# Reto 1

# 1. Objetivo 🎯

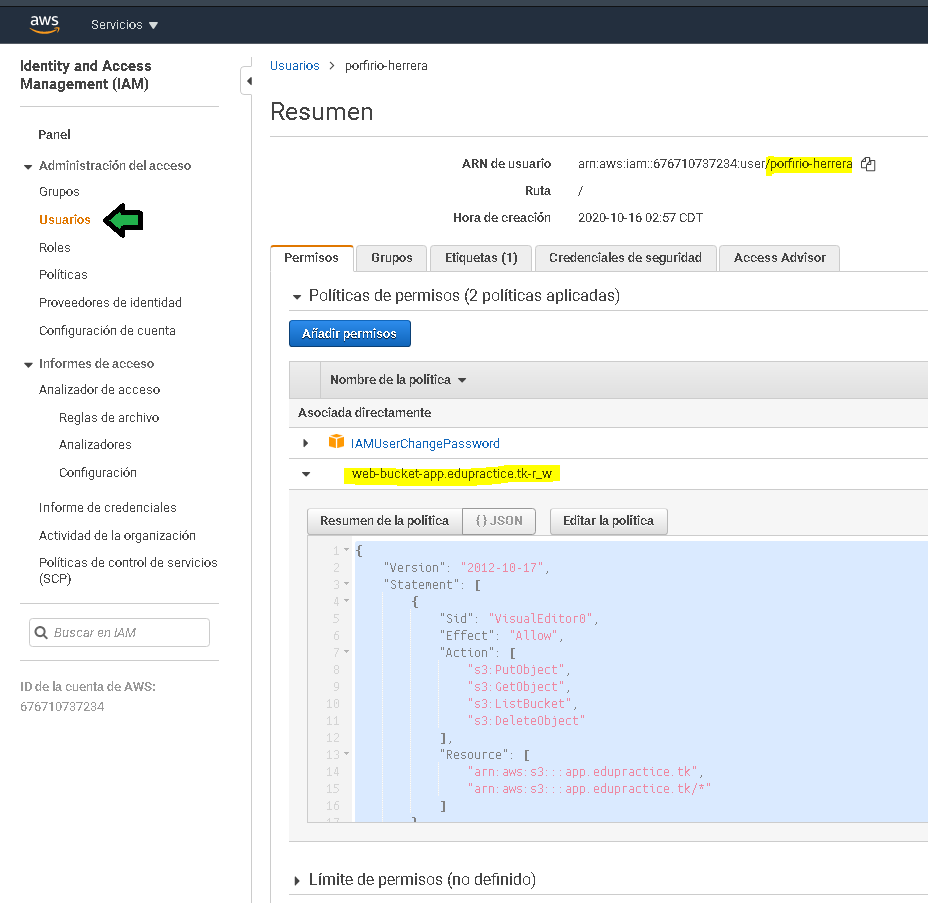
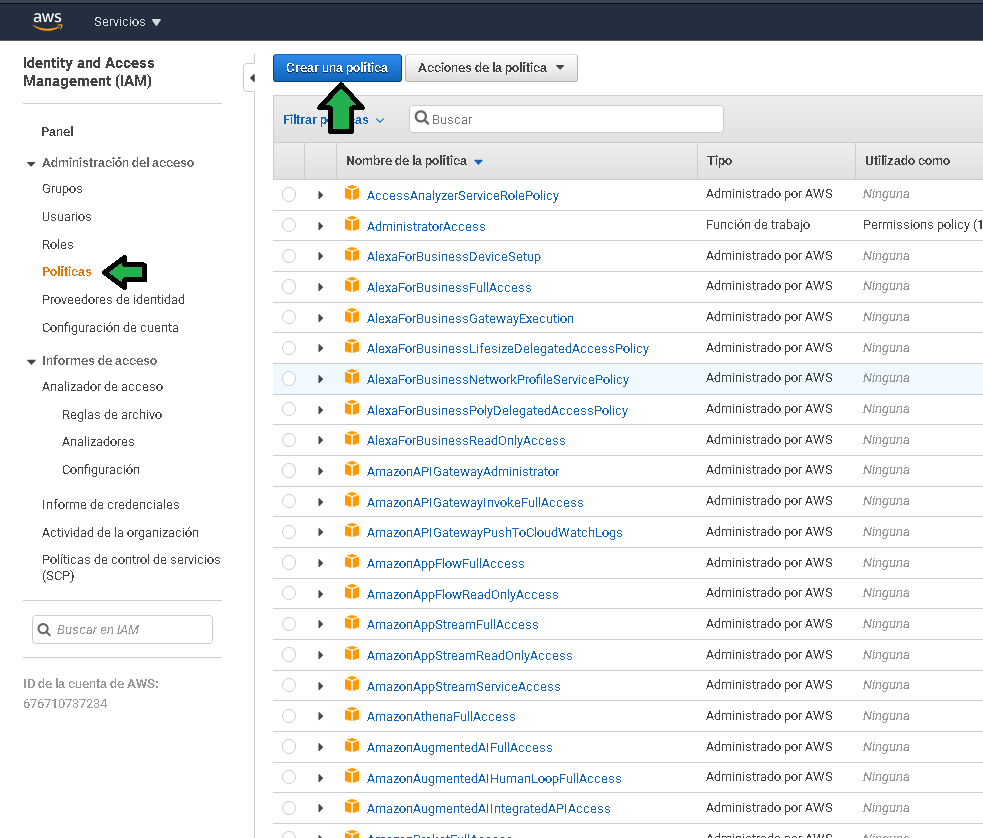
