Parametrización de hardware y software

Breve descripción:

El presente componente enseña a configurar y optimizar sistemas informáticos de manera eficiente. Aborda la virtualización de recursos, la gestión avanzada de sistemas operativos, la implementación de medidas de seguridad para proteger dispositivos, y la administración efectiva de redes. Se desarrollarán habilidades prácticas para mejorar el rendimiento, garantizar la seguridad de los equipos y enfrentar desafíos tecnológicos en diversos entornos.

Noviembre 2024

Tabla de contenido

Introducción

La tecnología actual se encuentra en constante evolución, y con ella, la necesidad de gestionar y optimizar los equipos de cómputo de manera eficiente. En este componente formativo, «Parametrización de hardware y software», exploraremos las técnicas y conocimientos para maximizar el rendimiento, la seguridad y la funcionalidad de los sistemas informáticos en entornos técnicos y profesionales. Desde la configuración inicial hasta la gestión avanzada de recursos, este módulo prepara a los estudiantes para enfrentar los retos tecnológicos del mundo moderno.

Uno de los aspectos más importantes en la parametrización es la correcta virtualización de sistemas, una tecnología que ha transformado la manera en que se utilizan y administran los recursos de hardware. Aprenderemos a identificar los tipos de virtualización, utilizar plataformas especializadas y gestionar recursos virtuales para asegurar que el hardware se use de manera óptima, sin desperdiciar capacidad y garantizando flexibilidad. Además, la comprensión de la virtualización abre puertas a soluciones innovadoras en el ámbito de la tecnología de la información.

La configuración de sistemas operativos también juega un papel central en la parametrización. Profundizaremos en aspectos como la configuración de BIOS/UEFI, los sistemas de arranque, y las técnicas para optimizar el rendimiento de los equipos. Estas habilidades son fundamentales para garantizar que los sistemas operativos funcionen de manera estable y segura, permitiendo que el hardware y el software operen en perfecta armonía y sean capaces de soportar las aplicaciones más demandantes.

Por último, la seguridad de punto final y la gestión de red serán pilares de este componente. Conoceremos cómo proteger los dispositivos contra amenazas externas

mediante antivirus y políticas de seguridad, y cómo implementar controles de acceso que salvaguarden la información sensible. También aprenderemos a gestionar redes de manera eficiente, aplicando configuraciones avanzadas que optimicen el uso compartido de recursos y mejoren la seguridad general de la infraestructura. Este enfoque integral garantizará que los estudiantes desarrollen una comprensión sólida de las prácticas modernas en la administración de hardware y software.

¡Bienvenido, aquí iniciarás un viaje de aprendizaje que te permitirá dominar las técnicas y configuraciones necesarias para optimizar el rendimiento y la seguridad de los sistemas informático!

Video 1. Parametrización de hardware y software

Enlace de reproducción del video

Síntesis del video: Parametrización de hardware y software
En el componente formativo «Parametrización de hardware y software», aprenderás a maximizar el potencial de los equipos informáticos mediante configuraciones avanzadas y técnicas de optimización. Se iniciará con la virtualización de sistemas, una tecnología que ha revolucionado la gestión de recursos de hardware. Se hará una exploración de los distintos tipos de virtualización y las plataformas que nos permiten aprovechar al máximo la capacidad de los equipos, haciendo que los recursos se distribuyan de manera más eficiente y adaptable a las necesidades actuales. Avanzando, se revisará la configuración de sistemas operativos, donde nos enfocaremos en la correcta configuración de la BIOS/UEFI con el fin de comprender los sistemas de arranque y la optimización del rendimiento del sistema. Luego, se tratará el tema de la seguridad de punto final, para proteger los dispositivos de ataques y amenazas externas. Aprenderemos a implementar antivirus y antimalware efectivos, establecer políticas de seguridad robustas y configurar controles de acceso que mantengan la información segura y lejos de manos no autorizadas. La gestión de redes cierra este recorrido formativo. Entenderemos cómo gestionar y proteger la infraestructura de red mediante la configuración de directorios activos, la correcta compartición de recursos, y la aplicación de políticas de grupo que garantizan un entorno seguro y organizado.

Aprenderemos a optimizar la conectividad y a proteger los datos, asegurando que la red funcione de manera eficiente y segura, incluso en los entornos más desafiantes.

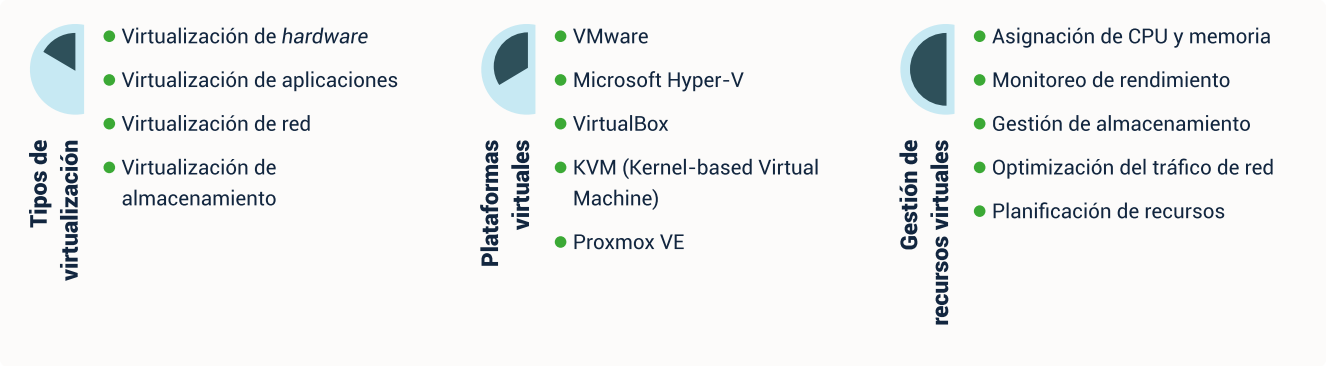
Este componente proporciona las herramientas y conocimientos necesarios para que los estudiantes se conviertan en expertos en parametrización, listos para enfrentar los retos tecnológicos con confianza.

