UNIVERSIDAD TECNOLÓGICA DE TECAMACHALCO

TECNOLOGÍAS DE LA INFORMACIÓN

A S I G N A T U R A

D I R E C C I Ó N D E P R O Y E C T O S I I

U N I D A D I

P R O Y E C T O : S E R V I D O R M I K R O T I K P C

DOCENTE:

JUAN CARLOS REYES PEDRAZA

ESTUDIANTES:

FATIMA TEHUINTLE AMAYO
MAURO LARA ARENAS
JOSÉ ALBERTO CAMPOS MÉNDEZ
NELLY JOYCE HERNÁNDEZ CRUZ

9° "A"
TIC ÁREA – (INFRAESTRUCTURA DE REDES INTELIGENTES Y CIBERSEGURIDAD)

CUATRIMESTRE MAYO – AGOSTO 2024

Contenido

Introducción 2

1. Lista de entregables desarrollados 3

2. Descripción de cada entregable 3

3. Informe desempeño del proyecto 3

3.1 Análisis del desempeño pasado 3

3.2 Estado actual de los riesgos e incidentes 4

3.3 Trabajo completado durante el periodo reportado 7

3.4 Resumen de cambios aprobados en el período 8

3.5 Resultado del análisis de variación 8

4. Reporte de actividades de aseguramiento de la calidad. 12

5. Evaluaciones de desempeño del equipo de trabajo 13

6. Análisis y evaluación de nuevos riesgos. 15

7. Registro de incidentes del proyecto. 17

8. Registro de cambios implementados 17

9. Solicitudes de cambio 18

10. Mediciones de valor ganado del proyecto 18

11. Pronósticos y proyecciones del proyecto 19

12. Reportes de auditorías 19

Conclusión 30

Bibliografías 31

Introducción

En el ámbito de las redes informáticas y telecomunicaciones, la implementación de servidores MikroTik PC representa un componente fundamental para la gestión eficiente y segura de redes. Estos servidores, basados en hardware estándar de PC y potenciados por el robusto sistema operativo RouterOS de MikroTik, permiten una amplia gama de funciones que van desde el enrutamiento avanzado hasta la gestión de ancho de banda y la seguridad de redes.

El desarrollo de un servidor MikroTik PC responde a la necesidad creciente de empresas y organizaciones por optimizar la gestión de sus redes, asegurando un rendimiento óptimo, alta disponibilidad y seguridad robusta. Este proyecto no solo implica la configuración y puesta en marcha de hardware y software especializado, sino también la implementación de políticas de seguridad y calidad de servicio (QoS) que garanticen una experiencia de red fluida y segura para todos los usuarios.

1. Lista de entregables desarrollados

2. Descripción de cada entregable

No.	Entregables	Descripción del Proyecto
1	Servidor PC	Un equipo físico que cumpla con las especificaciones necesarias para funcionar como un servidor.
2	Tarjetas de red	Interfaces de red adicionales para soportar múltiples conexiones.
3	Fuente de alimentación y componentes de enfriamiento.	Asegurar la estabilidad y el rendimiento del servidor.
4	Router OS	Instalación y configuración de software de enrutamiento que emule o se base en RouterOS de Mikrotik (como pfSense, OpenWrt, o una versión personalizada de Linux).
5	Manual del Usuario	Guía detallada para los usuarios finales sobre cómo utilizar y gestionar el servidor.
6	Documentación Técnica	Instrucciones detalladas sobre la instalación, configuración, y mantenimiento del hardware y software.
7	Plan de Proyecto	Documento que detalla las fases del proyecto, cronograma, y recursos necesarios.
8	Informes de Pruebas	Resultados de las pruebas de rendimiento y seguridad realizadas en el servidor.

3. Informe desempeño del proyecto

3.1 Análisis del desempeño pasado

Al interactuar con los equipos miKrotik se encontraron ciertas delimitantes de estos equipos, en su procesador, en su capacidad de administrar usuarios, un almacenamiento no estable.

Equipos más económicos no ofrecen opción de expansión como puertos adicionales o módulos de expansión limitando su uso en redes en crecimiento.

Aunque MiKrotik cuenta con una comunidad activa, el soporte técnico no puede ser tan robusto como el ofrecimiento de resolución de problemas con especialistas en este ámbito.

Los dispositivos Mikrotik varían significativamente en términos de CPU. Equipos de gama baja pueden tener procesadores con menos núcleos y menor velocidad, lo que limita su capacidad para manejar tráfico pesado o realizar tareas complejas.

La cantidad de RAM afecta directamente la capacidad de manejar múltiples conexiones simultáneas y procesos intensivos en memoria, como listas de control de acceso extensas o grandes tablas de enrutamiento.

Aunque muchos routers Mikrotik no requieren grandes cantidades de almacenamiento, aquellos utilizados para servicios como el proxy web o el almacenamiento de logs sí pueden verse limitados por la capacidad de almacenamiento interno.

3.2 Estado actual de los riesgos e incidentes

Riesgos de Hardware

Fallas de Hardware

- Riesgo: Los componentes del PC (CPU, RAM, disco duro, fuentes de poder) pueden fallar, causando interrupciones en el servicio.
- Solución: Seleccionar hardware de alta calidad y confiabilidad. Implementar redundancia en componentes críticos y tener piezas de repuesto disponibles.

Compatibilidad de Componentes

- Riesgo: No todos los componentes de hardware pueden ser totalmente compatibles con RouterOS.
- Solución: Verificar la compatibilidad del hardware con RouterOS antes de la adquisición. Consultar la documentación y foros de Mikrotik para identificar componentes probados y recomendados.

Riesgos de Software

Problemas de Instalación y Configuración

- Riesgo: Dificultades durante la instalación de RouterOS en un PC pueden llevar a una configuración incorrecta o incompleta.
- Solución: Seguir guías oficiales y tutoriales detallados de instalación. Realizar pruebas en un entorno de prueba antes de la implementación final.

Vulnerabilidades de Seguridad

- Riesgo: Vulnerabilidades en RouterOS pueden ser explotadas por atacantes, comprometiendo la seguridad del servidor.
- Solución: Mantener RouterOS actualizado con los últimos parches de seguridad. Configurar adecuadamente las políticas de seguridad y realizar auditorías regulares.

