4	4	5	4	5	4	3	4	4	4	50	3	18	3	15	2	15	2	17
151	4	4	4	4	4	4	4	5	4	5	5	5	52	3	17	3	19	3	19	3	16
152	5	5	5	4	5	4	4	4	4	4	4	4	52	3	17	3	16	2	16	2	19
153	4	4	4	5	4	5	4	3	4	5	4	3	49	3	16	2	16	2	16	2	17
154	4	4	4	5	4	3	4	5	4	4	4	4	49	3	16	2	16	2	16	2	17
155	5	4	5	5	5	5	4	5	5	4	5	4	56	3	19	3	18	3	18	3	19
156	5	4	4	4	4	4	4	5	4	4	4	5	51	3	17	3	17	3	17	3	17
157	4	4	4	4	4	4	4	4	4	4	5	4	49	3	16	2	17	3	17	3	16
158	3	3	3	4	5	3	4	3	3	3	4	5	43	2	15	2	15	2	15	2	13
159	3	4	3	4	5	4	3	4	3	3	3	3	42	2	16	2	12	2	12	2	14
160	4	4	3	5	4	4	4	4	4	3	4	4	47	3	16	2	15	2	15	2	16
161	4	4	4	4	4	5	4	4	5	4	4	4	50	3	17	3	17	3	17	3	16
162	4	4	4	4	5	4	5	5	4	5	5	5	54	3	19	3	19	3	19	3	16
163	3	3	3	4	3	4	4	4	4	4	4	4	44	2	15	2	16	2	16	2	13
164	4	5	4	4	4	5	5	3	5	4	4	4	51	3	17	3	17	3	17	3	17
165	4	4	4	4	4	4	4	4	5	4	5	5	51	3	16	2	19	3	19	3	16

166	5	4	5	4	5	5	5	5	5	5	4	5	57	3	20	3	19	3	19	3	18
167	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
168	4	4	5	3	4	4	5	4	5	4	5	4	51	3	17	3	18	3	18	3	16
169	4	4	4	4	4	4	4	5	4	4	4	4	49	3	17	3	16	2	16	2	16
170	5	5	5	5	5	5	5	4	5	4	4	4	56	3	19	3	17	3	17	3	20
171	3	3	3	4	3	4	3	3	3	4	4	5	42	2	13	2	16	2	16	2	13
172	4	3	4	4	4	3	5	4	3	4	5	4	47	3	16	2	16	2	16	2	15
173	4	4	4	4	4	4	4	4	3	4	3	4	46	2	16	2	14	2	14	2	16
174	4	4	5	4	4	4	4	4	4	4	4	4	49	3	16	2	16	2	16	2	17
175	4	5	4	5	4	4	5	4	5	4	4	4	52	3	17	3	17	3	17	3	18
176	4	4	4	4	4	3	3	3	4	3	4	3	43	2	13	2	14	2	14	2	16
177	4	5	5	4	5	4	5	4	4	4	4	4	52	3	18	3	16	2	16	2	18
178	4	4	4	3	3	3	3	4	3	3	3	4	41	2	13	2	13	2	13	2	15
179	3	3	3	3	3	4	3	4	3	4	4	4	41	2	14	2	15	2	15	2	12
180	5	4	5	4	4	4	4	4	5	4	4	4	51	3	16	2	17	3	17	3	18
181	4	4	4	4	3	4	4	4	4	4	5	4	48	3	15	2	17	3	17	3	16
182	4	4	4	4	4	3	3	4	3	3	3	4	43	2	14	2	13	2	13	2	16
183	4	4	4	4	4	4	5	4	5	4	5	5	52	3	17	3	19	3	19	3	16
184	3	4	3	4	3	4	3	4	3	4	3	4	42	2	14	2	14	2	14	2	14
185	4	5	4	3	4	4	4	4	4	4	4	5	49	3	16	2	17	3	17	3	16
186	4	4	4	4	4	4	4	4	4	3	4	4	47	3	16	2	15	2	15	2	16
187	4	5	4	5	5	5	4	5	4	4	4	4	53	3	19	3	16	2	16	2	18
188	4	4	4	4	4	4	4	4	4	5	4	4	49	3	16	2	17	3	17	3	16
189	3	3	3	3	3	3	3	3	3	3	3	3	36	2	12	2	12	2	12	2	12
190	3	4	4	4	4	4	4	4	4	4	4	4	47	3	16	2	16	2	16	2	15
191	4	4	4	4	5	4	5	4	5	5	4	3	51	3	18	3	17	3	17	3	16
192	4	4	3	4	3	3	4	5	3	4	3	5	45	2	15	2	15	2	15	2	15
193	3	3	4	3	4	4	4	5	3	4	5	5	47	3	17	3	17	3	17	3	13
194	5	4	4	4	5	4	5	4	3	4	4	4	50	3	18	3	15	2	15	2	17
195	4	4	4	4	4	4	4	5	4	5	5	5	52	3	17	3	19	3	19	3	16
196	5	5	5	4	5	4	4	4	4	4	4	4	52	3	17	3	16	2	16	2	19
197	4	4	4	5	4	5	4	3	4	5	4	3	49	3	16	2	16	2	16	2	17
198	4	4	4	5	4	3	4	5	4	4	4	4	49	3	16	2	16	2	16	2	17
199	5	4	5	5	5	5	4	5	5	4	5	4	56	3	19	3	18	3	18	3	19

200	5	4	4	4	4	4	4	5	4	4	4	5	51	3	17	3	17	3	17	3	17
201	4	4	4	4	4	4	4	4	4	4	5	4	49	3	16	2	17	3	17	3	16
202	3	3	3	4	5	3	4	3	3	3	4	5	43	2	15	2	15	2	15	2	13
203	3	4	3	4	5	4	3	4	3	3	3	3	42	2	16	2	12	2	12	2	14
204	4	4	3	5	4	4	4	4	4	3	4	4	47	3	16	2	15	2	15	2	16
205	4	4	4	4	4	5	4	4	5	4	4	4	50	3	17	3	17	3	17	3	16
206	4	4	4	4	5	4	5	5	4	5	5	5	54	3	19	3	19	3	19	3	16
207	3	3	3	4	3	4	4	4	4	4	4	4	44	2	15	2	16	2	16	2	13
208	4	5	4	4	4	5	5	3	5	4	4	4	51	3	17	3	17	3	17	3	17
209	4	4	4	4	4	4	4	4	5	4	5	5	51	3	16	2	19	3	19	3	16
210	5	4	5	4	5	5	5	5	5	5	4	5	57	3	20	3	19	3	19	3	18
211	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
212	4	4	5	3	4	4	5	4	5	4	5	4	51	3	17	3	18	3	18	3	16
213	4	4	4	4	4	4	4	5	4	4	4	4	49	3	17	3	16	2	16	2	16
214	5	5	5	5	5	5	5	4	5	4	4	4	56	3	19	3	17	3	17	3	20
215	3	3	3	4	3	4	3	3	3	4	4	5	42	2	13	2	16	2	16	2	13
216	4	3	4	4	4	3	5	4	3	4	5	4	47	3	16	2	16	2	16	2	15
217	4	4	4	4	4	4	4	4	3	4	3	4	46	2	16	2	14	2	14	2	16
218	4	4	5	4	4	4	4	4	4	4	4	4	49	3	16	2	16	2	16	2	17
219	4	5	4	5	4	4	5	4	5	4	4	4	52	3	17	3	17	3	17	3	18
220	4	4	4	4	4	3	3	3	4	3	4	3	43	2	13	2	14	2	14	2	16
221	4	5	5	4	5	4	5	4	4	4	4	4	52	3	18	3	16	2	16	2	18
222	4	4	4	3	3	3	3	4	3	3	3	4	41	2	13	2	13	2	13	2	15
223	3	3	3	3	3	4	3	4	3	4	4	4	41	2	14	2	15	2	15	2	12
224	5	4	5	4	4	4	4	4	5	4	4	4	51	3	16	2	17	3	17	3	18
225	4	4	4	4	3	4	4	4	4	4	5	4	48	3	15	2	17	3	17	3	16
226	4	4	4	4	4	3	3	4	3	3	3	4	43	2	14	2	13	2	13	2	16
227	4	4	4	4	4	4	5	4	5	4	5	5	52	3	17	3	19	3	19	3	16
228	3	4	3	4	3	4	3	4	3	4	3	4	42	2	14	2	14	2	14	2	14
229	4	5	4	3	4	4	4	4	4	4	4	5	49	3	16	2	17	3	17	3	16
230	4	4	4	4	4	4	4	4	4	3	4	4	47	3	16	2	15	2	15	2	16
231	4	4	4	5	4	4	4	4	5	5	4	4	51	3	16	2	18	3	18	3	17
232	3	4	4	5	5	4	4	4	5	5	4	4	51	3	17	3	18	3	18	3	16
233	4	4	4	5	4	5	5	4	5	4	5	4	53	3	18	3	18	3	18	3	17

234	4	4	4	4	5	4	4	4	4	4	4	4	49	3	17	3	16	2	16	2	16
235	4	4	4	4	4	4	4	4	5	5	5	5	52	3	16	2	20	3	20	3	16
236	4	4	4	5	5	4	4	5	5	5	5	5	55	3	18	3	20	3	20	3	17
237	4	3	4	4	4	4	4	3	4	4	3	4	45	2	15	2	15	2	15	2	15
238	3	3	4	4	3	3	3	3	3	3	4	4	40	2	12	2	14	2	14	2	14
239	4	4	4	5	5	4	4	4	5	5	5	5	54	3	17	3	20	3	20	3	17
240	5	5	4	5	5	4	4	5	5	5	5	4	56	3	18	3	19	3	19	3	19
241	5	5	5	5	4	4	5	4	4	4	5	5	55	3	17	3	18	3	18	3	20
242	4	5	4	5	4	5	5	5	5	5	4	5	56	3	19	3	19	3	19	3	18
243	4	4	4	5	5	4	4	4	5	5	4	4	52	3	17	3	18	3	18	3	17
244	5	4	4	5	4	5	4	3	5	5	5	5	54	3	16	2	20	3	20	3	18
245	4	4	4	3	4	5	4	4	4	4	4	4	48	3	17	3	16	2	16	2	15
246	4	4	5	5	4	5	4	4	4	5	5	3	52	3	17	3	17	3	17	3	18
247	4	4	3	5	4	4	4	3	5	5	4	4	49	3	15	2	18	3	18	3	16
248	4	4	4	5	4	5	5	4	5	5	4	4	53	3	18	3	18	3	18	3	17
249	4	4	3	4	4	4	4	3	4	5	5	5	49	3	15	2	19	3	19	3	15
250	4	3	3	4	4	3	3	3	4	4	4	4	43	2	13	2	16	2	16	2	14
251	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
252	3	3	3	4	2	3	3	2	2	2	3	3	33	2	10	2	10	2	10	2	13
253	5	5	5	3	3	3	3	3	3	3	5	4	45	2	12	2	15	2	15	2	18
254	3	3	3	4	3	3	4	4	4	3	4	3	41	2	14	2	14	2	14	2	13
255	4	3	4	3	4	3	4	5	4	4	4	3	45	2	16	2	15	2	15	2	14
256	4	4	3	5	5	4	4	4	5	5	4	3	50	3	17	3	17	3	17	3	16
257	3	3	3	4	4	3	3	3	4	4	4	4	42	2	13	2	16	2	16	2	13
258	3	4	4	3	3	3	4	4	4	4	4	4	44	2	14	2	16	2	16	2	14
259	4	4	3	4	4	4	4	4	4	4	5	5	49	3	16	2	18	3	18	3	15
260	5	5	5	4	4	5	4	5	5	4	5	5	56	3	18	3	19	3	19	3	19
261	4	4	3	4	3	4	4	4	4	4	4	4	46	2	15	2	16	2	16	2	15
262	4	4	4	4	4	3	3	4	4	4	4	4	46	2	14	2	16	2	16	2	16
263	4	5	5	4	4	4	5	5	4	5	4	4	53	3	18	3	17	3	17	3	18
264	4	4	4	4	3	4	4	4	4	5	5	4	49	3	15	2	18	3	18	3	16
265	4	3	4	4	3	3	3	4	3	4	4	4	43	2	13	2	15	2	15	2	15
266	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	16	2	16	2	12
267	5	5	5	4	4	4	4	4	4	4	4	4	51	3	16	2	16	2	16	2	19

268	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
269	4	4	3	4	4	4	4	4	4	4	4	4	47	3	16	2	16	2	16	2	15
270	5	5	5	5	5	5	5	5	5	5	5	5	60	3	20	3	20	3	20	3	20
271	5	5	5	5	5	5	5	5	5	5	5	5	60	3	20	3	20	3	20	3	20
272	4	3	4	3	4	4	3	4	3	4	4	3	43	2	15	2	14	2	14	2	14
273	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
274	4	4	4	4	4	4	4	4	4	5	4	4	49	3	16	2	17	3	17	3	16
275	4	4	3	3	3	3	4	4	4	3	4	4	43	2	14	2	15	2	15	2	14
276	4	4	4	4	4	3	3	4	4	4	5	4	47	3	14	2	17	3	17	3	16
277	4	4	5	4	3	4	5	5	5	4	3	5	51	3	17	3	17	3	17	3	17
278	5	5	4	5	4	5	4	4	4	4	3	5	52	3	17	3	16	2	16	2	19
279	4	4	4	4	5	4	5	4	5	5	4	3	51	3	18	3	17	3	17	3	16
280	4	4	3	4	3	3	4	5	3	4	3	5	45	2	15	2	15	2	15	2	15
281	3	3	4	3	4	4	4	5	3	4	5	5	47	3	17	3	17	3	17	3	13
282	5	4	4	4	5	4	5	4	3	4	4	4	50	3	18	3	15	2	15	2	17
283	4	4	4	4	4	4	4	5	4	5	5	5	52	3	17	3	19	3	19	3	16
284	5	5	5	4	5	4	4	4	4	4	4	4	52	3	17	3	16	2	16	2	19
285	4	4	4	5	4	5	4	3	4	5	4	3	49	3	16	2	16	2	16	2	17
286	4	4	4	5	4	3	4	5	4	4	4	4	49	3	16	2	16	2	16	2	17
287	5	4	5	5	5	5	4	5	5	4	5	4	56	3	19	3	18	3	18	3	19
288	5	4	4	4	4	4	4	5	4	4	4	5	51	3	17	3	17	3	17	3	17
289	4	4	4	4	4	4	4	4	4	4	5	4	49	3	16	2	17	3	17	3	16
290	3	3	3	4	5	3	4	3	3	3	4	5	43	2	15	2	15	2	15	2	13
291	3	4	3	4	5	4	3	4	3	3	3	3	42	2	16	2	12	2	12	2	14
292	4	4	3	5	4	4	4	4	4	3	4	4	47	3	16	2	15	2	15	2	16
293	4	4	4	4	4	5	4	4	5	4	4	4	50	3	17	3	17	3	17	3	16
294	4	4	4	4	5	4	5	5	4	5	5	5	54	3	19	3	19	3	19	3	16
295	3	3	3	4	3	4	4	4	4	4	4	4	44	2	15	2	16	2	16	2	13
296	4	5	4	4	4	5	5	3	5	4	4	4	51	3	17	3	17	3	17	3	17
297	4	4	4	4	4	4	4	4	5	4	5	5	51	3	16	2	19	3	19	3	16
298	5	4	5	4	5	5	5	5	5	5	4	5	57	3	20	3	19	3	19	3	18
299	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
300	4	4	5	3	4	4	5	4	5	4	5	4	51	3	17	3	18	3	18	3	16
301	4	4	4	4	4	4	4	5	4	4	4	4	49	3	17	3	16	2	16	2	16

302	5	5	5	5	5	5	5	4	5	4	4	4	56	3	19	3	17	3	17	3	20
303	3	3	3	4	3	4	3	3	3	4	4	5	42	2	13	2	16	2	16	2	13
304	4	3	4	4	4	3	5	4	3	4	5	4	47	3	16	2	16	2	16	2	15
305	4	4	4	4	4	4	4	4	3	4	3	4	46	2	16	2	14	2	14	2	16
306	4	4	5	4	4	4	4	4	4	4	4	4	49	3	16	2	16	2	16	2	17
307	4	5	4	5	4	4	5	4	5	4	4	4	52	3	17	3	17	3	17	3	18
308	4	4	4	4	4	3	3	3	4	3	4	3	43	2	13	2	14	2	14	2	16
309	4	5	5	4	5	4	5	4	4	4	4	4	52	3	18	3	16	2	16	2	18
310	4	4	4	3	3	3	3	4	3	3	3	4	41	2	13	2	13	2	13	2	15
311	3	3	3	3	3	4	3	4	3	4	4	4	41	2	14	2	15	2	15	2	12
312	5	4	5	4	4	4	4	4	5	4	4	4	51	3	16	2	17	3	17	3	18
313	4	4	4	4	3	4	4	4	4	4	5	4	48	3	15	2	17	3	17	3	16
314	4	4	4	4	4	3	3	4	3	3	3	4	43	2	14	2	13	2	13	2	16
315	4	4	4	4	4	4	5	4	5	4	5	5	52	3	17	3	19	3	19	3	16
316	3	4	3	4	3	4	3	4	3	4	3	4	42	2	14	2	14	2	14	2	14
317	4	5	4	3	4	4	4	4	4	4	4	5	49	3	16	2	17	3	17	3	16
318	4	4	4	4	4	4	4	4	4	3	4	4	47	3	16	2	15	2	15	2	16
319	4	5	4	5	5	5	4	5	4	4	4	4	53	3	19	3	16	2	16	2	18
320	4	4	4	4	4	4	4	4	4	5	4	4	49	3	16	2	17	3	17	3	16
321	3	3	3	3	3	3	3	3	3	3	3	3	36	2	12	2	12	2	12	2	12
322	3	4	4	4	4	4	4	4	4	4	4	4	47	3	16	2	16	2	16	2	15
323	4	4	4	5	4	4	4	4	5	5	4	4	51	3	16	2	18	3	18	3	17
324	3	4	4	5	5	4	4	4	5	5	4	4	51	3	17	3	18	3	18	3	16
325	4	4	4	5	4	5	5	4	5	4	5	4	53	3	18	3	18	3	18	3	17
326	4	4	4	4	5	4	4	4	4	4	4	4	49	3	17	3	16	2	16	2	16
327	4	4	4	4	4	4	4	4	5	5	5	5	52	3	16	2	20	3	20	3	16
328	4	4	4	5	5	4	4	5	5	5	5	5	55	3	18	3	20	3	20	3	17
329	4	3	4	4	4	4	4	3	4	4	3	4	45	2	15	2	15	2	15	2	15
330	3	3	4	4	3	3	3	3	3	3	4	4	40	2	12	2	14	2	14	2	14
331	4	4	4	5	5	4	4	4	5	5	5	5	54	3	17	3	20	3	20	3	17
332	5	5	4	5	5	4	4	5	5	5	5	4	56	3	18	3	19	3	19	3	19
333	5	5	5	5	4	4	5	4	4	4	5	5	55	3	17	3	18	3	18	3	20
334	4	5	4	5	4	5	5	5	5	5	4	5	56	3	19	3	19	3	19	3	18
335	4	4	4	5	5	4	4	4	5	5	4	4	52	3	17	3	18	3	18	3	17

336	5	4	4	5	4	5	4	3	5	5	5	5	54	3	16	2	20	3	20	3	18
337	4	4	4	3	4	5	4	4	4	4	4	4	48	3	17	3	16	2	16	2	15
338	4	4	5	5	4	5	4	4	4	5	5	3	52	3	17	3	17	3	17	3	18
339	4	4	3	5	4	4	4	3	5	5	4	4	49	3	15	2	18	3	18	3	16
340	4	4	4	5	4	5	5	4	5	5	4	4	53	3	18	3	18	3	18	3	17
341	4	4	3	4	4	4	4	3	4	5	5	5	49	3	15	2	19	3	19	3	15
342	4	3	3	4	4	3	3	3	4	4	4	4	43	2	13	2	16	2	16	2	14
343	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
344	3	3	3	4	2	3	3	2	2	2	3	3	33	2	10	2	10	2	10	2	13
345	5	5	5	3	3	3	3	3	3	3	5	4	45	2	12	2	15	2	15	2	18
346	3	3	3	4	3	3	4	4	4	3	4	3	41	2	14	2	14	2	14	2	13
347	4	3	4	3	4	3	4	5	4	4	4	3	45	2	16	2	15	2	15	2	14
348	4	4	3	5	5	4	4	4	5	5	4	3	50	3	17	3	17	3	17	3	16
349	3	3	3	4	4	3	3	3	4	4	4	4	42	2	13	2	16	2	16	2	13
350	3	4	4	3	3	3	4	4	4	4	4	4	44	2	14	2	16	2	16	2	14
351	4	4	3	4	4	4	4	4	4	4	5	5	49	3	16	2	18	3	18	3	15
352	5	5	5	4	4	5	4	5	5	4	5	5	56	3	18	3	19	3	19	3	19
353	4	4	3	4	3	4	4	4	4	4	4	4	46	2	15	2	16	2	16	2	15
354	4	4	4	4	4	3	3	4	4	4	4	4	46	2	14	2	16	2	16	2	16
355	4	5	5	4	4	4	5	5	4	5	4	4	53	3	18	3	17	3	17	3	18
356	4	4	4	4	3	4	4	4	4	5	5	4	49	3	15	2	18	3	18	3	16
357	4	3	4	4	3	3	3	4	3	4	4	4	43	2	13	2	15	2	15	2	15
358	3	3	3	3	3	3	3	3	4	4	4	4	40	2	12	2	16	2	16	2	12
359	5	5	5	4	4	4	4	4	4	4	4	4	51	3	16	2	16	2	16	2	19
360	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
361	4	4	3	4	4	4	4	4	4	4	4	4	47	3	16	2	16	2	16	2	15
362	5	5	5	5	5	5	5	5	5	5	5	5	60	3	20	3	20	3	20	3	20
363	5	5	5	5	5	5	5	5	5	5	5	5	60	3	20	3	20	3	20	3	20
364	4	3	4	3	4	4	3	4	3	4	4	3	43	2	15	2	14	2	14	2	14
365	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
366	4	4	4	4	4	4	4	4	4	5	4	4	49	3	16	2	17	3	17	3	16
367	4	4	3	3	3	3	4	4	4	3	4	4	43	2	14	2	15	2	15	2	14
368	4	4	4	4	4	3	3	4	4	4	5	4	47	3	14	2	17	3	17	3	16
369	4	4	5	4	3	4	5	5	5	4	3	5	51	3	17	3	17	3	17	3	17

370	5	5	4	5	4	5	4	4	4	4	3	5	52	3	17	3	16	2	16	2	19
371	4	4	4	4	5	4	5	4	5	5	4	3	51	3	18	3	17	3	17	3	16
372	4	4	3	4	3	3	4	5	3	4	3	5	45	2	15	2	15	2	15	2	15
373	3	3	4	3	4	4	4	5	3	4	5	5	47	3	17	3	17	3	17	3	13
374	5	4	4	4	5	4	5	4	3	4	4	4	50	3	18	3	15	2	15	2	17
375	4	4	4	4	4	4	4	5	4	5	5	5	52	3	17	3	19	3	19	3	16
376	5	5	5	4	5	4	4	4	4	4	4	4	52	3	17	3	16	2	16	2	19
377	4	4	4	5	4	5	4	3	4	5	4	3	49	3	16	2	16	2	16	2	17
378	4	4	4	5	4	3	4	5	4	4	4	4	49	3	16	2	16	2	16	2	17
379	5	4	5	5	5	5	4	5	5	4	5	4	56	3	19	3	18	3	18	3	19
380	5	4	4	4	4	4	4	5	4	4	4	5	51	3	17	3	17	3	17	3	17
381	4	4	4	4	4	4	4	4	4	4	5	4	49	3	16	2	17	3	17	3	16
382	3	3	3	4	5	3	4	3	3	3	4	5	43	2	15	2	15	2	15	2	13
383	3	4	3	4	5	4	3	4	3	3	3	3	42	2	16	2	12	2	12	2	14
384	4	4	3	5	4	4	4	4	4	3	4	4	47	3	16	2	15	2	15	2	16
385	4	4	4	4	4	5	4	4	5	4	4	4	50	3	17	3	17	3	17	3	16
386	4	4	4	4	5	4	5	5	4	5	5	5	54	3	19	3	19	3	19	3	16
387	3	3	3	4	3	4	4	4	4	4	4	4	44	2	15	2	16	2	16	2	13
388	4	5	4	4	4	5	5	3	5	4	4	4	51	3	17	3	17	3	17	3	17
389	4	4	4	4	4	4	4	4	5	4	5	5	51	3	16	2	19	3	19	3	16
390	5	4	5	4	5	5	5	5	5	5	4	5	57	3	20	3	19	3	19	3	18
391	4	4	4	4	4	4	4	4	4	4	4	4	48	3	16	2	16	2	16	2	16
392	4	4	5	3	4	4	5	4	5	4	5	4	51	3	17	3	18	3	18	3	16
393	4	4	4	4	4	4	4	5	4	4	4	4	49	3	17	3	16	2	16	2	16
394	5	5	5	5	5	5	5	4	5	4	4	4	56	3	19	3	17	3	17	3	20
395	3	3	3	4	3	4	3	3	3	4	4	5	42	2	13	2	16	2	16	2	13
396	4	3	4	4	4	3	5	4	3	4	5	4	47	3	16	2	16	2	16	2	15
397	4	4	4	4	4	4	4	4	3	4	3	4	46	2	16	2	14	2	14	2	16
398	4	4	5	4	4	4	4	4	4	4	4	4	49	3	16	2	16	2	16	2	17
399	4	5	4	5	4	4	5	4	5	4	4	4	52	3	17	3	17	3	17	3	18
400	4	4	4	4	4	3	3	3	4	3	4	3	43	2	13	2	14	2	14	2	16

Anexo 04: Evidencia de similitud digital



Página 1 of 99 - Portada

Identificador de la entrega tmoid::13080055462

Jorge Guillermo Pineda Becerra

“Implementación de una plataforma segura de aplicaciones y escritorios virtuales para mejorar el trabajo remoto en el Minis...

TRABAJO

TALLER 2024

Universidad Peruana de Ciencias e Informática

Detalles del documento

Identificador de la entrega

tmoid::13080055462

Fecha de entrega

15 nov 2024, 1:19 a.m. GMT-5

Fecha de descarga

15 nov 2024, 1:27 a.m. GMT-5

Nombre de archivo

TESIS_CASTILLO_PINEDA_14_11_2024.docx

Tamaño de archivo

606.3 KB

95 Páginas

30,629 Palabras

98,398 Caracteres



Página 1 of 99 - Portada

Identificador de la entrega tmoid::13080055462

8% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 15 palabras)

Fuentes principales

- 8%  Fuentes de Internet
- 1%  Publicaciones
- 4%  Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

-  **Texto oculto**
5 caracteres sospechosos en N.º de páginas
El texto es alterado para mezclarse con el fondo blanco del documento.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Anexo 05: Autorización de publicación en repositorio



FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACIÓN O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: Castillo Yarlequé Javier Francisco _____

DNI: 09049422 _____ Correo electrónico: javierex_cy@hotmail.com _____

Domicilio: Av. Surco 270, Santiago de Surco - Lima _____

Teléfono fijo: _____ Teléfono celular: 983708363 _____

2.- IDENTIFICACIÓN DEL TRABAJO Ó TESIS

Facultad/Escuela: Facultad de Ciencias e Ingeniería _____

Tipo: Trabajo de Investigación Bachiller () Tesis (X)

Título del Trabajo de Investigación / Tesis:

"Implementación de una Plataforma Segura de Aplicaciones y Escritorios Virtuales para mejorar el trabajo remoto del Ministerio de Defensa; 2023"

3.- OBTENER:

Bachiller () Título (X) Mg. () Dr. () PhD. ()

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (<http://repositorio.upci.edu.pe>), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):

(X) Sí, autorizo el depósito y publicación total.

() No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los
16 días del mes de noviembre de 2024.

Firma





FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACIÓN O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: Pineda Becerra Jorge Guillermo

DNI: 05788684 Correo electrónico: jpineda2000@gmail.com

Domicilio: Pasaje Buenaventura 141 dpto 401 Breña-Lima

Teléfono fijo: _____ Teléfono celular: 959118829

2.- IDENTIFICACIÓN DEL TRABAJO O TESIS

Facultad/Escuela: Facultad de Ciencias e Ingeniería

Tipo: Trabajo de Investigación Bachiller () Tesis (X)

Título del Trabajo de Investigación / Tesis:

"Implementación de una Plataforma Segura de Aplicaciones y Escritorios Virtuales para mejorar el
trabajo remoto del Ministerio de Defensa; 2023"

3.- OBTENER:

Bachiller () Título (X) Mg. () Dr. () PhD. ()

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (<http://repositorio.upci.edu.pe>), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):

(X) SI, autorizo el depósito y publicación total.

() No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los
16 días del mes de noviembre de 2024.

Firma



Anexo 06: Implementación de la solución

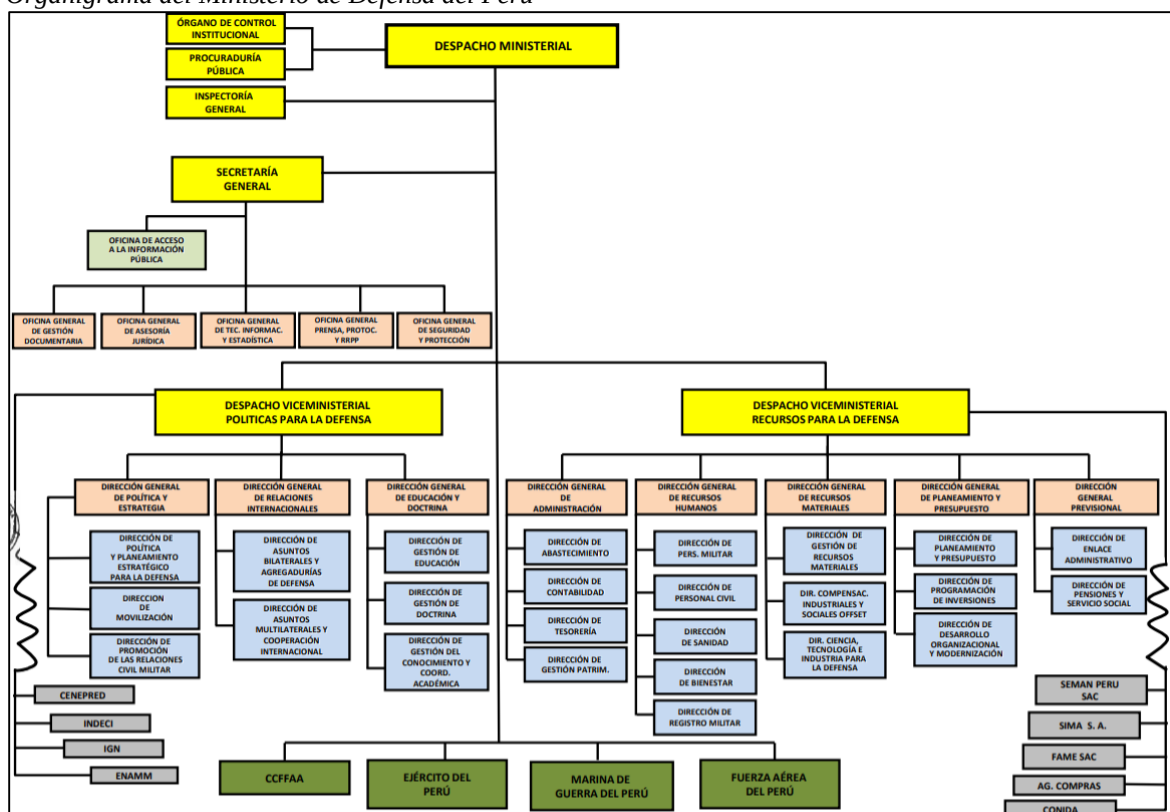
Descripción de la empresa

El Ministerio de Defensa fue creado por la Ley N°24654 y entro en vigencia el 1 de abril de 1987, para garantizar la soberanía, independencia del territorio y participar en el desarrollo nacional, a través de operaciones humanitarias como también en la gestión de riesgos de desastres. Esta encargada de dirigir, ejecutar supervisar y evaluar la Política de Seguridad y Defensa Nacional, en concordancia con lo dispuesto por el presidente de la República del Perú en calidad de Jefe Supremo de las Fuerzas Armadas.

Con respecto a Defensa Civil se realiza un trabajo compartido con los gobiernos regionales y locales, para realizar las labores que sean necesarias de forma preventiva, detección y respuesta ante incidentes que pongan en riesgo a los ciudadanos.

Figura1.

Organigrama del Ministerio de Defensa del Perú



Fuente: https://www.mindef.gob.pe/informacion/documentos/Organigrama_MINDEF.pdf, el 05 oct 2020

Incidentes de seguridad 2022 – 2023

A continuación, se muestra el registro de incidentes de seguridad reportados en el Ministerio de Defensa, durante los años 2022 y 2023:

Tabla 1.
Incidentes de seguridad año 2022

Evento de seguridad	Cantidad de incidentes de seguridad												Total de incidentes de seguridad por evento
	Ene-22	Feb-22	Mar-22	Abr-22	May-22	Jun-22	Jul-22	Ago-22	Set-22	Oct-22	Nov-22	Dic-22	
Software malicioso del tipo keylogger	0	0	1	0	0	0	1	0	0	0	0	1	3
Descargar un Ransomware	2	2	1	1	1	2	1	2	2	1	2	2	19
Propagar un malware	0	0	0	0	0	0	1	0	0	0	0	1	2
Ingeniería social / Phishing	1	2	0	2	1	1	1	2	1	2	1	2	16
Ejecución del malware	2	2	1	2	1	1	1	2	1	2	2	2	19
Robo de información	0	0	0	0	0	0	0	0	0	0	0	0	0
Total de Incidentes Mensual	5	6	3	5	3	4	5	6	4	5	5	8	59

Fuente: Elaboración propia

Tabla 2.
Incidentes incidentes año 2023

Evento de seguridad	Cantidad de incidentes de seguridad									Total de incidentes de seguridad por evento
	Ene-23	Feb-23	Mar-23	Abr-23	May-23	Jun-23	Jul-23	Ago-23	Set-23	
Software malicioso del tipo keylogger	0	0	1	2	1	1	2	1	1	9
Descargar un Ransomware	1	1	2	3	4	3	4	4	3	25
Propagar un malware	0	0	1	0	3	5	3	3	4	19
Ingeniería social / Phishing	2	3	9	6	4	8	6	5	9	52
Ejecución del malware	0	1	2	1	1	2	2	1	1	11
Robo de información	0	0	0	0	0	0	0	0	0	0
Total de incidentes mensual	3	5	15	12	13	19	17	14	18	116

Fuente: Elaboración propia

Con dicha información, se procede a consolidar la misma para la elaboración del Diagrama de Pareto correspondiente:

Tabla 3.
Tipos de eventos de seguridad

Evento de seguridad	Cantidad de incidentes de seguridad	Porcentaje de incidentes de seguridad	Porcentaje de incidentes de seguridad acumulado
Ingeniería social / Phishing	68	39	39
Descargar un Ransomware	44	25	64
Ejecución del malware	30	17	81
Propagar un malware	21	12	93
Software malicioso del tipo keylogger	12	7	100
Robo de información	0	0	100
TOTAL	175		

Fuente: Elaboración propia

Análisis de riesgo del activo – información digital

Utilizando la metodología de Magerit, se realizó el análisis y valoración del riesgo asociado al activo “Información Digital”:

Tabla 4.
Análisis de riesgo del activo – información digital

Identificación del Riesgo						Análisis del Riesgo			Evaluación
Nº	Activo	Etapas	Evento Adverso	Causas	Consecuencias	Evento Adverso	Probabilidad	Impacto	
1	Información Digital	Inicio de sesión del usuario	R1. Ataque externo	Ciberdelincuentes y grupos hacktivistas	El cifrado de todas las bases de datos del MINDEF.	R1	4	5	20
			R2. Ataque interno	Sabotaje del tipo lógico	Indisponibilidad de servicios.	R2	1	5	5
		Uso de los recursos informáticos (información digital)	R3. Error humano	Falta de conocimiento	Modificación o eliminación de información crítica.	R3	4	5	20
			R4. Acción física intencional	Sabotaje del tipo físico	Indisponibilidad física de servicios.	R4	1	5	5
		Gestión y almacenamiento de la información digital (Centro de Datos)	R5. Desastres naturales	Terremotos, inundaciones, etc.	Indisponibilidad de servicios.	R5	1	5	5
			R6. Sustracción de información	Infección por malware	Hurto, pérdida, integridad, etc de la información digital.	R6	5	5	25

Fuente: Elaboración propia

A continuación, se muestran las tablas de valoración empleadas en el análisis correspondiente:

Tabla 5.
Tablas de valoración del riesgo del activo – información digital

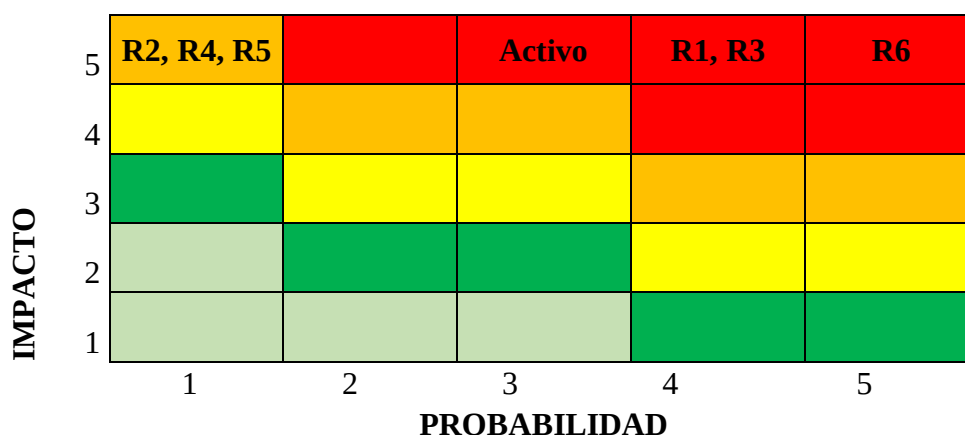
Probabilidad		
5	Prácticamente seguro	Una vez por semana
4	Probable	Una vez por mes
3	Posible	Una vez por semestre
2	Poco probable	Una vez por año
1	Muy raro	Cada cinco años
Riesgo		
5	Crítico	
4	Importante	
3	Apreciable	
2	Bajo	
1	Depreciable	

Impacto		
5	Muy Alto	Las consecuencias serían irreparables
4	Alto	Indisponibilidad de los servicios al 100% / Infección de la red al 60%
3	Medio	Indisponibilidad de los servicios al 40% / Infección de la red al 20%
2	Bajo	Indisponibilidad de los servicios al 10% / Infección de la red al 10%
1	Muy Bajo	Indisponibilidad de los servicios al 1% / Infección de la red al 1%

Fuente: Elaboración propia

Finalmente, se muestra el mapa de calor obtenido a partir de los resultados del análisis del riesgo del activo involucrado:

Tabla 6.
Mapa de calor del riesgo del activo – información digital



Fuente: Elaboración propia

Como se puede apreciar, el activo tiene un nivel de riesgo “Crítico”. El Ministerio de Defensa utiliza las VPN del tipo client-to-site como medio de comunicación entre sus trabajadores y los servicios tecnológicos que brinda, para la ejecución de sus labores correspondientes. En ese sentido, se procede a realizar el análisis del riesgo del mencionado medio de comunicación, aplicando la metodología Magerit:

Análisis de riesgo del proceso – Red privada virtual (VPN) Client To Site

Utilizando también la metodología de Magerit, se realizó el análisis y valoración del riesgo asociado al proceso “Red Privada Virtual (VPN) client-to-site”:

Tabla 7.

Análisis de riesgo del proceso – Red privada virtual (VPN) Client To Site

Identificación del Riesgo						Análisis del Riesgo			Evaluación
Nº	Proceso, Actividad o Tarea	Etapas	Evento Adverso	Causas	Consecuencias	Evento Adverso	Probabilidad	Impacto	
1	Red Privada Virtual (VPN) client-to-site	Al iniciar sesión del aplicativo (VPN) en la PC del usuario (en casa)	R1. Software malicioso del tipo keylogger	El usuario utiliza una PC de su propiedad	El cifrado de todas las bases de datos del MINDEF	R1	4	4	16
			R2. Descargar un Ransomware	La PC es utilizada por más de un miembro de la familia	Infección de la infraestructura tecnológica por software malicioso	R2	4	5	20
		Uso de los servicios de la infraestructura tecnológica (aplicaciones del MINDEF)	R3. Propagar un malware			R3	4	3	12
			R4. Ingeniería social/Phishing	La navegación del usuario a través del internet doméstico	Equipo infectado por software malicioso APT (por ejemplo, Keylogger)	R4	4	4	16
		Navegación por internet del usuario(en casa)	R5. Ejecución del malware			R5	3	4	12
			R6. Sustracción de información	Archivos infectados (word, excel, pdf, etc.)	Hurto, pérdida, integridad, etc. de la información digital	R6	5	4	20

Fuente: Elaboración propia

A continuación, se muestran las tablas de valoración empleadas en el análisis correspondiente:

Tabla 8.
Tablas de valoración del riesgo del proceso – Red privada virtual (VPN) Client To Site

Probabilidad		
5	Prácticamente seguro	Una vez por semana
4	Probable	Una vez por mes
3	Posible	Una vez por semestre
2	Poco probable	Una vez por año
1	Muy raro	Cada cinco años

Impacto		
5	Muy Alto	Las consecuencias serían irreparables
4	Alto	Indisponibilidad de los servicios al 100% / Infección de la red al 60%
3	Medio	Indisponibilidad de los servicios al 40% / Infección de la red al 20%
2	Bajo	Indisponibilidad de los servicios al 10% / Infección de la red al 10%
1	Muy Bajo	Indisponibilidad de los servicios al 1% / Infección de la red al 1%

Riesgo	
5	Crítico
4	Importante
3	Apreciable
2	Bajo
1	Depreciable

Fuente: Elaboración propia

Finalmente, se muestra el mapa de calor obtenido a partir de los resultados del análisis del riesgo del proceso en cuestión:

Tabla 9.
Mapa de calor del riesgo del proceso – Red privada virtual (VPN) Client To Site

IMPACTO	5				R2	
	4			R5	R1, R4 (Proceso)	R6
	3				R3	
	2					
	1					
		1	2	3	4	5
		PROBABILIDAD				

Fuente: Elaboración propia

Como se puede apreciar, este proceso tiene un nivel de riesgo “Crítico”. En ese sentido, se tiene la necesidad de realizar un tratamiento al proceso con el objetivo de minimizar el nivel de riesgo asociado. Según el Diagrama de Pareto realizado inicialmente, se deberían aplicar los controles necesarios sobre las 3 primeras categorías (Software malicioso del tipo keylogger, descarga de un Ransomware y propagación de un malware) y así poder reducir el riesgo a un 19%.

Para poder brindar atención a las 3 categorías en mención, se tendrían que aplicar los siguientes controles:

Tabla 10.
Mapa de calor de categorías software malicioso

CONTROL	CANTIDAD	COSTO	TIEMPO
Equipos de cómputo exclusivos para usuarios (Notebooks)	400 usuarios	S/. 2,000,000.00	2 años
Cifrador de Discos Duros		S/. 350,000.00	
Sistema de Protección para Dispositivos Finales (Endpoints)		S/. 40,000.00	

Fuente: Elaboración propia

Como se puede apreciar, se obtendría un costo de S/. 2,390,000.00 por 2 años para poder atender las categorías en mención y de tal forma poder cubrir el riesgo en un 81%. Sin embargo, para poder llegar al 100% deseado, tendríamos que considerar lo siguiente:

Tabla 11.
Mapa de calor de categorías software malicioso

CONTROL	CANTIDAD	COSTO	TIEMPO
VPN client-to-site	400 usuarios	S/. 200,000.00	2 años
Equipos de cómputo exclusivos para usuarios (Notebooks)		S/. 2,000,000.00	
Cifrador de Discos Duros		S/. 350,000.00	
Sistema de Protección para Dispositivos Finales (Endpoints)		S/. 40,000.00	
Sistema de Aprendizaje Automático		S/. 600,000.00	

Fuente: Elaboración propia

El costo total sería de S/. 3,190,000.00 por 2 años.

Plataforma segura de aplicaciones y escritorios de virtualización

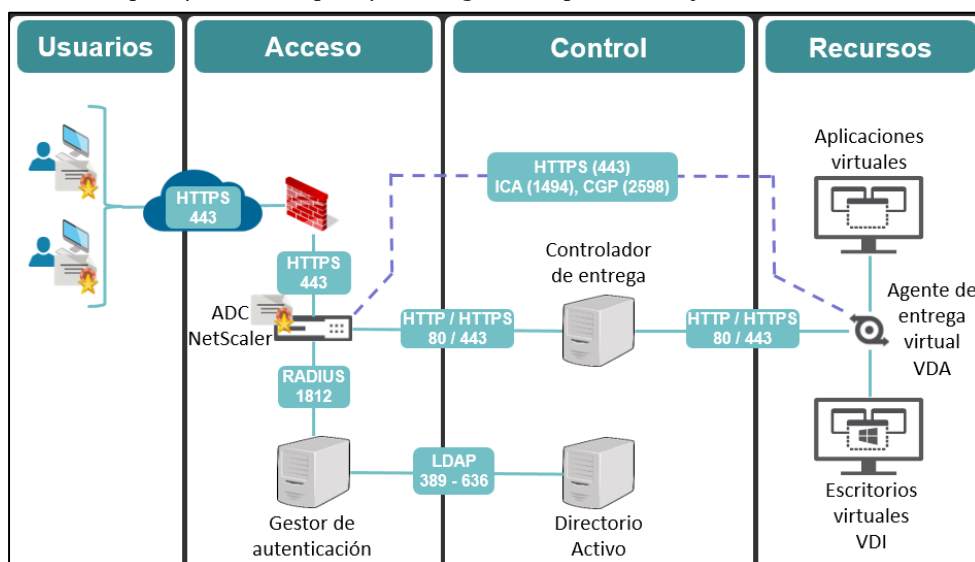
La plataforma segura de aplicaciones y escritorios virtuales se realizó sobre la base de dos tecnologías que son Citrix y RSA, en ese sentido el diseño está basado en soluciones como Xenapp, Xendesktop y RSA SecurID, realizando una sinergia entre ellas, cabe resaltar que la mencionada plataforma se puede acceder desde cualquier ubicación geográfica y desde cualquier dispositivo portable (notebook, Tablet, móvil, etc.) en la presente implementación se contempló 4 capas que paso a describir:

1. **Recursos.** - Son todas las aplicaciones y servicios tecnológicos que son albergados en la infraestructura tecnológica del MINDEF, por ejemplo: Intranet, correo, servidor de archivos, navegación a través de internet, office, Adobe, Winrar, etc.
2. **Control.** - Se realiza la gestión centralizada de los recursos a través de la generación de perfiles de usuario, de este modo permite la entrega de los recursos a demanda, utilizando los protocolos HTTPS, ICA y CGP.

3. **Acceso.** – Se presenta una interfaz web la cual es publicada a través de una ip pública, aquí se realiza la presentación de la plataforma, cabe resaltar que el usuario podrá acceder a ella desde cualquier ubicación geográfica y cualquier dispositivo portable (notebook, móvil, etc.), en esta capa se realiza la autenticación la cual es de doble factor a través de la solución SecurID de RSA.
4. **Usuario.** – La persona a la cual se prestará el servicio de la plataforma virtual de aplicaciones y escritorios virtuales, para lo cual se realizó un taller virtual para la capacitación en el manejo de la plataforma como usuario final.

Figura 2.

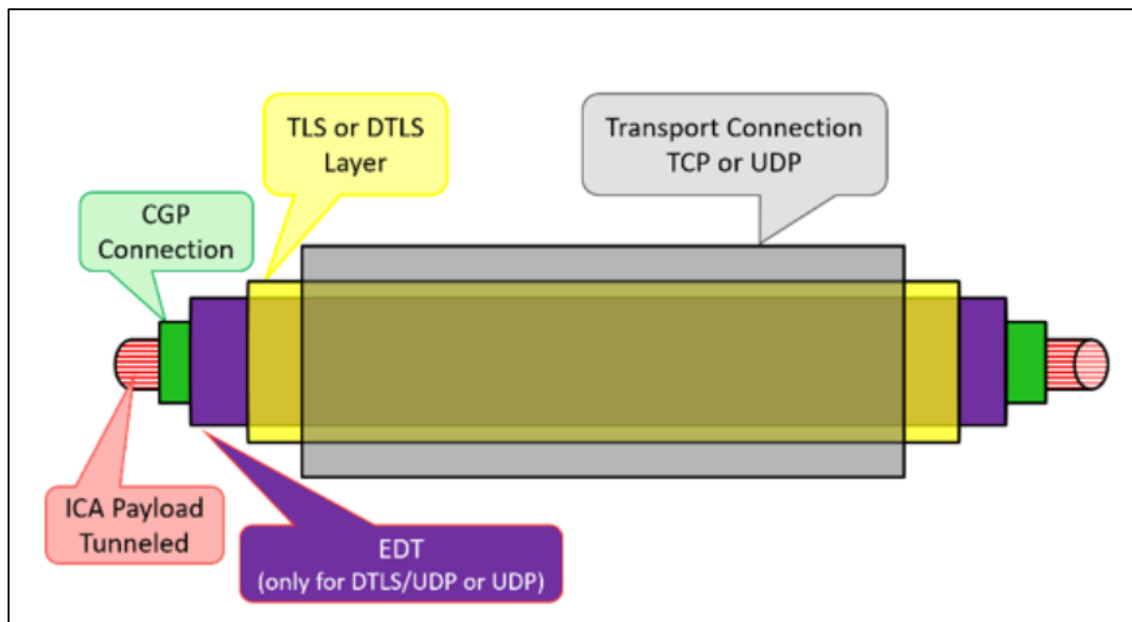
Arquitectura de la plataforma de la plataforma segura de aplicaciones y escritorios virtuales



Fuente: Elaboración propia

Topología de red

Figura 3.
Topología de red



Fuente: <https://www.citrix.com/blogs/2017/11/20/hdx-adaptive-transport-and-edt-icas-new-default-transport-protocol-part-ii/>

Análisis de la plataforma segura de aplicaciones y escritorios de virtualización

La plataforma segura de aplicaciones y escritorios virtuales se realizó sobre la base de dos tecnologías que son Citrix y RSA, en ese sentido el diseño está basado en soluciones como Xenapp, Xendesktop y RSA SecurID, realizando una sinergia entre ellas, la tecnología Citrix tiene una permanencia en el mercado tecnológico de 20 años aproximadamente y la tecnología RSA fue creada en los años 1996, en ese sentido ambas tecnologías han demostrado un buen soporte y permanencia en este mundo tecnológico, obteniendo una buena referencia empresarial.

