FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SERVICIOS GLOBALES EN WINDOWS SERVER 2019 PARA MEJORAR LA ADMINISTRACIÓN Y SEGURIDAD LÓGICA DE INFRAESTRUCTURA DE TI EN UNA ORGANIZACIÓN MULTI SEDE MASS

AUTOR(ES):

Figueroa Encarnación, Sheilla Lisbeth (orcid.org/0000-0003-4184-7446)

Huamán Solis,Axel Kevin(orcid.org/0000-0003-4967-6282)

Huillca Ancco, Luis Manuel Jeremy (orcid.org/0000-0002-6377-1844)

Navarro Benites, Alexandre Josue (orcid.org/0000-0003-2130-7418)

Pachas Vera, Cristian Ramiro (orcid.org/0000-0001-7312-1223)

Rojas Bernardo, Jonathan Anderson (orcid.org/0000-0003-3379-0996)

ASESOR(A):

Dr. Ordoñez Perez, Adilio Christian (orcid.org/0000-0003-3875-9576)

LIMA-PERÚ

2024-I

Generalidades:	
• Nivel:	Aplicado
• Objetivo de Desarrollo Sostenible y Meta:	Trabajo decente y crecimiento económico
• Línea de Investigación:	Tecnología de la información y comunicacion
• Línea de Responsabilidad Social Universitaria	Infraestructura de servicio de redes y comunicaciones

DEDICATORIA

Dedicamos este informe a nuestros padres, cuyo amor, sacrificio y apoyo inquebrantable han sido el motor que impulsa nuestro camino académico y profesional. A nuestro mentor, cuya orientación y sabiduría han sido fundamentales para nuestro crecimiento y desarrollo. Y a todos aquellos que de una u otra manera han contribuido en nuestra formación, gracias por ser parte de este viaje.

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento a Dios por ser mi guía durante mi trayectoria académica y profesional. También, a nuestros familiares por ser soporte y apoyo al seguimiento de nuestro proyecto; y por supuesto a nuestro asesor de curso por las indicaciones y retroalimentaciones que nos ha brindado para con nuestro informe práctico.

DECLARACIÓN DE AUTENTICIDAD

Yo, Figueroa Encarnación Sheilla Lisbeth, estudiante del programa de estudio de Ingeniería de Sistemas de la Universidad César Vallejo, sede /filial de Lima Norte; declaro que el trabajo académico titulado “SERVICIOS GLOBALES EN WINDOWS SERVER 2019 PARA MEJORAR LA ADMINISTRACIÓN Y SEGURIDAD LÓGICA DE INFRAESTRUCTURA DE TI EN UNA ORGANIZACIÓN MULTI SEDE MASS” presentado, para sustentar el trabajo de investigación formativa en la experiencia curricular de Networking and Comunications II.

Por lo tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajados académicos.

No he utilizado ninguna otra fuente distinta de aquellas expresadamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o a fines.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Lima, diciembre del 2023.

……

Figueroa Encarnación Sheilla Lisbeth

DNI: 73210844

DECLARACIÓN DE AUTENTICIDAD

Yo, Huaman Solis Axel Kevin, estudiante del programa de estudio de Ingeniería de Sistemas de la Universidad César Vallejo, sede /filial de Lima Norte; declaro que el trabajo académico titulado “SERVICIOS GLOBALES EN WINDOWS SERVER 2019 PARA MEJORAR LA ADMINISTRACIÓN Y SEGURIDAD LÓGICA DE INFRAESTRUCTURA DE TI EN UNA ORGANIZACIÓN MULTI SEDE MASS” presentado, para sustentar el trabajo de investigación formativa en la experiencia curricular de Networking and Comunications II.

Por lo tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajados académicos.

No he utilizado ninguna otra fuente distinta de aquellas expresadamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o a fines.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Lima, diciembre del 2023.

……..

Huaman Solis Axel Kevin

DNI: 72296869

DECLARACIÓN DE AUTENTICIDAD

Yo, Huillca Ancco Luis Manuel Jeremy, estudiante del programa de estudio de Ingeniería de Sistemas de la Universidad César Vallejo, sede /filial de Lima Norte; declaro que el trabajo académico titulado “SERVICIOS GLOBALES EN WINDOWS SERVER 2019 PARA MEJORAR LA ADMINISTRACIÓN Y SEGURIDAD LÓGICA DE INFRAESTRUCTURA DE TI EN UNA ORGANIZACIÓN MULTI SEDE MASS” presentado, para sustentar el trabajo de investigación formativa en la experiencia curricular de Networking and Comunications II.

Por lo tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajados académicos.

No he utilizado ninguna otra fuente distinta de aquellas expresadamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o a fines.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Lima, diciembre del 2023.

…….

