qualoom®

Inspiring Technology
for People

Checklist Integral para la Implementación de Oficinas Híbridas

Área de Soporte Informático
Fecha 12/05/2026
Versión 1.0
Clasificación: Público

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

qualoom®

Inspiring Technology
for People

Transformación del Entorno Laboral hacia el Modelo Híbrido

La adopción del modelo de oficina híbrida exige una infraestructura tecnológica sólida, segura y flexible que permita combinar el trabajo presencial con el remoto sin afectar la productividad ni la seguridad de la información.

Las organizaciones actuales dependen cada vez más de:

- Plataformas de colaboración en la nube
- Dispositivos portátiles corporativos
- Acceso remoto a sistemas críticos
- Herramientas digitales de comunicación

Este documento tiene como objetivo proporcionar un marco técnico de referencia que permita evaluar el nivel de preparación de una organización frente al trabajo híbrido, identificando carencias, riesgos y oportunidades de mejora.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Componentes IT del Puesto de Trabajo Híbrido

La falta de estandarización provoca problemas de compatibilidad, interrupciones del servicio y mayores riesgos de seguridad.
Por ello, es imprescindible definir un modelo único de puesto de trabajo que funcione de forma idéntica tanto en la oficina como en remoto.

Puesto de trabajo en oficina

El entorno presencial debe permitir que cualquier usuario pueda conectarse con su portátil y comenzar a trabajar de inmediato.
Para ello se requiere:

Docking stations universales

Simplifiquen la conexión del equipo a red, monitores y periféricos.

Monitores externos y periféricos corporativos

Mejora la productividad y la ergonomía.

Conectividad estable por cable y WiFi corporativa

Evitando depender de configuraciones manuales.

Infraestructura eléctrica y de red organizada

Que garantice disponibilidad y seguridad.

qualoom®

Inspiring Technology for People

Componentes IT del Puesto de Trabajo Híbrido

Equipamiento para teletrabajo

El usuario remoto debe disponer de herramientas equivalentes a las de la oficina:

- Portátil corporativo gestionado por TI
- Auriculares y cámara para reuniones virtuales
- Accesorios homologados para movilidad
- Acceso seguro a los sistemas corporativos

Todos los dispositivos deben estar:

- Registrados en el inventario corporativo
- Administrados mediante herramientas de gestión centralizada
- Protegidos con cifrado y políticas de seguridad
- Actualizados de forma automática

Gestión técnica del equipamiento

Para garantizar un funcionamiento correcto se deben aplicar controles periódicos:

- Verificación de hardware y estado de baterías
- Actualización de drivers y firmware
- nstalación de software corporativo estandarizado
- Comprobación del correcto funcionamiento de periféricos
- Sustitución preventiva de equipos obsoletos

qualoom®

Inspiring Technology
for People

Conectividad Estable y Segura

La conectividad es el pilar fundamental del modelo de trabajo híbrido.
Es imprescindible garantizar que tanto los usuarios en oficina como los usuarios remotos dispongan de conexiones seguras, estables y monitorizadas.

Conectividad en la oficina

La infraestructura de red corporativa debe estar preparada para soportar un alto volumen de dispositivos y accesos simultáneos. Requisitos principales simultáneos:

- **Redes WiFi** de alta densidad con cobertura total
- Segmentación del tráfico mediante VLAN
- Red cableada disponible para puestos críticos
- Sistemas de monitorización de rendimiento
- Gestión centralizada de puntos de acceso
- Políticas de calidad de servicio (QoS)

Objetivo

Garantizar una experiencia de conexión rápida, segura y estable para todos los empleados.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Conectividad Estable y Segura

Conectividad en remoto

El acceso desde ubicaciones externas introduce nuevos retos que deben ser gestionados por TI.

- Definición de requisitos mínimos de conexión (ancho de banda y estabilidad)
- Validación de la calidad de la conexión doméstica
- Acceso seguro a recursos corporativos
- Soporte técnico para configuraciones remotas
- Pruebas previas a la incorporación del usuario

Objetivo

Asegurar que el trabajador remoto pueda operar con el mismo nivel de servicio que en la oficina

Controles técnicos imprescindibles

Para mantener un entorno híbrido funcional y protegido, se deben verificar periódicamente:

- Configuración correcta de firewalls corporativos
- Funcionamiento de servicios DNS y DHCP
- Estado de gateways y rutas de acceso
- Pruebas de latencia, jitter y pérdida de paquetes
- Monitorización del consumo de ancho de banda
- Detección temprana de cuellos de botella

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Protección Integral en Modelos de Trabajo Distribuido

El modelo de trabajo híbrido amplía el perímetro tradicional de la organización.
Por este motivo, la seguridad informática debe evolucionar hacia un enfoque integral basado en la **protección del usuario, del dispositivo y de la información, independientemente del lugar desde el que se trabaje.**

Controles de seguridad esenciales

Para operar de forma segura en entornos híbridos es imprescindible implantar los siguientes mecanismos:

Autenticación multifactor (MFA)

Refuerzo obligatorio de la identidad del usuario mediante múltiples factores de autenticación.

Gestión de accesos basada en roles (RBAC)

Concesión de permisos únicamente en función de las necesidades reales de cada perfil.

Cifrado de dispositivos y comunicaciones

Protección de la información almacenada y transmitida para evitar accesos no autorizados.

Gestión centralizada de actualizaciones

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

qualoom®

Inspiring Technology
for People

Protección Integral en Modelos de Trabajo Distribuido

Protección avanzada del endpoint (EDR/XDR)

Detección y respuesta ante amenazas en tiempo real en todos los dispositivos corporativos.