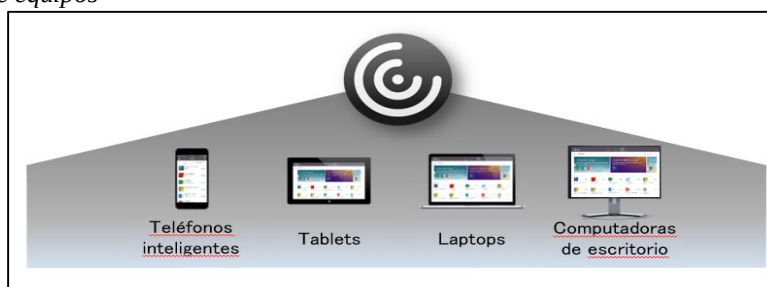
Figura 4.
Plataformas seguras de aplicaciones y escritorios de virtualización



Fuente: Elaboración propia

Esta plataforma segura permitirá al Ministerio de Defensa brindar a sus trabajadores sus servicios tecnológicos (aplicaciones y escritorios virtuales), sin preocuparse de que lo tenga instalada en el dispositivo portable de donde la ejecute, la mencionada plataforma permitirá hacer uso de los recursos tecnológicos del MINDEF sin preocuparse por la compatibilidad del equipo portable del usuario final ya que esta plataforma genera independencia del equipo de donde se conecta el usuario, minimizando los problemas de compatibilidad entre el equipo portable (notebook, Tablet, móvil, etc.) y la plataforma segura.

Figura 5.
Compatibilidad de equipos



Fuente: Elaboración propia

Una de las cosas resaltantes es que nos podemos conectar desde cualquier ubicación geográfica, cualquier tiempo (horario las 24x7x365 días del año) y utilizar cualquier dispositivo portátil para hacer uso de los recursos tecnológicos del MINDEF, son una de las grandes ventajas que ofrece nuestra plataforma segura de aplicaciones y escritorios remotos.

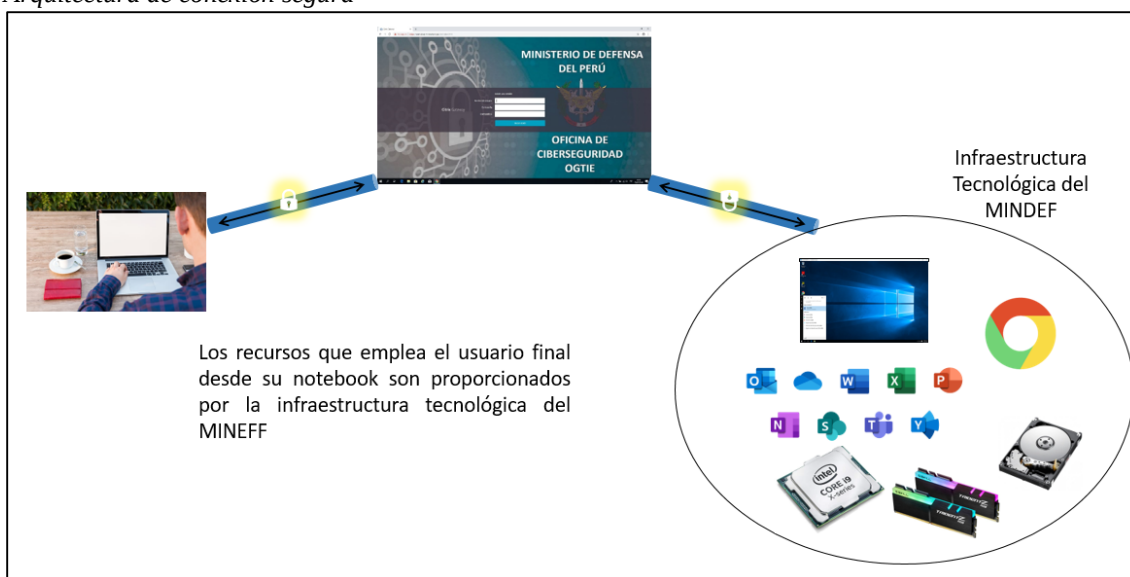
Figura 6.
Plataforma segura de aplicaciones y escritorios remotos



Fuente: Elaboración propia

Esta plataforma segura establece una conexión cifrada con el equipo portable del usuario final, los recursos son proporcionados por la infraestructura tecnológica del MINDEF, es necesario resaltar que al ejecutar esta acción, la plataforma no utiliza los recursos del equipo portable del usuario final, quiere decir, que no utiliza el disco duro, la memoria, procesador u otro recurso tecnológico, es por eso que esta plataforma segura no genera problemas de compatibilidad debido a que no necesita de los recursos del equipo con el que se establece la conexión, eso también incluye los periféricos como por ejemplo memorias extraíbles (USB) eso implica que así el usuario final introduzca un USB en su notebook, este dispositivo extraíble no genera ninguna relación, ni conexión con la plataforma segura del MIDENF, es por eso que los riesgos de sufrir alguna infección por software malicioso tiene un nivel bajo.

Figura 7.
Arquitectura de conexión segura



Fuente: Elaboración propia

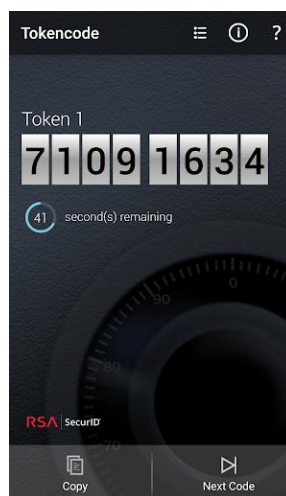
En el momento que el usuario final externo inicia sesión en la plataforma segura de aplicaciones y escritorios virtuales, el gestor de aplicaciones verifica el perfil del usuario el cual tiene configurado y hace entrega de los recursos tecnológicos para que pueda realizar las actividades que demande su función como trabajador del MINDEF, cada click del ratón y pulsaciones del teclado que realiza el usuario, en tiempo real la plataforma actualiza las pantallas del dispositivo, sincronizando las aplicaciones y escritorios virtuales albergados en la infraestructura tecnológica.

Esta plataforma usa una autenticación de doble factor, eso quiere decir que para que pueda darse este tipo se debe cumplir con dos requisitos, algo que conozco y algo que tengo, en ese sentido cuando decimos que es algo que conozco estamos hablando de la contraseña de usuario de directorio activo y cuando decimos algo que tenemos estamos hablando del token RSA.

El nombre RSA se refiere al acrónimo de Rivest, Shamir, and Adelman que son los creadores del algoritmo de autenticación por 2 factores. RSA SecurID, el cual es utilizado por el usuario para acceder a la plataforma segura de aplicaciones y escritorios virtuales.

La forma de autenticar de RSA SecurID consiste en un "token", ya sea físico (llavero) o software el cual es asignado a un usuario final externo, este token crea un código de autenticación con un intervalo de 30 segundos, usando un mecanismo de tiempo interno y la clave aleatoria codificada de fábrica de la tarjeta (conocida como "semilla"). La semilla es diferente para cada token y se carga en el servidor RSA SecurID correspondiente (RSA Authentication Manager, anteriormente ACE / Server) a medida que se van incrementando los tokens, cabe resaltar que el token físico está diseñado para ser resistente a la manipulación indebida para impedir la ingeniería inversa. La, fortaleza de este algoritmo es la factorización de números primos grandes lo cual dificulta realizar una intrusión o descifrado a esto le sumamos que va combinado con el temporizador interno del token.

Figura 8.
Token de acceso



Fuente: Elaboración propia

En el lado derecho hay un punto (que no se muestra en la imagen) que parpadea una vez por segundo, y a la izquierda hay una pila de seis barras horizontales apiladas verticalmente, cada una de las cuales desaparece una vez cada cinco segundos. Cada vez que pasan treinta segundos, el token se restablece y el token anterior se vuelve inválido.

Brindaremos un ejemplo publicado por Diego Córdoba el 8 noviembre, 2016, el escenario que presenta es, que ocurriría si el destinatario tiene su caja fuerte con dos llaves, una para cerrarla, y otra para abrirla, y nos envía su caja fuerte abierta junto con su llave para cerrarla.

Nosotros podríamos introducir el mensaje en dicha caja, cerrarla con la llave, y enviársela al destinatario. Nadie en la ruta podrá abrir la caja puesto que, si bien algunos habrán visto la llave para cerrarla, esta llave no sirve para abrirla, y solo el destinatario poseedor de la caja es quien tiene dicha clave.

Si lo igualamos a nuestro ejemplo del uso de la caja fuerte, sería equivalente a que el destinatario creara las llaves para poder cerrarla (pública) y para poder abrirla (privada).

1. Se eligen dos números primos, por ejemplo, $p=3$ y $q=11$
2. Calcula $n=p*q$, en este caso, $n=3*11=33$
3. Calcula $z=(p-1)*(q-1)$, en nuestro caso: $z=(3-1)*(11-1)=20$

A esta función se la denomina Función Phi o Fi de Euler.

4. Elige un número primo k , tal que k sea co-primo a z , por ejemplo, z no es divisible por k .

Tenemos varias opciones aquí, valores de k como pueden ser 7, 11, 13, 17 o 19 son válidos. 5 es primo, pero no es co-primo de k puesto que 20 (z) es divisible por 5.

Elegimos $k=7$ para simplificarnos los cálculos con un número pequeño.

5. La clave pública va a ser el conjunto de los números (n,k) , es decir, $(33,7)$.
6. Ahora se calcula la clave privada. Para ello, se elige un número j que verifique la siguiente ecuación:

$$k*j=1 \pmod{z}$$

En este caso:

$$7*j=1 \pmod{20}, \text{ es decir, un valor que verifique que}$$

$(7*j)/20$ sea una división con resto «1».

Para trabajar con números chicos en este ejemplo, podríamos decir que $21 / 20$ nos devuelve «algo» con resto 1, por lo que, para este caso particular, $(7*j) = 21$, de modo que $j=3$.

Esta es la clave privada, y no debe ser revelada nunca.

La Plataforma segura de aplicaciones y escritorios virtuales a través de la autenticación de doble factor del Sistema de Tokens, el cual es utilizado por los usuarios finales externos como control, de accesos a la mencionada plataforma, en ese sentido brinda un aseguramiento que permite minimizar el nivel de riesgo que puedan atentar contra la disponibilidad, integridad y confidencialidad de la información digital del MINDEF.

La solución planteada para el presente trabajo es la implementación de una Plataforma Virtual de Servicios, la cual está compuesta de un Sistema de Publicación de Aplicaciones y un Sistema de Autenticación de Doble Factor. Ambos sistemas trabajarán de la mano, por un lado, el primero permitirá brindar los recursos y servicios tecnológicos necesarios a los usuarios autorizados; mientras que el segundo, brindará un mecanismo de autenticación más robusto.

Es importante mencionar que la implementación de esta plataforma tiene el siguiente costo:

Tabla 12.
Costo de la plataforma

SISTEMA	CANTIDAD	COSTO	TIEMPO
Sistema de Publicación de Aplicaciones	400 usuarios	S/. 800,000.00	3 años
Sistema de Autenticación de Doble Factor			

Fuente: Elaboración propia

Continuando con el análisis correspondiente, a continuación, se muestran los registros de incidentes de seguridad reportados en el Ministerio de Defensa durante los meses de Julio, Agosto y Setiembre de 2022, correspondientes a la Plataforma Segura de aplicaciones y escritorios virtuales:

Tabla 13.
Total de incidentes de seguridad por evento

PLATAFORMA SEGURA DE APLICACIONES Y ESCRITORIOS VIRTUALES				
EVENTO DE SEGURIDAD	CANTIDAD DE INCIDENTES DE SEGURIDAD			TOTAL DE INCIDENTES DE SEGURIDAD POR EVENTO
	Jul-2	Ago-22	Set-22	
Software malicioso del tipo keylogger	0	0	0	0
Descargar un Ransomware	0	0	0	0
Propagar un malware	0	0	0	0
Ingeniería social / Phishing	1	0	1	2
Ejecución del malware	0	0	0	0
Robo de información	0	0	0	0
TOTAL DE INCIDENTES MENSUAL	1	0	1	2

Fuente: Elaboración propia

Con dicha información, se procede a consolidar la misma para la elaboración del Diagrama de Pareto correspondiente:

Tabla 14.

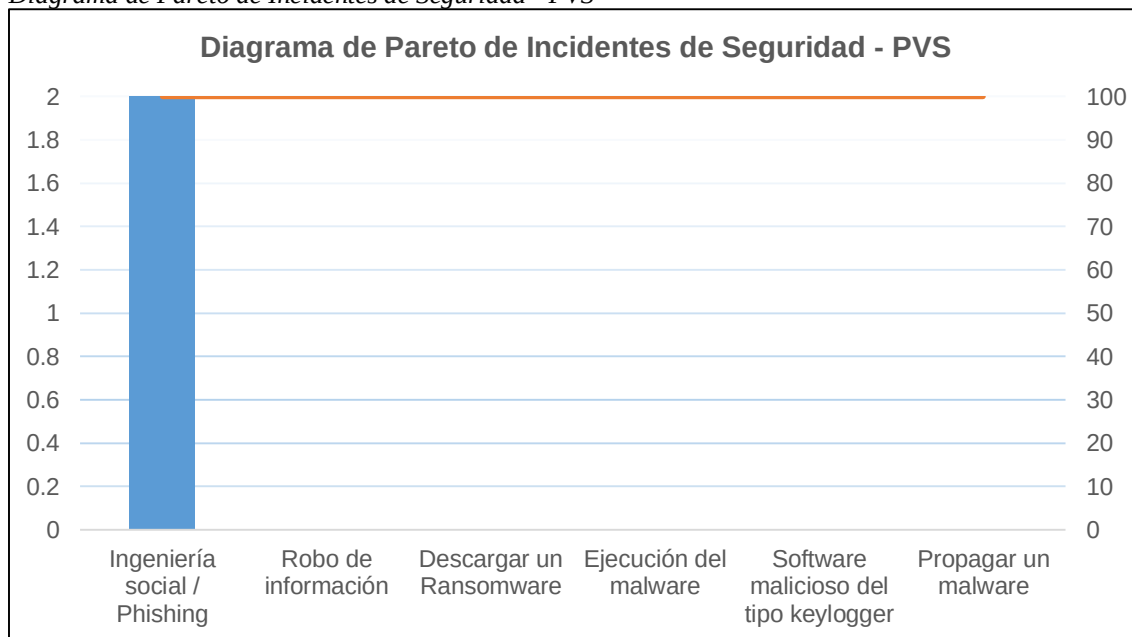
Porcentaje de incidentes de seguridad acumulado

PLATAFORMA SEGURA DE APLICACIONES Y ESCRITORIOS VIRTUALES			
EVENTO DE SEGURIDAD	Cantidad de incidentes de seguridad	Porcentaje de incidentes de seguridad	Porcentaje de incidentes de seguridad acumulado
Ingeniería social / Phishing	2	100	100
Robo de información	0	0	100
Descargar un Ransomware	0	0	100
Ejecución del malware	0	0	100
Software malicioso del tipo keylogger	0	0	100
Propagar un malware	0	0	100
TOTAL	2		

Fuente: Elaboración propia

Figura 9.

Diagrama de Pareto de Incidentes de Seguridad - PVS



Fuente: Elaboración propia

Del diagrama de Pareto realizado referente a los incidentes de seguridad con la Plataforma segura de aplicaciones y escritorios virtuales y su correspondiente análisis ejecutado, podemos decir que, si atendemos el primer evento, identificando sus causas y tomando las acciones pertinentes, se habrá solucionado el 100% de los incidentes de seguridad suscitados

en el Ministerio de Defensa. En este caso, por ejemplo, se podrían llevar a cabo charlas de concienciación y sensibilización en temas de seguridad de la información para los usuarios finales.

Análisis de riesgo del proceso – Plataforma segura de aplicaciones y escritorios virtuales

Utilizando también la metodología de Magerit, se realizó el análisis y valoración del riesgo asociado al proceso “Plataforma segura de aplicaciones y escritorios virtuales”:

Tabla 15.

Matriz de plataforma virtual de servicios (PVS)

Identificación del Riesgo						Análisis del Riesgo			Evaluación
Nº	Proceso, Actividad o Tarea	Etapas	Evento Adverso	Causas	Consecuencias	Evento Adverso	Probabilidad	Impacto	
1	Plataforma Virtual de Servicios (PVS)	Al iniciar sesión del aplicativo (PVS) en la PC del usuario (en casa)	R1. Software malicioso del tipo keylogger	El usuario utiliza una PC de su propiedad	El cifrado de todas las bases de datos del MINDEF	R1	1	4	4
			R2. Descargar un Ransomware	La PC es utilizada por más de un miembro de la familia	Infección de la infraestructura tecnológica por software malicioso	R2	1	5	5
		Uso de los servicios de la infraestructura tecnológica (aplicaciones del MINDEF)	R3. Propagar un malware			R3	1	3	3
			R4. Ingeniería social/Phishing	La navegación del usuario a través del internet doméstico	Equipo infectado por software malicioso APT (por ejemplo, Keylogger)	R4	1	4	4
		Navegación por internet del usuario (en casa)	R5. Ejecución del malware			R5	1	4	4
			R6. Sustracción de información	Archivos infectados (word, excel, pdf, etc.)	Hurto, pérdida, integridad, etc. de la información digital	R6	1	4	4

Fuente: Elaboración propia

A continuación, se muestran las tablas de valoración empleadas en el análisis correspondiente:

Tabla 16.

Tabla de valoración del riesgo asociado al proceso “Plataforma Virtual de Servicios”:

Probabilidad			Impacto		
5	Prácticamente seguro	Una vez por semana	5	Muy Alto	Las consecuencias serían irreparables
4	Probable	Una vez por mes	4	Alto	Indisponibilidad de los servicios al 100% / Infección de la red al 60%
3	Posible	Una vez por semestre	3	Medio	Indisponibilidad de los servicios al 40% / Infección de la red al 20%
2	Poco probable	Una vez por año	2	Bajo	Indisponibilidad de los servicios al 10% / Infección de la red al 10%
1	Muy raro	Cada cinco años	1	Muy Bajo	Indisponibilidad de los servicios al 1% / Infección de la red al 1%

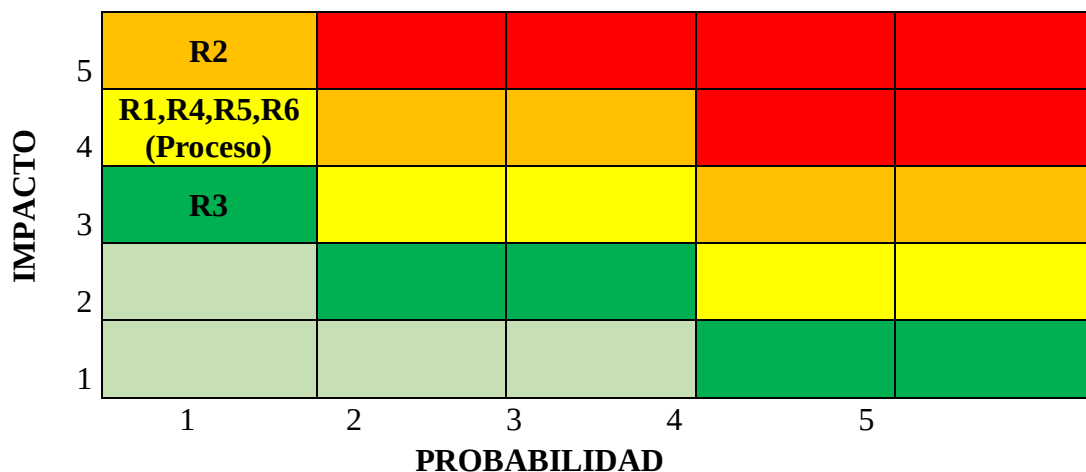
Riesgo	
5	Crítico
4	Importante
3	Apreciable
2	Bajo
1	Depreciable

Fuente: Elaboración propia

Finalmente, se muestra el mapa de calor obtenido a partir de los resultados del análisis del riesgo del proceso involucrado:

Tabla 17.

Mapa de calor del riesgo asociado al proceso “Plataforma Virtual de Servicios”:



Fuente: Elaboración propia

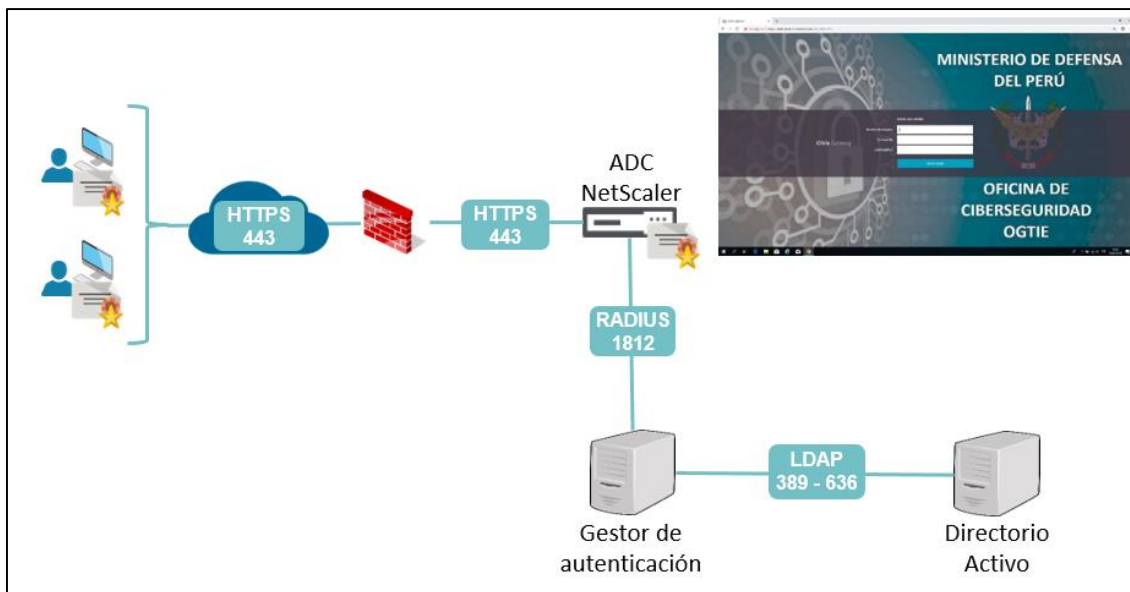
Como se puede apreciar, este proceso tiene un nivel de riesgo “Apreciable”. La implementación de esta plataforma está basada en los siguientes componentes:

ADC Netscaler. - La implementación de este sistema nos permitirá la publicación de la interfaz gráfica de la plataforma de aplicaciones y escritorios remotos por medio del protocolo HyperText Transfer Protocol Secure (https), el cual permite una conexión cifrada, con esta interfaz gráfica el usuario final externo podrá realizar la autenticación de doble factor utilizando un dispositivo de nombre token el cual genera una clave aleatoria, la cual es usada en conjunto con la clave asignada por el directorio activo, en ese sentido el usuario final externo ingresara sus dos claves para poder acceder, después de la validación correspondiente accederá a los recursos informáticos albergados en la infraestructura tecnológica del MINDEF. La implementación de este sistema cumple con las siguientes funciones:

- Publicación de servicios.
- Proporciona acceso a los usuarios finales externos hacia la infraestructura de Citrix.
- Representa el primer nivel de autenticación para los usuarios.
- Gestiona el tráfico que reciben los servicios.

Figura 10.

Arquitectura del sistema de publicación de la interfaz gráfica de la plataforma de aplicaciones y escritorios remotos

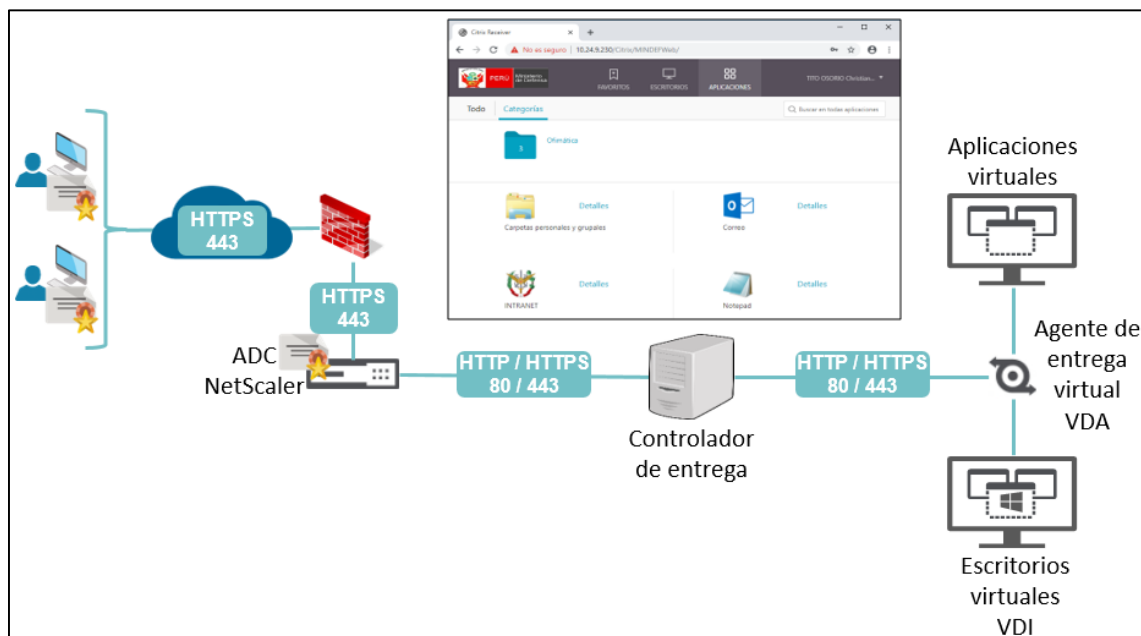


Fuente: Elaboración propia

Delivery Controller: - La implementación del Servidor de Controlador de entrega, nos permitirá crear los perfiles de los usuarios finales externos y de esta forma poder entregarle los servicios tecnológicos que necesitan para realizar sus actividades laborales, dentro de estos recursos se les podrá asignar aplicaciones, así como también escritorios virtuales (VDI), esta implementación nos permitirá la gestión centralizada de toda la plataforma, cabe resaltar que utiliza los protocolos HyperText Transfer Protocol Secure (https - 443) y HyperText Transfer Protocol (http - 80) para las comunicaciones con el ADC Netscaler y el Servidor de aplicaciones y los escritorios virtuales. La implementación de este sistema cumple con las siguientes funciones:

- Encargado de la administración total de la infraestructura Citrix.
- Gestiona los perfiles de cada usuario.
- Contiene el componente StoreFront el cual proporciona la lista de recursos disponibles para un usuario según su perfil configurado.
- Contiene los componentes base de datos y servidores de licencias.

Figura 11.
Arquitectura del servidor de controlador de entrega

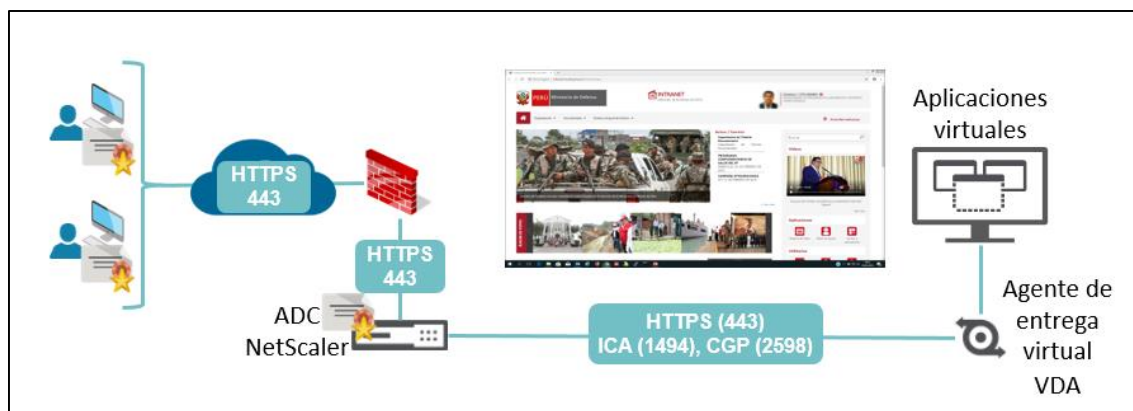


Fuente: Elaboración propia

Servidor de Aplicaciones. – La implementación de este sistema nos permitirá albergar todas las aplicaciones que estarán a disposición para los usuarios finales externos y que serán entregadas a demanda según su perfil, la comunicación se realizara a través de los protocolos Arquitectura de cómputo independiente (ICA) el cual es propietario CITRIX, HyperText Transfer Protocol Secure (https - 443), así como también usa las licencias de acceso al cliente (CAL) el cual permite compartir los recursos y puedan estar disponibles, como por ejemplo: el correo, la intranet, el office, el browser, etc. La implementación de este sistema cumple con las siguientes funciones:

- Contiene las aplicaciones que estarán disponibles para ser usadas por los usuarios.
- Emplea las licencias RDS-CAL para poder estar disponible.
- Contiene un agente que permitirá la disponibilidad de este recurso.

Figura 12.
Arquitectura de entrega d servicios al cliente

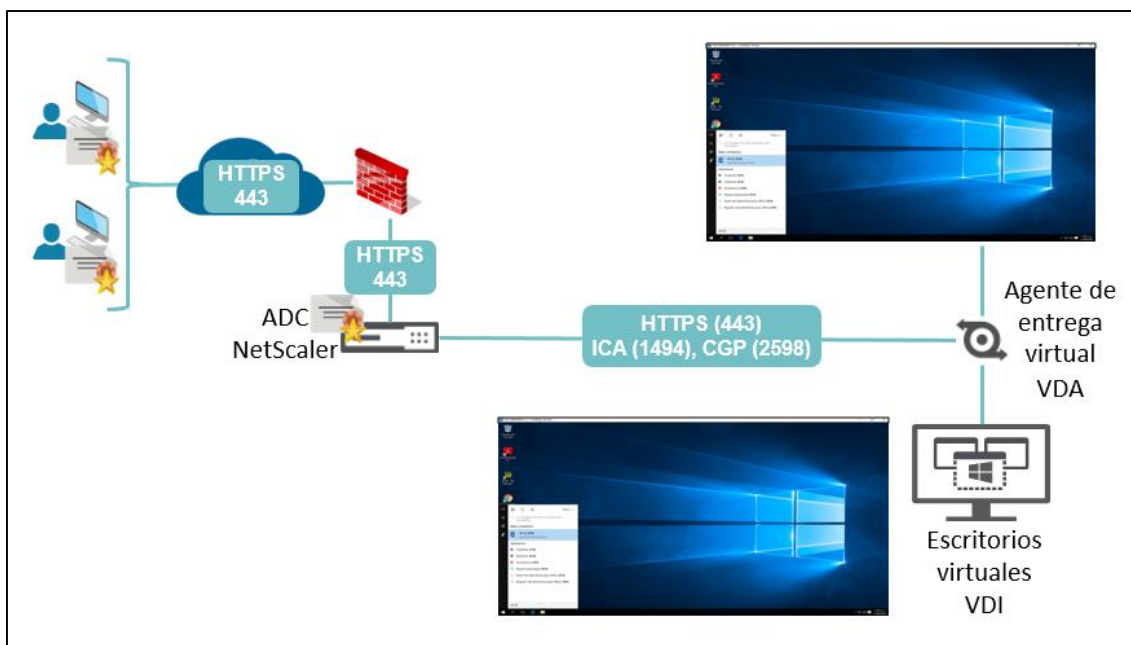


Fuente: Elaboración propia

Granja de escritorios. - La implementación de este sistema nos permitirá crear un catálogo de máquinas virtuales con sistema operativo de servidor, sistema operativo de escritorio y acceso remoto a PC (computadora física), cabe resaltar que se utiliza Citrix Gateway Protocol (CGP) para realizar la entrega del escritorio virtual, esta comunicación se da entre el usuario final externo y los VDA que se albergan en la plataforma segura. La implementación de este sistema cumple con las siguientes funciones:

- Conjunto de máquinas virtuales que contienen los escritorios remotos que estarán disponibles para los usuarios.
- Cada máquina virtual contiene un agente que permitirá la disponibilidad de este recurso.

Figura 12.
Arquitectura del funcionamiento de los escritorios virtuales



Fuente: Elaboración propia

Virtual Delivery Agent (VDA). – Este agente se instaló en cada máquina virtual o física de la granja de escritorios y de esta forma los recursos se encuentran disponibles para los usuarios finales externos, esta instalación permite que se registre en el Controller el cual establece una conexión entre la máquina virtual y el dispositivo portable del usuario.

Citrix StoreFront. – Permite la autenticación de los usuarios finales externos a los sitios donde se almacenan los recursos a su vez administra los escritorios virtuales donde acceden los usuarios.

Citrix Receiver. – Es instalado en los dispositivos portables de los usuarios finales externos, esto permite un acceso rápido y seguro desde cualquier dispositivo (notebook, Tablet, móvil, etc.).

Citrix Studio. - Es la consola de administración para realizar las configuraciones y la gestión de XenApp y XenDesktop, esto mejora la administración porque te permite

ejecutarlo en una sola consola y que no se realice de forma independiente, la forma de comunicación lo realiza por el puerto 80.

Authentication Manager. – Es una solución la cual permite realizar la gestión del control de accesos, como la creación de usuarios, asignación de token físicos o lógicos, sincronización, instalación de semillas, todas estas actividades lo realizan de una forma centralizada.

Autenticators (Tokens). – Son los dispositivos físicos o lógicos los cuales son asignados a los usuarios finales externos para que puedan acceder a la red, en este caso accederá a la plataforma segura de aplicaciones y escritorios virtuales.

Requerimientos Técnicos

Se describen los requerimientos con los que cuenta la Plataforma segura de aplicaciones y escritorios virtuales.

Tabla 18.

Requerimientos de la plataforma segura de aplicaciones y escritorios virtuales

REQUERIMIENTOS PLATAFORMA SEGURA DE APLICACIONES Y ESCRITORIOS VIRTUALES			
1	Citrix ADC - Netscaler	Citrix ADC MPX 5901 Standard Edition	01 Appliance físico
2	Citrix Delivery Controller (Controlador de Entrega)	DataCenter VM Standard 01 Windows Server 2012 R2 o 2016 con: - Core: 02 vCPU - Memoria: 08 GB RAM - Disco duro: 50 GB	01 Servidor físico (10 core, DD 2TB)
3	Citrix Applications Server (Servidor de Aplicaciones)	DataCenter VM Standard 01 Windows Server 2012/2016 Ingles con: - Core: 04 vCPU - Memoria: 16 GB RAM - Disco duro: 80 GB	
4		Licencias MS CAL	
5	RSA Authentication Manager (Gestor de autenticación)	SID Access Dell A130 Appliance	01 Appliance físico
6	RSA Authenticators (Tokens)	50 Hard-Token (Token físico) 350 Soft-Token (Token lógico)	400 Tokens
7	Escritorios Virtuales (VDI)	DataCenter VM Standard Windows 7 o Windows 10 con: - Core: 02 vCPU - Memoria: 3 GB RAM - Disco duro: 50 GB	50 VDI

Fuente: Elaboración propia

Análisis comparativo entre la VPN Client-To-Site y la plataforma segura de aplicaciones y escritorios virtuales

A continuación, se muestran los registros de incidentes de seguridad reportados en el Ministerio de Defensa durante los meses de Julio, Agosto y Setiembre de 2022, correspondientes a las dos soluciones de seguridad involucradas en el presente análisis:

Tabla 19.
Plataforma VPN Client-To-Site

VPN CLIENT-TO-SITE				
EVENTO DE SEGURIDAD	CANTIDAD DE INCIDENTES DE SEGURIDAD			TOTAL DE INCIDENTES DE SEGURIDAD POR EVENTO
	Jul-22	Ago-22	Set-22	
Software malicioso del tipo keylogger	2	1	1	4
Descargar un Ransomware	4	4	3	11
Propagar un malware	3	3	4	10
Ingeniería social / Phishing	6	5	9	20
Ejecución del malware	2	1	1	4
Robo de información	0	0	0	0
TOTAL DE INCIDENTES MENSUAL	17	14	18	49

Fuente: Elaboración propia

Tabla 20.
Plataforma segura de aplicaciones y escritorios virtuales

PLATAFORMA SEGURA DE APLICACIONES Y ESCRITORIOS VIRTUALES				
EVENTO DE SEGURIDAD	CANTIDAD DE INCIDENTES DE SEGURIDAD			TOTAL DE INCIDENTES DE SEGURIDAD POR EVENTO
	Jul-22	Ago-22	Set-22	
Software malicioso del tipo keylogger	0	0	0	0
Descargar un Ransomware	0	0	0	0
Propagar un malware	0	0	0	0
Ingeniería social / Phishing	1	0	1	2
Ejecución del malware	0	0	0	0
Robo de información	0	0	0	0
TOTAL DE INCIDENTES MENSUAL	1	0	1	2

Fuente: Elaboración propia

Con la información obtenida, se procedió a realizar un análisis comparativo entre las soluciones de seguridad informática involucradas en el presente trabajo, consolidando los datos para la elaboración de los Diagramas de Pareto correspondientes:

Tabla 21.

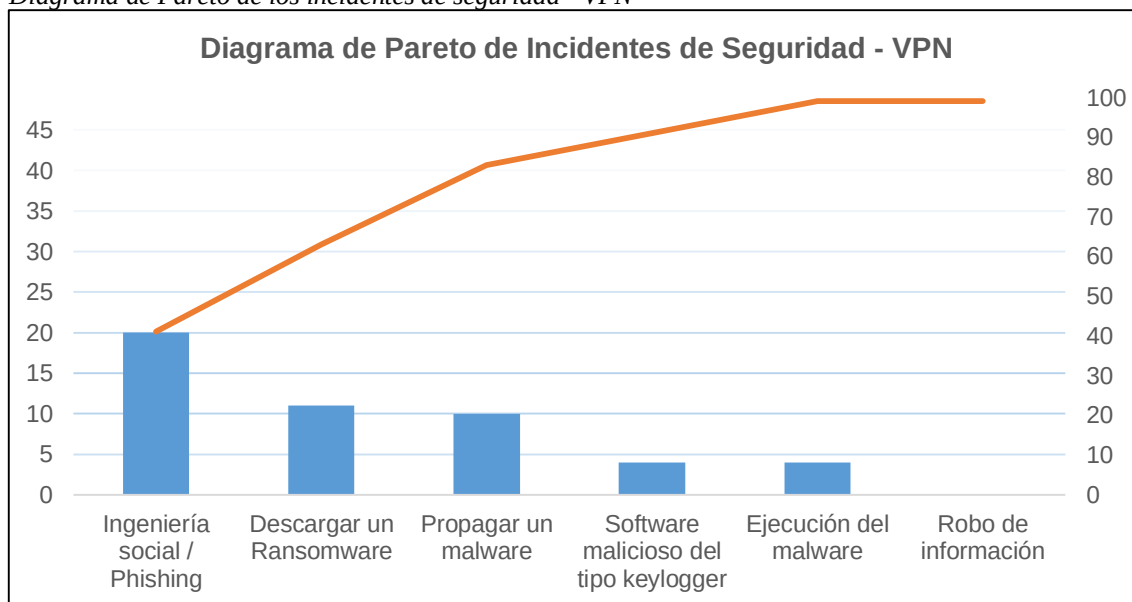
Análisis de los incidentes de seguridad - VPN

VPN CLIENT-TO-SITE			
EVENTO DE SEGURIDAD	Cantidad de incidentes de seguridad	Porcentaje de incidentes de seguridad	Porcentaje de incidentes de seguridad acumulado
Ingeniería social / Phishing	20	41	41
Descargar un Ransomware	11	22	63
Propagar un malware	10	20	83
Software malicioso del tipo keylogger	4	8	91
Ejecución del malware	4	8	99
Robo de información	0	0	99
TOTAL	49		

Fuente: Elaboración propia

Figura 13.

Diagrama de Pareto de los incidentes de seguridad - VPN



Fuente: Elaboración propia

Del diagrama de Pareto realizado referente a los incidentes de seguridad con los VPN CLIENT-TO-SITE y su correspondiente análisis ejecutado, podemos observar que

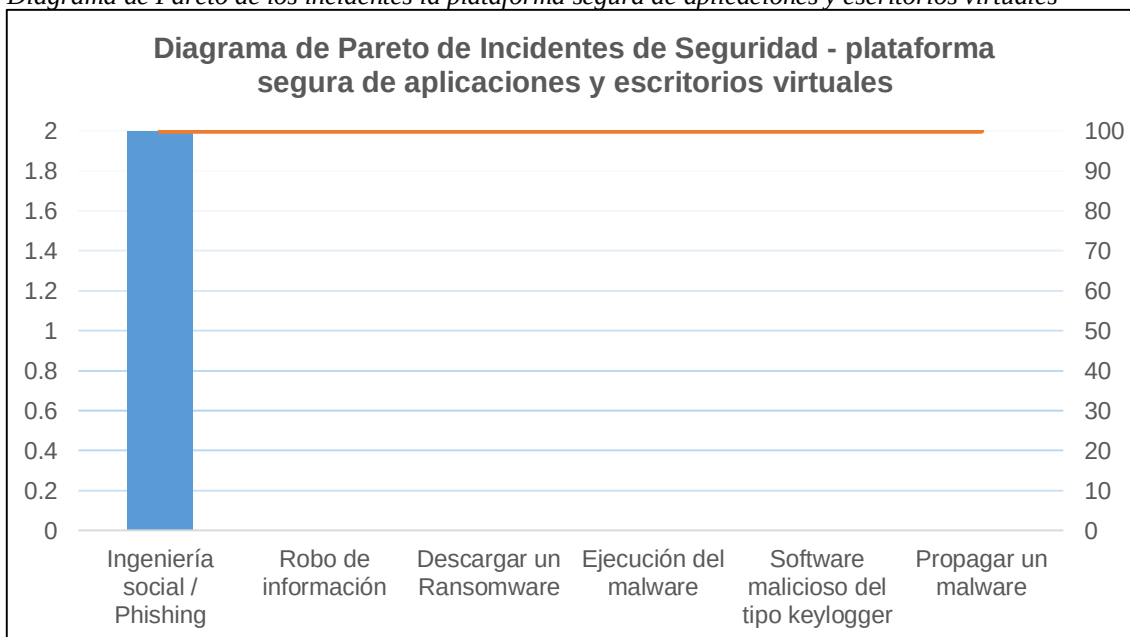
durante los tres meses involucrados en este comparativo se tiene el mismo comportamiento evidenciado en el análisis inicial de esta solución. En este caso, si atendemos los tres primeros eventos, identificando sus causas y tomando las acciones pertinentes, se habrá solucionado el 83% de los incidentes de seguridad suscitados en el Ministerio de Defensa.

Tabla 22.
Plataforma segura de aplicaciones y escritorios virtuales

PLATAFORMA SEGURA DE APLICACIONES Y ESCRITORIOS VIRTUALES			
EVENTO DE SEGURIDAD	Cantidad de incidentes de seguridad	Porcentaje de incidentes de seguridad	Porcentaje de incidentes de seguridad acumulado
Ingeniería social / Phishing	2	100	100
Robo de información	0	0	100
Descargar un Ransomware	0	0	100
Ejecución del malware	0	0	100
Software malicioso del tipo keylogger	0	0	100
Propagar un malware	0	0	100
TOTAL	2		

Fuente: Elaboración propia

Figura 13.
Diagrama de Pareto de los incidentes la plataforma segura de aplicaciones y escritorios virtuales



Fuente: Elaboración propia

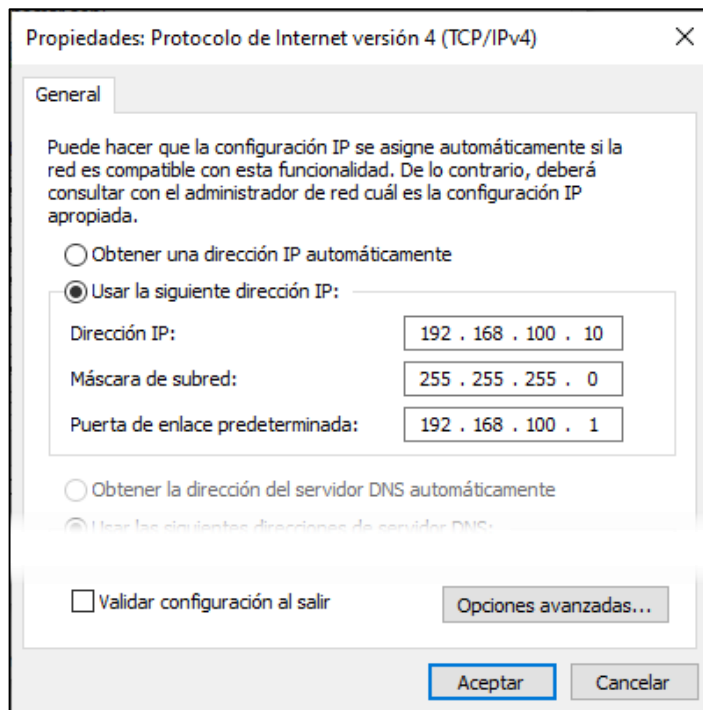
Comparando los resultados de los Diagramas de Pareto realizados referente a los incidentes de seguridad con los VPN CLIENT-TO-SITE y la Plataforma Segura de Aplicaciones y Escritorios Virtuales, podemos observar que con esta última plataforma de seguridad se logra minimizar el nivel de riesgos asociados. Por un lado, con los VPN CLIENT-TO-SITE se tendría que atender las 3 primeras categorías; mientras que, con la Plataforma Virtual de Servicios se tendría que atender sólo la primera categoría.

Finalmente, es importante mencionar que, mantener la solución de VPN CLIENT-TO-SITE y de esta forma tener que aplicar los controles necesarios para disminuir el nivel de riesgo, demandaría realizar un costo de S/. 3,190,000.00 por un periodo de 2 años. Mientras que, implementar la Plataforma Virtual de Servicios demandaría un costo de S/. 800,000.00 por un periodo de 3 años.

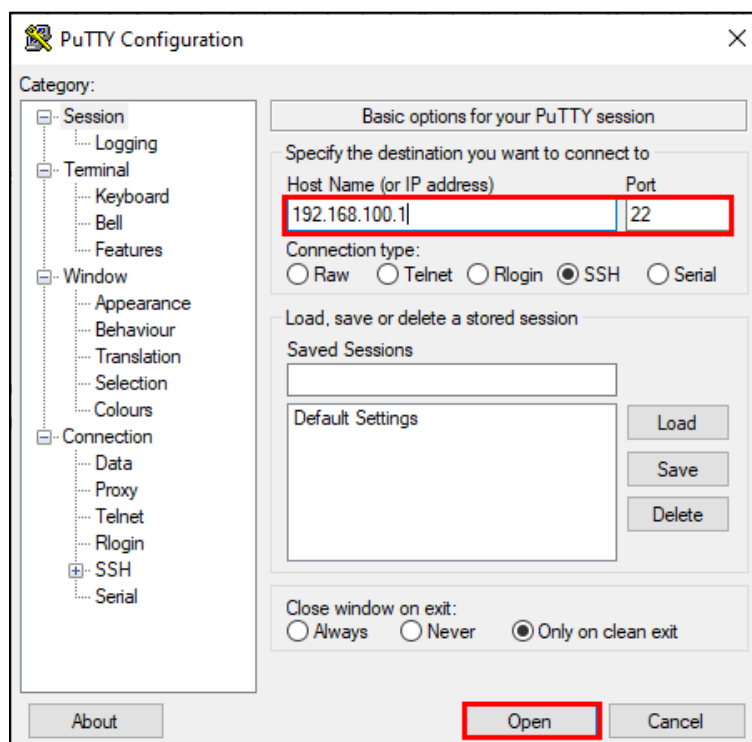
Procedimiento de instalación de CITRIX ADC (NETSCALER)

Paso 1: Conectar una laptop al puerto de administración del appliance.

Paso 2: Asignar una dirección IP dentro del segmento de red 192.168.100.0/24.



Paso 3: Ingresar por SSH al appliance, a través de la siguiente dirección IP por defecto que tiene el mismo.



Paso 4: Iniciar sesión con las credenciales por defecto que tiene el equipo.

```
192.168.100.1 - PuTTY
login as: nsroot
Pre-authentication banner message from server:
| #####
> ##
| #
> #
| #
| #      WARNING: Access to this system is for authorized users only
> #
| #      Disconnect IMMEDIATELY if you are not an authorized user!
> #
| #
> #
| #####
> ##
|
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Last login: Tue Jun  9 03:09:37 2020 from 192.168.100.10
Done
> █
```

Paso 5: Digitar los comandos “shell” y “nsconfig” para acceder a los parámetros de configuración del equipo.

```
192.168.100.1 - PuTTY
Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.

root@ns# nsconfig
NSCONFIG NS12.0.

REVIEW CONFIGURATION PARAMETERS MENU
-----
This menu allows you to view and/or modify the NetScaler's configuration.
Each configuration parameter displays its current value within brackets
if it has been set. To change a value, enter the number that is displayed
next to it.
-----
    1. NetScaler's IP address: [192.168.100.1]
    2. Netmask: [255.255.255.0]
    3. Advanced Network Configuration.
    4. Time zone.
    5. Network firewall mode: [0]
    6. Cancel all the changes and exit.
    7. Apply changes and exit.
Select a menu item from 1 to 7 [7]: █
```

Paso 6: Digitar la opción 1 para configurar la dirección IP y máscara de red que se asignará a la interface de gestión del equipo.

```

192.168.100.1 - PuTTY
Select a menu item from 1 to 7 [7]: 1

NetScaler's IP Address
-----
This specifies the NetScaler's IP address.

Enter the NetScaler's IP address [192.168.100.1]: 192.168.1.250

Netmask
-----
This specifies the netmask for the network in which the NetScaler
is being installed.

Enter the netmask [255.255.255.0]: 255.255.255.0
  
```

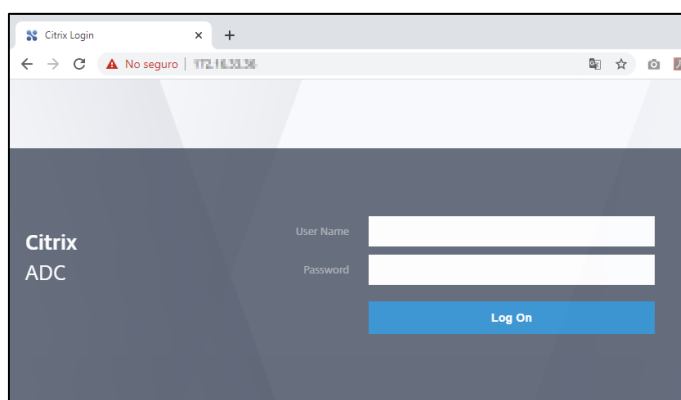
Paso 7: Digitar la opción 7 para aplicar los cambios y aceptar las solicitudes de guardado y reinicio del equipo.

```

192.168.100.1 - PuTTY
REVIEW CONFIGURATION PARAMETERS MENU
-----
This menu allows you to view and/or modify the NetScaler's configuration.
Each configuration parameter displays its current value within brackets
if it has been set. To change a value, enter the number that is displayed
next to it.
-----
1. NetScaler's IP address: [192.168.1.250]
2. Netmask: [255.255.255.0]
3. Advanced Network Configuration.
4. Time zone.
5. Network firewall mode: [0]
6. Cancel all the changes and exit.
7. Apply changes and exit.
Select a menu item from 1 to 7 [7]: 7
The configuration must be saved and the system rebooted for these settings to take effect.
Do you want to save the new configuration? [Yes]: yes
Do you want to reboot the system now? [No]: yes
  
```

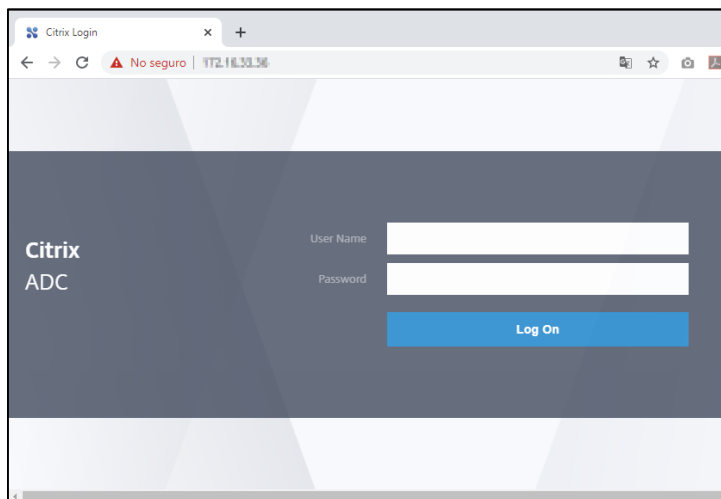
Paso 8: Desconectar la laptop de la interface de administración del equipo y conectar esta última a la red de la institución.