Huillca Ancco Luis Manuel Jeremy

DNI: 60574278

DECLARACIÓN DE AUTENTICIDAD

Yo, Navarro Benites Alexandre Josue, estudiante del programa de estudio de Ingeniería de Sistemas de la Universidad César Vallejo, sede /filial de Lima Norte; declaro que el trabajo académico titulado “SERVICIOS GLOBALES EN WINDOWS SERVER 2019 PARA MEJORAR LA ADMINISTRACIÓN Y SEGURIDAD LÓGICA DE INFRAESTRUCTURA DE TI EN UNA ORGANIZACIÓN MULTI SEDE MASS” presentado, para sustentar el trabajo de investigación formativa en la experiencia curricular de Networking and Comunications II.

Por lo tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajados académicos.

No he utilizado ninguna otra fuente distinta de aquellas expresadamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o a fines.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Lima, diciembre del 2023.

…….

Navarro Benites Alexandre Josue

DNI: 75295726

DECLARACIÓN DE AUTENTICIDAD

Yo, Pachas Vera Cristian Ramiro, estudiante del programa de estudio de Ingeniería de Sistemas de la Universidad César Vallejo, sede /filial de Lima Norte; declaro que el trabajo académico titulado “SERVICIOS GLOBALES EN WINDOWS SERVER 2019 PARA MEJORAR LA ADMINISTRACIÓN Y SEGURIDAD LÓGICA DE INFRAESTRUCTURA DE TI EN UNA ORGANIZACIÓN MULTI SEDE MASS” presentado, para sustentar el trabajo de investigación formativa en la experiencia curricular de Networking and Comunications II.

Por lo tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajados académicos.

No he utilizado ninguna otra fuente distinta de aquellas expresadamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o a fines.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Lima, diciembre del 2023.

……

Pachas Vera Cristian Ramiro

DNI: 72524681

DECLARACIÓN DE AUTENTICIDAD

Yo, Rojas Bernardo Jonathan Anderson, estudiante del programa de estudio de Ingeniería de Sistemas de la Universidad César Vallejo, sede /filial de Lima Norte; declaro que el trabajo académico titulado “SERVICIOS GLOBALES EN WINDOWS SERVER 2019 PARA MEJORAR LA ADMINISTRACIÓN Y SEGURIDAD LÓGICA DE INFRAESTRUCTURA DE TI EN UNA ORGANIZACIÓN MULTI SEDE MASS” presentado, para sustentar el trabajo de investigación formativa en la experiencia curricular de Networking and Communications II.

Por lo tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos.

No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.

Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o a fines.

Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.

De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Lima, diciembre del 2023.

……..……..

Rojas Bernardo Jonathan Anderson

DNI: 47436421

ÍNDICE DE CONTENIDO

RESUMEN

Nuestro proyecto de investigación de tecnologías de información y comunicación con mención a infraestructura de servicios de redes y comunicaciones titulado “Servicios globales en Windows Server 2019 para mejorar la administración y seguridad lógica de infraestructura de TI en una organización - multi sede MASS”, comprende sobre la implementación de servicios de seguridad para la mejora y protección de la información almacenada en las diferentes sucursales de las tiendas MASS alrededor del Perú con el objetivo de innovar en las tecnologías de información de esta misma organización, resguardar el acceso de su personal por medio de una equiparada gestión dependiendo de los roles sometidos y proteger el almacenamiento de información ante cualquier hurto, manipulación y/o ataque cibernético perjudiciales para la estructura tecnológica de la organización.

La ciberseguridad es la práctica de prevenir intrusiones no autorizadas en una organización por parte de personas externas. Actualmente estamos viendo una variedad de formas en que los ciberdelincuentes pueden comprometer los sistemas y utilizar técnicas muy avanzadas para identificar ataques informáticos. Como todos sabemos, la seguridad lógica de la infraestructura consiste en comprender los servicios, puertos, actualizaciones, vulnerabilidades y amenazas existentes. Tome medidas preventivas antes de que existan amenazas que puedan causar complicaciones financieras y/o legales para su negocio. En el campo de la seguridad informática, se sabe que el activo más importante de una organización, más importante aún si pertenece a un organismo gubernamental, por lo tanto la responsabilidad de los responsables de dichos activos es mayor, por lo que cuentan con estrictas medidas de seguridad. protocolos y políticas diseñadas para mitigar todo tipo de riesgos de la información.

La implementación de soluciones para la administración y seguridad lógica en las tecnologías de información en los diferentes puntos de venta de la empresa de productos de primera necesidaD, MASS, ayuda en la gestión efectiva de acceso a la información por parte de los usuarios que vienen a ser el personal perteneciente al minimarket y resguardar los datos e información tanto suyos como de los clientes como mecanismos de seguridad cibernética y administración informática para desarrollar el buen funcionamiento en conjunto con las sede principal y sucursales.

