

Desafío - Bucket S3 IAM

En este desafío validaremos nuestros conocimientos de Seguridad de Aplicaciones en la nube y Gestión de Identidades en la nube. Para lograrlo, necesitarás aplicar lo aprendido hasta el momento, utilizando de apoyo las presentaciones con estos contenidos, además de los siguientes enlaces:

<https://medium.com/@emmanuelwright/create-iam-users-and-s3-buckets-in-aws-264e78281f7f>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example1.html>

Lee todo el documento antes de comenzar el desarrollo **grupal de máximo 3 integrantes**, para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

Descripción

Aplicando los conceptos y herramientas aprendidas hasta ahora, se requiere la implementación de un grupo llamado Desarrollo, dentro existirán los usuarios Paula y Juan. Además, otro grupo llamado operaciones y dentro los usuarios Paula y Juan. Se le otorgarán los accesos a los bucket según la imagen de referencia:



Sus Iniciales_developer



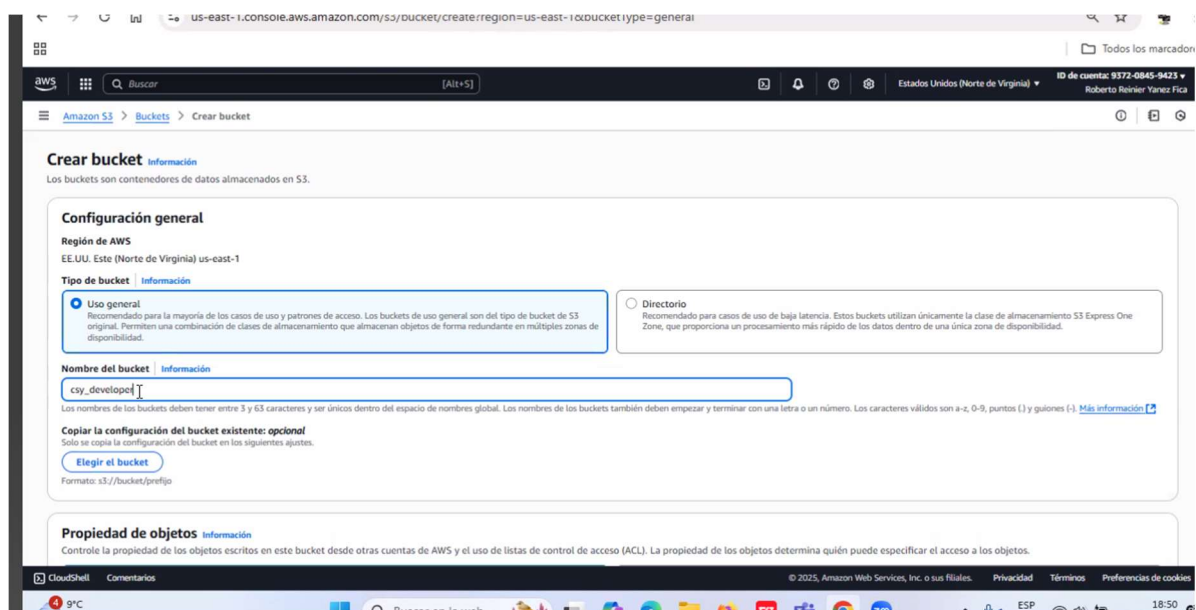
Sus Iniciales_operations



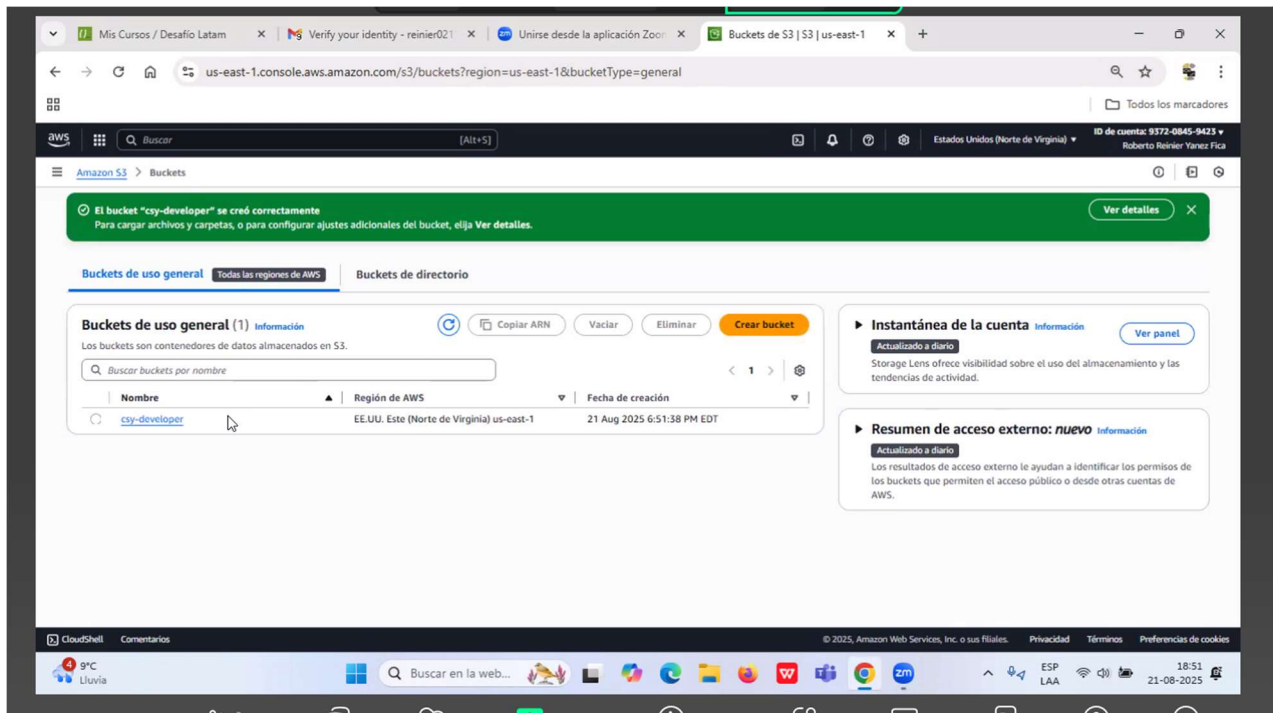
Requerimientos

1. Realizar las siguientes tareas:
 - Cree los bucket S3 sus_iniciales_developer y sus_iniciales_operations
 - Cree los grupos Desarrollo y operaciones
 - Cree los usuarios Paula y Juan - Paulo y Juana