Paso 9: Finalmente, validar el acceso a la plataforma Citrix ADC (Netscaler) a través del navegador web.

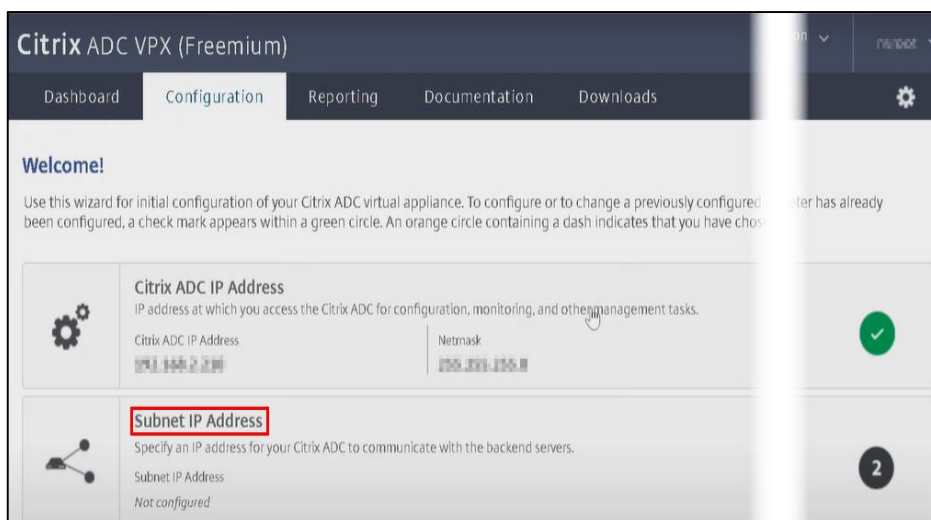


Procedimiento configuración de CITRIX ADC (NETSCALER)

Paso 1: Iniciar sesión en la plataforma Citrix ADC (Netscaler) para proceder con la configuración inicial.



Paso 2: En la pantalla de bienvenida ya se encuentra configurada la dirección IP de gestión de la plataforma, por ende, proceder con la configuración de la dirección IP subnet.



Subnet IP Address

A subnet IP address is used by the Citrix ADC to communicate with the backend servers. Citrix ADC uses this subnet IP address as a source IP address to proxy the client connections as well as to send monitor probes to check the health of the backend servers.

The infographic shows the usage of SNIP in client server communication.

Depending on your network topology, you might have to configure additional subnet IP addresses.

For more information about subnet IP addresses, [click here](#).

Subnet IP Address*

Netmask*

255 . 255 . 255 . 0

Done Do It Later

Paso 3: Ingresar el hostname del equipo, la dirección IP del servidor DNS, la zona horaria y la dirección IP del servidor NTP (en caso de tener disponible uno).

Welcome!

Use this wizard for initial configuration of your Citrix ADC virtual appliance. To configure or to change a previously configured field that has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip the step.

	Citrix ADC IP Address IP address at which you access the Citrix ADC for configuration, monitoring, and other management tasks.	Citrix ADC IP Address 192.168.1.10	Netmask 255.255.255.0	✓	
	Subnet IP Address Specify an IP address for your Citrix ADC to communicate with the backend servers.	Subnet IP Address 192.168.1.10		✓	
	Host Name, DNS IP Address, Time Zone and NTP Server Specify a host name to identify your Citrix ADC, an IP address for a DNS server to resolve domain names, the time zone and qualified domain name of the NTP server which is required for Citrix ADC clock synchronization.	Host Name Not configured	DNS IP Address Not configured	Time Zone CoordinatedUniversalTime	3

Host Name, DNS IP Address, Time Zone and NTP Server

Specify a host name to identify your Citrix ADC. When you generate the Universal license for your Citrix ADC, you need to specify a host name. Specify the time zone and name of the NTP server which is required for Citrix ADC clock synchronization.

Host Name

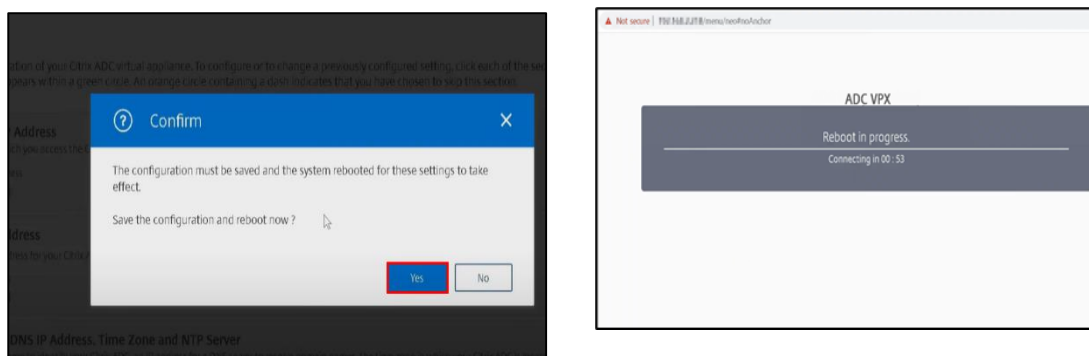
DNS IP Address

Time Zone*

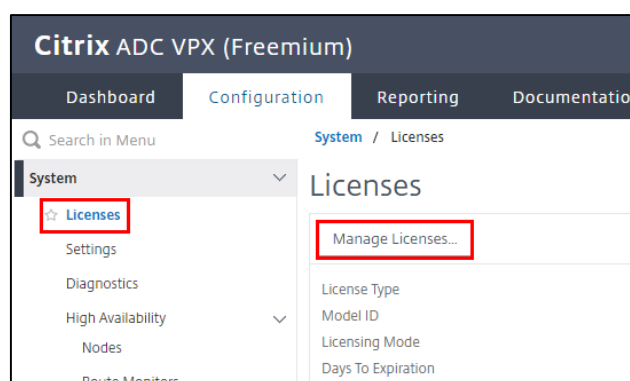
NTP Server

Done Do It Later

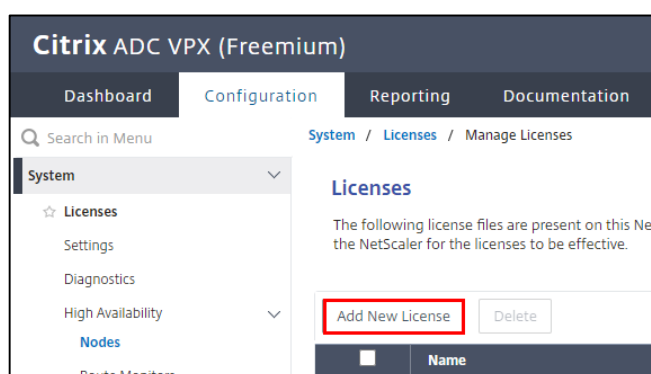
Paso 4: Proceder con el guardado y reinicio del equipo (solicitado automáticamente por el sistema).



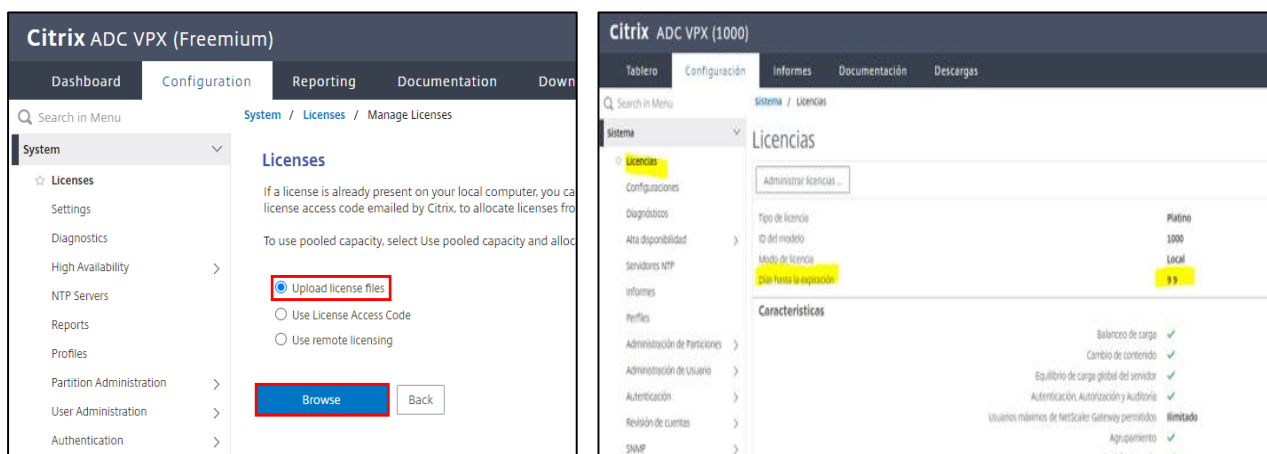
Paso 5: Luego de volver a ingresar a la plataforma, instalar la licencia de la solución. Para ello, ingresar a la opción “**Manage Licenses...**”.



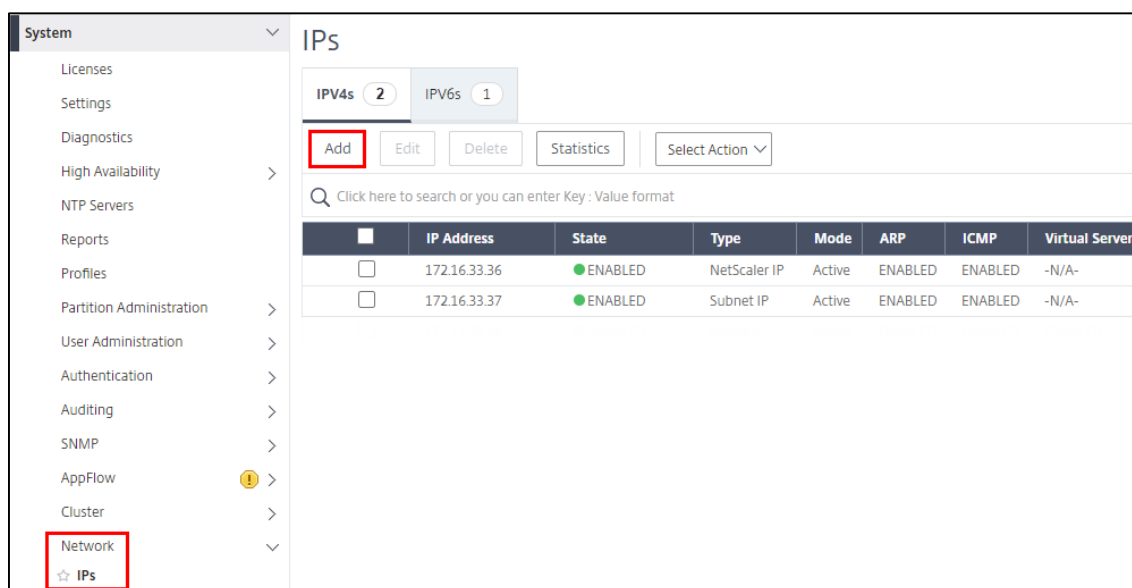
Paso 6: Seleccionar la opción “**Add New License**” para poder agregar la licencia de la solución correspondiente.



Paso 7: Marcar la opción “**Upload license files**” y seleccionar el botón “**Browse**” para ubicar el archivo de la licencia que será cargada a la plataforma.



Paso 8: Ingresar a la opción “**System > Network > IPs**” y seleccionar la opción “**Add**” para agregar la dirección IP virtual con la que se realizará la publicación del servicio.



Paso 9: Configurar la dirección IP virtual según el siguiente detalle.

Create IP Address

IP Address*
172 . 16 . 30 . 30

Netmask*
255 . 255 . 255 . 255

IP Type*
Virtual IP

Virtual Router ID

ICMP Response*
NONE

ARP Response*
NONE

Traffic Domain

☒ State

Options

☒ ARP ☒ ICMP
☒ Virtual Server ☐ Enable dynamic routing
☐ Decrement TTL ☐ Network Route

Host Route

☐ Enable

Tag
0

Gateway IP

Metric

OSPF Link-State Advertisement (LSA) Type

☒ TYPE5 ☐ TYPE1

Area

Virtual Server Route Health Injection (RHI)

Virtual Server RHI Level
☐ NONE ☒ ONE_VSERVER ☐ ALL_VSERVERS ☐ VSVR_CNTRL

Virtual Server RHI Mode
☒ DYNAMIC_ROUTING ☐ RISE

Application Access Controls

☐ Enable Management Access control to support the below listed applications.

Create **Close**

Paso 10: Ingresar a la opción “**System > Authentication > Basic Policies > LDAP**” para agregar la política de comunicación con el Directorio Activo para la validación de los usuarios de red.

En la pestaña “**Servers**”, seleccionar la opción “**Add**” para agregar la dirección IP del servidor AD:

System

LDAP

Policies 0 **Servers 0**

Add Edit Delete

Click here to search or you can enter Key - Value format

Name	Server Name	IP Address	Port	Server Type	Time-out (seconds)
No items					

LDAP

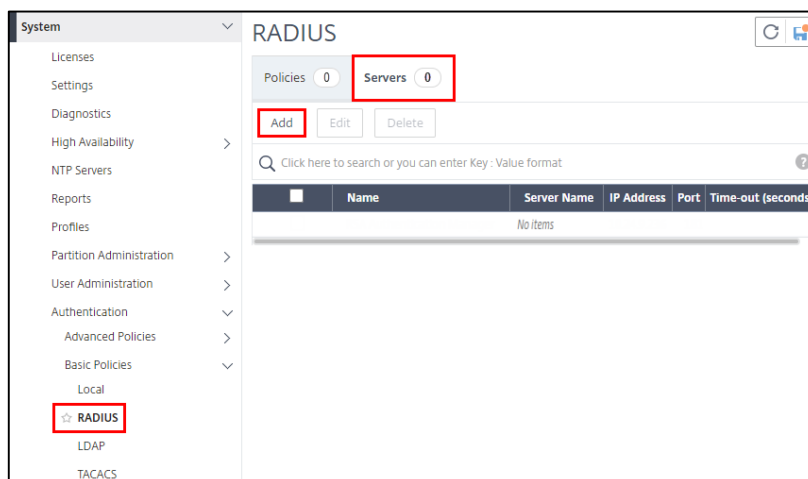
Configurar la dirección IP del servidor AD según el siguiente detalle:

En la pestaña “**Policies**”, seleccionar la opción “**Add**” para agregar la política de comunicación con el servidor AD:

Configurar la política según el siguiente detalle:

Paso 11: Ingresar a la opción “**System > Authentication > Basic Policies > RADIUS**” para agregar la política de comunicación con el RSA Authentication Manager para la autenticación de doble factor.

En la pestaña “**Servers**”, seleccionar la opción “**Add**” para agregar la dirección IP del servidor RSA Authentication Manager:



Configurar la dirección IP del servidor RSA Authentication Manager según el siguiente detalle:

Create Authentication RADIUS Server

Name*
RSA Authentication Manager

☐ Server Name ☒ Server IP

IP Address*
11.22.33.44

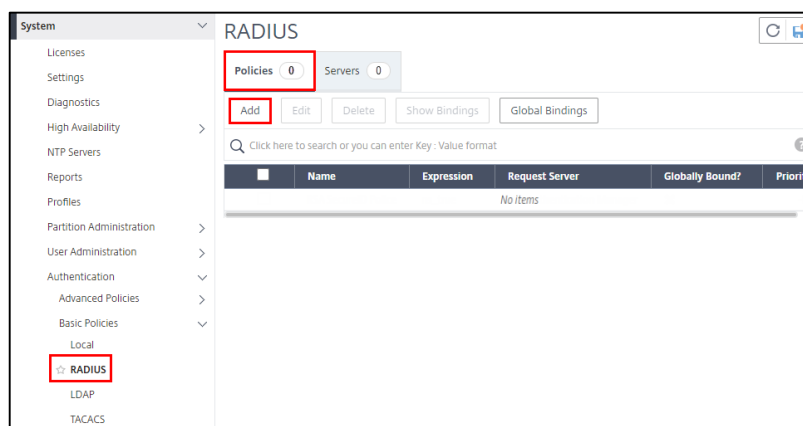
Port
1812

Secret Key*
.....

Confirm Secret Key*
.....

Time-out (seconds)
30

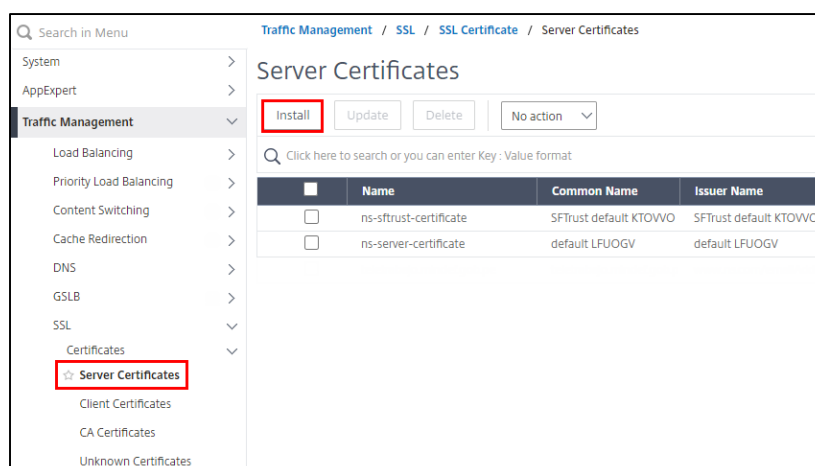
En la pestaña **“Policies”**, seleccionar la opción **“Add”** para agregar la política de comunicación con el servidor RSA Authentication Manager:



Configurar la política según el siguiente detalle:

The screenshot shows the 'Create Authentication RADIUS Policy' form. The 'Name' field is 'RSA SecurID Police'. The 'Server' dropdown is set to 'RSA Authentication Manager'. The 'Expression' field is 'ns_true'. The 'Create' button is highlighted.

Paso 12: Ingresar a la opción **“Traffic Management > SSL > Certificates > Server Certificates”** y seleccionar la opción **“Instalar”** para importar el certificado SSL que será utilizado para el portal web.



Crear un nombre de registro y seleccionar los archivos correspondientes al certificado a importar:

Install Server Certificate

Certificate-Key Pair Name*
iuletrabaja.mindel.gob.pe

Certificate File Name*
Choose File P12Cert.cer

Key File Name*
Choose File P12Cert.cer

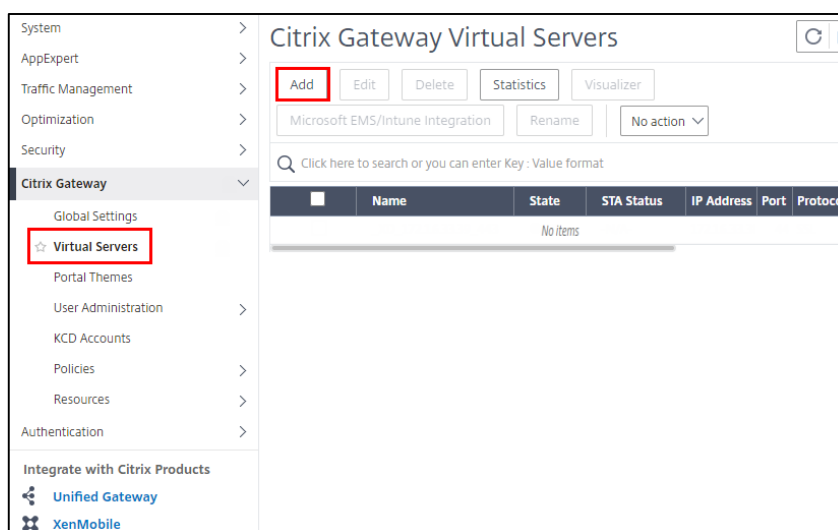
☒ Notify When Expires

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period
30

Install Close

Paso 13: Ingresar a la opción “Citrix Gateway > Virtual Servers” y seleccionar la opción “Add” para agregar la configuración del servidor virtual VPN.



Configurar el servidor virtual VPN según el siguiente detalle:

VPN Virtual Server

Basic Settings

Name*
_XD_172.16.17.19_443

IP Address Type*
IP Address

IP Address*
172.16.17.19

Port*
443

Advanced Settings

☐ ICA Only
☒ Enable Authentication
☐ Double Hop
☒ Down State Flush
 IP Range IP Set settings
☐ Logout On Smart Card Removal
☐ Login Once

☒ DTLS
☒ AppFlow Logging
☐ ICA Proxy Session Migration
☒ State
☐ Enable Device Certificate
 CA for Device Certificate

Configured (0) Remove All
 No items
 Add

Comments

OK Cancel

Paso 14: Asociar el certificado de servidor, las políticas de autenticación LDAP y RADIUS y las políticas de sesión, al servidor virtual VPN creado. En primer lugar, ingresar a la configuración seleccionando en el nombre creado.

Citrix Gateway / Citrix Gateway Virtual Servers

Citrix Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Microsoft EMS/Intune Integration

Click here to search or you can enter Key : Value format

	Name	State	STA Status	IP Address	Port	Protocol
☐	_XD_172.16.17.19_443	UP	-N/A-	172.16.17.19	443	SSL

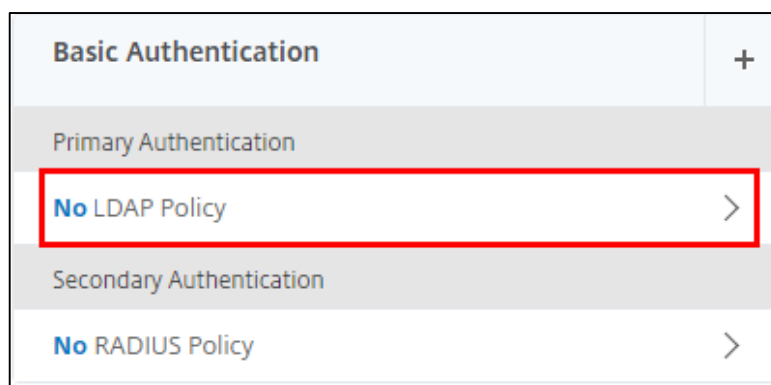
En la sección “**Certificate**”, seleccionar la opción “**Server Certificate**”:

Certificate

No Server Certificate >

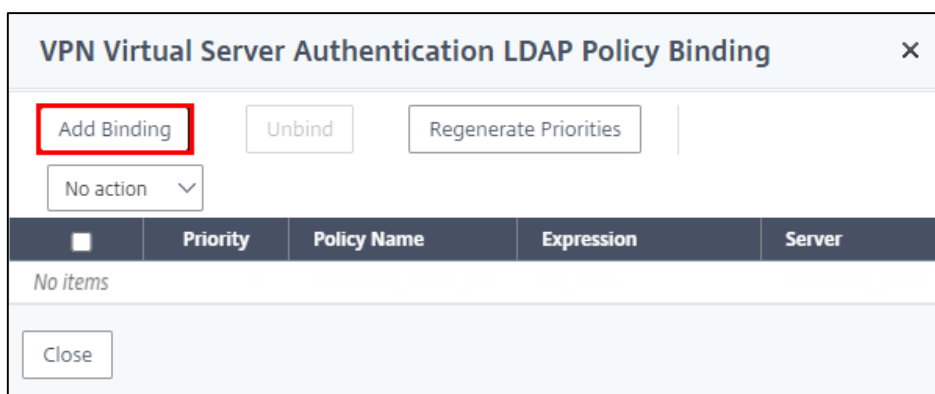
No CA Certificate >

En la sección **“Basic Authentication”**, seleccionar la opción **“LDAP Policy”**:



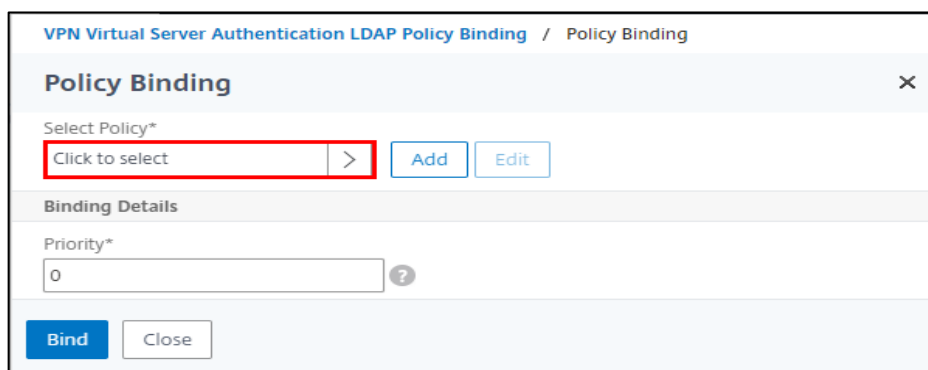
The screenshot shows the 'Basic Authentication' configuration panel. It has a header 'Basic Authentication' with a '+' icon. Below it, there are two sections: 'Primary Authentication' and 'Secondary Authentication'. Under 'Primary Authentication', the 'No LDAP Policy' option is highlighted with a red box. Under 'Secondary Authentication', the 'No RADIUS Policy' option is visible.

Seleccionar la opción **“Add Binding”** para añadir la política de comunicación con el servidor AD:



The screenshot shows the 'VPN Virtual Server Authentication LDAP Policy Binding' dialog. It has a title bar with a close button. Below the title bar, there are three buttons: 'Add Binding' (highlighted with a red box), 'Unbind', and 'Regenerate Priorities'. Below these buttons is a dropdown menu with 'No action' selected. Below the dropdown is a table with columns: 'Priority', 'Policy Name', 'Expression', and 'Server'. The table is empty, showing 'No items'. At the bottom left is a 'Close' button.

En la sección **“Select Policy”**, seleccionar la opción **“Click to select”**:



The screenshot shows the 'Policy Binding' configuration panel. It has a title bar with a close button. Below the title bar, there is a section 'Select Policy*' with a dropdown menu showing 'Click to select' (highlighted with a red box). To the right of the dropdown are 'Add' and 'Edit' buttons. Below this is a section 'Binding Details' with a 'Priority*' field containing the value '0'. At the bottom are 'Bind' and 'Close' buttons.

Elegir la política LDAP configurada previamente:

VPN Virtual Server Authentication LDAP Policy Binding / Policy Binding / LDAP Policies

LDAP Policies

Buttons: Select, Add, Edit, Delete, Show Bindings, Global Bindings

Search: Click here to search or you can enter Key : Value format

	Name	Expression	Request Server	Globally Bound?	Priority
☒	10.24.9.50_LDAP_pol	NS_TRUE	10.24.9.50_LDAP	X	

Seleccionar la opción “**Bind**” para asociar la política elegida:

VPN Virtual Server Authentication LDAP Policy Binding / Policy Binding

Policy Binding

Select Policy*
 > Add Edit ?

► More

Binding Details

Priority*
 ?

Buttons: Bind, Close

También, en la sección “**Basic Authentication**”, seleccionar la opción “**RADIUS Policy**”:

Basic Authentication +

Primary Authentication

No LDAP Policy >

Secondary Authentication

No RADIUS Policy >

Seleccionar la opción **“Add Binding”** para añadir la política de comunicación con el servidor RSA Authentication Manager:

VPN Virtual Server Authentication RADIUS Policy Binding ×

Add Binding Unbind Regenerate Priorities

No action ▼

Priority	Policy Name	Expression	Server
No items			

Close

En la sección **“Select Policy”**, seleccionar la opción **“Click to select”**:

VPN Virtual Server Authentication RADIUS Policy Binding / Policy Binding

Policy Binding ×

Select Policy*

Click to select > Add Edit

Binding Details

Priority*

100 ?

Bind Close

Elegir la política RADIUS configurada previamente:

VPN Virtual Server Authentication RADIUS Policy Binding / Policy Binding / RADIUS Policies

RADIUS Policies ×

Select Add Edit Delete Show Bindings

Global Bindings

Click here to search or you can enter Key : Value format ?

Name	Expression	Request Server	Globally Bound?
● RSA SecureID Policy	ns_true	RSA Authentication Manager	×

Seleccionar la opción “**Bind**” para asociar la política elegida:

VPN Virtual Server Authentication RADIUS Policy Binding / Policy Binding

Policy Binding

Select Policy*

RSA SecureID Police > [Add](#) [Edit](#) ?

► More

Binding Details

Priority*

100 ?

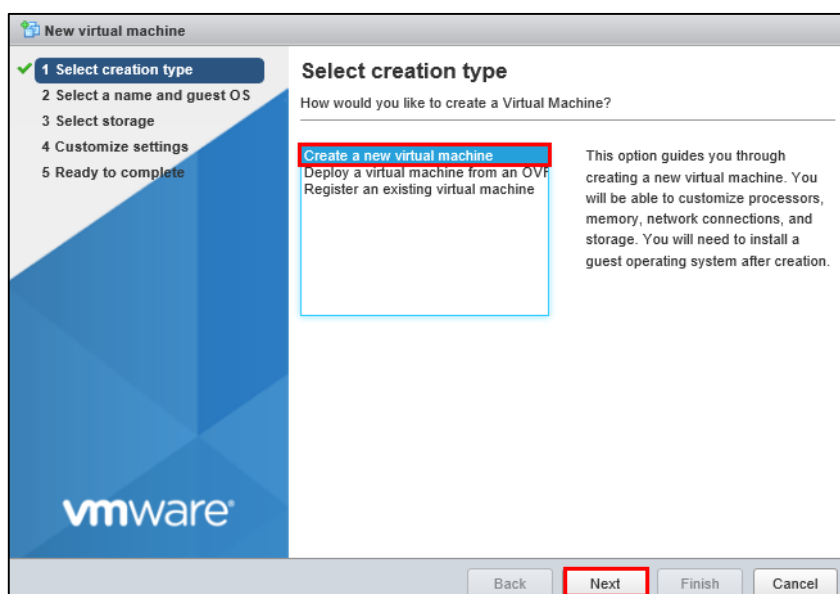
[Bind](#) [Close](#)

Paso 15: Configurar los siguientes parámetros SSL dentro del servidor virtual VPN.

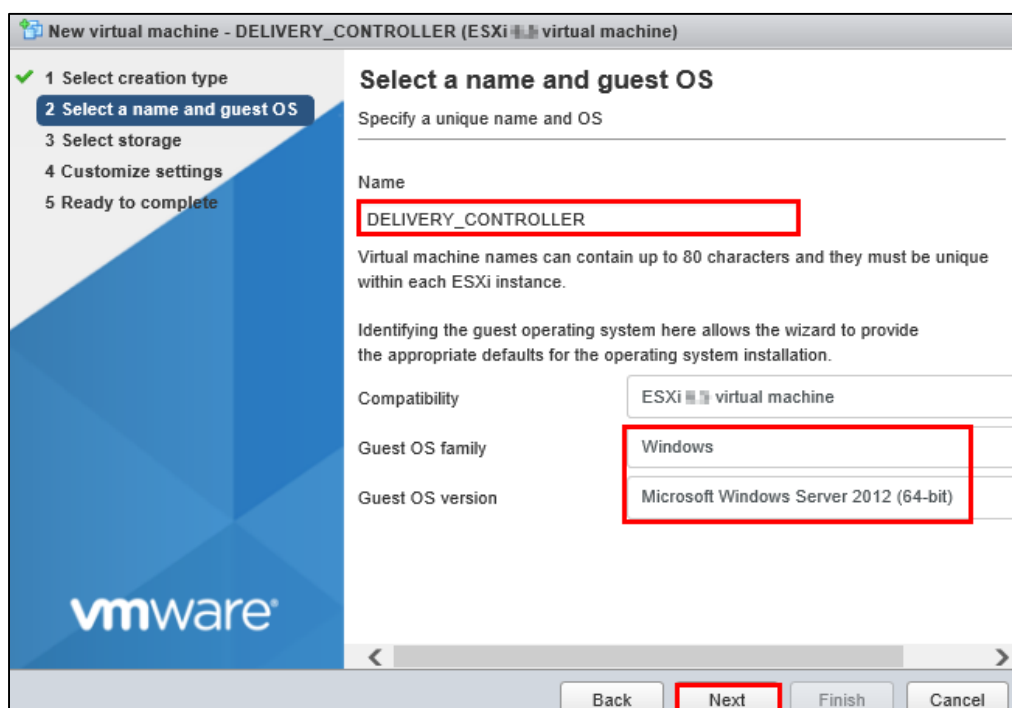
SSL Parameters					
Enable DH Param	DISABLED	Clear Text Port	0	OCSF Stapling	DISABLED
Enable DH Key Expire Size Limit	DISABLED	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
Enable Ephemeral RSA	ENABLED	Client Authentication	DISABLED	SSLv2	DISABLED
Refresh Count	0	Send Close-Notify	YES	SSLv3	ENABLED
Enable Session Reuse	ENABLED	PUSH Encryption Trigger	Always	TLSv1	ENABLED
Time-out	120	SNI Enable	DISABLED	TLSv11	ENABLED
SSL Redirect	DISABLED	HSTS	DISABLED	TLSv12	ENABLED
Strict Signature Digest Check	DISABLED	Max Age	0	TLSv13	DISABLED
		Include Subdomains	NO		
		TLS13 Session Tickets Per Authcontext	1		

Procedimiento instalación de Citrix delivery controller

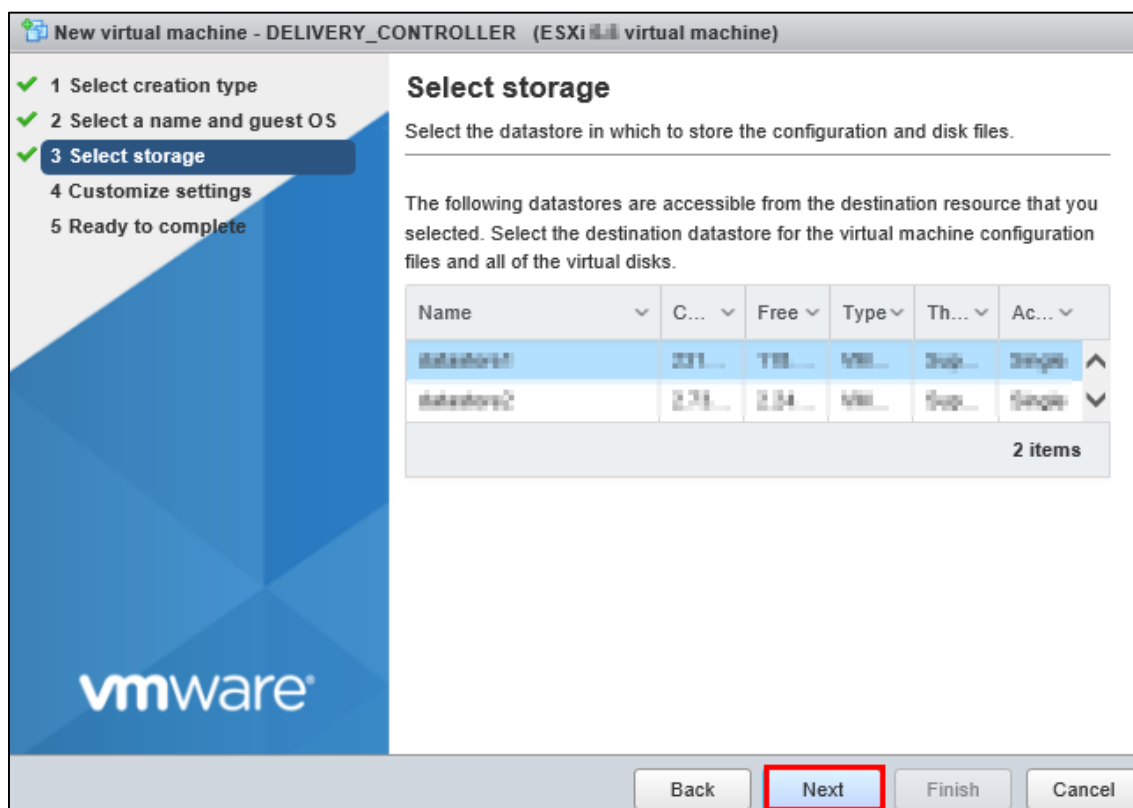
Paso 1: Crear una nueva máquina virtual con sistema operativo Microsoft Windows Server (versión 2012 R2 o 2016), el cual albergará la plataforma Citrix Delivery Controller y demás componentes.



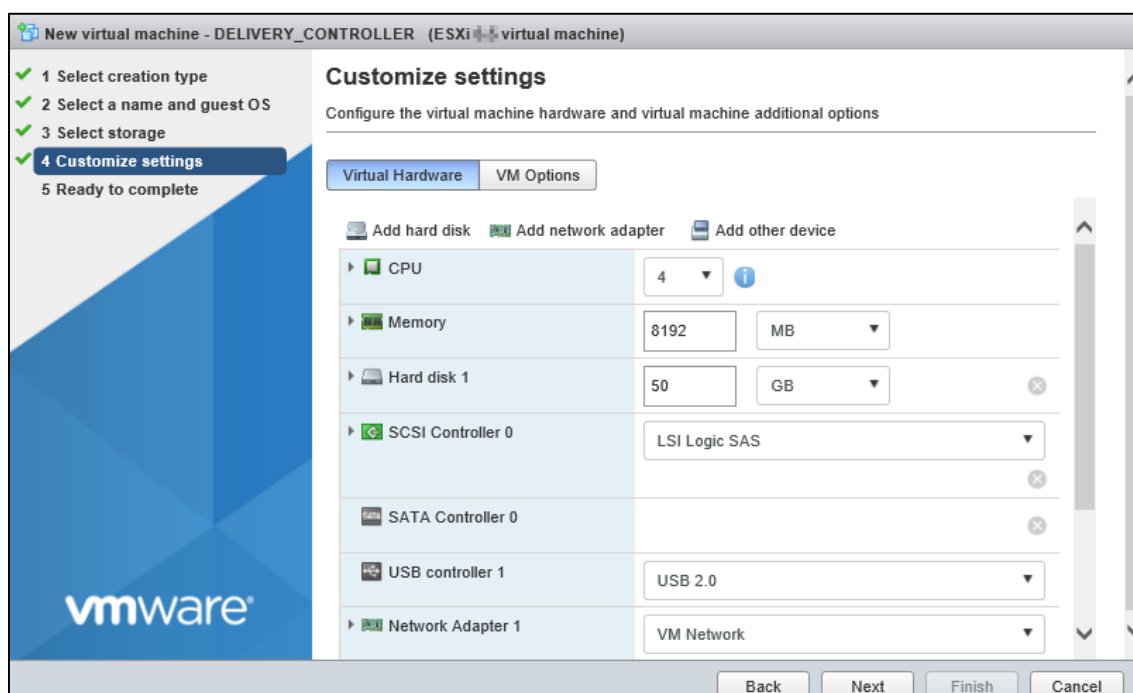
Paso 2: Ingresar un nombre para la máquina virtual, seleccionar el sistema operativo y versión correspondiente (por ejemplo, Microsoft Windows Server 2012). Dar click en “Next”.



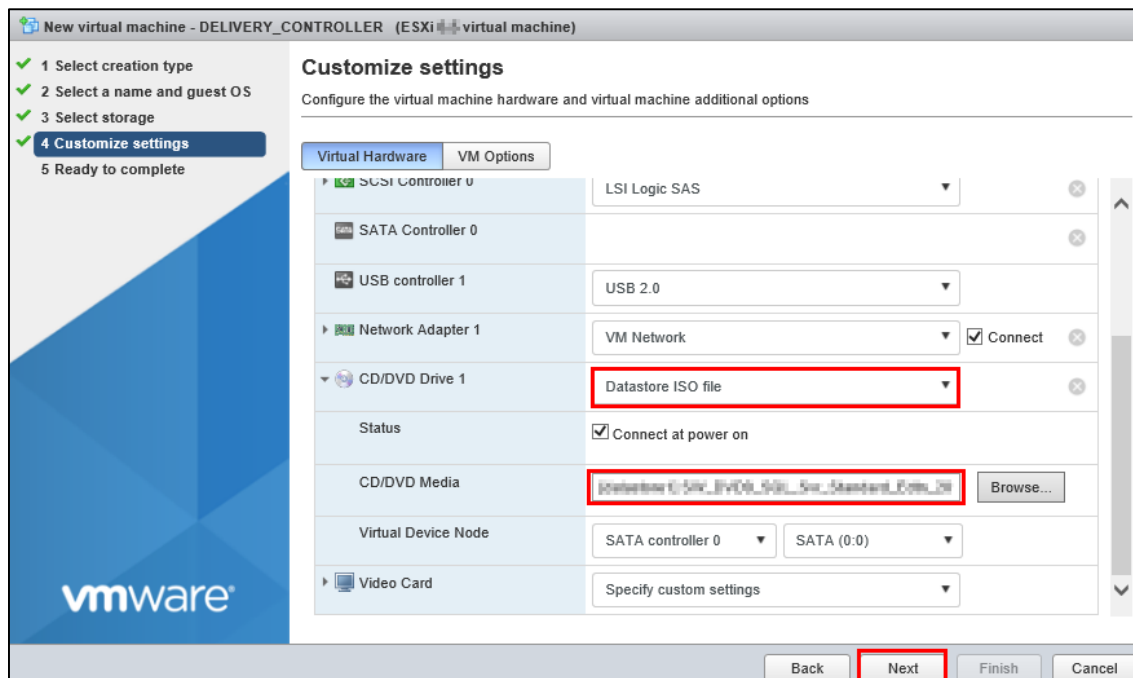
Paso 3: Seleccionar el datastore en donde se almacenará la configuración de esta máquina virtual. Dar click en “Next”.



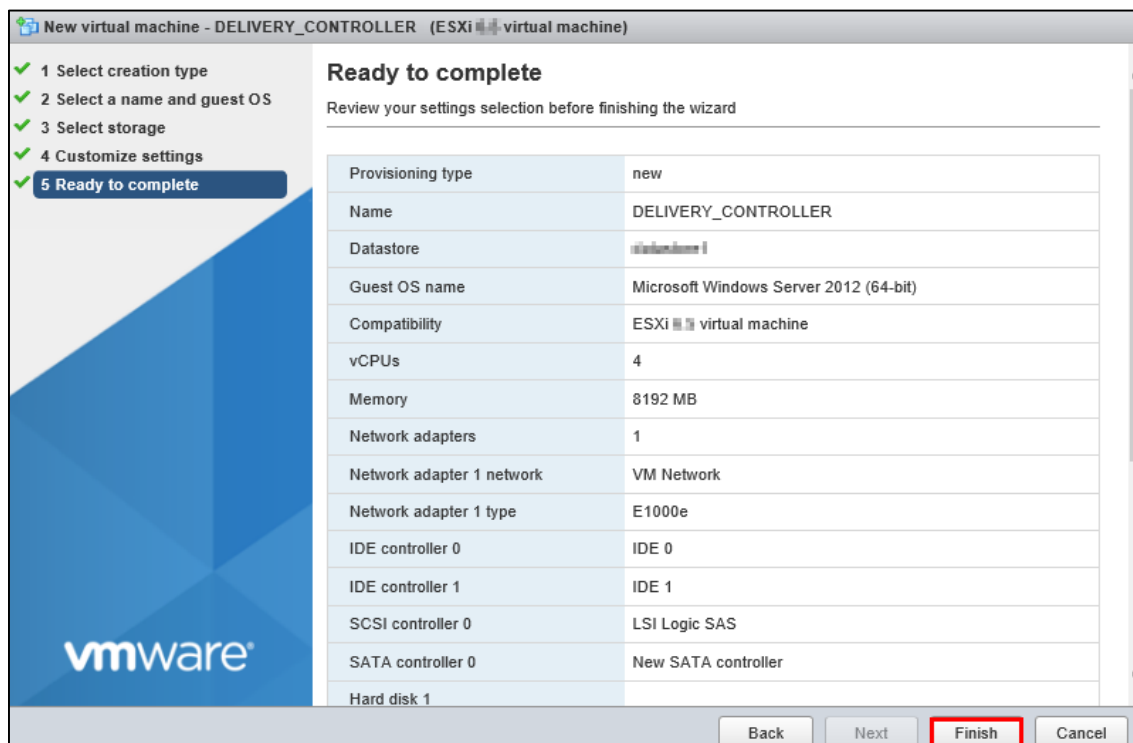
Paso 4: Ingresar los parámetros de almacenamiento y procesamiento que se asignará a esta máquina virtual.



Paso 5: En el campo “CD/DVD Drive 1”, seleccionar la opción “Datastore ISO File” (ubicar el archivo ISO del sistema operativo almacenado en el datastore) y habilitar la opción “Connect at power on”. Dar click en “Next”.



Paso 6: Seleccionar la opción “Finish” para finalizar la creación de la máquina virtual.



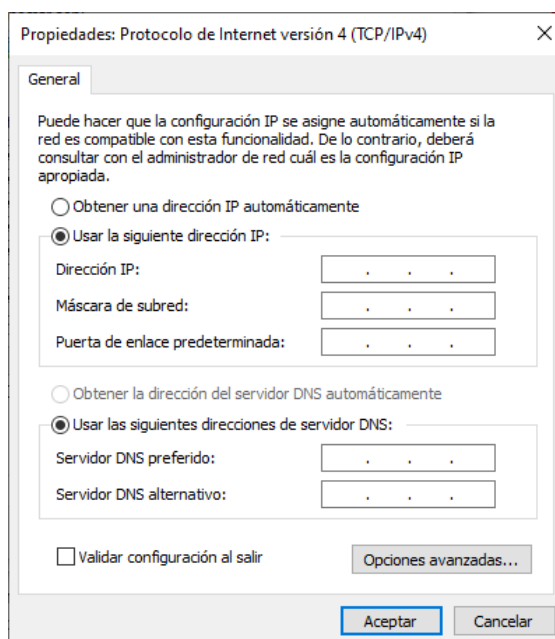
Paso 7: Encender la máquina virtual y esperar que el archivo ISO se ejecute automáticamente. Luego, proceder con la instalación correspondiente de la versión de Windows involucrada.



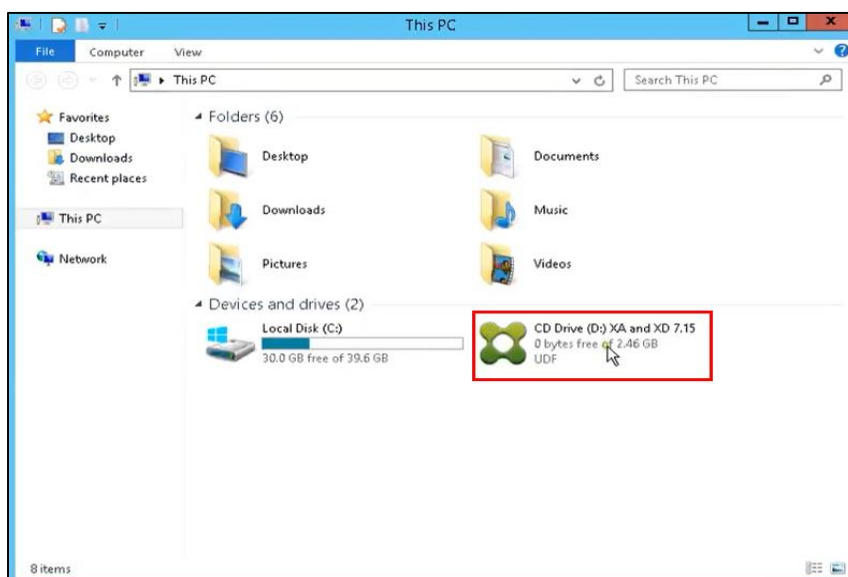
Paso 8: Luego de culminar la instalación, la máquina virtual se reiniciará y estará lista para ser utilizada.



Paso 9: Ingresar el direccionamiento de red asignado a este equipo y agregarlo al dominio de la institución.



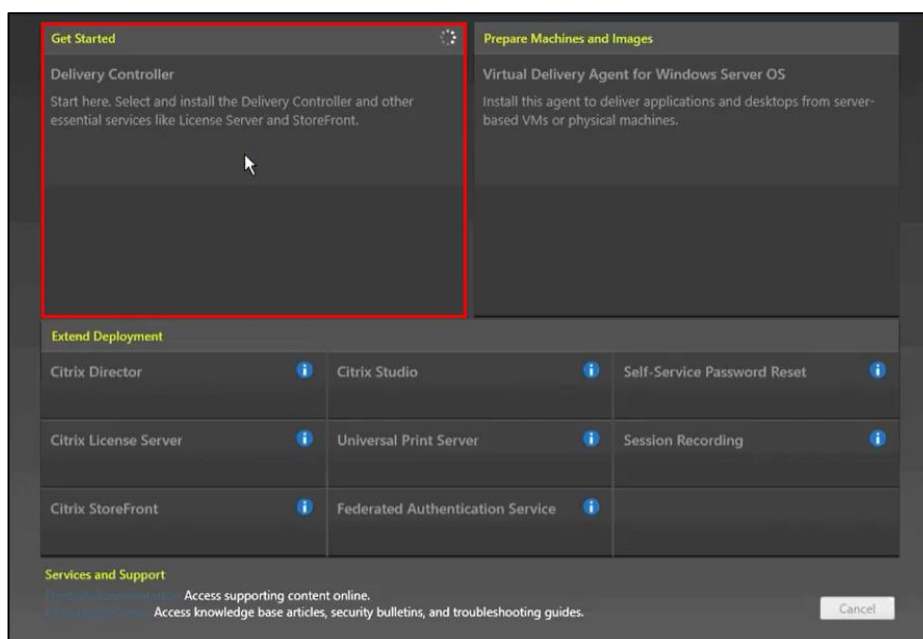
Paso 10: Ejecutar el instalador correspondiente de la plataforma Citrix.



