**UNIVERSIDAD DE GUAYAQUIL**

**FACULTAD DE CIENCIAS MATEMATICAS Y FISICA**

**CARRERA DE INGENERIA EN SISTEMAS COMPUTACIONALES**

**MATERIA:**

**SISTEMAS OPERATIVOS DISTRIBUIDOS**

**DOCENTE:**

**ING. CRESPO LEÓN CHRISTOPHER GABRIEL**

**ESTUDIANTE:**

**ANGIE ARACELY SALAZAR SALAZAR**

**TEMA DE PROYECTO:**

**REPLICACIÓN ENTRE REGIONES DE S3 Y BLOQUEO DE OBJETOS DE S3**

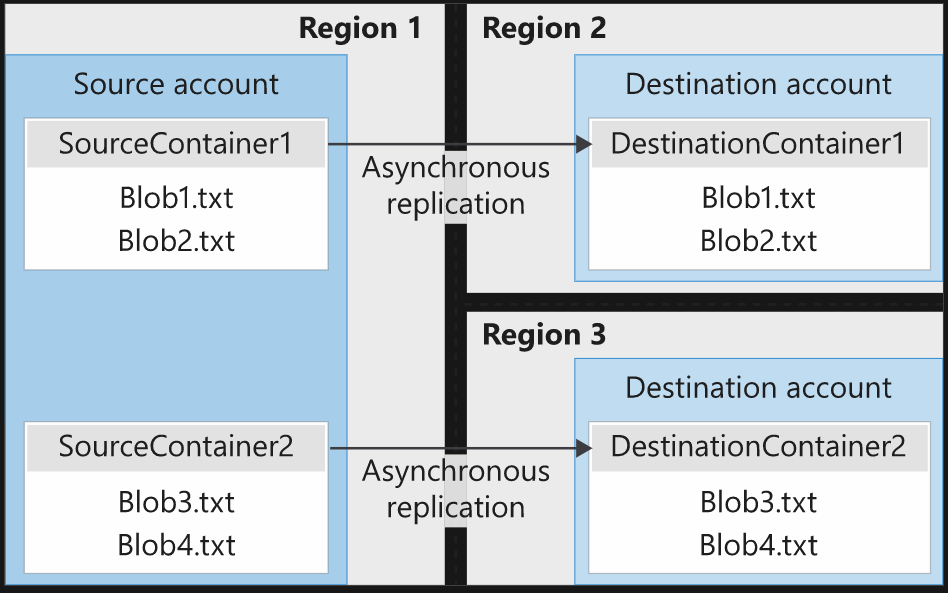
**CURSO:**

**ISI – S – NO – 7 – 4**

**Replicación entre regiones de S3 y Bloqueo de objetos de S3**

**Replicación de objetos**

La replicación nos permite copiar objetos entre buckets de Amazon S3 de forma automática y asincrónica. Los buckets que están configurados para reproducción de objetos pueden pertenecer a la misma Cuenta de AWS o a cuentas diferentes. El objeto se puede reproducir en un solo bucket de destino o en varios. Los buckets de destino pueden estar en diferentes Regiones de AWS o dentro de la misma región que el bucket de origen.



De forma predeterminada, la replicación solo admite la copia de nuevos objetos de Amazon S3 una vez habilitada. Para habilitar la replicación de objetos, añada una configuración de replicación a su bucket de origen. La configuración mínima, debe proporcionar lo siguiente:

* El bucket o buckets de destino en los que desea que Amazon S3 replique objetos
* Un rol de AWS Identity and Access Management (IAM) que Amazon S3 pueda asumir para reproducir objetos en su nombre

