# Ejemplo 3 - Habilitar Macie

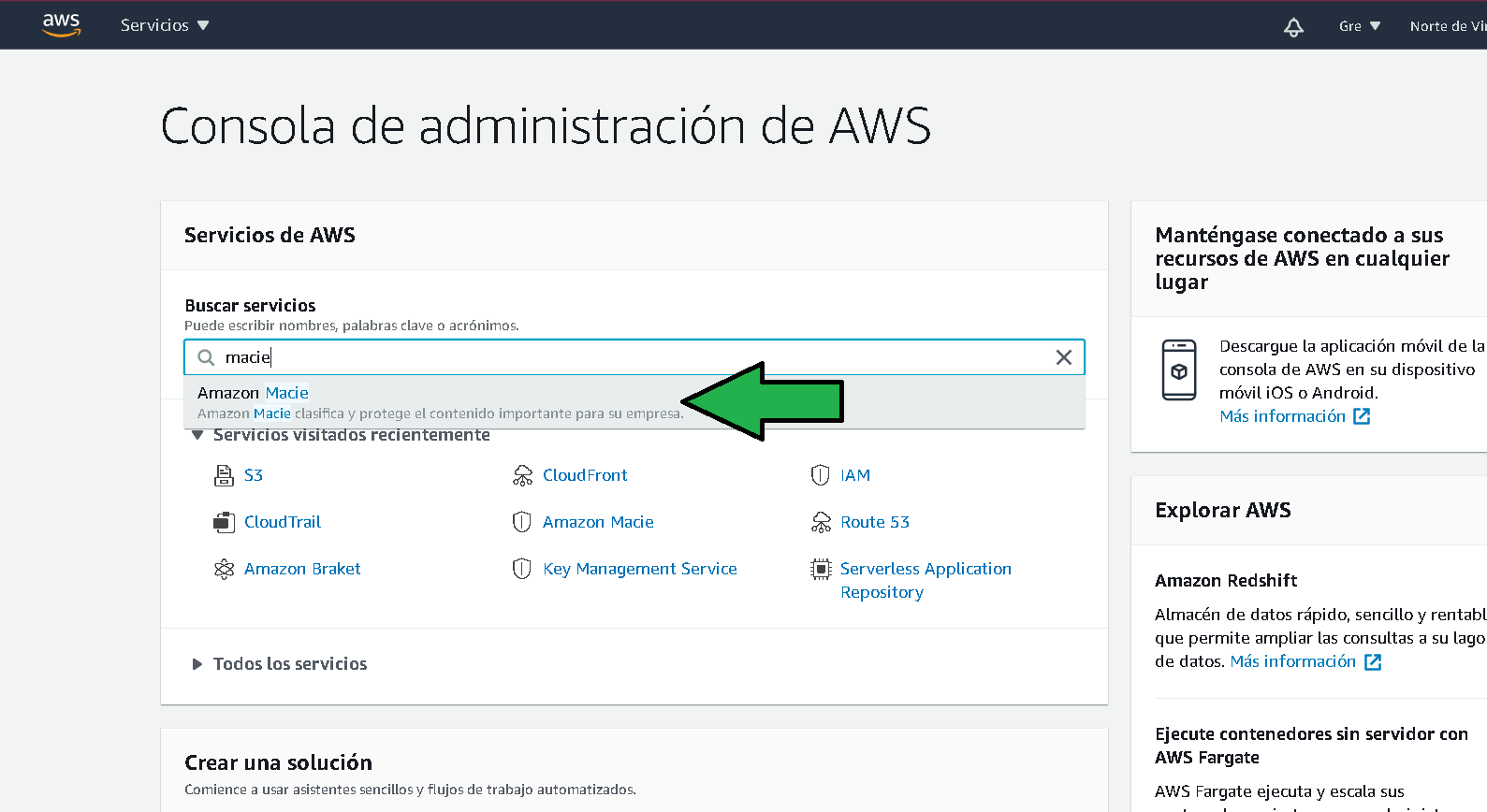
# 1. Objetivo 🎯

* En un bucket S3 buscar información sensible.