Riesgos Operativos

Sobrecarga de Recursos

- Riesgo: Uso excesivo de CPU, memoria o almacenamiento puede degradar el rendimiento del servidor.
- Solución: Monitorizar constantemente el uso de recursos. Planificar la capacidad y optimizar las configuraciones para evitar sobrecargas. Escalar el hardware si es necesario.

Errores Humanos

- Riesgo: Configuraciones incorrectas o cambios no documentados pueden causar fallos en la red.
- Solución: Implementar controles de cambios estrictos y realizar pruebas antes de aplicar cambios en producción. Capacitar adecuadamente al personal técnico.

Riesgos de Conectividad

Interferencias y Problemas de Señal (para Dispositivos Inalámbricos)

- Riesgo: Interferencias de otras redes o dispositivos pueden afectar la calidad de la conexión inalámbrica.
- Solución: Realizar estudios de sitio para identificar interferencias y ajustar canales y potencias de transmisión adecuadamente. Utilizar tecnologías avanzadas como el beamforming.

Problemas de Enrutamiento y Configuración de Red

- Riesgo: Errores en la configuración de enrutamiento pueden llevar a pérdida de conectividad o bucles de red.
- Solución: Realizar revisiones exhaustivas de la configuración de enrutamiento. Implementar protocolos de enrutamiento redundantes y mecanismos de protección contra bucles.

Riesgos de Mantenimiento y Actualización

Problemas Durante Actualizaciones de Firmware/Software

- Riesgo: Actualizaciones pueden fallar o introducir nuevos errores y vulnerabilidades.
- Solución: Probar las actualizaciones en un entorno de prueba antes de implementarlas en producción.

Falta de Mantenimiento Regular

- Riesgo: No realizar mantenimiento regular puede llevar a acumulación de problemas que eventualmente causan fallos.
- Solución: Establecer un calendario de mantenimiento regular que incluya revisiones de seguridad, actualizaciones y limpieza física del hardware.

Riesgos de Escalabilidad y Crecimiento

Crecimiento No Planeado de la Red

- Riesgo: Un aumento inesperado de dispositivos o tráfico puede sobrecargar el servidor y reducir el rendimiento.
- Solución: Planificar la escalabilidad de la red y monitorizar el crecimiento de tráfico. Implementar soluciones de balanceo de carga y optimización del tráfico.

Riesgos de Compatibilidad

Incompatibilidad con Otros Dispositivos de Red

- Riesgo: Problemas de compatibilidad con otros dispositivos o software pueden causar interrupciones o baja performance.
- Solución: Verificar las especificaciones y realizar pruebas de compatibilidad antes de integrar nuevos dispositivos o software en la red.

Estrategias Generales de Mitigación

- Monitoreo Continuo: Implementar sistemas de monitoreo para vigilar el estado y el rendimiento del servidor en tiempo real.
- Capacitación: Asegurar que el personal esté bien capacitado en la configuración, operación y mantenimiento del servidor Mikrotik en PC.
- Documentación: Mantener documentación detallada de las configuraciones, cambios y procedimientos de emergencia.
- Planificación de Contingencia: Desarrollar y mantener planes de contingencia y recuperación ante desastres para minimizar el impacto de cualquier incidente.

3.3 Trabajo completado durante el periodo reportado

Actividad 1. Investigación de requisitos de Hardware

Requisitos de Hardware

- PC o Servidor: Un equipo con suficientes recursos (CPU, RAM, almacenamiento) según las necesidades de la red.
- Tarjetas de Red: Al menos dos interfaces de red, una para la conexión WAN y otra para la LAN. Pueden ser tarjetas Ethernet o interfaces Wi-Fi compatibles.
- Medio de Instalación: Un USB o CD/DVD para instalar RouterOS.

Actividad 2. Investigación de instalación

Pasos para la Instalación

Descargar RouterOS:

- Visitar el sitio web oficial de MikroTik y descargar la versión ISO de RouterOS.

Crear Medio de Instalación:

- Utilizar herramientas como Rufus (para USB) o cualquier software de grabación de discos para crear el medio de instalación.
- Iniciar la herramienta y seguir las instrucciones para crear un medio de arranque con la ISO descargada.

Configuración del BIOS:

- Acceder al BIOS del servidor y configurar el arranque desde el dispositivo USB o CD/DVD.
- Asegurarse de que el arranque seguro (Secure Boot) esté deshabilitado si se utiliza un medio USB.

Instalación de RouterOS:

- Conectar el medio de instalación al PC y reiniciar.
- Seguir las instrucciones en pantalla para instalar RouterOS. Seleccionar las particiones y configuraciones necesarias.
- Finalizada la instalación, el sistema pedirá reiniciar y arrancará en RouterOS.

Configuración Inicial:

- Acceder a RouterOS a través de Winbox (herramienta de administración de MikroTik) o mediante terminal (SSH o consola).

- Configurar las interfaces de red: asignar direcciones IP, establecer reglas de firewall, configurar NAT, etc.

3.4 Resumen de cambios aprobados en el período

El objetivo de este resumen es documentar los cambios aprobados durante el período especificado para el desarrollo del servidor Mikrotik PC. Este resumen incluye detalles sobre cada cambio, su impacto esperado y la justificación para su aprobación.

(Hasta el momento no se ha realizado algún cambio)

3.5 Resultado del análisis de variación

Variaciones Anticipadas

Uso de CPU

- **Expectativa**: Se espera que el uso de CPU varíe significativamente durante las horas pico debido a la carga de trabajo de los usuarios.
- **Anticipación de Variación**: Incrementos del 60% al 80% durante las horas pico, con disminuciones al 20%-30% durante las horas no pico.
- **Medidas de Mitigación**: Implementación de optimización de procesos y distribución de carga.

Uso de Memoria RAM

- **Expectativa**: Uso elevado y constante de RAM debido a las aplicaciones y servicios ejecutados.
- **Anticipación de Variación**: Mantenerse entre el 60% y el 80%, con picos hasta el 90%.
- **Medidas de Mitigación**: Considerar la opción de aumentar la capacidad de RAM si es necesario.

Uso de Ancho de Banda

- **Expectativa**: Variación significativa en el uso de ancho de banda durante el día, con picos durante las horas de trabajo.
- **Anticipación de Variación**: Uso de ancho de banda entre 50 Mbps y 200 Mbps durante picos.
- **Medidas de Mitigación**: Implementar políticas de calidad de servicio (QoS) para gestionar y optimizar el uso de ancho de banda.