**Con la Replicación de objetos podemos:**

* **Replicar objetos conservando los metadatos**: puede utilizar la replicación para realizar copias de los objetos en las que se conserven todos los metadatos, como la hora de creación del objeto original y los ID de versión. Esta capacidad es importante si necesita asegurarse de que la réplica sea idéntica al objeto de origen.
* **Replicar objetos en diferentes clases de almacenamiento**: puede utilizar la replicación para colocar objetos directamente en S3 Glacier, S3 Glacier Deep Archive u otra clase de almacenamiento en los buckets de destino. También puede replicar los datos en la misma clase de almacenamiento y utilizar las políticas de ciclo de vida en los buckets de destino para mover objetos a una clase de almacenamiento con menos actividad conforme adquiere antigüedad.
* **Mantener copias de objetos con distintos propietarios**: independientemente de quién sea el propietario del objeto de origen, puede indicar a Amazon S3 que cambie la propiedad de la réplica a la Cuenta de AWS que posee el bucket de destino. Esto se conoce como la opción de invalidación del propietario. Puede usar esta opción para restringir el acceso a las réplicas de objetos.
* **Mantener los objetos almacenados en varias Regiones de AWS:** puede establecer varios buckets de destino en diferentes Regiones de AWS para garantizar las diferencias geográficas en el lugar donde se guardan los datos. Esto podría ser útil para cumplir ciertos requisitos de conformidad.
* **Reproducir objetos en 15 minutos**: puede utilizar el control de tiempo de reproducción de S3 (S3 RTC) para reproducir sus datos en la misma Región de AWS o en distintas regiones dentro de un periodo predecible. S3 RTC replica el 99,99 % de los objetos nuevos almacenados en Amazon S3 dentro de un plazo de 15 minutos (con el respaldo de un acuerdo de nivel de servicio).

**Requisitos de replicación**



**La replicación requiere lo siguiente:**

* El propietario del bucket de origen debe tener habilitadas las Regiones de AWS de origen y destino en su cuenta. El propietario del bucket de destino debe tener la región de destino habilitada en su cuenta.
* Ambos buckets de origen y destino deben tener habilitado el control de versiones.
* Amazon S3 debe tener permisos para replicar objetos desde el bucket de origen al bucket o buckets de destino en su nombre.
* Si el propietario del bucket de origen no posee el objeto en el bucket, el propietario del objeto debe conceder al propietario del bucket los permisos READ y READ\_ACP con la lista de control de acceso (ACL) del objeto.
* Si el bucket de origen tiene habilitado el bloqueo de objetos de S3, los buckets de destino deben tener también esa característica habilitada.

**Si va a definir la configuración de reproducción en un escenario entre cuentas en el que los buckets de origen y destino pertenecen a diferentes Cuentas de AWS, se aplica el siguiente requisito:**

* El propietario de los buckets de destino debe conceder al propietario del bucket de origen permisos para replicar objetos con una política de bucket.
* Los buckets de destino no se pueden configurar como buckets de pago por solicitante.

**Configuración de la replicación**

Para habilitar la replicación, simplemente añada una configuración de replicación a su bucket de origen. La configuración indica a Amazon S3 que replique los objetos de la forma especificada. En la configuración de replicación, debe proporcionar lo siguiente:

* **Los buckets de destino**: el bucket o buckets en los que desea que Amazon S3 replique los objetos.
* **Los objetos que desea replicar**: puede replicar todos los objetos del bucket de origen o de un subconjunto. Para identificar un subconjunto, proporcione un prefijo de nombre de clave, una o más etiquetas de objeto, o ambos en la configuración.
* Por ejemplo, si configura una regla de replicación para replicar solo objetos con el prefijo de nombre de clave Tax/, Amazon S3 replica objetos con claves como Tax/doc1 o Tax/doc2. Pero no un objeto con la clave Legal/doc3. Si especifica el prefijo y una o más etiquetas, Amazon S3 replica solo los objetos que tienen un prefijo de clave específico y las etiquetas.

Además de estos requisitos mínimos, puede elegir las siguientes opciones:

* **Clase de almacenamiento de réplica**: de forma predeterminada, Amazon S3 almacena réplicas de objetos mediante la misma clase de almacenamiento que el objeto de origen. Puede especificar una clase de almacenamiento diferente para las réplicas.
* **Propiedad de la réplica**: Amazon S3 supone que una réplica de objeto es propiedad del titular del objeto de origen. Por tanto, cuando replica objetos, también replica la lista de control de acceso (ACL) del objeto correspondiente. Si los buckets de origen y destino pertenecen a dos Cuentas de AWS diferentes, puede configurar la reproducción para cambiar el propietario de una réplica a la Cuenta de AWS que posee el bucket de destino.