# 2. Requisitos 📌

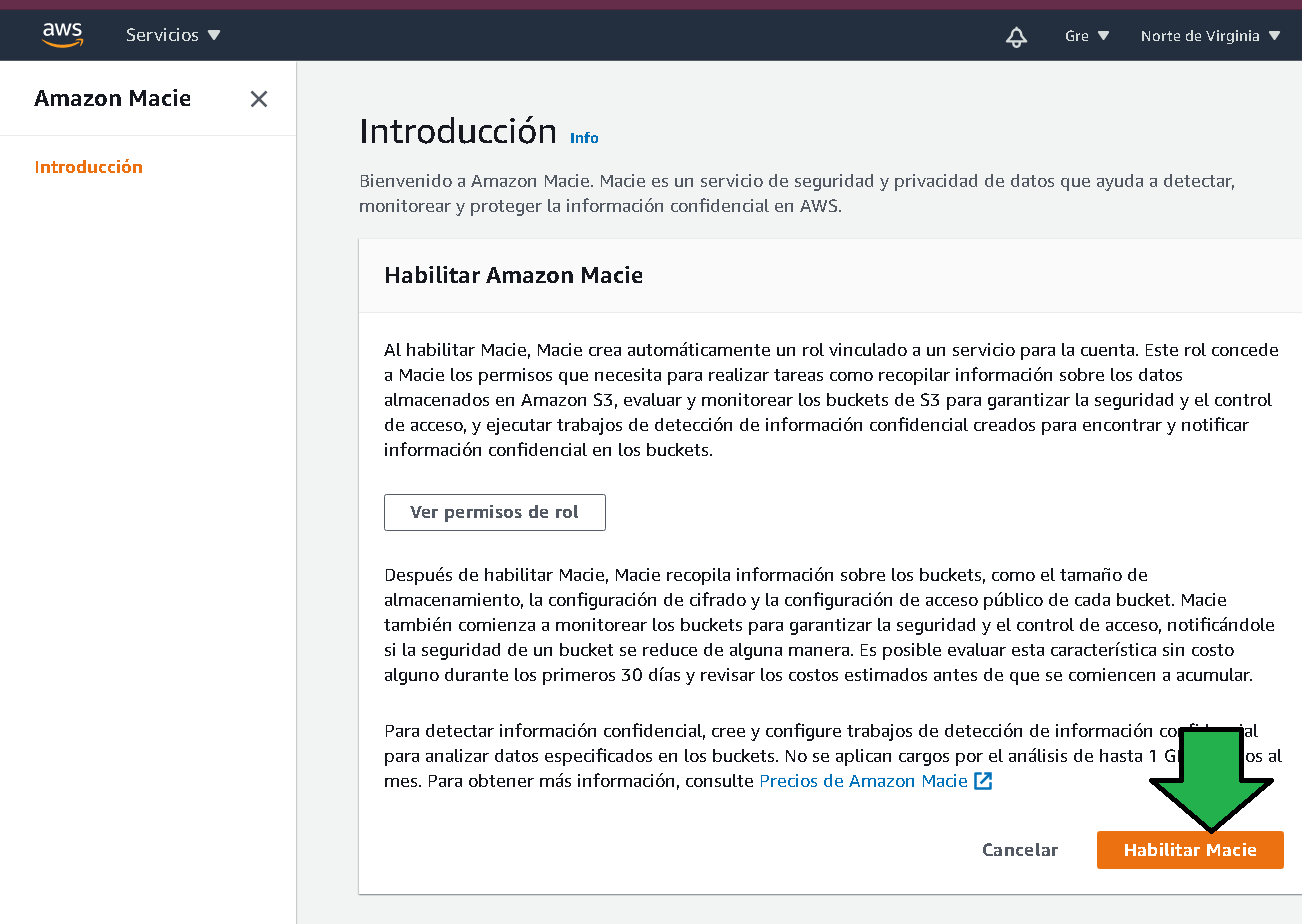
* AWS CLI instalado y configurado.
* Un bucket S3 con algunos archivos que simularán ser archivos con información sensible.

# 3. Desarrollo 📑

1. Ingresar a la consola de AWS buscando el servicio Amazon Macie. 
2. Habilitar Macie, al habilitarlo se genera un rol con la política necesaria para que el servicio acceda al servicio S3.

