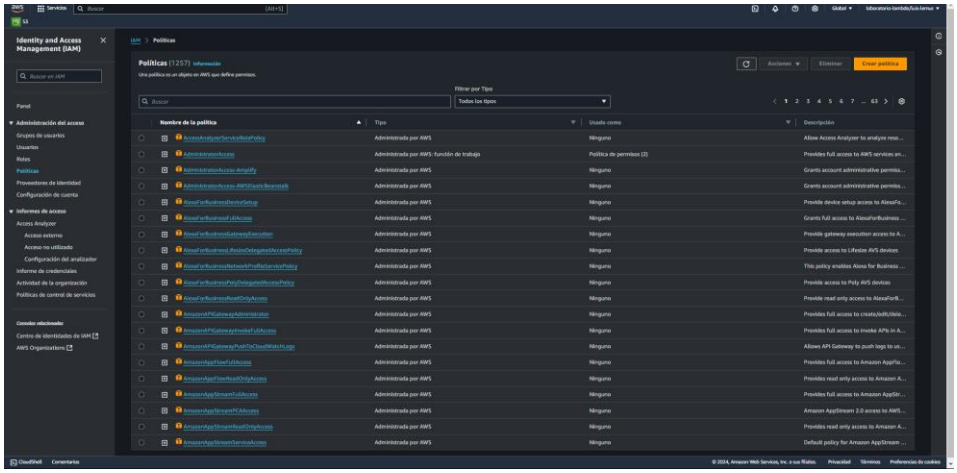
PRACTICA LAMBDA, SECRETS MANAGER Y CLOUDWATCH

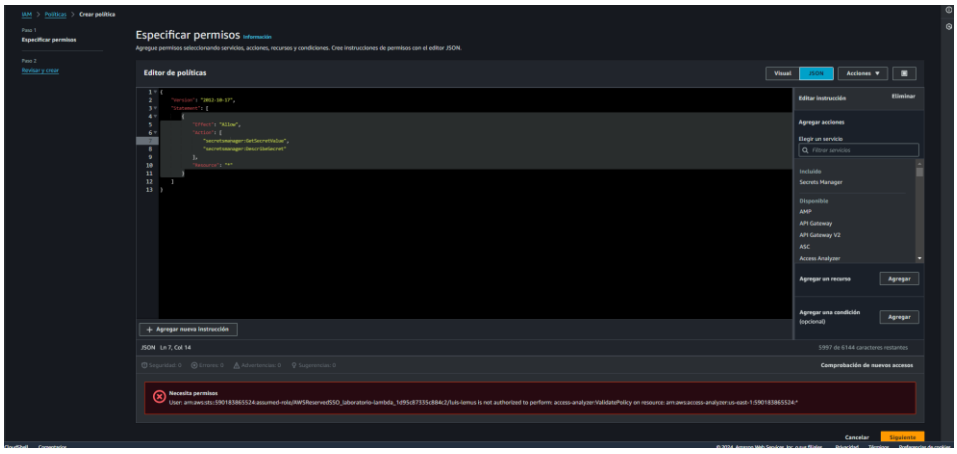
Paso 1: Crear una nueva política en IAM

1. Inicia sesión en la **Consola de AWS**.
2. Navega al servicio **IAM (Identity and Access Management)**.
3. En el menú lateral izquierdo, selecciona **Políticas**.
4. Haz clic en el botón **Crear Política.**



Paso 2: Definir permisos utilizando JSON

1. Dentro del apartado **Crear Política**, selecciona la pestaña **JSON** para especificar los permisos.
2. En la sección de JSON, ingresa la siguiente estructura para permitir acceso de solo lectura a Secrets Manager:



