

Manual técnico de soporte informático – Versión 2026

Área de Soporte Informático

Fecha 17/02/2026

Versión 1.0

Clasificación: Público

ÍNDICE

01**Soporte IT: Pilar Estratégico de la Operación Tecnológica****02****Inventario y Mantenimiento de Hardware****03****Administración y Estándares de Sistemas****04****Diagnóstico y Resolución de Incidencias de Red****05****Procedimientos de Soporte para Sistemas Empresariales****06****Protocolos de Seguridad y Cumplimiento****07****Flujos de Trabajo y Niveles de Intervención****08****Herramientas Esenciales para el Soporte Técnico****09****Gestión de documentación y conocimiento**

Soporte IT: Pilar Estratégico de la Operación Tecnológica

El soporte informático no es únicamente un recurso operativo; constituye un **elemento estratégico dentro de la infraestructura tecnológica de la organización**. Su implementación adecuada asegura la continuidad operativa, minimiza riesgos de interrupción y garantiza una experiencia de usuario final óptima, manteniendo los servicios TI disponibles, eficientes y seguros.

El equipo de soporte técnico actúa como **interfaz entre los usuarios y los sistemas corporativos**, gestionando incidencias, realizando mantenimiento preventivo y administrando herramientas críticas. Su trabajo coordinado con los departamentos de **infraestructura, redes, seguridad informática y desarrollo de software** permite una gestión integral de la plataforma tecnológica, asegurando que los procesos de negocio se ejecuten sin interrupciones.

Soporte IT: Pilar Estratégico de la Operación Tecnológica

Microinformática

Gestión de estaciones de trabajo, portátiles, dispositivos móviles y periféricos corporativos.

Aplicaciones corporativas y sistemas críticos

Soporte a software ofimático, herramientas colaborativas, sistemas ERP/CRM y aplicaciones web internas.

Redes e infraestructura

Diagnóstico, mantenimiento y resolución de incidencias en redes, conectividad, servidores y dispositivos de usuario.

Servicio al usuario final

Atención de incidencias, asesoramiento técnico, resolución de problemas y seguimiento de tickets según los SLA corporativos.

Inventario y mantenimiento de hardware

La gestión del hardware corporativo es fundamental para garantizar la continuidad operativa y minimizar fallos en los equipos y periféricos utilizados por usuarios y departamentos TI. Un inventario actualizado y un mantenimiento preventivo sistemático prolongan la vida útil de los dispositivos y aseguran un rendimiento óptimo.

Hardware corporativo

Estaciones de trabajo y portátiles

Actualizaciones de firmware, validación de memoria y almacenamiento.

Dispositivos móviles

Configuración segura y sincronización con MDM corporativo.

Servidores

Monitoreo, actualización de firmware y revisión de redundancia.

Periféricos

- **Impresoras, escáneres y multifuncionales:** mantenimiento y actualización de drivers.
- Monitores y docking stations: limpieza y verificación de conectores.

Administración y Estándares de Sistemas

La administración de **sistemas operativos** es un componente esencial del soporte corporativo, ya que garantiza la estabilidad, seguridad y eficiencia de los equipos dentro de la organización. Cada plataforma (Windows, Linux, macOS) requiere procedimientos específicos para asegurar cumplimiento con **políticas de seguridad, actualizaciones regulares y configuración óptima para la operación empresarial.**



Windows

Configuración base

Aplicación de GPOs (Group Policy Objects) y políticas de seguridad corporativas.

Gestión de perfiles y software

Administración de cuentas de usuario, control de permisos, instalación de actualizaciones críticas y supervisión de aplicaciones instaladas.

Actualizaciones y parches

Planificación de despliegue de parches y control de versiones para mantener estabilidad y seguridad del sistema.

Administración y Estándares de Sistemas



Linux

Distribuciones soportadas

Selección de versiones corporativas estables y mantenidas.

Supervisión de procesos y servicios críticos

Monitoreo de logs, servicios de red y recursos del sistema para garantizar disponibilidad y rendimiento.

Hardening básico

Configuración de firewall, permisos de archivos, desactivación de servicios innecesarios y aseguramiento de acceso SSH.

Gestión de paquetes y repositorios

Instalación, actualización y auditoría de software mediante gestores de paquetes (APT, YUM, DNF).



MacOs

MDM Corporativo

Administración centralizada de dispositivos, políticas de seguridad y despliegue de software.

Políticas de seguridad y cifrado

Monitoreo de logs, servicios de red y recursos del sistema para garantizar disponibilidad y rendimiento.

Configuración de red y acceso seguro

Ajustes de VPN, WiFi corporativa y restricciones de acceso a servicios internos.