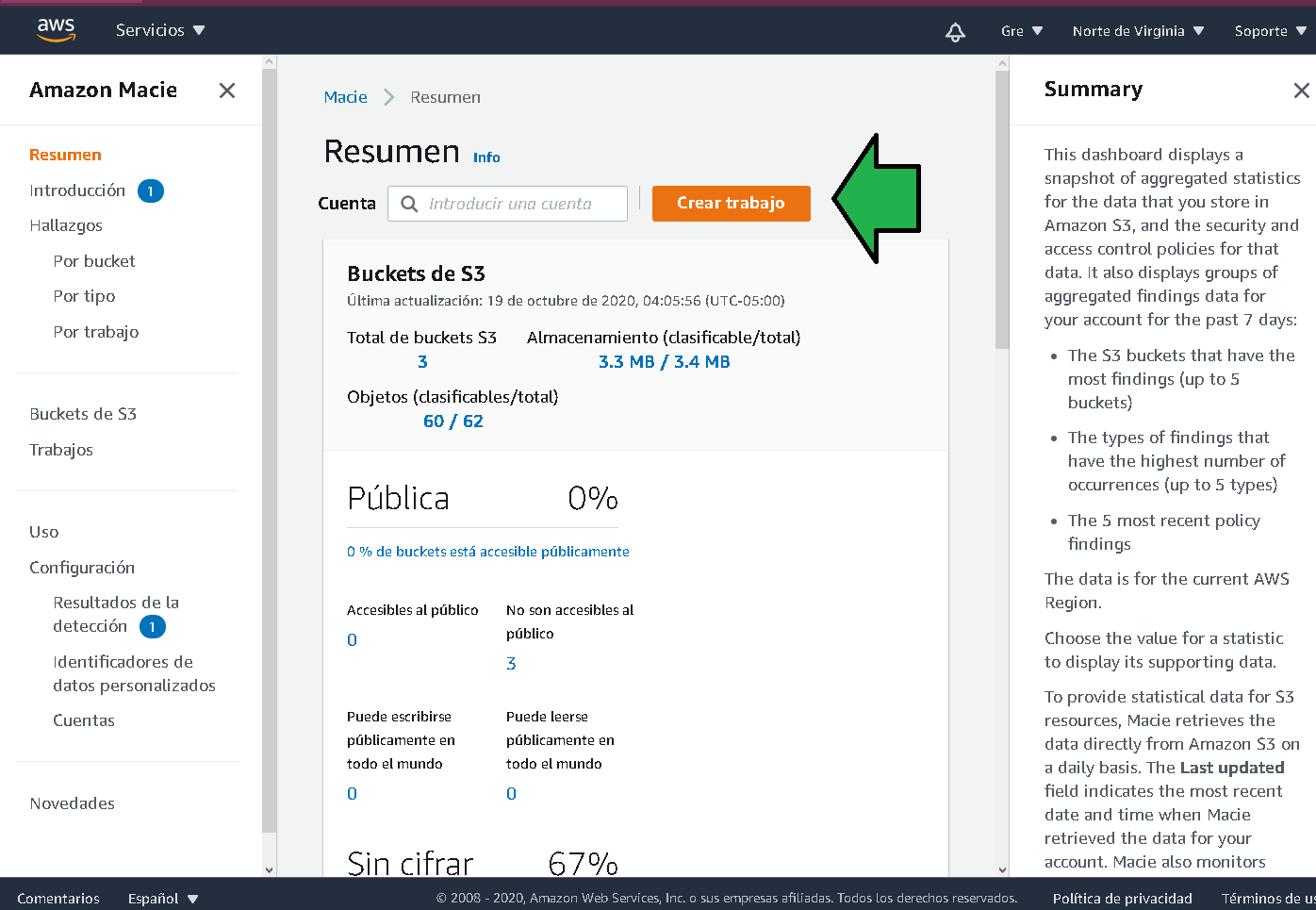


ej3-habilitar-macie.png



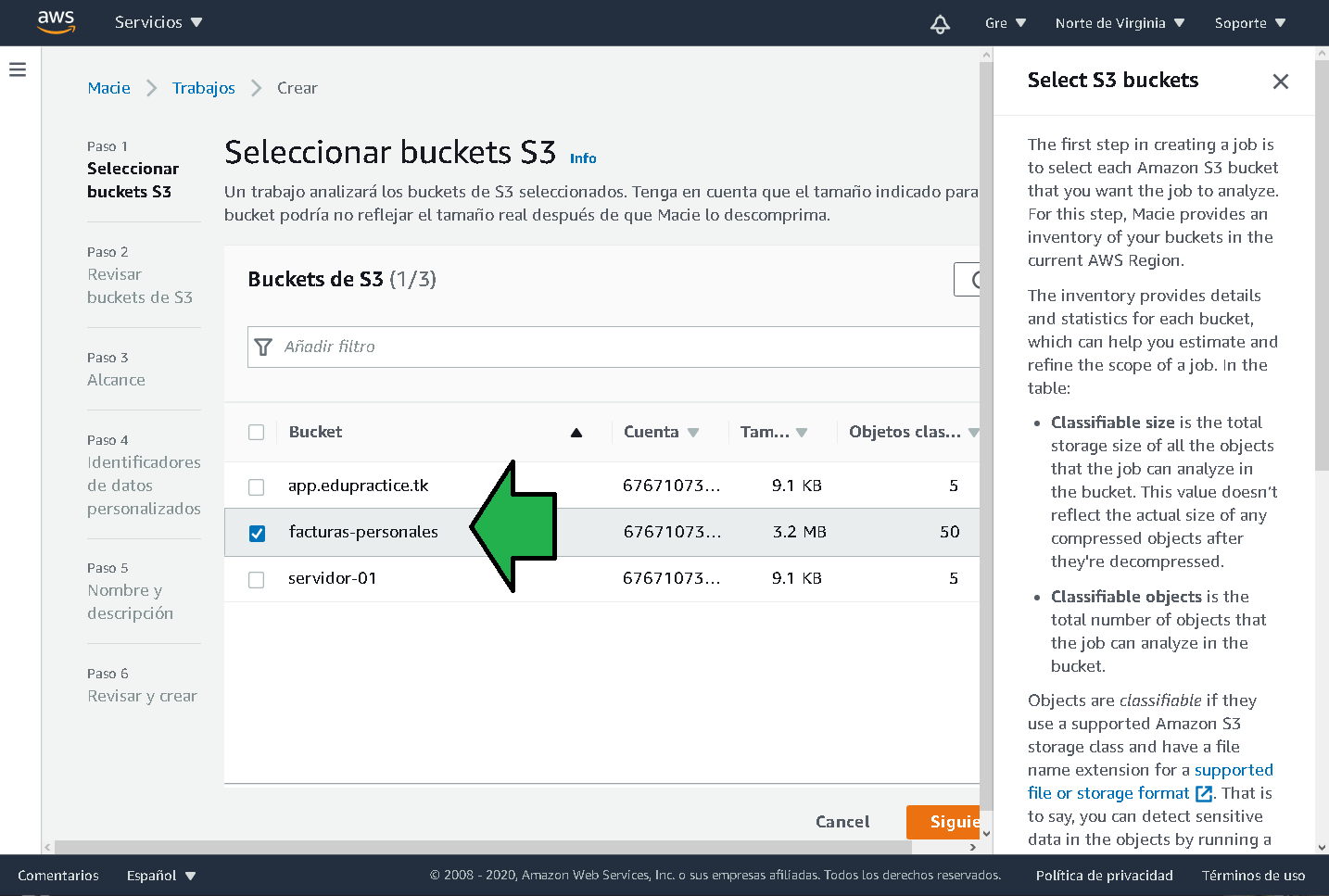
ej3-habilitar-macie-02.png

1. Al habilitar el servicio, Macie da un reporte de los buckets a los que tiene acceso. Habrá que ejecutar un trabajo de escaneo