Puede configurar la reproducción mediante la API de REST, el SDK de AWS, la AWS CLI o la consola de Amazon S3.

**Precio de replicación S3**

Para la replicación S3 (replicación entre regiones y replicación en la misma región), paga los cargos de S3 por almacenamiento en los tipos de almacenamiento S3 de destino seleccionados, los cargos de almacenamiento para la copia principal, las solicitudes PUT de replicación y las tarifas de recuperación de almacenamiento de acceso no frecuente que se apliquen. Para CRR, también paga la transferencia de datos saliente entre regiones desde S3 a cada región de destino. Cuando usa el control de tiempo de replicación de S3, también abona una tarifa por la transferencia de datos de control de tiempo de replicación y los cargos de las métricas de replicación de S3 que se facturen a la misma tasa que las métricas personalizadas de Amazon CloudWatch.

El precio del almacenamiento y las solicitudes PUT de la copia replicada se basa en la región de AWS de destino seleccionada, mientras que los precios de las transferencias de datos entre regiones se basan en la región de AWS de origen.

|  |  |
| --- | --- |
| **SERVICIO** | **COSTO** |
| Transferencia de datos de control de tiempo de replicación S3. | 0,015 USD por GB |

El precio de la transferencia de datos de control de tiempo de replicación de Amazon S3 es el mismo en todas las regiones de AWS. El control de tiempo de reproducción está disponible en todas las regiones comerciales de AWS, excepto las regiones AWS GovCloud (US), la región AWS China (Pekín) y la región AWS China (Ningxia).

**Bloqueo de objetos de S3**

El bloqueo de objetos evita la eliminación de objetos durante un período de retención definido por el cliente, para que pueda imponer políticas de retención como un nivel adicional para la protección de datos o para fines de conformidad normativa. Puede migrar las cargas de trabajo desde sistemas tipo escritura única, lectura múltiple (WORM, write-once-read-many) hacia Amazon S3 y configurar el bloqueo de objetos de S3 al nivel del objeto y del bucket para evitar la eliminación de una versión del objeto con anterioridad a la fecha que figura en "Retain Until" (Retener hasta) o en "Legal Hold" (Retención legal). La protección con bloqueo de objetos de S3 se mantiene independientemente de en qué clase de almacenamiento resida el objeto y durante todas las transiciones de ciclo de vida de S3 entre las clases de almacenamiento.

Se usa en conjunto con el control de versiones de S3, que protege a los objetos de la sobreescritura, y así usted puede garantizar la inmutabilidad de los objetos durante el tiempo durante el cual se encuentre implementada la protección del bloqueo de objetos de S3. Puede aplicar esta protección mediante la asignación de una fecha en "Retain Until" (Retener hasta) o en "Legal Hold" (Retención legal) a un objeto usando AWS SDK, AWS CLI, REST API o la consola de administración de S3. Puede aplicar la configuración de retención dentro de una solicitud PUT o aplicarla en un objeto existente después de su creación. Para rastrear qué objetos tienen este tipo de bloqueo de S3, puede consultar un informe de inventario de S3 que incluye el estado WORM de los objetos.

El bloqueo de objetos de S3 puede configurarse en uno de los dos modos. Cuando se implementa en modo Governance (Control), las cuentas de AWS con permisos de IAM específicos pueden quitar el bloqueo de objetos. Si requiere mayor inmutabilidad para poder cumplir con la normativa, puede usar el modo Compliance (Conformidad). En este modo, ningún usuario puede eliminar la protección, ni siquiera la cuenta raíz.

El bloqueo de objetos de S3 ha sido evaluado según la Regla 17a-4 (f) de la SEC, la Regla 4511 de FINRA y la Regulación 1.31 de la CFTC de Cohasset Associates. Cohasset Associates es una firma de consultoría de gestión especializada en administración de registros y control de la información. Puede descargar una copia del informe de evaluación de Cohasset Associates de la documentación técnica sobre la característica de bloqueo de objetos de S3. Luego, puede entregar el informe de evaluación a su ente regulador cuando le notifique su decisión de usar Amazon S3 para los datos regulados.