Diagnóstico y Resolución de Incidencias de Red

La infraestructura de red es el **pilar de la conectividad corporativa**, y su correcta gestión es crítica para la continuidad de los servicios TI. El soporte técnico debe contar con procedimientos estandarizados para **identificar, diagnosticar y resolver incidencias de conectividad**, así como validar que la infraestructura física y lógica funcione según los estándares corporativos

Todo técnico de soporte debe comprender los componentes clave de la red:

DHCP (Dynamic Host Configuration Protocol)

Asignación automática de direcciones IP a dispositivos.

DNS (Domain Name System)

Resolución de nombres de dominio para acceder a recursos internos y externos.

VLANs (Virtual LANs)

Segmentación de red para seguridad y eficiencia de tráfico.

WiFi corporativa

Configuración segura, autenticación y cobertura en toda la organización.

Proxies y firewalls

Control de acceso y filtrado de tráfico de manera centralizada.

Diagnóstico y Resolución de Incidencias de Red

Procedimientos ante incidencias comunes

Pérdida de conectividad

- Verificar la conexión física y los indicadores LED de switches y routers.
- Comprobar la configuración IP y asignación DHCP.

Problemas de resolución DNS

- Validar que los servidores DNS estén accesibles.
- Probar resolución de nombres mediante nslookup o dig.

Lentitud de red o saturación de ancho de banda

- Monitorear tráfico en switches y routers.
- Identificar dispositivos o aplicaciones que consuman excesivo ancho de banda.

Conflictos de IP

- Revisar asignaciones DHCP y reservas.
- Identificar dispositivos con IP duplicada y reasignar según políticas corporativas.

Diagnóstico y Resolución de Incidencias de Red

Validación de infraestructura

- Revisar cableado estructurado y conectores RJ-45 para asegurar continuidad física.
- Comprobar switches, routers y puntos de acceso, verificando configuración, firmware y logs de eventos.
- Validar redundancia de enlaces y segmentación de VLANs.

Checklist técnico de diagnóstico

-  Ejecutar pruebas básicas: ping, traceroute, nslookup / dig.
-  Confirmar puerta de enlace y rutas de red correctas.
-  Evaluar conectividad en diferentes capas del modelo OSI, identificando si el fallo es físico, de enlace, de red o de transporte.
-  Documentar cada acción y resultado para trazabilidad.

Procedimientos de Soporte para Sistemas Empresariales

El soporte a aplicaciones corporativas es fundamental para garantizar la **continuidad operativa** y la **productividad** de los usuarios. Su correcta gestión permite resolver incidencias de forma ágil y asegurar la estabilidad de los sistemas empresariales.

Ambitos de soporte

- Aplicaciones ofimáticas y herramientas colaborativas.
- Sistemas CRM, ERP y plataformas corporativas.
- Aplicaciones web internas y servicios en la nube.
- Integraciones con proveedores y sistemas externos.

Incidencias habituales

- Fallos de autenticación y accesos denegados.
- Problemas de compatibilidad o versiones desactualizadas.
- Errores de configuración y permisos de usuario.
- Lentitud o indisponibilidad del servicio.

Procedimientos de Soporte para Sistemas Empresariales

Procedimiento de actuación

- Verificación inicial del problema y su alcance.
- Revisión de conectividad y configuración del usuario.
- Análisis de logs y mensajes de error.
- Aplicación de solución estándar o escalado técnico.

Escalado y documentación

- Derivación a equipos especializados o proveedores cuando sea necesario.
- Registro completo de la incidencia en el sistema de tickets.
- Documentación de causa, acciones realizadas y solución aplicada.

Protocolos de Seguridad y Cumplimiento

La seguridad informática es un eje fundamental en las actividades de soporte. Todo técnico debe actuar conforme a políticas corporativas de seguridad, garantizando la protección de la información, la integridad de los sistemas y la confidencialidad de los datos gestionados.

Gestión de accesos

Aplicación del principio de privilegios mínimos, otorgando únicamente los permisos estrictamente necesarios.

Uso responsable de cuentas administrativas y control de sesiones privilegiadas.

Bloqueo y revocación inmediata de accesos ante cambios de rol o desvinculaciones.

Gestión segura de credenciales, evitando el almacenamiento no autorizado de contraseñas.

Actualizaciones y mitigación de vulnerabilidades

Instalación periódica de parches de seguridad en sistemas operativos y aplicaciones.

Verificación del estado de antivirus, EDR y herramientas de protección corporativa.

Evaluación de configuraciones inseguras y aplicación de medidas de hardening

Protocolos de Seguridad y Cumplimiento

Contención de incidentes

Identificación temprana de comportamientos anómalos o posibles infecciones de malware.

Aislamiento de equipos comprometidos y notificación al área de seguridad.

Seguimiento de procedimientos internos de respuesta ante incidentes.

Registro y auditoría

Trazabilidad de cambios efectuados en configuraciones o sistemas.