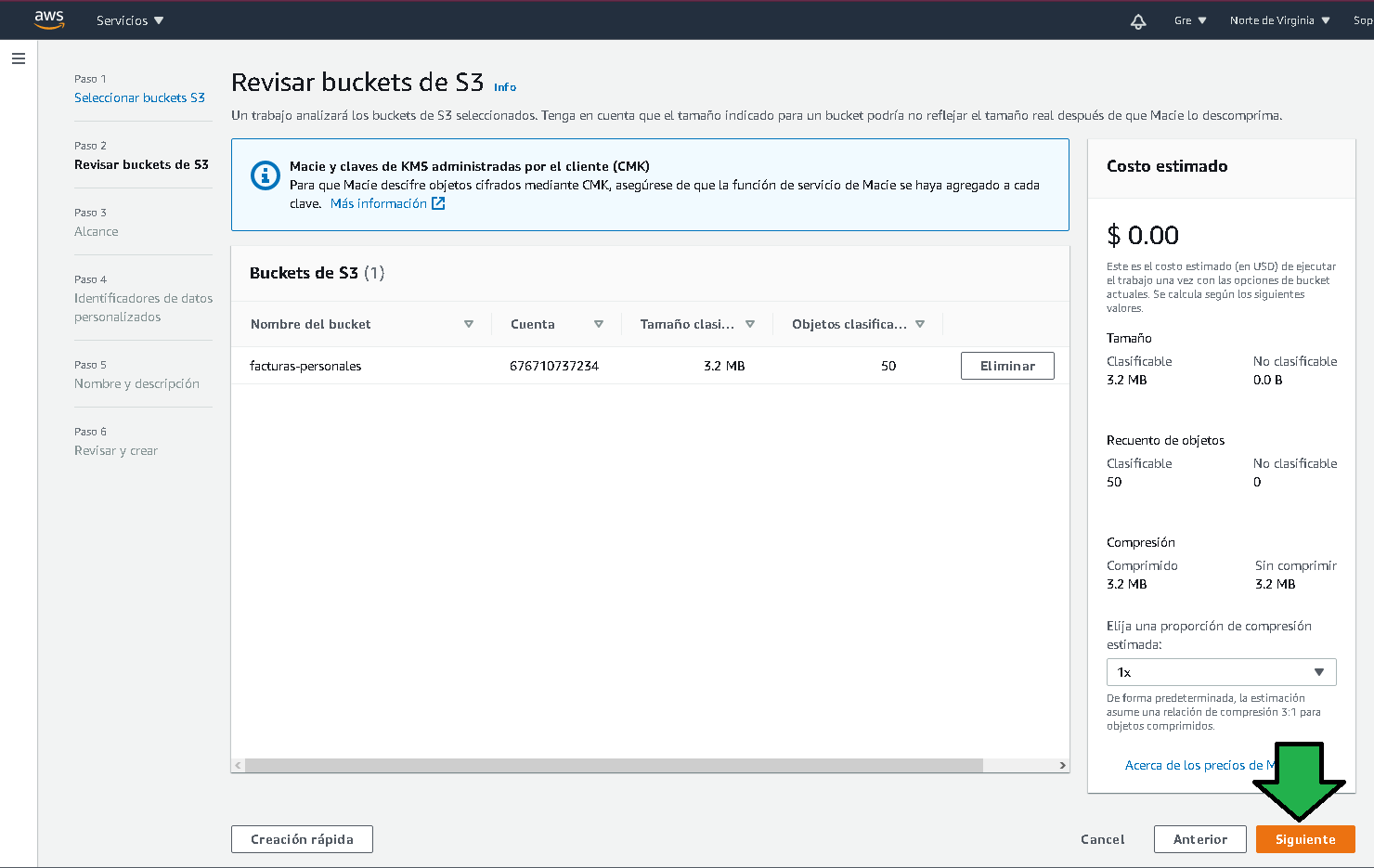
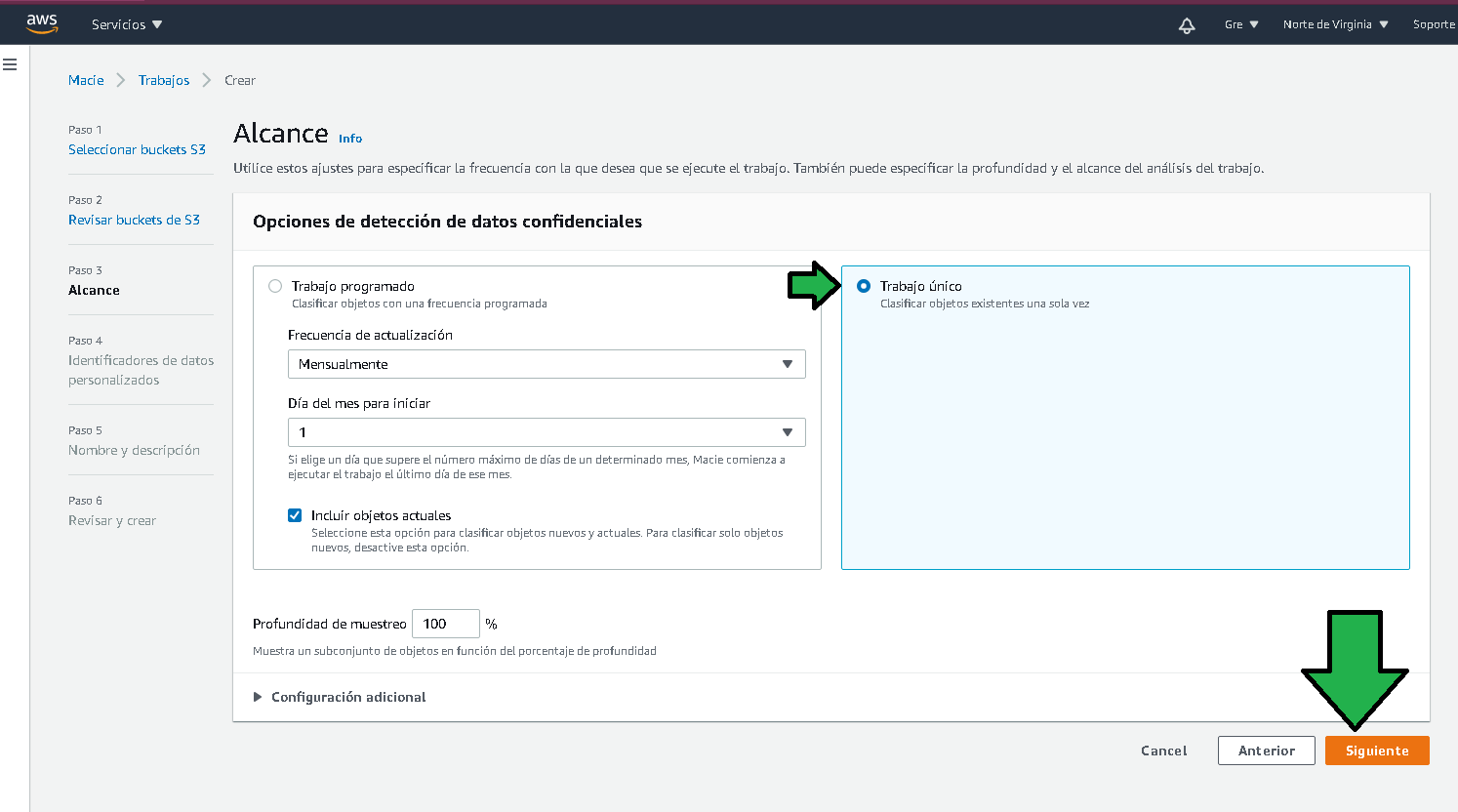