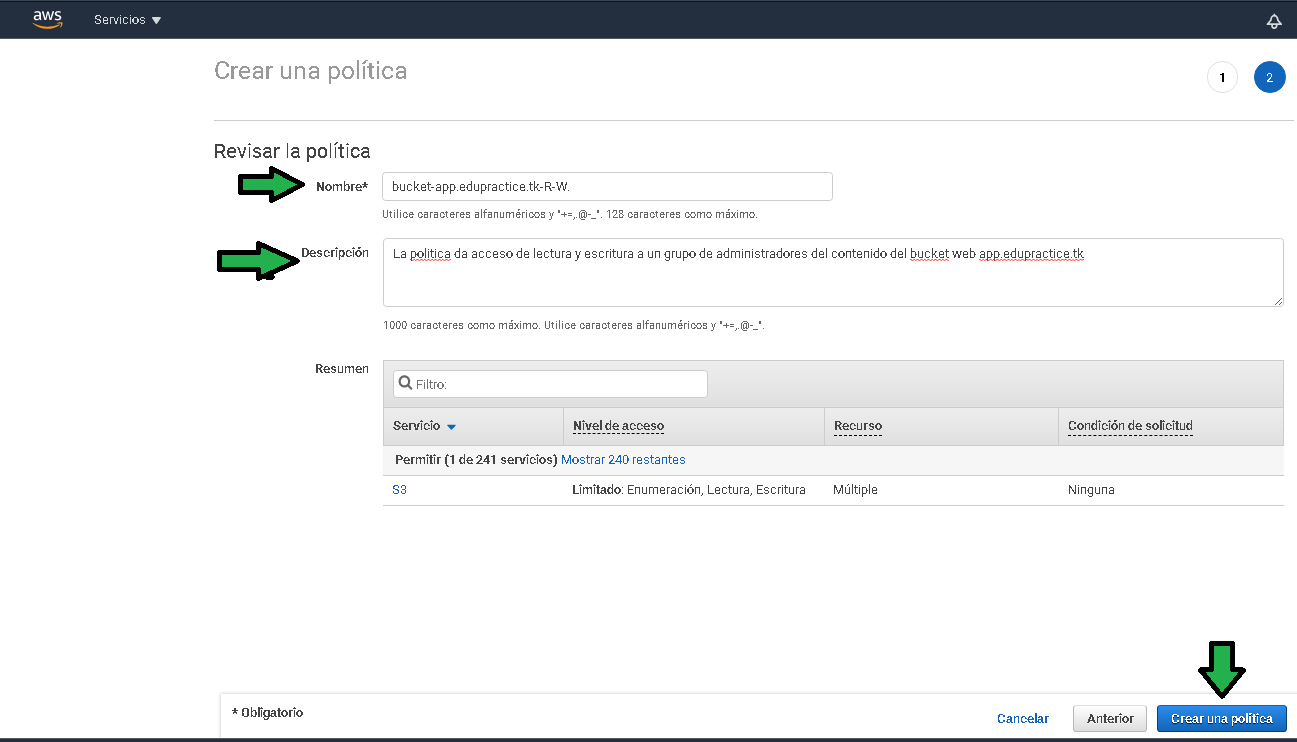
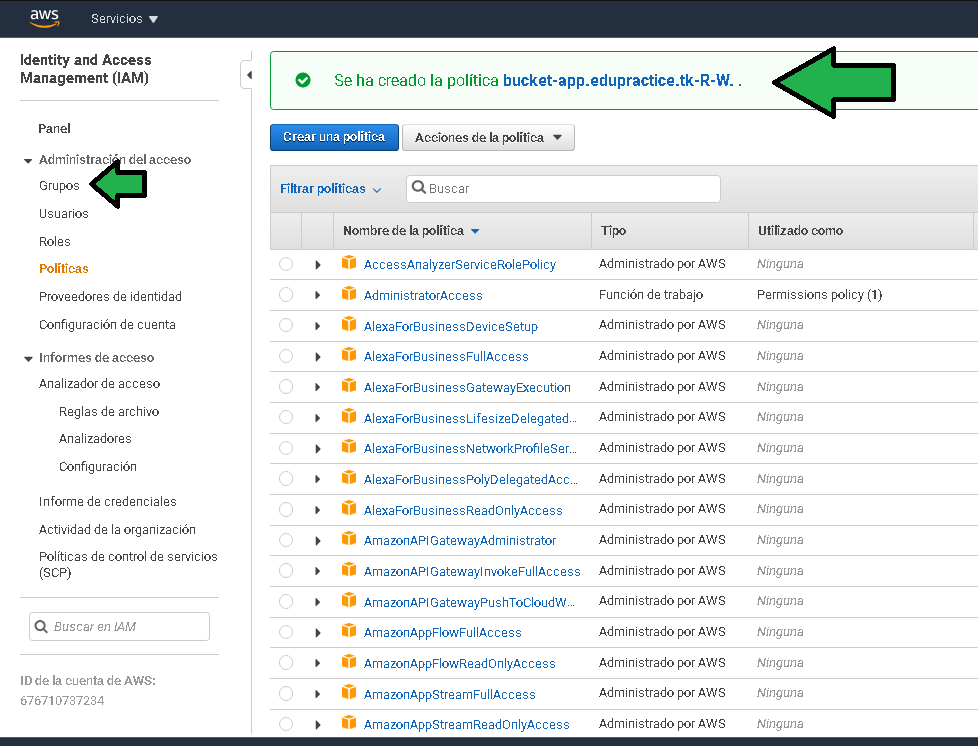
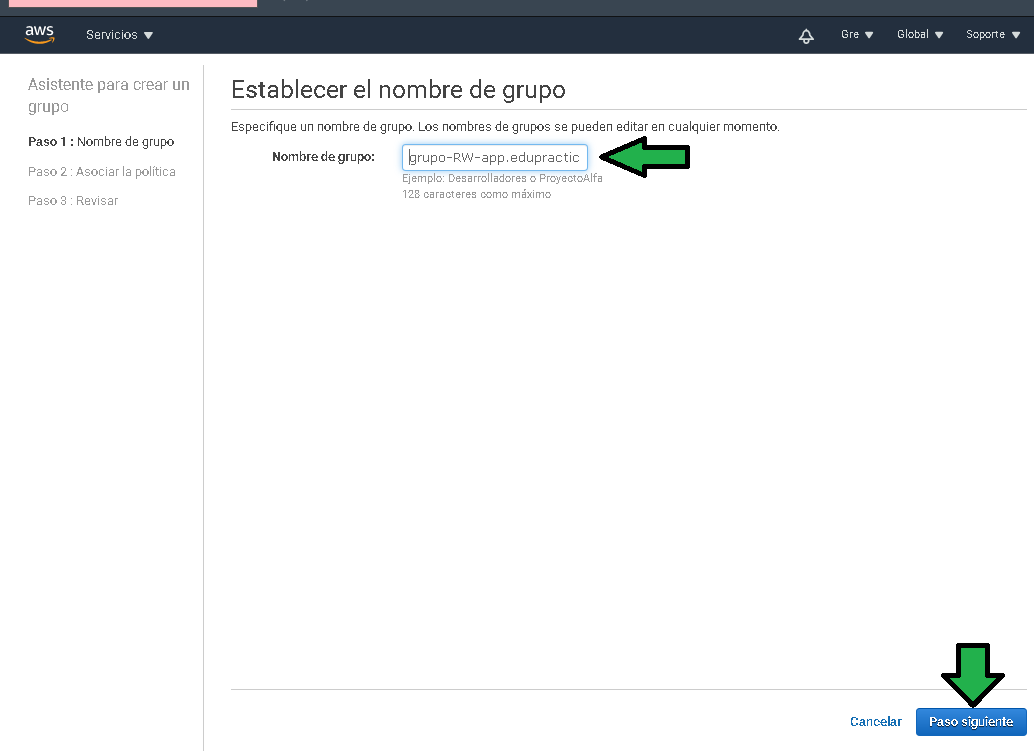