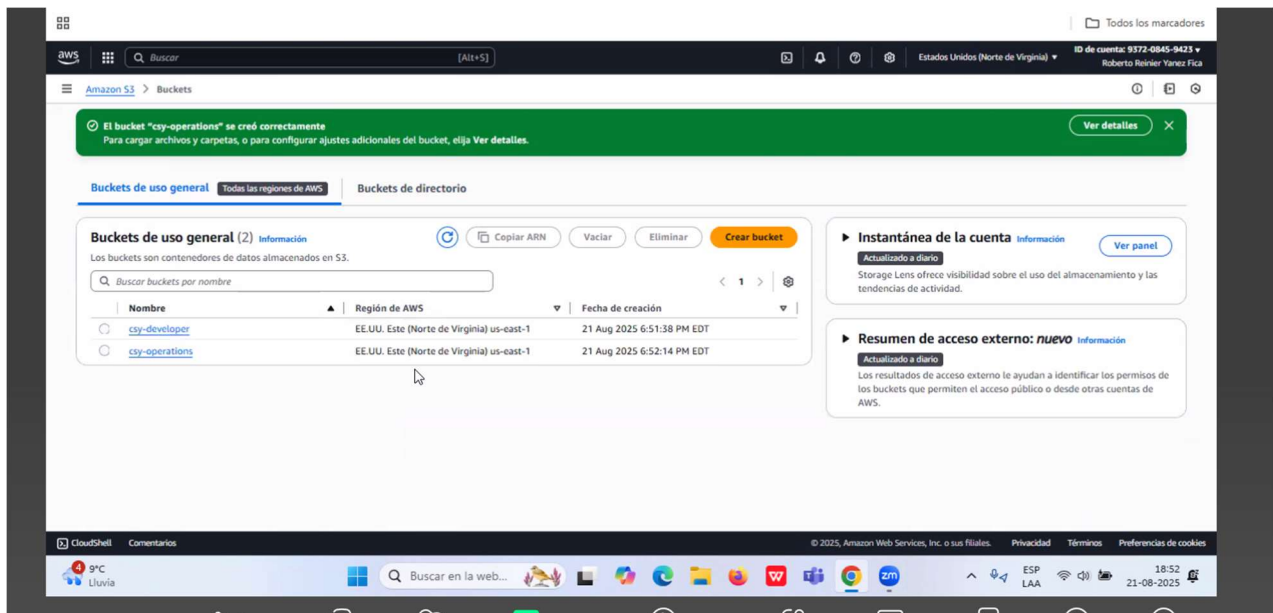
En primer lugar, se empieza creando los Bucket, según el requerimiento, la configuración del bucket es de uso general y todos los parámetros se dejan por defecto.



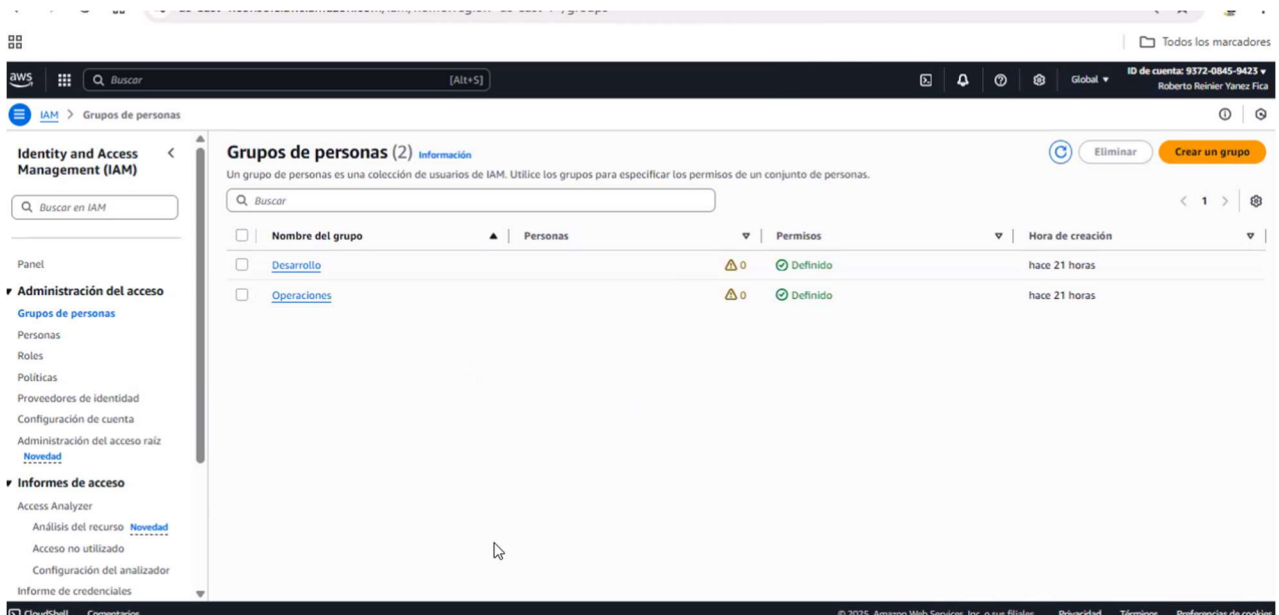
Primer Bucket creado, llamado csy-developer.