¡Alístate para descubrir cómo una configuración adecuada y medidas de seguridad bien implementadas pueden transformar completamente el rendimiento y la protección de tus sistemas!

1. Virtualización de sistemas

La virtualización de sistemas ha transformado el uso de los recursos de hardware, permitiendo a las organizaciones y usuarios gestionar múltiples entornos de manera eficiente y flexible. Este capítulo explorará en profundidad los tipos de virtualización, las plataformas disponibles, y las mejores prácticas para la gestión de recursos virtuales.

Figura 1. Virtualización de sistemas y su gestión



Fuente. OIT, 2024.

1.1. Tipos de virtualización

La virtualización abarca varias categorías, y cada una se aplica a diferentes contextos y necesidades tecnológicas:

- **Virtualización de hardware**: este tipo permite la creación de múltiples máquinas virtuales que operan como sistemas independientes en un solo servidor físico. Cada máquina virtual tiene su propio sistema operativo, lo que facilita la consolidación de servidores y reduce costos operativos. Las organizaciones suelen usar esta virtualización para optimizar el uso de

recursos físicos, facilitar el mantenimiento y mejorar la disponibilidad de los servicios.

- **Virtualización de aplicaciones**: aquí, las aplicaciones se ejecutan en entornos aislados, eliminando conflictos con el sistema operativo o con otras aplicaciones instaladas. Esto es útil en entornos corporativos donde se requiere que diferentes versiones del software funcionen sin interferencias. Ejemplos de esta tecnología incluyen herramientas como Microsoft App-V o VMware ThinApp.
- **Virtualización de red**: esta categoría divide una red física en múltiples redes virtuales, o agrupa múltiples redes físicas en una sola red virtualizada. Con este enfoque, se puede gestionar el tráfico de red de manera más eficiente, mejorando la seguridad y la flexibilidad. Ejemplos incluyen la creación de VLANs y el uso de SDN (Software-Defined Networking) para gestionar redes de manera dinámica.
- **Virtualización de almacenamiento**: aquí, el almacenamiento físico se combina y se presenta como un único recurso gestionado. Esto simplifica la administración y permite la asignación dinámica del espacio según las necesidades. Las soluciones de virtualización de almacenamiento son comunes en grandes centros de datos y entornos corporativos que requieren un acceso flexible a grandes volúmenes de datos.

Cada tipo de virtualización tiene ventajas y desafíos específicos, y su implementación debe ser cuidadosamente planificada para maximizar los beneficios y minimizar los posibles problemas.

1.2. Plataformas virtuales

Las plataformas virtuales permiten implementar soluciones de virtualización con distintas capacidades y características. A continuación, se describen algunas de las más reconocidas:

- **VMware**: una de las plataformas líderes en el sector de la virtualización. Ofrece soluciones como VMware Workstation, VMware ESXi y vSphere, que permiten gestionar entornos de servidores complejos. VMware es muy valorada por su capacidad de recuperación ante desastres y las funcionalidades avanzadas de administración.
- **Microsoft Hyper-V**: esta plataforma, incluida en los sistemas operativos Windows Server, permite virtualizar tanto servidores como escritorios. Hyper-V es conocida por su integración con otros servicios de Microsoft, facilitando la gestión y seguridad en redes corporativas.
- **VirtualBox**: desarrollado por Oracle, VirtualBox es una herramienta de código abierto que soporta múltiples sistemas operativos en un entorno virtualizado. Es ampliamente utilizada por desarrolladores y estudiantes para realizar pruebas y ejecutar entornos de desarrollo.
- **KVM (Kernel-based Virtual Machine)**: una solución de virtualización de código abierto que convierte el kernel de Linux en un hipervisor. KVM es ideal para entornos empresariales que requieren estabilidad y eficiencia, y es compatible con muchas distribuciones de Linux.
- **Proxmox VE**: una plataforma de virtualización de código abierto que permite la gestión de máquinas virtuales y contenedores. Es conocida por

su interfaz web intuitiva y sus funciones de alta disponibilidad, respaldo y replicación.

Estas plataformas se eligen según las necesidades de rendimiento, presupuesto y compatibilidad del entorno en el que se van a utilizar.

1.3. Gestión de recursos virtuales

Una gestión adecuada de los recursos virtuales es necesaria para mantener el rendimiento y la estabilidad de los sistemas virtualizados. Aquí se explican las principales estrategias y herramientas:

- **Asignación de CPU y memoria**: una de las tareas críticas en la gestión de entornos virtuales es asignar los recursos de CPU y memoria de manera eficiente. Esto implica distribuir los recursos físicos del servidor según las demandas de cada máquina virtual, evitando la sobreasignación, que puede degradar el rendimiento del sistema.
- **Monitoreo de rendimiento**: las herramientas de monitoreo permiten analizar en tiempo real el uso de recursos, identificar cuellos de botella y tomar decisiones informadas para ajustar las configuraciones. Las métricas incluyen el uso de la CPU, memoria, almacenamiento y la latencia de la red.
- **Gestión de almacenamiento**: en un entorno virtual, el almacenamiento es un recurso compartido que debe administrarse cuidadosamente. Se pueden usar tecnologías como el aprovisionamiento fino (`thin provisioning`) para asignar espacio de manera dinámica según sea

necesario, evitando el desperdicio de recursos y mejorando la eficiencia del almacenamiento.

- **Optimización del tráfico de red**: configurar las redes virtuales para minimizar la latencia y el congestionamiento es fundamental. Esto se logra mediante la segmentación de redes, el uso de conmutadores virtuales y la priorización del tráfico basado en las necesidades de cada máquina virtual.
- **Planificación de recursos**: anticipar el crecimiento y las futuras necesidades de los recursos es vital para garantizar que el entorno virtualizado pueda escalar sin problemas. Esto incluye prever actualizaciones de hardware y ajustar las configuraciones según el uso proyectado.