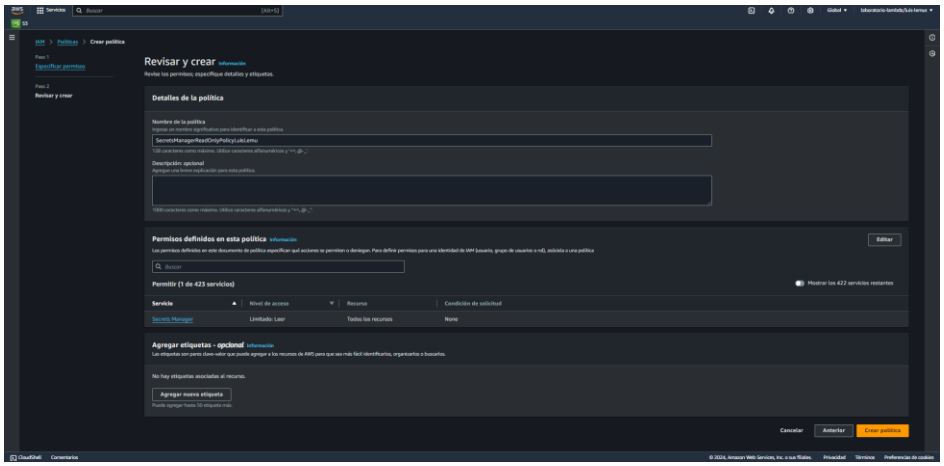
3. Esta política permite específicamente las acciones GetSecretValue y DescribeSecret para todos los secretos en Secrets Manager.

Paso 3: Revisar y crear la política

1. Después de ingresar el JSON, haz clic en **Next: Tags** para agregar etiquetas opcionales si las necesitas (puedes saltarte este paso si no deseas añadir etiquetas).
2. Haz click en **Siguiente**.

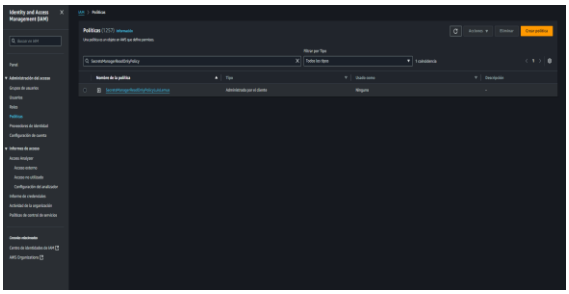
Paso 4: Asignar nombre y descripción a la política

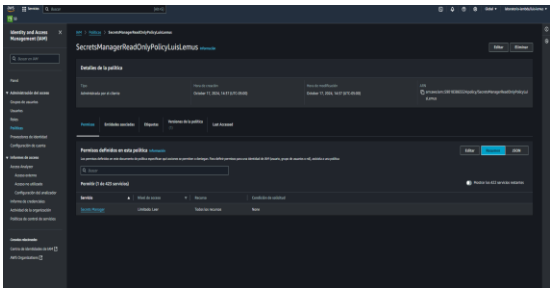
1. En la página de revisión, asigna un nombre a la política en el campo **Nombre**. Ingresa: SecretsManagerReadOnlyPolicyLuisLemus.
2. (Opcional) Agrega una descripción breve en el campo **Descripción** para identificar el propósito de la política.
3. Haz clic en **Crear Política** para finalizar.



Resultado

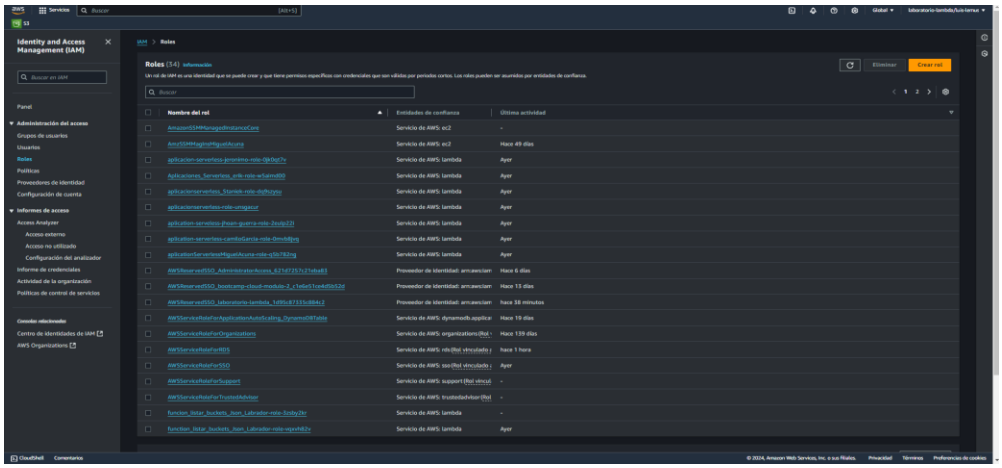
Ya habrás creado una política con permisos de solo lectura en Secrets Manager, nombrada SecretsManagerReadOnlyPolicyLuisLemus.