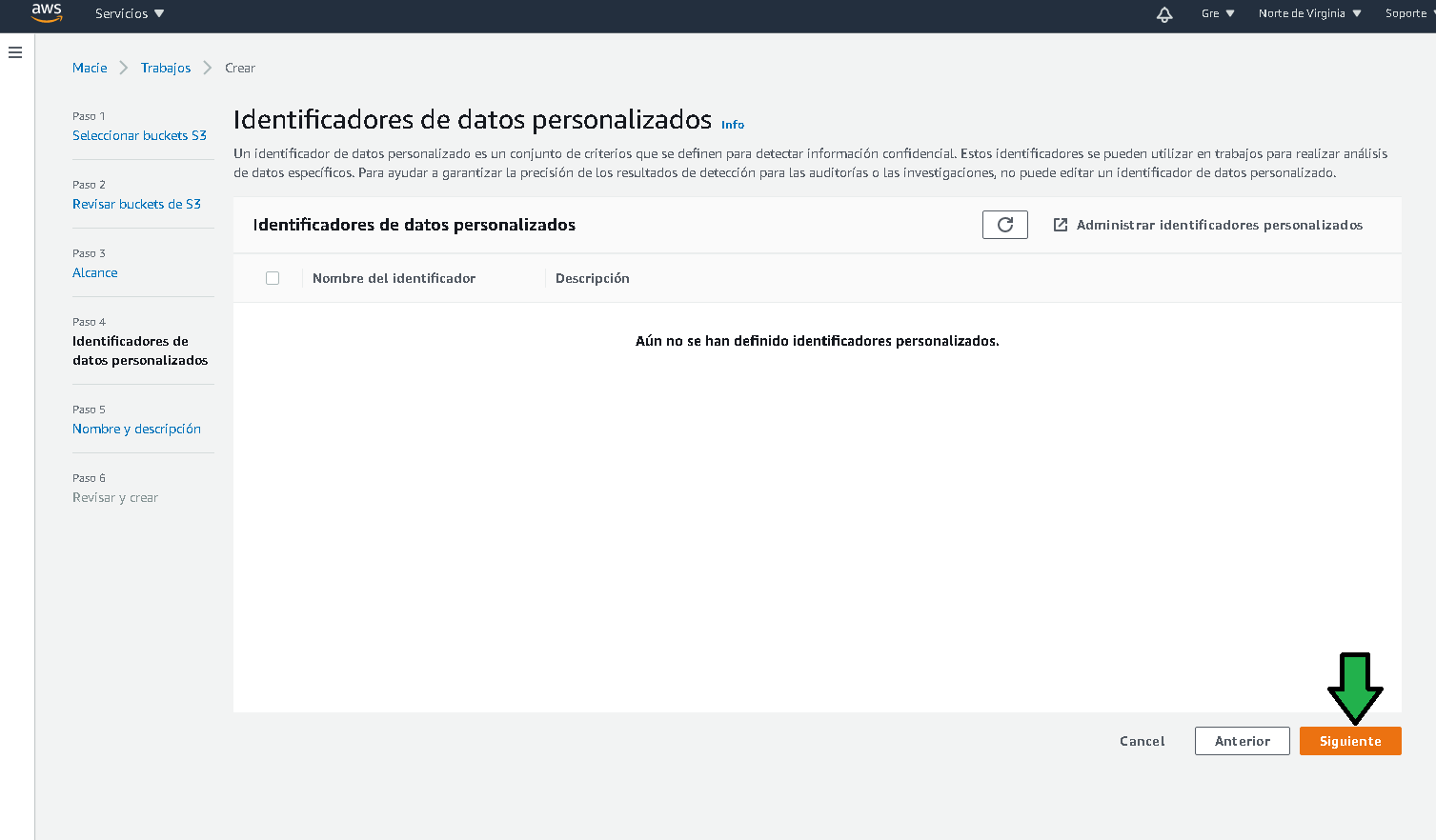