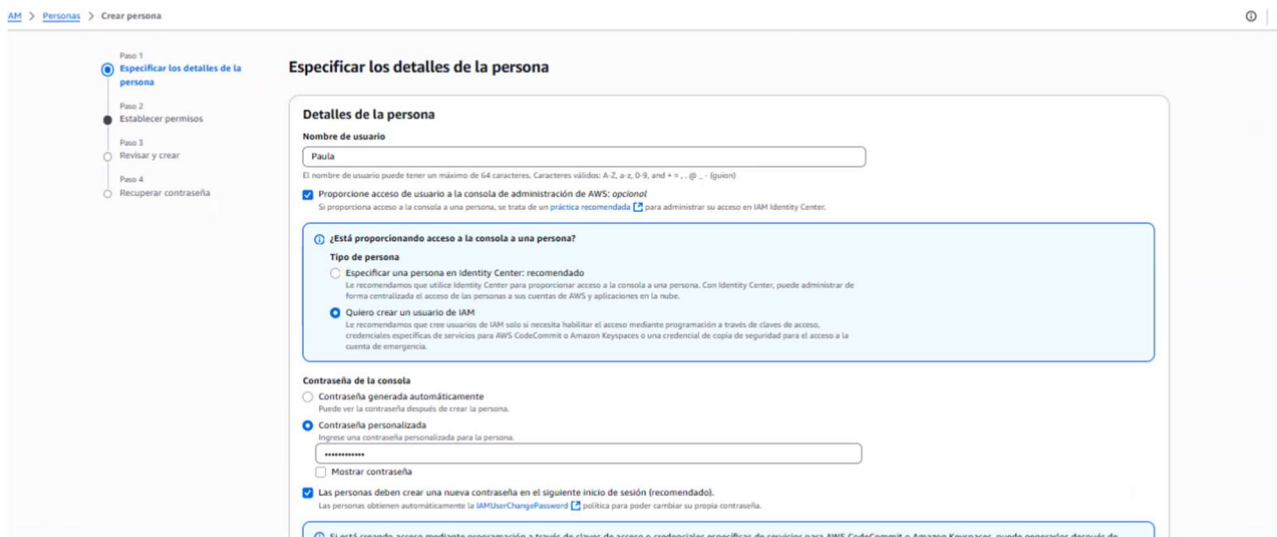
Finalmente se tienen los 2 bucket ya creados



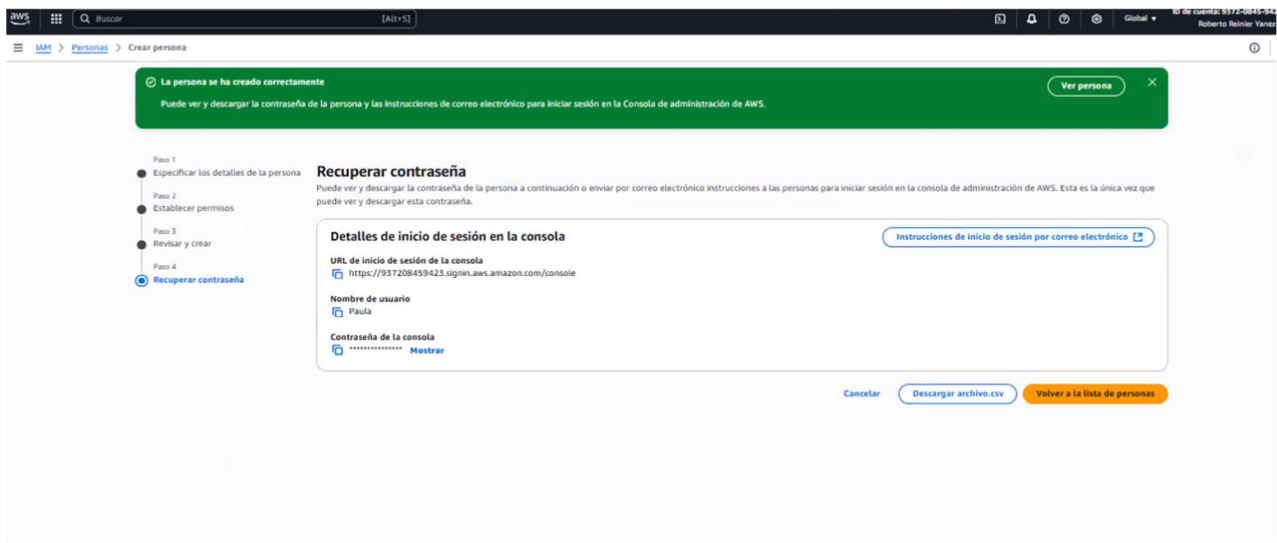
Después de crear los Bucket, hay que dirigirse a la pestaña grupo de personas, y crear los 2 grupos que se alojaran en los Bucket, “Desarrollo” y “Operaciones”



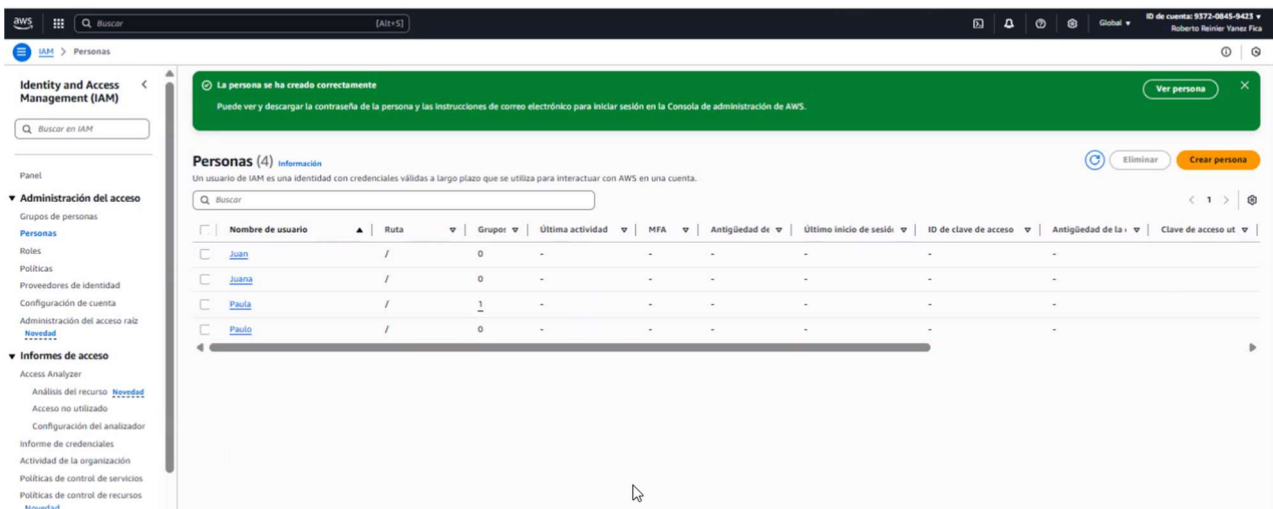
Con los grupos creados, se puede seguir con el siguiente requerimiento de crear las personas que serán incluidos en estos espacios creados. Según la configuración de la pagina de personas que se presenta a continuación.