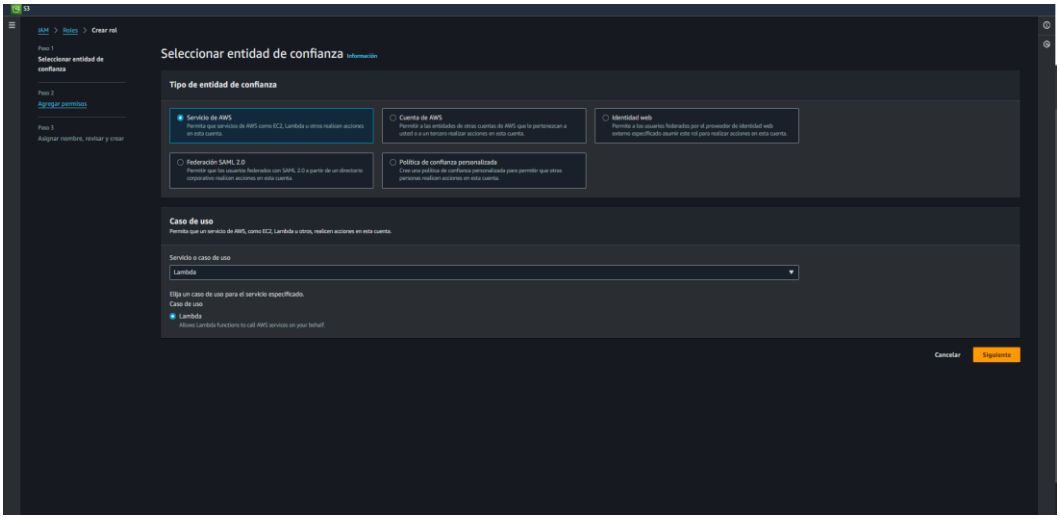
Paso 5: Crear un nuevo rol en IAM

1. Inicia sesión en la **Consola de AWS**.
2. Navega al servicio **IAM (Identity and Access Management)**.
3. En el menú lateral izquierdo, selecciona **Roles**.
4. Haz clic en el botón **Crear Rol.**



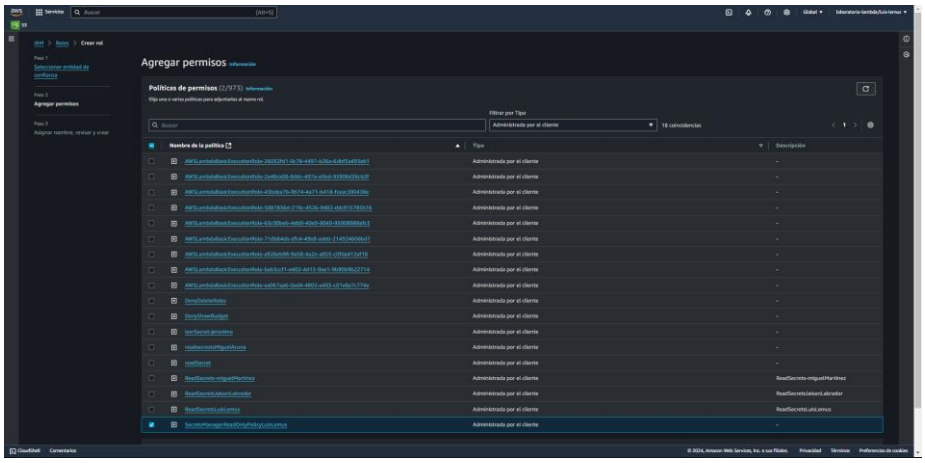
Paso 6: Seleccionar el tipo de entidad de confianza

1. En la página de creación del rol, selecciona **Servicio de AWS** como entidad de confianza.
2. En la lista de servicios, selecciona **Lambda**.
3. Haz clic en **Siguiente.**



