Documentación Técnica: Soporte, Mantenimiento e Infraestructura

Elaborado por: Javier Rodríguez Y David Fernández

Manuales y Fichas de Instalación de Infraestructura

La instalación y configuración adecuada de la infraestructura tecnológica es fundamental para garantizar un desempeño óptimo y seguro en cualquier organización. Este proceso requiere una planificación estratégica detallada que permita determinar las necesidades específicas de la red y los recursos involucrados.

Planificación de la Red

Antes de proceder con la instalación física, es imprescindible realizar un análisis para definir el tipo y alcance de la red, considerando aspectos como el número de usuarios, la distribución física del espacio y los requerimientos de ancho de banda. La planificación debe contemplar también el crecimiento futuro y la escalabilidad del sistema.

Selección de Topologías de Red

La elección de la topología adecuada impacta directamente en la eficiencia y la seguridad de la red. Se utilizan comúnmente las siguientes topologías:

- **Estrella:** Cada dispositivo se conecta a un nodo central, generalmente un switch o hub, facilitando la gestión y el aislamiento de fallos.
- **Malla:** Todos los nodos están interconectados, lo que proporciona alta redundancia y tolerancia a fallos, aunque requiere mayor inversión en cableado.
- **Bus:** Los dispositivos se conectan a un único canal común; es más simple pero menos escalable y menos resistente a fallos.
- **Anillo:** Los dispositivos se conectan en un circuito cerrado, donde la información circula en un sentido, ofreciendo un equilibrio entre eficiencia y costo.

Tipos de Cableado

Para la infraestructura física, el tipo de cable utilizado es clave para el rendimiento y la estabilidad de la red:

- **UTP (Unshielded Twisted Pair):** Es el cable más común para redes LAN. Su instalación es sencilla y económica, adecuado para distancias cortas y velocidades de hasta 1 Gbps.

- **Fibra Óptica:** Ideal para conexiones de alta velocidad y largas distancias. Ofrece mayor inmunidad a interferencias electromagnéticas y ancho de banda superior.

Instalación y Configuración de Dispositivos de Red

Los dispositivos esenciales incluyen routers, switches y puntos de acceso (AP). La instalación debe asegurar compatibilidad tanto física como lógica, así como configuraciones seguras y eficientes:

- **Routers:** Configurar las rutas, definir políticas de seguridad y controlar el acceso entre redes internas y externas.
- **Switches:** Establecer segmentos de red, configurar VLANs para segmentación y optimización del tráfico.
- **Puntos de Acceso:** Adecuada ubicación para cobertura inalámbrica, utilización de protocolos de seguridad como WPA3 y autenticación robusta.

Herramientas y Validación

Para garantizar una instalación eficaz, se debe trabajar con herramientas especializadas como testers de cableado, analizadores de red y software de diagnóstico. La validación consiste en verificar la conectividad, la correcta asignación de direcciones IP y la funcionalidad de todos los dispositivos instalados. Se recomienda registrar en fichas técnicas todos los detalles de la instalación para futuras referencias y mantenimiento.

Manual de Instalación de Equipos Informáticos

Este manual proporciona una guía detallada para la instalación y configuración inicial de los equipos informáticos utilizados en entornos corporativos, incluyendo ordenadores de escritorio, portátiles, impresoras y periféricos asociados.

Requerimientos Técnicos

Para asegurar la correcta función de cada equipo, es necesario verificar lo siguiente antes de la instalación:

- **Compatibilidad de hardware:** Confirmar que los componentes internos (procesador, memoria RAM, discos, puertos) sean compatibles con el sistema operativo y software corporativo.
- **Conectividad física:** Identificar puertos disponibles (USB, HDMI, Ethernet) y conexiones necesarias para periféricos y red.
- **Software requerido:** Asegurar la disponibilidad de controladores (drivers) y aplicaciones básicas para el correcto funcionamiento.

Procedimiento de Instalación

1. **Desembalaje y verificación:** Inspeccionar los equipos para detectar daños físicos y comprobar que los accesorios y cables estén completos.
2. **Montaje físico:** Ubicar los equipos en el área destinada, establecer las conexiones eléctricas y de red, y conectar periféricos como teclado, mouse, impresora y monitor.
3. **Encendido y configuración inicial:** Realizar el primer arranque, configurar parámetros básicos del BIOS/UEFI si es necesario, y verificar detección de hardware.
4. **Instalación de drivers y software base:** Instalar controladores oficiales según el modelo del equipo y las recomendaciones del fabricante. Seguir con la instalación de sistema operativo estandarizado y aplicaciones corporativas básicas.
5. **Configuración de red y seguridad:** Establecer ajustes de red (IP, dominio, acceso a recursos compartidos) y aplicar políticas de seguridad iniciales, como antivirus y firewall.

