qualoom®

Inspiring Technology
for People

Guía técnica de **Respaldo y Recuperación de datos del usuario final**

Área de Seguridad
Fecha 28/05/2025
Versión 1.0

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

Introducción

En un **ecosistema digital** donde los datos son el principal activo de cualquier organización, su pérdida puede traducirse en consecuencias operativas, legales y financieras graves. Por ello, la planificación y ejecución de estrategias de respaldo y recuperación no debe limitarse a tareas de rutina técnica, sino enmarcarse dentro de una **política integral de gestión de la información.**

Esta guía está diseñada para profesionales de soporte microinformático, técnicos de sistemas y responsables IT que buscan establecer o **mejorar sus políticas de respaldo**. Aporta una base teórica sólida, herramientas prácticas y directrices técnicas contrastadas por experiencia profesional en campo.

qualoom®

Inspiring Technology
for People

Conceptos **fundamentales**

¿Por qué es crítico respaldar datos?

Los datos del usuario final suelen ser los más expuestos a la pérdida o corrupción debido diferentes factores como, el uso cotidiano en dispositivos susceptibles a fallos, la exposición a entornos externos (USBs, descargas, correos maliciosos) o la alta frecuencia de edición y actualización.

Amenazas comunes

Ransomware: Cifra los archivos y exige un rescate.

Errores humanos: Eliminación accidental o sobrescritura.

Fallo de hardware: Especialmente en discos duros sin redundancia.

Daños físicos: Incendios, agua, impactos.

Ciberataques: Inyecciones de malware, sabotajes internos.

Objetivos del backup

RTO (Recovery Time Objective): Tiempo máximo aceptable para recuperar los datos.

RPO (Recovery Point Objective): Cantidad máxima de datos que pueden perderse sin impacto crítico.

qualoom®

Inspiring Technology
for People

Tipos **de backup**

Backup completo

- Copia todos los archivos seleccionados.
- Ideal como base semanal o mensual.
- Requiere mayor capacidad y tiempo

Incremental

- Solo guarda archivos modificados desde el último backup (de cualquier tipo).
- Rapidez y eficiencia en espacio.
- Restauración más compleja: requiere la última copia completa y todas las incrementales.

Diferencial

- Guarda cambios desde el último backup completo.
- Restauración más rápida que el incremental, pero uso de espacio mayor.

En espejo

- Reproducción exacta y constante.
- Muy útil en entornos de alta disponibilidad.
- No conserva versiones anteriores.

Otros tipos

- **Continuo (CDP):** Guarda cada cambio en tiempo real.
- **Snapshots:** Copia instantánea del estado del sistema, frecuente en entornos virtualizados.

qualoom®

Inspiring Technology
for People

ESTRATEGIAS EFECTIVAS DE BACKUP

Regla 3-2-1 en profundidad
3 copias: Original + 2 copias de seguridad.
2 formatos: Disco duro + nube, cinta + NAS, etc.
1 fuera del sitio: Prevención ante desastres físicos.

Comparativa local vs nube

Aspecto	Backup Local	Backup en la nube
Velocidad	Alta en recuperación	Depende del ancho de banda
Seguridad	Alta si cifrado y aislado	Requiere controles estrictos
Coste inicial	Alto	Bajo (SaaS)
Escalabilidad	Limitada físicamente	Escalable y flexible

Automatización
Uso de tareas programadas, scripts personalizados (PowerShell, Bash), software con cronogramas inteligentes y alertas automáticas.

Supervisión continua
Logs centralizados
Dashboards de estado
Integración con herramientas SIEM

qualoom®

Inspiring Technology
for People

TECNOLOGÍAS Y HERRAMIENTAS DISPONIBLES

Comerciales

- Veeam: Líder en entornos virtualizados (VMware, Hyper-V).
- Acronis Cyber Backup: Protección contra malware y backup unificado.
- Commvault: Gestión masiva de datos empresariales.