Documentación detallada de todas las intervenciones realizadas.

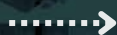
Cumplimiento de normativas internas y requisitos de auditoría.

Procedimientos de Soporte para Sistemas Empresariales

El servicio de soporte técnico se organiza en **niveles de atención** para garantizar una gestión eficiente de incidencias, optimizar tiempos de respuesta y asegurar que cada problema sea tratado por el personal adecuado.

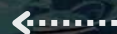
Nivel 1

Atención inicial



- Registro y categorización de tickets.
- Resolución de incidencias estándar.
- Asistencia directa al usuario final.
- Escalado documentado a niveles superiores cuando sea necesario.

- Diagnóstico técnico avanzado.
- Intervención en configuraciones de sistemas y aplicaciones.
- Coordinación con equipos de redes, infraestructura y seguridad.
- Aplicación de soluciones técnicas complejas.

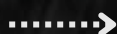


Nivel 2

Soporte especializado

Nivel 3

Soporte experto



- Resolución de incidencias críticas.
- Interacción con fabricantes y proveedores.
- Análisis de causa raíz (RCA).
- Implementación de correcciones definitivas.

Herramientas Esenciales para el Soporte Técnico

El soporte informático requiere un conjunto de herramientas profesionales que permitan gestionar incidencias, administrar equipos y garantizar la continuidad operativa de forma eficiente, segura y trazable.

Monitorización

Supervisión del estado de equipos, servicios y red, con alertas automáticas.

Gestión de tickets

Registro, seguimiento y priorización de incidencias según SLA.

Control remoto

Asistencia técnica segura a los usuarios finales.

Diagnóstico

Análisis de hardware, software y rendimiento del sistema.

Gestión de parches

Despliegue de actualizaciones y control de versiones.

Inventario TI

Control de activos, licencias y ciclo de vida de dispositivo

Gestión de documentación y conocimiento

La gestión del conocimiento es un elemento estratégico dentro del soporte informático. La correcta documentación de procedimientos, incidencias y soluciones permite transformar la experiencia diaria del equipo técnico en un **recurso estructurado y reutilizable**, mejorando la eficiencia operativa y la calidad del servicio.

Base de conocimiento (Knowledge Base – KB)

Una base de conocimiento actualizada y organizada constituye el principal repositorio de información técnica del departamento de soporte. Su objetivo es:

Centralizar soluciones a problemas recurrentes.

Facilitar la resolución rápida de incidencias.

Unificar criterios técnicos y procedimientos.

Reducir tiempos de diagnóstico y escalado.

La KB debe mantenerse accesible, estructurada y en constante actualización para reflejar la realidad del entorno tecnológico.

Gestión de documentación y conocimiento

Documentación de procedimientos estándar (SOP)

Todos los procesos críticos del área de soporte deben estar formalmente documentados mediante procedimientos operativos estándar, que incluyan:

Pasos detallados de resolución.

Herramientas necesarias.

Responsables y niveles de escalado.

Recomendaciones y buenas prácticas.

Esto garantiza uniformidad en la actuación del equipo y continuidad del servicio ante cambios de personal.

Registro de incidencias y soluciones

Cada intervención técnica debe quedar registrada de manera clara y completa:

- Descripción del problema.
- Causa identificada.
- Acciones realizadas.
- Solución aplicada

Permite generar estadísticas, detectar tendencias y prevenir la repetición de fallos.

Gestión de documentación y conocimiento

Uso de plantillas técnicas

El empleo de plantillas estandarizadas para tickets, informes y procedimientos asegura:

Coherencia en la información registrada.

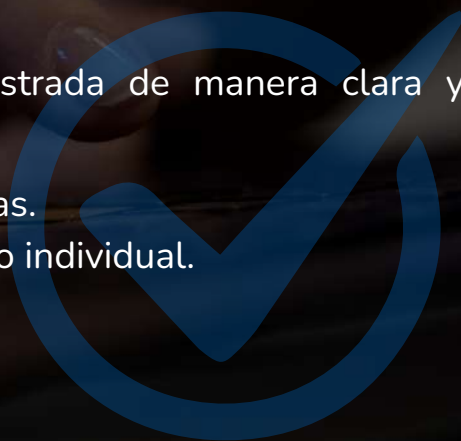
Claridad en la comunicación técnica.

Facilidad para auditorías y revisiones.

Beneficios operativos

Cada intervención técnica debe quedar registrada de manera clara y completa:

- Mayor rapidez en la resolución de incidencias.
- Reducción de dependencia del conocimiento individual.
- Formación más ágil de nuevos técnicos.
- Mejora continua del servicio de soporte.



Fortalece la eficiencia de tu soporte técnico.

CONTACTA CON NOSOTROS



www.qualoom.es



contacto@qualoom.es



(+34) 91 236 4808