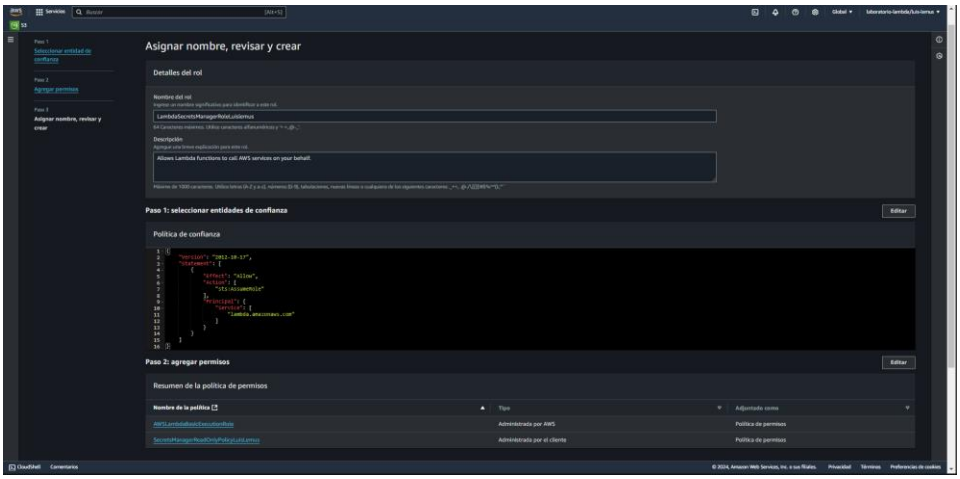
Paso 7: Adjuntar la política al rol

1. En la página Adjuntar políticas de permisos, utiliza el campo de búsqueda para encontrar la política personalizada que creaste anteriormente, SecretsManagerReadOnlyPolicyLuisLemus.
2. Marca la casilla junto a la política SecretsManagerReadOnlyPolicyLuisLemus.
3. Haz clic en Siguiente: Revisar.



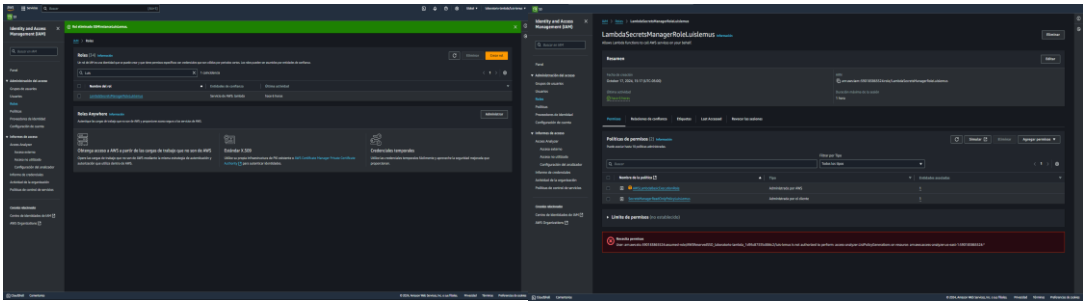
Paso 8: Revisar y crear el rol

1. En la página de revisión, asigna un nombre al rol, como: LambdaSecretsManagerRoleLuisLemus.
2. (Opcional) Agrega una descripción en el campo **Descripción** para identificar el propósito del rol.
3. Haz clic en **Crear rol** para finalizar.



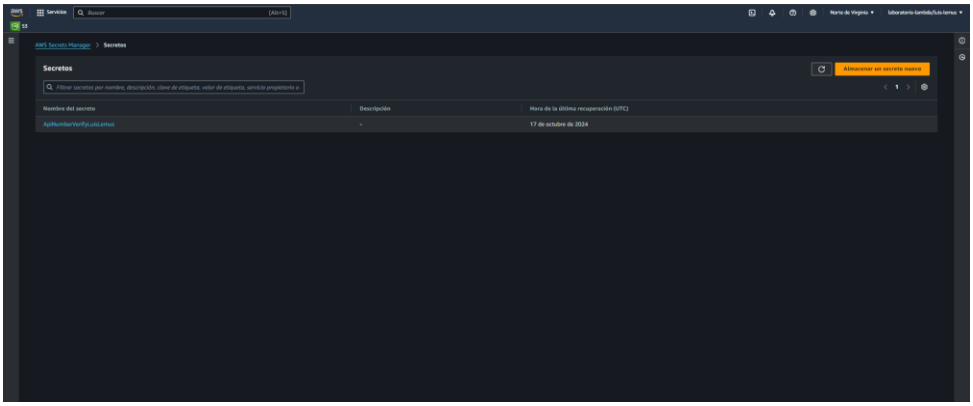
Resultado

Ya habrás creado un rol en IAM llamado LambdaSecretsManagerRoleLuisLemus, y la política de solo lectura para Secrets Manager (SecretsManagerReadOnlyPolicyLuisLemus) se habrá adjuntado correctamente durante el proceso de creación del rol.