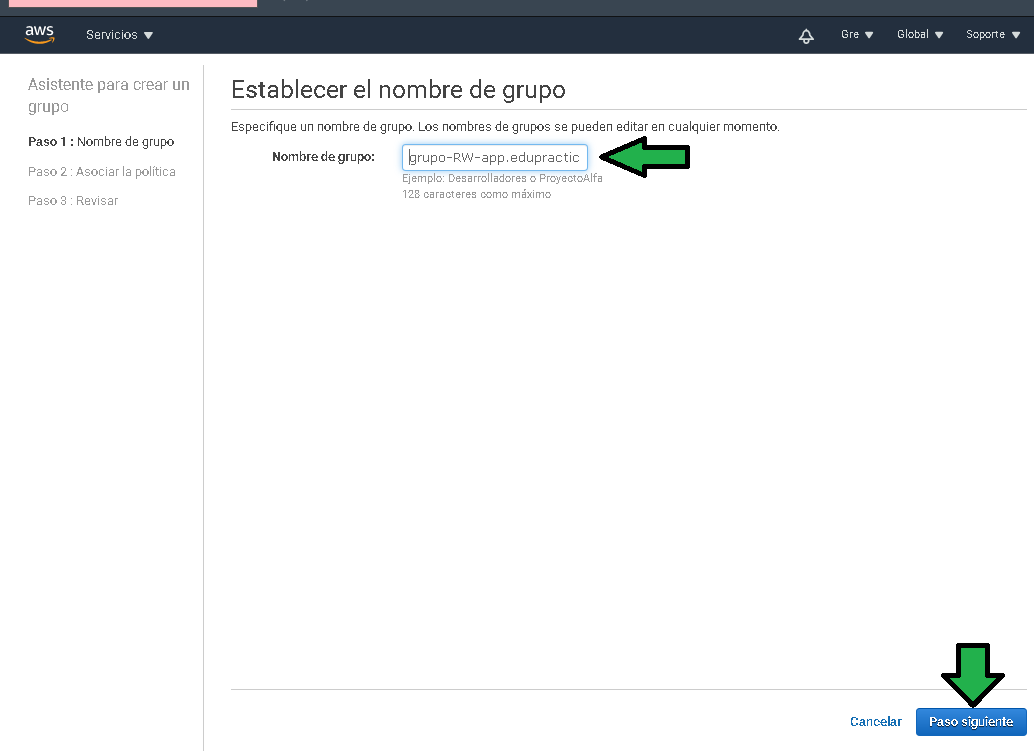
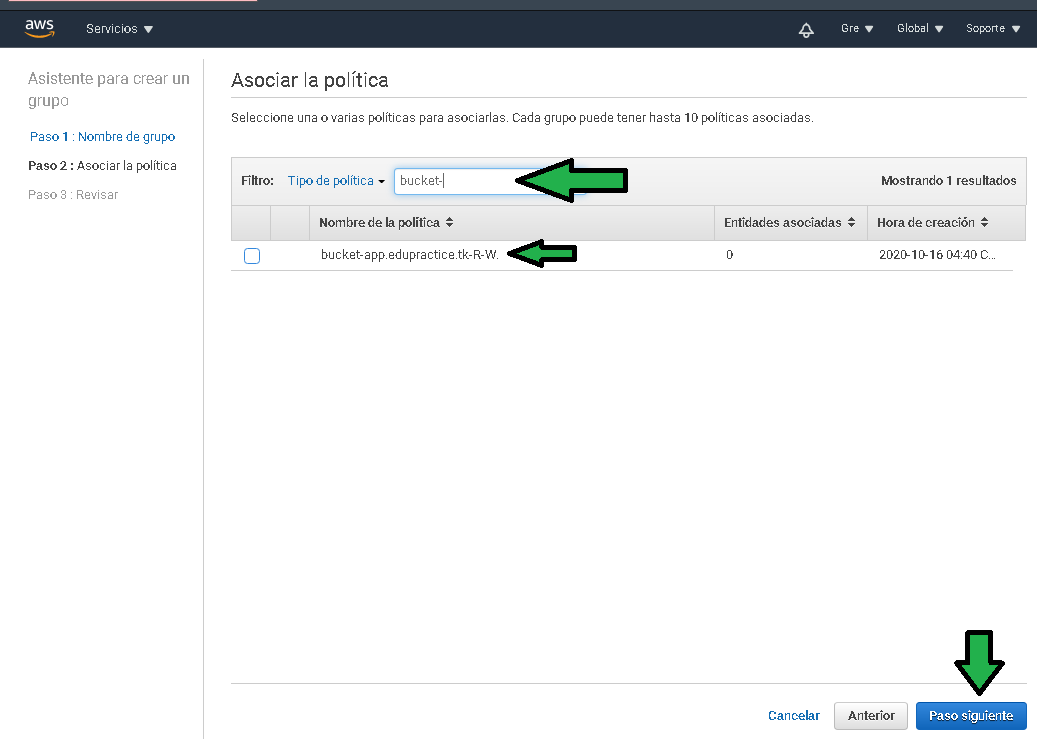