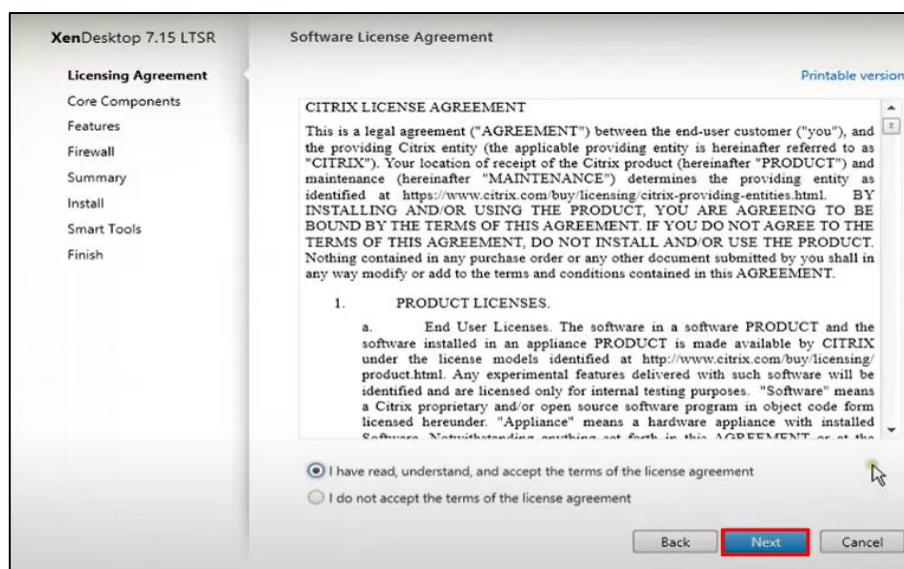
Paso 11: En primer lugar, seleccionar el botón “**Start**” en la opción “**XenDesktop**”, debido a que se realizará la virtualización de aplicaciones y escritorios.



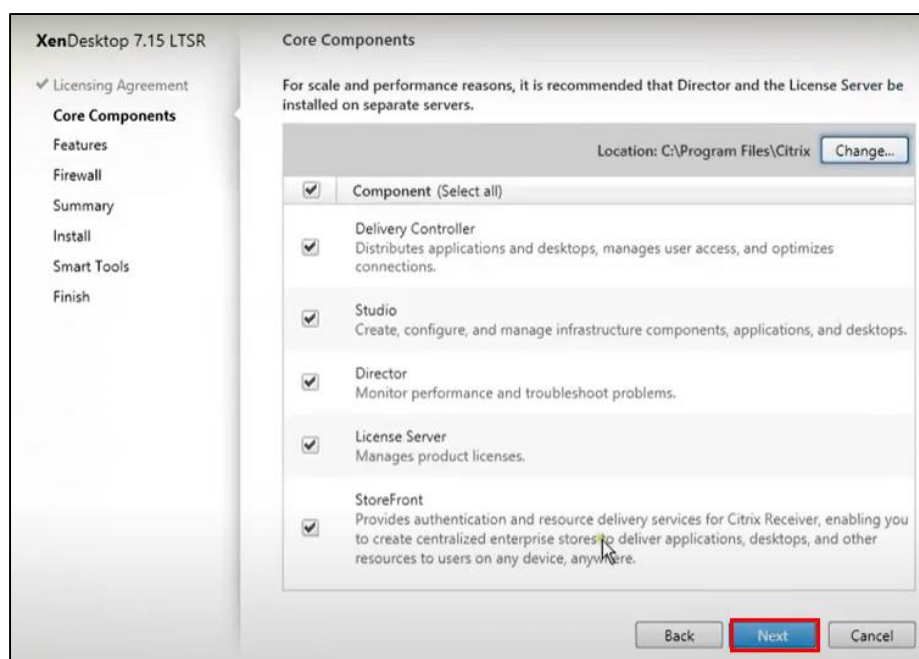
Paso 12: Seleccionar la opción “**Delivery Controller**”.



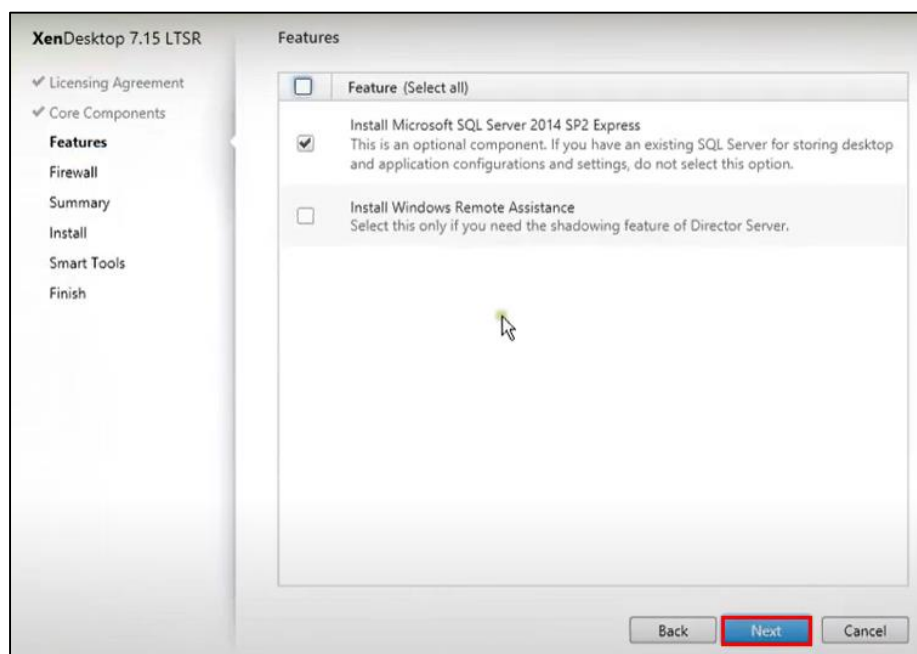
Paso 13: Aceptar los términos de licencia correspondientes.



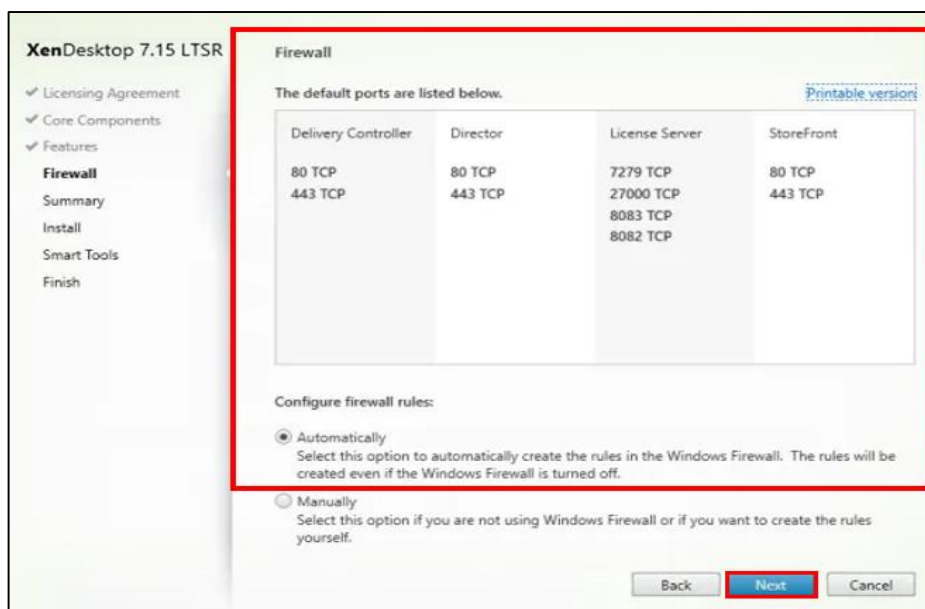
Paso 14: Elegir los componentes que se instalarán (en este caso, todos los componentes estarán en el mismo servidor) y seleccionar el botón “Next”.



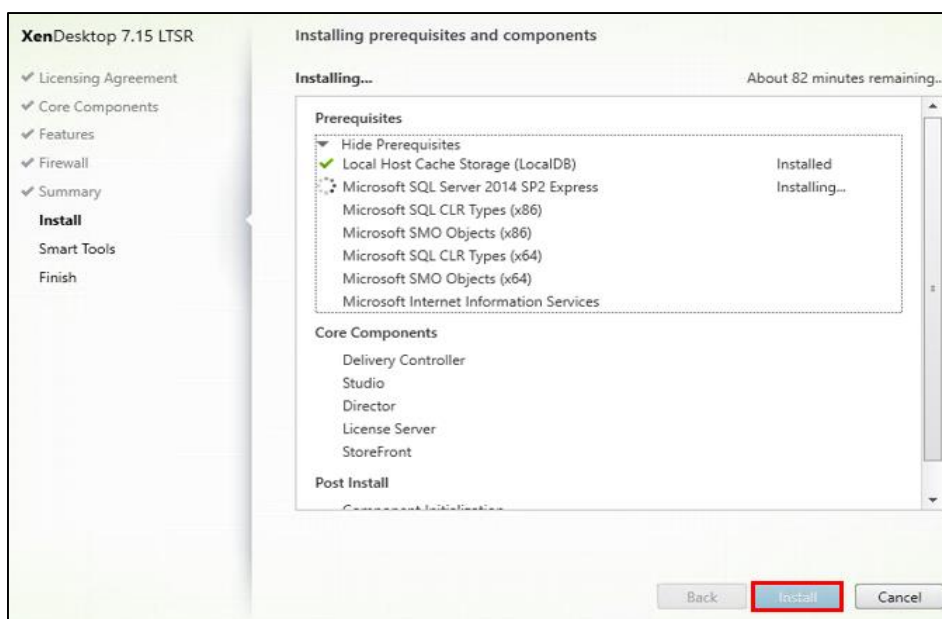
Paso 15: Elegir la característica de instalación de la base de datos correspondiente y seleccionar el botón “Next”.



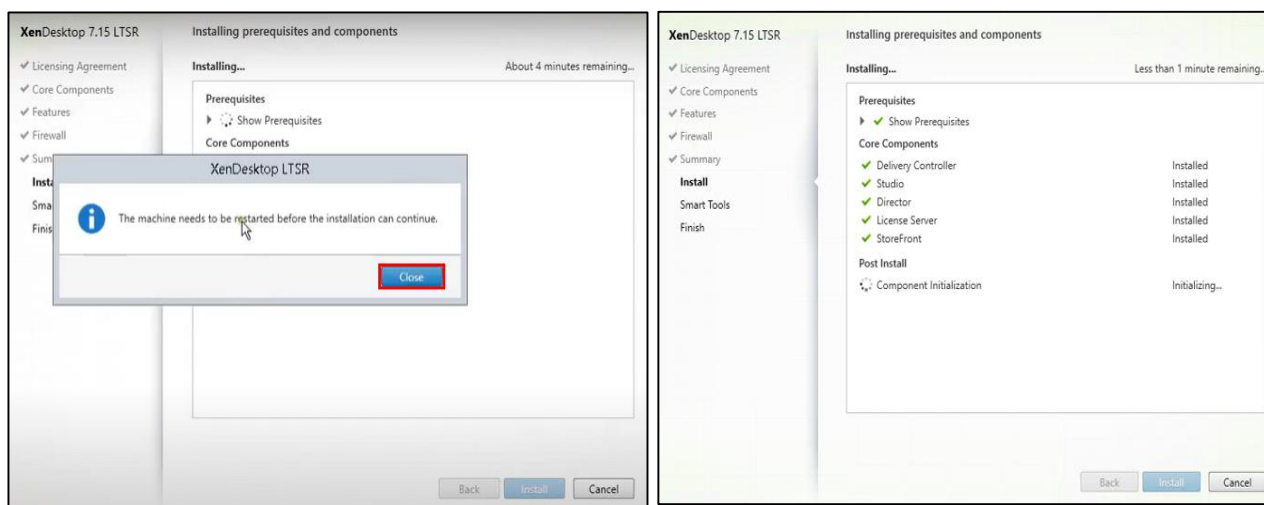
Paso 16: Corroborar que se tienen abiertos los puertos de comunicación necesarios, seleccionar la opción de configuración automática y dar click en “Next”.



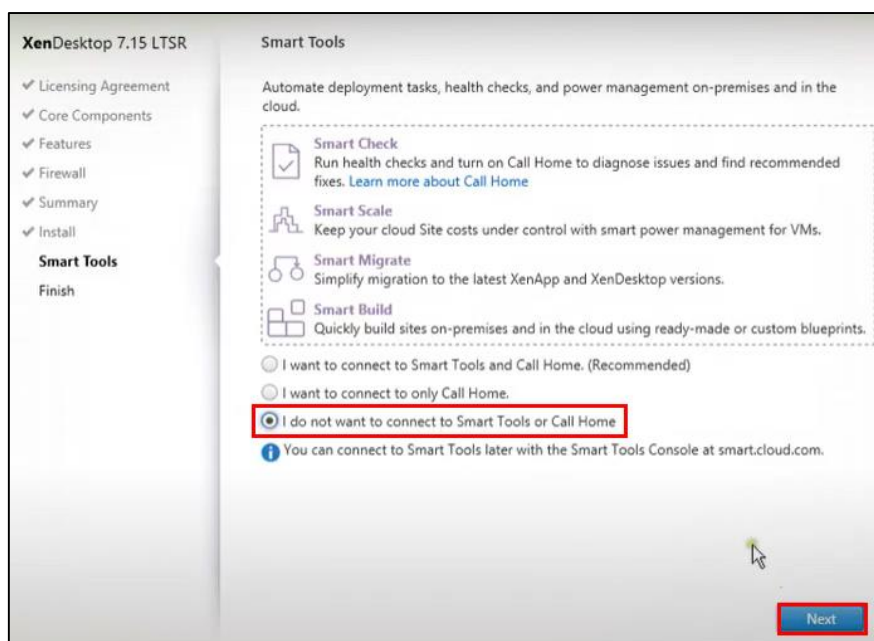
Paso 17: Proceder con la instalación correspondiente (botón “Install”).



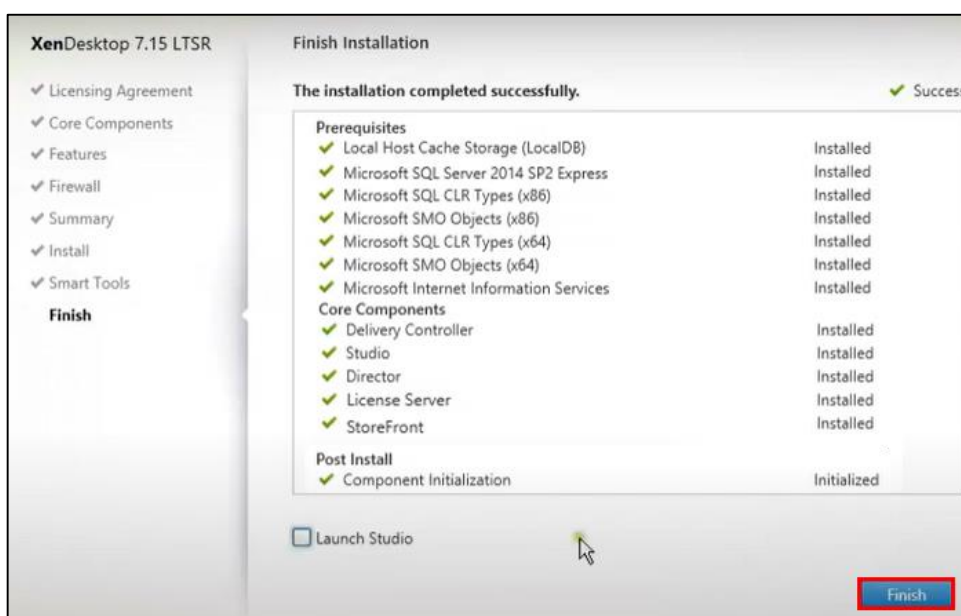
Paso 18: Durante el proceso de instalación se solicitará el reinicio de la máquina virtual para luego continuar (botón “Close” para proceder con el reinicio).



Paso 19: Elegir la casilla para no conectar con Smart Tools y seleccionar el botón “Next”.

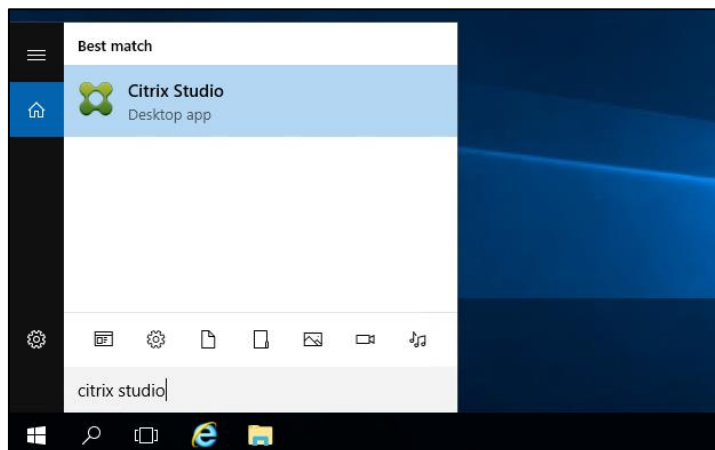


Paso 20: Finalizar el proceso de instalación, seleccionando la opción “Finish”.

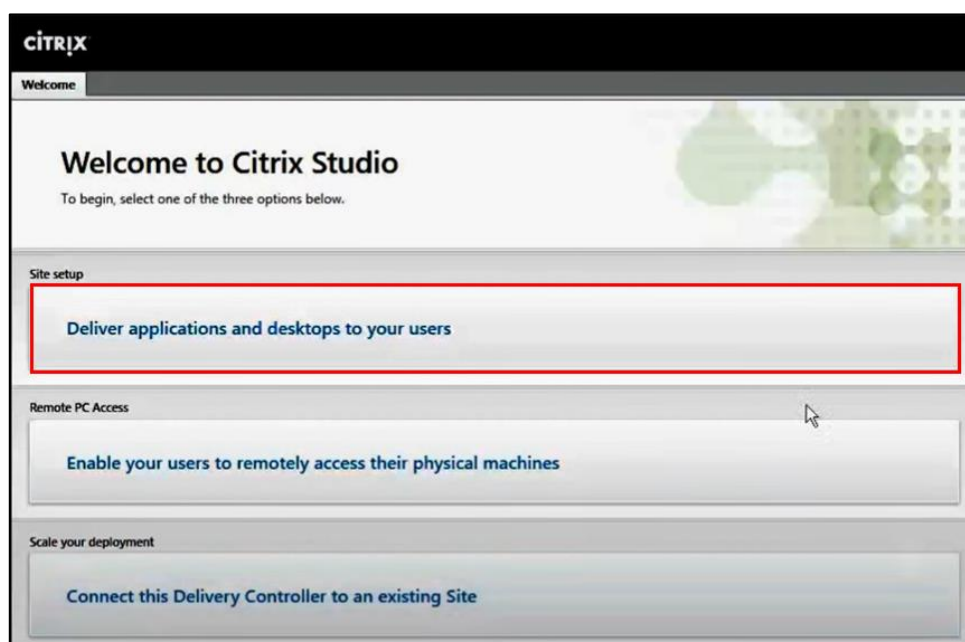


Procedimiento configuración de Citrix delivery controller

Paso 1: Abrir la aplicación “Citrix Studio” para realizar toda la configuración de la plataforma.



Paso 2: Crear el site que será usado para este despliegue, seleccionando la opción “Deliver applications and desktops to your users”.



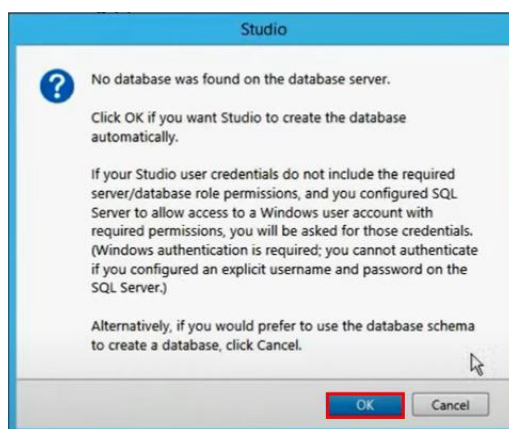
Paso 3: Ingresar el nombre del site a configurar. Dar click en “Next”.

The screenshot shows the 'Site Setup' wizard in the 'Introduction' step. On the left, a sidebar lists the steps: Introduction, Databases, Licensing, Connection, Network, Additional Features, and Summary. The main area contains an 'Introduction' section with text explaining the two options for creating a new site. Below this, a question asks 'What kind of Site do you want to create?' with two radio button options: 'A fully configured, production-ready Site (recommended for new users)' (selected) and 'An empty, unconfigured Site'. A 'Site name:' label is followed by a text input field containing 'Citrix', which is highlighted with a red rectangle. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red rectangle and a mouse cursor), and 'Cancel'.

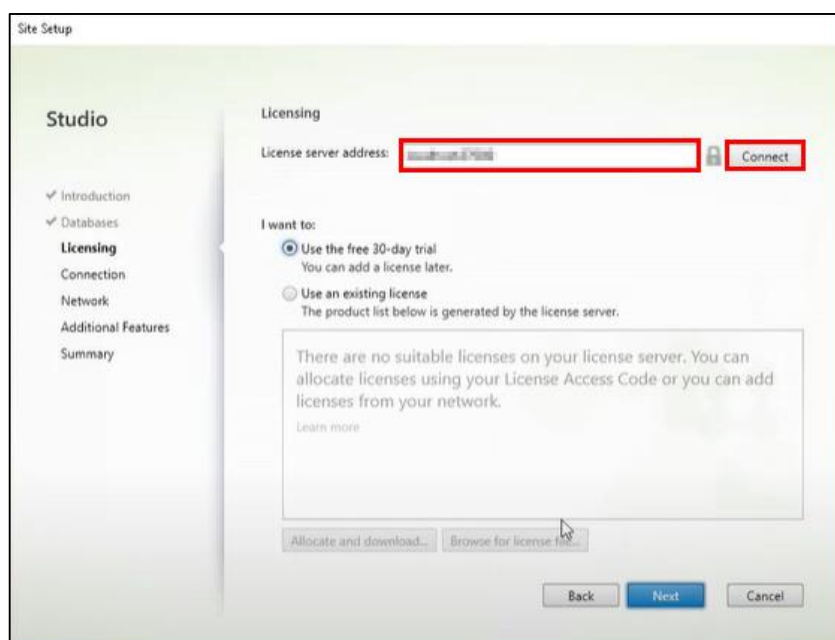
Paso 4: Seleccionar la opción “Create and set up databases from Studio” y mantener los demás datos. Dar click en “Next”.

The screenshot shows the 'Site Setup' wizard in the 'Databases' step. The left sidebar now has 'Databases' selected. The main area has a 'Databases' section with text explaining that databases store information about site setup, configuration logging, and monitoring. It offers two options: 'Create and set up databases from Studio (You can provide details of existing empty databases)' (selected and highlighted with a red rectangle) and 'Generate scripts to manually set up databases on the database server'. Below this, a 'Provide database details' section contains a table with three columns: 'Data type', 'Database name', and 'Location (formats)'. The table has three rows: 'Site' with 'CitrixCitrixSite' and 'localhost\\sqlexpress', 'Monitoring' with 'CitrixCitrixMonitoring' and 'localhost\\sqlexpress', and 'Logging' with 'CitrixCitrixLogging' and 'localhost\\sqlexpress'. A blue information icon and text state: 'Default database names and SQL Server Express location are provided'. Below the table, there is a section for 'Specify additional Delivery Controllers for this Site' with a 'Learn more' link and a 'Select...' button, showing '1 selected'. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red rectangle and a mouse cursor), and 'Cancel'.

Paso 5: Seleccionar el botón “OK” para aceptar la creación automática de la base de datos local.



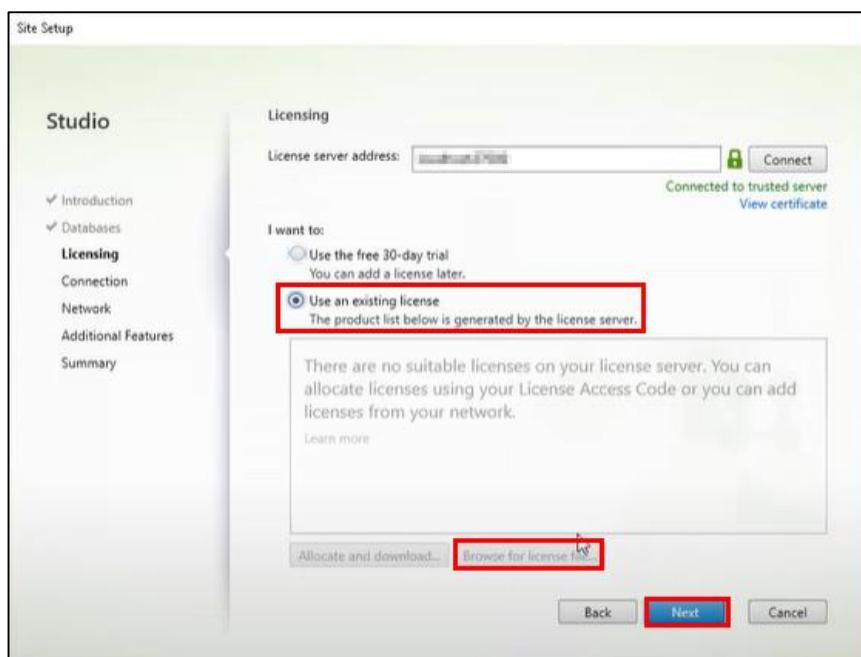
Paso 6: Ingresar la dirección del servidor de licencia y seleccionar la opción “Connect”.



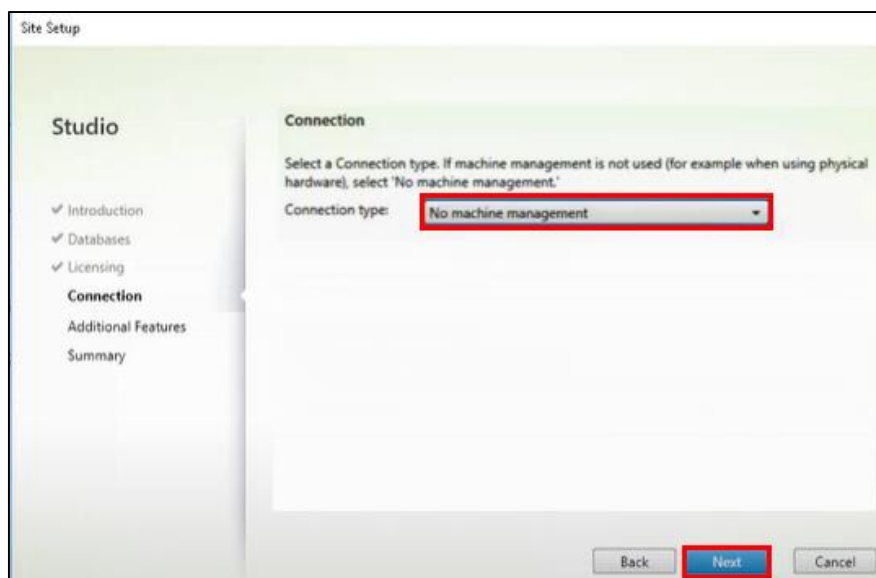
Paso 7: Seleccionar la opción “Connect me” y luego “Confirm”.



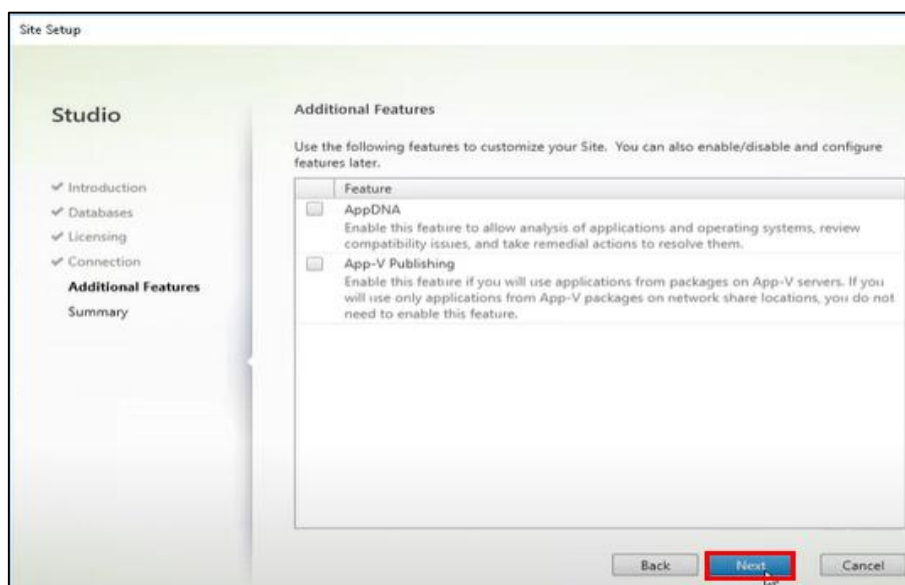
Paso 8: Importar la licencia correspondiente, seleccionando la opción **“Use an existing license”** y luego **“Browse for license file...”** (para ubicar y elegir el archivo). Dar click en **“Next”**.



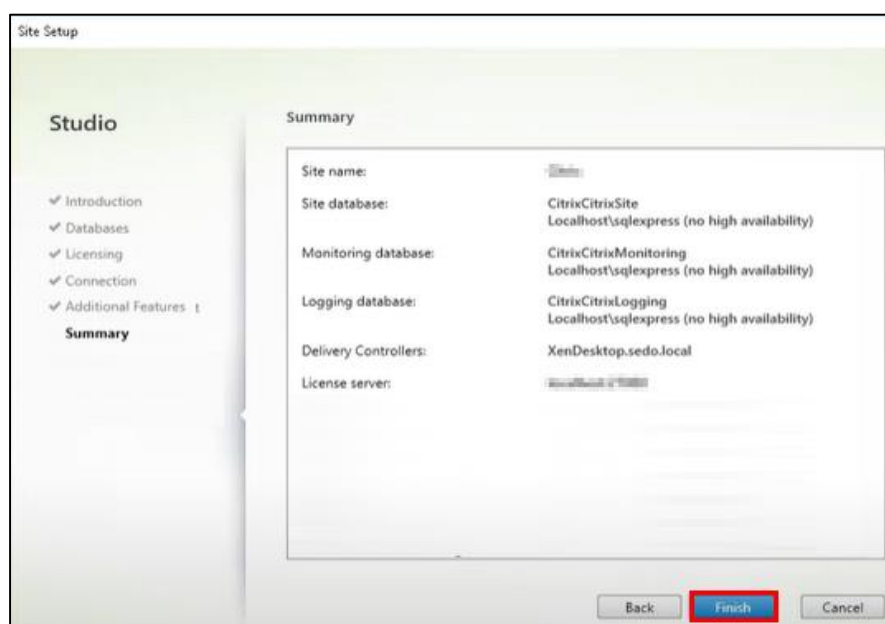
Paso 9: Seleccionar la opción **“No machine management”**. Dar click en **“Next”**.



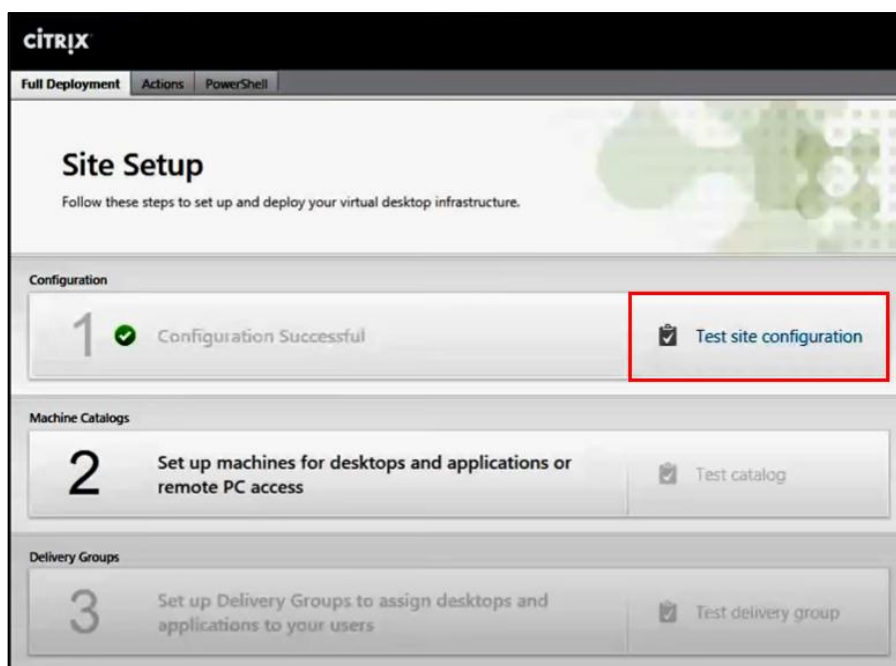
Paso 10: En la sección “Additional Features” no marcar ninguna opción adicional. Dar click en “Next”.



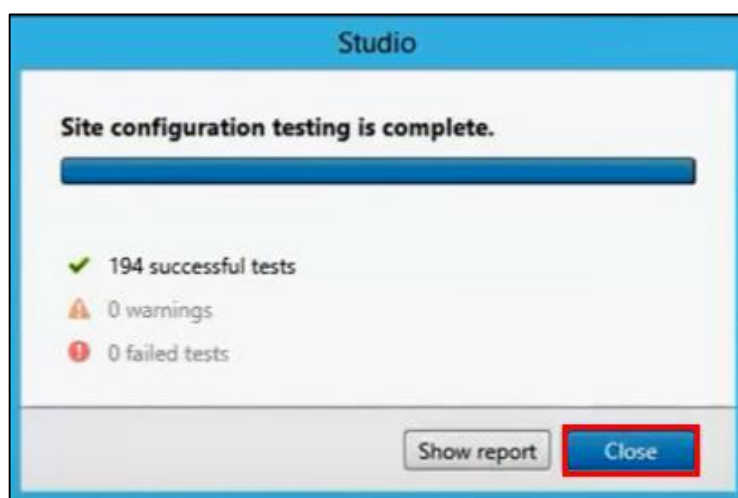
Paso 11: Revisar el resumen de la configuración del componente Citrix Studio y seleccionar la opción “Finish”.



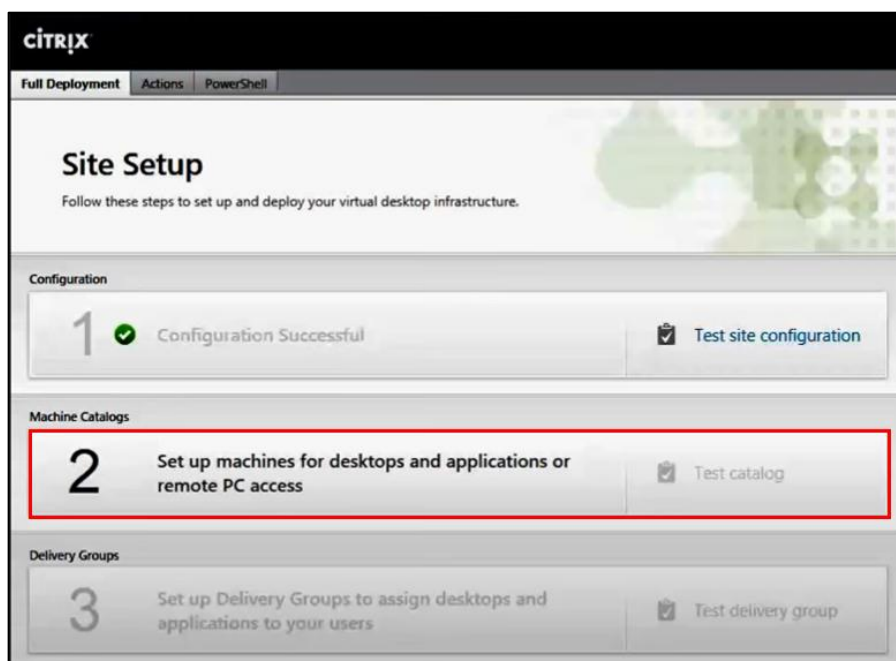
Paso 12: Seleccionar la opción “**Test site configuration**” para validar la configuración.



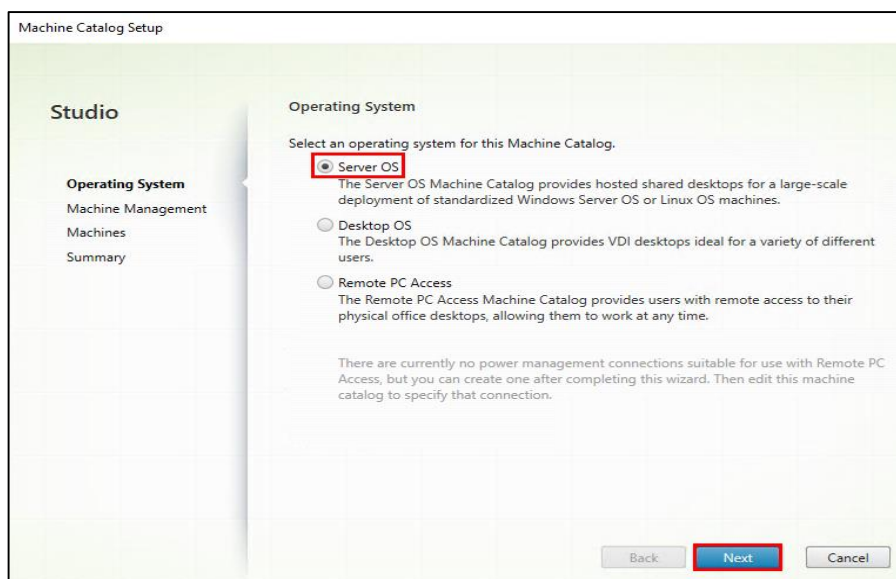
Luego del resultado satisfactorio, dar click en “**Close**”.



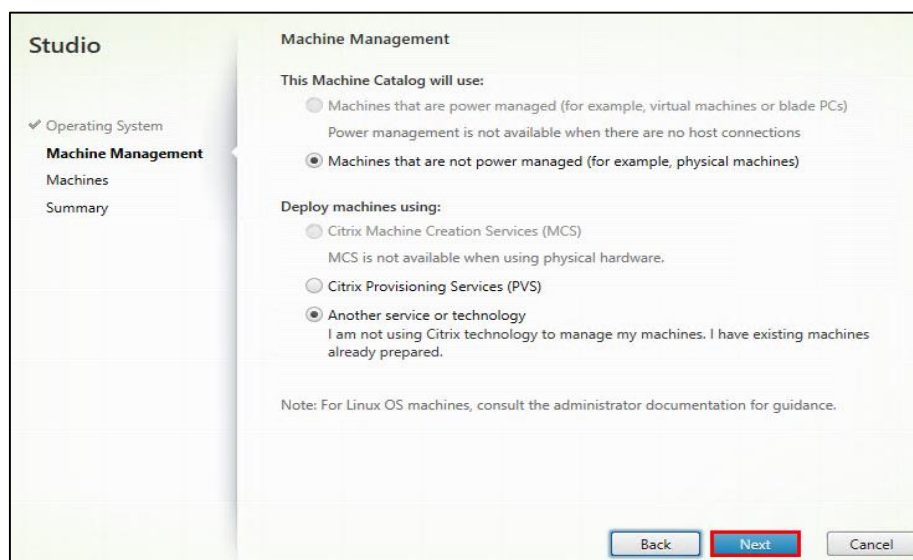
Paso 13: Seleccionar la **opción 2** para configurar las máquinas para los escritorios y aplicaciones.



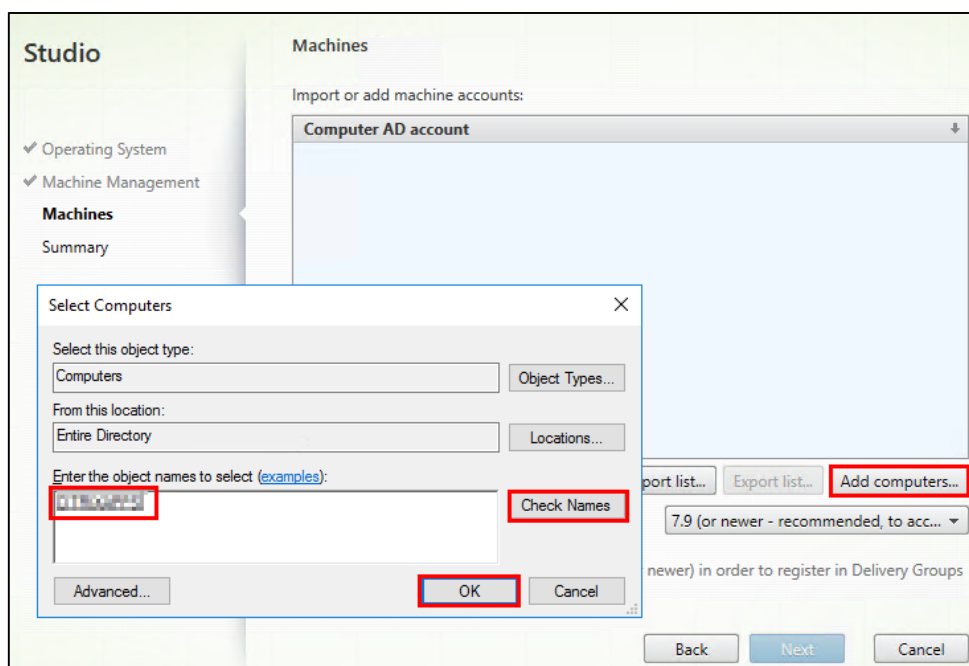
Paso 14: Seleccionar la opción “**Server OS**”. Dar click en “**Next**”.



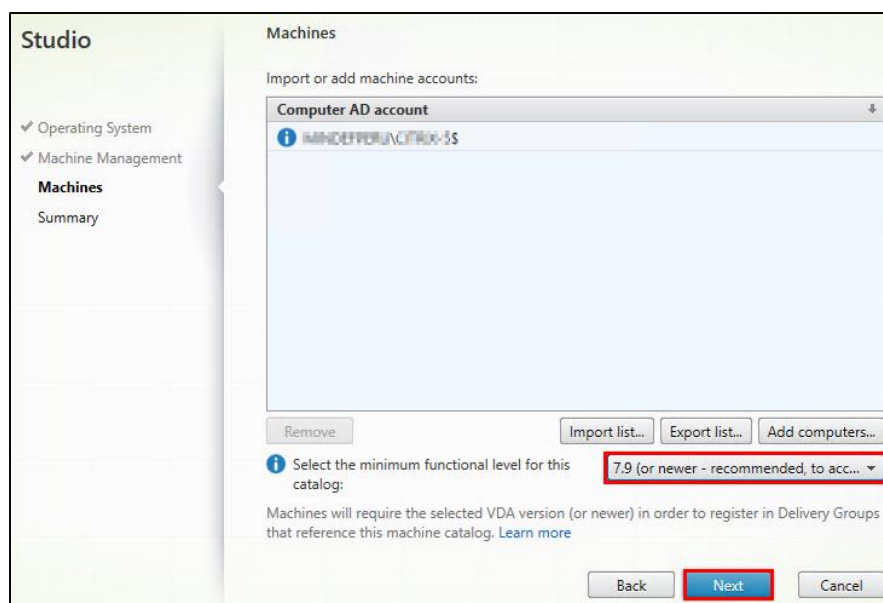
Paso 15: Seleccionar las opciones mostradas en la siguiente imagen y dar click en “Next”.



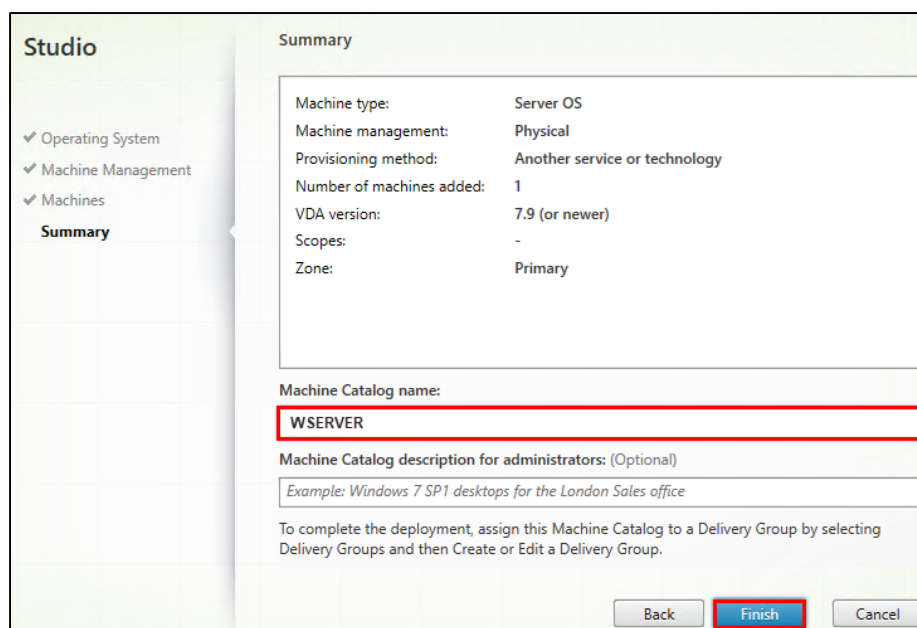
Paso 16: Seleccionar la opción “Add computers...”, luego ingresar y validar el nombre del servidor de aplicaciones. Dar click en “OK”.



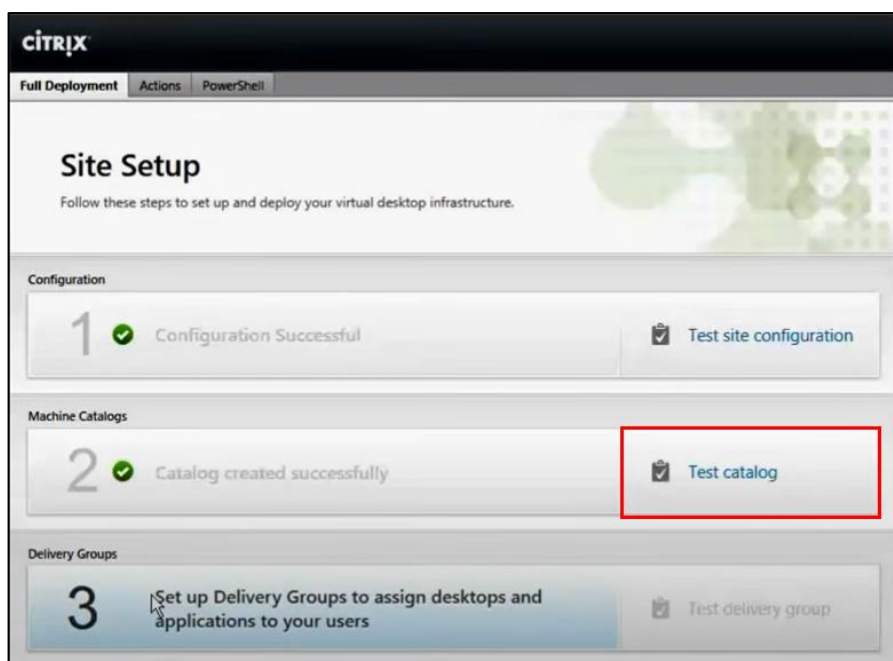
Paso 17: Seleccionar la versión de VDA recomendada y dar click en “Next”.



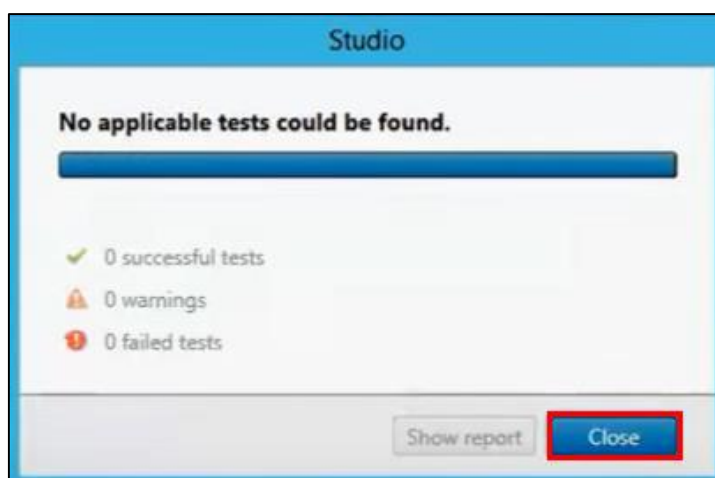
Paso 18: Verificar los datos, colocar un nombre al catálogo de máquina del tipo Server OS y dar click en “Finish”.



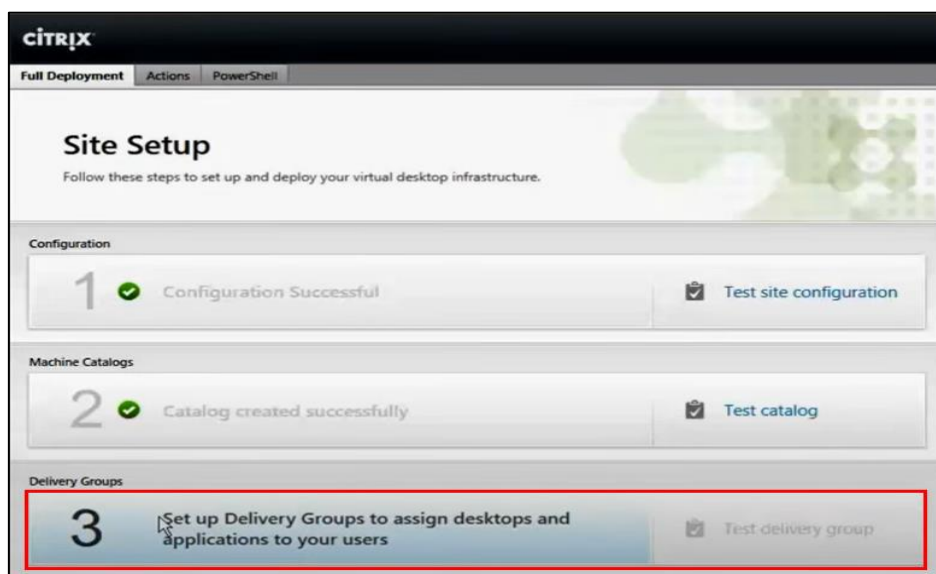
Paso 19: Seleccionar la opción “**Test catalog**” para validar la configuración.