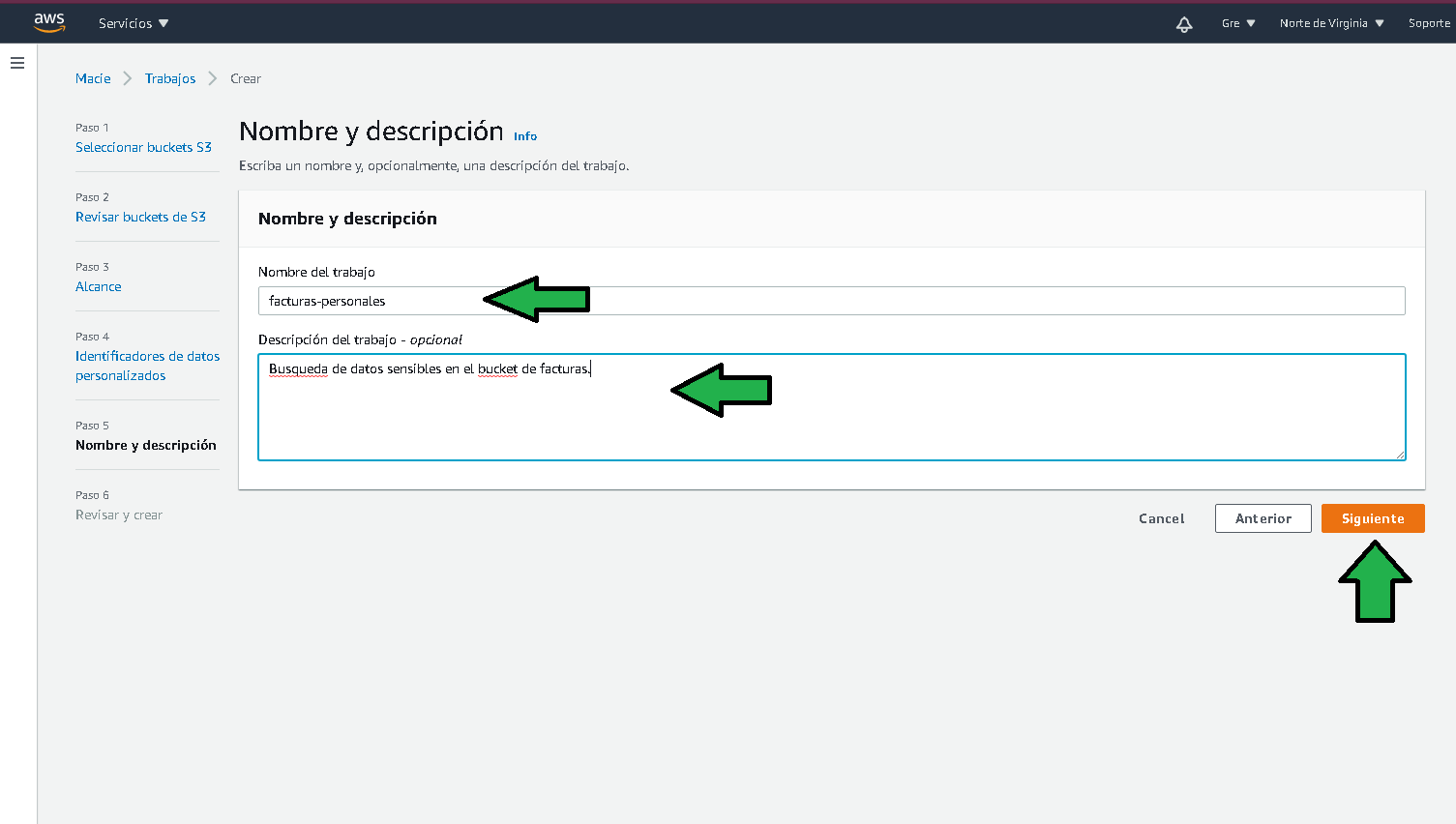
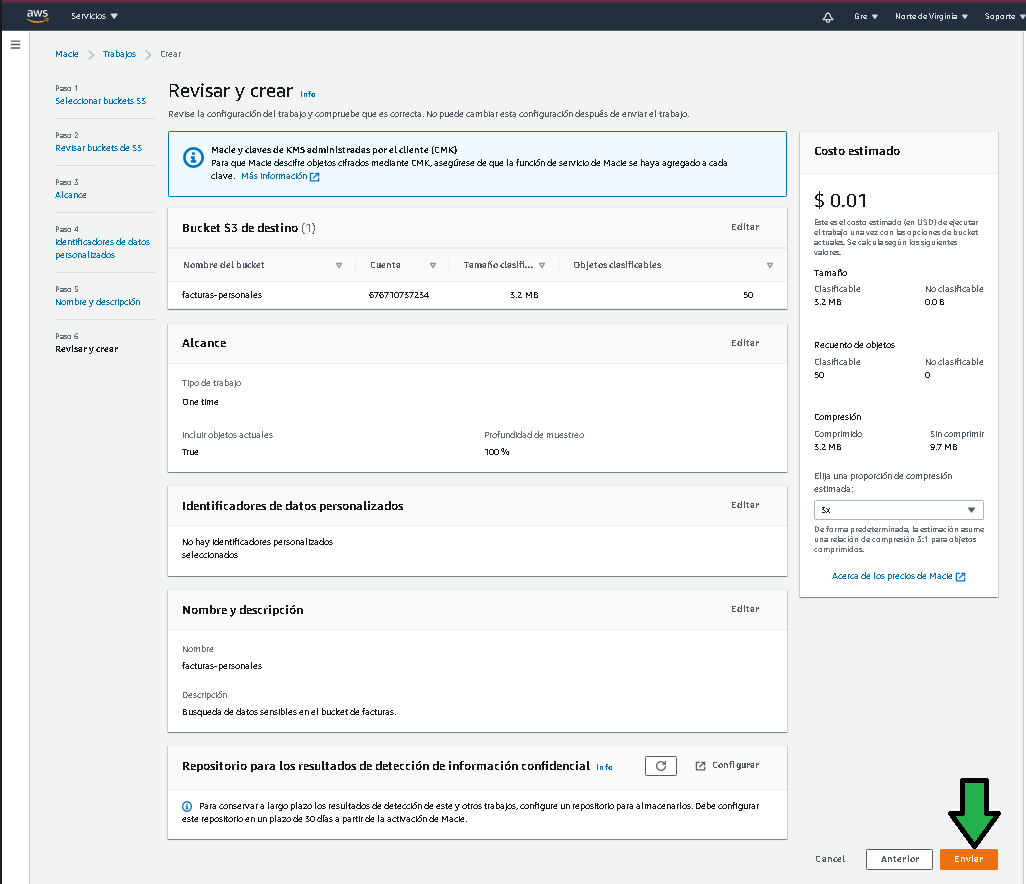