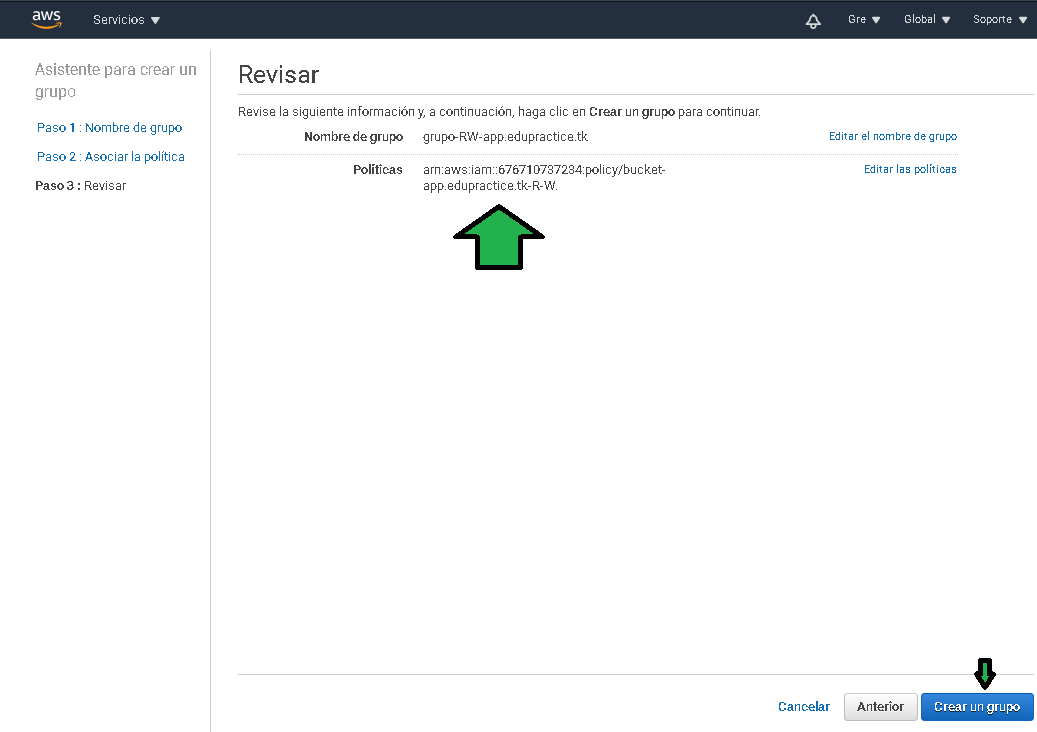
* Establecer una administración mantenible de políticas y usuarios.