La siguiente imagen muestra el ultimo paso de la creación de personas, donde ya se puede observar el URL de inicio de sesión, nombre y contraseña creada.

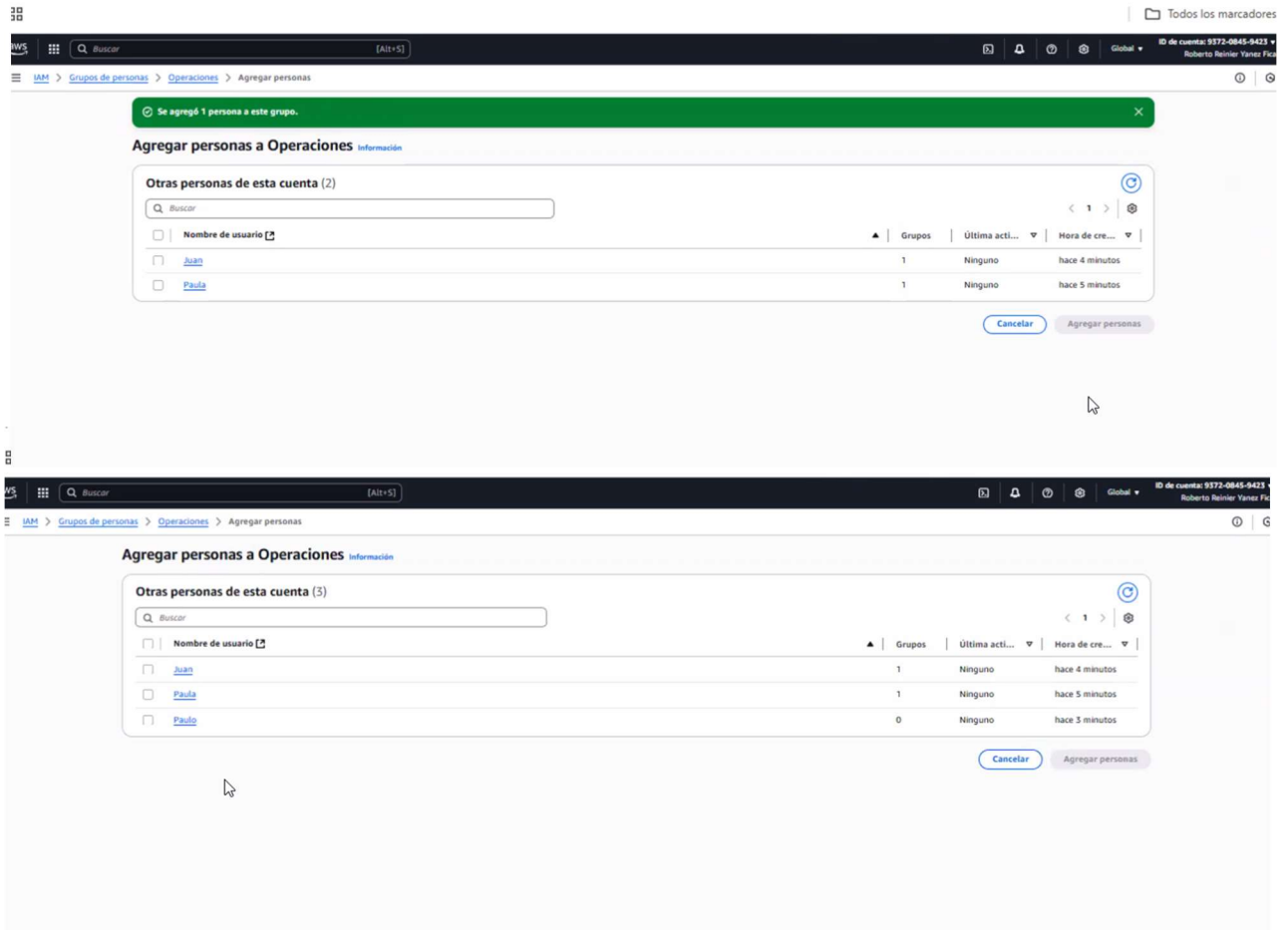


A continuación, ya se puede observar a las 4 personas creadas según el requerimiento.