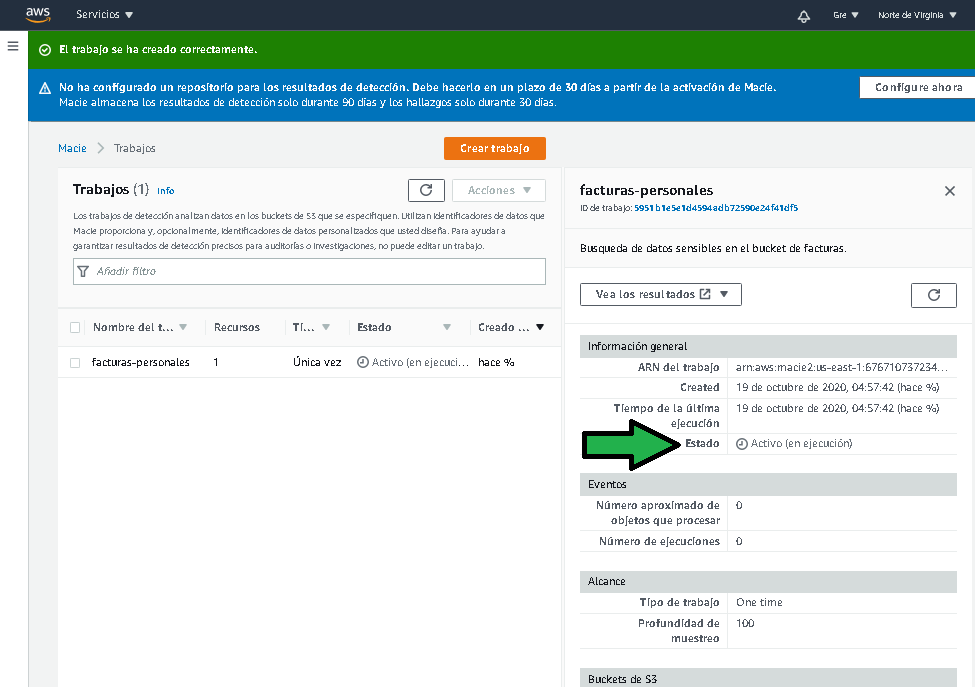