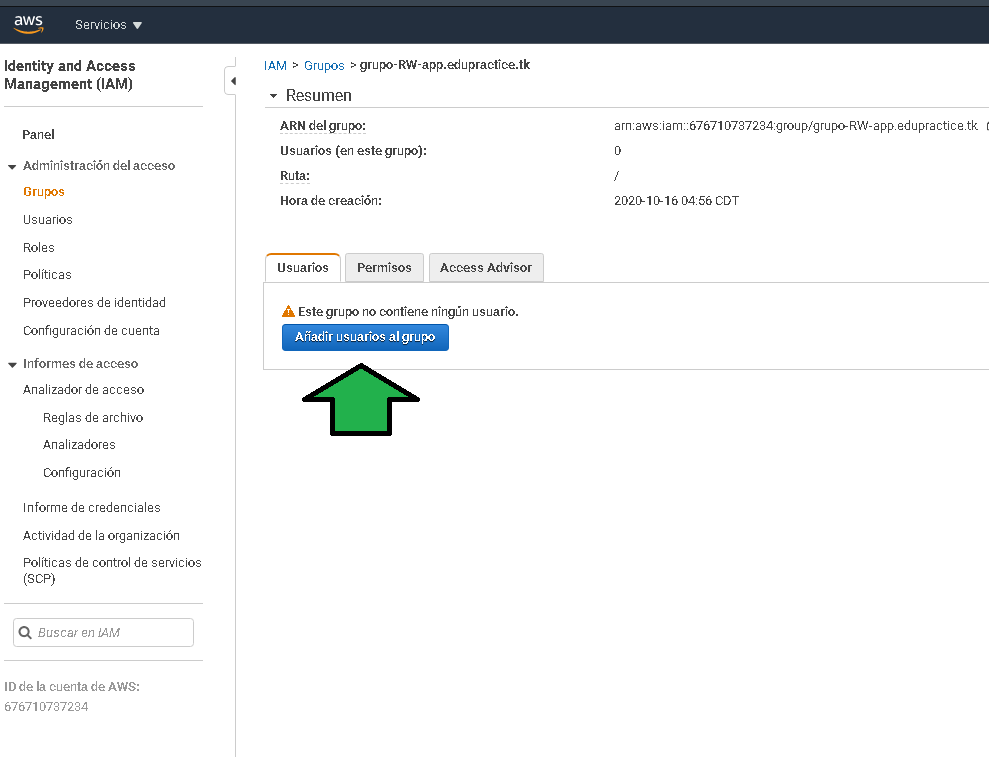
# 2. Requisitos 📌

* Una cuenta de usuario de IAM con una **política insertada**, es decir una política agregada directamente al usuario.