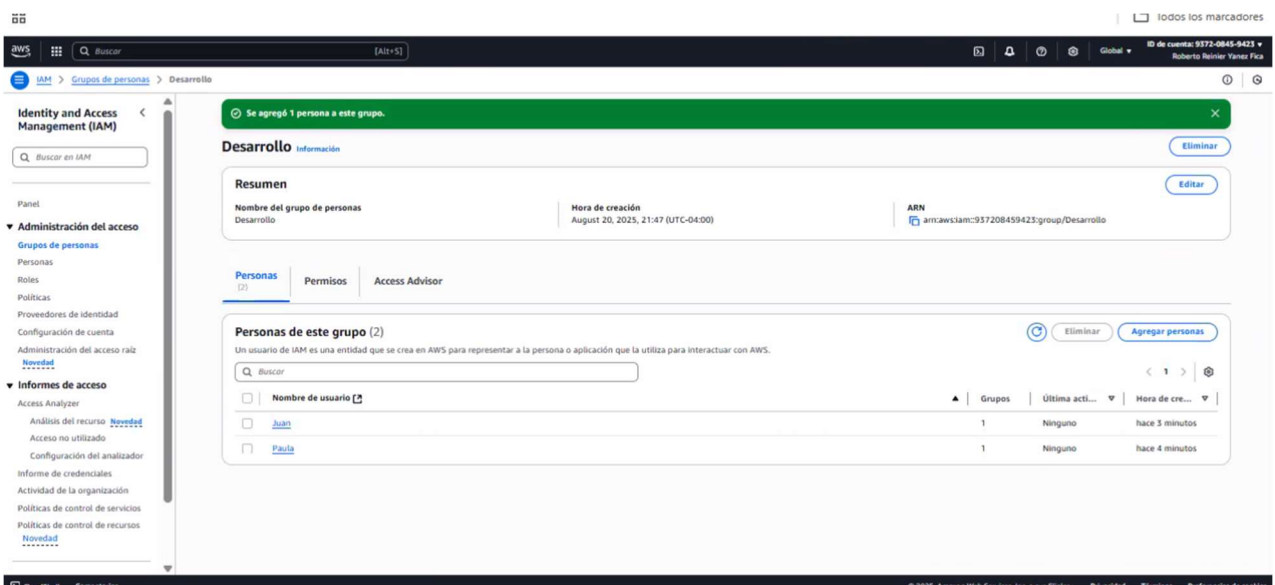


2. Asignar los usuarios a sus respectivos grupos según lo siguiente:

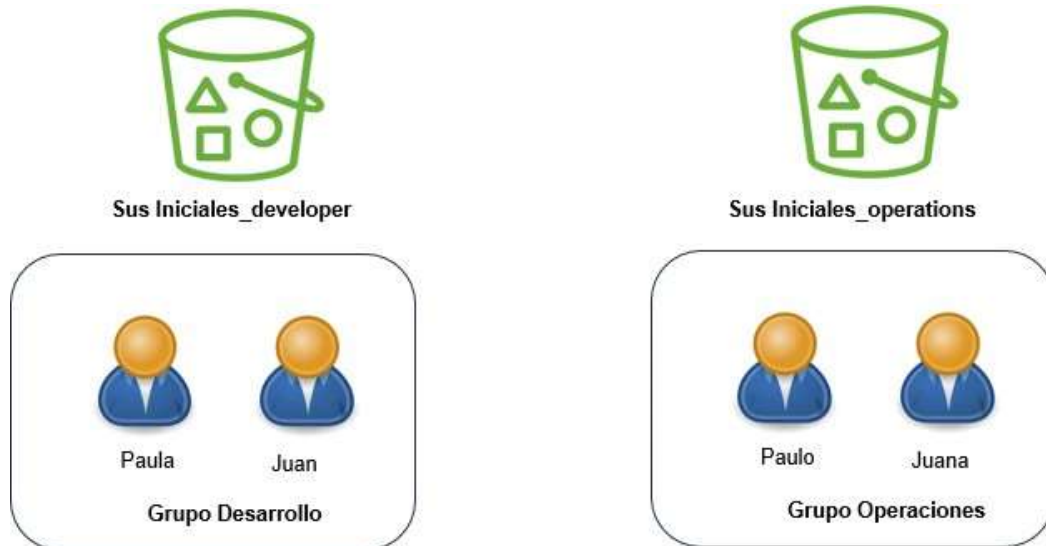
Para poder asignar los Usuarios a cada grupo se debe ingresar en la pestaña del grupo y dirigirse a la pestaña agregar personas, de igual forma como se observa en las siguientes imágenes.



En la siguiente imagen ya puede ver el grupo con las personas asignada en él.



Establecer los permisos necesarios para que solo los usuarios definidos tengan acceso a los bucket respectivos, según lo siguiente:



El entregable es un PDF con pantallazos del resultado final y una breve explicación, donde el nombre del archivo debe ser buckets3_Iniciales_nombre_Apellido.pdf (ejemplo buckets3_Iniciales_nombre_Apellido_jsilva.pdf). Indicando que es el requerimiento 3, el cual debe ser entregado según las indicaciones del docente a cargo. **(4 Puntos)**

Una vez asignado las personas a los grupos se debe crear la política de permiso, según la siguiente imagen, en donde se terminará de asignar los permisos necesarios a cada usuario, esta política se ingresa en formato JSON.

Vamos al botón políticas

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options like 'Administración del acceso', 'Personas', 'Roles', 'Políticas', 'Proveedores de identidad', 'Configuración de cuenta', 'Administración del acceso raíz', 'Novedad', 'Informes de acceso', 'Access Analyzer', 'Análisis del recurso', 'Acceso no utilizado', 'Configuración del analizador', 'Informe de credenciales', and 'Actividad de la organización'. The main content area is titled 'Políticas (1387)' and includes a search bar, a filter dropdown set to 'Todos los tipos', and a table of policies. The table has columns for 'Nombre de la política', 'Tipo', 'Usado como', and 'Descripción'. The 'Crear política' button is located in the top right corner of the main content area.

