Protocolo de Respaldo y Recuperación (DR) – Buckets Amazon S3

Autor(es)/Equipo: Unelab

Cliente/Organización: Fincloud

Versión: 1.0

Tabla de Contenidos

1. Objetivo

Establecer el protocolo vigente de Fincloud para **proteger, respaldar y recuperar** información almacenada en **Amazon S3**, asegurando continuidad operativa ante:

- Borrado accidental y sobrescritura
- Cambios no autorizados o corrupción lógica
- Ransomware (borrado masivo o cifrado/alteración de datos)
- Falla regional (Disaster Recovery)

2. Alcance

Este protocolo aplica a **todos los buckets S3 administrados por Fincloud** que almacenen datos operacionales, de clientes, evidencia o auditoría.

Incluye:

- Controles de protección de datos (versionado, retención e inmutabilidad cuando corresponde)
- Replicación para continuidad y DR
- Seguridad mínima obligatoria (IAM, KMS, bloqueo de acceso público)
- Monitoreo y alertas operacionales
- Procedimientos de restauración y recuperación ante desastre
- Plan de pruebas, auditoría y control de cambios

No incluye:

- Backups de servicios distintos a S3 (RDS/EBS/EC2, etc.)
- DR completo de aplicaciones (solo la recuperación a nivel de almacenamiento y el cambio de origen a bucket DR)

3. Definiciones

- **RPO:** máxima pérdida de datos tolerable en tiempo.
- **RTO:** tiempo máximo para recuperar operación/datos.
- **Región Primaria:** región donde opera el bucket principal.
- **Región Secundaria (DR):** región secundaria destinada a recuperación ante desastres.
- **Cuenta Primaria:** cuenta AWS operativa.
- **Versioning:** mantiene versiones anteriores de objetos.
- **MFA Delete:** exige MFA para borrado permanente y operaciones críticas en buckets versionados.
  Object Lock (WORM): retención inmutable por período definido.
- **CRR:** replicación entre regiones (Cross-Region Replication).

4. Protocolo actual

Fincloud opera sus buckets S3 bajo los siguientes controles obligatorios:

1. **Versioning habilitado** en todos los buckets del alcance.
2. **Replicación CRR** habilitada desde Región Primaria hacia:
    - un bucket espejo en **Región Secundaria (DR)**
3. Replicación configurada para incluir:
    - **todas las versiones**,
    - **delete markers**,
    - **tags y metadatos**,
    - **cifrado**.
4. Política estándar de **retención y ciclo de vida** aplicada a objetos y versiones (sección 7).
5. Seguridad obligatoria: **Block Public Access**, **SSE-KMS**, permisos por roles y MFA en administración (sección 8).
6. Toda restauración y cambio de configuración se registra mediante **ticket**, con evidencias y aprobaciones (secciones 13 y 16).

5. Objetivos de recuperación (RPO/RTO)

- **RPO: ≤ 15 minutos**
- **RTO: ≤ 60 minutos**

El cumplimiento de RPO/RTO se basa en versionado + replicación CRR y los procedimientos de restauración definidos en este documento.

6. Estrategia de respaldo vigente

La estrategia de respaldo S3 en Fincloud se compone de tres capas aplicadas de forma conjunta:

6.1 Capa 1: Protección lógica – Versioning + MFA Delete

- Los buckets operan con **Versioning** habilitado.
- Para buckets críticos, Fincloud mantiene **MFA Delete** habilitado.
- La recuperación ante borrado/sobrescritura se realiza restaurando versiones o eliminando delete markers, según corresponda.

6.2 Capa 2: Continuidad y DR – CRR (Región Secundaria)

- La replicación se ejecuta hacia la Región Secundaria.
- Se mantiene un objetivo operacional de replicación alineado al **RPO ≤ 15 minutos**.

6.3 Capa 3: Gobernanza – Retención y ciclo de vida

- Todos los buckets del alcance aplican transición de almacenamiento y expiración final, incluyendo versiones no actuales.

7. Retención y ciclo de vida

Esta política aplica a **objetos y versiones** (actuales y no actuales).

7.1 Transición por antigüedad

- **Día 0–30:** S3 Standard
- **Día 31–90:** S3 Standard-IA
- **Día 91–365:** S3 Glacier Flexible Retrieval
- **Desde día 366:** S3 Glacier Deep Archive

7.2 Retención total

- **Retención total: 5 años**
- Se configura expiración final para objetos y versiones no actuales.

7.3 Inmutabilidad (auditoría/evidencia)

- Datos de auditoría/evidencia operan con **Object Lock** en modo **Compliance** por **5 años**.

8. Seguridad mínima obligatoria

8.1 IAM y control de acceso

- Acceso bajo principio **least privilege**.
- Roles operacionales:
  - `S3ReadOnlyRole`
  - `S3AppWriteRole` (limitado por prefijos)
  - `S3AdminRole`
- Acciones administrativas críticas restringidas a `S3AdminRole` con MFA:
  - cambios de policy, replicación, lifecycle, KMS, Object Lock
  - borrados masivos o eliminación de versiones

8.2 Cifrado

- En reposo: **SSE-KMS** obligatorio con CMK administrada por Fincloud.
- En tránsito: TLS obligatorio.