2. Configuración de sistemas operativos

La correcta configuración de los sistemas operativos es fundamental para asegurar que los equipos de cómputo funcionen de manera óptima, segura y eficiente. En esta sección, se detallan los aspectos de la configuración, desde el arranque hasta la optimización del rendimiento.

2.1. BIOS/UEFI

La BIOS (Basic Input/Output System) y la UEFI (Unified Extensible Firmware Interface) son sistemas fundamentales que inician el hardware de un equipo y preparan el entorno para que el sistema operativo se cargue. Entender la función de ambos sistemas y cómo configurarlos es fundamental para optimizar el rendimiento y la seguridad de los equipos.

La BIOS es el firmware tradicional que controla las funciones básicas del hardware de la computadora. Cuando se enciende un equipo, la BIOS ejecuta una serie de pruebas conocidas como POST (Power-On Self Test) para asegurarse de que los principales componentes, como el procesador, la memoria RAM y los discos duros, estén funcionando correctamente.

a) **Interfaz de configuración**:

   La BIOS ofrece una interfaz simple basada en texto a la que se accede presionando una tecla específica (como F2, F10 o Delete) durante el arranque. Desde esta interfaz, se pueden ajustar configuraciones básicas, como el orden de arranque, la gestión de dispositivos, y las opciones de seguridad.

b) **Configuraciones comunes**:

- **Orden de arranque**: permite elegir el dispositivo desde el cual se iniciará el sistema operativo (disco duro, unidad USB, CD/DVD, etc.).
- **Configuración de dispositivos**: habilita o deshabilita componentes como puertos USB, tarjetas de red, y dispositivos de almacenamiento.
- **Opciones de seguridad**: incluyen la configuración de contraseñas para proteger el acceso a la BIOS y al equipo.

Aunque la BIOS ha sido un estándar durante décadas, tiene algunas limitaciones, como el soporte para particiones de disco mayores de 2 TB y una interfaz anticuada.

c) UEFI: Avances y beneficios

La UEFI es la evolución moderna de la BIOS, diseñada para superar sus limitaciones y ofrecer una experiencia más segura y flexible. La UEFI tiene una arquitectura más avanzada, permitiendo tiempos de arranque más rápidos, un mejor manejo de hardware moderno y soporte para interfaces gráficas.

- **Interfaz gráfica y usabilidad**: a diferencia de la BIOS, la UEFI proporciona una interfaz gráfica más intuitiva, con soporte para mouse y configuraciones avanzadas que son más fáciles de manejar.
- **Compatibilidad con discos grandes**: la UEFI puede gestionar particiones de disco de hasta 9.4 zettabytes, lo que la hace ideal para sistemas modernos que usan discos de alta capacidad.
- **Funciones de seguridad mejoradas**: una de las características más importantes de la UEFI es el Secure Boot, que impide que se cargue

software malicioso durante el arranque. Esta función verifica la firma de los sistemas operativos y aplicaciones de arranque, asegurando que solo se ejecute software confiable.

d) Configuraciones Importantes en UEFI

- **Modo de arranque**: la UEFI permite seleccionar entre el modo de arranque UEFI o Legacy (compatibilidad con BIOS antigua). Se debe elegir el modo adecuado según el sistema operativo instalado.
- **Administración de hardware**: se pueden realizar configuraciones avanzadas para gestionar mejor el rendimiento del procesador, la memoria, y las tarjetas gráficas.
- **Actualización de firmware**: la UEFI facilita las actualizaciones de firmware, que son necesarias para mantener la compatibilidad con hardware nuevo y corregir vulnerabilidades de seguridad.

e) Diferencias entre BIOS y UEFI

- **Velocidad de arranque**: la UEFI ofrece tiempos de arranque más rápidos debido a su diseño optimizado.
- **Seguridad**: UEFI proporciona medidas de seguridad adicionales como el Secure Boot, mientras que la BIOS carece de estas funciones avanzadas.
- **Interfaz**: la BIOS utiliza una interfaz de texto básica, mientras que la UEFI ofrece una experiencia gráfica con soporte para mouse.

2.2. Sistemas de arranque

El sistema de arranque es el proceso mediante el cual un equipo de cómputo carga el sistema operativo y lo prepara para ser utilizado. Una configuración adecuada

del sistema de arranque garantiza que el equipo inicie correctamente y pueda acceder a los recursos necesarios.

a) **Tipos de sistemas de arranque**

- **Arranque dual (Dual Boot)**: permite tener instalados dos sistemas operativos en un solo equipo y elegir cuál cargar al inicio. Esto es útil cuando se necesita trabajar con diferentes sistemas, como Windows y Linux.
- **Arranque desde dispositivos externos**: configurar el equipo para que pueda arrancar desde dispositivos externos, como unidades USB o discos ópticos, se hace necesario para tareas de recuperación y mantenimiento. Esta opción se establece en la BIOS/UEFI y se prioriza según la necesidad.

b) **Configuración del gestor de arranque**

El gestor de arranque es un programa que permite seleccionar qué sistema operativo se cargará en un equipo con arranque dual. Ejemplos comunes de gestores de arranque son GRUB (utilizado en Linux) y Windows Boot Manager.

- **Modificar el orden de arranque**: cambiar la prioridad de los dispositivos desde el gestor de arranque, en caso de que se necesite iniciar desde un disco duro secundario o una unidad USB.
- **Configuraciones avanzadas**: algunos gestores de arranque permiten opciones como tiempo de espera para la selección de un sistema operativo predeterminado o ajustes personalizados para arrancar en modo seguro.

c) **Problemas comunes y soluciones**

- **Error en el gestor de arranque**: a veces, el gestor de arranque puede corromperse debido a actualizaciones fallidas o instalaciones incorrectas.