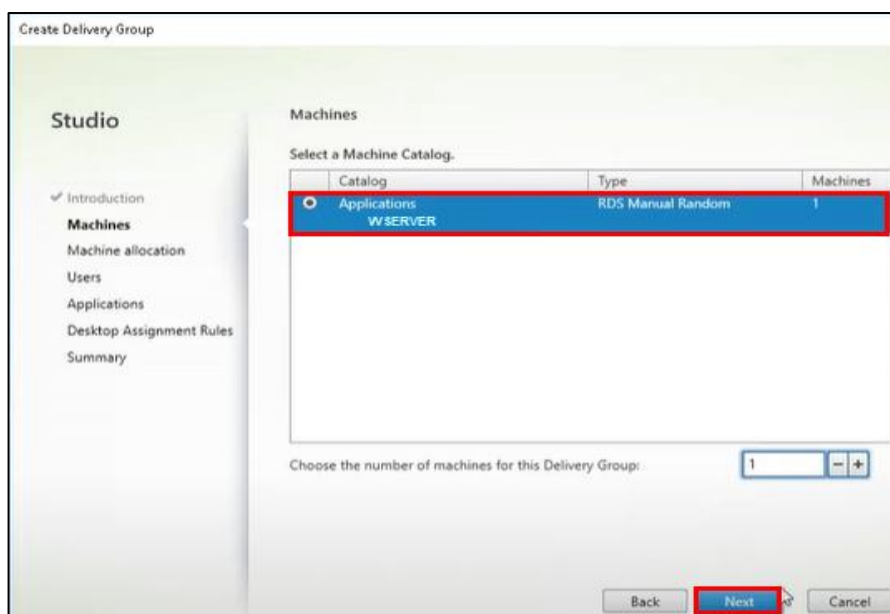
Luego del resultado obtenido (en este caso, no hay test disponible para este tipo de configuración), dar click en “**Close**”.



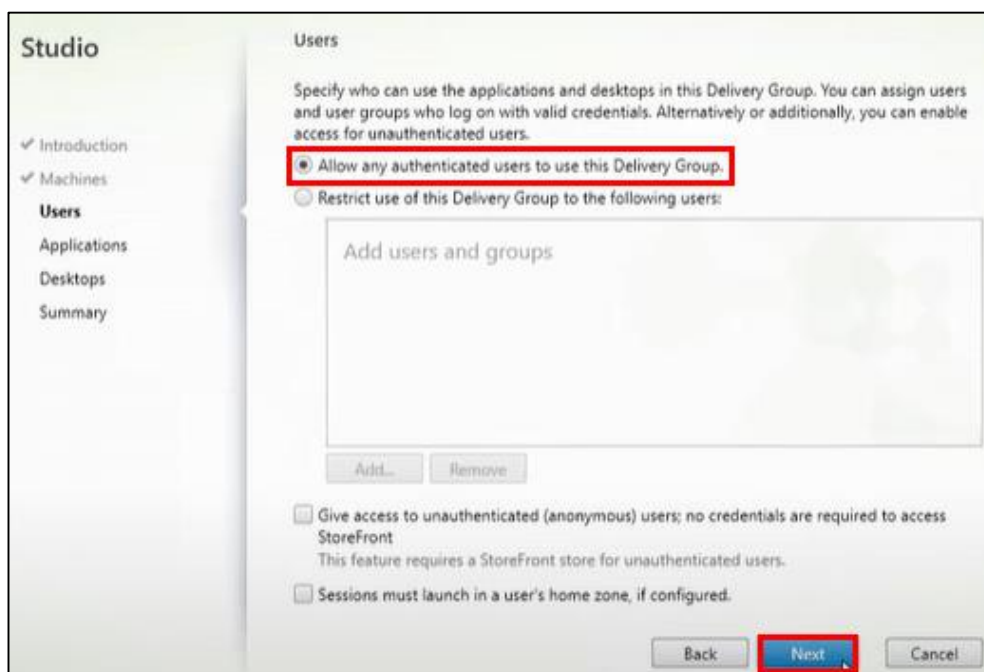
Paso 20: Seleccionar la **opción 3** para configurar los grupos de entrega para la asignación de escritorios y aplicaciones a los usuarios.



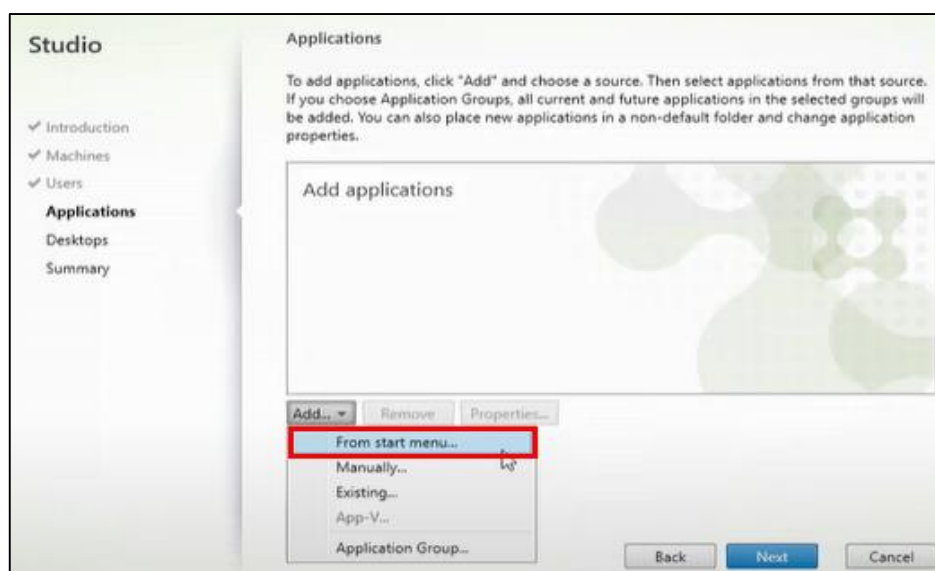
Paso 21: Seleccionar el catálogo de máquina del tipo Server OS creado (relacionado al servidor de aplicaciones) y dar click en “Next”.



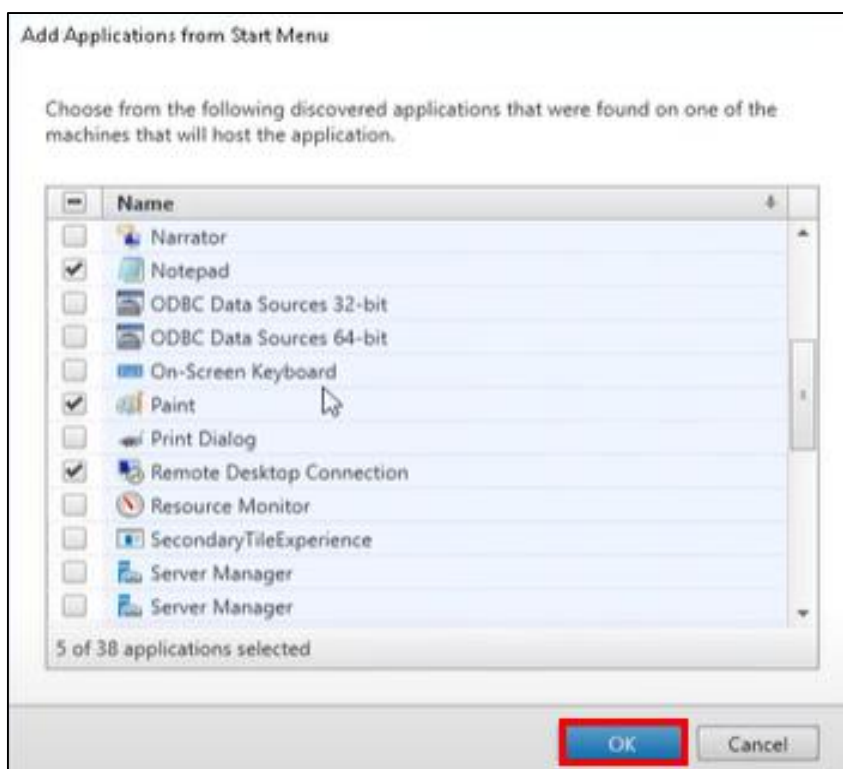
Paso 22: Para el caso de las aplicaciones virtuales, permitir el acceso a todos los usuarios autenticados. Dar click en “Next”.



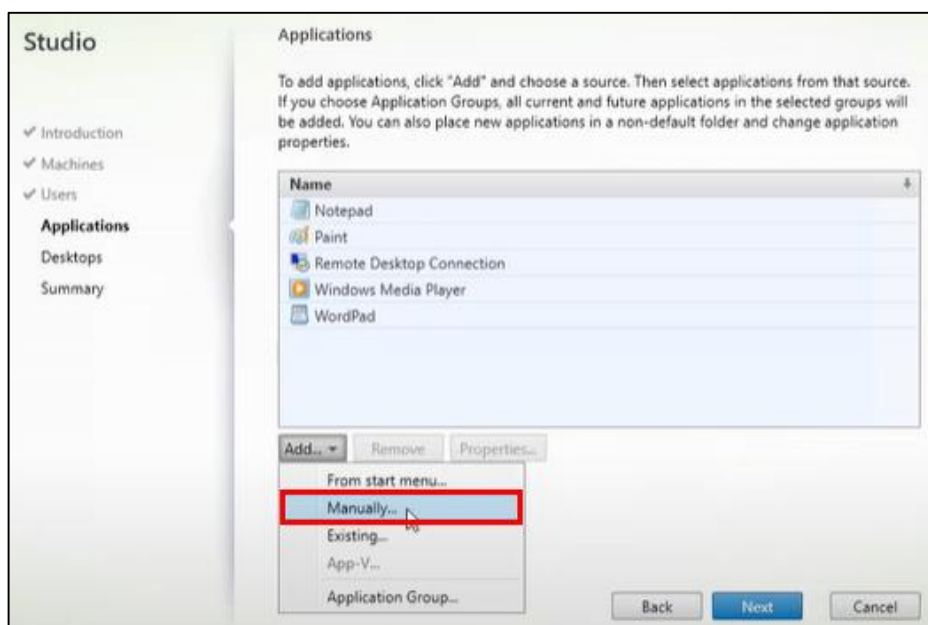
Paso 23: Seleccionar la opción “Add... > From start menu...” para agregar las aplicaciones.



Luego, elegir las aplicaciones necesarias del listado y dar click en **“OK”**:



Para agregar un navegador web, seleccionar la opción **“Add... > Manually...”**:



Seleccionar la opción “**Browse...**” para ubicar la ruta del archivo ejecutable del navegador web involucrado, ingresar un nombre para la aplicación y dar click en “**OK**”:

Add Applications Manually

Add an Application Manually

You can add applications from the virtual machine in this Delivery Group or from a different network location.

Path to the executable file:

Example: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe **Browse...**

Command line argument (optional):

Example: http://www.example.com

Working directory:

Example: %ProgramFiles(x86)%\Internet Explorer **Browse...**

Application name (for user):

Example: Example Web Site

Application name (for administrator):

Example: Internet Explorer - Example Web Site

OK **Cancel**

A continuación, verificar las aplicaciones agregadas y dar click en “**Next**”:

Studio

Applications

To add applications, click "Add" and choose a source. Then select applications from that source. If you choose Application Groups, all current and future applications in the selected groups will be added. You can also place new applications in a non-default folder and change application properties.

Name

- Internet Explorer
- Notepad
- Paint
- Remote Desktop Connection
- Windows Media Player
- WordPad

Add... **Remove** **Properties...**

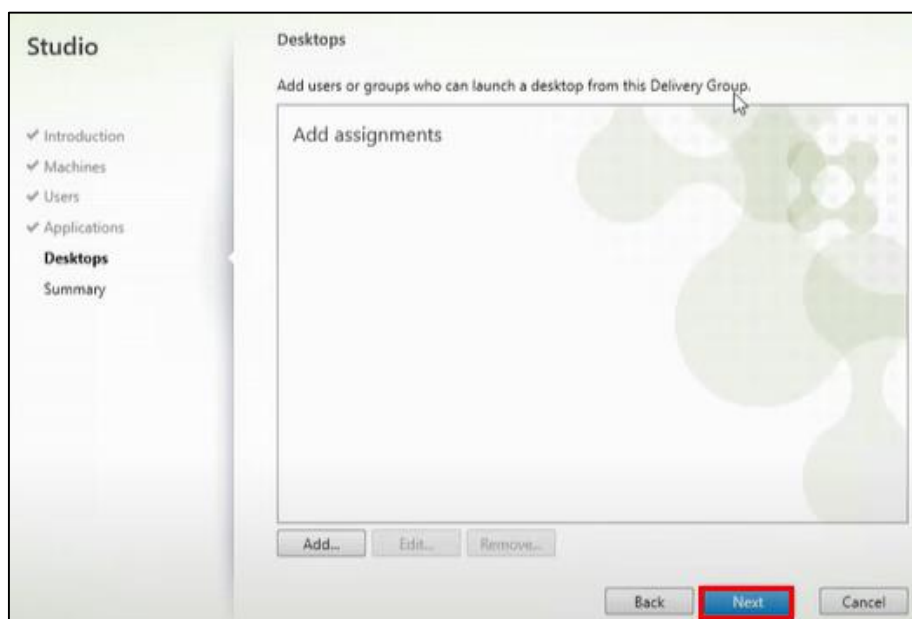
Place the new applications in folder:

Applications\

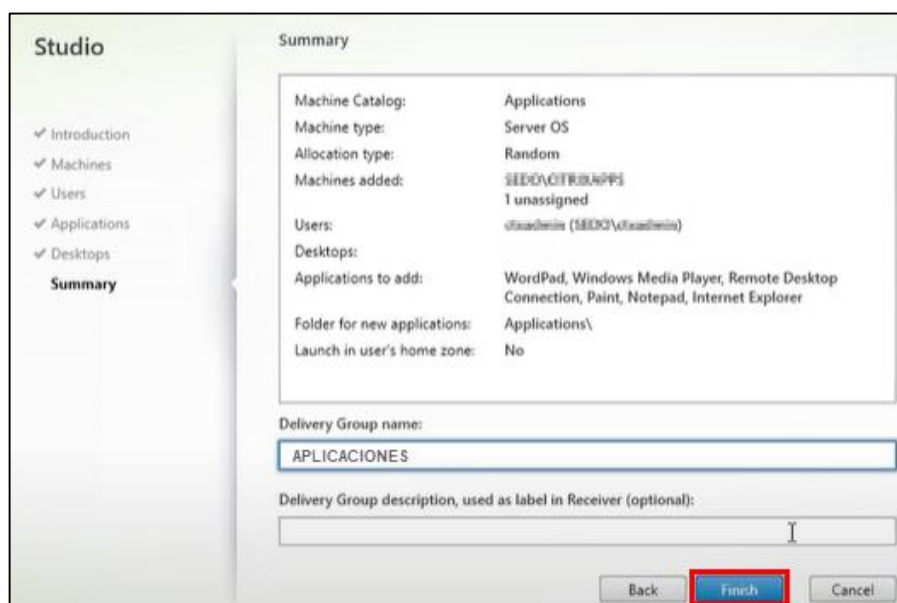
Change...

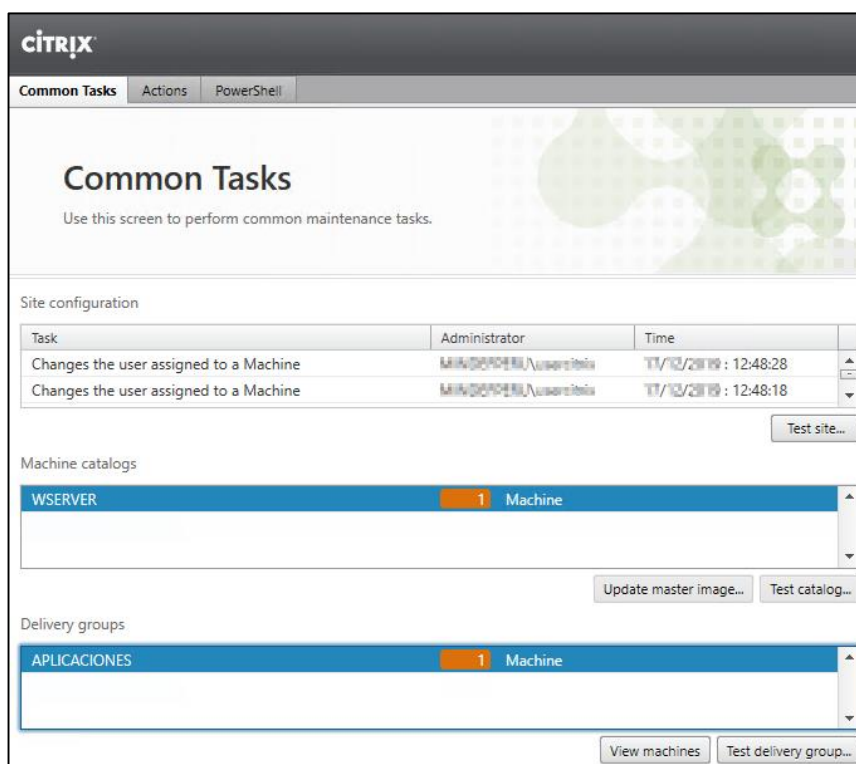
Back **Next** **Cancel**

Paso 24: No agregar ningún escritorio en esta opción, debido a que el Delivery Group que se está creando solo será de aplicaciones.

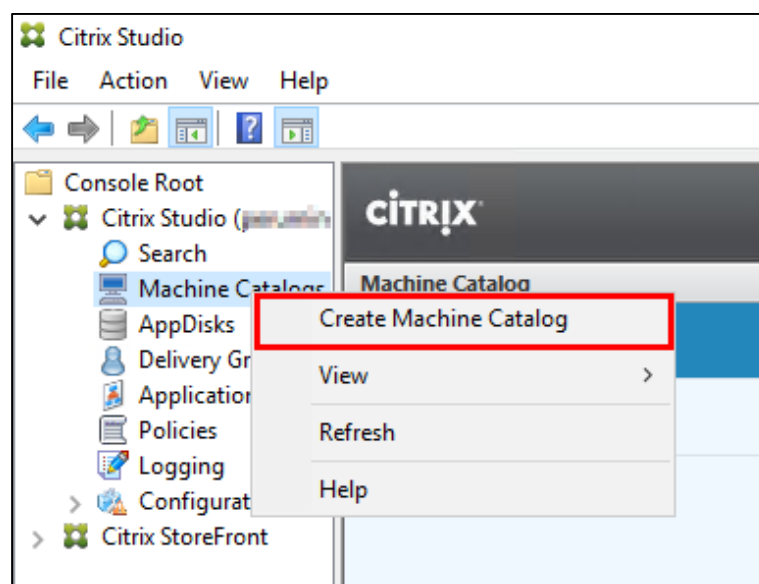


Paso 25: Verificar las configuraciones, asignar un nombre al Delivery Group y dar click en “Finish”.

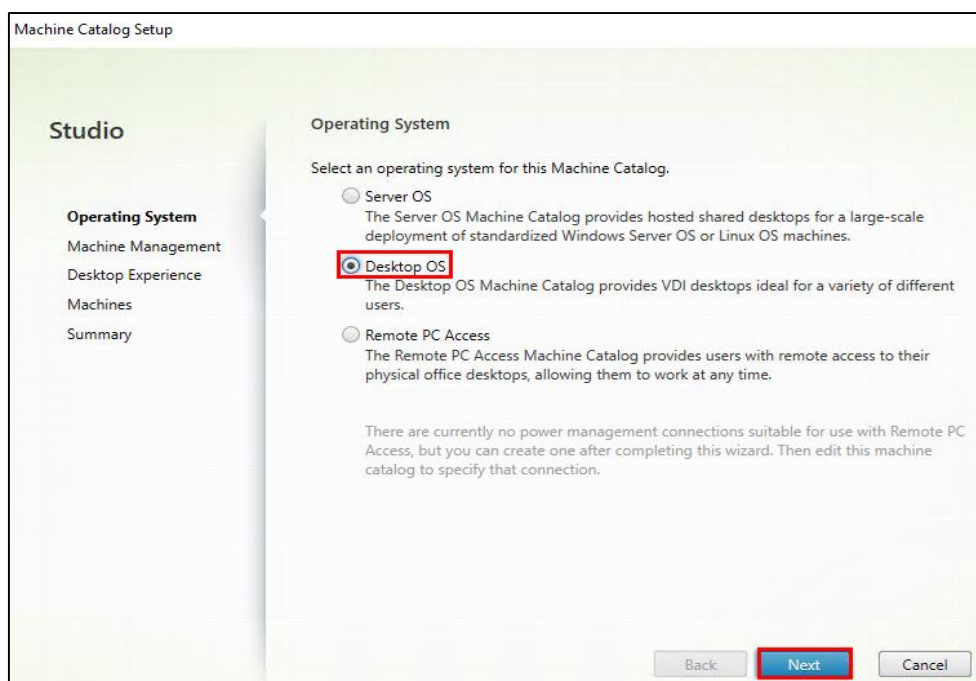




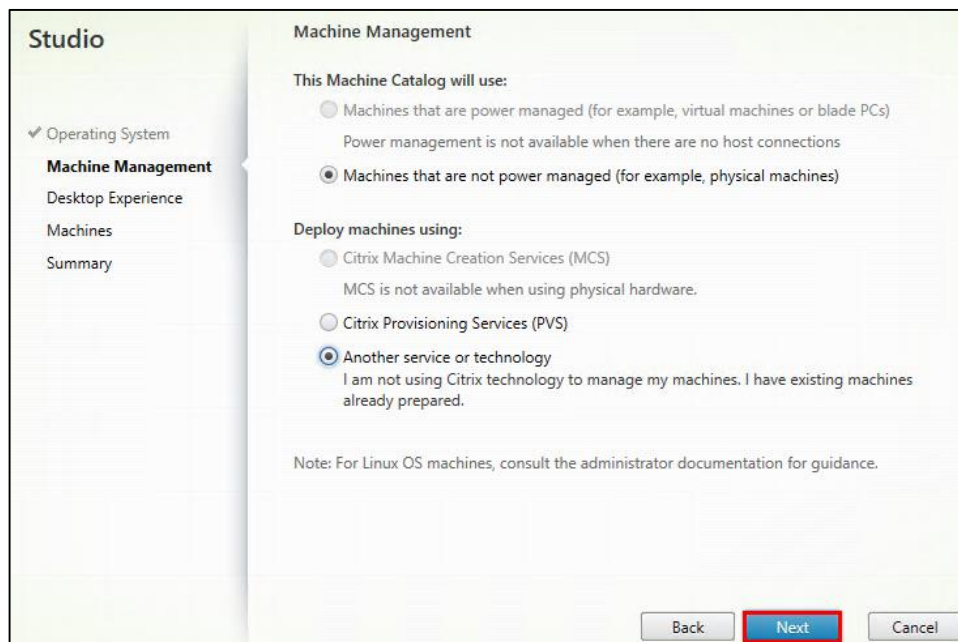
Paso 26: Crear un nuevo catálogo de máquina (Machine Catalogs) del tipo Desktop OS. Para ello, dar click derecho en la opción “**Machine Catalogs**” y elegir “**Create Machine Catalog**”.



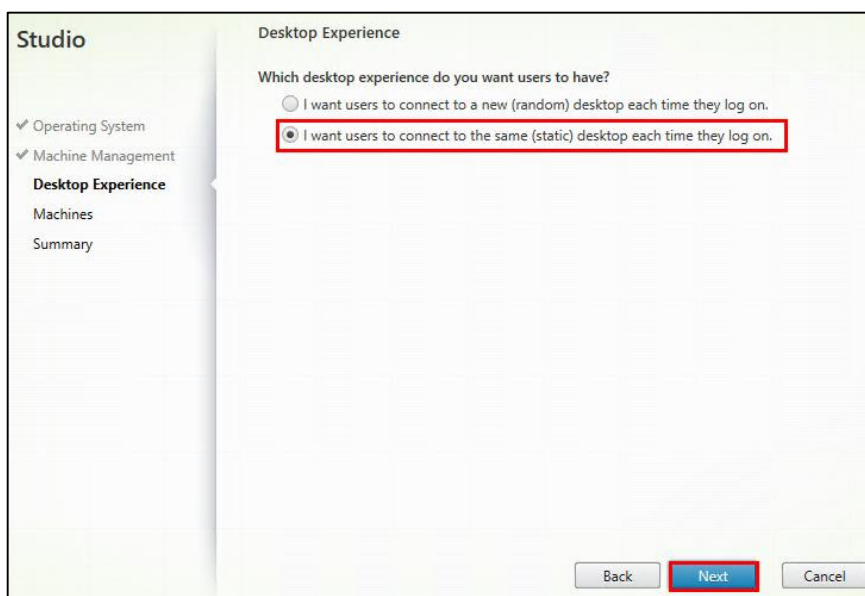
Paso 27: Seleccionar la opción “Desktop OS” y dar click en “Next”.



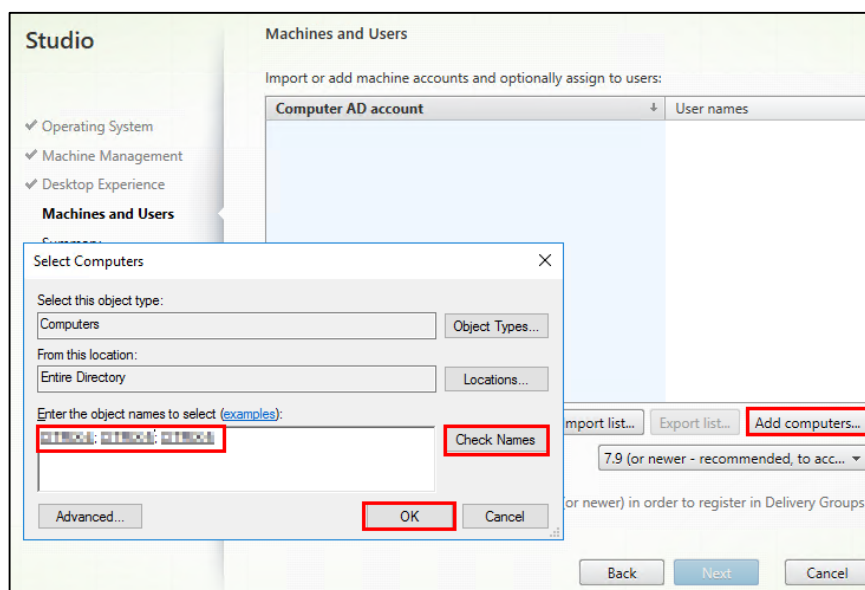
Paso 28: Seleccionar las opciones mostradas en la siguiente imagen y dar click en “Next”.



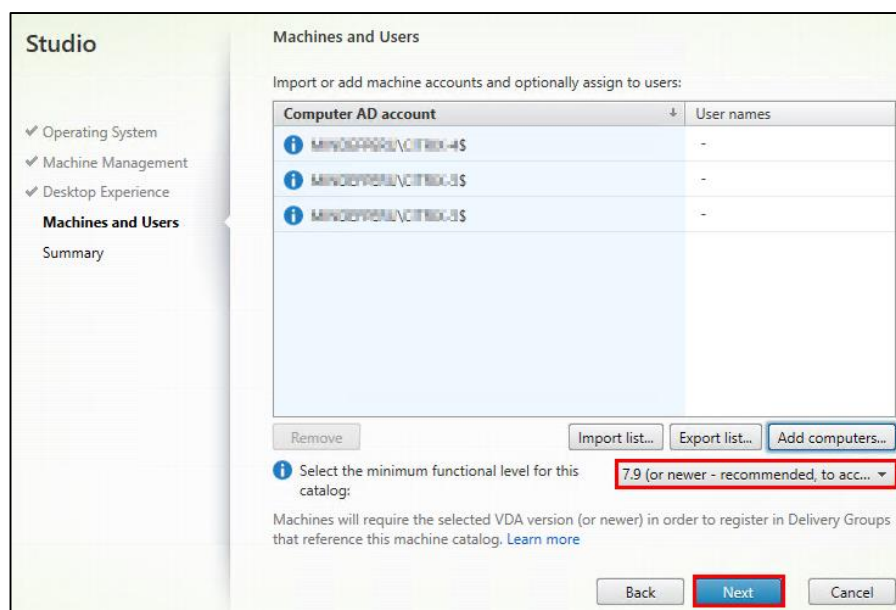
Paso 29: Seleccionar la opción para que los usuarios se conecten al mismo escritorio que tengan asignado. Dar click en “**Next**”.



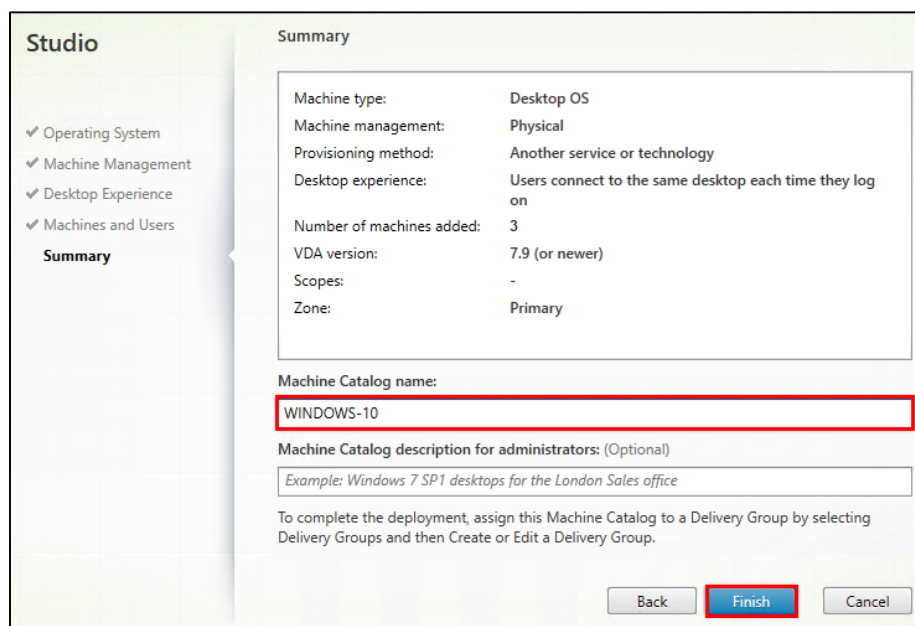
Paso 30: Seleccionar la opción “**Add computers...**”, luego ingresar y validar los nombres de los escritorios. Dar click en “**OK**”.



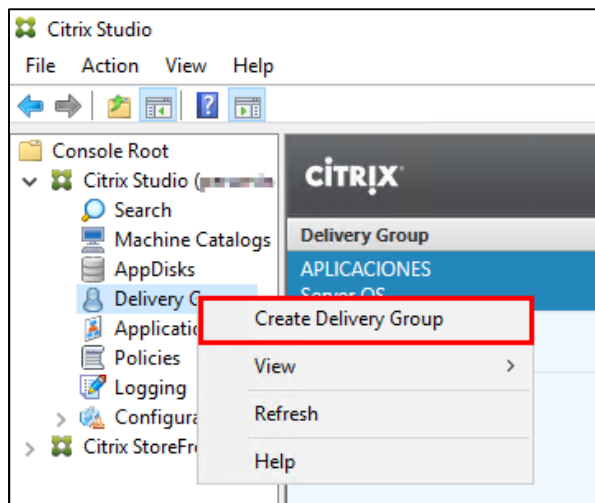
Paso 31: Seleccionar la versión de VDA recomendada y dar click en “Next”.



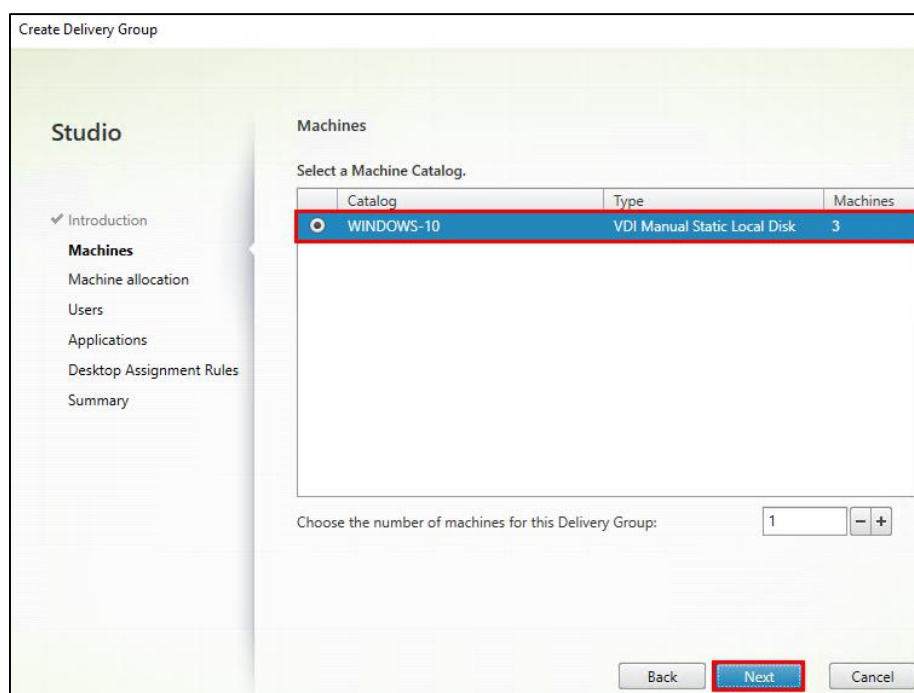
Paso 32: Verificar los datos, colocar un nombre al catálogo de máquina del tipo Desktop OS y dar click en “Finish”.



Paso 33: Crear un nuevo grupo de entrega (Delivery Groups) para los escritorios. Para ello, dar click derecho en la opción “**Delivery Groups**” y elegir “**Create Delivery Group**”.



Paso 34: Seleccionar el catálogo de máquina del tipo Server OS creado (relacionado al servidor de aplicaciones) y dar click en “**Next**”.



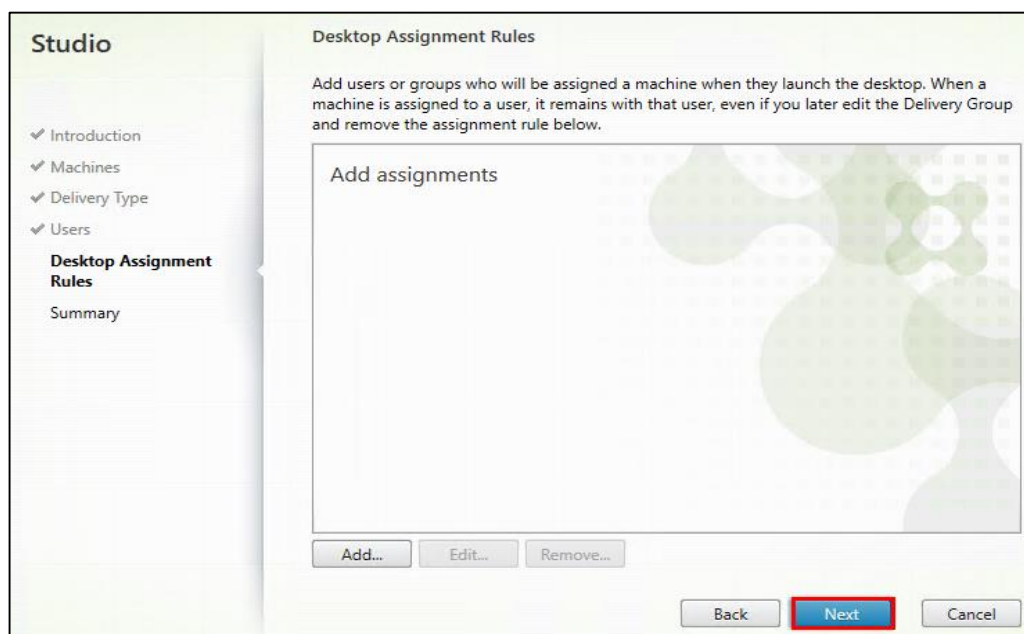
Paso 35: En este caso, como se trata de escritorios virtuales, seleccionar la opción “Desktops” y dar click en “Next”.

The screenshot shows the 'Studio' application window with the 'Delivery Type' configuration pane. On the left sidebar, the navigation menu includes 'Introduction', 'Machines', 'Delivery Type' (selected), 'Users', 'Desktop Assignment Rules', and 'Summary'. The 'Delivery Type' pane contains the following text: 'You can use the machines in the Catalog to deliver desktops or applications to your users. Use the machines to deliver:'. Below this, there are two radio button options: 'Desktops' (which is selected and highlighted with a red rectangle) and 'Applications'. A note below the options states: 'Note: For Linux OS machines, consult the administrator documentation for guidance.' At the bottom right of the pane, there are three buttons: 'Back', 'Next' (highlighted with a red rectangle), and 'Cancel'.

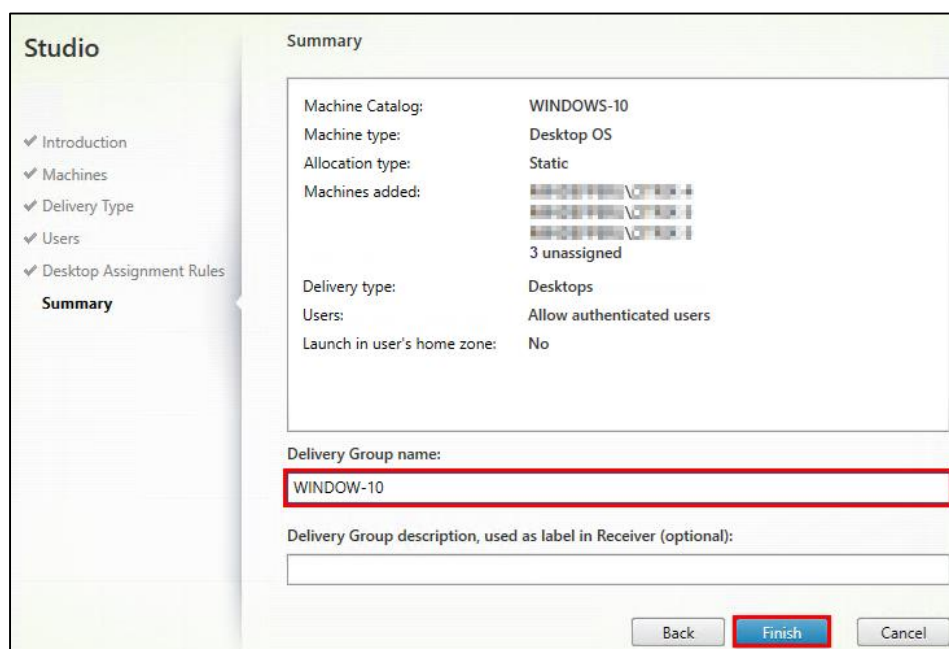
Paso 36: Al igual que en el caso de las aplicaciones virtuales, permitir el acceso a todos los usuarios autenticados. Dar click en “Next”.

The screenshot shows the 'Studio' application window with the 'Users' configuration pane. On the left sidebar, the navigation menu includes 'Introduction', 'Machines', 'Delivery Type', 'Users' (selected), 'Desktop Assignment Rules', and 'Summary'. The 'Users' pane contains the following text: 'Specify who can use the applications and desktops in this Delivery Group. You can assign users and user groups who log on with valid credentials.' Below this, there are two radio button options: 'Allow any authenticated users to use this Delivery Group.' (which is selected and highlighted with a red rectangle) and 'Restrict use of this Delivery Group to the following users:'. Below the options is a large text box labeled 'Add users and groups'. At the bottom left of the pane, there are two buttons: 'Add...' and 'Remove'. At the bottom right of the pane, there are three buttons: 'Back', 'Next' (highlighted with a red rectangle), and 'Cancel'.

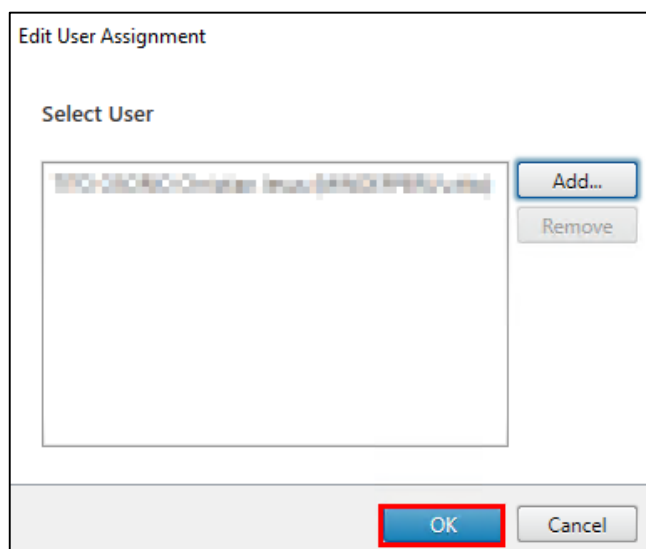
Paso 37: No agregar ninguna regla de asignación de escritorio en esta opción. Dar click en “Next”.



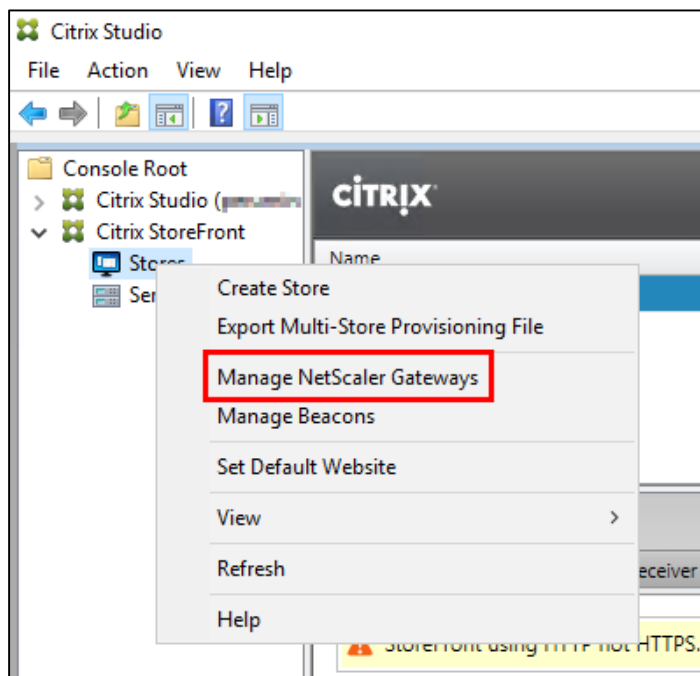
Paso 38: Verificar las configuraciones, asignar un nombre al Delivery Group y dar click en “Finish”.



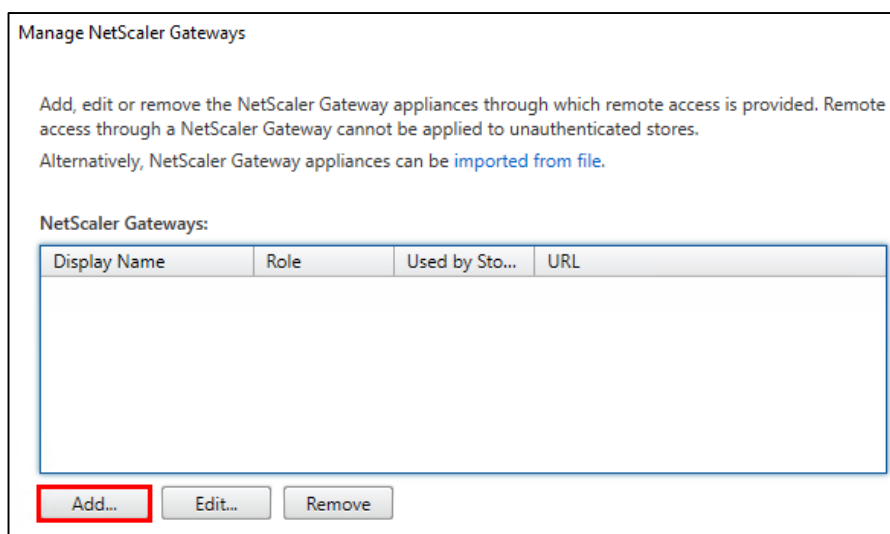
Paso 42: Selección la opción “OK” para guardar y aplicar los cambios realizados (asignación de escritorio virtual a usuario final).



Paso 43: Crear un nuevo NetScaler Gateway. Para ello, en la sección “Citrix StoreFront”, dar click derecho en la opción “Stores” y elegir “Manage NetScaler Gateways”.



Paso 44: Seleccionar la opción “Add...” para agregar un nuevo NetScaler Gateway.



Manage NetScaler Gateways

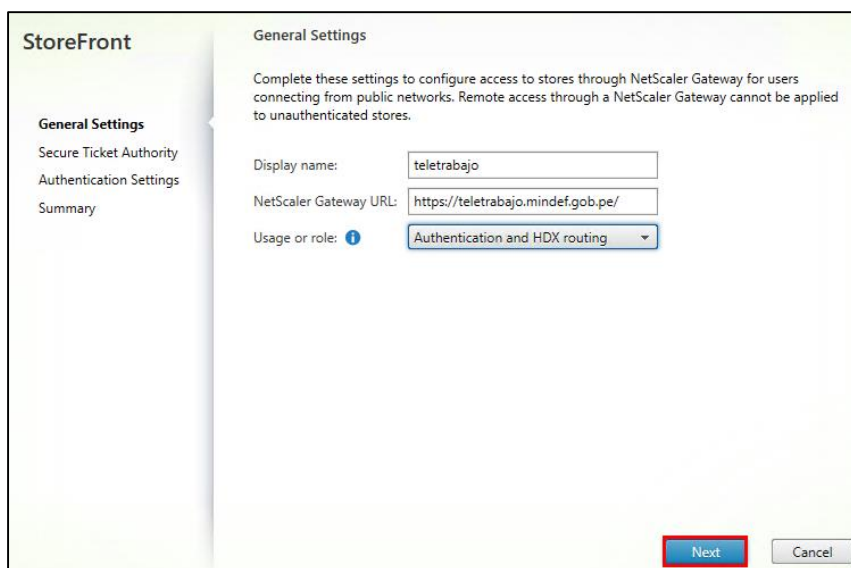
Add, edit or remove the NetScaler Gateway appliances through which remote access is provided. Remote access through a NetScaler Gateway cannot be applied to unauthenticated stores. Alternatively, NetScaler Gateway appliances can be imported from file.

NetScaler Gateways:

Display Name	Role	Used by Sto...	URL
--------------	------	----------------	-----

Add... Edit... Remove

Paso 45: Ingresar un nombre de identificación, la URL para la conexión externa de los usuarios y seleccionar el role que se muestra en la siguiente imagen. Dar click en “Next”.



StoreFront

General Settings

Complete these settings to configure access to stores through NetScaler Gateway for users connecting from public networks. Remote access through a NetScaler Gateway cannot be applied to unauthenticated stores.

Display name: teletrabajo

NetScaler Gateway URL: https://teletrabajo.mindef.gob.pe/

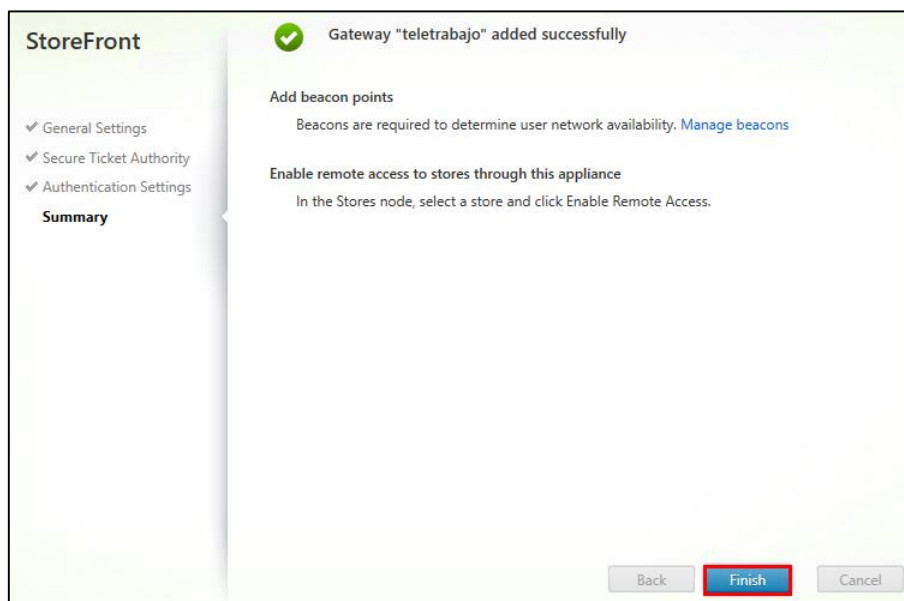
Usage or role: Authentication and HDX routing

Next Cancel

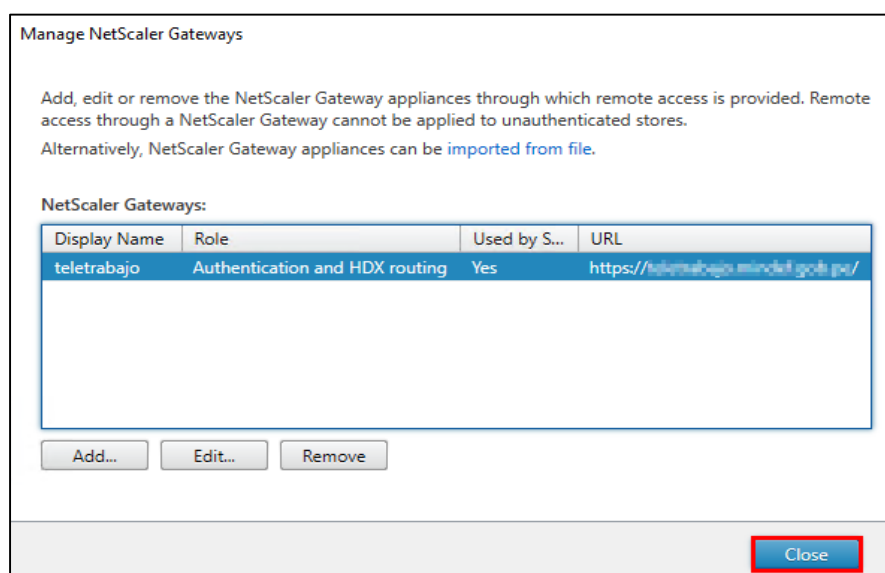
Paso 46: Seleccionar la opción “Add...” para agregar el enlace del STA (http://IP_servidor_DC). Dar click en “Next”.

Paso 47: Mantener los siguientes parámetros por defecto y dar click en “Create”.

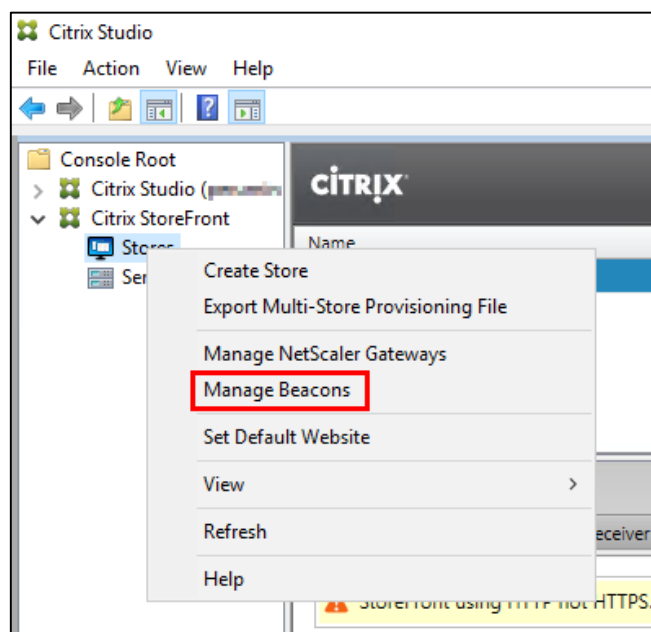
Paso 48: Culminar el proceso seleccionando la opción “Finish”.