ABSTRACT

Our information and communication technologies research project with a mention in network and communications services infrastructure titled “Global Services in Windows Server 2019 to improve the management and logical security of IT infrastructure in an organization - multi-site MASS”, includes about the implementation of security services for the improvement and protection of the information stored in the different branches of the MASS stores around Peru with the objective of innovating in the information technologies of this same organization, protecting the access of its staff through an equivalent management depending on the roles submitted and protect the storage of information against any theft, manipulation and/or cyber attack detrimental to the technological structure of the organization.

Cybersecurity is the practice of preventing unauthorized intrusions into an organization by outsiders. We are currently seeing a variety of ways that cybercriminals can compromise systems and use very advanced techniques to identify cyber attacks. As we all know, logical infrastructure security is about understanding existing services, ports, updates, vulnerabilities, and threats. Take preventive measures before threats exist that could cause financial and/or legal complications for your business. In the field of computer security, it is known that the most important asset of an organization, even more important if it belongs to a government agency, therefore the responsibility of those responsible for said assets is greater, which is why they have strict measures. of security. protocols and policies designed to mitigate all types of information risks.

The implementation of solutions for the administration and logical security in information technologies in the different points of sale of the essential products company, MASS, helps in the effective management of access to information by users who come to be the personnel belonging to the minimarket and safeguard the data and information of both theirs and the clients as cybersecurity and computer administration mechanisms to develop proper functioning in conjunction with the main headquarters and branches.

I. INTRODUCCIÓN

1.1. Realidad problemática

La administración y seguridad lógica dentro de la infraestructura de TI trata lo más posible que la contribución al funcionamiento eficiente y seguro en las organizaciones empresariales internacionales dedicadas al comercio de víveres a precios bajos se lleven a cabo gratificantemente, sin embargo, la presencia de incidentes informáticos dentro de estas las obliga a preocuparse de sus recursos tanto informáticos como económicos. Torres (2020) indica que las organizaciones internacionales contienen grandes informaciones que están a la vista de los llamados hackers cuyo objetivo es hurtar suficiente información confidencial de estas mismas organizaciones tecnológicamente, generando que se incremente constantemente las amenazas tanto de robo de información como de activos de las mismas organizaciones ya sean públicas o privadas causadas por una acción voluntaria provocada por un individuo o por herramientas tecnológicas desconocidas puesto que la protección de información no es totalmente segura.

A nivel nacional, las organizaciones dedicadas a este rubro de los minimarkets se ven expuestas a que sus sucursales puedan sufrir incidencias informáticas como la falta de recursos y capacitación en su seguridad cibernética, vulnerabilidades en su software, riesgo a cumplimiento de medidas de ciberseguridad, gestión de contraseñas débiles para el personal, falta de políticas de seguridad y riesgo de acceso no autorizado que debilitan el funcionamiento interno de estas mismas. Debido al progreso de las grandes, pequeñas y microempresas en el Perú, las organizaciones de diferentes rubros a los que se dedican deben estar alertas para enfrentar los problemas de seguridad a causa del uso de servicios de tecnologías gratuitos y ausencia de políticas de seguridad que provocan ataques cibernéticos externos, fraudes y robo de información (Chavarría & Rubio, 2021).

La empresa MASS está dedicada a la venta de productos de primera necesidad a bajos precios cuyo propósito es ser la más grande cadena de puntos de venta a las que los peruanos puedan acudir para encontrar productos de primera necesidad cercanos a su hogar y con los mejores precios.

La empresa MASS, no es ajeno a estos problemas ya que en la administración y seguridad lógica de infraestructura de TI se presentan varios problemas, uno de los tantos problemas está asociado a la gestión de acceso a más recursos de los necesarios por parte de personal dependiendo de su rol, este genera una brecha en su seguridad con respecto al aumento de riesgo de filtraciones de datos o manipulación malintencionada de información.

La empresa MASS ofrece los servicios de red más comunes en sucursales de puntos de ventas de primera necesidad, tales como la conectividad de red confiable y segura en todas sus tiendas permitiendo la comunicación fluida entre las ubicaciones y con su sede central que incluye servicios de internet de alta velocidad, conexiones VPN para garantizar la seguridad de la transmisión de datos y redes privadas internas para comunicaciones internas. También tiene servicios de red para sus sistemas de punto de venta (POS), que son críticos para procesar transacciones de clientes que implica asegurar conexiones confiables y seguras a servidores centrales, así como la integración de sistemas de pago electrónico y procesamiento de tarjetas. De igual manera, servicios de almacenamiento centralizado de datos en la nube o en servidores locales para garantizar la disponibilidad y seguridad de la información en todas sus ubicaciones ya que facilita la gestión y el acceso a datos críticos, como inventario, historiales de transacciones y datos de clientes. Otro servicio importante en la empresa MASS es la seguridad de red que protege sus sistemas y datos contra amenazas cibernéticas tales como firewalls, sistemas de detección de intrusiones, filtrado de contenido web y sistemas de prevención de pérdida de datos (DLP) con el fin de garantizar la integridad y confidencialidad de la información. No nos podemos olvidar de los servicios de soporte y mantenimiento de red que garantizan el funcionamiento continuo de sus sistemas e incluyen monitoreo proactivo de la red, resolución de problemas, actualizaciones de software y parches de seguridad, así como asistencia técnica para usuarios finales en todas las ubicaciones.