Gestión e Inventario

Para mantener un registro actualizado de los activos informáticos, es imprescindible documentar la siguiente información en el sistema de inventario:

- Número de serie y modelo del equipo
- Ubicación física asignada
- Fecha de instalación
- Características técnicas principales
- Responsable asignado

Este registro facilita el seguimiento de mantenimiento, soporte y eventual actualización o reemplazo, contribuyendo a una gestión eficiente del parque tecnológico.

Configuraciones Estándar de Equipos

Para garantizar la uniformidad, seguridad y eficiencia en la gestión de los equipos informáticos, es indispensable establecer configuraciones estándar que se apliquen de manera homogénea en toda la organización. Este estándar abarca aspectos fundamentales como el sistema operativo, las aplicaciones oficiales autorizadas y las políticas de seguridad informática.

Sistemas Operativos

La organización admite principalmente dos sistemas operativos para todos los equipos: **Windows** y **Linux**. Esta selección responde a criterios de compatibilidad con aplicaciones corporativas, estabilidad y soporte técnico. La gestión del licenciamiento debe realizarse centralizadamente para evitar incumplimientos y facilitar auditorías.

Se recomienda implementar imágenes preconfiguradas que incluyan el sistema operativo junto con las configuraciones básicas y aplicaciones necesarias. Este método facilita la instalación rápida y uniforme, asegurando que cada equipo disponga de:

- Actualizaciones automáticas habilitadas para parches de seguridad y mejoras del sistema.
- Configuraciones regionales y de idioma estandarizadas.
- Compatibilidad con controladores oficiales de hardware aprobados por la organización.

Además, los administradores deben mantener un plan de pruebas y validación previo a la liberación de nuevas imágenes, para evitar problemas de estabilidad o incompatibilidades.

Aplicaciones Oficiales

Para asegurar la productividad y seguridad del entorno informático, se establecen aplicaciones oficiales y obligatorias que deben estar instaladas en todos los equipos. Entre ellas se incluyen:

- **Suite de oficina:** Microsoft Office o su equivalente autorizado, para la creación y gestión de documentos, hojas de cálculo y presentaciones.
- **Navegadores web corporativos:** versiones controladas y actualizadas de navegadores como Microsoft Edge o Google Chrome, configurados con políticas de seguridad y acceso restringido cuando corresponda.
- **Software antivirus y antimalware:** productos corporativos centralizados que se actualizan automáticamente para proteger contra amenazas informáticas.
- **Herramientas de comunicación y colaboración:** aplicaciones aprobadas para mensajería instantánea, videoconferencia y gestión de proyectos.

Es fundamental controlar las versiones instaladas para evitar vulnerabilidades y garantizar la interoperatividad entre usuarios. La instalación y actualización de estas aplicaciones debe ser gestionada a través de plataformas centralizadas que permitan auditoría y despliegue masivo.

Políticas de Seguridad Informática

Las políticas de seguridad forman la base para proteger la información y los recursos tecnológicos de la organización. Entre las configuraciones estándar más importantes se encuentran:

- **Contraseñas seguras:** Se debe exigir una longitud mínima, combinación de caracteres alfanuméricos y renovación periódica. No se permite compartir credenciales.
- **Cifrado de discos duros:** Todos los equipos deben utilizar tecnologías de cifrado (por ejemplo, BitLocker en Windows) para proteger datos ante pérdida o robo del dispositivo.

- **Control de accesos:** Implementación de mecanismos de autenticación fuerte, restricción de accesos físicos y lógicos según roles y responsabilidades.
- **Copia de seguridad periódica:** Las configuraciones establecen la frecuencia y medios para realizar backups automáticos de datos críticos, así como la verificación periódica de la integridad de las copias.
- **Actualizaciones y parches de seguridad:** Todas las actualizaciones deben aplicarse oportunamente para evitar vulnerabilidades conocidas.

El cumplimiento estricto de estas políticas debe ser monitorizado con herramientas de gestión centralizadas que permitan detectar y responder ante incumplimientos o incidentes de seguridad.

Informes de Pruebas de Diagnóstico de Equipos Informáticos

La realización periódica de diagnósticos a los equipos informáticos es un componente clave para mantener la operatividad y prolongar la vida útil del parque tecnológico. Estos diagnósticos permiten identificar de manera anticipada posibles fallos en el hardware o el software, facilitando intervenciones preventivas.

Herramientas de Diagnóstico Utilizadas

Existen diversas herramientas especializadas que ayudan a evaluar el estado de los componentes principales de los equipos:

- **CrystalDiskInfo:** Software dirigido a la monitorización del estado de los discos duros y unidades SSD, analizando parámetros SMART para detectar sectores dañados o un posible fallo inminente.
- **MemTest86:** Utilizado para evaluar la integridad de la memoria RAM mediante pruebas exhaustivas que detectan errores y problemas físicos.
- **Diagnósticos del sistema operativo:** Herramientas nativas o de terceros para evaluar el rendimiento del CPU, estabilidad del sistema y presencia de errores en el software instalado.