Gratuitas

- Rsync: Replicación basada en bloques, ideal para scripts.
- Duplicati: Compresión, cifrado y subida a múltiples servicios.
- Cobian Backup: Interfaz sencilla, ideal para escritorios y PYMEs.

En la nube

- Google Workspace + Vault: Versionado y retención legal.
- Microsoft 365 + OneDrive/SharePoint: Integración nativa con entornos Windows.
- Dropbox Business: Control granular de permisos.

Evaluación comparativa

- Soporte técnico
- Velocidad de restauración
- Compatibilidad OS
- Políticas de versionado

qualoom®

Inspiring Technology
for People

FLUJOS Y PROCEDIMIENTOS OPERATIVOS

IDENTIFICACIÓN → CLASIFICACIÓN → SELECCIÓN DE ESTRATEGIA → CONFIGURACIÓN

Flujo recomendado

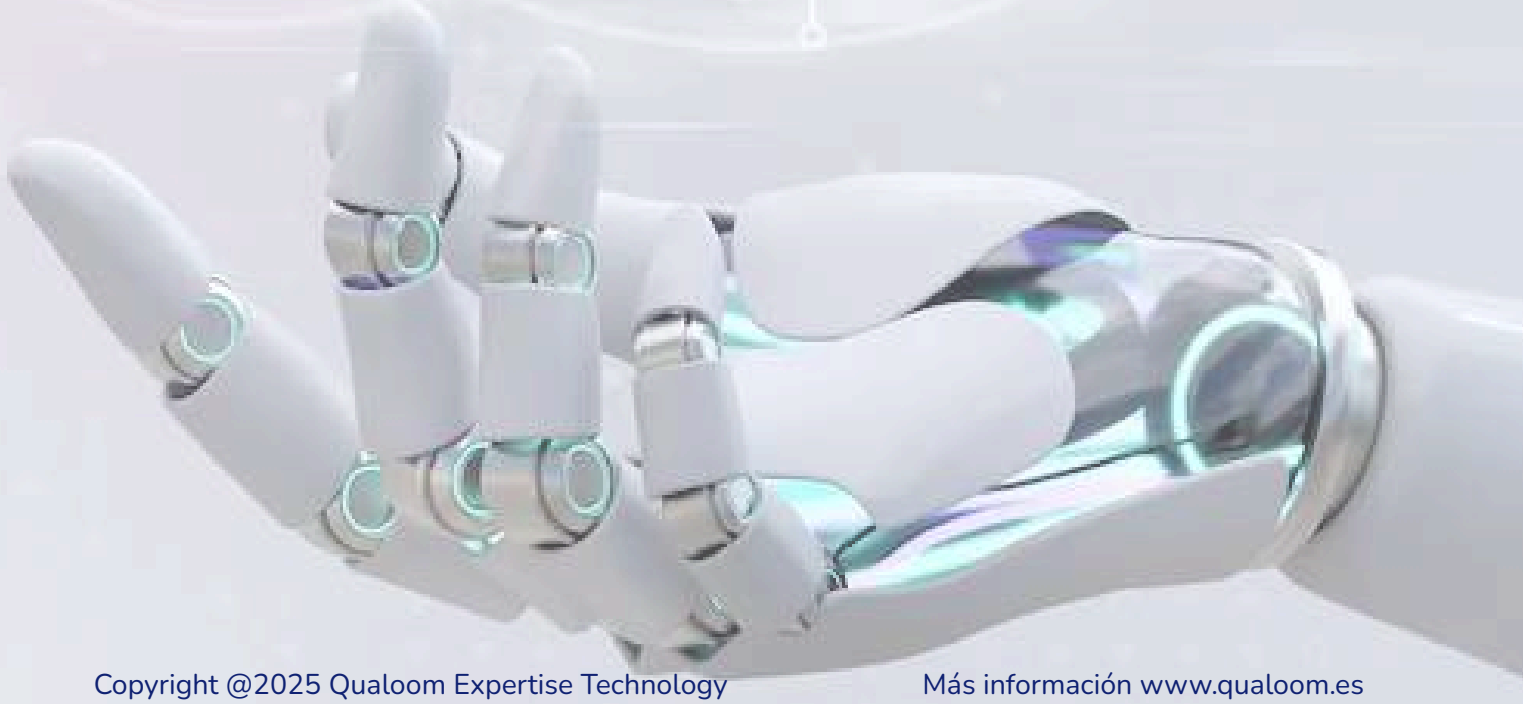
EJECUCIÓN → SUPERVISIÓN → VERIFICACIÓN

Restauración en diferentes escenarios

- Archivo individual eliminado: Acceso a versión previa.
- Cifrado por ransomware: Reimágenes y restauración completa.
- Corrupción del sistema: Restauración desde imagen o snapshot.

Pruebas de recuperación

- Simulación trimestral o semestral
- Cronogramas de recuperación documentados
- Responsables designados



Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

PROTOCOLOS Y POLÍTICAS DE SEGURIDAD

Políticas de retención

- Datos críticos: 1 año o más
- Operacionales: 30-90 días
- Proyectos: según SLA contractual

Verificación

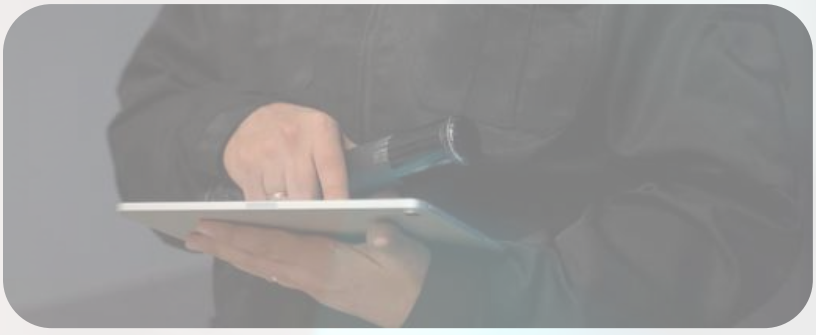
- Checksums automáticos
- Comparación hash previa y posterior
- Pruebas automatizadas de integridad

Seguridad