Latencia de Red

- **Expectativa**: Latencia moderada durante operaciones normales, con incrementos durante picos de tráfico.
- **Anticipación de Variación**: Latencia promedio entre 10 ms y 30 ms, con picos hasta 50 ms.
- **Medidas de Mitigación**: Optimización de la configuración de red y QoS para minimizar la latencia durante picos.

Tasa de Paquetes Perdidos

- **Expectativa**: Baja tasa de pérdida de paquetes, con incrementos durante los picos de tráfico.
- **Anticipación de Variación**: Pérdida de paquetes menor al 1%, con picos hasta 2%.
- **Medidas de Mitigación**: Revisar y optimizar la configuración de red para minimizar la pérdida de paquetes.

3.6 Conclusión proyectada del proyecto (incluido el tiempo y el costo)

Objetivo del Proyecto

Desarrollar e implementar un servidor Mikrotik PC para gestionar y optimizar la red, proporcionando un servicio de alta calidad y confiabilidad a los usuarios.

Alcance del Proyecto

Objetivos Específicos

- Configurar un servidor Mikrotik PC robusto y eficiente.
- Garantizar la estabilidad y seguridad de la red.
- Monitorear el rendimiento del servidor y la red.
- Implementar políticas de calidad de servicio (QoS) y gestión de tráfico.

Entregables Principales

- Servidor Mikrotik PC completamente configurado y operando.
- Documentación de configuración y operación del servidor.
- Informes de monitoreo y análisis de rendimiento.
- Plan de mantenimiento y soporte técnico.

Recursos y Requisitos

Hardware Requerido

- **Procesador**: AMD Sempron™ 2.80 GHz
- **Memoria RAM**: 2 GB
- **Almacenamiento**: 200 GB HDD
- **Tarjeta de Red**: Compatible con Mikrotik RouterOS

Software Requerido

- **Sistema Operativo**: Mikrotik RouterOS (última versión estable)
- **Herramientas de Monitoreo**: The Dude, MRTG, PRTG, Zabbix, winbox.

Plan de Trabajo y Cronograma

Fases del Proyecto

1. **Fase de Planificación (2 semanas)**
    - Definición de objetivos y alcance.
    - Revisión de requisitos de hardware y software.
    - Asignación de roles y responsabilidades.
    - Desarrollo del plan de proyecto detallado.
2. **Fase de Adquisición (1 semana)**
    - Adquisición de hardware y software necesarios.
    - Verificación de compatibilidad y calidad del equipo.
3. **Fase de Implementación (4 semanas)**
    - Instalación de Mikrotik RouterOS.
    - Configuración inicial del servidor.
    - Implementación de políticas de QoS y seguridad.
    - Pruebas de rendimiento y estabilidad.
4. **Fase de Monitoreo y Ajustes (2 semanas)**
    - Configuración de herramientas de monitoreo.

- Análisis de variaciones y ajustes necesarios.
- Documentación de configuraciones y procedimientos.

5. **Fase de Capacitación y Entrega (1 semana)**
    - Capacitación del personal de soporte y administración.
    - Entrega de documentación y manuales de usuario.
    - Validación de cumplimiento de objetivos y cierre del proyecto.

Costos de Hardware

1. **Procesador**
    - AMD Sempron™ 2.80 GHz
    - Costo Aproximado: $40 USD
    - Costo en MXN: $680 MXN
2. **Memoria RAM**
    - 2 GB DDR3 RAM
    - Costo Aproximado: $20 USD
    - Costo en MXN: $340 MXN
3. **Almacenamiento**
    - 200 GB HDD
    - Costo Aproximado: $30 USD
    - Costo en MXN: $510 MXN
4. **Tarjeta de Red**
    - Compatible con Mikrotik RouterOS
    - Costo Aproximado: $15 USD
    - Costo en MXN: $255 MXN
5. **Otros Componentes**
    - Caja/Torre
    - Fuente de Alimentación

- Ventiladores/Cooling
- Costo Aproximado Total: $50 USD
- Costo en MXN: $850 MXN

Total, de Costos de Hardware: $2,635 MXN

Costos de Software

1. **Sistema Operativo**
    - Mikrotik RouterOS (Licencia Nivel 4)
    - Costo Aproximado: $45 USD
    - Costo en MXN: $765 MXN
2. **Herramientas de Monitoreo**
    - The Dude (Gratis)
    - MRTG, PRTG, Zabbix (Gratis para versiones básicas o pruebas)
    - Costo Total Aproximado: $0 USD
    - Costo en MXN: $0 MXN

Total, de Costos de Software: $765 MXN

Concepto	Costo en USD	Costo en MXN
Hardware	$155	$2,635
Software	$45	$765
Total	$200	$3,400

4. Reporte de actividades de aseguramiento de la calidad.

Evaluar la calidad de un servidor Mikrotik PC de acuerdo con normas y estándares específicos implica un enfoque sistemático que abarca múltiples aspectos, desde la seguridad y la gestión hasta el rendimiento y la operatividad.

Seguridad

ISO/IEC 27001:2013

Implementación de un SGSI: Verificar que exista un Sistema de Gestión de Seguridad de la Información formalmente establecido, documentado y mantenido.

Evaluación de riesgos: Realizar una evaluación de riesgos periódica y documentar las medidas de mitigación adoptadas.

NIST SP 800-53

Controles de seguridad: Implementar y auditar controles específicos como autenticación multifactor, cifrado de datos en tránsito y reposo, y auditorías de acceso.

Monitoreo continuo: Establecer sistemas de monitoreo continuo para detectar y responder a incidentes de seguridad.

Calidad

ISO 9001:2015

Sistema de gestión de calidad: Establecer y mantener un SGC que cubra todos los aspectos operativos del servidor, incluyendo planificación, operación, verificación y mejora.

Auditorías internas: Realizar auditorías internas regulares para evaluar la conformidad con los procedimientos de calidad establecidos.

Redes y Comunicaciones

IEEE 802.1X

Autenticación de red: Implementar autenticación basada en puertos para controlar el acceso a la red.

Seguridad de red: Verificar que las configuraciones de red cumplan con las mejores prácticas de seguridad.