Herramientas como el Disco de Reparación de Windows o comandos como boot-repair en Linux pueden ayudar a solucionar estos problemas.

- **No se detecta el sistema operativo**: verificar que el sistema operativo esté correctamente instalado y que el disco sea reconocido por la BIOS/UEFI. También puede ser necesario reparar el MBR (Master Boot Record) o la tabla de particiones.

2.3. Optimización de rendimiento

La optimización del rendimiento del sistema operativo es un proceso continuo que involucra ajustes y configuraciones para asegurar que los recursos de hardware sean utilizados de manera eficiente. Una buena optimización mejora la velocidad, la estabilidad y la experiencia del usuario.

a) Configuraciones para mejorar el rendimiento

- **Deshabilitar programas de inicio innecesarios**: muchos programas se configuran para iniciarse automáticamente con el sistema operativo, lo que puede ralentizar el arranque. Utilizar el Administrador de tareas de Windows o herramientas equivalentes en otros sistemas para deshabilitar programas que no son indispensables.
- **Ajustar las opciones de energía**: configurar el plan de energía adecuado según las necesidades del usuario. Por ejemplo, en portátiles, se puede seleccionar un plan de alto rendimiento cuando se necesita la máxima potencia o un plan de ahorro de energía para prolongar la duración de la batería.

- **Limpieza de disco**: usar herramientas como Liberador de espacio en disco en Windows o BleachBit en Linux para eliminar archivos temporales, caché y otros elementos innecesarios que ocupan espacio.

b) Optimización del uso de memoria (RAM)

- Administrar procesos en segundo plano: Identificar y cerrar aplicaciones que consumen mucha memoria a través del Administrador de Tareas o el Monitor de Recursos. En sistemas como Linux, se pueden usar comandos como htop para gestionar procesos.
- Aumentar el tamaño de la memoria virtual: En algunos casos, se puede mejorar el rendimiento aumentando la memoria virtual, que es un espacio en el disco duro que actúa como un complemento de la RAM. Esto se configura desde las opciones avanzadas del sistema operativo.

c) Actualizaciones de software

- **Actualizar el sistema operativo**: mantener el sistema operativo actualizado es fundamental para garantizar el rendimiento y la seguridad. Las actualizaciones corrigen vulnerabilidades y optimizan el uso de recursos.
- **Controladores de hardware**: asegurarse de que los controladores de los dispositivos estén actualizados. Esto incluye la tarjeta gráfica, el adaptador de red y otros periféricos que pueden afectar el rendimiento del sistema.

d) Desfragmentación y optimización del disco

- En sistemas con discos duros mecánicos (HDD), la desfragmentación organiza los archivos de manera que se acceda a ellos más rápidamente. En sistemas con unidades de estado sólido (SSD), la desfragmentación no es

necesaria, pero existen herramientas de optimización que pueden prolongar la vida útil del disco.

3. Seguridad de punto final

La seguridad de punto final es un aspecto fundamental en la protección de los equipos de cómputo y la información almacenada en ellos. En esta sección, abordaremos las medidas y herramientas que se utilizan para proteger los dispositivos de amenazas externas, incluyendo antivirus y antimalware, políticas de seguridad, y el control de acceso.

3.1. Antivirus y antimalware

Los antivirus y las soluciones antimalware son herramientas que sirven para detectar y eliminar software malicioso que pueda comprometer la seguridad de un equipo. Estas amenazas incluyen virus, troyanos, ransomware, spyware y otros programas dañinos.

a) Funcionamiento de los antivirus

- **Análisis en tiempo real**: los antivirus modernos monitorean constantemente las actividades en el equipo para identificar y bloquear amenazas antes de que puedan causar daño. Esto incluye la revisión de archivos descargados, correos electrónicos y dispositivos externos conectados al equipo.
- **Actualizaciones de definiciones de virus**: los fabricantes de antivirus actualizan regularmente sus bases de datos de definiciones para proteger contra nuevas amenazas. Se deben mantener estas actualizaciones para que el antivirus sea efectivo.
- **Escaneos programados**: configurar el software antivirus para realizar análisis periódicos del sistema ayuda a detectar y eliminar amenazas que puedan haber pasado desapercibidas.

b) Tipos de software antimalware

- **Antispyware**: se enfoca en detectar y eliminar programas que recolectan información del usuario sin su consentimiento, como contraseñas o datos personales.
- **Antiransomware**: ofrece protección específica contra software malicioso que cifra los archivos del usuario y exige un pago para liberarlos.
- **Software de eliminación de adware**: diseñado para identificar y remover programas que muestran anuncios no deseados o modifican la experiencia del usuario en el navegador.

El uso de una combinación de herramientas de seguridad puede proporcionar una protección más robusta contra diversas amenazas.

Tabla 1. Características y ejemplos de antivirus y antimalware

Aspecto	Descripción	Ejemplos
Análisis en tiempo real.	Monitorea continuamente las actividades en el sistema para detectar y bloquear amenazas de inmediato.	Norton, Kaspersky, Bitdefender.
Actualizaciones de definiciones.	Las bases de datos de virus y malware se actualizan regularmente para proteger contra las últimas amenazas conocidas.	McAfee, Avast, ESET.
Escaneos programados.	Permite configurar análisis periódicos del sistema para identificar y eliminar posibles amenazas de manera automática.	Avira, Sophos, Windows Defender.