Paso 9: Crear un nuevo secreto

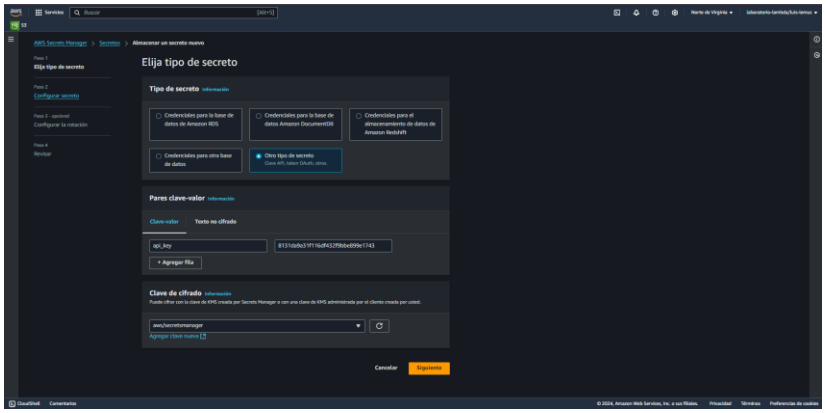
1. En la página principal de Secrets Manager, haz clic en el botón Almacenar un nuevo secreto.



Paso 10: Seleccionar el tipo de secreto

1. En la página **Elegir el tipo de secreto**, selecciona **Otro tipo de secreto**.

Esto te permitirá definir tus propios pares clave-valor.



Paso 11: Definir los pares clave-valor

1. En la sección **Pares clave/valor**, agrega un par clave-valor donde la clave sea api_key y el valor sea tu clave de API específica.

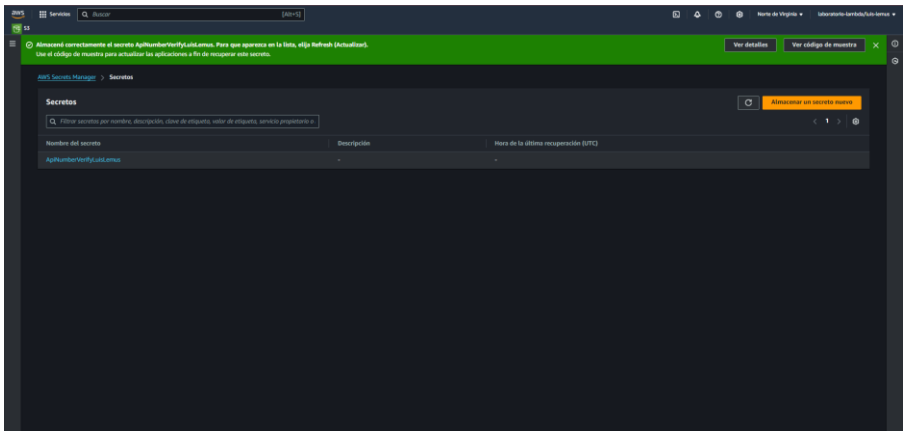
Ejemplo:

- Clave: api_key
- Valor: tu_valor_de_api_key

2. Si deseas añadir más pares clave-valor, puedes hacer clic en **Agregar otro par clave/valor**, aunque en este caso solo has especificado uno.
3. Y luego le das Siguiente al resto de opciones porque no haremos ningún cifrado ni configuraremos la rotación
4. Al final Revisamos y creamos el secreto.