Indicadores de Calidad

1. Disponibilidad: Mantener un tiempo de actividad (uptime) del servidor acorde con los acuerdos de nivel de servicio (SLA).
2. Rendimiento: Monitorear y optimizar el rendimiento del servidor para asegurar una respuesta rápida y eficiente.
3. Cumplimiento: Evaluar el cumplimiento con todas las normas y regulaciones aplicables.
4. Seguridad: Medir la efectividad de los controles de seguridad implementados y la capacidad de respuesta ante incidentes.
5. Satisfacción del usuario: Recoger y analizar la retroalimentación de los usuarios para evaluar su satisfacción con los servicios proporcionados por el servidor.

5. Evaluaciones de desempeño del equipo de trabajo

Objetivos de la Evaluación de Desempeño

Las evaluaciones de desempeño del equipo de trabajo tienen los siguientes objetivos:

- **Medir la eficiencia y efectividad del equipo** durante las diferentes fases del proyecto.
- **Identificar áreas de mejora** y brindar retroalimentación constructiva.
- **Fomentar el desarrollo profesional** y el aprendizaje continuo.
- **Asegurar que los objetivos del proyecto se cumplan** dentro del presupuesto y del cronograma establecido.

Criterios de Evaluación

Se utilizarán los siguientes criterios para evaluar el desempeño de cada miembro del equipo:

1. **Cumplimiento de Objetivos**
    - Entrega de tareas dentro de los plazos establecidos.
    - Calidad y precisión de las entregas.
2. **Conocimiento Técnico y Habilidades**
    - Competencia en el uso de herramientas y tecnologías relevantes.
    - Capacidad para resolver problemas técnicos.
3. **Trabajo en Equipo y Colaboración**
    - Capacidad para trabajar de manera efectiva con otros miembros del equipo.
    - Contribuciones a la discusión y resolución de problemas del equipo.
4. **Comunicación**
    - Claridad y efectividad en la comunicación oral y escrita.
    - Proactividad en la comunicación de problemas y avances.
5. **Adaptabilidad y Flexibilidad**
    - Capacidad para adaptarse a cambios en los requisitos del proyecto.
    - Manejo efectivo de situaciones imprevistas.
6. **Innovación y Proactividad**
    - Aportación de ideas innovadoras y mejoras.
    - Iniciativa para tomar responsabilidades adicionales cuando sea necesario.

Metodología de Evaluación

1. **Evaluaciones Periódicas**

    - **Frecuencia**: Mensualmente.
    - **Formato**: Reuniones uno a uno entre el evaluador y el evaluado.
    - **Contenido**: Revisión del desempeño basado en los criterios establecidos, retroalimentación constructiva y establecimiento de objetivos para el próximo período.

2. **Autoevaluación**

    - **Frecuencia**: Al finalizar cada fase del proyecto.
    - **Formato**: Cuestionario de autoevaluación donde el miembro del equipo evalúa su propio desempeño.

6. Análisis y evaluación de nuevos riesgos.

Desarrollar y mantener un servidor Mikrotik PC implica diversos riesgos que pueden afectar su seguridad, rendimiento y operatividad. Identificar estos riesgos y tomar medidas preventivas es esencial para asegurar la calidad y continuidad del servicio.

- **Riesgos de Seguridad**

Vulnerabilidades en el Software

Fallos de seguridad en el sistema operativo Mikrotik o en el software de terceros. Mantener el software actualizado, aplicar parches de seguridad tan pronto como estén disponibles, y utilizar configuraciones seguras basadas en benchmarks como los de CIS.

- **Riesgos de Rendimiento**

Sobrecarga del Sistema

Exceso de carga en CPU, memoria, o ancho de banda que puede degradar el rendimiento del servidor. Monitorear continuamente el uso de recursos, optimizar configuraciones de red, y planificar la capacidad para el futuro crecimiento.

Malas Configuraciones de Red

Configuraciones de red incorrectas que pueden causar problemas de rendimiento o interrupciones. Seguir mejores prácticas de configuración, realizar pruebas exhaustivas antes de implementar cambios, y mantener una documentación clara de la configuración de la red.

- **Riesgos de Disponibilidad**

Fallas de Hardware

Fallos en componentes físicos como discos duros, fuentes de alimentación, o ventiladores. Implementar redundancia en componentes críticos, realizar mantenimiento preventivo regular, y tener repuestos disponibles.

Interrupciones de Energía

Cortes de energía que pueden causar apagones del servidor. Utilizar fuentes de alimentación ininterrumpida (UPS) y generadores de respaldo, y asegurar que el entorno de operación tenga un suministro eléctrico estable.

- **Riesgos Operativos**

Errores Humanos

Configuraciones incorrectas, borrado accidental de datos, o implementación de cambios sin pruebas adecuadas. Capacitar adecuadamente al personal, implementar procedimientos de control de cambios, y mantener un registro detallado de todas las operaciones realizadas.

Falta de Monitoreo y Alertas

Falta de detección temprana de problemas debido a la ausencia de sistemas de monitoreo y alertas. Implementar herramientas de monitoreo en tiempo real, establecer umbrales de alerta, y revisar regularmente los registros y métricas de rendimiento.

- **Riesgos de Cumplimiento y Legales**

No Cumplimiento de Normativas

Incumplimiento de regulaciones y estándares de la industria que puede resultar en sanciones legales. Mantenerse actualizado con las normativas aplicables, realizar auditorías de cumplimiento regularmente, y documentar todas las políticas y procedimientos de seguridad.

Matriz de riesgos

Riesgo	PO	CR	PO*CR	Estrategia
Cambios de los requisitos	0.3	7	2.1	Mitigar
Incompatibilidad de Sistema	0.4	6	2.4	Mitigar
Fallo en pruebas	0.4	6	2.4	Mitigar
Problemas de desempeño	0.3	5	1.5	Mitigar
Usabilidad de usuario	0.5	4	2.0	Mitigar
Retraso en entregas	0.2	7	1.0	Evitar
Vulnerabilidad del equipo	0.3	8	2.4	Mitigar

7. Registro de incidentes del proyecto.

Objetivo del Registro de Incidentes

Documentar y analizar los incidentes que ocurren durante el desarrollo del servidor Mikrotik PC para identificar causas, soluciones y acciones preventivas, asegurando la mejora continua del proyecto.