Aspecto	Descripción	Ejemplos
Antispyware.	Software especializado en detectar y eliminar programas que recolectan información del usuario sin autorización.	Malwarebytes, Spybot, Adaware.
Antiransomware.	Ofrece protección contra malware que cifra archivos y exige un rescate, impidiendo el acceso del usuario a sus datos.	Bitdefender, Kaspersky, Webroot.
Eliminación de adware.	Identifica y remueve programas que muestran anuncios no deseados o interfieren con la experiencia del usuario en el navegador.	Malwarebytes, AdwCleaner, Avast.
Protección web.	Analiza y bloquea sitios web maliciosos, evitando que el usuario acceda a páginas que puedan comprometer su seguridad.	Norton Safe Web, McAfee WebAdvisor.
Herramientas de cuarentena.	Aísla los archivos sospechosos para evitar que afecten al sistema hasta que se decida eliminarlos o restaurarlos.	AVG, Kaspersky, Windows Defender.
Informes y notificaciones.	Proporciona reportes detallados sobre las amenazas detectadas y notifica al usuario cuando se requiere acción inmediata.	Symantec, Trend Micro, F-Secure.

Fuente. OIT, 2024.

3.2. Políticas de seguridad

Las políticas de seguridad establecen directrices para proteger los datos y los sistemas de una organización o un usuario individual. Estas políticas definen cómo se deben manejar, almacenar y proteger los recursos informáticos.

a) **Principales elementos de las políticas de seguridad**

- **Contraseñas seguras**: se debe requerir el uso de contraseñas complejas que combinen letras, números y caracteres especiales, y que se actualicen periódicamente. Herramientas como los gestores de contraseñas pueden ayudar a mantener estas credenciales seguras.
- **Políticas de actualización**: se deben establecer directrices para mantener el sistema operativo y el software actualizados. Las actualizaciones corrigen vulnerabilidades que pueden ser explotadas por atacantes.
- **Acceso a datos sensibles**: limitar el acceso a información crítica solo a personas autorizadas es importante para prevenir fugas o robos de datos. Esto incluye el uso de permisos específicos y autenticación multifactorial (MFA) cuando sea posible.

b) **Concienciación y capacitación**

- La formación de los usuarios en buenas prácticas de seguridad es fundamental para minimizar riesgos. Esto incluye el reconocimiento de correos electrónicos de phishing, la importancia de no compartir contraseñas, y la precaución al conectar dispositivos USB desconocidos.

3.3. Control de acceso

El control de acceso es una medida de seguridad que regula quién puede acceder a qué recursos dentro de un sistema informático. Este control garantiza que solo las personas autorizadas puedan interactuar con datos sensibles o realizar acciones críticas en el sistema.

a) **Tipos de control de acceso**

- **Control de acceso basado en roles (RBAC)**: asigna permisos a los usuarios según su función dentro de una organización. Por ejemplo, un administrador de red puede tener acceso total, mientras que un usuario estándar solo tiene permisos limitados.
- **Control de acceso basado en atributos (ABAC)**: permite o niega el acceso a los recursos según atributos específicos, como la ubicación, el tipo de dispositivo o la hora del día. Este método es más flexible y adecuado para entornos que requieren un alto nivel de personalización.
- **Listas de control de acceso (ACLs)**: especifican qué usuarios o grupos tienen permiso para acceder a ciertos recursos, y qué acciones pueden realizar (leer, escribir, ejecutar).

b) **Herramientas y métodos de control de acceso**

- **Software de autenticación**: las herramientas de autenticación aseguran que solo los usuarios legítimos puedan acceder al sistema. Esto incluye el uso de contraseñas, tokens de seguridad, o autenticación biométrica (como huellas dactilares o reconocimiento facial).
- **Sistemas de gestión de identidades (IDM)**: automatizan el proceso de asignación y gestión de permisos, asegurando que se cumplan las políticas de seguridad.

El control de acceso no solo protege los datos, sino que también ayuda a prevenir el uso indebido de los recursos de la red, manteniendo un entorno informático seguro.

4. Gestión de red

La gestión de red es un aspecto central en cualquier entorno informático, ya que permite configurar, mantener y asegurar la conectividad y el acceso a recursos compartidos de manera eficiente. En esta sección, se abordarán conceptos y prácticas relacionados con la gestión de directorios, recursos compartidos y políticas de grupo.

4.1. Directorio activo y dominios

El **Directorio Activo (Active Directory)** es un servicio desarrollado por Microsoft que facilita la administración centralizada de usuarios, equipos y recursos en una red basada en Windows. Es utilizado principalmente en entornos corporativos para gestionar permisos y políticas de seguridad de manera eficiente.

a) Conceptos

- **Dominio**: un dominio es un conjunto de usuarios, grupos y dispositivos que comparten una base de datos de Directorio Activo. Permite a los administradores gestionar de manera centralizada las cuentas y recursos de la red.
- **Controlador de dominio**: es el servidor que ejecuta el Directorio Activo y se encarga de autenticar a los usuarios y gestionar las políticas de seguridad. Se asegura de que solo los usuarios autorizados puedan acceder a los recursos de la red.

b) Funciones del Directorio Activo

- **Gestión de usuarios y grupos**: permite crear, modificar y eliminar cuentas de usuario, y organizar a los usuarios en grupos para asignar permisos de manera más eficiente.

- **Autenticación**: valida las credenciales de los usuarios cuando intentan acceder a recursos de la red, proporcionando un alto nivel de seguridad.
- **Políticas de seguridad**: los administradores pueden configurar políticas de grupo que aplican configuraciones de seguridad y de sistema a los usuarios y equipos en el dominio.

c) Ventajas de usar el directorio activo

- **Centralización**: simplifica la gestión de la red al permitir a los administradores controlar todo desde un único punto.
- **Escalabilidad**: se adapta a redes de cualquier tamaño, desde pequeñas oficinas hasta grandes organizaciones con miles de dispositivos.
- **Seguridad**: ofrece una estructura robusta para proteger los datos y recursos de la red mediante autenticación y políticas de acceso.

4.2. Recursos compartidos

Compartir recursos en una red permite a los usuarios acceder de manera eficiente a archivos, impresoras y otros dispositivos. Una correcta configuración de estos recursos es fundamental para optimizar la colaboración y el uso de los dispositivos.

a) Tipos de recursos compartidos

- **Archivos y carpetas**: los archivos y carpetas pueden compartirse en la red, permitiendo a los usuarios colaborar y trabajar en documentos de forma simultánea. Los administradores pueden asignar permisos de lectura, escritura o edición para controlar el acceso.

