Checklist de Auditoría Veeam

Backup Infrastructure Assessment · jpcasco.com

v1.0 · 2025

AUDITOR	ENTORNO	FECHA	SCORE
nombre completo	producción / DR / test	dd/mm/aaaa	__ / 10

Marca cada control como **OK**, **NOK** o **N/A**. Un resultado por debajo de 7/10 requiere plan de acción inmediato. Prioridad: **CRÍTICO** → **ALTO** → **BUENAS PRÁCTICAS**.

01 INVENTARIO DE JOBS

- [ ] Todos los VMs/servidores críticos tienen job asignado — CRÍTICO
  Comprobar en Infrastructure > Managed Servers
- [ ] Jobs activos y sin errores en las últimas 24 h — CRÍTICO
  Home > Jobs — verificar estado "Success" o "Warning"
- [ ] Nomenclatura de jobs coherente y documentada — ALTO
  Facilita auditorías futuras y handover
- [ ] Jobs de agentes (físicos/cloud) incluidos en el inventario — ALTO
  Veeam Agent for Windows/Linux registrados

02 RETENCIÓN Y POLÍTICA RPO/RTO

- [ ] Política de retención ≥ 14 restore points o según SLA — CRÍTICO
  Job > Edit > Storage > Retention Policy
- [ ] RPO documentado y verificado contra frecuencia de job — CRÍTICO
  RPO de 24 h → job diario como mínimo
- [ ] RTO estimado para los sistemas Tier-1 — ALTO
  Tiempo de restauración completo documentado
- [ ] GFS (abuelo-padre-hijo) configurado para cumplimiento legal — BUENAS PRÁCTICAS
  Backup > Advanced Settings > GFS

03 VERIFICACIÓN DE RESTAURACIÓN

- [ ] SureBackup job configurado para VMs críticas — CRÍTICO
  Verifica integridad del backup arrancando la VM
- [ ] Prueba de restauración manual realizada en los últimos 90 días — CRÍTICO
  Instant Recovery o Full Restore documentado
- [ ] Resultado de SureBackup: 100% Success en último ciclo — ALTO
  Home > Last 24 hours > SureBackup
- [ ] Restore drill documentado con tiempo real de recuperación — BUENAS PRÁCTICAS
  Fundamental para el BIA / plan de continuidad

04 REPOSITORIOS Y ALMACENAMIENTO

- [ ] Capacidad libre > 20 % en todos los repositorios — CRÍTICO
  Backup Infrastructure > Backup Repositories
- [ ] Alertas de espacio configuradas (umbral recomendado: 80 %) — ALTO
  Options > Notifications > Disk space threshold

- [ ] SOBR (Scale-Out) configurado con política de placement — BUENAS PRÁCTICAS
  Recomendado para entornos medianos/grandes
- [ ] Inmutabilidad habilitada en al menos un repositorio — CRÍTICO
  Hardened Repository (Linux) o Object Storage con Lock

05 MODO DE TRANSPORTE DE DATOS

- [ ] Modo de transporte óptimo configurado (HotAdd o Direct SAN) — ALTO
  NBD sólo como fallback — impacta rendimiento de red
- [ ] Proxy dedicado para tareas de backup (no el vCenter) — ALTO
  Backup Infrastructure > Backup Proxies
- [ ] Throttling de ancho de banda configurado en horario producción — BUENAS PRÁCTICAS
  Options > Traffic > Network traffic rules

06 CIFRADO

- [ ] Cifrado en reposo habilitado en repositorios sensibles — CRÍTICO
  Repository > Edit > Advanced > Encryption
- [ ] Cifrado en tránsito habilitado para backups remotos/cloud — ALTO
  Job > Storage > Advanced > Enable backup file encryption
- [ ] Contraseña de cifrado almacenada en gestor de passwords (no en Veeam) — CRÍTICO
  Veeam guarda el hash — exportar la clave es responsabilidad tuya

07 ALERTAS Y NOTIFICACIONES

- [ ] Notificaciones por email habilitadas y verificadas — CRÍTICO
  Options > Email Settings — enviar test email
- [ ] Destinatarios de alertas actualizados (no cuentas genéricas) — ALTO
  Evitar alias tipo "it@empresa.com" no monitorizados
- [ ] Integración SNMP o SIEM configurada (si aplica) — BUENAS PRÁCTICAS
  Splunk / Sentinel / Zabbix con traps de Veeam
- [ ] Alerta de job fallido ≤ 1 h tras fallo — CRÍTICO
  Crítico para detectar ventanas de backup perdidas

08 REGLA 3-2-1 Y COPIA OFFSITE

- [ ] Al menos 3 copias de datos críticos existentes — CRÍTICO
  Producción + backup primario + offsite/cloud
- [ ] Copia en ≥ 2 medios diferentes (disco + cinta o cloud) — CRÍTICO
  Regla 3-2-1 original de Peter Krogh
- [ ] 1 copia offsite o en cloud (Azure Blob, S3, Wasabi…) — CRÍTICO
  Backup Copy Job o Direct-to-Cloud configurado
- [ ] 1 copia air-gapped o inmutable (regla 3-2-1-1-0) — ALTO
  Hardened Repo o cinta con eject automático

09 LICENCIAS

- [ ] Licencia válida y no expirada — CRÍTICO
  Help > About > License Information — caducidad

- [ ] Cobertura de sockets/instancias suficiente para el entorno actual — ALTO
  Verificar tras adición de nuevos hosts ESXi
- [ ] Renovación planificada con 30 días de antelación — ALTO
  Crear tarea en calendario del equipo

10 ACCESOS Y RBAC

- [ ] Roles Veeam definidos: Veeam Operator ≠ Veeam Administrator — CRÍTICO
  Users and Roles — principio de mínimo privilegio
- [ ] Sin cuentas de servicio compartidas entre equipos — CRÍTICO
  Cada persona o sistema con cuenta propia
- [ ] MFA habilitado para acceso a consola Veeam (si VBR 12+) — ALTO
  Configuration > General > Multi-factor Authentication
- [ ] Revisión de accesos realizada en los últimos 90 días — BUENAS PRÁCTICAS
  Documentar quién tiene acceso y con qué rol

TABLA DE PUNTUACIÓN

Puntuación	Nivel de Riesgo	Acción Recomendada
9 – 10	EXCELENTE	Mantener y revisar trimestral
7 – 8	BUENO	Resolver ítems ALTO en 30 días
5 – 6	MODERADO	Plan de acción en 2 semanas
0 – 4	CRÍTICO	Acción inmediata — escalado dirección