Incidente: Retraso en la Entrega de Hardware

- **Fecha del Incidente**: 13/06/2024
- **Descripción**: La entrega del procesador AMD Sempron™ 2.80 GHz y la memoria RAM se retrasó debido a problemas de suministro del proveedor.
- **Impacto**: Retraso de una semana en la fase de instalación y configuración inicial.
- **Acciones Tomadas**:
    - Contacto con el proveedor para obtener una nueva fecha de entrega.
    - Ajuste del cronograma del proyecto para acomodar el retraso.
- **Acciones Preventivas**:
    - Establecer un contrato con penalizaciones por retrasos.
    - Mantener un inventario mínimo de hardware crítico.
- **Estado**: Resuelto

Fecha	Incidente	Impacto	Acciones Tomadas	Estado
13/06/2024	Retraso en la Entrega de Hardware	Retraso de una semana	Contacto con proveedor, ajuste de cronograma	Resuelto

8. Registro de cambios implementados

Objetivo del Registro de Cambios

Documentar todos los cambios aprobados e implementados durante el desarrollo del servidor Mikrotik PC, asegurando un seguimiento detallado y una gestión efectiva de los cambios.

(Hasta el momento no se ha realizado algún cambio)

9. Solicitudes de cambio

Aumentar la Seguridad

- Firewall Avanzado: Implementar reglas de firewall más estrictas y específicas para proteger la red contra ataques.
- IDS/IPS: Integrar un sistema de detección y prevención de intrusiones para identificar y mitigar amenazas.
- Seguridad VPN: Mejorar la configuración de VPN con cifrado más fuerte y autenticación de dos factores.

Mejorar el Rendimiento

- Ajuste de QoS: Configurar Quality of Service (QoS) para priorizar el tráfico crítico y mejorar la calidad de servicios como VoIP y videoconferencias.
- Balanceo de Carga: Implementar balanceo de carga para distribuir el tráfico de red de manera más eficiente y evitar sobrecargas.
- Optimización del Hardware: Actualizar componentes de hardware, como agregar más memoria RAM o un SSD más rápido.

Ampliar la Funcionalidad

- Redundancia y Alta Disponibilidad: Configurar una configuración de alta disponibilidad (HA) con un segundo servidor para asegurar continuidad de servicio en caso de falla.
- VLANs y Segmentación: Crear VLANs adicionales para segmentar mejor la red y mejorar la gestión del tráfico y la seguridad.

Actualizaciones y Mantenimiento

- Actualizaciones Automáticas: Configurar actualizaciones automáticas del RouterOS y otros componentes de software.
- Plan de Mantenimiento: Establecer un plan de mantenimiento regular para revisar y actualizar configuraciones, firmware y hardware.
- Backup y Recuperación: Implementar una estrategia robusta de respaldo y recuperación para asegurar que los datos y configuraciones estén protegidos.

10. Mediciones de valor ganado del proyecto

Valor Planificado (PV)						
Tarea	**Duración (días)**	**Costo Planificado**	**Fecha de Inicio**	**Fecha de Fin**	**Costo Real**	**% Completado**
Planificación	5	1000	27/05/2024	07/06/2024	900	100%
Adquisición	7	2000	10/06/2024	14/06/2024	1500	100%

Instalación	10	2000	24/06/2024	28/06/2024	2000	50%
Configuración	8	2000	01/07/2024	12/07/2024	1000	30%
Pruebas y Ajustes	5	2000	22/07/2024	26/07/2024	0	25%

11. Pronósticos y proyecciones del proyecto

PV Total hasta el 26/07/2024:

PV Total = $900 (Planificación) + $1500 (Adquisición) + $2000 (Instalación) + $1000 (Configuración) + $0 (Pruebas y Ajustes)

PV Total = $5400

Por lo tanto, el Valor Planificado (PV) del proyecto de servidores MikroTik PC hasta el 26/07/2024 es de $5400.

12. Reportes de auditorías

1. Información General

Objetivo de la Auditoría: Evaluar la configuración actual, seguridad, rendimiento y procesos de desarrollo relacionados con el servidor MikroTik PC.

Fecha de la Auditoría: viernes 2 de agosto del 2024

Auditor: José Alberto Campos Méndez

Ubicación: Tecamachalco, Puebla

2. Alcance de la Auditoría

Componentes Auditados:

- Configuración de RouterOS
- Seguridad de la red
- Rendimiento del hardware
- Logs y monitoreo
- Procesos de desarrollo y despliegue

3. Metodología

- Revisión Documental: Análisis de la documentación y configuraciones existentes.
- Verificación en Sitio: Inspección física y revisión directa del equipo y su configuración.

- Entrevistas: Conversaciones con el equipo de desarrollo para entender los procesos y prácticas.
- Pruebas y Diagnósticos: Ejecución de pruebas de conectividad, seguridad y rendimiento.

4. Hallazgos y Observaciones

4.1 Configuración de RouterOS

Configuración IP: 192.168.1.0

IP pública: Sin dirección por el momento

IP privada: Sin dirección por el momento

Subred: 255.255.255.0

Interfaces y VLANs:

Interfaces activas: (Lista de interfaces)

VLAN configuradas:

Configuración de DHCP:192.168.1.0/24

DHCP Server activo: Sí

Rango de IPs: 192.168.1.0/24

4.2 Seguridad de la Red

Firewall y Reglas:

Reglas configuradas: (Lista de reglas)

Reglas de filtrado: (Detalles de filtrado)

VPN Configuración:

Tipo de VPN: [PPTP/L2TP/IPsec]

Usuarios configurados: (Lista de usuarios)

Actualización del Software:

Versión actual de RouterOS: (Versión)

Última actualización: (Fecha de actualización)

4.3 Rendimiento del Hardware

Estado del Hardware:

CPU: procesador sempron 2.5 ghz

Memoria RAM: 2 de ram

Disco Duro: 250 GB

Monitoreo de Recursos:

Uso de ancho de banda: 100 Mg

Conexiones activas: 2

5. Conclusiones y Recomendaciones

Conclusiones:

- Estado general del servidor MikroTik PC.
- El equipo se encuentra trabajando de manera correcta de tanta manera física y lógica

Recomendaciones:

- Fortalecer Seguridad: Revisar y actualizar las reglas del firewall.
- Optimizar Configuración de DHCP: Ajustar el rango de IPs y excluir IPs reservadas.
- Mejorar Procesos de Desarrollo: Implementar prácticas de integración continua y despliegue automatizado.
- Implementar Monitoreo Continuo: Configurar alertas para eventos críticos.