- Cifrado AES-256
- Accesos segregados
- Autenticación multifactor (MFA)
- Registro de accesos y modificaciones

Normativas y compliance

- RGPD/LOPDGDD: Consentimiento y derecho a eliminación.
- ISO/IEC 27001: Gestión de seguridad de la información.
- SOX/HIPAA: Controles internos y protección de datos sanitarios.



qualoom®

Inspiring Technology
for People

CASOS PRÁCTICOS Y EXPERIENCIA EN CAMPO

Escenarios reales

- Microempresa: Copia diaria en disco externo + respaldo semanal en la nube gratuita.
- PYME con 50 empleados: Veeam + repositorio NAS + Azure Backup.
- Corporación internacional: Cluster de backup replicado geográficamente + disaster recovery automatizado

Lecciones clave

- Probar siempre la recuperación
- Evitar depender de un solo formato
- Educar al usuario final sobre prácticas seguras

Contingencia

- Integración con el plan DRP (Disaster Recovery Plan)
- SLA internos y externos
- Contacto con proveedores críticos

CONCLUSIÓN

La gestión del respaldo y la recuperación de datos va más allá de una solución técnica: es una responsabilidad estratégica para garantizar la continuidad operativa y la resiliencia organizacional. La correcta planificación, implementación y prueba de sistemas de backup permite enfrentar amenazas modernas como el ransomware, errores humanos o catástrofes naturales.

Con esta guía, el profesional de soporte microinformático tiene las herramientas y criterios necesarios para liderar políticas robustas, escalables y seguras de respaldo de datos.