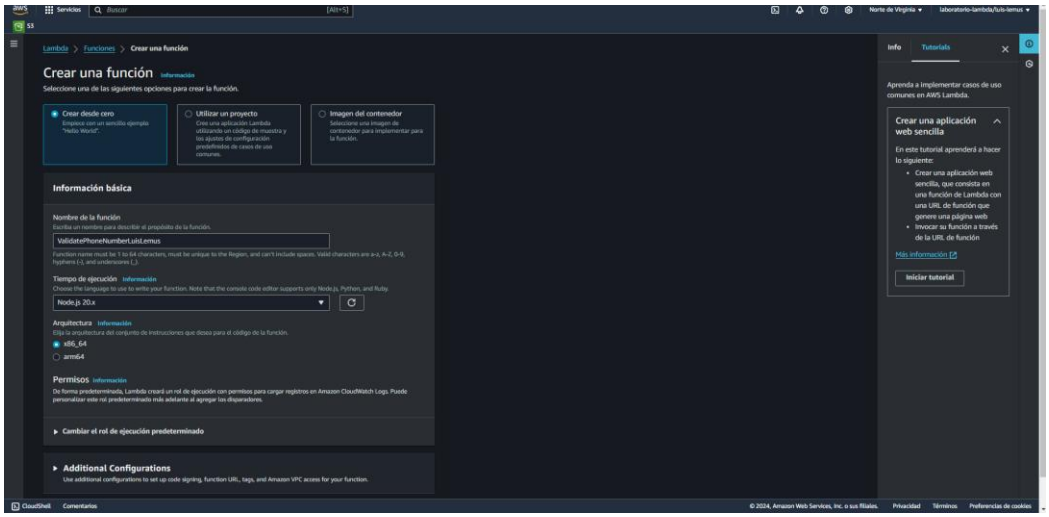
Resultado

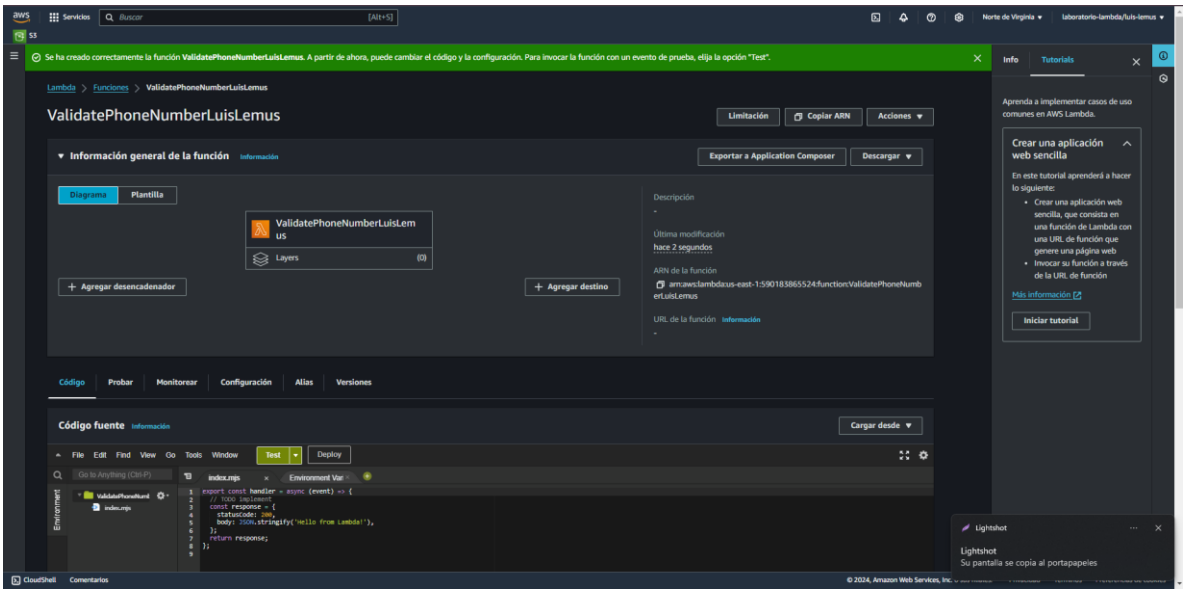
Ya habrás creado un secreto en Secrets Manager con el tipo "Otro tipo de secreto", utilizando pares clave-valor donde definiste api_key, y has dejado la clave de cifrado predeterminada sin cambios.