Formato del Informe de Diagnóstico

El informe debe estructurarse con la siguiente información clara y precisa para facilitar su análisis y seguimiento:

- **Fecha y hora de la prueba:** Registro temporal para identificar/testing la vigencia del diagnóstico.
- **Identificación del dispositivo:** Incluye nombre, número de serie y ubicación, para facilitar la trazabilidad.
- **Herramienta de diagnóstico empleada:** Especificación del software y versión usada en la prueba.

- **Resultados detallados:** Estado de cada componente evaluado, valorando parámetros críticos y errores detectados.
- **Recomendaciones prácticas:** Acciones sugeridas para mantenimiento, reparación o reemplazo de componentes según diagnóstico.

Importancia del Historial y Seguimiento

Es fundamental mantener un registro histórico detallado y organizado de todos los diagnósticos realizados. Este historial permite:

- Detectar patrones recurrentes de fallos en modelos o áreas específicas.
- Planificar intervenciones preventivas basadas en datos confiables.
- Tomar decisiones informadas para la renovación o actualización del equipamiento.
- Mejorar la gestión del soporte técnico con evidencia documentada.

Para ello, se recomienda utilizar bases de datos o plataformas de gestión documental que permitan acceso rápido, filtros avanzados y generación de reportes periódicos para la supervisión continua del estado del parque tecnológico.

Planes de Mantenimiento de Equipos Informáticos

Los planes de mantenimiento de los equipos informáticos se estructuran en dos grandes categorías: **mantenimiento preventivo** y **mantenimiento correctivo**. Cada uno cumple un rol fundamental para asegurar la disponibilidad, rendimiento y seguridad del parque tecnológico.

Mantenimiento Preventivo

El mantenimiento preventivo abarca un conjunto de tareas planificadas que se realizan periódicamente, con el objetivo de anticipar y minimizar la ocurrencia de fallos. Entre las acciones más relevantes se incluyen:

- **Limpieza física de componentes:** eliminación de polvo y suciedad de ventiladores, disipadores, puertos y superficies internas para evitar recalentamientos y fallos eléctricos.
- **Revisión y actualización del sistema operativo:** instalación de parches y actualizaciones críticas que mejoran la estabilidad y la seguridad del equipo.
- **Análisis del rendimiento:** monitoreo de CPU, memoria y espacio en disco para detectar cuellos de botella o degradación del funcionamiento.
- **Comprobaciones de seguridad:** verificación del estado del antivirus, firewalls y política de contraseñas, asegurando que no existan vulnerabilidades abiertas.

Se recomienda realizar estas actividades con una frecuencia de *3 a 6 meses*, dependiendo del uso y criticidad del equipo, para maximizar su vida útil y minimizar interrupciones.

Mantenimiento Correctivo

Este mantenimiento se refiere a la intervención reactiva tras detectar una falla o incidencia. Incluye:

- **Reparación o sustitución de piezas dañadas:** como discos duros, memorias, fuentes de alimentación o periféricos.
- **Reinstalación de software:** restauración del sistema operativo o aplicaciones, en caso de corrupción o mal funcionamiento.
- **Recuperación de datos:** mediante herramientas especializadas para minimizar la pérdida de información crítica.
- **Resolución de incidentes técnicos:** diagnóstico y solución de problemas de hardware y software que afectan la operatividad.

Es crucial que cada intervención correctiva quede debidamente documentada, registrando fecha, causa del fallo, acciones realizadas y resultados. Esta trazabilidad facilita análisis futuros, mejora la gestión y contribuye a la planificación efectiva del mantenimiento preventivo.

Manual de Gestión Medioambiental

La gestión medioambiental en el área de soporte informático es una responsabilidad clave que busca minimizar el impacto ambiental derivado de la operación tecnológica. Para ello, se implementan políticas y procedimientos orientados al manejo adecuado de los residuos electrónicos y a la promoción de prácticas sostenibles dentro de la organización.

Gestión de Residuos de Aparatos Eléctricos y Electrónicos (RAEE)

El manejo responsable de los RAEE está regulado por normativas nacionales e internacionales que exigen una correcta segregación, almacenamiento y disposición final de estos residuos. La organización debe trabajar exclusivamente con gestores autorizados que cumplan con los estándares legales y ambientales para el reciclaje y tratamiento de estos materiales. Esto garantiza la reducción de la contaminación y la recuperación de materiales valiosos, evitando riesgos para la salud y el entorno.

Inventario y Control de Equipos Fuera de Uso

Es fundamental contar con un registro actualizado y detallado de los equipos que han sido dados de baja o que ya no cumplen los requisitos técnicos o normativos para su uso. Estos dispositivos deben ser identificados y etiquetados claramente, para luego ser almacenados temporalmente en un área segura hasta su disposición definitiva.

Este proceso permite controlar su trazabilidad, evitar pérdidas o extravíos, y cumplir con las obligaciones legales vigentes, minimizando así posibles sanciones y daños ambientales.