- **Impresoras**: las impresoras compartidas son accesibles desde cualquier dispositivo en la red, facilitando su uso por parte de varios usuarios sin la necesidad de conexiones directas.
- **Unidades de red**: una unidad de red es un espacio de almacenamiento asignado a un usuario o grupo, accesible desde cualquier equipo en la red. Es útil para almacenar documentos y datos importantes de manera centralizada.

b) Configuración y permisos

- **Permisos de acceso**: los administradores pueden configurar diferentes niveles de permisos, como acceso solo de lectura o permisos completos para modificar y eliminar archivos.
- **Seguridad de los recursos**: es importante proteger los recursos compartidos mediante autenticación y control de acceso, asegurándose de que solo las personas autorizadas puedan utilizarlos.

c) Buenas prácticas

- **Organización de carpetas**: mantener una estructura de carpetas bien organizada ayuda a los usuarios a encontrar y gestionar archivos de manera eficiente.
- **Monitoreo y auditoría**: utilizar herramientas para monitorear el uso de los recursos compartidos y realizar auditorías de seguridad periódicas.

4.3. Políticas de grupo

Las Políticas de Grupo (Group Policy) son una característica de Windows que permite a los administradores controlar de manera centralizada las configuraciones y restricciones de los equipos y usuarios en un dominio.

a) **Funciones de las políticas de grupo**

- **Configuración de seguridad**: los administradores pueden aplicar políticas para exigir contraseñas seguras, bloquear dispositivos externos como unidades USB, y definir restricciones de acceso.
- **Configuración de escritorio**: se pueden establecer configuraciones específicas, como la apariencia del escritorio, programas predeterminados y restricciones en el menú de inicio.
- **Automatización de tareas**: las políticas de grupo permiten automatizar tareas comunes, como la instalación de software o la actualización de configuraciones de red.

b) **Ejemplos de uso**

- **Restringir el acceso a aplicaciones**: se pueden bloquear aplicaciones no autorizadas para proteger los equipos de software malicioso o no deseado.
- **Configuración de red**: aplicar configuraciones de red predefinidas a todos los dispositivos, como la asignación de servidores DNS o la configuración de proxy.
- **Bloqueo de dispositivos**: restringir el uso de dispositivos externos para proteger la red de posibles infecciones de malware.

c) **Administración de políticas de grupo**

- **Consola de gestión**: la consola de gestión de políticas de grupo permite crear y aplicar políticas de manera centralizada. Las políticas pueden aplicarse a toda la organización o a grupos específicos según las necesidades.

- **Actualización de políticas**: las políticas de grupo se aplican automáticamente al iniciar sesión o mediante comandos de actualización, garantizando que todos los dispositivos cumplan con las configuraciones establecidas.

Tabla 2. Ejemplos de configuraciones de políticas de grupo y su impacto

Configuración de política	Descripción	Impacto en la red
Contraseñas seguras obligatorias.	Exige que las contraseñas tengan una longitud mínima, combinando letras, números y símbolos.	Mejora la seguridad al dificultar los intentos de acceso no autorizado.
Bloqueo de dispositivos USB.	Restringe el uso de dispositivos de almacenamiento USB para evitar la transferencia de datos no autorizados.	Previene el robo de información y la infección por malware desde USB.
Actualización automática de software.	Fuerza a todos los equipos a instalar actualizaciones del sistema operativo y software de seguridad.	Mantiene todos los dispositivos actualizados y protegidos contra vulnerabilidades.
Configuración del Firewall.	Establece reglas específicas para el firewall en cada dispositivo de la red, permitiendo o denegando tráfico según las necesidades de seguridad.	Controla el tráfico de red y protege los dispositivos de accesos maliciosos.
Acceso restringido a Panel de Control y Configuración.	Impide que los usuarios realicen cambios en la configuración del sistema.	Evita alteraciones que puedan comprometer el rendimiento o la seguridad.
Configuración de proxy en navegadores.	Define automáticamente el servidor proxy que deben usar los navegadores en la red.	Controla y monitorea el tráfico de Internet, mejorando la seguridad y la administración del uso de la red.
Deshabilitar el uso de aplicaciones específicas.	Prohíbe la ejecución de software no autorizado, como programas de entretenimiento o aplicaciones de alto riesgo.	Reduce el riesgo de ejecutar aplicaciones maliciosas y mejora la productividad.

Configuración de política	Descripción	Impacto en la red
Control de acceso a recursos compartidos.	Configura permisos específicos para que solo ciertos usuarios o grupos puedan acceder a carpetas y archivos en la red.	Protege datos sensibles y organiza el acceso según las necesidades del usuario.
Desconexión automática por inactividad.	Cierra automáticamente la sesión de los usuarios después de un período de inactividad.	Aumenta la seguridad al reducir la exposición en dispositivos desatendidos.

Fuente. OIT, 2024.