Con S3 el bloqueo de objetos, puede almacenar objetos utilizando un modelo de escritura única, lectura múltiple (WORM). El bloqueo de objetos puede ayudar a evitar que los objetos se eliminen o sobrescriban durante un período de tiempo fijo o indefinidamente. Puede utilizar el bloqueo de objetos para ayudar a cumplir con los requisitos reglamentarios que requieren almacenamiento WORM, o simplemente para agregar otra capa de protección contra cambios y eliminación de objetos.



**El bloqueo de objetos proporciona dos formas de administrar la retención de objetos: períodos de retención y retenciones legales.**

* **Período de retención:** especifica un período de tiempo fijo durante el cual un objeto permanece bloqueado. Durante este período, su objeto está protegido por WORM y no se puede sobrescribir ni eliminar.
* **Retención legal:**brinda la misma protección que un período de retención, pero no tiene fecha de vencimiento. En cambio, una retención legal permanece vigente hasta que la elimine explícitamente. Las retenciones legales son independientes de los períodos de retención.

Una versión de objeto puede tener un período de retención y una retención legal, uno, pero no el otro, o ninguno.

El bloqueo de objetos solo funciona en depósitos con versiones, y los períodos de retención y las retenciones legales se aplican a las versiones de objetos individuales. Cuando bloquea una versión de objeto, Amazon S3 almacena la información de bloqueo en los metadatos para esa versión de objeto. La colocación de un período de retención o retención legal sobre un objeto protege solo la versión especificada en la solicitud. No impide que se creen nuevas versiones del objeto.

Si coloca un objeto en un depósito que tiene el mismo nombre de clave que un objeto protegido existente, Amazon S3 crea una nueva versión de ese objeto, lo almacena en el depósito según lo solicitado e informa que la solicitud se completó correctamente. La versión protegida existente del objeto permanece bloqueada según su configuración de retención.

**Configurar el bloqueo de objetos de S3 mediante la consola**

Para utilizar el bloqueo de objetos de S3, siga estos pasos básicos:

1. Cree un nuevo depósito con el bloqueo de objetos habilitado.
2. (Opcional) Configure un período de retención predeterminado para los objetos colocados en el depósito.
3. Coloque los objetos que desea bloquear en el cubo.
4. Aplique un período de retención, una retención legal o ambos a los objetos que desea proteger.

Antes de bloquear cualquier objeto, debe habilitar un depósito para usar el bloqueo de objetos de S3. Habilitas el bloqueo de objetos cuando creas un depósito. Después de habilitar el bloqueo de objetos en un depósito, puede bloquear los objetos en ese depósito. Cuando crea un depósito con el bloqueo de objetos habilitado, no puede inhabilitar el bloqueo de objetos ni suspender el control de versiones para ese depósito.

**Para habilitar la retención legal de bloqueo de objetos**

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el Cubos lista, seleccione el nombre del cubo que desea.
3. En la lista Objetos, elija el nombre del objeto para el que desea habilitar o deshabilitar la retención legal.
4. Se abre la vista general del objeto, que muestra las propiedades de su objeto.
5. En Retención legal de bloqueo de objeto, elija Editar.
6. En Retención legal, elija Activar o Desactivar.
7. Elija Guardar cambios.

**Para editar la configuración de retención de Object Lock**

1. En la lista Objetos, elija el nombre del objeto para el que desea editar la configuración de retención de Bloqueo de objetos.
2. Se abre la vista general del objeto, que muestra las propiedades de su objeto.
3. En Retención de bloqueo de objetos, elija Editar.
4. En Retención, elija Activar o Desactivar.
5. En el modo de retención, elija el modo de gobierno o el modo de cumplimiento.
6. En el cuadro Retener hasta la fecha, ingrese la fecha en la que el objeto ya no está protegido por el modo de retención elegido.
7. Elija Guardar cambios.