Crear política

Seleccionamos json y aplicamos el siguiente código

The screenshot shows the 'Crear política' (Create policy) page in the AWS IAM console. The 'JSON' tab is selected, displaying the following policy document:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "ListarBucketsvisibles",
6       "Effect": "Allow",
7       "Action": "s3:ListAllMyBuckets",
8       "Resource": "*"
9     },
10    {
11      "Sid": "AccessBacsdeveloper",
12      "Effect": "Allow",
13      "Action": [
14        "s3:ListBucket",
15        "s3:GetObject",
16        "s3:PutObject"
17      ],
18      "Resource": [
19        "arn:aws:s3:::csy-developer",
20        "arn:aws:s3:::csy-developer/*"
21      ]
22    }
23  ]
24 }
```

On the right, the 'Editar instrucción' (Edit statement) panel is visible, showing a 'Seleccionar una instrucción' (Select a statement) button and a '+ Agregar nueva instrucción' (Add new statement) button.

Luego seleccionamos siguiente

The screenshot shows the 'Revisar y crear' (Review and create) page in the AWS IAM console. The 'Revisar y crear' step is selected, and the 'Información' (Information) tab is active. The page displays the following details:

- Nombre de la política** (Policy name): (128 caracteres como máximo. Utilice caracteres alfanuméricos y "+", "@", ".", "_").
- Descripción: opcional** (Optional description): (1000 caracteres como máximo. Utilice caracteres alfanuméricos y "+", "@", ".", "_").
- Permisos definidos en esta política** (Permissions defined in this policy): A table with columns for 'Servicio' (Service), 'Nivel de acceso' (Access level), 'Recurso' (Resource), and 'Condición de solicitud' (Request condition). The table shows 53 permissions, with the first row being 's3' with 'Limitado: Enumerar, Leer' (Limited: Enumerate, Read) access level, 'Multiple' resource, and 'None' condition.

Generamos el nombre de la política y creamos la política ahora la asignaremos a los grupos necesarios las políticas anteriormente creadas

Ingresamos al grupo en caso de ejemplo desarrollo

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like 'Grupos de personas', 'Personas', 'Roles', 'Políticas', etc. The main content area is titled 'Desarrollo' and shows a 'Resumen' section with details like 'Nombre del grupo de personas: Desarrollo', 'Hora de creación: August 21, 2025, 19:35 (UTC-04:00)', and 'ARN: arn:aws:iam:174774135718:group/Desarrollo'. Below this, there are tabs for 'Personas', 'Permisos', and 'Access Advisor'. The 'Permisos' tab is active, showing 'Políticas de permisos (0)' and a search bar. The bottom of the page shows a message: 'No hay recursos que mostrar'.

Vamos a botón añadir permisos y seleccionamos añadir política Buscamos el nombre de la política creada en nuestro caso Política-desarrollo

The screenshot shows the 'Añadir permisos' page in the AWS IAM console. The main content area is titled 'Asociar políticas de permisos a Desarrollo'. It shows a search bar with 'Politi' entered, resulting in 2 coincidencias. The search results table lists two policies: 'Política-desarrollo' and 'Política-operaciones'. The 'Política-desarrollo' policy is selected. The bottom of the page shows a 'Cancelar' button and an 'Asociar políticas' button.

Seleccionamos la política