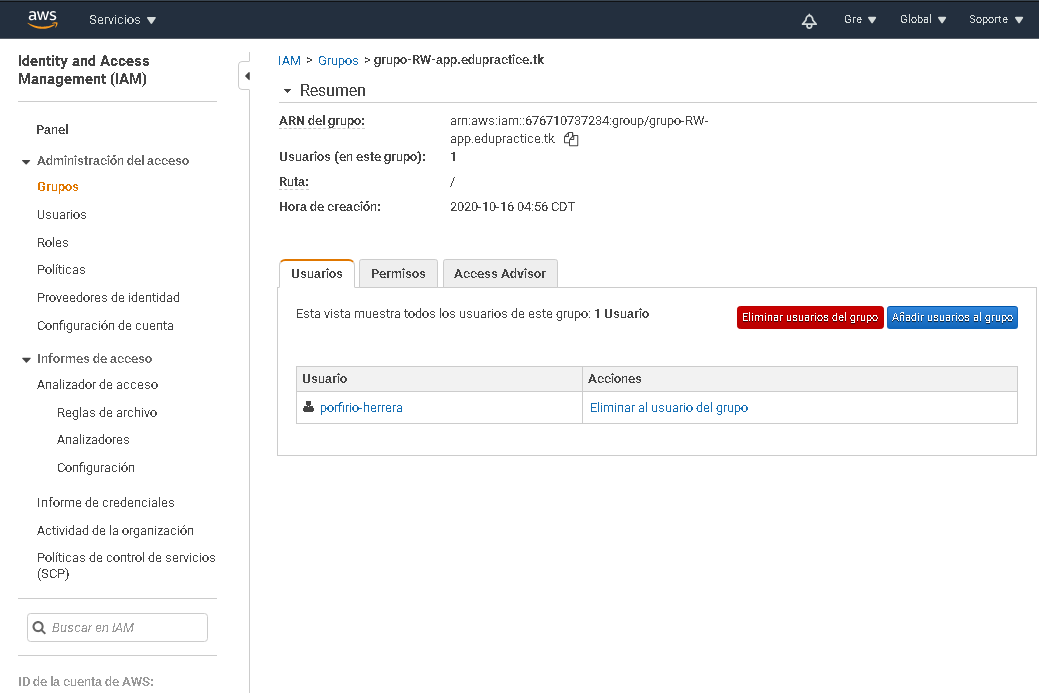
# 3. Desarrollo 📑

Una política insertada es una política que no puede ser rehusada ya que solo está disponible para el usuario para la que se generó. En el escenario que se deban agregar 20 usuarios para administrar el contenido del bucket configurado como servidor web habría que ir en cada usuario agregando la política, si la política se requiere cambiar en el futuro habrá que ir en cada usuario cambiando a política proceso en el cual es muy propenso a error humano pudiendo no aplicar correctamente las políticas de acceso o denegación a algún usuario. Se generará un grupo, a ese grupo se agregará una política, así si se requiere usar esa política solo habría que agregar a los 20 usuarios al grupo sin necesidad de ir definiendo la política usuario por usuario.

1. Ingresar a IAM, usuarios y seleccionar le usuario con la política insertada. Expandir la política insertada y copiar el contenido JSON de la política. 
2. Dirigirse al menú de políticas y luego dar click en “crear una nueva política”, con ello se generará una política que puede ser reutilizada. 
3. Dar click en JSON, copiar la política previamente copiada y dar click en “Revisar política”. 
4. AL pasar a revisión se debe especificar el nombre de la política y una descripción, la descripción debe ser lo suficientemente detallada para saber a que aplica la política y para que fue diseñada. 
5. Creada la política habrá que dirigirse a “Grupos”  Dar click en “Crear grupo” 
6. Establecer un nombre al grupo. 
7. Se busca la política recién creada para asociarla al grupo. 
8. Revisar que la política asociada es correcta, después dar click en “Crear grupo” 
9. Ingresar al grupo recién creado, para agregar usuarios. Todos los usuarios agregados tendrán aplicada la política asociada al grupo, basta con sacar al usuario del grupo para que la política deje de aplicarle.