6. Acciones Correctivas y Plan de Seguimiento

Fecha de próxima auditoría: 10/agosto/2024

Objetivos y metas a revisar en la próxima auditoría.

Revisión compleja del servidor

Firma del Auditor: _____

Fecha: _____

13. Cambios aprobados

Aumentar la Seguridad	**Mejorar el Rendimiento**	**Ampliar la Funcionalidad**	**Actualizaciones y Mantenimiento**	**Aprobación**
Firewall Avanzado	Ajuste de QoS	Redundancia y Alta Disponibilidad	Actualizaciones Automáticas	Si
IDS/IPS	Balanceo de Carga	VLANs y Segmentación	Plan de Mantenimiento	Si

Seguridad VPN	Optimización del Hardware		Backup y Recuperación	Si

14. Reportes de desempeño del control de la calidad

Objetivo del reporte:

Evaluar el desempeño del control de calidad en el servidor MikroTik PC.

Configuración del Control de Calidad

QoS (Quality of Service): Se han configurado colas de prioridad para asegurar el ancho de banda para VoIP y aplicaciones críticas.

Firewall y reglas: Reglas de firewall implementadas para filtrar tráfico no deseado y asegurar el control de calidad.

Scripts y programación: Se utiliza un script para monitorear y ajustar dinámicamente las colas de QoS según la carga de red.

Datos Recogidos

Análisis de tráfico: El tráfico promedio antes de la implementación de QoS era de 100 Mbps. Después de la implementación, el tráfico se ha estabilizado en un promedio de 90 Mbps, con picos ocasionales hasta 95 Mbps.

Latencia y jitter: La latencia promedio antes era de 50 ms, y ahora se mantiene en promedio 30 ms. El jitter se redujo de 20 ms a 5 ms en promedio.

Pérdida de paquetes: Antes de QoS, la pérdida de paquetes era del 2%. Con QoS implementado, la pérdida de paquetes se ha reducido al 0.5% en condiciones normales de carga.

Ancho de banda: Distribución del ancho de banda mejorada, con asignación efectiva para VoIP y aplicaciones críticas.

Análisis de Desempeño

Comparación con estándares: Los resultados cumplen con los estándares recomendados para una red de oficina pequeña.

Identificación de cuellos de botella: Se identificó que ciertos picos de tráfico aún pueden causar congestión temporalmente. Se recomienda ajustar las colas de QoS para manejar mejor estos eventos.

Impacto de las configuraciones: La implementación de QoS ha mejorado significativamente la calidad del servicio para aplicaciones sensibles al retraso.

Recomendaciones

Ajustes necesarios: Ajustar las colas de QoS para manejar mejor los picos de tráfico.

Mejoras en la infraestructura: Considerar actualizaciones de hardware para soportar crecimiento futuro.

Prácticas recomendadas: Monitorear regularmente los KPIs y ajustar las configuraciones de QoS según sea necesario.

Conclusiones

Resumen de hallazgos: La implementación de QoS en el servidor MikroTik PC ha mejorado significativamente el desempeño y la estabilidad de la red.

Impacto en el negocio: El mejor control de calidad ha beneficiado la productividad de los usuarios al minimizar interrupciones en el servicio.

Pasos siguientes: Continuar monitoreando y ajustando las configuraciones de QoS para optimizar aún más el desempeño de la red.

15. Reporte de monitoreo de riesgos

El objetivo es identificar posibles problemas y proponer medidas de mitigación para asegurar una implementación exitosa y segura del servidor.

Riesgos de Hardware

- Fallas en el Disco Duro: Si el servidor utiliza discos duros tradicionales (HDD), estos pueden fallar debido a desgaste mecánico. Los discos de estado sólido (SSD) también tienen una vida útil limitada en términos de ciclos de escritura.
- Sobrecarga de CPU: Los servidores pueden sobrecargarse si se les exige más de lo que la CPU puede manejar, lo que puede llevar a ralentizaciones y posibles fallos del sistema.
- Problemas de Memoria (RAM): Fallos en los módulos de RAM pueden causar inestabilidad del sistema, reinicios inesperados y pérdida de datos.
- Fallo de la Fuente de Alimentación: Una fuente de alimentación defectuosa puede causar apagones inesperados, reinicios y daños en otros componentes del servidor.
- Calentamiento: Los servidores pueden generar una gran cantidad de calor, y si no se disipan adecuadamente, pueden sobrecalentarse, lo que puede llevar a la degradación de componentes y fallos prematuros.
- Problemas con la Placa Base: La placa base puede sufrir daños debido a variaciones de voltaje, cortocircuitos o simplemente debido al envejecimiento.
- Componentes de Red Defectuosos: Las tarjetas de red o los puertos pueden fallar, lo que podría llevar a una pérdida de conectividad o a una disminución en el rendimiento de la red.

- Interferencia Electromagnética (EMI): La proximidad a dispositivos que generan EMI puede interferir con el funcionamiento del servidor y causar problemas intermitentes.
- Problemas de Conectividad Física: Los cables y conectores pueden desgastarse o dañarse, lo que puede resultar en conexiones intermitentes o fallos de red.
- Falta de Mantenimiento y Limpieza: El polvo y otros residuos pueden acumularse en el hardware, causando problemas de sobrecalentamiento y fallos de componentes.

Riesgos de Software

- Vulnerabilidades de Seguridad: Las vulnerabilidades en el software pueden ser explotadas por atacantes para obtener acceso no autorizado, ejecutar código malicioso o causar interrupciones en el servicio.
- Configuraciones Incorrectas: Errores en la configuración pueden llevar a problemas de rendimiento, fallos en la conectividad o brechas de seguridad.
- Ataques de Denegación de Servicio (DoS/DDoS): Los ataques DoS o DDoS pueden sobrecargar el servidor, haciendo que los servicios sean inaccesibles.
- Exposición de Servicios Críticos: Exponer servicios críticos (como SSH, Winbox, API) a la red pública puede aumentar el riesgo de ataques.
- Problemas de Actualización: Actualizaciones mal ejecutadas o interrumpidas pueden dejar el sistema en un estado inestable o inutilizable.
- Malware y Software Malicioso: El malware puede infectar el servidor, causando pérdida de datos, degradación del rendimiento o comprometiendo la seguridad.
- Pérdida de Datos: Fallos en el sistema o errores humanos pueden resultar en la pérdida de configuraciones y datos importantes.
- Interferencias y Conflictos de Software: Interferencias entre diferentes servicios o conflictos con el sistema operativo pueden causar inestabilidad.
- Dependencias de Software: Dependencias no actualizadas o incompatibles pueden causar fallos en el sistema.
- Acceso No Autorizado: Acceso no autorizado a través de credenciales comprometidas o brechas de seguridad puede llevar a la manipulación de configuraciones y datos.
- Errores de Software o Bugs: Los errores en el software pueden causar comportamientos inesperados, inestabilidad del sistema y vulnerabilidades.