8.3 Acceso público

- **Block Public Access habilitado** en todos los buckets.
- Bucket policies aplican:
  - denegación de cargas sin SSE-KMS,
  - denegación de acciones administrativas fuera de roles autorizados.

9. Configuración técnica

9.1 Bucket Región Primaria

1. Crear bucket bajo naming estándar.
2. Habilitar Versioning.
3. Habilitar Block Public Access.
4. Configurar SSE-KMS por defecto.
5. Aplicar bucket policy (deny sin SSE-KMS + restricciones administrativas).
6. Aplicar tags obligatorias (`Environment`, `Owner`, `DataClass`, `Retention=7y`, `Criticality`, `ContainsAuditData`).

9.2 Buckets DR (Región Secundaria)

1. Crear bucket espejo en Región Secundaria.
2. Habilitar Versioning en ambos.
3. Configurar SSE-KMS con CMK del destino.
4. Habilitar Block Public Access.

9.3 Replicación CRR

1. Configurar role de replicación con permisos mínimos.
2. Configurar replicación a ambos destinos (Región Secundaria).
3. Incluir versiones, delete markers, tags/metadatos y cifrado.
4. Validar replicación con objeto de prueba.

9.4 Lifecycle

1. Configurar transiciones según sección 7.
2. Aplicar también a versiones no actuales.
3. Configurar expiración final 7 años.

9.5 Object Lock (auditoría/evidencia)

1. Habilitar Object Lock en bucket correspondiente.
2. Aplicar retención Compliance 7 años por prefijos de evidencia.
3. Validar que no existan permisos para reducir retención.

10. Monitoreo y alertas

Alertas obligatorias:

- Replicación atrasada (brecha respecto del RPO)
- Errores de replicación
- Cambios en policies/replication/lifecycle/KMS
- Picos anómalos de deletes/puts
- Denegaciones repetitivas o accesos anómalos

Auditoría:

- Registro de cambios y restauraciones con ticket y evidencias.
- CloudTrail habilitado según estándar interno.

11. Procedimientos de restauración (Runbook)

11.1 Borrado accidental

1. Abrir ticket “S3 Restore – Delete”.
2. Identificar bucket y key/prefijo.
3. Listar versiones y delete markers.
4. Restaurar versión correcta / eliminar delete marker.
5. Validar integridad y disponibilidad.
6. Cierre con causa raíz y acciones preventivas.

11.2 Sobrescritura/cambio no deseado

1. Abrir ticket “S3 Restore – Overwrite”.
2. Identificar la versión correcta por fecha/ETag/tamaño.
3. Restaurar versión a la key original.
4. Validar consumo por procesos.

11.3 Recuperación desde Glacier/Deep Archive

1. Abrir ticket “S3 Restore – Archive”.
2. Solicitar restore.
3. Esperar la ventana de restauración.
4. Copiar a clase de acceso necesaria para consumo.
5. Validar y cerrar.

11.4 Ransomware / borrado masivo

1. Revocar permisos de write/delete a roles no esenciales.
2. Validar estado de versiones y Object Lock (si aplica).
3. Restaurar desde versiones previas o desde bucket DR.
4. Revisar CloudTrail, rotar credenciales y endurecer políticas.
5. Post-mortem y mejoras.

12. Recuperación ante desastre (DR)

12.1 Disparadores

- Interrupción/degradación regional severa
- Indisponibilidad del bucket primario
- Incidente que requiera continuidad desde DR

12.2 Failover

1. Declarar incidente y activar canal de crisis.
2. Confirmar bucket DR (consistencia y último objeto replicado).
3. Cambiar configuración de aplicaciones para usar bucket DR.
4. Validar flujos críticos y monitorear.

12.3 Failback

1. Confirmar estabilidad en región primaria.
2. Sincronizar diferencias si corresponde.
3. Revertir aplicaciones al bucket primario.
4. Validación final y cierre.

13. Pruebas y auditoría

- **Mensual:** prueba de restauración con evidencias.
- **Trimestral:** simulacro DR validando RPO/RTO.
- **Anual:** auditoría de policies, roles, KMS, lifecycle, evidencias y control de cambios.

14. Gobernanza y control de cambios

- Todo cambio en replication/lifecycle/policies/KMS/Object Lock se gestiona por ticket con:
    - motivo, impacto, plan de rollback y aprobación.
- Toda restauración se registra con evidencias (objeto, versión restaurada, timestamp y validación).

15. Roles y responsabilidades (RACI)

Actividad	Responsable (R)	Aprueba (A)	Consultado (C)	Informado (I)
Configuración S3 (Versioning/CRR/Lifecycle)	DevOps	Seguridad	App Team	Stakeholders
IAM/KMS	Seguridad	Seguridad Lead	DevOps	Stakeholders
Monitoreo y alertas	DevOps	DevOps Lead	Seguridad	Stakeholders
Restauraciones	Operaciones/DevOps	DevOps Lead	App Team	Stakeholders
Simulacros DR	DevOps	Cliente/CTO	Seguridad/App Team	Stakeholders

16. Checklist operativo

Semanal

- Validación de alertas de replicación y errores
- Validación de cambios no autorizados en configuración
- Revisión de señales anómalas (deletes/puts)

Mensual

- Restore test con evidencias
- Revisión de ejecución de lifecycle y retenciones
- Validación de cifrado y permisos

Trimestral

- Simulacro DR y plan de mejoras