The screenshot shows the 'Añadir permisos' page in the AWS IAM console, with the 'Política-desarrollo' policy selected. The search results table lists two policies: 'Política-desarrollo' and 'Política-operaciones'. The 'Política-desarrollo' policy is selected. The bottom of the page shows a 'Cancelar' button and an 'Asociar políticas' button.

Y asociamos la política
Y veremos que tenemos asociada una entidad

The screenshot shows the AWS IAM console interface. On the left is a navigation pane with sections like 'Administración del acceso' and 'Informes de acceso'. The main content area is titled 'Desarrollo' and shows the 'Resumen' tab. It displays the group name 'Desarrollo', its creation time, and its ARN. Below this, the 'Políticas de permisos' section shows a table with one policy named 'Política-desarrollo' associated with the group.

Nombre de la política	Tipo	Entidades asociadas
Política-desarrollo	Administrada por el cliente	1

después de crear esto verificaremos el acceso de usuarios y veremos la funcionalidad de los permisos

The screenshot shows the 'IAM user sign in' page. It includes a header with the title and an information icon. Below the header, there is a section for 'Account ID or alias' with a text input field containing '174774135718' and a link for users who don't have an account. A checkbox for 'Remember this account' is present. The 'IAM username' section has a text input field with 'Paula'. The 'Password' section has a password input field with masked characters. There is a checkbox for 'Show Password' and a link for 'Having trouble?'. At the bottom, there is a large orange 'Sign in' button and a button for 'Sign in using root user email'.

Password reset ⓘ

Your account **(174774135718)** password has expired or requires a reset.

To continue, please verify your old and set a new password for **Paula** (not you?).

Old Password

☒ Show Password

New Password

Confirm New Password

☒ Show Password

Matches

Confirm Password Change

Elegimos s3

aws

Buscar

[Alt+S]

Europa (Estocolmo)

ID de cuenta: 1747-7413-5718

Paula

Amazon S3

Buckets de uso general

Buckets de directorio

Buckets de tablas

Buckets vectoriales

Concesiones de acceso

Puntos de acceso (buckets de uso general, sistemas de archivos FSx)

Puntos de acceso (buckets de directorio)

Puntos de acceso del objeto Lambda

Puntos de acceso de varias regiones

Operaciones por lotes

Analizador de acceso de IAM para S3

Configuración de bloqueo de acceso múltiple correspondiente a

Buckets de uso general (2) Información

Copiar ARN

Vaciar

Eliminar

Crear bucket

Los buckets son contenedores de datos almacenados en S3.

Buscar buckets por nombre

< 1 >

	Nombre	Región de AWS	Fecha de creación
<input type="radio"/>	cys-developer	EE.UU. Este (Ohio) us-east-2	21 Aug 2025 7:34:19 PM -04
<input type="radio"/>	cys-operations	EE.UU. Este (Ohio) us-east-2	21 Aug 2025 7:34:49 PM -04

Instantánea de la cuenta Información

Actualizado a diario

Ver panel

Storage Lens ofrece visibilidad sobre el uso del almacenamiento y las tendencias de actividad.

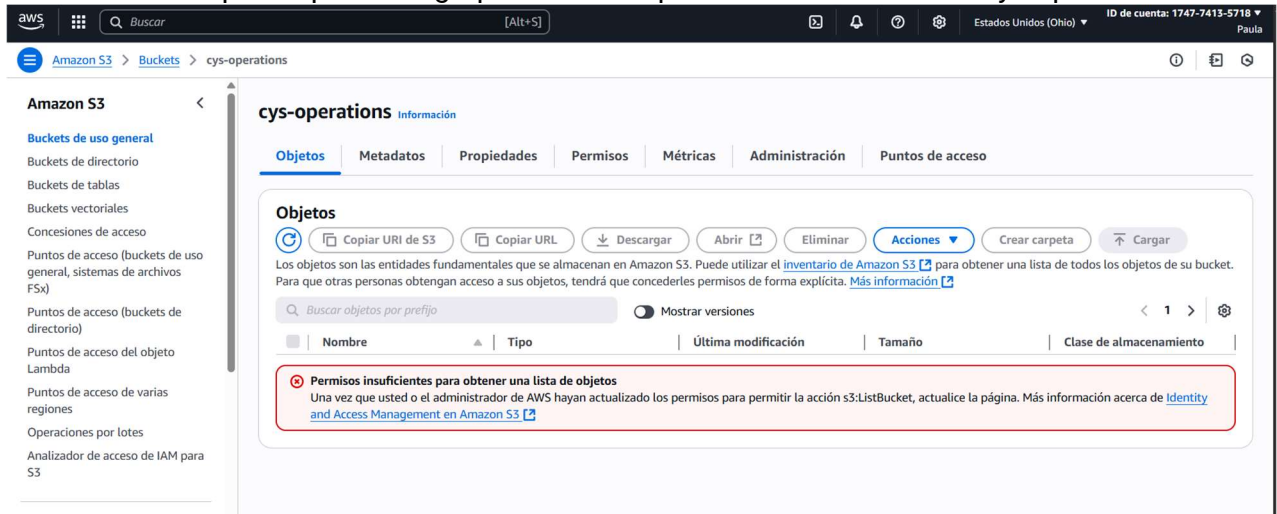
Resumen de acceso externo: nuevo

Actualizado a diario

Información

Los resultados de acceso externo le ayudan a identificar los permisos de los buckets que permiten el acceso público o desde otras cuentas de AWS.

Y verificamos si paula que es de grupo Desarrollo puede acceder al bucket cys-operations



Amazon S3 > Buckets > cys-operations

cys-operations Información

Objetos | Metadatos | Propiedades | Permisos | Métricas | Administración | Puntos de acceso