Paso 12: Crear una nueva función Lambda

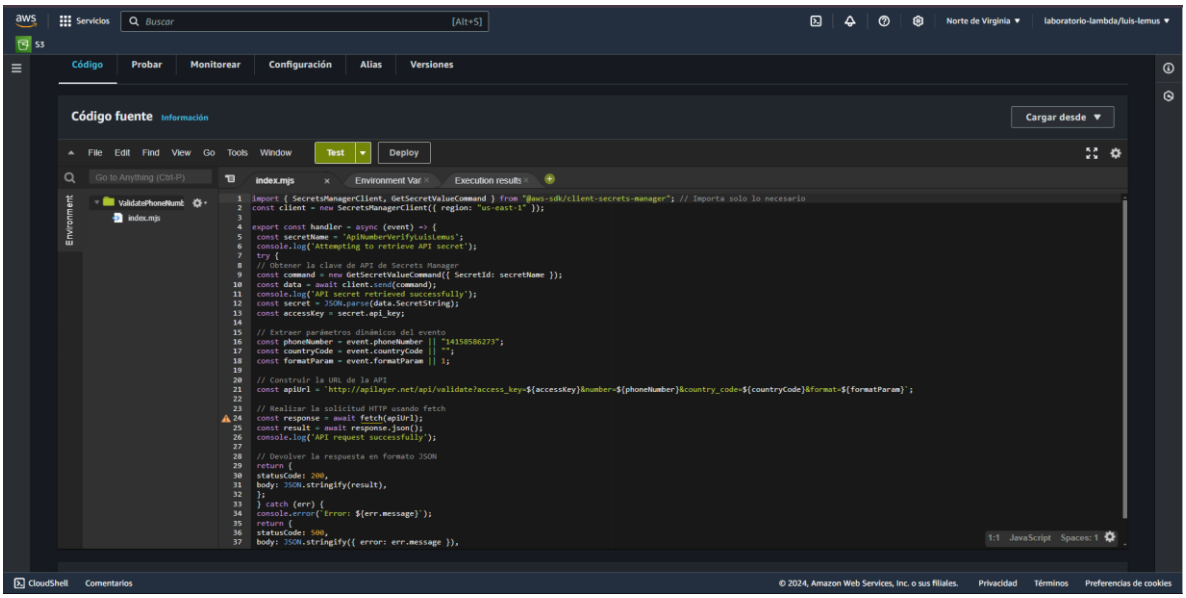
1. En la página principal de Lambda, haz clic en el botón **Crear función.**
2. Selecciona la opción **Crear desde cero.**
3. Ingresa los siguientes datos:
    - **Nombre de la función:** ValidatePhoneNumberLuisLemus.
    - **Tiempo de ejecución:** Selecciona Node.js 20.x.
4. **En Permisos:**
    - Selecciona Usar un rol existente.
    - Elige el rol previamente creado, llamado **LambdaSecretsManagerRoleLuisLemus.**
5. **Haz clic en Crear función.**





Paso 13: Agregar el código a la función Lambda

1. En la página de configuración de la función, ve a la sección **Código**.
2. Elimina cualquier código de ejemplo que aparezca.
3. Sustituye el código existente por el siguiente:

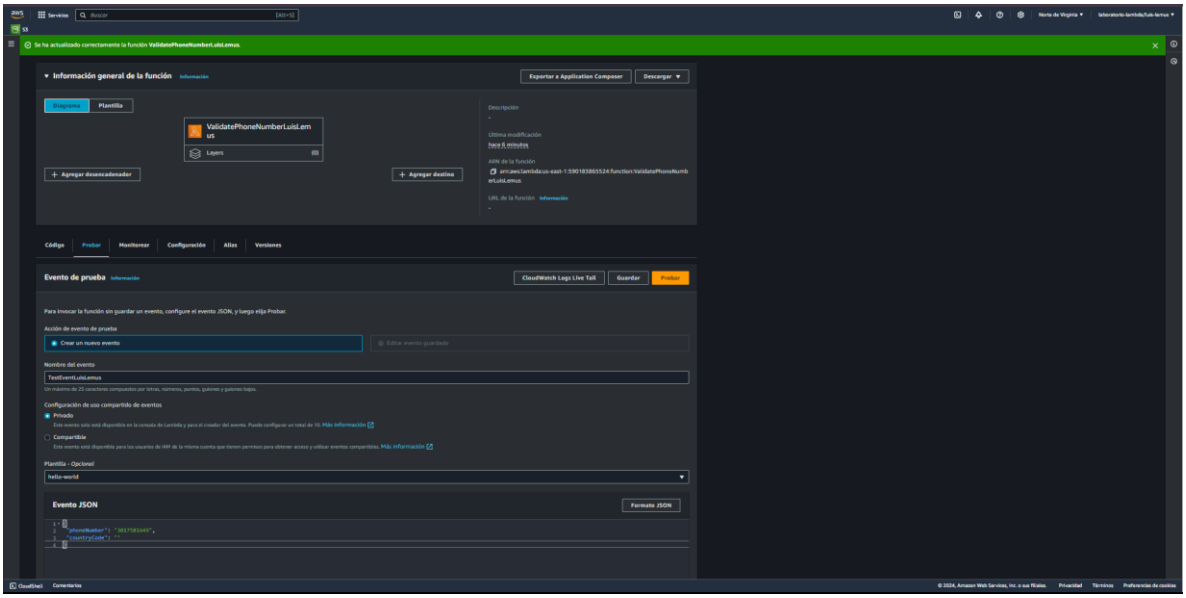


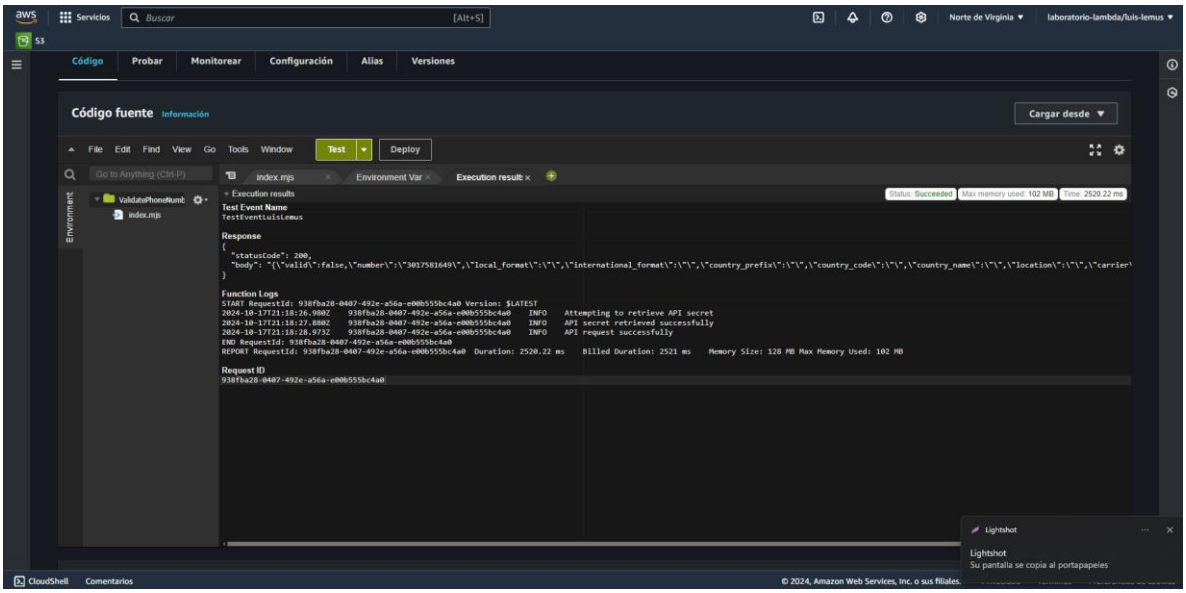
Paso 14: Crear un evento de prueba

1. En la parte superior de la pantalla de configuración de la función, haz clic en **Probar**.
2. En la ventana emergente, ingresa el nombre del evento de prueba, por ejemplo, TestEventPhoneNumber.
3. En el campo **JSON de entrada**, ingresa lo siguiente:

```
{
  "phoneNumber": "14158586273",
  "countryCode": ""
}
```

4. Haz clic en **Crear** para guardar el evento de prueba.





Paso 15: Revisar los logs en Amazon CloudWatch

1. En la consola de AWS, busca **CloudWatch**.
2. En **CloudWatch**, selecciona **Registros** y busca el grupo de registros correspondiente a tu función Lambda.
3. Revisa los logs para verificar los detalles de la ejecución, como la obtención del secreto desde **Secrets Manager** y la respuesta de la API pública.

Adjunto estará el CSV donde se ven los logs.