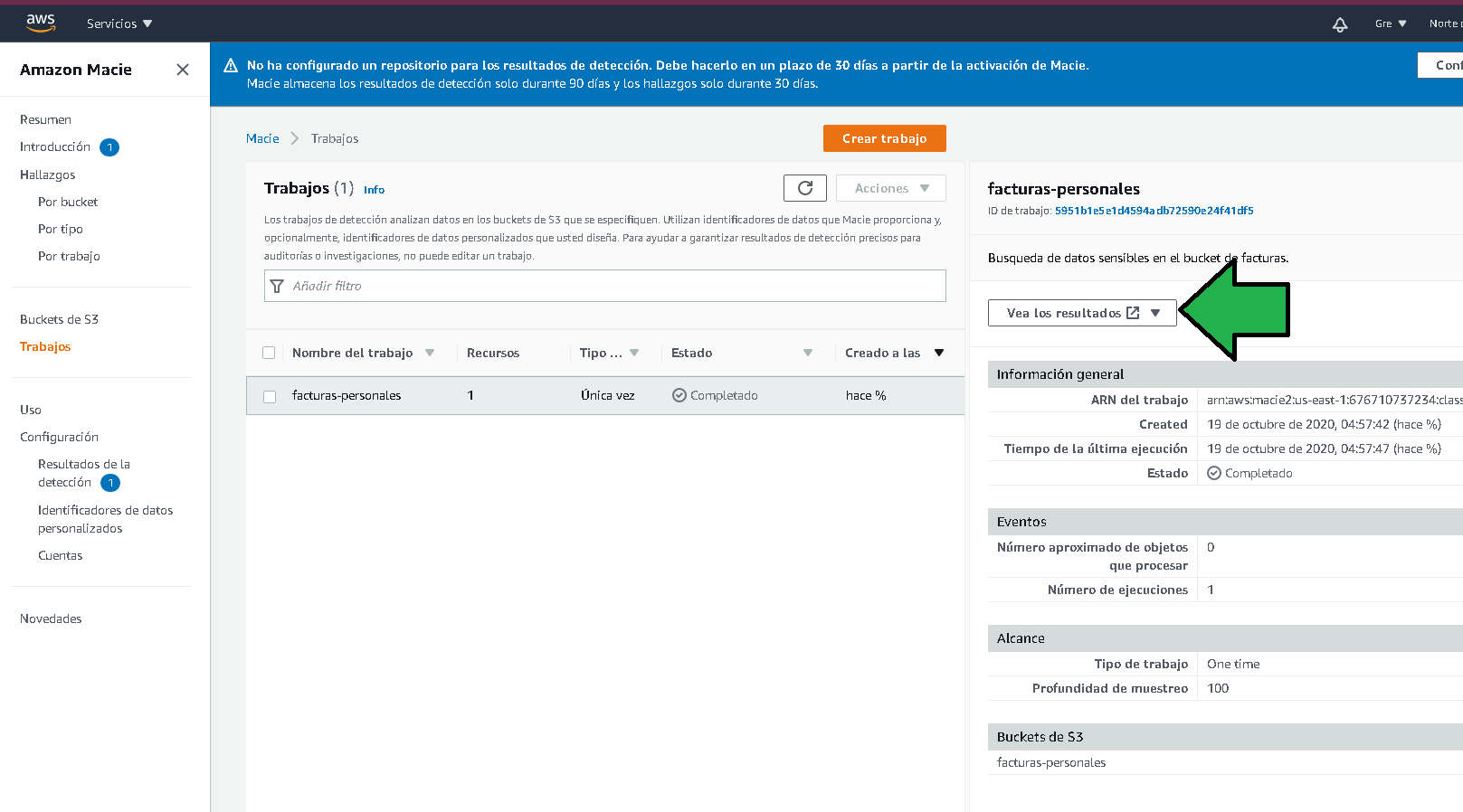
ej3-macie-dashboard-01.png

1. Se debe seleccionar el o los buckets para ser analizados.



ej3-buckets-selected.png

1. Confirmar el bucket y el costo estimado. 
2. Para no incurrir en costos periódicos se deberá seleccionar como trabajo único. 
3. En la siguiente pantalla se pueden escoger identificadores personales, son patrones basados en regex o palabras clave que deben ser identificados como información sensible, por defecto Macie ya detecta nombres,direcciones y números de tarjetas de crédito. 
4. Se asigna un nombre y descripción para el trabajo. 
5. Se revisan los datos configurados, de ser correctos se finaliza la configuración. 
6. El trabajo comienza a ejecutarse. 
7. Completado el trabajo se tendrá acceso a un reporte de hallazgos.



ej3-macie-job-done.png

1. Verificando el contenido del archivo se puede ver que son 4 nombres encontrados y reportados. 