Los problemas asociados a la administración y seguridad lógica de infraestructura de TI en la empresa MASS son las vulnerabilidades de seguridad atractivos para los ciberataques debido a la cantidad de datos confidenciales manejados, como

información de tarjetas de crédito y datos personales de los clientes; las vulnerabilidades en el software, los sistemas operativos o los dispositivos conectados pueden ser explotadas por hackers para acceder a esta información sensible. La administración inadecuadamente de los privilegios de acceso de los empleados y contratistas también es un problema dentro de la empresa ya que la falta de una gestión eficaz de accesos lleva a brechas de seguridad y fugas de datos. La falta de actualización oportuna puede dejar al sistema vulnerable a exploits conocidos y ataques de malware. Las fallas en la seguridad física como las cadenas de puntos de venta de MASS también deben considerarse en sus sistemas y datos ya que el acceso no autorizado a servidores, terminales de punto de venta u otros dispositivos puede comprometer la seguridad de la información. También las fugas de datos debido a ataques cibernéticos, errores humanos o fallos en los sistemas de seguridad que tienen graves repercusiones tanto para la empresa como para sus clientes, incluida la pérdida de confianza y la responsabilidad legal.

De seguir con esta situación problemática, la empresa MASS estaría afectada en la confianza de sus clientes primordiales para el progreso y legado de la misma, dañar la reputación de su marca establecida en el mercado peruano desde hace varios años, también el impacto financiero que pueden sufrir de aquí en adelante, problemas legales que dañarían la integridad de la empresa, interrupción de sus actividades como causa de su poca productividad y pérdida de competitividad que provocaría la pérdida de clientes hasta el cierre de sus locales de venta establecidos.

1.2. Formulación del Problema

PROBLEMA PRINCIPAL:

¿Cómo influyen los servicios globales en WS 2019 en la administración y seguridad lógica de infraestructura de TI en la empresa Mass?

PROBLEMA ESPECÍFICO:

Al alinear estas recomendaciones con tus objetivos específicos, puedes proporcionar un enfoque más holístico y robusto que no solo aborde la gestión de accesos y la seguridad, sino que también promueva una infraestructura de TI resiliente y conforme a las mejores prácticas de seguridad. Esto será esencial para

proteger los datos sensibles y garantizar la continuidad del negocio en la empresa Mass.

- Implementar de un Sistema de Gestión de Identidades y Accesos
- Reforzar de la Autenticación y Credenciales
- Garantizar Conectividad Confiable y Segura
-

1.3. Justificación

Justificación Institucional

Sus análisis ofrecen un enfoque integral sobre cómo las empresas pueden organizarse para fortalecer su seguridad cibernética y mejorar sus operaciones para salvaguardar sus activos de información y garantizar su éxito a largo plazo. (Daniel Miessler 2019)

El estudio realizado fue garantizar la gestión y procesamiento de datos en las sucursales de la empresa , lo cual permitió alcanzar los propósitos estratégicos y cumplir con la misión de cada área gestionando así Información. La seguridad lógica en informática es un aspecto esencial de la seguridad de cada sucursal de la empresa , Implica llevar a cabo acciones , evitar y resguardar los sistemas y datos de posibles amenazas y vulnerabilidades. El cuestionamiento radicalmente es en evitar las consecuencias de un robo de información y disminuir los riesgos en los sistemas internos de la empresa. Además, la seguridad lógica se enfoca en detectar y mitigar los daños de manera saliente, antes de que se produzcan. Optimizar los procesos administrativos,Optimizar la toma de decisiones , agilizar la interacción y cooperación efectivas, y asegurar la protección de los datos son ventajas fundamentales de la informática en la gestión.

Justificación Tecnológica

aborda temas enfocados al desarrollo con la seguridad cibernética. Estos pueden incluir la importancia de implementar medidas de seguridad efectivas Para salvaguardar los sistemas y la información de los peligros en el ámbito cibernético, así como para administrar , los elementos vinculados a la protección de datos, también podemos analizar tácticas para detectar y reducir las debilidades en los sistemas de información así como la importancia del cumplimiento normativo en el ámbito de la seguridad cibernética.(Joseph Steinberg 2020)

La implementación de un servicio de la organización MULTI SEDE MASS tiene un impacto tecnológico significativo, este proyecto implica tanto innovación como el estudio de tecnologías existentes. Como investigadores, nos enfocaremos en analizar y evaluar este impacto para compartir nuestros hallazgos con la sociedad.