Vulnerabilidades de Seguridad

- Vulnerabilidades en el Sistema Operativo (RouterOS): Bugs y fallos en el sistema operativo pueden ser explotados por atacantes para obtener acceso no autorizado o ejecutar código malicioso.
- Contraseñas Débiles o por Defecto: Contraseñas débiles o no cambiadas desde las predeterminadas pueden ser fácilmente adivinadas o descifradas.

- Exposición de Servicios de Administración: Servicios de administración como Winbox, SSH, API y HTTP expuestos a Internet pueden ser blanco de ataques de fuerza bruta y explotación de vulnerabilidades.
- Ataques de Fuerza Bruta: Los atacantes pueden intentar adivinar las credenciales mediante ataques de fuerza bruta.
- Configuraciones Inseguras: Configuraciones incorrectas o inseguras pueden crear brechas de seguridad.
- Vulnerabilidades en Servicios y Protocolos: Servicios y protocolos obsoletos o inseguros (como Telnet y FTP) pueden ser explotados.
- Falta de Cifrado de Datos: La transmisión de datos sin cifrar puede ser interceptada y leída por atacantes.
- Vulnerabilidades en la Red Interna: Los atacantes pueden explotar dispositivos y servicios dentro de la red interna si no están adecuadamente protegidos.
- Acceso no Autorizado a la API: Las API pueden ser explotadas si no están adecuadamente protegidas.
- Ataques de Denegación de Servicio (DoS): Los ataques DoS pueden sobrecargar el servidor, haciendo que los servicios sean inaccesibles.
- Ingeniería Social y Phishing: Los atacantes pueden utilizar técnicas de ingeniería social para engañar a los usuarios y obtener acceso.
- Infección por Malware y Software Malicioso: El malware puede infectar el servidor, comprometiendo su seguridad y funcionalidad.

Riesgos Operacionales

- Interrupciones de Energía: Las interrupciones de energía pueden causar apagones inesperados, pérdida de datos y corrupción del sistema.
- Fallas de Hardware: Fallos en componentes críticos como el disco duro, memoria RAM, CPU o tarjetas de red pueden interrumpir el servicio.
- Errores Humanos: Los errores humanos en la configuración, mantenimiento o actualización del servidor pueden causar interrupciones del servicio o vulnerabilidades de seguridad.
- Actualizaciones Fallidas: Las actualizaciones del sistema operativo o del software pueden fallar, causando inestabilidad o interrupciones en el servicio.
- Problemas de Red: Problemas como congestión de red, fallos de conectividad o configuración incorrecta pueden afectar la operación del servidor.
- Capacidad y Escalabilidad: Un servidor puede alcanzar su límite de capacidad en términos de procesamiento, memoria o almacenamiento, afectando su rendimiento.
- Fallas en la Configuración de Seguridad: Configuraciones de seguridad deficientes pueden dejar el servidor vulnerable a ataques.

- Incompatibilidad de Software: Las actualizaciones o nuevos componentes de software pueden ser incompatibles con el sistema actual, causando fallos o inestabilidad.
- Gestión Inadecuada de Logs y Registros: La falta de gestión de logs puede dificultar la resolución de problemas y la detección de incidentes de seguridad.
- Dependencia de Personal Clave: La dependencia de una o pocas personas para la operación y mantenimiento del servidor puede ser riesgosa si estas personas no están disponibles.
- Problemas de Licenciamiento: El uso de software sin las licencias adecuadas puede causar problemas legales y técnicos.
- Resiliencia y Recuperación ante Desastres: La falta de planes de recuperación ante desastres puede prolongar la recuperación de fallos graves.
- Resiliencia y Recuperación ante Desastres: La falta de planes de recuperación ante desastres puede prolongar la recuperación de fallos graves.

Capacitación del Personal

1. Conocimientos Básicos de MikroTik y RouterOS: El personal debe tener una comprensión sólida de los conceptos básicos de MikroTik y RouterOS.
    - Contenido de Capacitación:
    - Introducción a MikroTik y RouterOS.
    - Instalación y configuración inicial de RouterOS.
    - Uso de la interfaz gráfica (Winbox) y la línea de comandos (CLI).
2. Configuración de Red y SeguridadEs crucial que el personal comprenda cómo configurar y asegurar la red.
    - Configuración de interfaces de red y VLANs.
    - Configuración de direcciones IP y rutas estáticas.
    - Implementación de NAT y firewalls.
    - Configuración de VPNs (PPTP, L2TP, OpenVPN, etc.).
    - Mejores prácticas de seguridad, incluyendo contraseñas, autenticación multifactor y listas de control de acceso (ACLs).
3. Gestión de Tráfico y Calidad de Servicio (QoS): Optimizar la gestión del tráfico y la calidad del servicio es vital para mantener un rendimiento de red adecuado.
    - Configuración de colas y límites de ancho de banda.
    - Implementación de QoS para priorizar el tráfico crítico.
    - Monitoreo y gestión del uso del ancho de banda.
4. Monitorización y Diagnóstico: el personal debe ser capaz de monitorizar el rendimiento de la red y diagnosticar problemas.
    - Uso de herramientas de monitoreo de MikroTik (The Dude, SNMP, syslog).
    - Diagnóstico de problemas de red utilizando ping, traceroute y otras herramientas.

- Análisis de logs y registros de eventos.
- Configuración de alertas y notificaciones.