Acceso remoto seguro

Conexiones protegidas mediante VPN corporativa o arquitecturas Zero Trust (ZTNA).

Procedimientos de respuesta a incidentes

Protocolos claros para la detección, contención y recuperación ante ciberincidentes.

Gestión del dispositivo corporativo

Cada equipo utilizado en el entorno híbrido debe cumplir una serie de requisitos mínimos de seguridad:

- Registro obligatorio en plataformas de gestión (MDM/UEM)
- Políticas de bloqueo automático y contraseñas robustas
- Control de aplicaciones instaladas
- Configuración remota y borrado seguro en caso de pérdida
- Monitorización continua del estado del dispositivo

Este enfoque permite a TI mantener el control y la protección incluso fuera de la red corporativa.

qualoom®

Inspiring Technology
for People

Ecosistema Digital para la Productividad Híbrida

La colaboración digital es el núcleo del trabajo híbrido.

El objetivo es garantizar que los procesos de comunicación y colaboración sean **eficientes, seguros y estandarizados** en toda la organización.

Herramientas esenciales

Video conferencia corporativa

Plataformas certificadas que aseguren calidad de audio/video, cifrado de extremo a extremo y compatibilidad con calendarios corporativos.

Integración con calendarios y directorios:

Sincronización automática de agendas y permisos de acceso, evitando conflictos de programación y garantizando seguridad en la gestión de usuarios.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Ecosistema Digital para la Productividad Híbrida

Gestión documental en la nube

Almacenamiento centralizado con control de versiones, permisos granulares y cifrado de información sensible.

Mensajería empresarial segura

Comunicación instantánea protegida, con historial auditable y cumplimiento de normativas de privacidad.

Sistemas de reserva de recursos

Herramientas para gestionar salas, equipos y otros recursos compartidos, optimizando la utilización de espacios físicos y virtuales.

Controles operativos

Para asegurar un ecosistema colaborativo confiable, deben verificarse:

- Versiones actualizadas de todas las aplicaciones corporativas.
- Validación de permisos y accesos de cada usuario.
- Pruebas regulares de audio y video en plataformas de videoconferencia.
- Sincronización y compatibilidad entre dispositivos móviles, portátiles y estaciones de trabajo.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Soporte Técnico para Entornos Híbridos

En un entorno de trabajo híbrido, los usuarios acceden a los sistemas corporativos desde distintas ubicaciones y dispositivos.
Esta realidad exige un modelo de soporte técnico capaz de ofrecer **asistencia eficiente, coherente y segura,** independientemente del lugar desde el que se trabaje.

Modelo de atención al usuario

El servicio de soporte debe basarse en procesos estandarizados y canales claramente definidos:

Canales de soporte unificados

Permitan al usuario contactar con TI a través de un punto único de entrada.

Sistema de ticketing centralizado

Para el registro, clasificación y seguimiento de incidencias.

Priorización de incidencias

Considerando impacto en el negocio y urgencia.

Procedimientos específicos

Para incidencias críticas, con criterios de escalado definidos.

Gestión técnica y soporte remoto

La resolución de incidencias en entornos híbridos debe apoyarse principalmente en capacidades de gestión remota:

Herramientas de control remoto seguras para asistencia al usuario.

Monitorización básica del estado de los dispositivos y servicios.

qualoom®

Inspiring Technology
for People

Soporte Técnico para Entornos Híbridos

Automatización de tareas recurrentes, como actualizaciones y parches.

Capacidad de intervención rápida sin necesidad de desplazamiento físico.

Estas prácticas permiten **reducir tiempos de respuesta y mejorar la experiencia del usuario.**

Controles operativos esenciales

Para garantizar la eficacia del soporte técnico, es necesario mantener:

- Inventario actualizado de dispositivos y usuarios.
- Control de versiones de sistemas operativos y aplicaciones.
- Registro histórico de incidencias y soluciones aplicadas.
- Documentación básica de procedimientos y buenas prácticas.

qualoom®

Inspiring Technology
for People

Estrategias de Continuidad y Recuperación Tecnológica

En un entorno híbrido, la continuidad operativa es crítica para garantizar que los servicios y sistemas corporativos permanezcan disponibles, incluso ante fallos, incidentes o desastres.

El objetivo es asegurar la **disponibilidad ininterrumpida de los servicios críticos,** minimizando el impacto en la operación y protegiendo la información corporativa.

Elementos clave de continuidad

Planes de respaldo y restauración

- Definición de políticas de backup para sistemas, aplicaciones y datos críticos.
- Frecuencia de copias según criticidad y requerimientos legales.
- Procedimientos claros de restauración para distintos escenarios de pérdida de información.

Redundancia de sistemas críticos

- **Servidores y aplicaciones con duplicidad o failover automático.**
- **Infraestructura de red y almacenamiento con alta disponibilidad.**

qualoom®

Inspiring Technology
for People

Estrategias de **Continuidad y Recuperación** Tecnológica

Alta disponibilidad en la nube

- Servicios críticos alojados en plataformas cloud con replicación geográfica.
- Monitoreo continuo de disponibilidad y rendimiento.

Planes BC/DR adaptados al trabajo híbrido

- Escenarios de contingencia que incluyan tanto usuarios presenciales como remotos.
- Procedimientos de comunicación, acceso a recursos y recuperación de operaciones.

Pruebas periódicas de recuperación

- Simulaciones regulares de fallos y desastres.
- Validación de tiempos de restauración y efectividad de los planes.
- Documentación de hallazgos para mejorar continuamente los procesos.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Evaluación y Mejora del Entorno Híbrido

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

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Fortalece la eficiencia de tu soporte técnico.

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808

Más información www.qualoom.es