La implementación de este proyecto requerirá un tiempo adecuado, siguiendo las pautas de la norma ISO/IEC 27001.detalla esta norma, la duración del proyecto dependerá del nivel de seguridad y del gestionamiento del sistema de la seguridad . Es aconsejable tener asesores externos para llevar a cabo este procedimiento de manera eficaz.

El propósito fundamental de la implementación de este servicio integral es salvaguardar la privacidad, autenticidad y accesibilidad de los datos en la empresa. Esto se consigue a través del análisis de riesgos y la aplicación de acciones para reducirlos. La norma ISO 27001 se fundamenta en la administración de riesgos, investigando de manera exhaustiva.

Justificación Económica

amplia cobertura de Windows Server 2019, abordando temas como las nuevas características, mejoras de rendimiento, administración del sistema, configuración de servicios y seguridad. También podría incluir casos de uso, ejemplos prácticos y consejos sobre cómo aprovechar al máximo esta versión del sistema operativo de servidor de Microsoft. (Mitch Tulloch 2019)

Dentro del ámbito de los sistemas operativos para servidores, se reconoce que las opciones proporcionadas por Windows Server son las más destacadas.Especialmente, Windows Server 2019 ha demostrado ser una opción altamente mejorada, con una amplia gama de atributos y soluciones que permiten una gestión eficiente para cualquier organización que desee Expandir las sucursales de la empresa. Estamos evaluando servicios como implementación, ajuste, cuidado, servidor DNS y Active directory, junto con la formación requerida para garantizar un entorno de trabajo óptimo.

También se tienen en cuenta las buenas prácticas, la capacitación se promueve el aprovechamiento de las soluciones implementadas, y se ofrecen consejos y propuestas para garantizar un uso adecuado de los entornos y la gestión de acceso de los usuarios, así como la comunicación de elementos en los dominios de la organización. Nos aseguramos de que invertir en mejoras para el negocio sea invaluable.

cantidad del desarrollo del proyecto

S/. 42,750 SOLES , 11400 DOLARES AMERICANOS

N°	SERVICIO / PRODUCTO	PRECIO	MONEDA
1	CONFIGURACION DE SERVIDOR DNS	4500	USD
2	CONFIGURACION DE ACTIVE DIRECTORY	2300	USD
3	CAPACITACION DE GESTION DE ACTIVE DIRECTORY	2500	USD
4	COMPRA DE LICENCIAS DE WINDOWS SERVER 19 (POR SERVIDOR)	350	USD
5	INSTALACION ESTANDAR DE WINDOWS SERVER 19 (POR SERVIDOR)	450	USD
6	CAPACITACION Y GESTIONAMIENTO DE LA SEGURIDAD LOGICA	1300	USD
	TOTAL DE SERVICIOS ADMINISTRACIÓN Y SEGURIDAD LÓGICA DE INFRAESTRUCTURA DE TI EN UNA ORGANIZACIÓN MULTI SEDE MAS	11400	USD

1.4. Objetivos

Objetivo General

Implementar servicios globales en Windows Server 2019 para fortalecer la administración y seguridad lógica de la infraestructura de TI en la empresa MASS, con el fin de mitigar riesgos, proteger datos sensibles y garantizar la continuidad del negocio.

Objetivos específicos

1) **Gestión de Acceso Eficiente:**

- Implementar políticas de control de acceso basadas en roles para garantizar que el personal solo tenga acceso a los recursos necesarios para realizar sus funciones.

- Utilizar la autenticación multifactor (MFA) para reforzar la seguridad de las cuentas de usuario y prevenir accesos no autorizados.

2) **Garantizar Conectividad Confiable y Segura:**

- Configurar conexiones VPN para encriptar el tráfico entre las sucursales y la sede central, asegurando así la seguridad de la transmisión de datos.
- Implementar firewalls y sistemas de detección de intrusiones para proteger la red contra amenazas externas.

3) Asegurar la Integridad y Disponibilidad de los Datos:

- Establecer políticas de respaldo regulares y realizar pruebas de recuperación de desastres para garantizar la disponibilidad de los datos en caso de fallos o ataques.
- Utilizar servicios de almacenamiento centralizado en la nube o servidores locales con mecanismos de cifrado para proteger la información sensible.

4) Mantenimiento Proactivo y Actualización de Software:

- Implementar un plan de mantenimiento proactivo que incluya monitoreo continuo de la red, actualizaciones de software y parches de seguridad.
- Realizar auditorías regulares de seguridad para identificar y remediar posibles vulnerabilidades en el sistema.