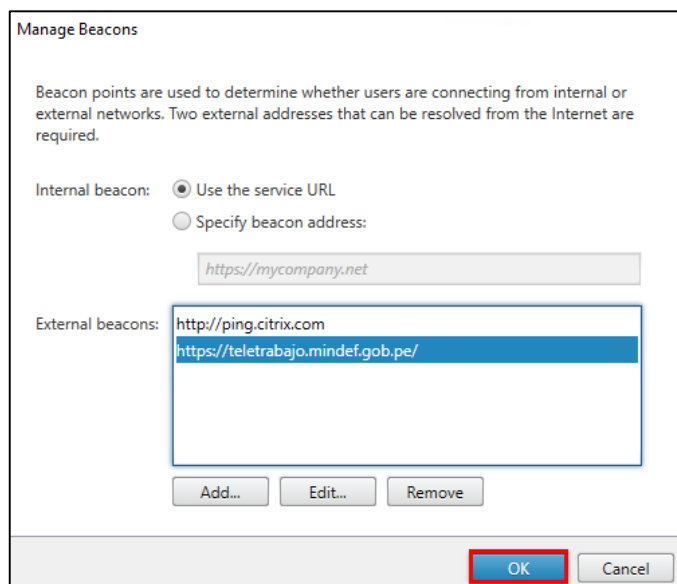
Paso 49: Cerrar la ventana de gestión de NetScaler Gateways, dando click en “Close”.



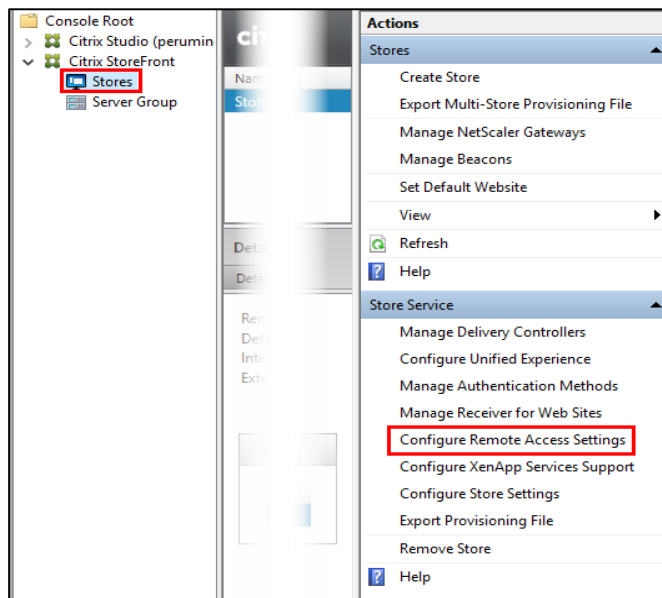
Paso 50: En la sección “Citrix StoreFront”, dar click derecho en la opción “Stores” y elegir “Manage Beacons”.



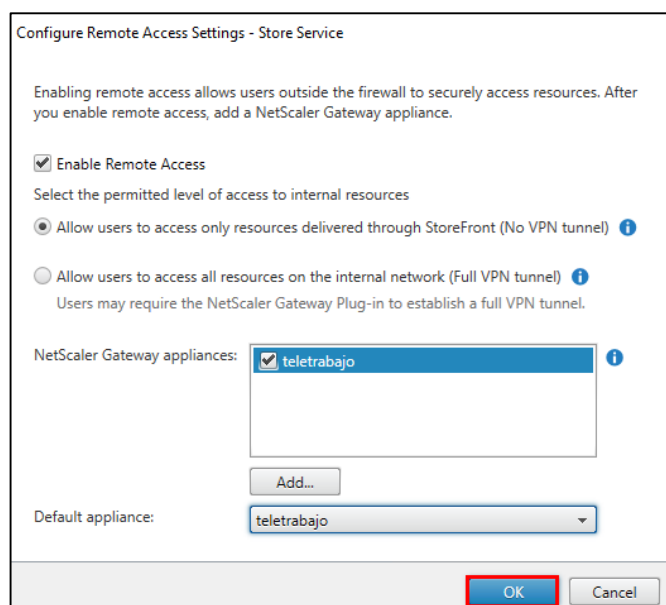
Paso 51: En la sección “Internal beacon”, mantener la configuración “Use the service URL”. En la sección “External beacons”, agregar las dos URLs que se muestran en la siguiente imagen. Dar click en “OK”.



Paso 52: Por último, en la opción “**Citrix StoreFront > Stores**”, seleccionar la opción “**Configure Remote Access Settings**” (ubicado en la zona derecha, sección “**Actions > Store Service**”).

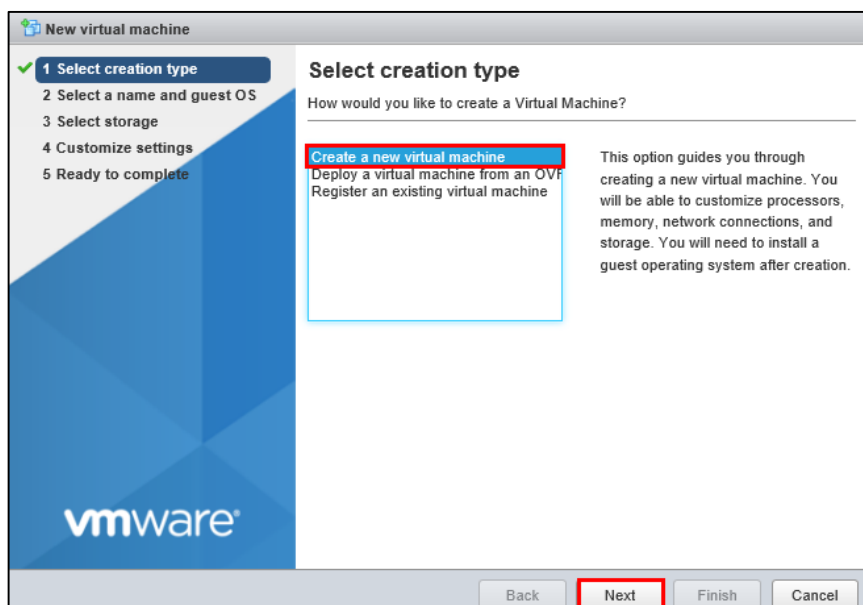


Paso 53: Finalmente, habilitar la opción de “**Remote Access**”, seleccionar la opción “**No VPN tunnel**” y el NetScaler Gateway creado previamente. Dar click en “**OK**”.

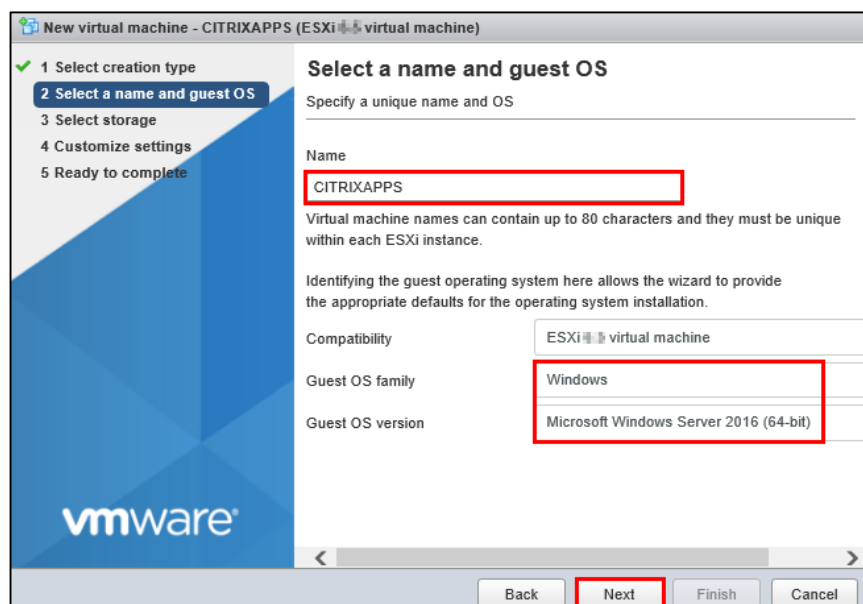


Procedimiento de instalación de Citrix applications server

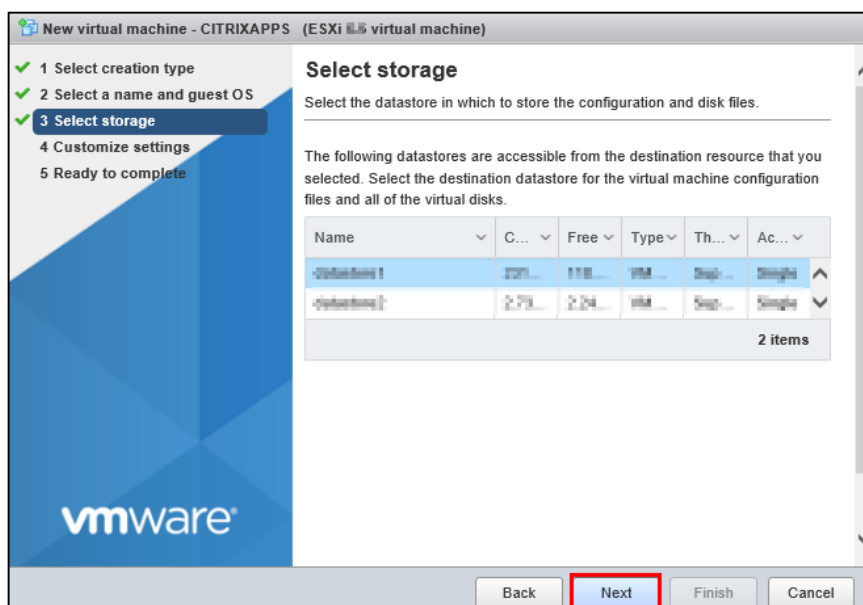
Paso 1: Crear una nueva máquina virtual con sistema operativo Microsoft Windows Server (versión 2012 o 2016 inglés), el cual albergará la plataforma Citrix Applications Server y demás componentes.



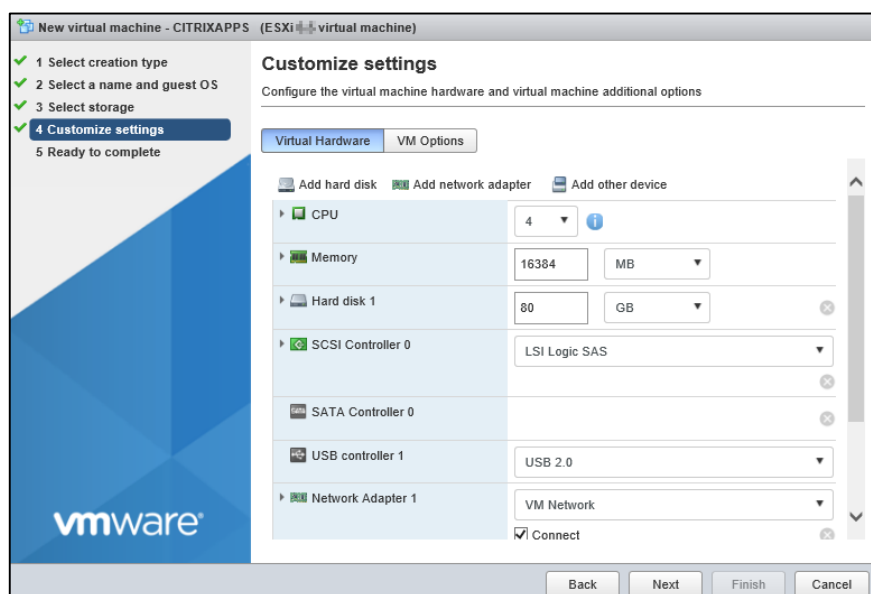
Paso 2: Ingresar un nombre para la máquina virtual, seleccionar el sistema operativo y versión correspondiente (por ejemplo, Microsoft Windows Server 2016). Dar click en “Next”.



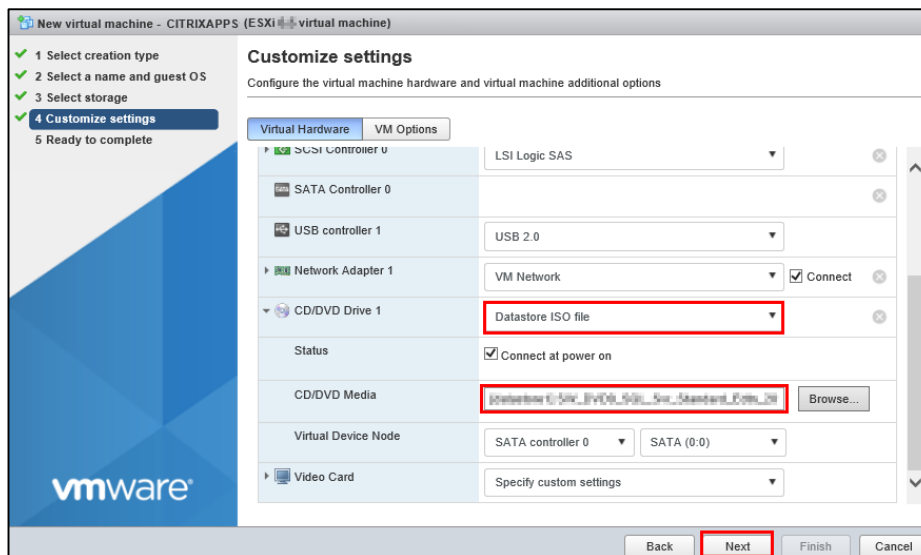
Paso 3: Seleccionar el datastore en donde se almacenará la configuración de esta máquina virtual. Dar click en “Next”.



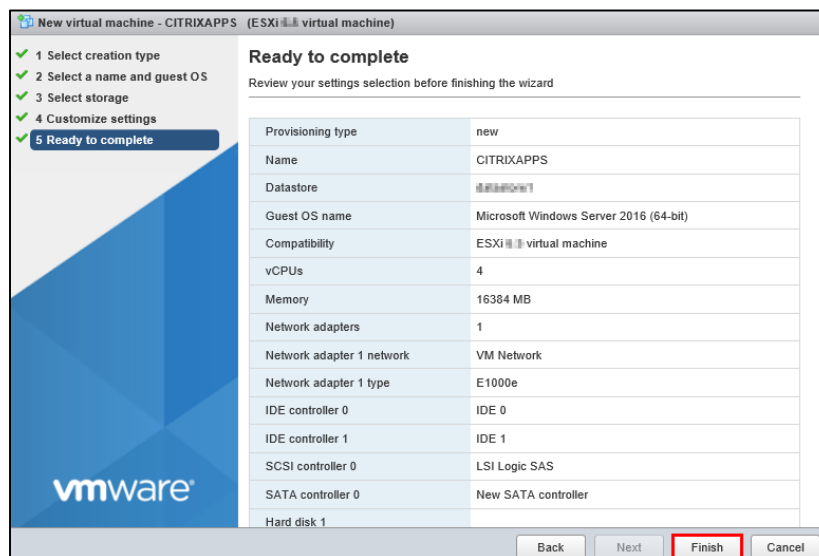
Paso 4: Ingresar los parámetros de almacenamiento y procesamiento que se asignará a esta máquina virtual.



Paso 5: En el campo “CD/DVD Drive 1”, seleccionar la opción “Datastore ISO File” (ubicar el archivo ISO del sistema operativo almacenado en el datastore) y habilitar la opción “Connect at power on”. Dar click en “Next”.



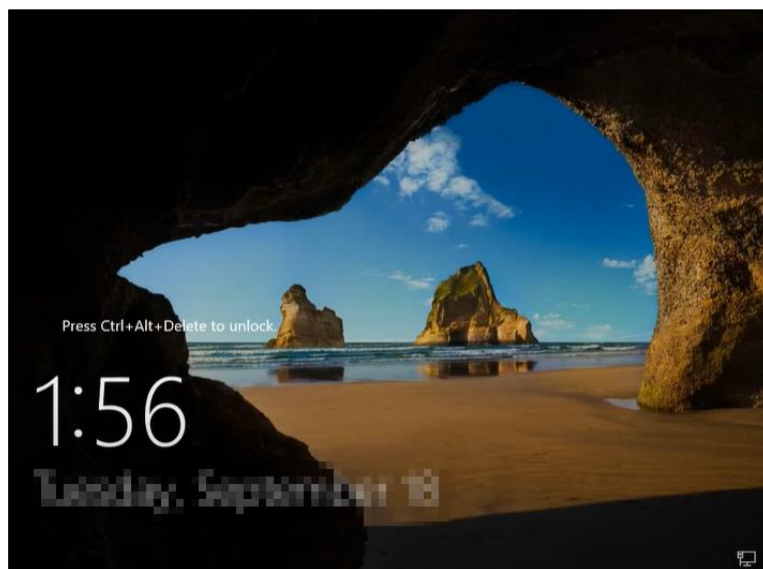
Paso 6: Seleccionar la opción “Finish” para finalizar la creación de la máquina virtual.



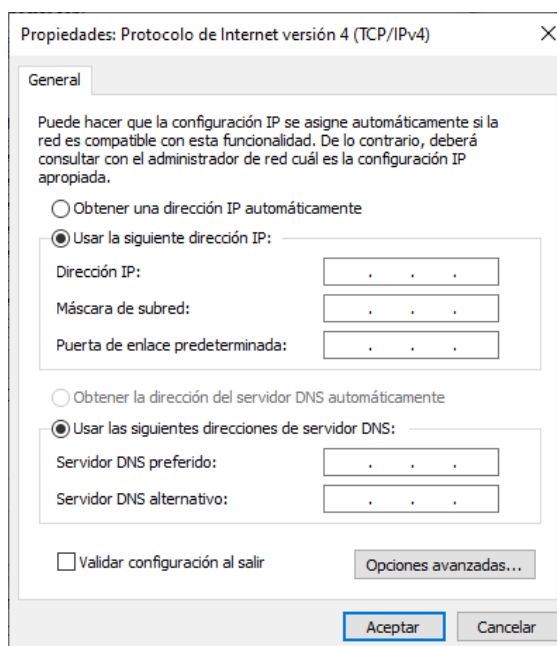
Paso 7: Encender la máquina virtual y esperar que el archivo ISO se ejecute automáticamente. Luego, proceder con la instalación correspondiente de la versión de Windows involucrada.



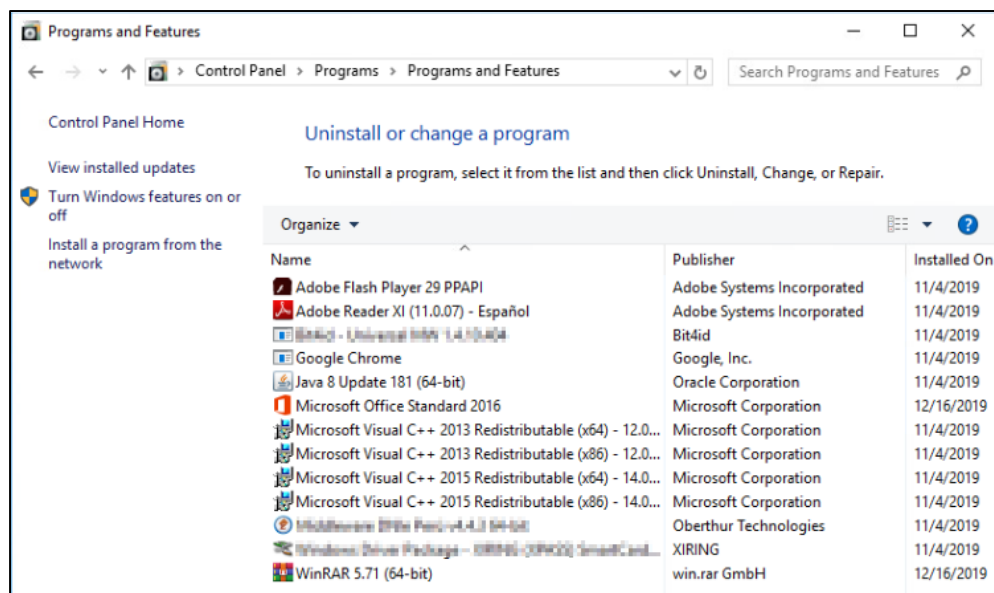
Paso 8: Luego de culminar la instalación, la máquina virtual se reiniciará y estará lista para ser utilizada.



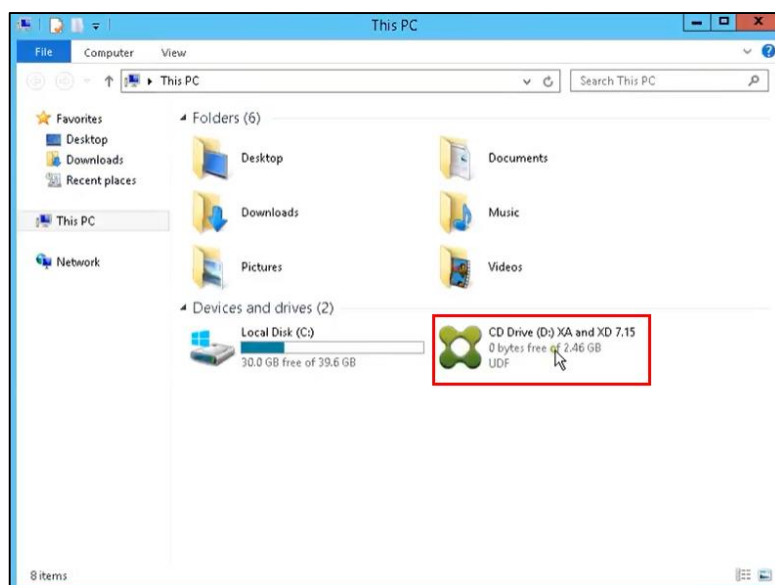
Paso 9: Ingresar el direccionamiento de red asignado a este equipo y agregarlo al dominio de la institución.



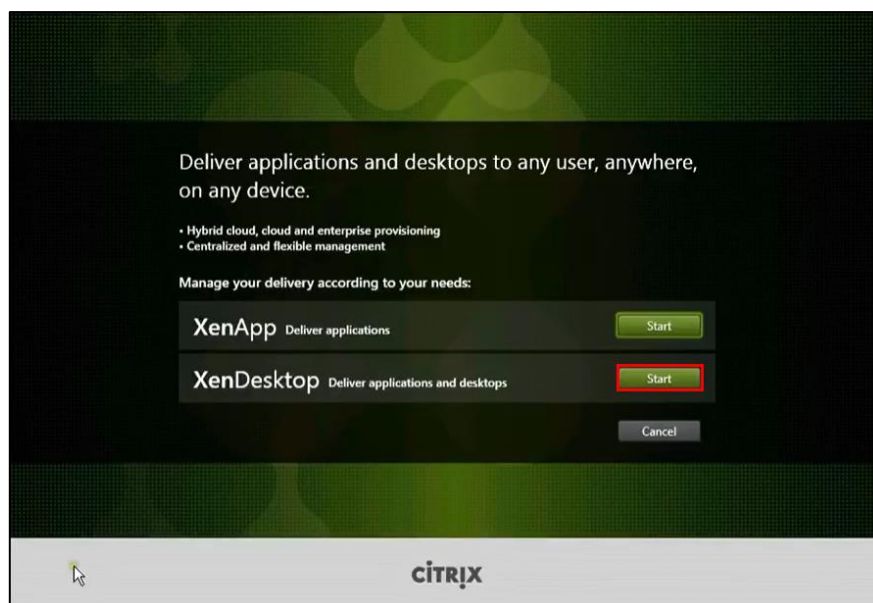
Paso 10: Instalar todas las aplicaciones que serán necesarias para la virtualización correspondiente (por ejemplo, Google Chrome, Suite de Office, entre otros).



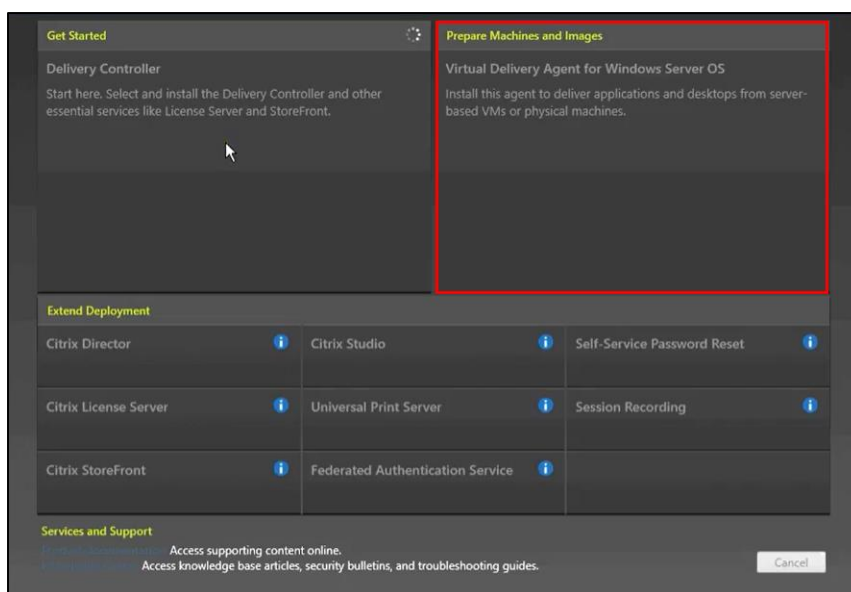
Paso 11: Ejecutar el instalador correspondiente de la plataforma Citrix.



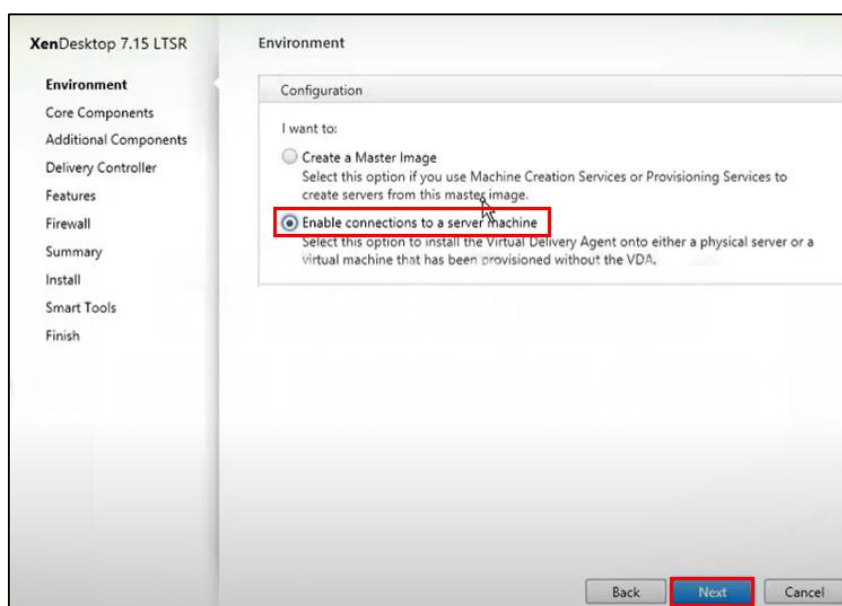
Paso 12: En primer lugar, seleccionar el botón “Start” en la opción “XenDesktop”, debido a que se realizará la virtualización de aplicaciones y escritorios.



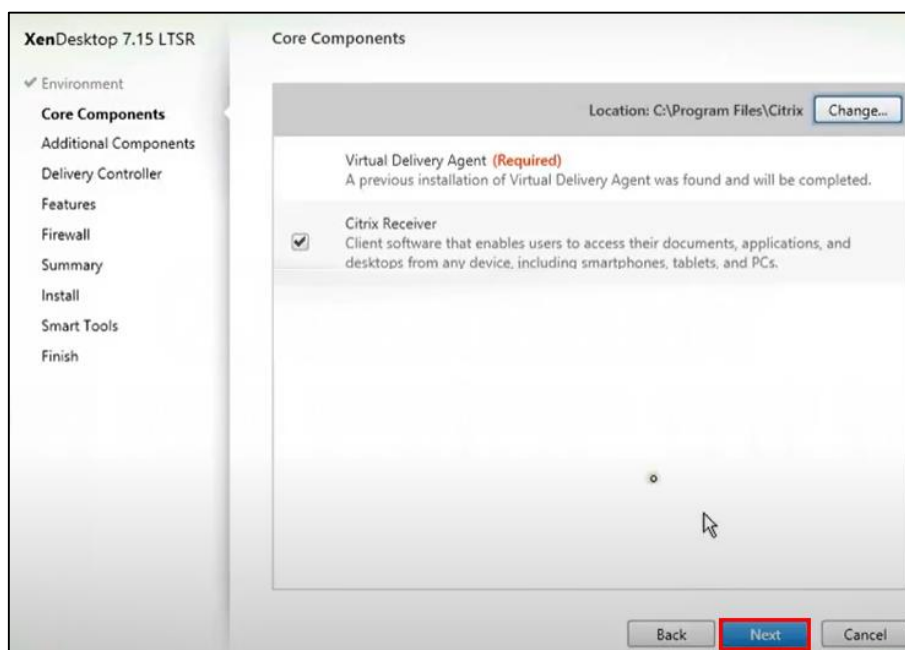
Paso 13: Seleccionar la opción **“Virtual Delivery Agent for Windows Server OS”**.



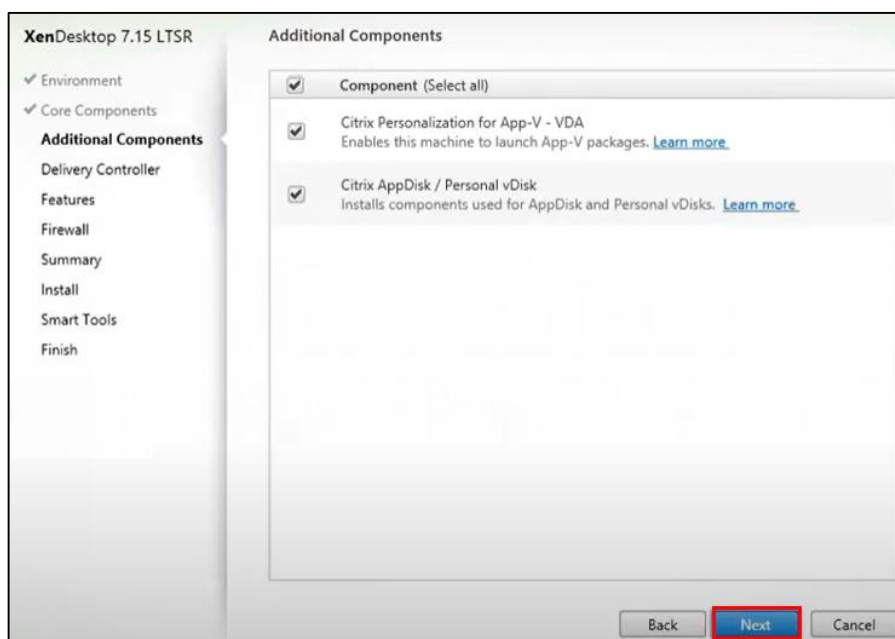
Paso 14: Seleccionar la opción **“Enable connections to a server machine”** y dar click en **“Next”**.



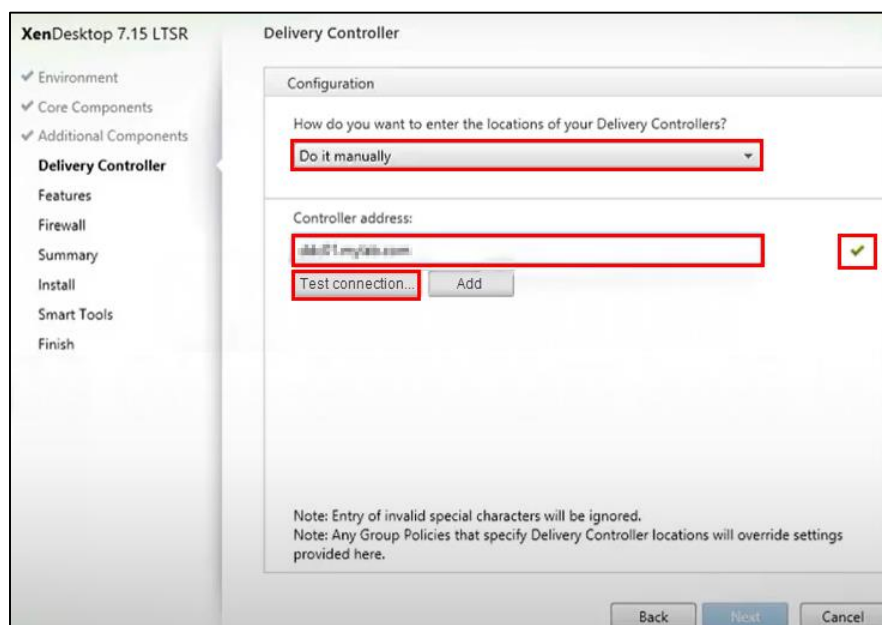
Paso 15: Mantener las opciones por defecto, con la opción de “Citrix Receiver” habilitada, y dar click en “Next”.



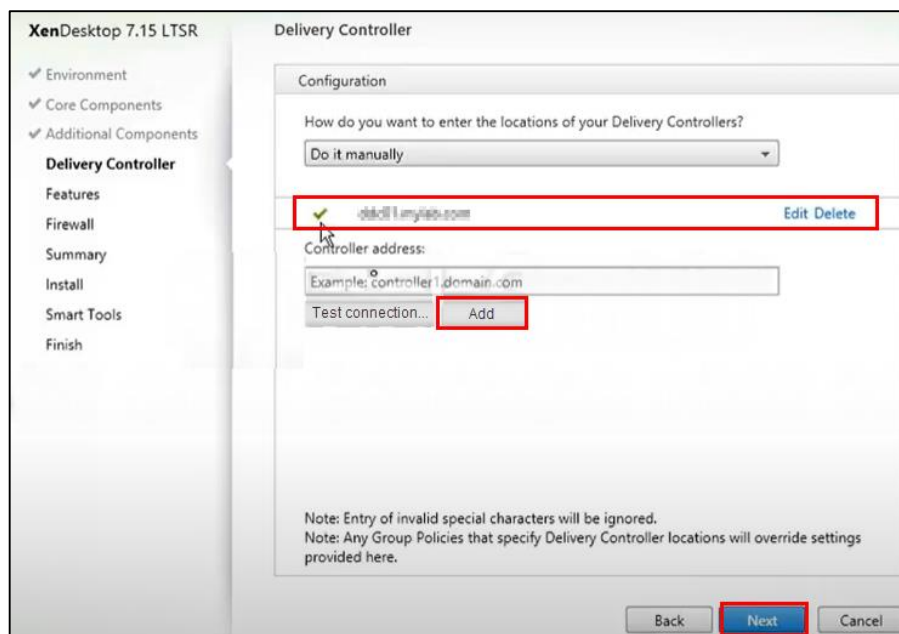
Paso 16: Seleccionar todos los componentes adicionales y dar click en “Next”.



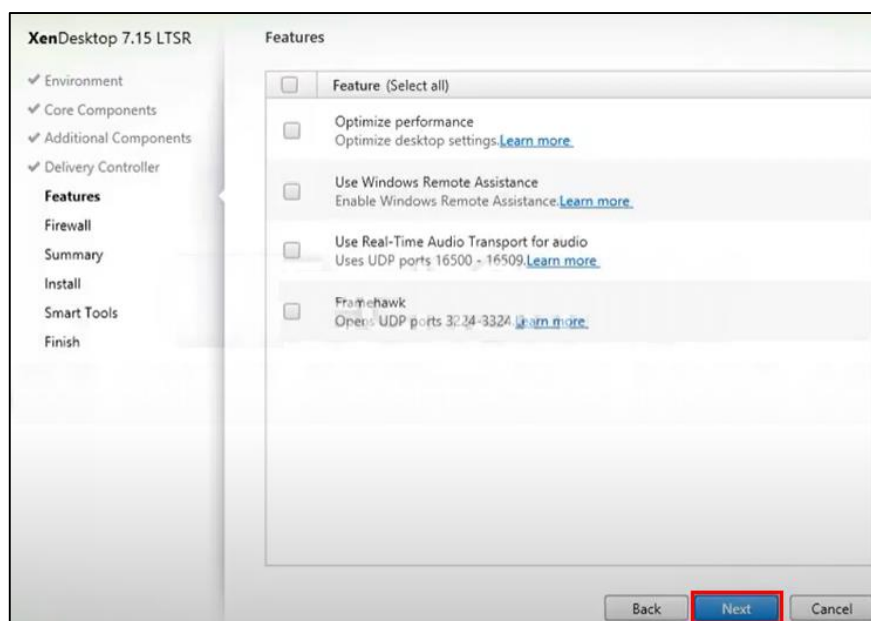
Paso 17: Seleccionar la opción de configuración manual, ingresar el hostname del Delivery Controller y dar click en “**Test connection**” para validar la comunicación.



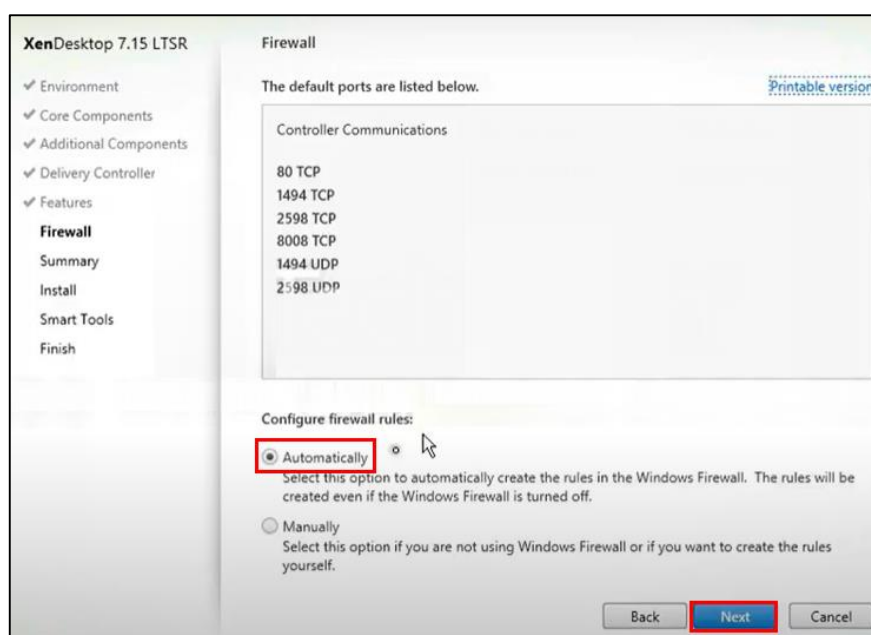
Paso 18: Seleccionar la opción “Add” y dar clic en “Next”.



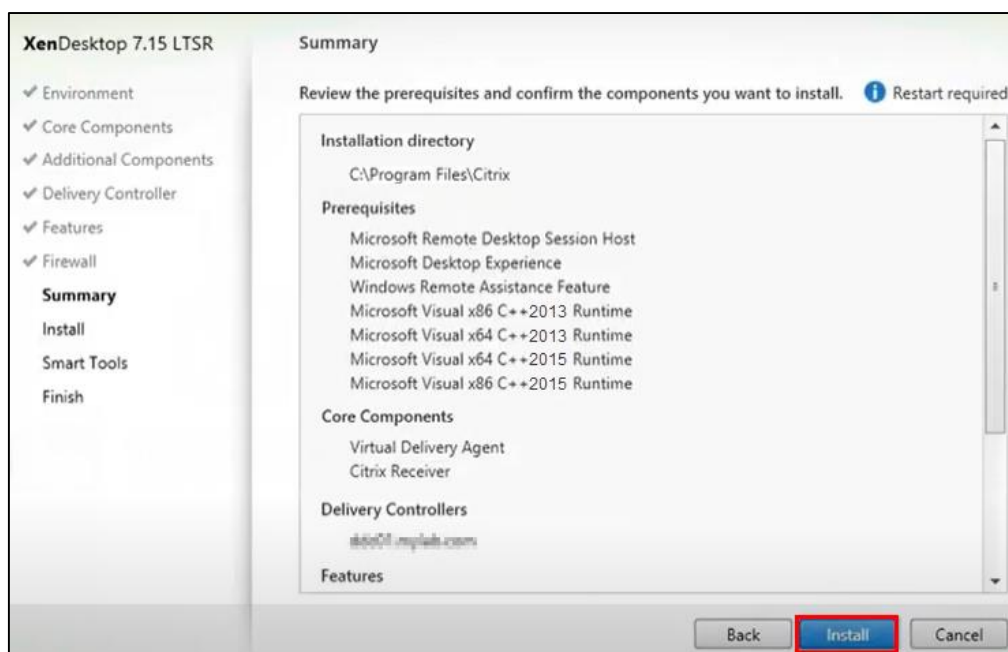
Paso 19: Seleccionar todas las características que se habilitarán. Dar click en “Next”.



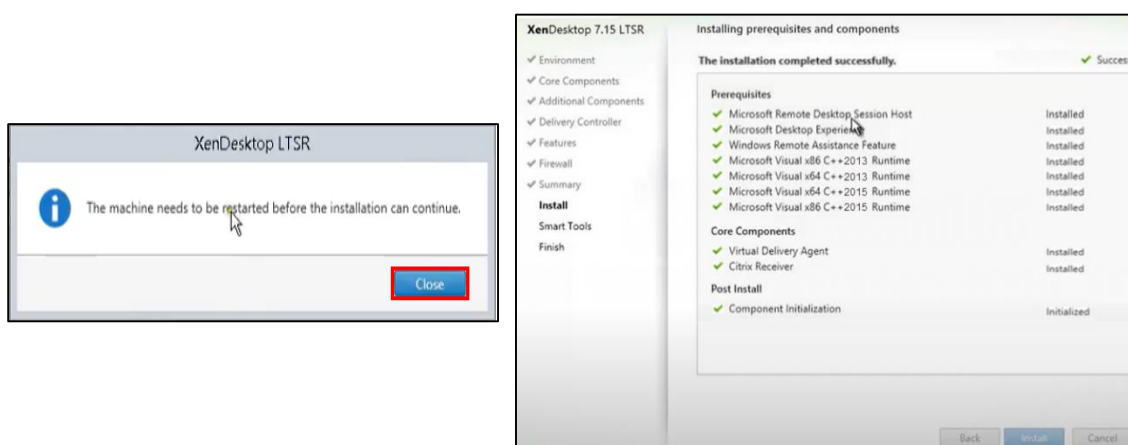
Paso 20: Seleccionar la opción de configuración automática y dar click en “Next”.



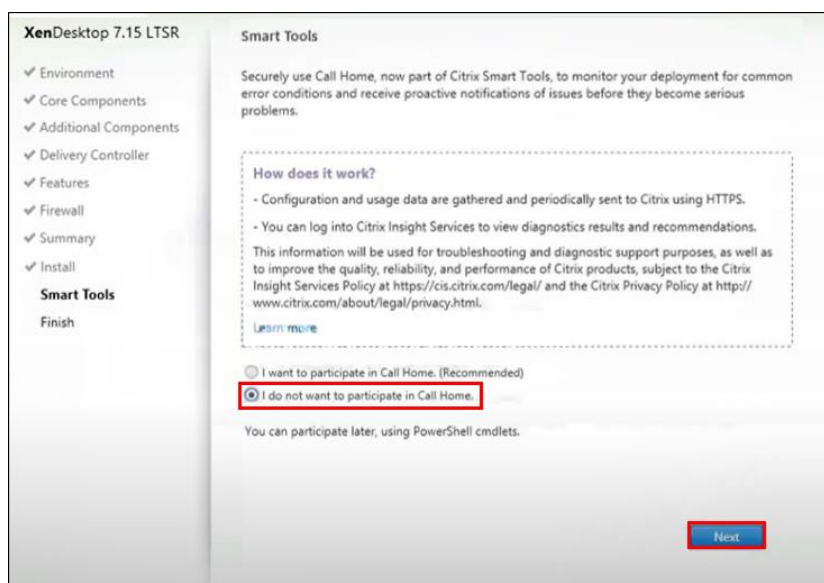
Paso 21: Iniciar al proceso de instalación dando click en “**Install**”.



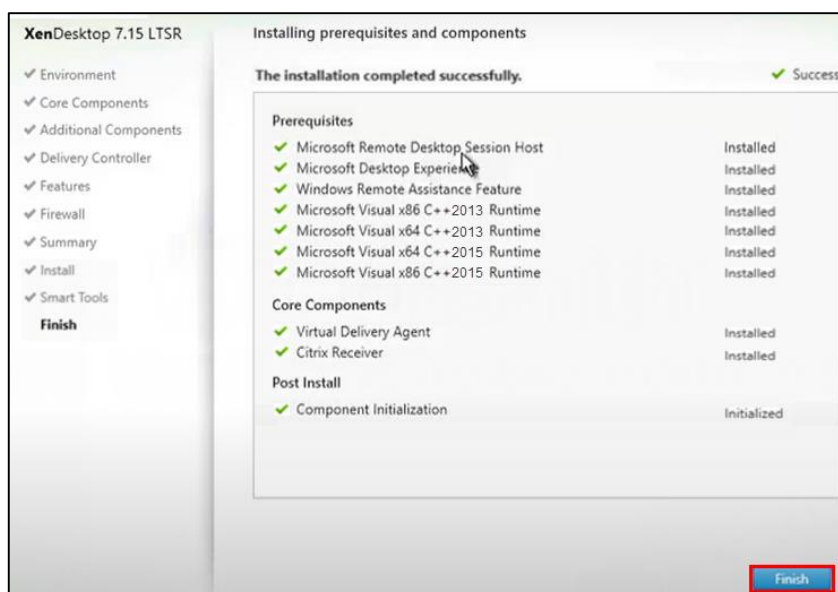
Paso 22: Durante el proceso de instalación se solicitará el reinicio de la máquina virtual para luego continuar (botón “**Close**” para proceder con el reinicio).



Paso 23: Elegir la casilla para no conectar con Smart Tools (Call Home) y seleccionar el botón “Next”.

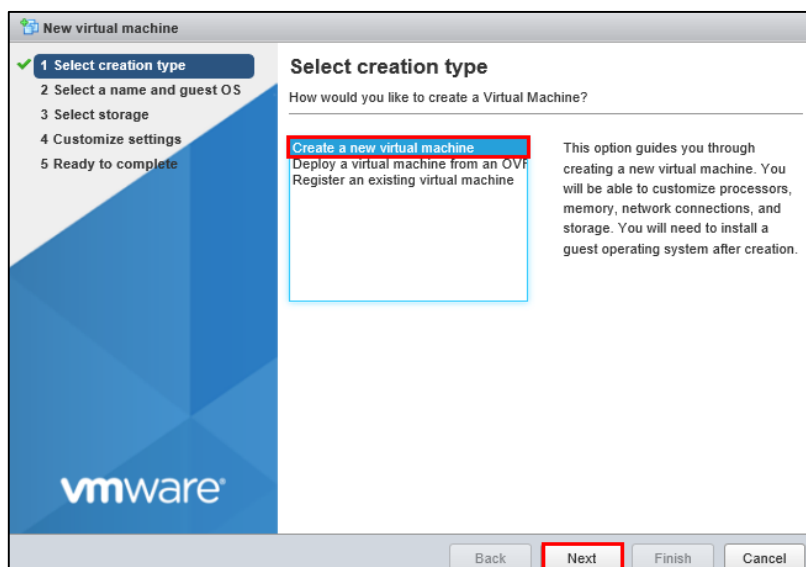


Paso 24: Finalizar el proceso de instalación, seleccionando la opción “Finish”.

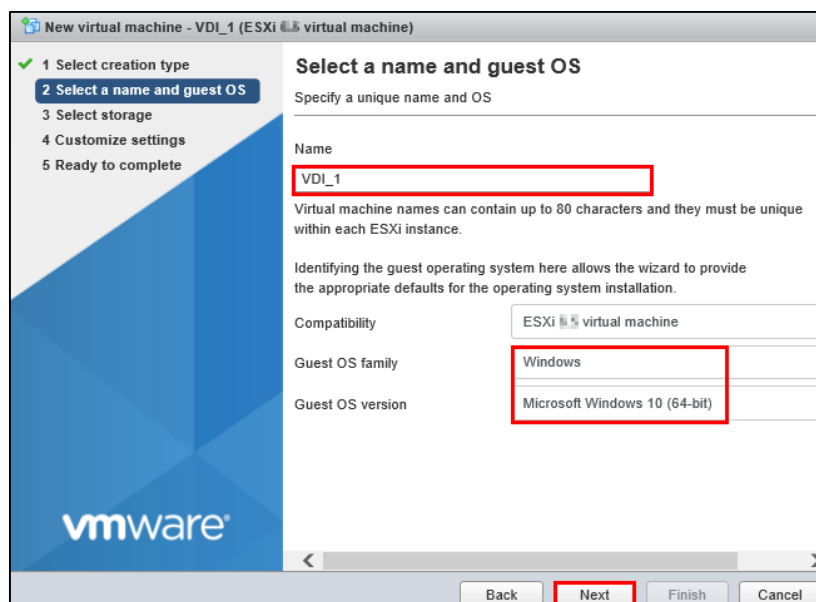


Procedimiento de instalación de virtual desktop infrastructure (VDI)

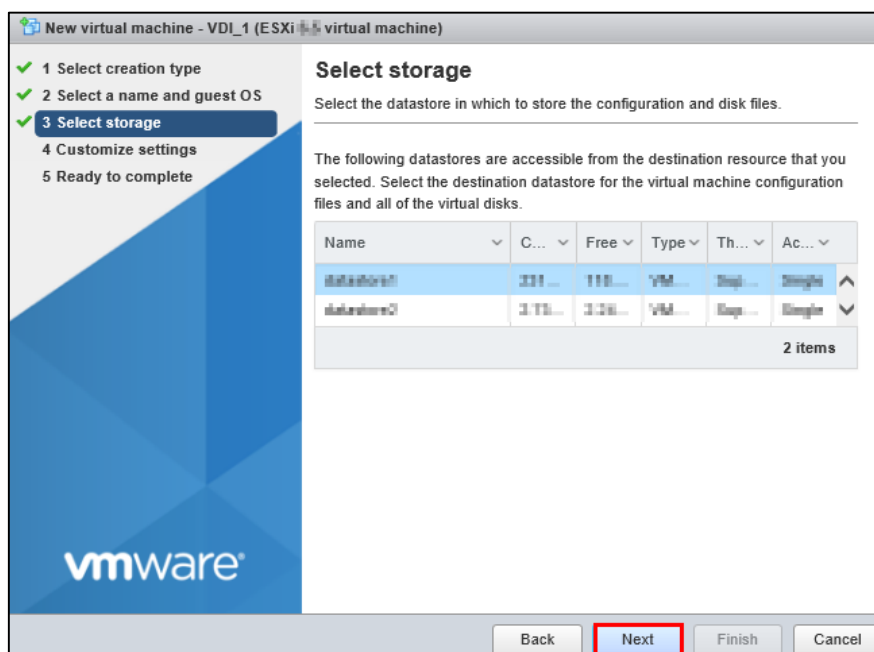
Paso 1: Crear una nueva máquina virtual con sistema operativo Microsoft Windows (versión 7 o 10), el cual albergará la plataforma Citrix Virtual Desktop Infrastructure (VDI) y demás componentes.