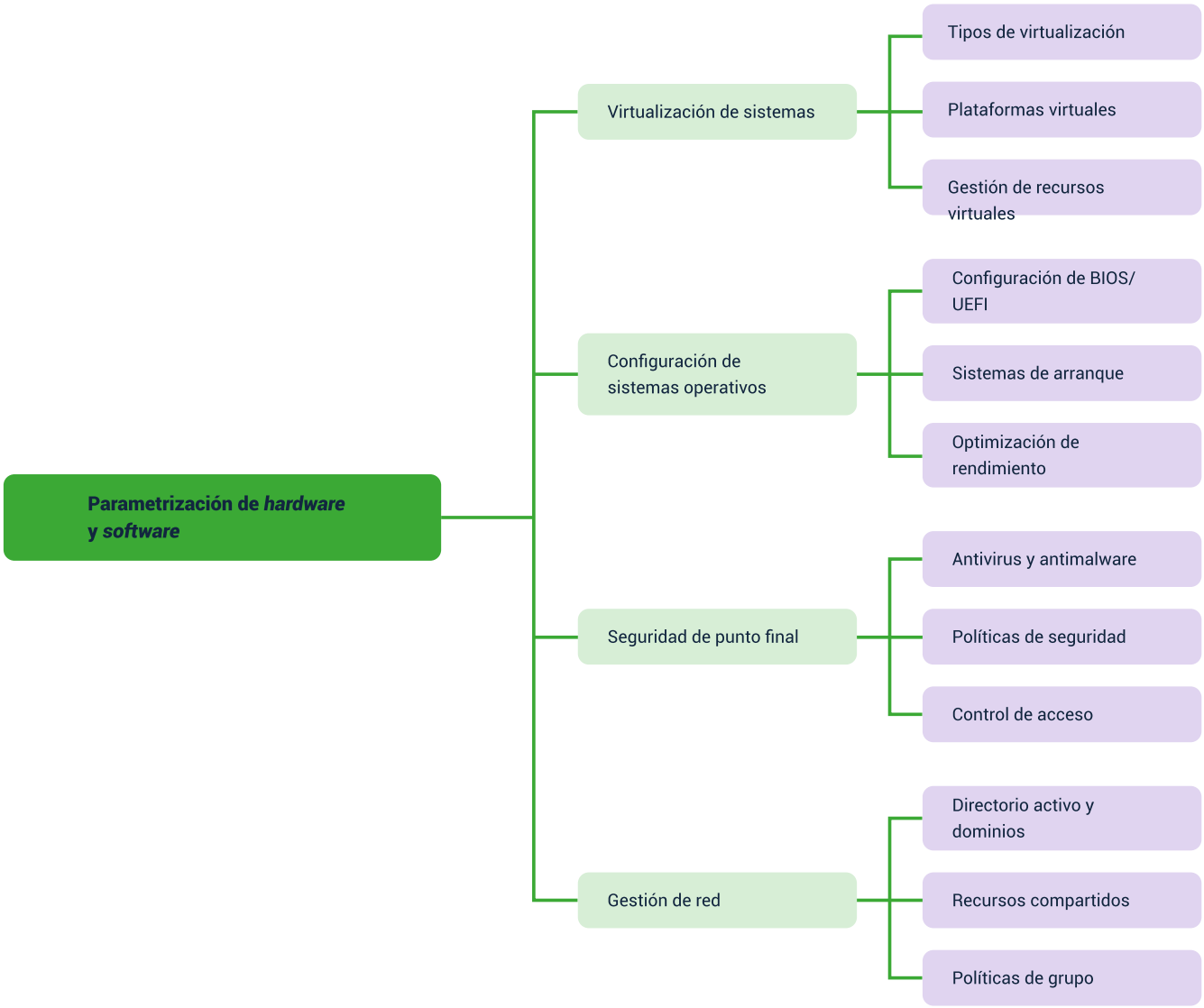
Síntesis

Este componente abarca los principios y técnicas necesarias para la parametrización de hardware y software, proporcionando un enfoque integral desde la virtualización hasta la gestión de la seguridad. Se inicia con una exploración de los distintos tipos de virtualización y las plataformas que permiten maximizar la eficiencia de los recursos de hardware, destacando las tecnologías que optimizan el uso compartido y la administración de recursos.

Se profundiza en la configuración de sistemas operativos, abordando configuraciones avanzadas de BIOS/UEFI y los sistemas de arranque, junto con técnicas de optimización que aseguran un funcionamiento estable y eficiente de los equipos. Se enfatiza cómo estas configuraciones impactan directamente el rendimiento general y la estabilidad de los sistemas informáticos.

El componente también aborda la seguridad de punto final, presentando estrategias para proteger los dispositivos mediante antivirus y antimalware, y detallando la implementación de políticas de seguridad efectivas y controles de acceso robustos. Estas medidas deben tenerse en cuenta para mantener la integridad de los datos y proteger los equipos de amenazas externas.

Finalmente, se examina la gestión de redes, que incluye la administración de directorios activos, la compartición eficiente de recursos, y la aplicación de políticas de grupo. Estas prácticas aseguran una infraestructura de red organizada y segura, facilitando tanto la colaboración como la protección de la información sensible en diversos entornos tecnológicos.



Fuente. OIT, 2024.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Virtualización de sistemas	Ecosistema de Recursos Educativos Digitales SENA. (2023c, octubre 17). Virtualización CPU.	Video	https://www.youtube.com/watch?v=lGLzCzgrcF8
1. Virtualización de sistemas	Ecosistema de Recursos Educativos Digitales SENA. (2023a, marzo 23). Los sistemas operativos por su estructura: Visión interna.	Video	https://www.youtube.com/watch?v=RjuFT03PSyw
2. Configuración de sistemas operativos	Ecosistema de Recursos Educativos Digitales SENA. (2023, octubre 24). Gestión de equipos informáticos	Video	https://www.youtube.com/watch?v=dJ0rNne1xuY
2. Configuración de sistemas operativos	Ecosistema de Recursos Educativos Digitales SENA. (2023c, octubre 18). Características de los sistemas operativos.	Video	https://www.youtube.com/watch?v=TGYx-geVl8E
3. Seguridad de punto final	Ecosistema de Recursos Educativos Digitales SENA. (2021, 2 octubre). Herramientas y estrategias de protección: antivirus gratuitos.	Video	https://www.youtube.com/watch?v=jqL1RwFft-0
3. Seguridad de punto final	Ecosistema de Recursos Educativos Digitales SENA. (2024, 3 abril). Seguridad perimetral.	Video	https://www.youtube.com/watch?v=l5_sSIAD8Wo
4. Gestión de red	Ecosistema de Recursos Educativos Digitales SENA. (2023b, abril 17). Sistemas operativos en red.	Video	https://www.youtube.com/watch?v=oy1cr57wi5M

Glosario

Antivirus: Software diseñado para detectar, prevenir y eliminar programas maliciosos que puedan dañar el sistema o robar información.