5) Capacitación y Concienciación del Personal:

- Ofrecer programas de capacitación en seguridad cibernética para todo el personal, con énfasis en prácticas seguras de uso de tecnología y manejo de información confidencial.
- Fomentar una cultura de seguridad en toda la organización, promoviendo la importancia de proteger los activos de la empresa.

6) Cumplimiento Normativo:

- Asegurarse de que la infraestructura de TI cumpla con las regulaciones de seguridad y privacidad pertinentes, como GDPR y PCI DSS, para evitar posibles sanciones legales y pérdida de confianza de los clientes.

Verbo (V): Implementar

Variable (VI): Servicios globales en Windows Server 2019

Indicador (indicador): Nivel de mejora en la administración y seguridad lógica de la infraestructura de TI

Valor Deseado (VD): Mejora significativa en la protección de datos sensibles, mitigación de riesgos y garantía de la continuidad del negocio.

Entorno: Empresa MASS, dedicada a la venta de productos de primera necesidad a bajos precios, con sucursales distribuidas en múltiples ubicaciones y enfrentando desafíos de seguridad informática debido a la cantidad de datos confidenciales manejados y las vulnerabilidades en la gestión de acceso y en la seguridad de la red.

1.5. Antecedentes

Nivel Nacional

A nivel nacional, tenemos a Bermeo (2019) quien ha realizado una investigación en Tumbes - Perú, con el objetivo de implementar un sistema virtual para mejorar la gestión de los servicios TI de una empresa. Se aplicó una metodología cuantitativa, no experimental, descriptiva y transversal, usando como instrumento de medición un cuestionario que se aplicó a una muestra de 24 trabajadores. El cual obtuvo como resultado que el 100% de los participantes si necesitaban de una infraestructura virtual. Por lo que, llegó a la conclusión de que existe la necesidad de implementar la infraestructura virtual para la mejora de la gestión de servicios de TI de la empresa.

Así mismo, López (2019) hizo un estudio en Tumbes - Perú, con el objetivo de proponer mejoras en la red de datos gestionada con Windows Server de un centro de salud. Se aplicó una metodología cuantitativa, no experimental, con una muestra de 16 participantes. Sus resultados indicaron que el 63% de la muestra no se sentían contentos con el rendimiento de la red, mientras que un 81% consideró necesaria una mejora de la red de datos. Por lo que, concluyeron que estos hallazgos respaldan la necesidad de realizar cambios para optimizar la comunicación y la gestión de datos, lo que puede contribuir significativamente a la mejora continua de la calidad en el ámbito organizacional.

Además, Ticona y Mestanza (2023) hicieron una investigación en Perú, el cual tenía como objetivo mejorar la infraestructura tecnológica de la institución mediante el diseño y la implementación de los servicios de Windows Server, ante problemas recurrentes como fallos en conexiones, vulnerabilidades informáticas, entre otros, se propuso un cambio lógico en la red. Se aplicó la metodología MSF o Microsoft

Solution Framework para su estudio, el cual resultó en mejoras significativas en estabilidad, velocidad y seguridad de la red. De manera que, llegó a la conclusión de que la implementación mejoró significativamente la seguridad, administración de la red, asegurando una infraestructura de red óptima y segura para la institución.

Nivel Internacional

Respecto a nivel internacional, Eduard (2023) hizo una investigación en Bogotá - Colombia, el cual se centraba en la implementación de un servidor de dominio con Windows Server 2016 para una empresa, con el fin de simplificar la gestión de recursos de red y mejorar la seguridad de los datos. Se aplicó una metodología tradicional o en cascada, el cual resultó en una exploración desde la instalación inicial hasta la configuración detallada del servidor, reflejando su capacidad para ofrecer un control centralizado sobre la autenticación de usuarios y la aplicación de políticas de seguridad. Por lo que, llegó a concluir que la implementación del servidor de dominio contribuye a la mejora de la seguridad, eficiencia y gestión de red de una organización, de manera que la investigación es una guía práctica para diseñar, implementar y mantener una infraestructura de red robusta y confiable.

Por otra parte, Ardila y Daza (2020) hicieron una investigación en Bogotá - Colombia, el cual se centraba en verificar y mejorar el nivel de seguridad del Active directory de Windows Server, así mismo, se aplicó un método de estudio llamado Pen Testing White Box. Por lo que, se obtuvieron resultados donde la configuración predeterminada reveló vulnerabilidades, pero llegó a la conclusión de que al aplicar buenas prácticas, se reduce la exposición.