**Precio de Bloqueo de Objetos S3**

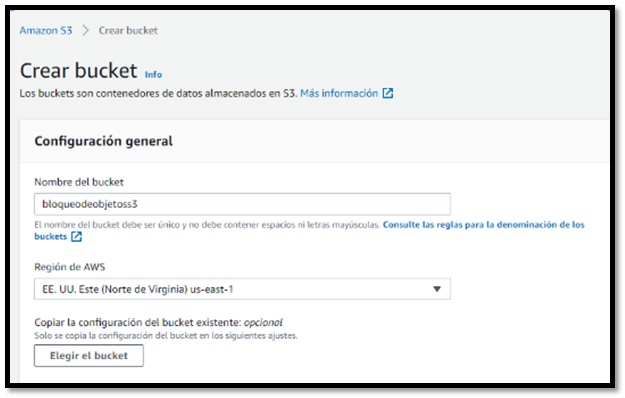
Amazon S3 Glacier y S3 Glacier Deep Archive son clases de almacenamiento seguro, duradero y de muy bajo costo en la nube de Amazon S3 para archivar datos y hacer copias de seguridad a largo plazo. Están diseñadas para brindar una durabilidad del 99,999999999 % y ofrecen capacidades de conformidad y seguridad integrales que pueden ayudar a cumplir los requisitos normativos más estrictos. Los clientes pueden almacenar datos por tan solo 1 USD por terabyte al mes, lo que representa un ahorro significativo en comparación con las soluciones locales. Amazon S3 Glacier proporciona tres opciones de acceso a los archivos, que van desde unos pocos minutos a varias horas, y S3 Glacier Deep Archive ofrece dos opciones de acceso, que van desde 12 a 48 horas, lo que las convierte en opciones adecuadas para diversas necesidades de recuperación a la vez que mantienen los costos bajos.

|  |  |
| --- | --- |
| Estándar - Acceso poco frecuente de S3\*: para almacenar datos de larga vida, pero con poco acceso que requieren de acceso de milisegundos |  |
| Todo el almacenamiento/mes | 0,0125 USD por GB |
| S3 Única zona - Acceso poco frecuente\*: para almacenar datos recreables con poco acceso que requieren de acceso de milisegundos |  |
| Todo el almacenamiento/mes | 0,01 USD por GB |
| S3 Glacier\*\*: para almacenar copias de seguridad y archivos a largo plazo con opción de recuperación de 1 minuto a 12 horas |  |
| Todo el almacenamiento/mes | 0,004 USD por GB |
| S3 Glacier Deep Archive\*\*: para almacenar archivos de datos a largo plazo a los que se accede una o dos veces al año y que se pueden recuperar dentro de un plazo de 12 horas |  |
| Todo el almacenamiento/mes | 0,00099 USD por GB |

**Implementación**

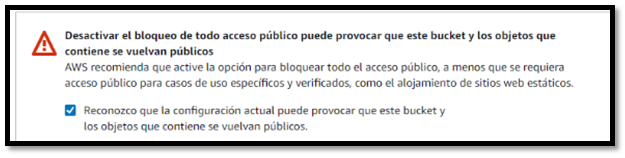
**Paso 1: Crear contenedor**

* Colocar un nombre y seleccionar la región: el nombre del bucket debe ser único y no debe contener espacios ni letras mayúsculas.