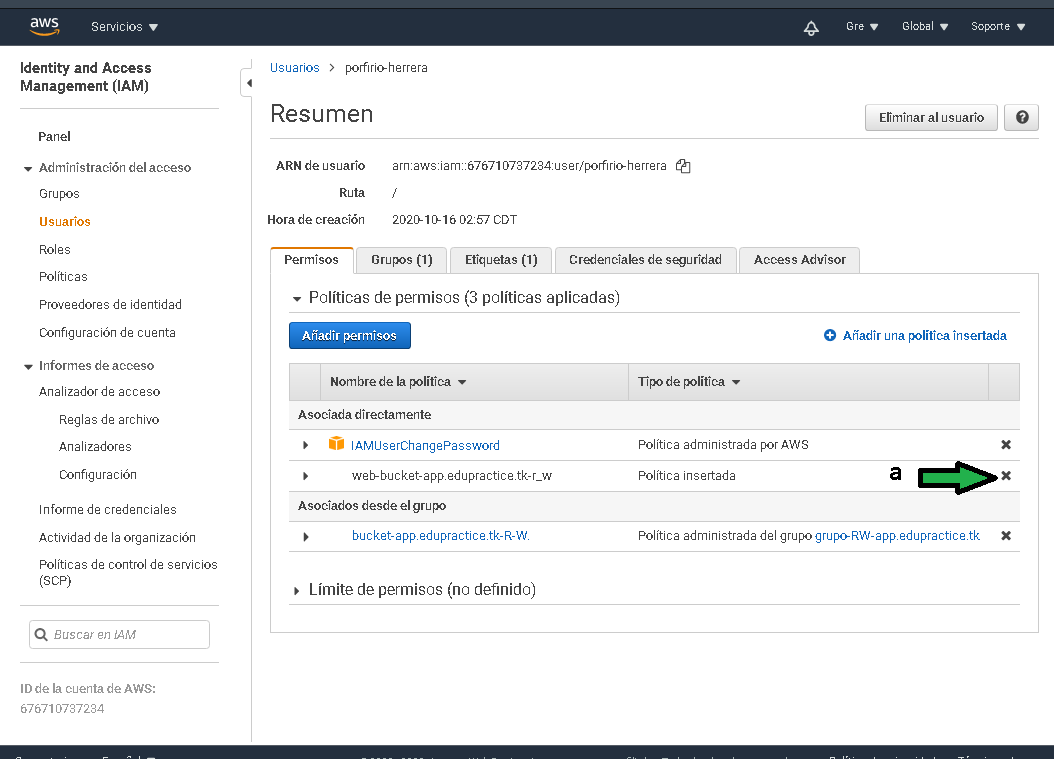


r1-add-user.png



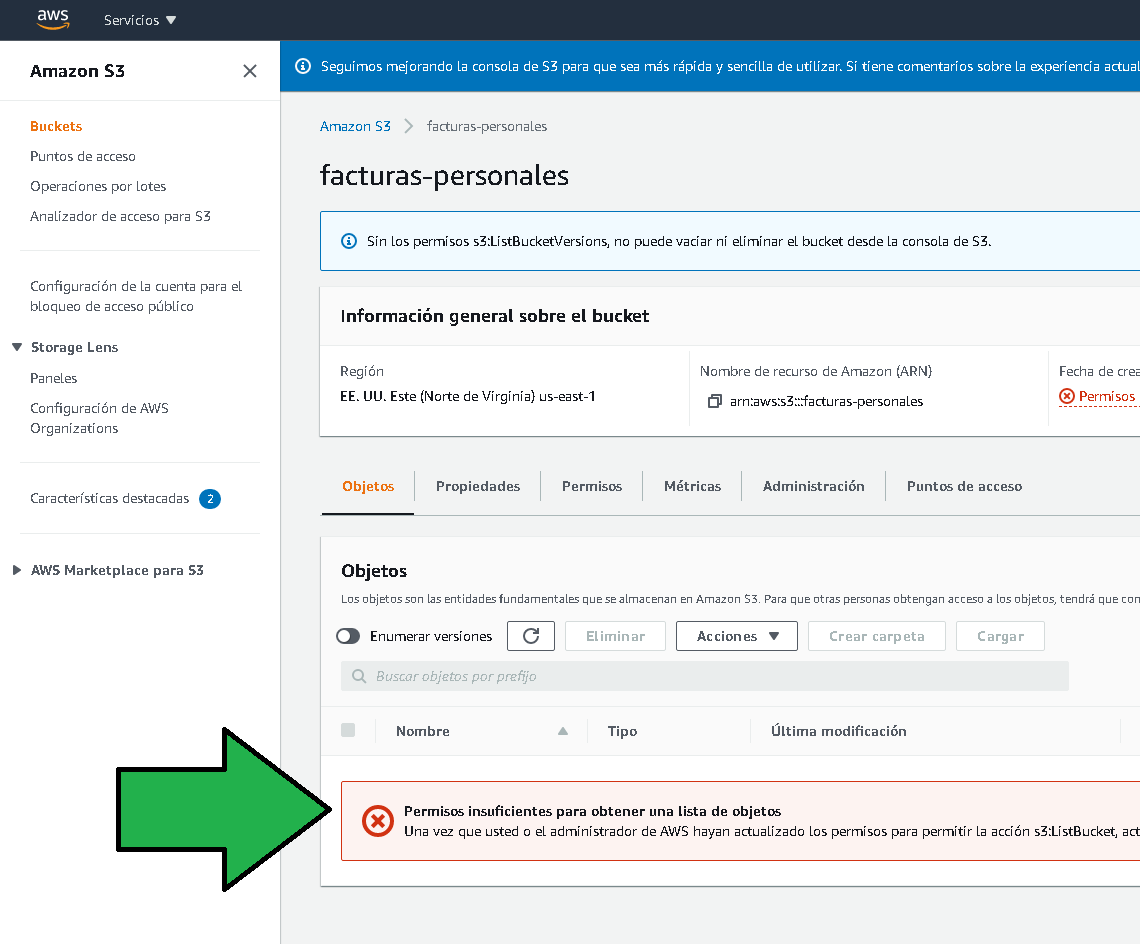
r1-add-user-done.png

1. Al ingresar el usuario se observa aún la política administrada, también se observan las políticas aplicadas al usuario por medio de la pertenencia a grupos de IAM. Ya se puede eliminar con seguridad la política insertada (a) con ello se ha generado una estructura de permisos bastante mantenible.