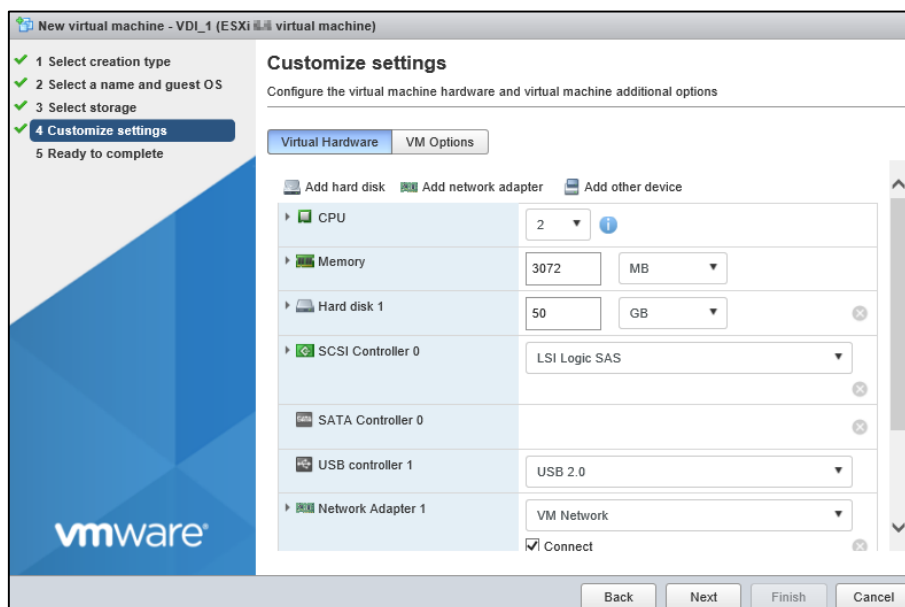
Paso 2: Ingresar un nombre para la máquina virtual, seleccionar el sistema operativo y versión correspondiente (por ejemplo, Microsoft Windows 10). Dar click en “Next”.



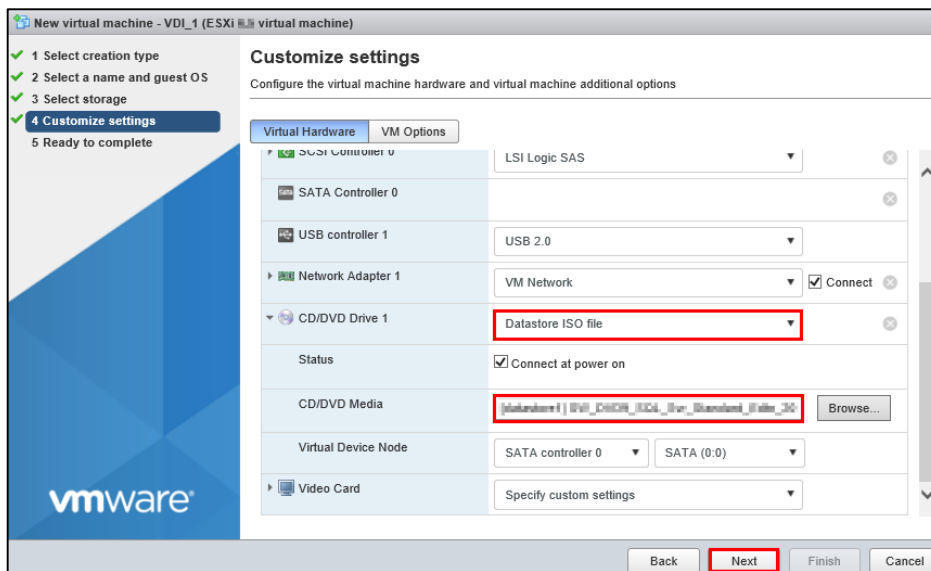
Paso 3: Seleccionar el datastore en donde se almacenará la configuración de esta máquina virtual. Dar click en “Next”.



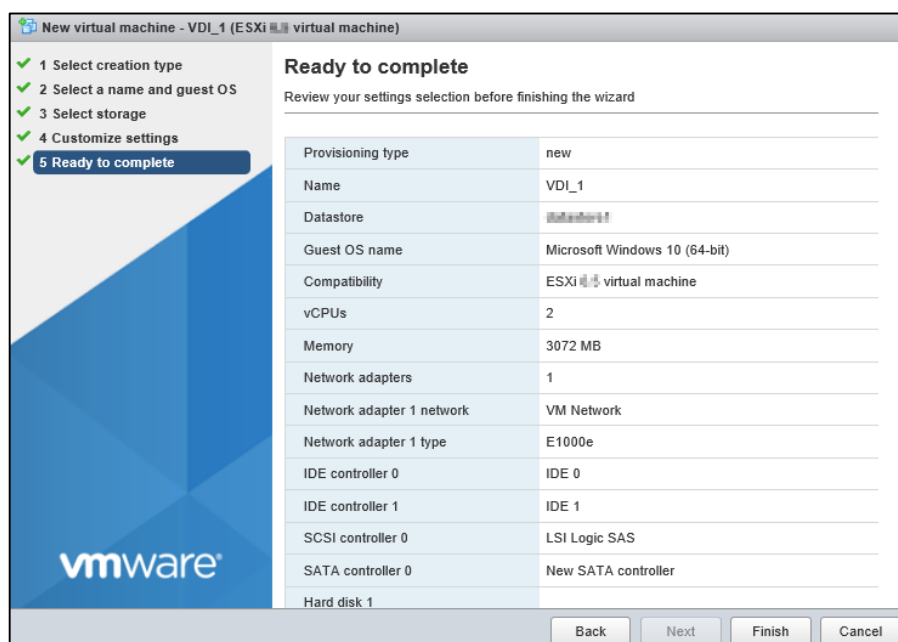
Paso 4: Ingresar los parámetros de almacenamiento y procesamiento que se asignará a esta máquina virtual. Dar click en “Next”.



Paso 5: En el campo “CD/DVD Drive 1”, seleccionar la opción “Datastore ISO File” (ubicar el archivo ISO del sistema operativo almacenado en el datastore) y habilitar la opción “Connect at power on”. Dar click en “Next”.



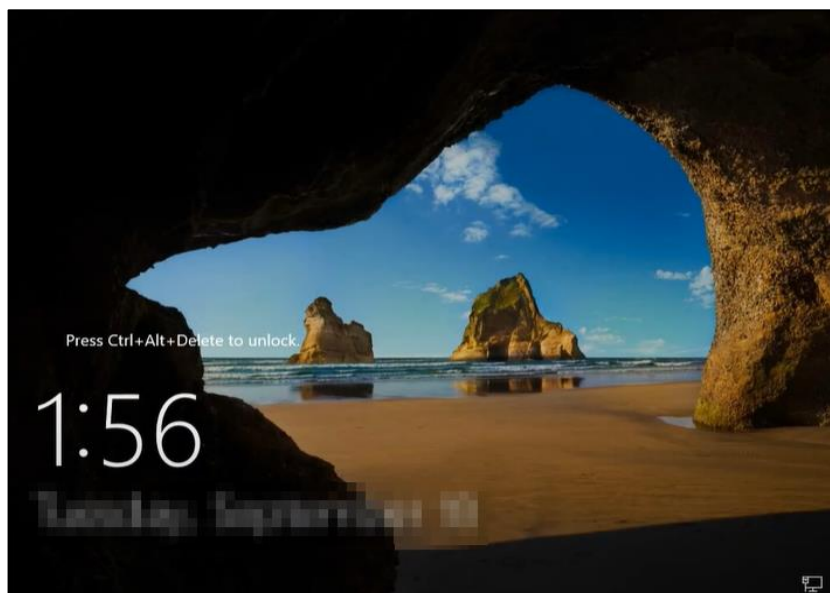
Paso 6: Seleccionar la opción “Finish” para finalizar la creación de la máquina virtual.



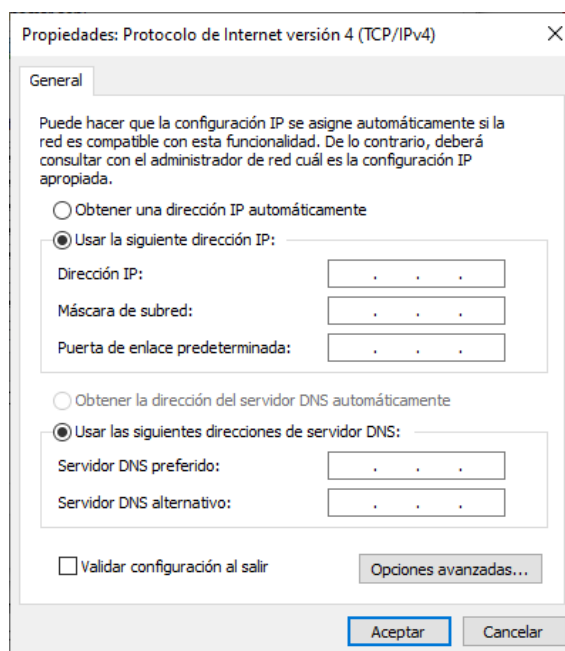
Paso 7: Encender la máquina virtual y esperar que el archivo ISO se ejecute automáticamente. Luego, proceder con la instalación correspondiente de la versión de Windows involucrada.



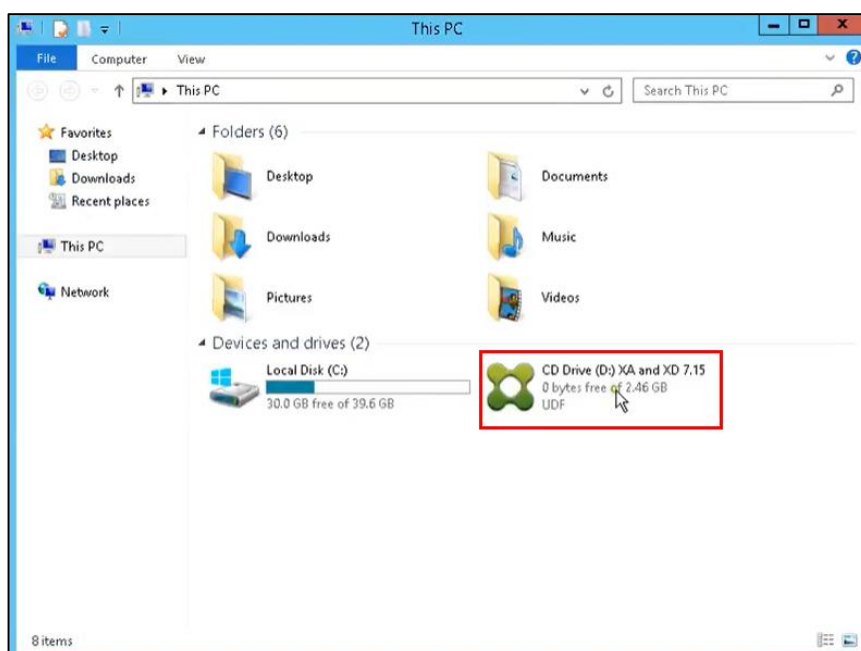
Paso 8: Luego de culminar la instalación, la máquina virtual se reiniciará y estará lista para ser utilizada.



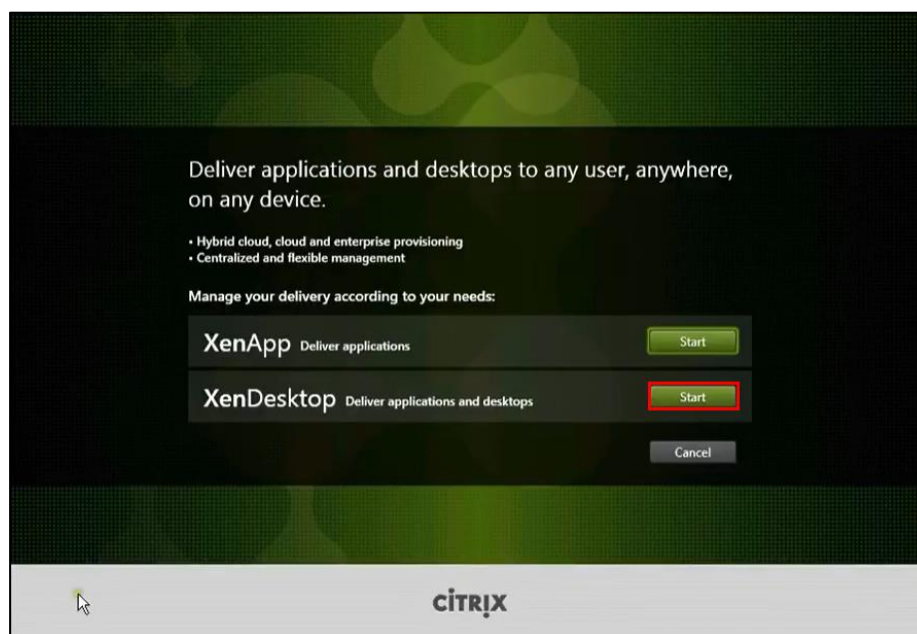
Paso 9: Ingresar el direccionamiento de red asignado a este equipo y agregarlo al dominio de la institución.



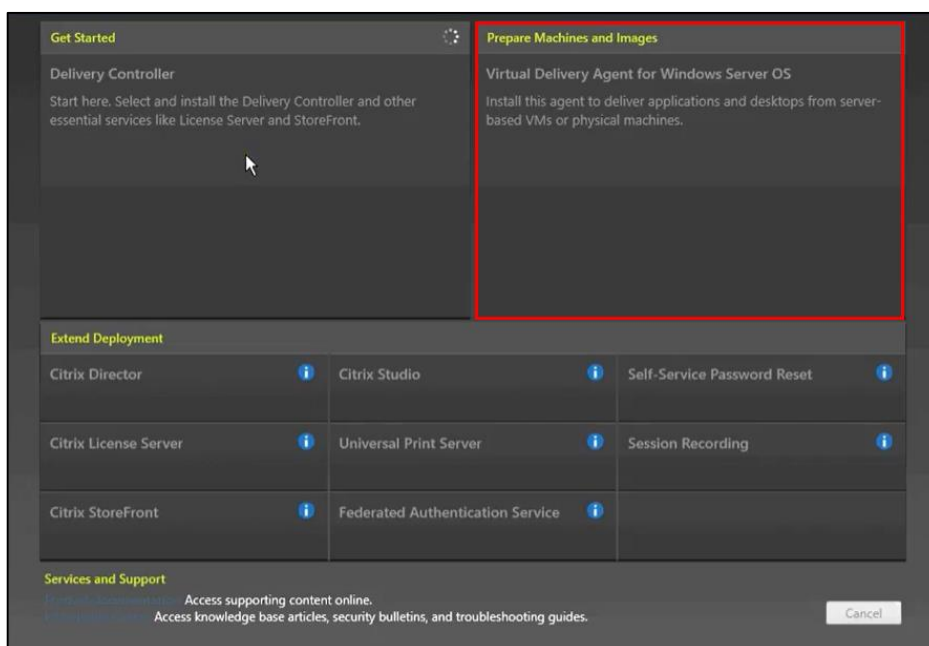
Paso 10: Ejecutar el instalador correspondiente de la plataforma Citrix.



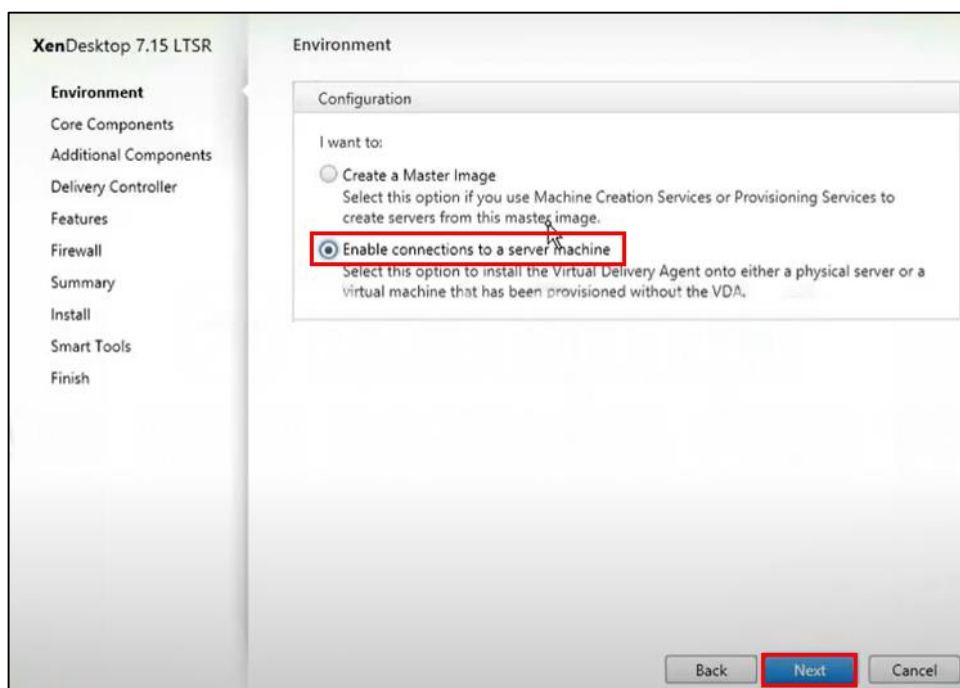
Paso 11: En primer lugar, seleccionar el botón “**Start**” en la opción “**XenDesktop**”, debido a que se realizará la virtualización de aplicaciones y escritorios.



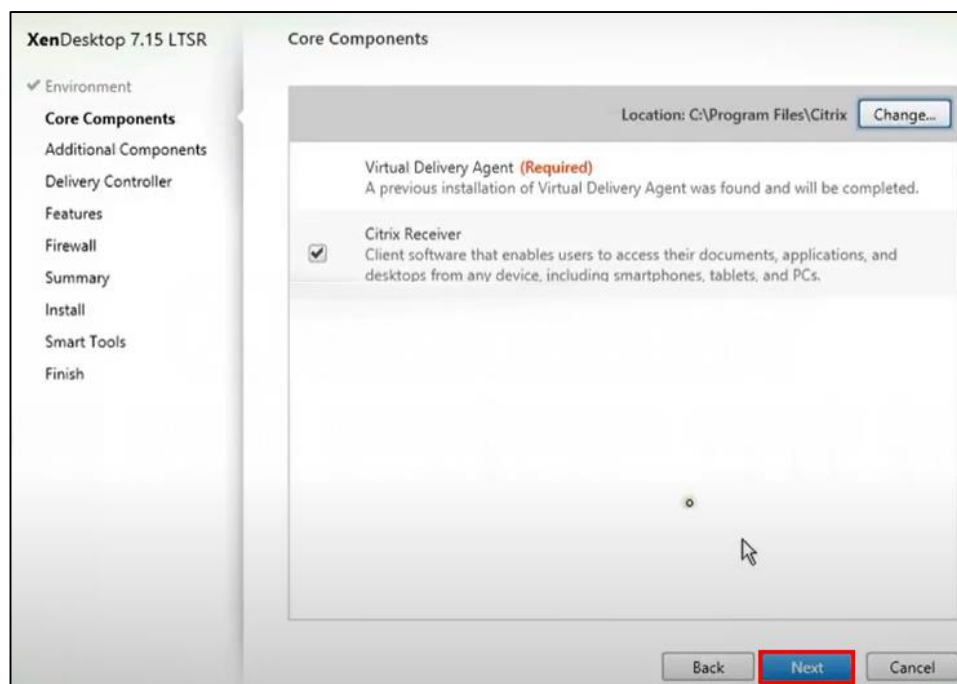
Paso 12: Seleccionar la opción “**Virtual Delivery Agent for Windows Server OS**”.



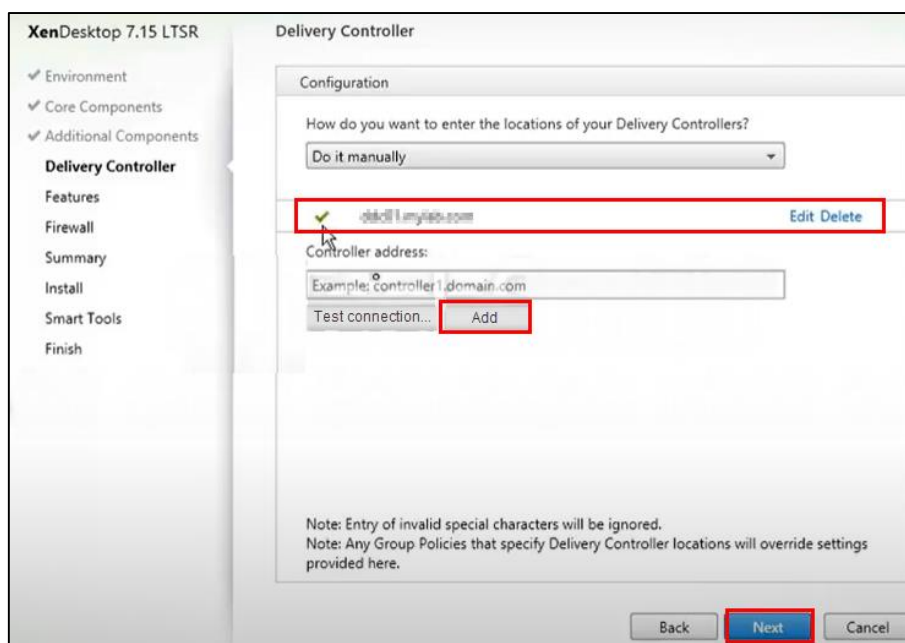
Paso 13: Seleccionar la opción **“Enable connections to a server machine”** y dar click en **“Next”**.



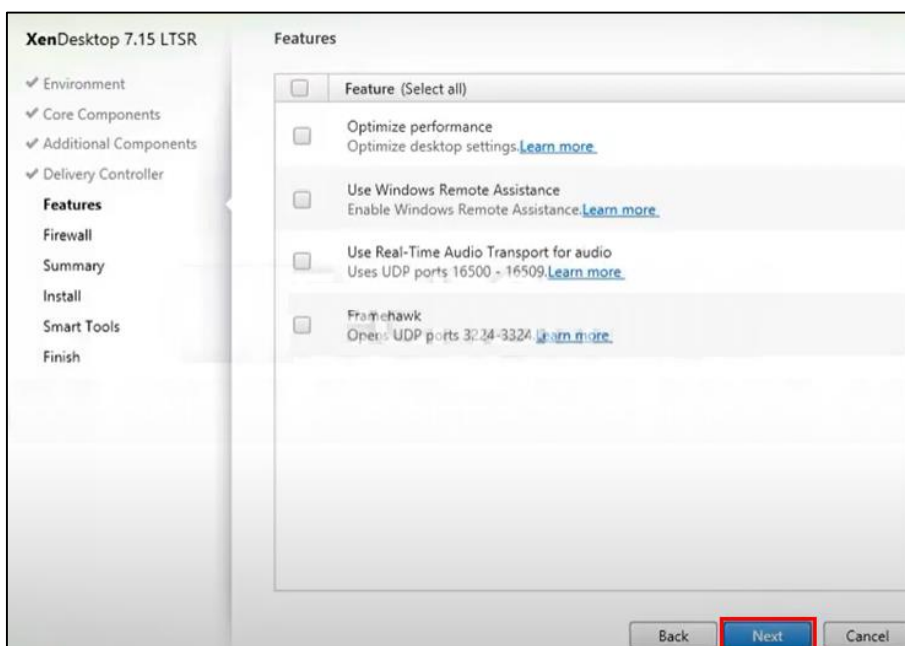
Paso 14: Mantener las opciones por defecto, con la opción de **“Citrix Receiver”** habilitada, y dar click en **“Next”**.



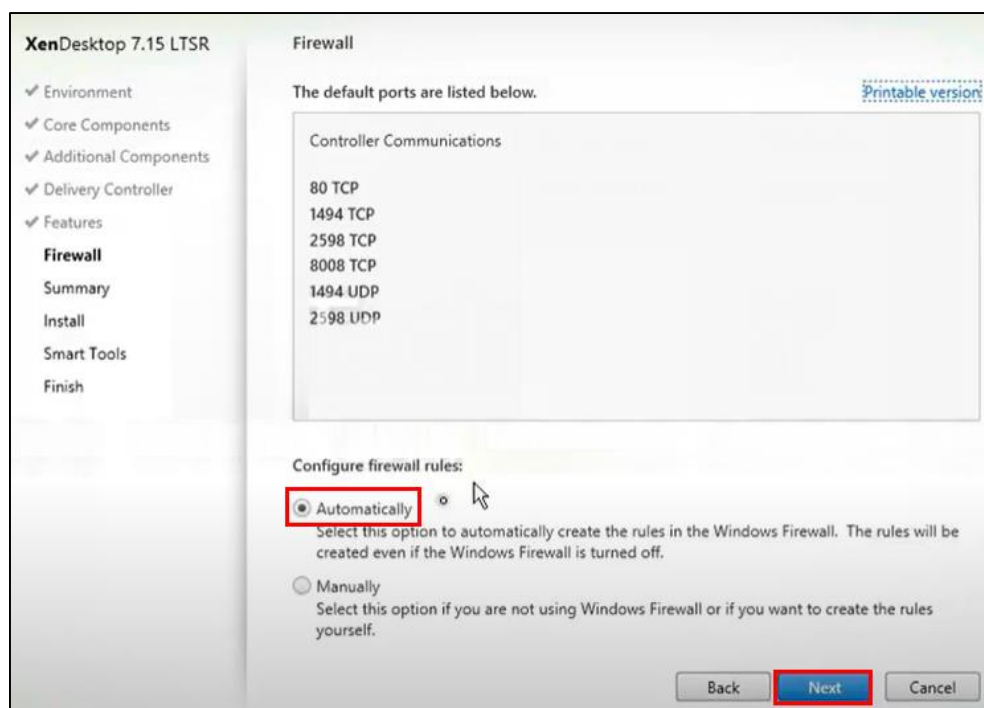
Paso 17: Seleccionar la opción “Add” y dar clic en “Next”.



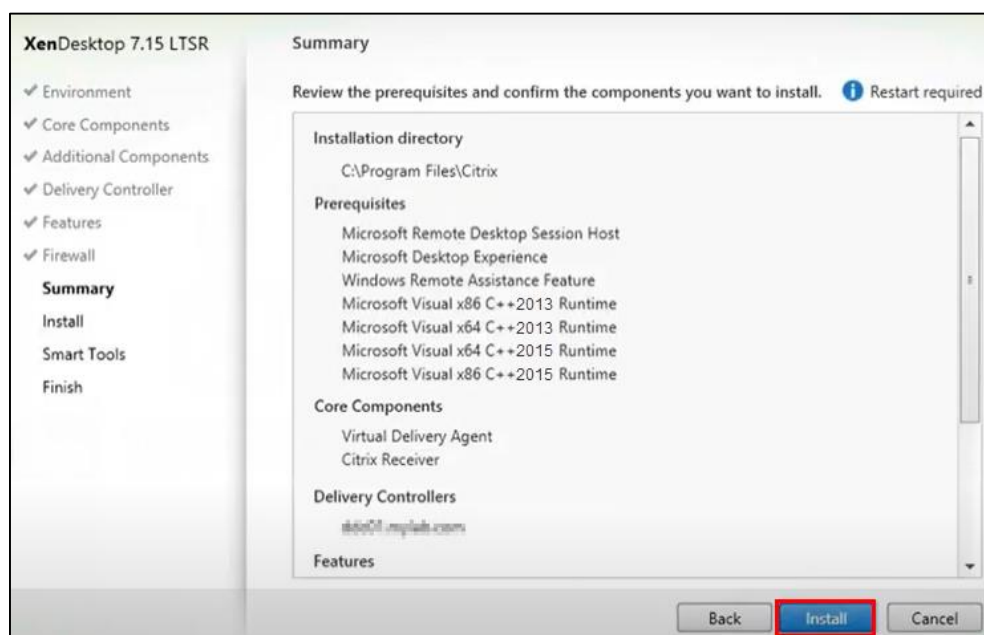
Paso 18: Seleccionar todas las características que se habilitarán. Dar click en “Next”.



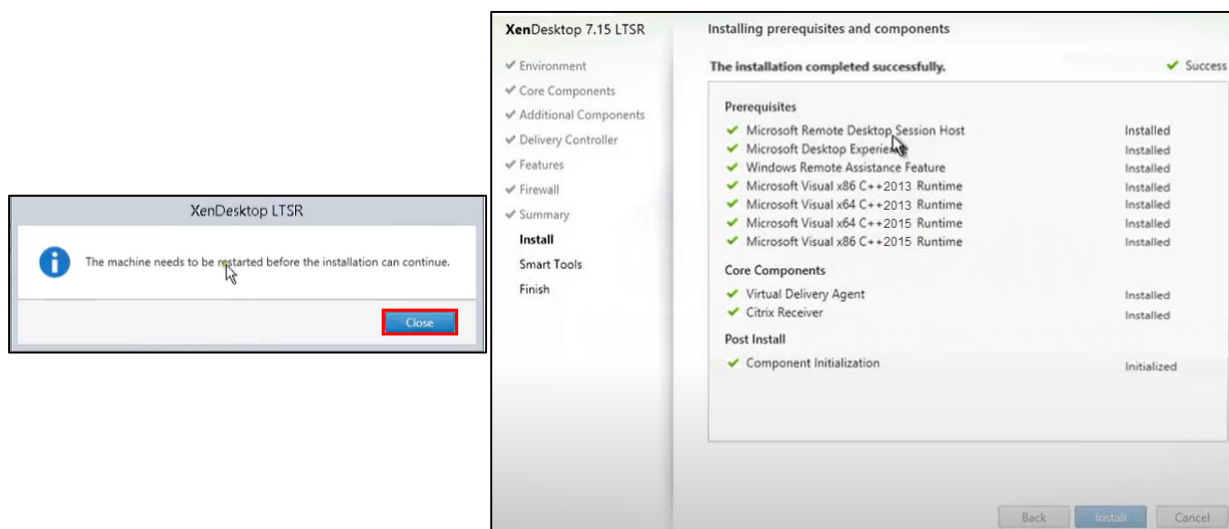
Paso 19: Seleccionar la opción de configuración automática y dar click en **Next**”.



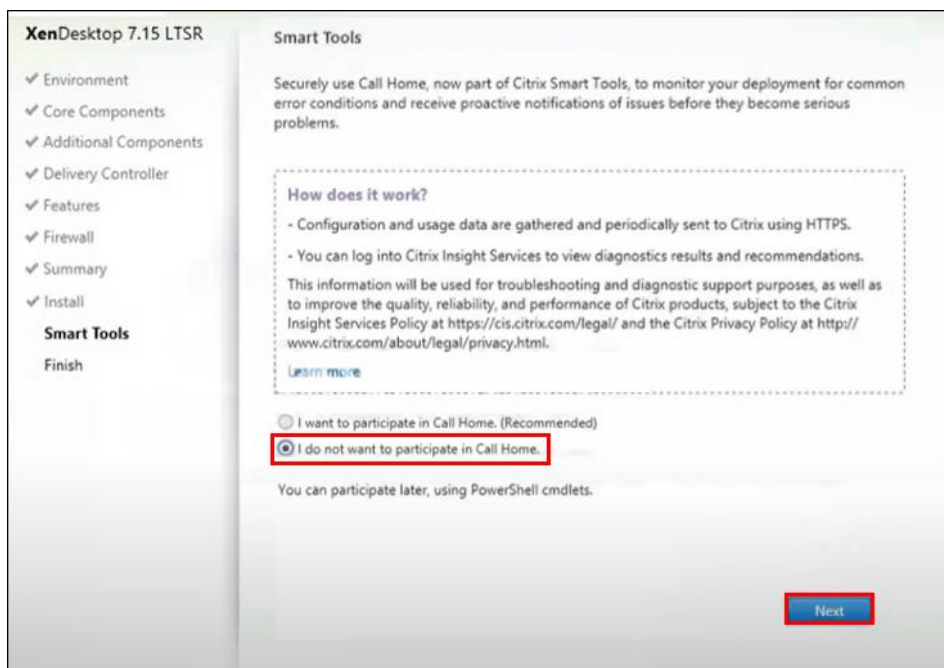
Paso 20: Iniciar al proceso de instalación dando click en **“Install”**”.



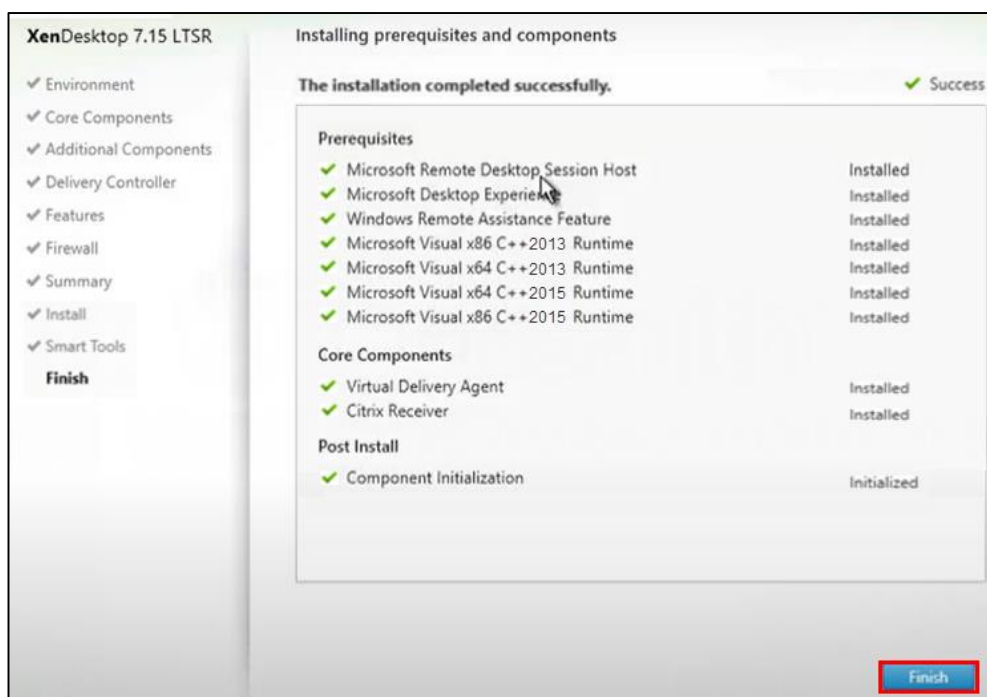
Paso 21: Durante el proceso de instalación se solicitará el reinicio de la máquina virtual para luego continuar (botón “Close” para proceder con el reinicio).



Paso 22: Elegir la casilla para no conectar con Smart Tools (Call Home) y seleccionar el botón “Next”.



Paso 23: Finalizar el proceso de instalación, seleccionando la opción “**Finish**”.



NOTA: Realizar este procedimiento para cada VDI (escritorio virtual) a crear.

Procedimiento de instalación de rsa authentication manager

Paso 1: Conectar un monitor y teclado al appliance, luego proceder con el encendido del mismo.

Paso 2: Seleccionar la opción más adecuada para el teclado (en este caso, opción 1).

```
Available keyboard layouts:
1. English (United States)
2. English (United Kingdom)
3. German (Germany)
4. French (France)
5. English (United States - Dvorak)

Keyboard layout choice (1-5): 1
```

Paso 3: En la pantalla de inicio, seleccionar la opción “**Start RSA Authentication Manager**”, presionar “**ENTER**” y esperar a que el equipo cargue automáticamente.

Paso 4: Ingresar la configuración de red asignada para este equipo (hostname, dirección IP, máscara de red, default Gateway y servidor DNS).

```
Network Settings
Press Enter for the next parameter. You will be prompted
ting them.

Fully qualified Hostname: rsa-auth-01.com
IP Address: 172.27.4.100
Subnet Mask: 255.255.255.0
Default Gateway: 172.27.4.254
Primary DNS Server: 172.27.4.100
Secondary DNS Server: 172.27.4.100
```

Paso 5: Verificar que los datos ingresados sean correctos y digitar la opción “y”.

```
Are these network settings correct? (y/n)
Applying network settings...
```

Paso 6: Recordar la URL y código de acceso de configuración (Quick Setup URL y Quick Setup Access Code) para proceder con la configuración del appliance con un Authentication Manager.

```
To complete the appliance configuration, access Quick Setup at:
https://172.27.4.254/
Quick Setup Access Code: 2FpTEqLk

To confirm the authenticity of the appliance, verify that the SHA-1
fingerprint of the certificate presented during Quick Setup matches the SHA-1
fingerprint displayed below.

4C 56 E9 55 5E 55 46 53 99 CC 63 54 FE 9F 39 F2 32 FC 36 DA

root@lab login: _
```

Paso 7: Conectar la interface del appliance a la red de la institución.

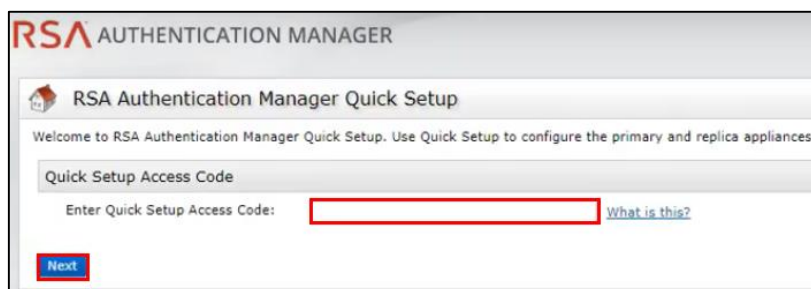
Procedimiento configuración de rsa authentication manager

Paso 1: Copiar el archivo de la licencia a una ubicación accesible en el equipo de cómputo (por ejemplo, laptop) que será usado para realizar la configuración inicial del appliance (no descomprimir el archivo).

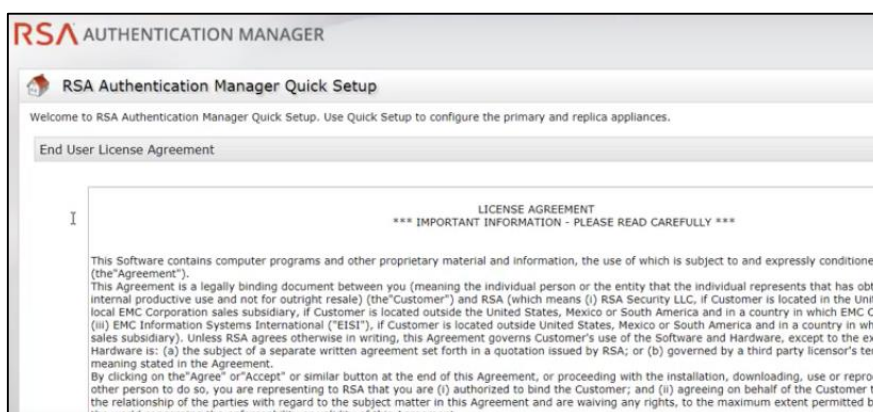
Paso 2: Ingresar a la URL de configuración del equipo “**https://IP_appliance/**”.



Paso 3: Digitar el código de acceso de configuración para ingresar a la plataforma. Dar click en “Next”.



Paso 4: Aceptar el acuerdo de licencia de usuario final (EULA). Dar click en “Accept”.



Paso 7: Dar click en “**Choose File**” para ubicar el archivo de licencia y luego “**Upload**”.



Primary Quick Setup

1. License File 2. Date & Time 3. OS Password 4. Initial Administration

Upload and review your license file.

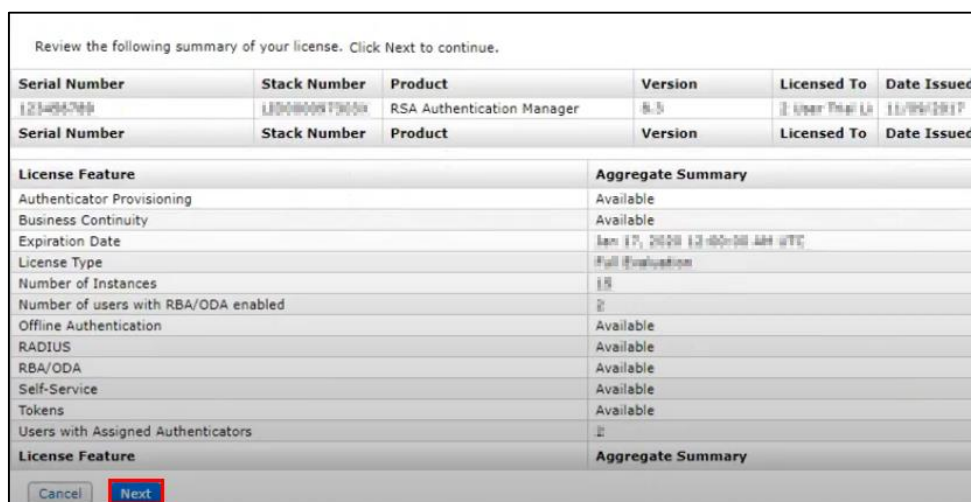
License File

Navigate to the location of your license file (.zip), and click Upload.

Upload License File: **Choose File** No file chosen **Upload**

Cancel Next

Paso 8: Verificar la información de la licencia y dar click en “**Next**”.



Review the following summary of your license. Click Next to continue.

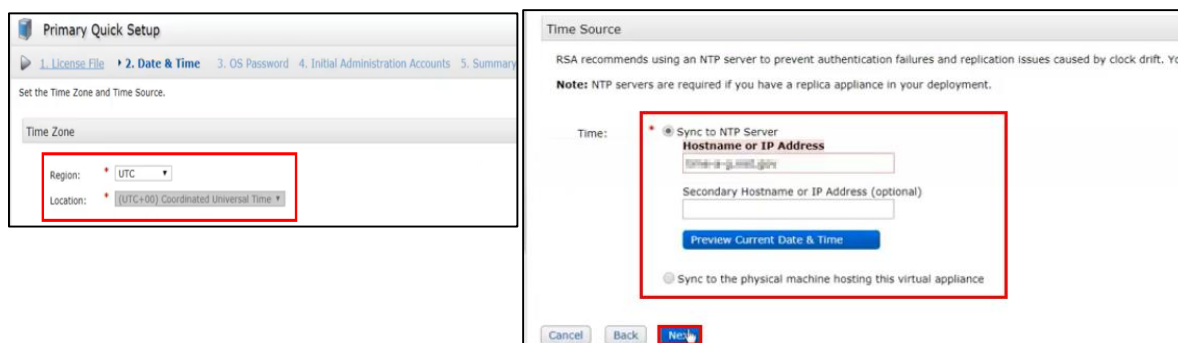
Serial Number	Stack Number	Product	Version	Licensed To	Date Issued
1234567890	1234567890	RSA Authentication Manager	8.5	Super User License	11/06/2017

Serial Number	Stack Number	Product	Version	Licensed To	Date Issued
1234567890	1234567890	RSA Authentication Manager	8.5	Super User License	11/06/2017

License Feature	Aggregate Summary
Authenticator Provisioning	Available
Business Continuity	Available
Expiration Date	Jan 17, 2020 12:00:00 AM UTC
License Type	Full Evaluation
Number of Instances	15
Number of users with RBA/ODA enabled	2
Offline Authentication	Available
RADIUS	Available
RBA/ODA	Available
Self-Service	Available
Tokens	Available
Users with Assigned Authenticators	2

Cancel **Next**

Paso 9: Seleccionar la zona horaria y definir el origen del reloj. Dar click en “**Next**”.



Primary Quick Setup

1. License File 2. Date & Time 3. OS Password 4. Initial Administration Accounts 5. Summary

Set the Time Zone and Time Source.

Time Zone

Region: UTC

Location: (UTC+00) Coordinated Universal Time

Time Source

RSA recommends using an NTP server to prevent authentication failures and replication issues caused by clock drift. You

Note: NTP servers are required if you have a replica appliance in your deployment.

Time:

☒ Sync to NTP Server

Hostname or IP Address: 192.168.1.100

Secondary Hostname or IP Address (optional):

Preview Current Date & Time

☐ Sync to the physical machine hosting this virtual appliance

Cancel Back **Next**

Paso 10: Configurar una contraseña para el usuario de sistema operativo. Dar click en “Next”.



Primary Quick Setup

1. License File 2. Date & Time 3. OS Password 4. Initial Administration

An operating system account is required to access the operating system directly or through the Security Console.

Operating System Password Settings

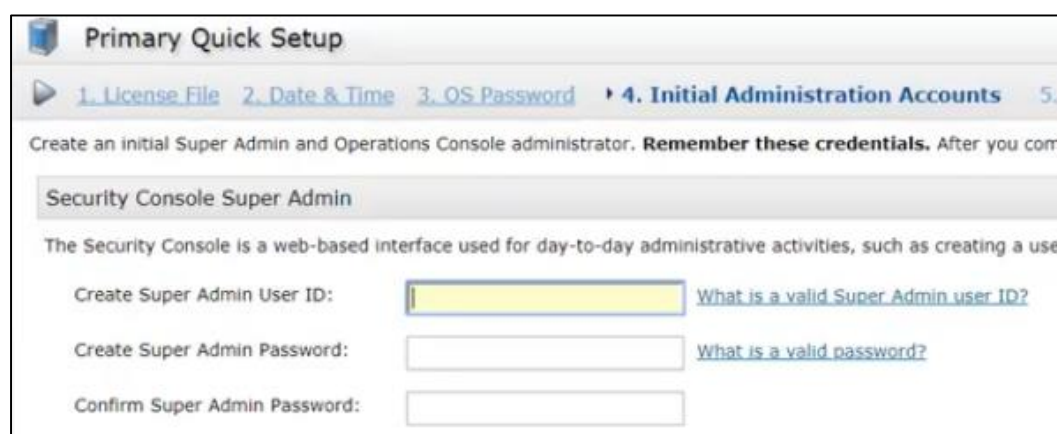
Operating System User ID: rsaadmin

Create Operating System Password:

Confirm Operating System Password:

Cancel Back **Next**

Paso 11: Configurar un usuario y contraseña para las cuentas “Super Admin” y “Operations Console Admin”. Dar click en “Next”.



Primary Quick Setup

1. License File 2. Date & Time 3. OS Password 4. Initial Administration Accounts 5. Initial Administration Accounts

Create an initial Super Admin and Operations Console administrator. **Remember these credentials.** After you complete this step, you will be able to log in to the Security Console and the Operations Console.

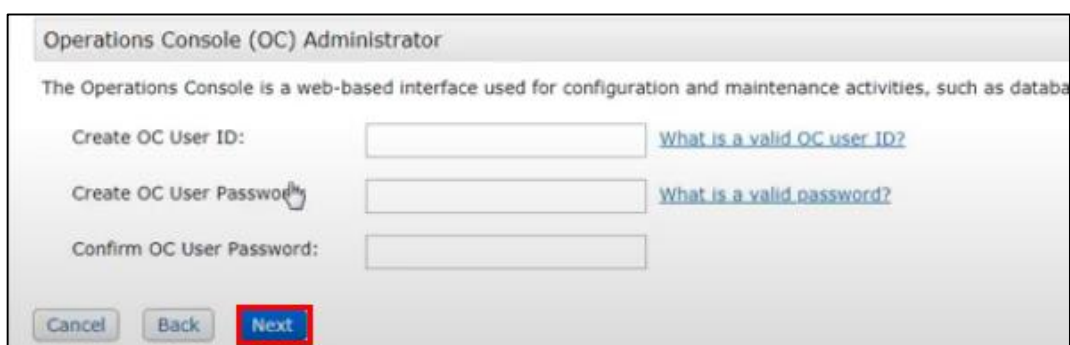
Security Console Super Admin

The Security Console is a web-based interface used for day-to-day administrative activities, such as creating a user or changing a password.

Create Super Admin User ID: [What is a valid Super Admin user ID?](#)

Create Super Admin Password: [What is a valid password?](#)

Confirm Super Admin Password:



Operations Console (OC) Administrator

The Operations Console is a web-based interface used for configuration and maintenance activities, such as database backup and recovery.

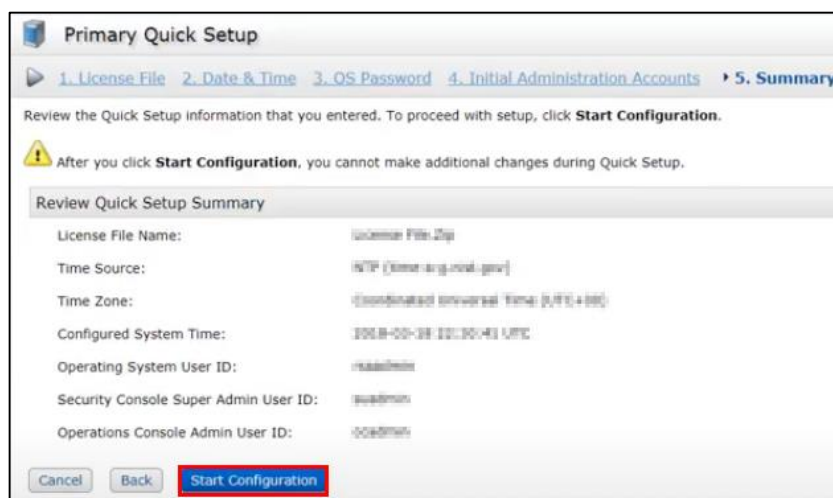
Create OC User ID: [What is a valid OC user ID?](#)

Create OC User Password: [What is a valid password?](#)

Confirm OC User Password:

Cancel Back **Next**

Paso 12: Verificar la configuración inicial realizada y dar click en “**Start Configuration**”.



Primary Quick Setup

1. License File 2. Date & Time 3. OS Password 4. Initial Administration Accounts 5. Summary

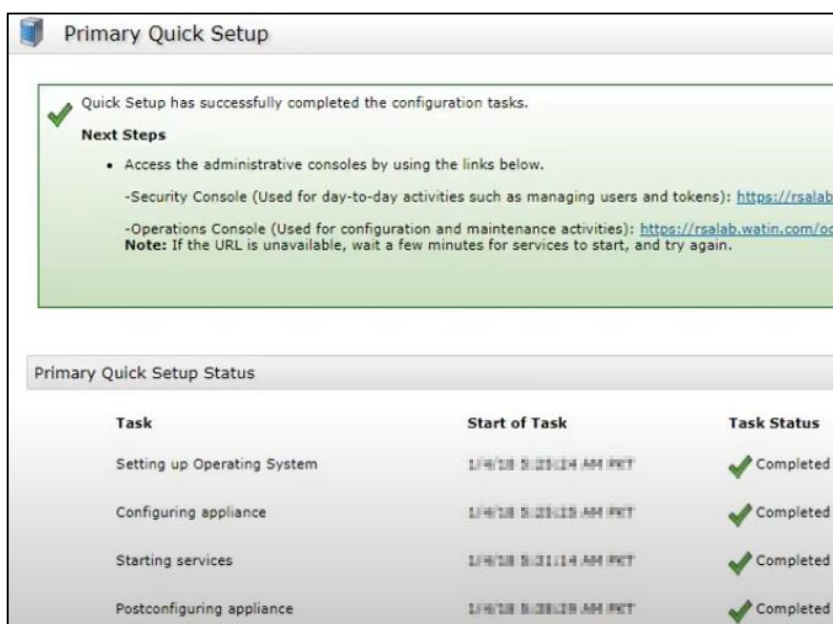
Review the Quick Setup information that you entered. To proceed with setup, click **Start Configuration**.

⚠ After you click **Start Configuration**, you cannot make additional changes during Quick Setup.