5. Actualizaciones y Mantenimiento: Mantener el software y el hardware actualizados y en buen estado es crucial para la seguridad y el rendimiento.
    - Contenido de Capacitación:
    - Procedimientos para actualizar RouterOS y otros componentes de software.
    - Mantenimiento regular del hardware y revisión de configuraciones.
    - Gestión de copias de seguridad y restauración de configuraciones.
6. Planificación y Recuperación ante Desastres: Estar preparado para fallos y desastres es fundamental para minimizar el tiempo de inactividad.
    - Contenido de Capacitación:
    - Desarrollo y prueba de planes de recuperación ante desastres.
    - Implementación de medidas de redundancia y alta disponibilidad.
    - Procedimientos para la recuperación rápida de fallos del sistema.
7. Prácticas de Seguridad: La seguridad debe ser una prioridad constante en la administración de servidores y redes.
    - Contenido de Capacitación:
    - Protección contra amenazas comunes (DDoS, intrusiones, malware).
    - Configuración de alertas y respuestas ante incidentes.
    - Mejores prácticas de seguridad cibernética.
8. Documentación y Procedimientos Estándar: Mantener una documentación adecuada y seguir procedimientos estándar es clave para una operación consistente y segura.
    - Contenido de Capacitación:
    - Creación y mantenimiento de documentación de red y configuraciones.
    - Uso de procedimientos operativos estándar (SOPs) para tareas comunes.
    - Registro de cambios y auditorías.
    - Estrategias de Capacitación
    - Cursos y Certificaciones: Inscribir al personal en cursos y certificaciones oficiales de MikroTik, como MTCNA (MikroTik Certified Network Associate) y niveles avanzados.
    - Entrenamiento Interno: Realizar sesiones de capacitación interna y talleres prácticos para compartir conocimientos y resolver problemas específicos de la organización.
    - Simulaciones y Prácticas: Utilizar entornos de prueba y simulaciones para practicar configuraciones, actualizaciones y respuesta a incidentes.
    - Documentación y Recursos: Proveer acceso a documentación, manuales, tutoriales en línea y foros de soporte de MikroTik.

Capacitar adecuadamente al personal no solo mejora la eficiencia y efectividad en la gestión del servidor MikroTik PC, sino que también contribuye a una red más segura y robusta.

Riesgos de Red

- Ataques de Denegación de Servicio (DoS/DDoS): Los ataques DoS o DDoS pueden sobrecargar el servidor con tráfico, haciendo que los servicios sean inaccesibles.
- Acceso No Autorizado: Acceso no autorizado a la red puede permitir a los atacantes comprometer sistemas y datos
- Interceptación de Tráfico (Sniffing): El tráfico de red puede ser interceptado y analizado por atacantes, comprometiendo la confidencialidad de los datos.
- Configuraciones Incorrectas: Configuraciones incorrectas de red pueden crear vulnerabilidades y problemas de rendimiento.
- Rutas y Redundancia de Red: Fallos en la redundancia de red pueden causar interrupciones en el servicio.
- Problemas de Latencia y Rendimiento: Alta latencia y problemas de rendimiento pueden degradar la calidad del servicio y la experiencia del usuario.
- Vulnerabilidades en Protocolos de Red: Vulnerabilidades en protocolos de red pueden ser explotadas por atacantes.
- Segmentación Inadecuada de la Red: La falta de segmentación de la red puede permitir el movimiento lateral de atacantes una vez dentro de la red.
- Interferencia Electromagnética (EMI): La interferencia electromagnética puede afectar la calidad de la señal y el rendimiento de la red.
- Dependencias de Proveedores Externos La dependencia de servicios y proveedores externos puede introducir riesgos adicionales.
- Pérdida de Conectividad a Internet: La pérdida de conectividad a Internet puede afectar la disponibilidad de servicios y aplicaciones.
- Exposición de Servicios Críticos a Internet: Exponer servicios críticos a Internet puede aumentar el riesgo de ataques.

16. Cambios en las estrategias de atención de interesados

Estrategia	Reuniones de Progreso	Boletines Semanales	Sesiones	Actualización de Documentación en Tiempo Real	Encuestas de Satisfacción Mensuales
Plan de acción	Reuniones de progreso bi-semanales.	Enviar boletines informativos cortos cada semana.	Organizar sesiones de feedback cada dos semanas.	Utilizar una plataforma de documentación colaborativa.	Enviar encuestas breves de satisfacción cada mes.
Beneficios	Mayor control y seguimiento	Mantener a todos informados	Recibir retroalimentación continua y ajustar	Asegurar que la documentación del proyecto	Medir la satisfacción de los interesados y

	del progreso, detección temprana de problemas.	regularmente sin esperar a los informes mensuales.	el enfoque del proyecto según sea necesario.	esté siempre actualizada y accesible.	abordar cualquier preocupación de manera oportuna.

Conclusión

El desarrollo de un servidor MikroTik PC no solo representa una inversión en tecnología avanzada de redes, sino también un compromiso con la eficiencia operativa y la seguridad de datos. Este proyecto se enfocará en aprovechar al máximo las capacidades de MikroTik RouterOS para proporcionar una solución robusta y adaptable a las necesidades cambiantes del entorno empresarial moderno.

El éxito de este proyecto no solo se mide por la implementación técnica, sino también por el impacto positivo que tiene en las operaciones diarias de la organización. A medida que evolucionen las tecnologías y las necesidades del mercado, el servidor MikroTik PC seguirá siendo una piedra angular en la infraestructura de red de la empresa, proporcionando estabilidad, seguridad y eficiencia en el manejo de sus recursos digitales.

En conclusión, el desarrollo de un servidor MikroTik PC ha sido un paso significativo hacia la modernización y optimización de la infraestructura de red, preparando a la organización para enfrentar los desafíos tecnológicos del futuro con confianza y solidez.

Bibliografías

Jaraba, C. [@camilojaraba]. (2009, octubre 15). Mikrotik - 1. Instalacion de RouterOS en un PC. Youtube. https://www.youtube.com/watch?v=-iwFM2eprI8

Internet., M. [@masinternet]. (2022, enero 31). Comparativo mikrotik en pc, contra el fisico. checa el rendimiento. Youtube. https://www.youtube.com/watch?v=gUhfbtNbYCQ

Internet., M. [@masinternet]. (2023, junio 17). lanzamos hoy 17/06/23 Sistema Mikrotik en pc, procesador XEON 3.3, 12 Núcleos. Youtube. https://www.youtube.com/watch?v=AfMQJpOZJnk