Objetos

Copiar URI de S3 Copiar URL Descargar Abrir Eliminar Acciones Crear carpeta Cargar

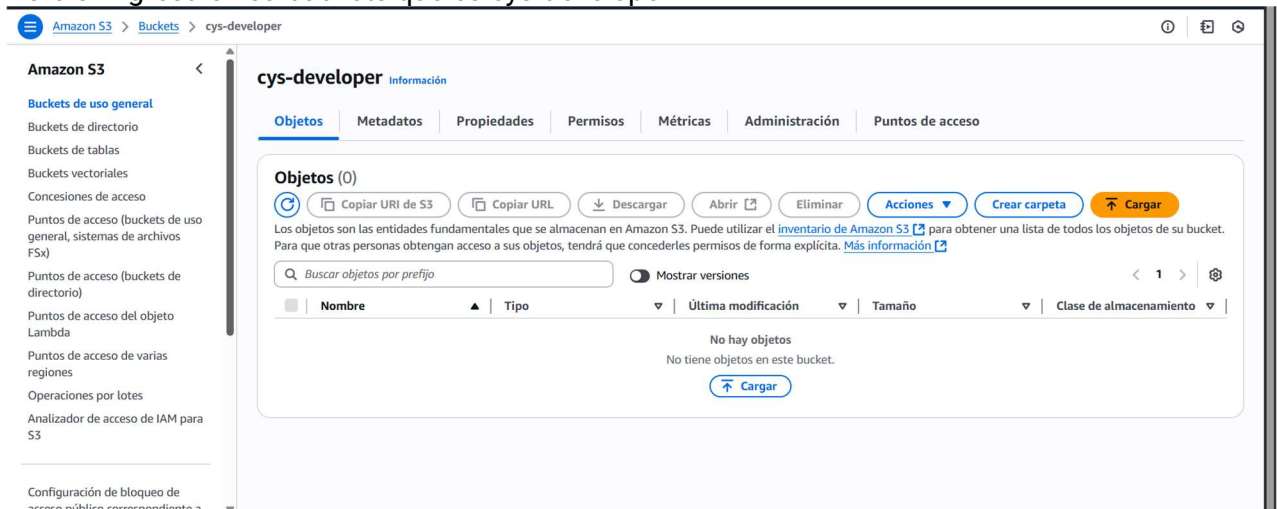
Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el [inventario de Amazon S3](#) para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)

Buscar objetos por prefijo Mostrar versiones

Nombre Tipo Última modificación Tamaño Clase de almacenamiento

Permisos insuficientes para obtener una lista de objetos
Una vez que usted o el administrador de AWS hayan actualizado los permisos para permitir la acción s3:ListBucket, actualice la página. Más información acerca de [Identity and Access Management en Amazon S3](#)

Pero si ingresa en su buckets que es cys-developer



Amazon S3 > Buckets > cys-developer

cys-developer Información

Objetos | Metadatos | Propiedades | Permisos | Métricas | Administración | Puntos de acceso

Objetos (0)

Copiar URI de S3 Copiar URL Descargar Abrir Eliminar Acciones Crear carpeta Cargar

Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el [inventario de Amazon S3](#) para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)

Buscar objetos por prefijo Mostrar versiones

Nombre Tipo Última modificación Tamaño Clase de almacenamiento

No hay objetos
No tiene objetos en este bucket.
Cargar

Ahora se comprobará acceso de un usuario del grupo operaciones y comprobaremos que no tiene acceso al bucket developer
también como la anterior nos solicita cambio de contraseña

Password reset ⓘ

Your account (**174774135718**) password has expired or requires a reset.

To continue, please verify your old and set a new password for **Paulo** (not you?).

Old Password

.....

☐ Show Password

New Password

.....

Confirm New Password

.....

☐ Show Password

Matches

Confirm Password Change

aws

Q Buscar

[Alt+S]

Estados Unidos (Ohio)

Id de cuenta: 1747-7413-5718

Paulo

Amazon S3

Buckets de uso general

Buckets de directorio

Buckets de tablas

Buckets vectoriales

Concesiones de acceso

Puntos de acceso (buckets de uso general, sistemas de archivos FSx)

Puntos de acceso (buckets de directorio)

Puntos de acceso del objeto Lambda

Puntos de acceso de varias regiones

Operaciones por lotes

Analizador de acceso de IAM para S3

Configuración de bloqueo de

Buckets de uso general

Todas las regiones de AWS

Buckets de directorio

Buckets de uso general (2) Información

Copiar ARN

Vaciar

Eliminar

Crear bucket

Los buckets son contenedores de datos almacenados en S3.

Q Buscar buckets por nombre

< 1 >

	Nombre	Región de AWS	Fecha de creación
<input type="radio"/>	cys-developer	EE.UU. Este (Ohio) us-east-2	21 Aug 2025 7:34:19 PM -04
<input type="radio"/>	cys-operations	EE.UU. Este (Ohio) us-east-2	21 Aug 2025 7:34:49 PM -04

Instantánea de la cuenta Información

Actualizado a diario

Ver panel

Storage Lens ofrece visibilidad sobre el uso del almacenamiento y las tendencias de actividad.

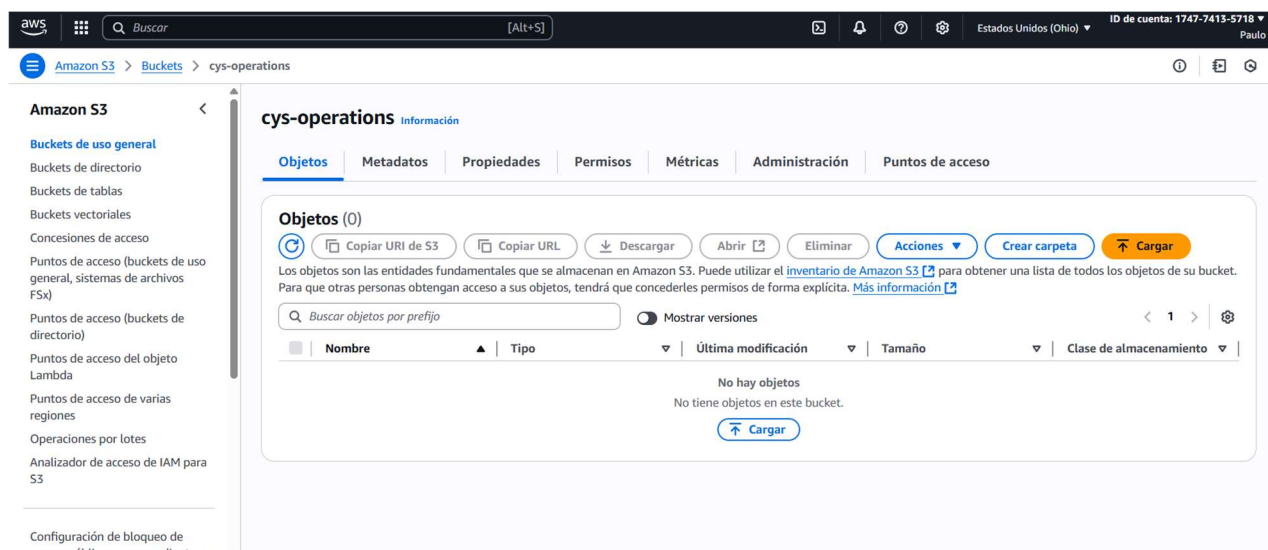
Resumen de acceso externo: nuevo

Actualizado a diario

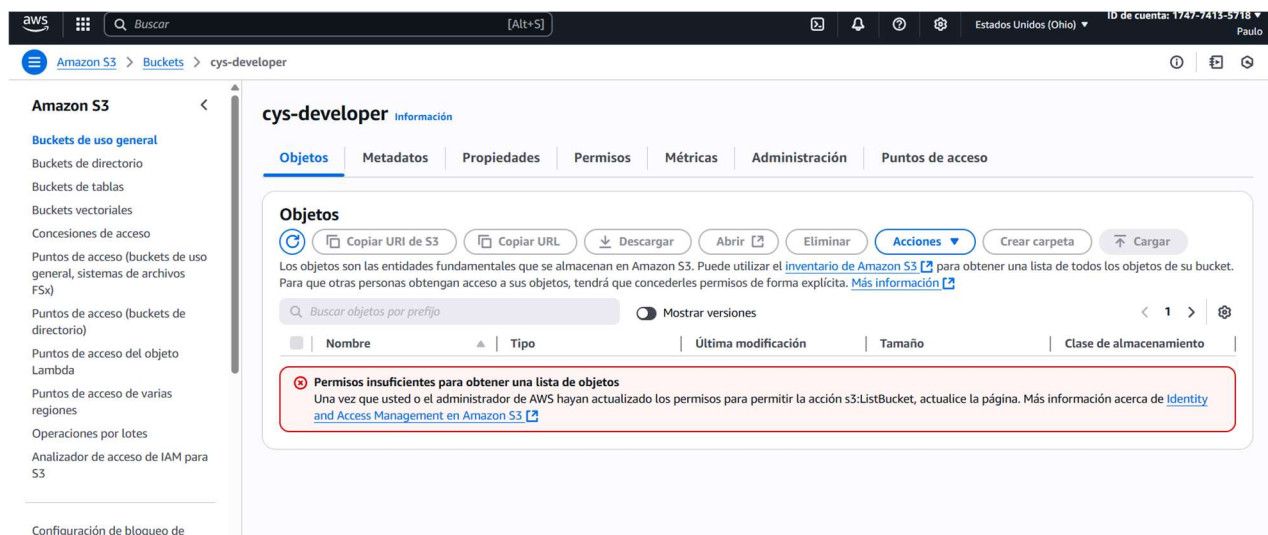
Información

Los resultados de acceso externo le ayudan a identificar los permisos de los buckets que permiten el acceso público o desde otras cuentas de AWS.

En este caso como es usuario de cys operation tiene acceso a este recurso



Revisaremos si Paulo Tiene Acceso a cys-developer



Como Verificamos usuario no tiene acceso al bucket cys-developer