Aprovisionamiento fino (Thin Provisioning): técnica de gestión de almacenamiento que asigna espacio dinámicamente, evitando el desperdicio de recursos.

Arranque dual (Dual Boot): configuración que permite tener múltiples sistemas operativos instalados en un mismo equipo y elegir cuál arrancar.

BIOS: Firmware básico que inicializa el hardware del sistema y carga el sistema operativo al encender el equipo.

Control de acceso: medidas y mecanismos que limitan quién puede acceder a ciertos datos o recursos dentro de un sistema.

Directorio Activo (Active Directory): servicio de Microsoft que centraliza la administración de usuarios, equipos y recursos en una red basada en Windows.

Firewall: sistema de seguridad que controla el tráfico de red, permitiendo o bloqueando conexiones según reglas definidas.

Gestión de red: proceso de administrar y optimizar la conectividad y el acceso a recursos en una red informática.

Gestor de arranque: programa que permite seleccionar qué sistema operativo iniciar en equipos con arranque dual.

Memoria virtual: espacio en el disco duro que actúa como un complemento de la memoria RAM, utilizado cuando la RAM está llena.

Políticas de Grupo (Group Policy): configuraciones de Windows que permiten a los administradores gestionar y controlar el entorno de trabajo de los usuarios y equipos.

Protección web: característica de los antivirus que bloquea el acceso a sitios web maliciosos para proteger la seguridad del usuario.

Recursos compartidos: archivos, carpetas, impresoras o dispositivos accesibles para varios usuarios en una red.

Secure Boot: función de seguridad de UEFI que verifica la autenticidad del software de arranque para prevenir la carga de malware.

Segmentación de red: división de una red en segmentos más pequeños y seguros para mejorar la gestión y proteger el tráfico de datos.

UEFI: interfaz de firmware moderna que reemplaza al BIOS, proporcionando una interfaz gráfica y mayor seguridad.

VirtualBox: software de virtualización de código abierto que permite ejecutar múltiples sistemas operativos en un solo equipo.

Virtualización: tecnología que permite ejecutar múltiples sistemas operativos o aplicaciones en un solo servidor físico mediante máquinas virtuales.

VLAN (Virtual Local Area Network): tecnología que crea redes separadas dentro de una misma infraestructura física, mejorando la seguridad y eficiencia del tráfico.

Referencias bibliográficas

Andrews, J. (2019). Guía A+ para el Soporte Técnico en TI (Hardware y Software) (9ª ed.). Cengage Learning.

Aranda Córdoba, J. R. (2015). Desarrollo y reutilización de componentes software y multimedia mediante lenguajes de guión. IC Editorial.

Aranda Vera, Á. (2015). Instalación y parametrización del software. IC Editorial.

Caicedo Rendón, A. M., Pino Correa, F. J., & Pino Anacona, A. F. (2018). ISO/IEC 29110 para procesos software en las pequeñas empresas. AENOR.

Dembowski, K. (2003). El Gran Libro de Hardware. Marcombo.

Díaz Coca, M. J. (2016). Desarrollo de componentes software para el manejo de dispositivos. IC Editorial.

Eito Brun, R., & Sicilia Urbán, M. (2020). Gestión de innovación y procesos software: normativa y mejores prácticas. Servicio de Publicaciones, Universidad de Alcalá.

García Bermúdez, J. C. (2016). Diseño de elementos software con tecnologías basadas en componentes. IC Editorial.

Manovich, L. (2014). El software toma el mando. Editorial UOC.

Moreno Pérez, J. C. (2015). Administración de software de un sistema informático. RA-MA Editorial.

Patterson, D. A., & Hennessy, J. L. (2018). Estructura y diseño de computadores: La interfaz hardware/software (4ª ed.). Reverté.

Pérez Carvajal, R. J. (2016). Mantenimiento del software. IC Editorial.

Piattini Velthuis, M., & Garzás Parra, J. (2015). Fábricas de software: experiencias, tecnologías y organización. RA-MA Editorial.

Piattini Velthuis, M., Vizcaíno Barceló, A., & García Rubio, F. O. (2014). Desarrollo global de software. RA-MA Editorial.

Pressman, R. S. (2010). Ingeniería del software: Un enfoque práctico (7ª ed.). McGraw-Hill.

Rodríguez Monje, M. J., Pino, F., & Rodríguez Monje, M. (2018). Modelo de madurez de ingeniería del software Versión 2.0 (MMIS V.2). AENOR.

Rodríguez Villalobos, A. (2017). Grafos: software para la construcción, edición y análisis de grafos. Bubok Publishing S.L.

Saavedra Fernández, T. (2015). Selección, instalación y configuración del software de servidor de mensajería electrónica. IC Editorial.

Salazar Torres, J. A., & Ibañez Olvera, M. (2015). Simulación de una descarga eléctrica a través de software libre. Ediciones y Gráficos Eón.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2014). Fundamentos de sistemas operativos (9ª ed.). McGraw-Hill.

Sommerville, I. (2011). Ingeniería del software (9ª ed.). Pearson Educación.

Stallings, W. (2015). Organización y arquitectura de computadores (9ª ed.). Pearson Educación.

Tanenbaum, A. S., & Bos, H. (2015). Sistemas operativos modernos (4ª ed.). Pearson Educación.

Ullman, J. D., & Widom, J. (2013). Fundamentos de bases de datos (4ª ed.). Pearson Educación.

Villada Romero, J. L. (2016). Instalación y configuración del software de servidor web. IC Editorial.

Villar Cueli, J., & Huércano Ruíz, F. (2014). Implementación e integración de elementos software con tecnologías basadas en componentes. IC Editorial.

Créditos

Elaborado por:

Organización Internacional del Trabajo