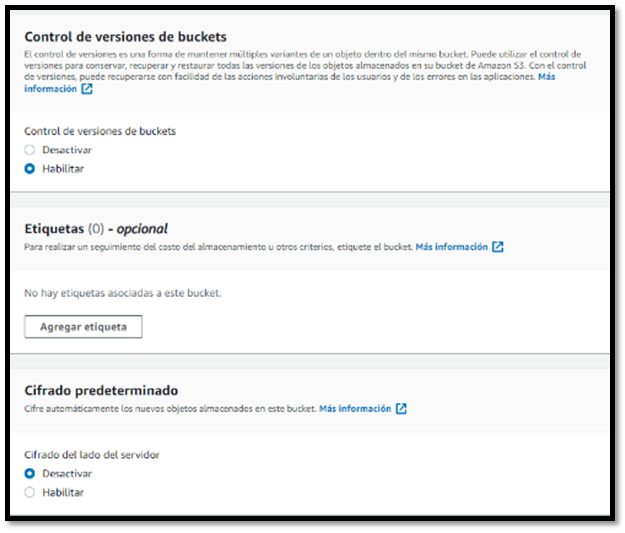


**Paso 2: Configuración de bloqueo de acceso público para este bucket**

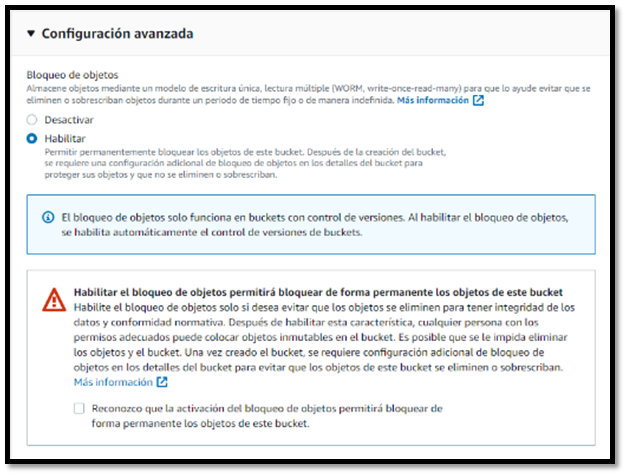
* Desmarcar la opción Bloquear todo el acceso público y marcar la casilla de la parte inferior.

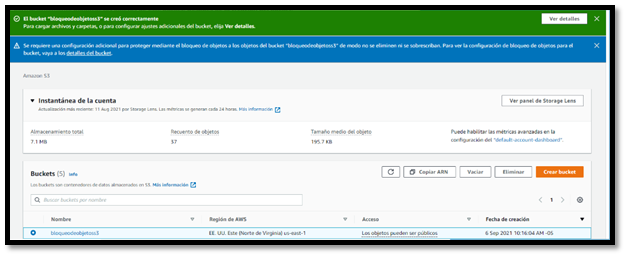
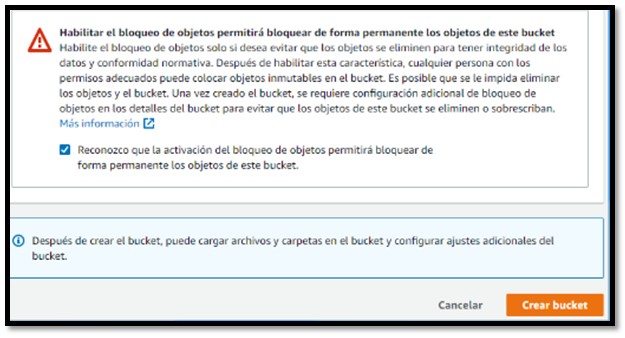


**Paso 3: Habilitar el control de versiones**

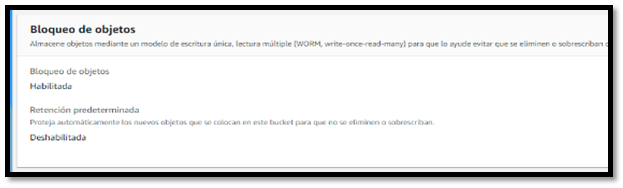


**Paso 4: Desplegar la opción de configuración avanzada, Habilitar la opción de bloqueo de Objetos y marcar la casilla en la parte inferior.**

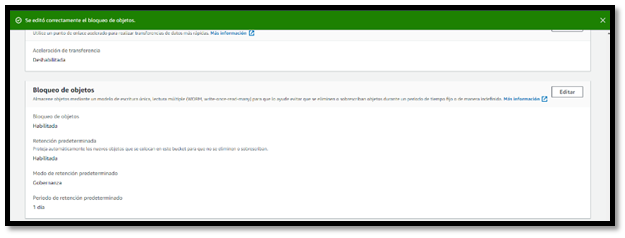
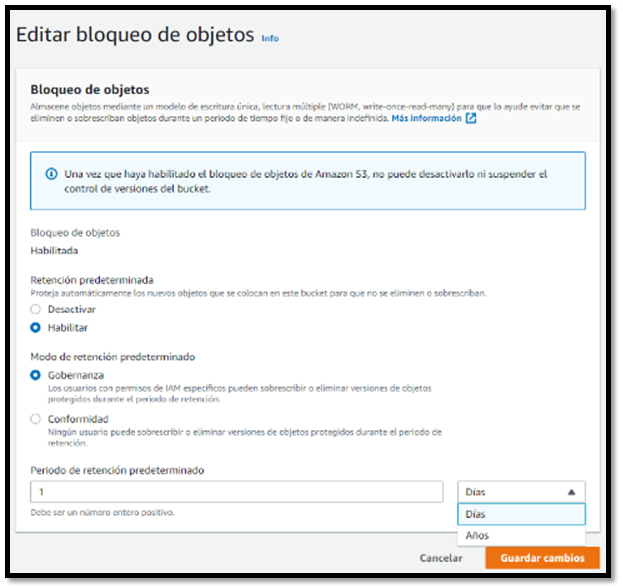