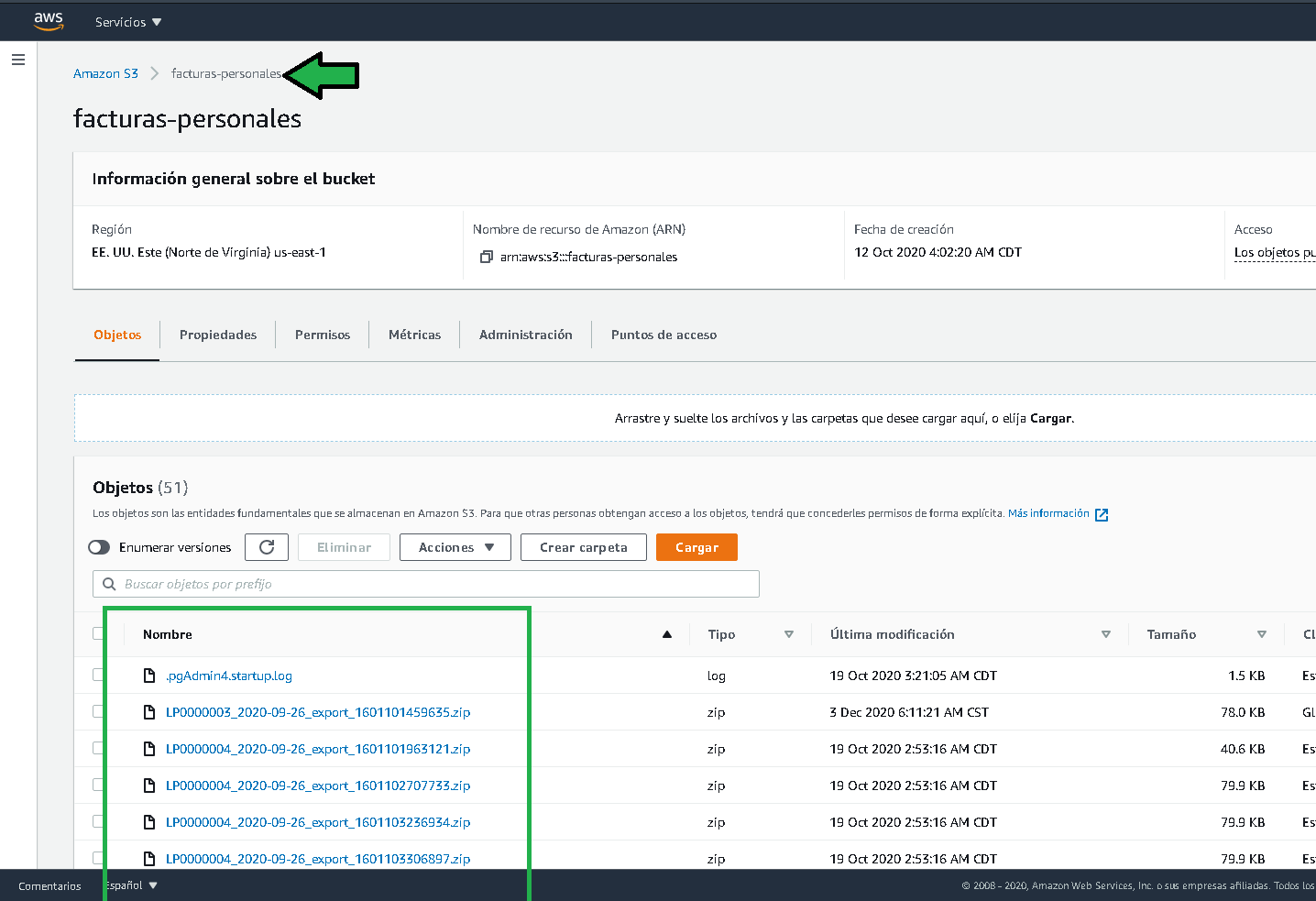


r1-remove-inserted-policy.png

1. Se comprueba que el comportamiento de los permisos del usuario sigan siendo los correctos después de eliminar la política insertada. ¡Éxito!



r1-access-denied-bucket-01.png



r1-access-granted.png