1.6. Teoría relacionada al tema

Los servicios globales en Windows Server 2019

Los servicios globales se refieren a funciones y servicios diseñados para proporcionar capacidades globales o de infraestructura en una red empresarial o en un entorno de servidor. Y en Windows Server 2019, destacan los siguientes:

- **Active Directory (AD):** Servicio de directorio que almacena información sobre objetos en una red, como usuarios, grupos, equipos y recursos

compartidos. Es fundamental para la autenticación y autorización en entornos empresariales de Windows.

- **DNS (Domain Name System):** Proporciona la resolución de nombres de dominio a direcciones IP y viceversa. Es esencial para la comunicación en redes TCP/IP y para acceder a recursos mediante nombres de dominio.
- **DHCP (Dynamic Host Configuration Protocol):** Permite la asignación automática de direcciones IP y configuraciones de red a dispositivos en una red. Facilita la administración de direcciones IP en una red y simplifica la configuración de dispositivos.
- **Servicios de archivo y almacenamiento:** Ofrece una variedad de servicios y características para el almacenamiento de archivos, incluidos Servicios de Archivos y Almacenamiento de Windows (FSRM), SMB (Server Message Block), y opciones de almacenamiento definido por software como Storage Spaces Direct.
- **Servicios de impresión:** Proporciona servicios para configurar y administrar impresoras en una red, permitiendo a los usuarios compartir impresoras y enviar trabajos de impresión desde diferentes dispositivos.
- **Servicios de implementación y actualización:** Incluye características para la implementación automatizada de sistemas operativos y aplicaciones, como Windows Server Update Services (WSUS) para la gestión de actualizaciones y Windows Deployment Services (WDS) para la implementación de sistemas operativos.
- **Servicios de seguridad:** Ofrece una serie de servicios y características de seguridad, incluido Windows Defender para protección contra malware y amenazas, y Windows Firewall para controlar el tráfico de red.
- **Servicios de acceso remoto:** Permite a los usuarios acceder de forma remota a recursos de red mediante protocolos como Remote Desktop Services (RDS) y VPN (Virtual Private Network)

Estos son algunos de los servicios globales más destacados en Windows Server 2019, pero hay muchos otros disponibles según las necesidades específicas de la red y la infraestructura empresarial.

La administración de infraestructura de TI

La administración de infraestructura de TI en Windows Server 2019 abarca una serie de prácticas y herramientas diseñadas para gestionar eficientemente los recursos de tecnología de la información dentro de una organización. Aquí hay algunas áreas clave de enfoque en la administración de infraestructura de TI en este entorno:

- **Administración de servidores:** Esto incluye la instalación, configuración y mantenimiento de servidores Windows Server 2019. Se trata de asegurar que los servidores estén correctamente configurados para cumplir con los requisitos de la organización, así como para garantizar su disponibilidad, rendimiento y seguridad.
- **Administración de Active Directory:** Active Directory es fundamental en un entorno de Windows Server para la gestión centralizada de usuarios, grupos, políticas de seguridad y recursos compartidos. La administración de Active Directory implica la creación, modificación y eliminación de objetos de directorio, así como la configuración de permisos y políticas.
- **Administración de redes:** Esto incluye la configuración y administración de servicios de red como DNS, DHCP, enrutamiento y servicios de acceso remoto. También implica monitorear el tráfico de red, optimizar el rendimiento y garantizar la seguridad de la red.
- **Administración de almacenamiento:** En Windows Server 2019, la administración de almacenamiento implica la configuración y gestión de soluciones de almacenamiento como Storage Spaces, Storage Spaces Direct y sistemas de archivos distribuidos. Esto incluye la asignación de espacio de almacenamiento, la configuración de redundancia y la implementación de políticas de almacenamiento.
- **Administración de seguridad:** La administración de seguridad implica la implementación y el mantenimiento de medidas de seguridad para proteger los recursos de TI contra amenazas como malware, intrusiones y acceso no autorizado. Esto puede incluir la configuración de firewalls, la implementación de políticas de seguridad, la gestión de certificados y el monitoreo de registros de eventos.
- **Administración de sistemas de copia de seguridad y recuperación:** Esto implica la configuración y administración de soluciones de copia de seguridad

y recuperación de desastres para proteger los datos críticos de la organización. Esto puede incluir la programación de copias de seguridad, la realización de pruebas de recuperación y la gestión de copias de seguridad fuera del sitio.

- **Administración de virtualización:** En entornos donde se utiliza la virtualización, la administración de infraestructura de TI también implica la gestión de hipervisores, máquinas virtuales y recursos virtuales. Esto puede incluir la creación, configuración, migración y monitorización de máquinas virtuales, así como la asignación de recursos.

La administración de infraestructura de TI en Windows Server 2019 abarca una amplia gama de actividades destinadas a garantizar que los recursos de TI de una organización sean eficientes, seguros y estén disponibles cuando se necesiten. Esto implica la gestión de servidores, redes, almacenamiento, seguridad, copias de seguridad y virtualización, entre otros aspectos.