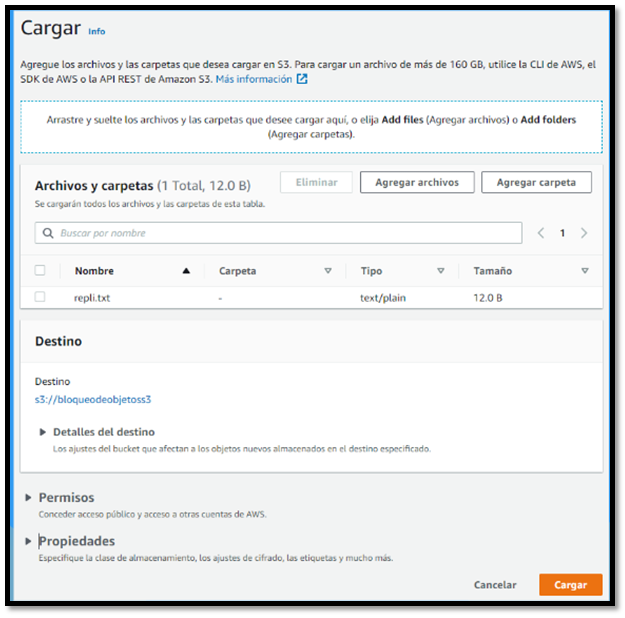
**Paso 5: Seleccionamos el objeto, propiedades, bloqueo de objetos y abrimos la opción de editar.**

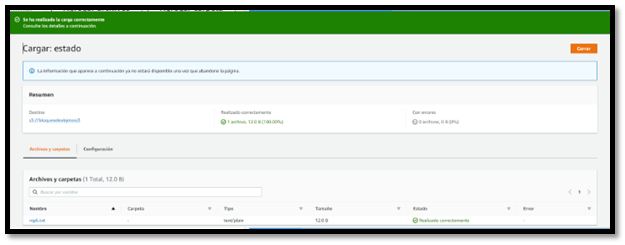


**Paso 6: Habilitar la retención predeterminada**

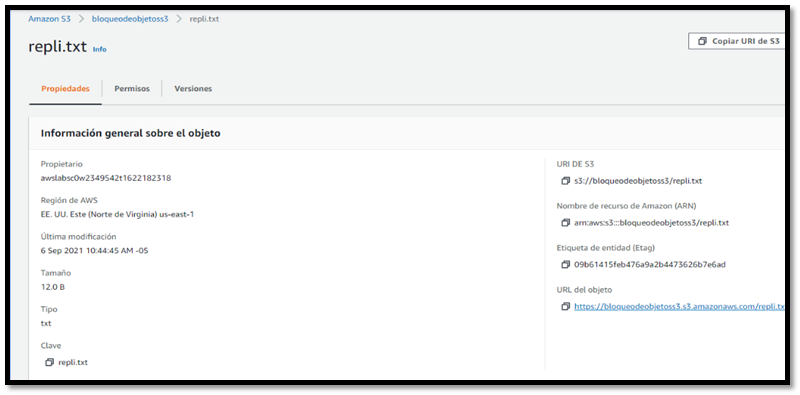


**Paso 7: Subir objetos**

* Seleccionamos la opción agregar archivos



* Realización del bloqueo de objetos





**Conclusión:** El bloqueo de objetos nos ayuda para evitar la eliminación de objetos durante un período de retención definido por el cliente, para que pueda imponer políticas de retención como un nivel adicional para la protección de datos o para fines de conformidad normativa.