Review Quick Setup Summary

License File Name:	License File.Zip
Time Source:	NTP (time.windows.com)
Time Zone:	(Coordinated Universal Time (UTC)+00)
Configured System Time:	2008-09-28 12:00:00 UTC
Operating System User ID:	rsalabadmin
Security Console Super Admin User ID:	rsalabadmin
Operations Console Admin User ID:	rsalabadmin

Cancel Back **Start Configuration**



Primary Quick Setup

✓ Quick Setup has successfully completed the configuration tasks.

Next Steps

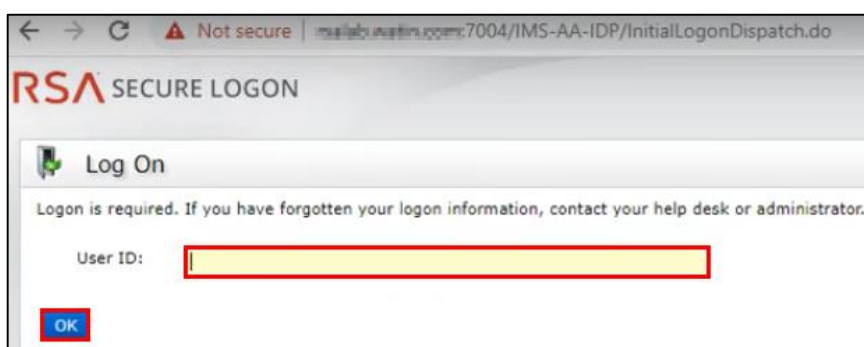
- Access the administrative consoles by using the links below.
 - Security Console (Used for day-to-day activities such as managing users and tokens): <https://rsalab.watin.com/sc>
 - Operations Console (Used for configuration and maintenance activities): <https://rsalab.watin.com/oc>

Note: If the URL is unavailable, wait a few minutes for services to start, and try again.

Primary Quick Setup Status

Task	Start of Task	Task Status
Setting up Operating System	1/1/08 9:00:00 AM PST	✓ Completed
Configuring appliance	1/1/08 9:00:00 AM PST	✓ Completed
Starting services	1/1/08 9:00:00 AM PST	✓ Completed
Postconfiguring appliance	1/1/08 9:00:00 AM PST	✓ Completed

Paso 13: Ingresar al portal de inicio de sesión del Security Console (https://hostname_appliance/sc). Digitar el usuario y dar click en “**OK**”.



← → ↻ ⚠ Not secure | rsalab.watin.com:7004/IMS-AA-IDP/InitialLogonDispatch.do

RSA SECURE LOGON

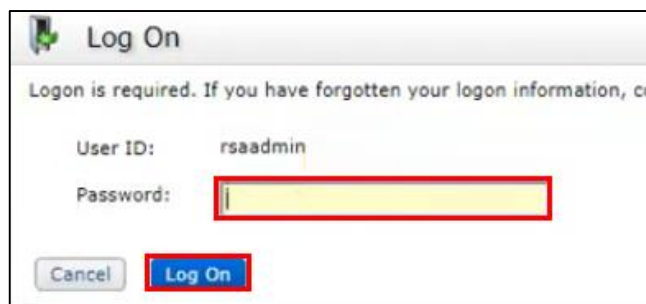
Log On

Logon is required. If you have forgotten your logon information, contact your help desk or administrator.

User ID:

OK

Digitar la contraseña correspondiente y dar click en “Log On”.



Log On

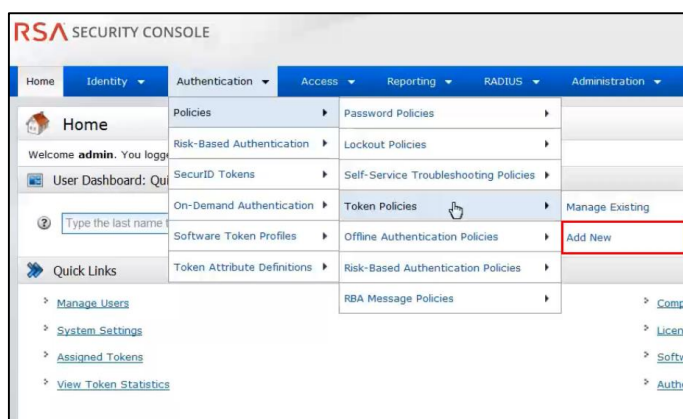
Logon is required. If you have forgotten your logon information, co

User ID: rsaadmin

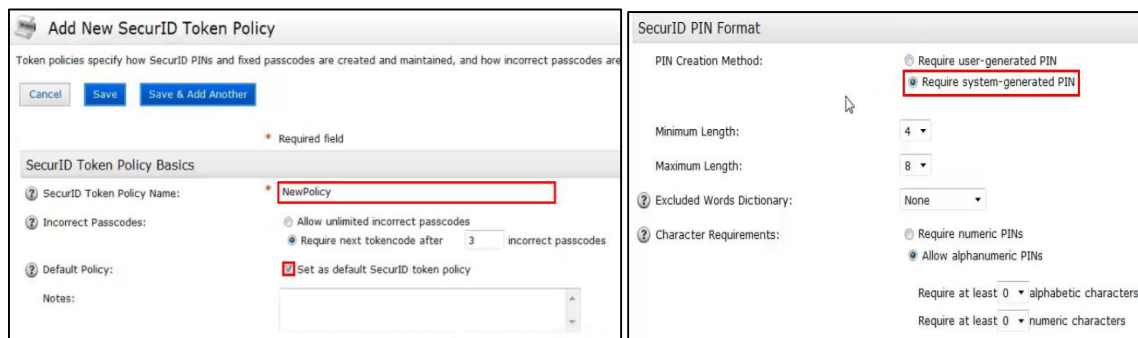
Password:

Cancel Log On

Paso 14: Ingresar a la opción “**Authentication > Policies > Token Policies > Add New**” para poder crear una política de Token.



Paso 15: Asignar un nombre a la política de Token y configurar de acuerdo al siguiente detalle (mantener las configuraciones por defecto de aquellas opciones que no se muestran).



Add New SecurID Token Policy

Token policies specify how SecurID PINs and fixed passcodes are created and maintained, and how incorrect passcodes are handled.

Cancel Save Save & Add Another

SecurID Token Policy Basics

SecurID Token Policy Name:

Incorrect Passcodes:

- ☐ Allow unlimited incorrect passcodes
- ☒ Require next tokencode after 3 incorrect passcodes

Default Policy:

- ☒ Set as default SecurID token policy

Notes:

SecurID PIN Format

PIN Creation Method:

- ☐ Require user-generated PIN
- ☒ Require system-generated PIN

Minimum Length: 4

Maximum Length: 8

Excluded Words Dictionary: None

Character Requirements:

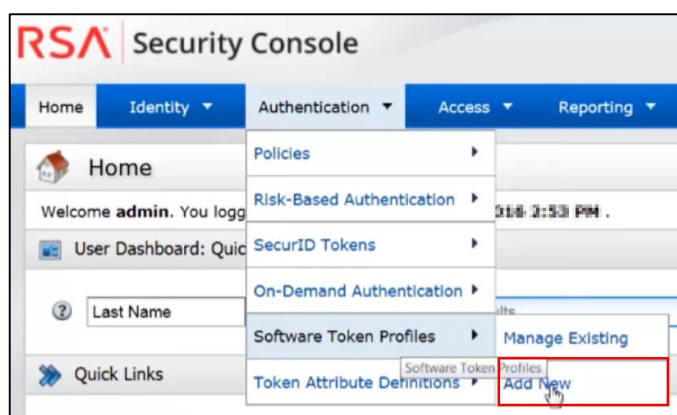
- ☐ Require numeric PINs
- ☒ Allow alphanumeric PINs

Require at least 0 alphabetic characters

Require at least 0 numeric characters

Al culminar, dar click en “**Save**” para guardar la configuración.

Paso 16: Ingresar a la opción “**Authentication > Software Token Profiles > Add New**” para poder crear un perfil de Software Token.



Paso 17: Asignar un nombre al perfil de Hardware Token y configurar de acuerdo al siguiente detalle (mantener las configuraciones por defecto de aquellas opciones que no se muestran).

Al culminar, dar click en “Save” para guardar la configuración.

Authentication Type: ☒ PIN integrated with tokencode (PINPad-style)
☐ PIN followed by tokencode (Fob-style)
☐ No PIN required (Tokencode)

Delivery Method: ☒ Dynamic Seed Provisioning (CT-KIP) ☐ File Based (SDTID)

☐ User imports token using CT-KIP activation URL and code
☒ User imports token via QR code in Self-Service Console

Device Specific Attributes

[What are device specific attributes?](#)

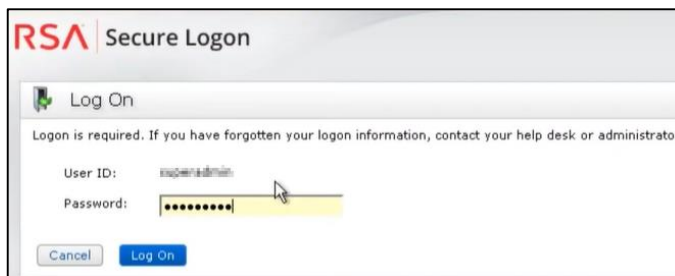
Attribute Name	Description	Data Type
DeviceSerialNumber	Android device type or application-generated Device ID	STRING
Nickname	Software Token Nickname	STRING

Attribute Name Description Data Type

Cancel Save Save & Add Another

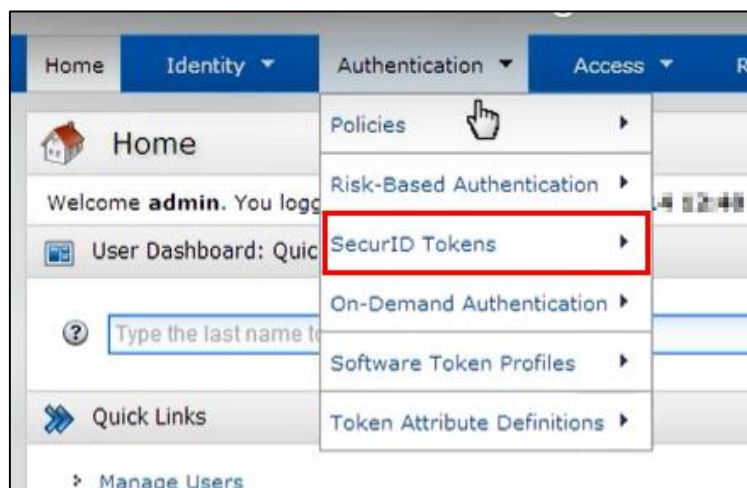
Procedimiento de asignación de Token RSA al usuario autorizado

Paso 1: Acceder al portal web de la plataforma Security Console de RSA a través del enlace “<https://hostname-rsa/sc>”:

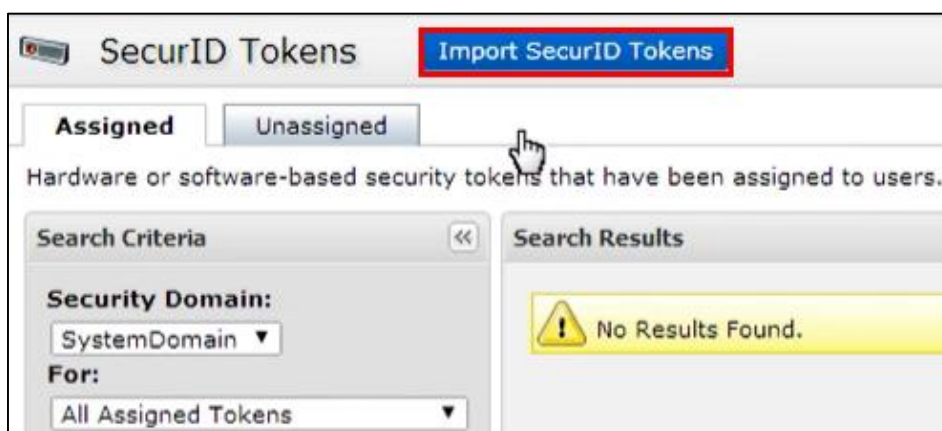


Paso 2: Para el caso de los Hardware Token, importar la semilla correspondiente.

Ingresar a la opción “**Authentication > SecurID Tokens**”:



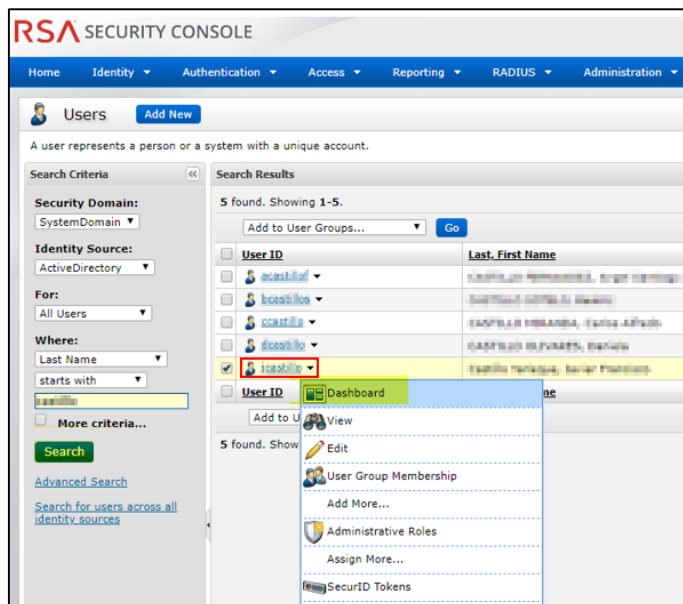
Seleccionar la opción “**Import SecurID Tokens**”:



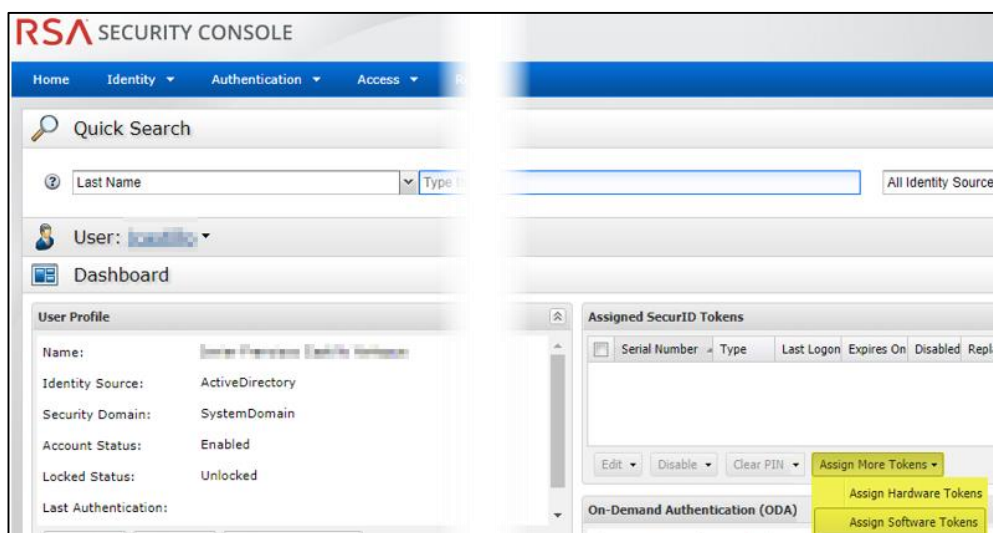
Asignar un nombre a la tarea de importación de la semilla, ubicar el archivo correspondiente en la opción “**Choose File**” y dar click en “**Submit Job**”. Luego esperar a que la tarea termine de ejecutarse para tener disponibles los Token:

Paso 3: Ingresar a la gestión de usuarios, a través de la ruta “**Identity > Users > Manage Existing**”.

Paso 4: En los criterios de búsqueda seleccionar los parámetros que se muestran a continuación y digitar, por ejemplo, el apellido del usuario. Luego de ubicarlo, desplegar las opciones disponibles y seleccionar **“Dashboard”**:



Paso 5: Dentro de los detalles del usuario, en la sección **“Assigned SecurID Tokens”**, seleccionar la opción **“Assign More Tokens”** y elegir entre las opciones Hardware Tokens o Software Tokens.



Paso 6: Del listado general de tokens, marcar la casilla de aquel que se encuentra libre y que será asignado al usuario involucrado, seleccionando la opción **“Assign”**.

Listado de Software Token:

User: [User Name] ▼

Assign SecurID Tokens

Imported and unassigned tokens are listed below. Select token(s) to assign to the selected user(s).

Search Criteria

Security Domain: SystemDomain ▼

For: All Unassigned Tokens ▼

Where: Serial Number ▼

contains ▼

More criteria...

Search Results

500 found. Showing 1-250.

Assign

Serial Number	Token Type	Algorithm	Requires Passcode	Disabled	Expires On
[Serial Number]	SecurID Software Token	AES-TIME	✓	✓	8/29/14 8:00:00
[Serial Number]	SecurID Software Token	AES-TIME	✓	✓	8/29/14 8:00:00
[Serial Number]	SecurID Software Token	AES-TIME	✓	✓	8/29/14 8:00:00
[Serial Number]	SecurID Software Token	AES-TIME	✓	✓	8/29/14 8:00:00

Listado de Hardware Token:

User: [User Name] ▼

Assign SecurID Tokens

Imported and unassigned tokens are listed below. Select token(s) to assign to the selected user(s).

Search Criteria

Security Domain: SystemDomain ▼

For: All Unassigned Tokens ▼

Where: Serial Number ▼

contains ▼

More criteria...

Search

Search Results

20 found. Showing 1-20.

Assign

Serial Number	Token Type	Algorithm	Requires Passcode	Disabled	Expires On
[Serial Number]	SecurID 800	AES-TIME	✓	✓	8/29/14 8:00:00
[Serial Number]	SecurID 800	AES-TIME	✓	✓	8/29/14 8:00:00
[Serial Number]	SecurID 800	AES-TIME	✓	✓	8/29/14 8:00:00
[Serial Number]	SecurID 800	AES-TIME	✓	✓	8/29/14 8:00:00
[Serial Number]	SecurID 800	AES-TIME	✓	✓	8/29/14 8:00:00

Paso 7: Seleccionar el Serial Number del Token asignado para proceder a ingresar a sus opciones y distribuirlo.

User: [User Name] ▼

Assigned SecurID Tokens

Cancel

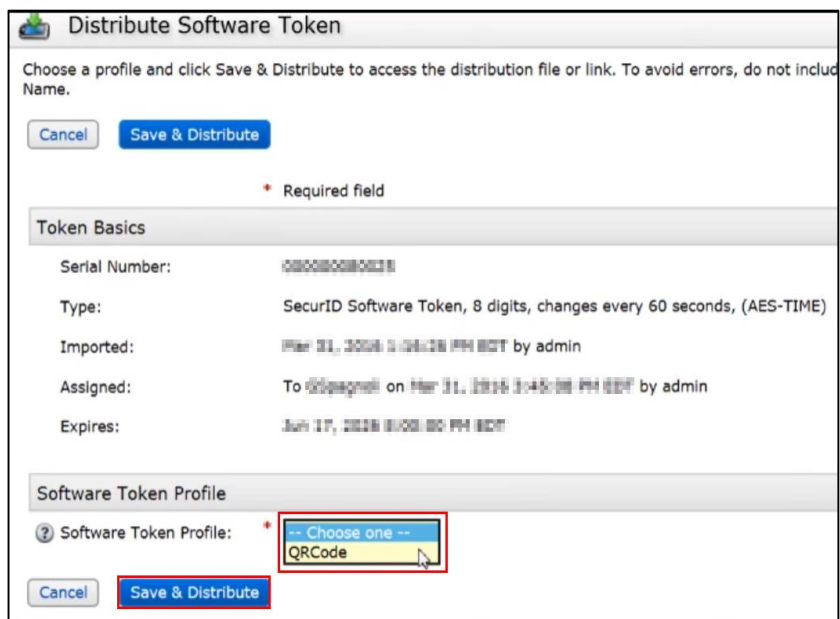
✓ Assigned 1 token(s) to 1 user(s). For software tokens, click the token and select options to distribute.

Assigned SecurID Tokens Assign Token

The following tokens are assigned to the selected user.

Serial Number	Token Type	SecurID PIN	Token Status	Enabled for Online Access
[Serial Number]	SecurID 800	Not Set	Active	

Paso 8: Realizar la distribución correspondiente, según el tipo de Token asignado. Elegir el perfil correspondiente y seleccionar la opción “**Save & Distribute**”.



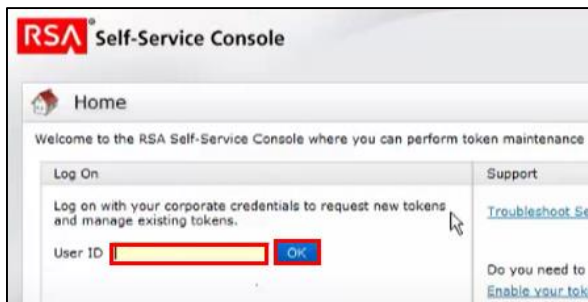
The screenshot shows a window titled "Distribute Software Token". At the top, it says: "Choose a profile and click Save & Distribute to access the distribution file or link. To avoid errors, do not include Name." Below this are "Cancel" and "Save & Distribute" buttons. A section labeled "Token Basics" contains the following information:

- Serial Number: 00000000000000000000000000000000
- Type: SecurID Software Token, 8 digits, changes every 60 seconds, (AES-TIME)
- Imported: Mar 31, 2016 3:45:18 PM EDT by admin
- Assigned: To 00000000 on Mar 31, 2016 3:45:18 PM EDT by admin
- Expires: Jun 17, 2016 03:00:00 PM EDT

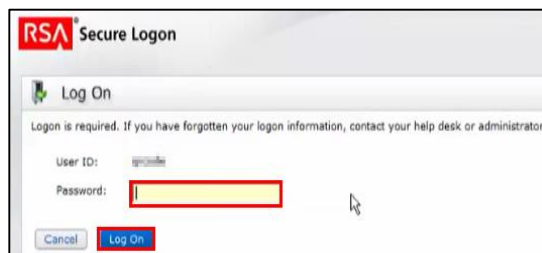
Below the token basics is a section titled "Software Token Profile". It contains a label "Software Token Profile:" followed by a dropdown menu. The dropdown menu is open, showing "-- Choose one --" and "QRCode". The "QRCode" option is highlighted. At the bottom of the dialog are "Cancel" and "Save & Distribute" buttons.

Paso 9: Realizar la activación del Token asignado.

El usuario debe acceder al portal web de la plataforma Self-Service Console de RSA a través del enlace “**https://hostname-rsa/ss**”, con sus credenciales de red:



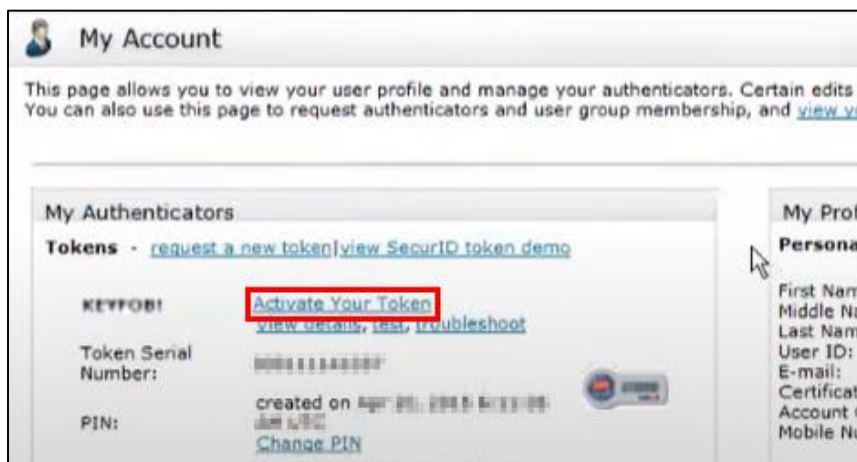
The screenshot shows the "RSA Self-Service Console" Home page. It has a header with the RSA logo and the text "Self-Service Console". Below the header is a "Home" section with a welcome message: "Welcome to the RSA Self-Service Console where you can perform token maintenance...". There are two main sections: "Log On" and "Support". The "Log On" section contains the text: "Log on with your corporate credentials to request new tokens and manage existing tokens." Below this is a "User ID" input field and an "OK" button. The "Support" section contains links for "Troubleshoot Se..." and "Do you need to... Enable your toke...".



The screenshot shows the "RSA Secure Logon" page. It has a header with the RSA logo and the text "Secure Logon". Below the header is a "Log On" section with the text: "Logon is required. If you have forgotten your logon information, contact your help desk or administrator." There are two input fields: "User ID:" and "Password:". Below these fields are "Cancel" and "Log On" buttons.

➤ Activación hardware Token

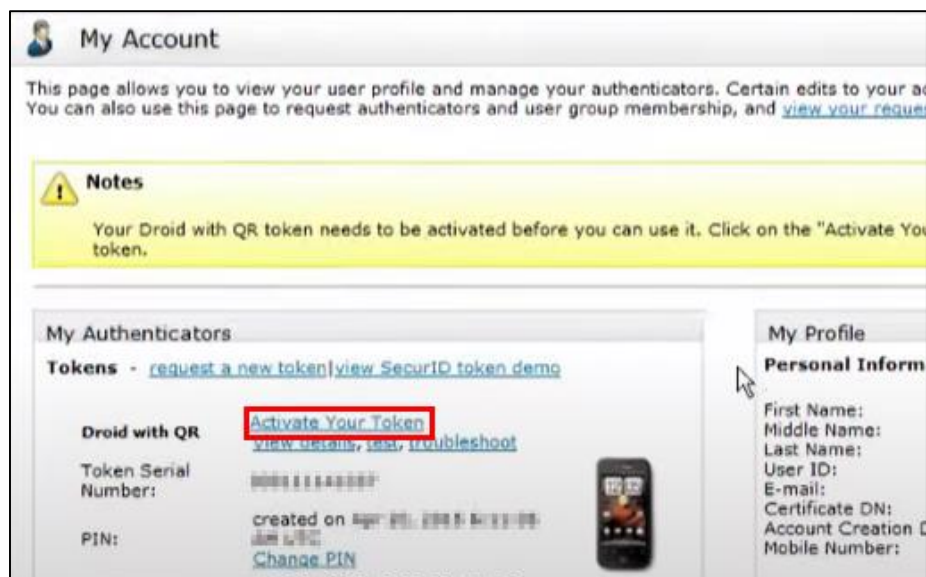
Seleccionar la opción “**Activate Your Token**” y luego crear el PIN correspondiente:

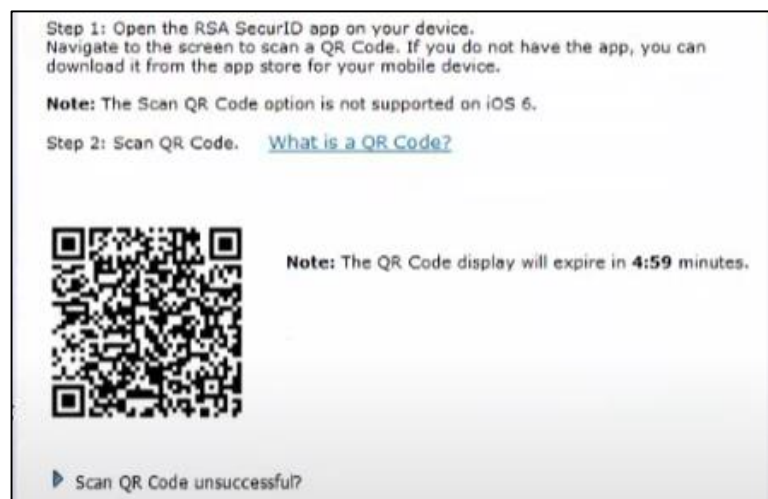


Luego de activar el token físico, en el portal web de acceso realizar su verificación para el acceso correspondiente.

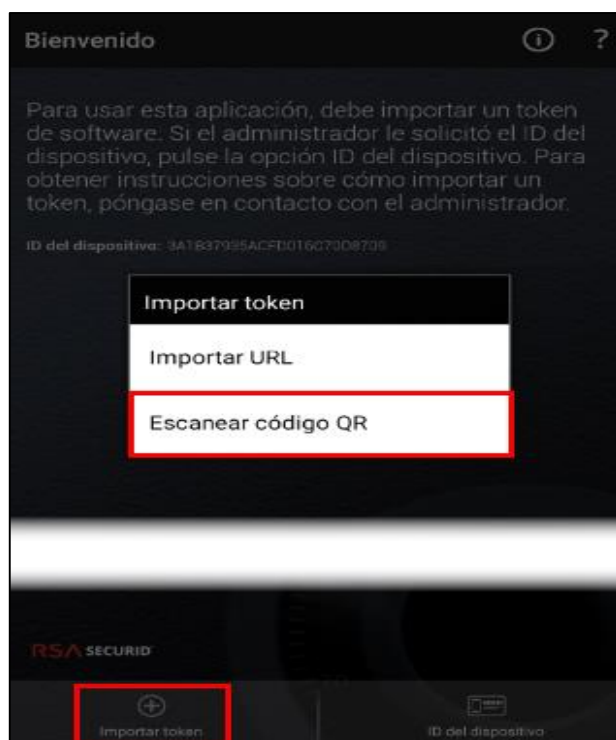
➤ Activación software TOKEN

Seleccionar la opción “**Activate Your Token**” y luego crear el PIN correspondiente:





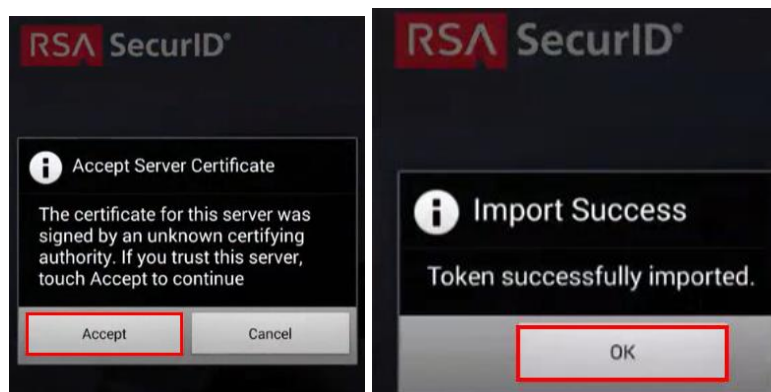
En el dispositivo móvil, ingresar al aplicativo “**RSA SecurID Software Token**” (previamente instalado) y seleccionar la opción “**Importar token > Escanear código QR**” para proceder con el escaneo del código generado en el paso anterior:



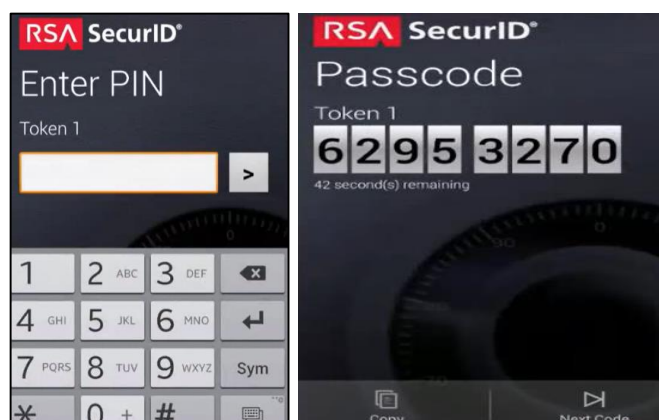
En el portal web de la plataforma Self-Service Console de RSA aparecerá la siguiente ventana. Dar click en “Close”.



En el dispositivo móvil, aceptar el certificado correspondiente. Dar click en “Accept” y luego en “OK”.



Finalmente, ingresar el número de PIN creado previamente para el token asignado:



Procedimiento de acceso al entorno virtual de teletrabajo

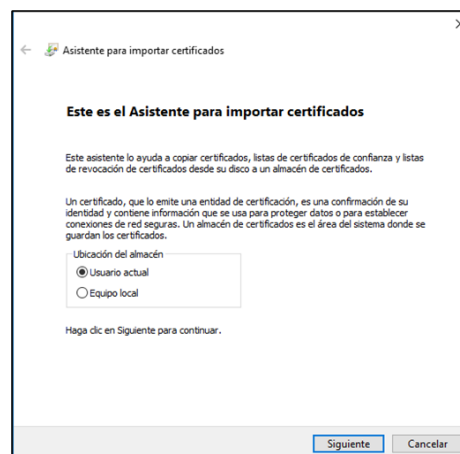
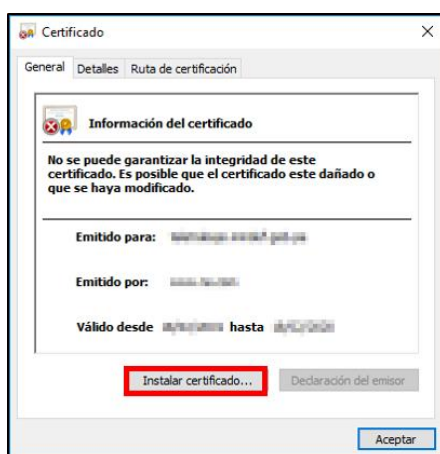
1. Instalación de certificados digitales

Para que el usuario final autorizado pueda ingresar al entorno virtual de Citrix fuera del área de trabajo, sólo necesitará de un dispositivo móvil con acceso a internet y tener instalado los certificados digitales correspondientes. Estos últimos son pre-requisito para el acceso al portal, serán proporcionados por la institución y se deberán instalar de forma local. A continuación, se muestran los pasos para la instalación de los mismos:

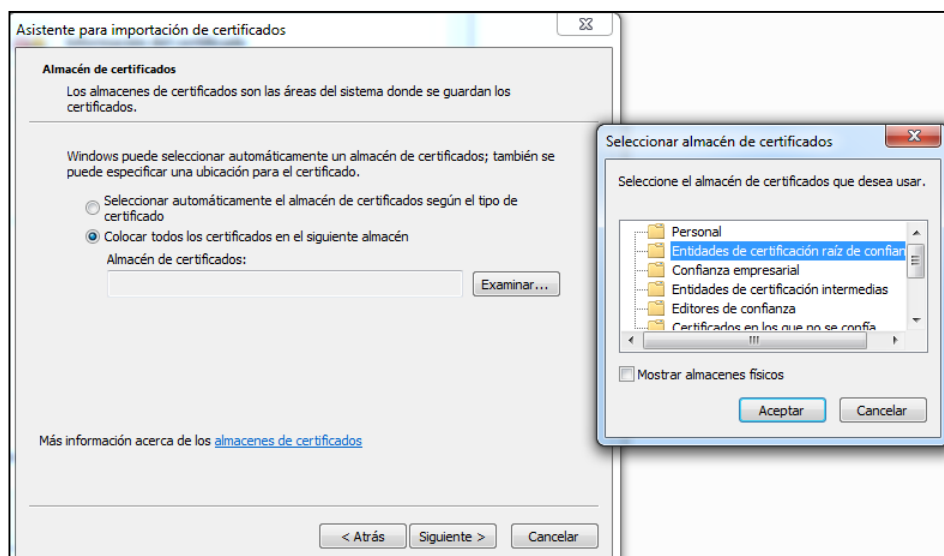
Paso 1: Ubicar los archivos, correspondientes a los certificados, en su dispositivo/equipo.



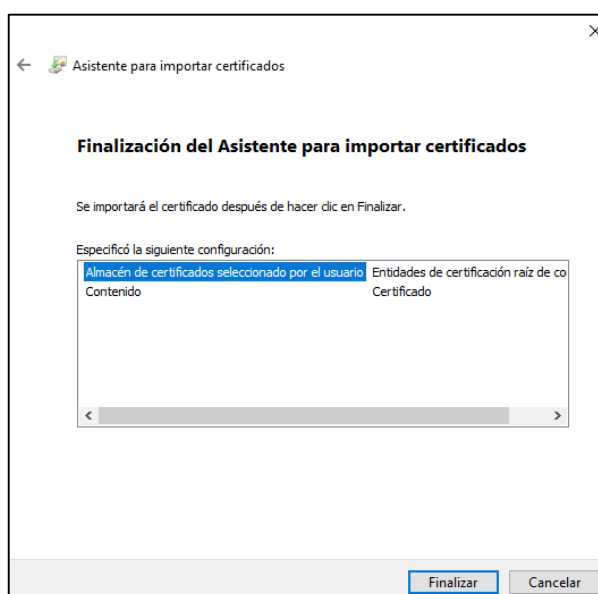
Paso 2: Abrir uno de ellos (doble click izquierdo) y seleccionar la opción “**Instalar certificado...**” para iniciar con el asistente de importación de certificados. Luego, dejar seleccionada la opción por defecto “**Usuario actual**” y dar click en “**Siguiente**”.



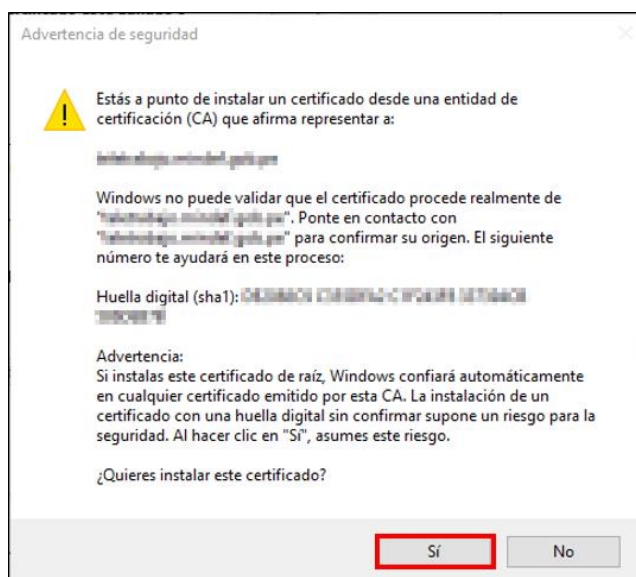
Paso 3: Seleccionar la opción “Colocar todos los certificados en el siguiente almacén” y luego “Examinar...”. A continuación, en la lista de carpetas que se muestra, seleccionamos “Entidades de certificación raíz de confianza”, luego damos click en “Aceptar” y, por último, en “Siguiente”.



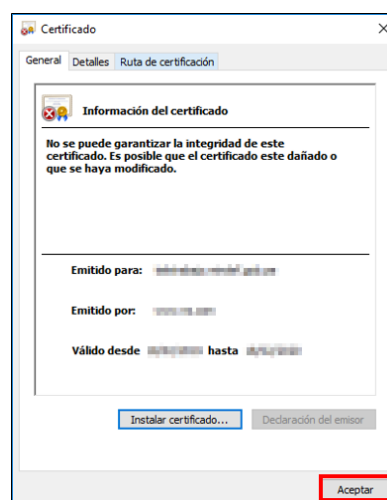
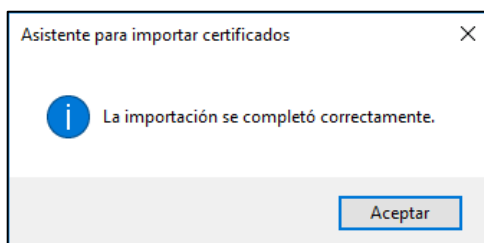
Paso 4: Luego de elegir y confirmar la carpeta en donde se almacenarán los certificados, se procede a seleccionar la opción “Finalizar” para que el proceso de importación se ejecute.



Paso 5: Se abrirá una ventana en donde seleccionaremos la opción “**Sí**” para confirmar el proceso de instalación del certificado.



Paso 6: Finalmente, luego de que el proceso de importación sea exitoso, seleccionamos la opción “**Aceptar**”.

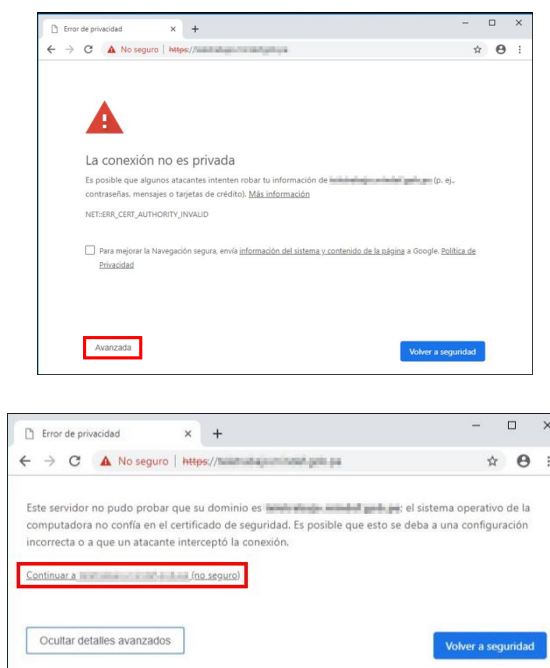


Al concluir, se deberá repetir los mismos pasos con el segundo certificado.

2. Acceso al entorno virtual de teletrabajo

Una vez concluido el proceso de instalación de los certificados digitales, el usuario final autorizado podrá ingresar a interactuar al entorno virtual de Citrix por medio de un navegador web. A continuación, se muestran los pasos a seguir:

Paso 1: Ingresar mediante un navegador web a la dirección/enlace configurado para el acceso al entorno virtual. Si es la primera vez que ingresa, visualizará la siguiente pantalla en donde deberá seleccionar la opción “**Avanzada**” y luego “**Continuar a ... (no seguro)**” para que se muestre la pantalla de inicio de sesión.

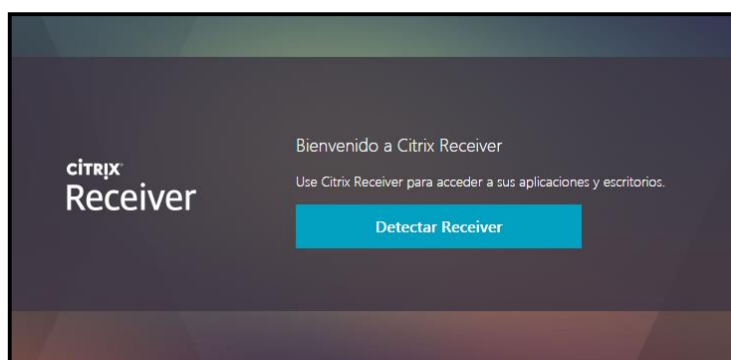


Paso 2: Ingresar las credenciales según el siguiente detalle:

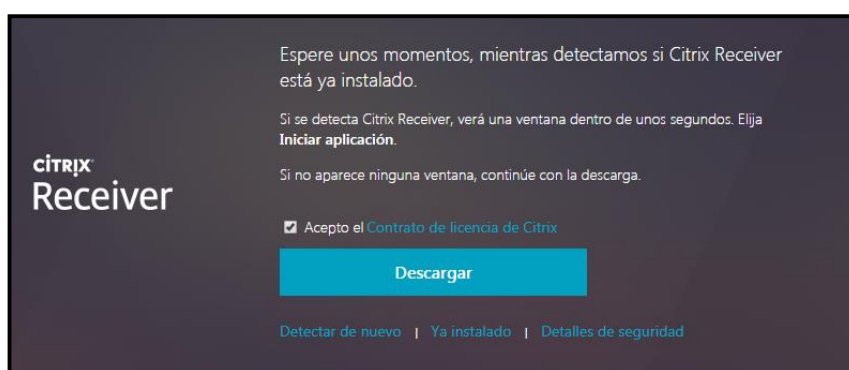
- **Primer campo:** colocar el nombre del usuario con el que normalmente accede cuando va a usar su equipo que tiene asignado dentro de las instalaciones del MINDEF.
- **Segundo campo:** ingresar la contraseña que usa normalmente para acceder al equipo que tiene asignado dentro de las instalaciones del MINDEF.
- **Tercer campo:** ingresar el PIN seguido del código que en ese momento haya generado el token físico o lógico que se le fue asignado.



Paso 3: Al ser la primera vez que accede a este sistema, le aparecerá la siguiente pantalla, en donde debe seleccionar la opción “**Detectar Receiver**”.



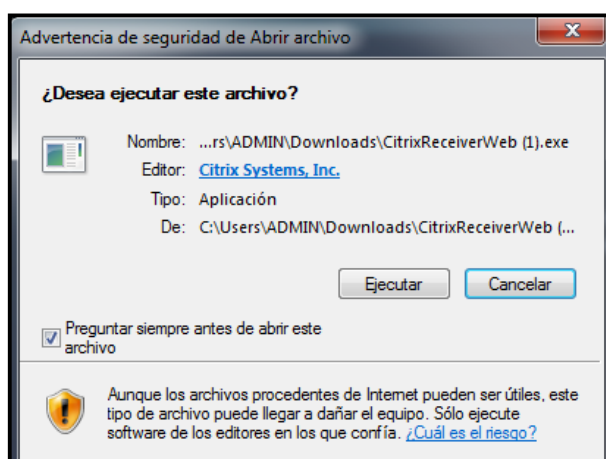
Paso 4: En el caso que sea un nuevo usuario tendrá que descargar el Agente de Citrix (Receiver), para ello seleccionar la opción “Acepto el Contrato de licencia de Citrix” y “Descargar”.



El agente descargado se mostrará en la barra inferior:



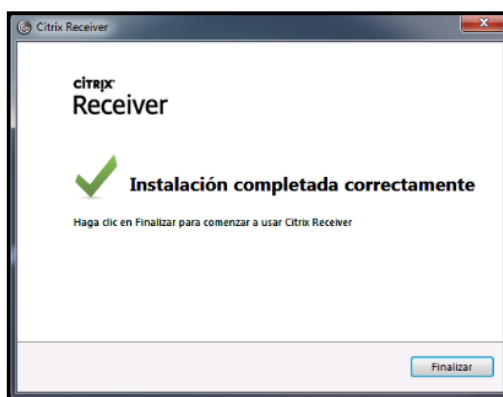
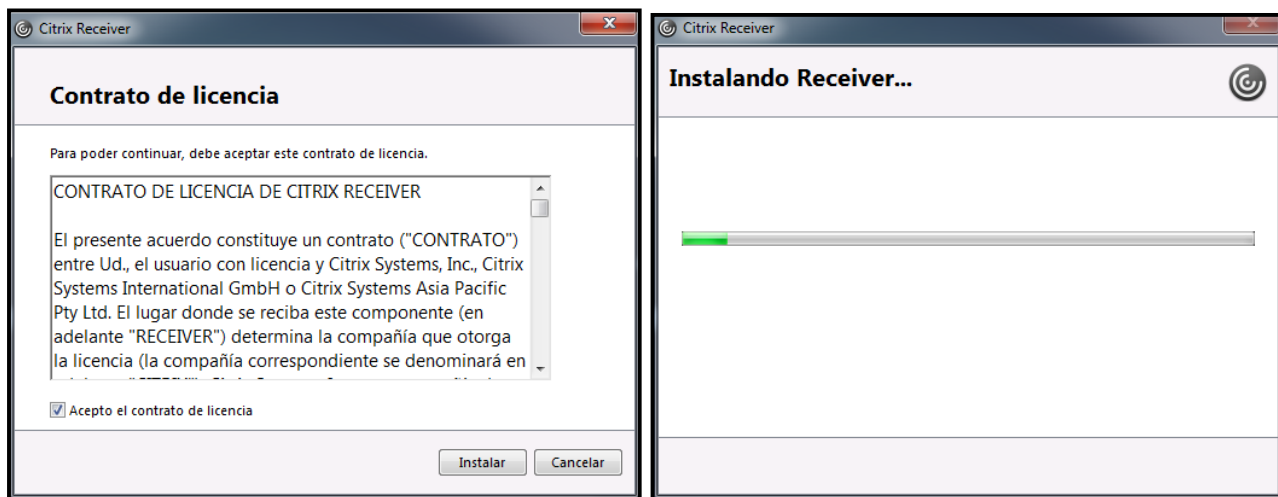
Paso 5: Una vez que termine la descarga, se deberá ejecutar (click izquierdo) el agente de acuerdo con los siguientes pasos.



Dar inicio al proceso de instalación, seleccionando la opción “Iniciar”:



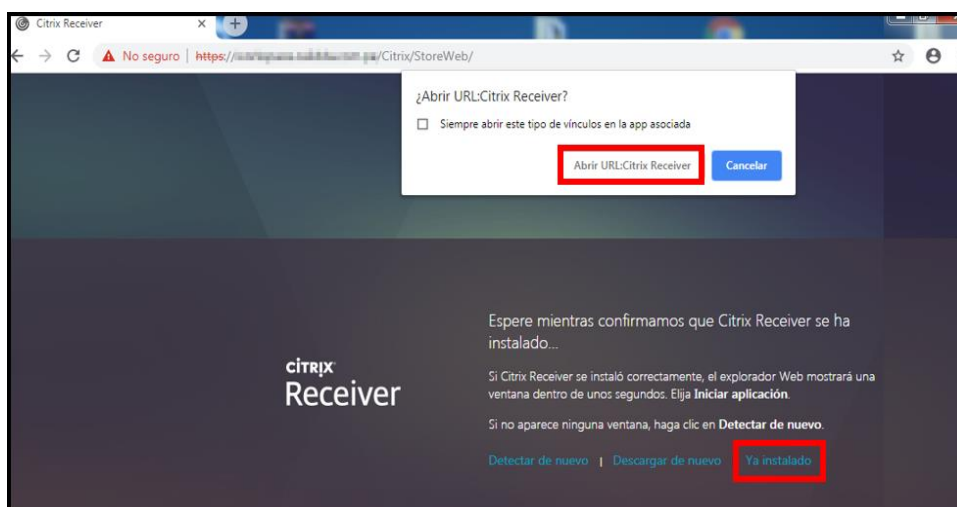
Marcar la opción de aceptación de contrato de licencia y seleccionar la opción “Instalar”:



El agente de Citrix sólo se instala una vez, al finalizar con la instalación se debe seleccionar la opción “Continuar”:

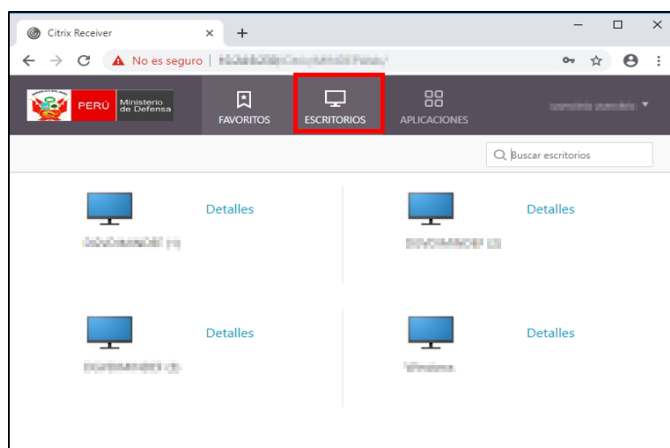


Finalmente, seleccionar las opciones “**Abrir URL: Citrix Receiver**” y “**Ya instalado**”:



En este punto, ya se encontrará dentro del entorno virtual de Citrix, en donde tendrá acceso tanto a los escritorios virtuales como a las aplicaciones virtuales que se les hayan sido habilitadas/asignadas:

▪ Escritorios Virtuales



Aplicaciones Virtuales