La seguridad lógica de infraestructura de TI

La seguridad lógica de la infraestructura de TI se refiere a proteger los activos digitales y los datos de una organización mediante el uso de medidas y controles de seguridad específicos a nivel de software y configuración. En el contexto de Windows Server 2019, existen varias prácticas y herramientas que pueden utilizarse para garantizar la seguridad lógica de la infraestructura de TI:

- **Políticas de seguridad y control de acceso:** Establecer políticas de seguridad sólidas que regulen quién tiene acceso a qué recursos y datos en la red. Esto puede incluir la implementación de políticas de contraseñas fuertes, la configuración de permisos de usuario y grupo a nivel de archivo y carpeta, y la aplicación de políticas de seguridad de red.
- **Firewalls y reglas de filtrado:** Configurar firewalls en servidores Windows Server 2019 para controlar el tráfico de red entrante y saliente. Esto puede incluir la creación de reglas de filtrado para permitir o denegar ciertos tipos de tráfico según las necesidades de la organización.
- **Actualizaciones de seguridad:** Mantener los sistemas actualizados con los últimos parches de seguridad y actualizaciones de software es fundamental

para proteger contra vulnerabilidades conocidas. Windows Server 2019 ofrece herramientas como Windows Update Services (WSUS) para gestionar y distribuir actualizaciones de seguridad de manera centralizada.

- **Antivirus y antimalware:** Instalar software antivirus y antimalware en los servidores para detectar y eliminar amenazas de malware. Windows Server 2019 incluye Windows Defender como una solución antivirus integrada que puede proporcionar una capa adicional de protección.
- **Auditoría y registro de eventos:** Habilitar la auditoría y el registro de eventos en los servidores para realizar un seguimiento de las actividades de usuario y detectar posibles intrusiones o actividades maliciosas. Windows Server 2019 ofrece funciones de auditoría avanzadas que permiten registrar eventos específicos y generar informes detallados de actividad.
- **Cifrado de datos:** Utilizar el cifrado para proteger datos confidenciales tanto en reposo como en tránsito. Windows Server 2019 admite el cifrado de unidades con BitLocker y el cifrado de datos en redes con protocolos como HTTPS y Protocolo de escritorio remoto seguro (RDPS).
- **Control de acceso basado en roles (RBAC):** Implementar controles de acceso basados en roles para restringir el acceso a recursos y funcionalidades del sistema según la función y los privilegios del usuario. Esto ayuda a limitar el riesgo de acceso no autorizado a datos y sistemas críticos.
- **Detección y respuesta ante incidentes (EDR):** Implementar soluciones de detección y respuesta ante incidentes para identificar y responder a amenazas en tiempo real. Estas soluciones pueden ayudar a detectar actividades maliciosas y tomar medidas correctivas rápidas para mitigar el impacto.

Al implementar estas medidas y controles de seguridad lógica en Windows Server 2019, las organizaciones pueden fortalecer la protección de su infraestructura de TI y reducir el riesgo de brechas de seguridad y ataques cibernéticos.

REFERENCIAS BIBLIOGRÁFICAS

Ardila-Flórez, C. D. & Daza-Castro, J. A. (2020). Verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Ingeniería. Programa de Ingeniería de Sistemas. Especialización en Seguridad de la Información. Bogotá, Colombia. https://repository.ucatolica.edu.co/entities/publication/b4f480d5-45b7-4d38-a0fb-a24f8e85df01

Bermeo Oyola, J. C. (2019). Implementación de una Infraestructura virtual para mejorar la gestión de los servicios TI de La empresa Complex del Perú S.A.C.-Tumbes; 2019. https://repositorio.uladech.edu.pe/handle/20.500.13032/11055

Chavarria, L., & Rubio, N. (2021). *Arquitectura de seguridad de la información para la protección de activos digitales en Pymes* [Universidad Peruana de Ciencias Aplicadas]. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/657808/ChavarriaA_L.pdf?sequence=3

Edward (2023). Implementación de servidor de dominio Windows Server 2016. https://repository.universidadean.edu.co/handle/10882/12972

López, J. (2019). Propuesta de mejora en la red de datos administrada con windows server en el Centro de Salud Global – Tumbes; 2019. https://repositorio.uladech.edu.pe/handle/20.500.13032/11928

Gustavo, B. (2019, enero 18). ¿Qué es un CMS? Definición, funciones y ejemplos. Tutoriales Hostinger. https://www.hostinger.es/tutoriales/que-es-un-cms

Ticona, I. H. y Mestanza, C. A. (2023). Implementación y Diseño de Servicios de Red con Windows Server realizados a una Institución del Estado. https://repositorioacademico.upc.edu.pe/handle/10757/670351

Torres, C. (2020). PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A [Universidad Técnica De Ambato]. https://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf