

Santiago Hernández Ramos

Gestión de Bases de Datos

Configuración de una cuenta de AWS

Introducción

En este ejercicio práctico el alumno deberá configurar la cuenta de Amazon Web Services que se utilizará a lo largo de esta asignatura y de la siguiente.

Para ello, el alumno deberá completar todas las secciones que se indican en el enunciado.

El entregable para este ejercicio debe consistir en un informe técnico en el que se muestre mediante capturas de pantalla el resultado final de la configuración de cada uno de los apartados numerados a continuación.

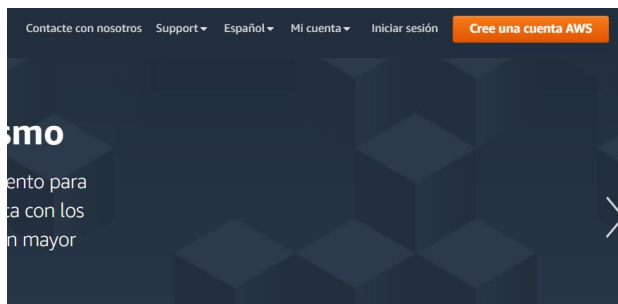
IMPORTANTE: El desarrollo de este ejercicio es imprescindible para poder completar los siguientes ejercicios de este módulo y del siguiente.

IMPORTANTE: El alumno será responsable de la gestión y eliminación de la cuenta de AWS.

Enunciado

1. Creación de la cuenta de AWS

Accedemos a <https://aws.amazon.com/es/> y pulsamos sobre “Cree una cuenta de AWS”



Completamos el formulario de registro. Asegúrate de elegir el tipo de cuenta personal y el *support plan* gratuito.

Explore los productos de la capa gratuita con una cuenta de AWS nueva.

Para obtener más información, visite aws.amazon.com/free.



Registrarse en AWS

Dirección de correo electrónico

Utilizará esta dirección de correo electrónico para iniciar sesión en su nueva cuenta de AWS.

Contraseña

Confirmar la contraseña

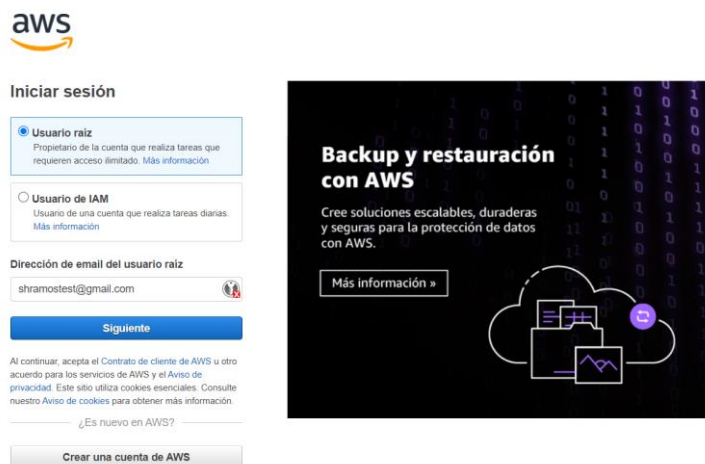
Nombre de la cuenta de AWS

Elija un nombre para la cuenta. Podrá cambiarlo en la configuración de la cuenta después de registrarse.

Continuar (paso 1 de 5)

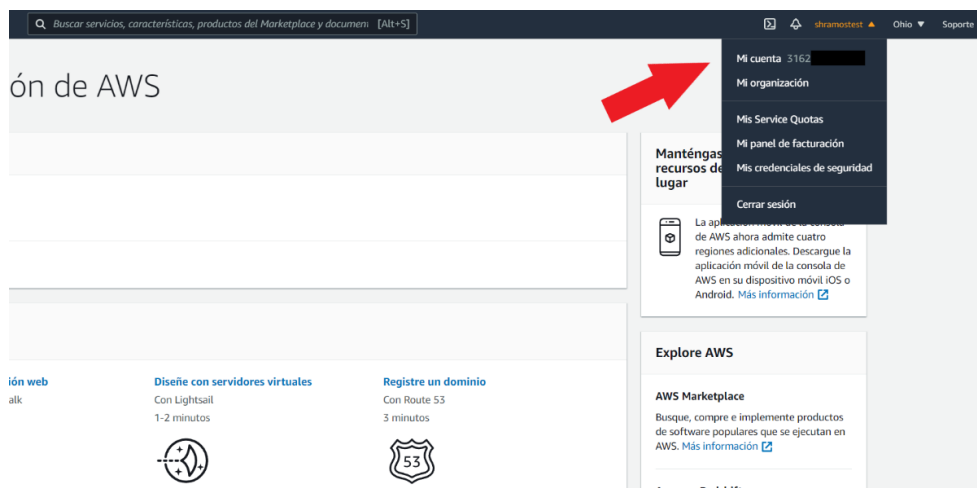
[Iniciar sesión en una cuenta de AWS existente](#)

Una vez completado el registro, accedemos a nuestra cuenta introduciendo el correo electrónico y la contraseña en el formulario de login.



The image shows the AWS login interface. On the left is the 'Iniciar sesión' (Sign in) form. It has two radio buttons: 'Usuario raíz' (Root user) and 'Usuario de IAM' (IAM user). Below these is a text field for the email address, which contains 'shramostest@gmail.com'. A 'Siguiendo' (Next) button is below the email field. At the bottom of the form is a link '¿Es nuevo en AWS?' and a button 'Crear una cuenta de AWS'. To the right of the form is a promotional banner for 'Backup y restauración con AWS' (Backup and restoration with AWS). The banner has a dark background with binary code and a cloud icon. It says 'Cree soluciones escalables, duraderas y seguras para la protección de datos con AWS.' and has a 'Más información' (More information) button.

La interfaz que se muestra inmediatamente después de realizar el *login* se corresponde con la consola de administración de AWS. En la esquina superior derecha podemos acceder a los detalles de nuestra cuenta y a nuestro número de cuenta, que utilizaremos más adelante para acceder a la consola de administración.



Por defecto, el acceso a la información económica solo está disponible únicamente para el usuario root.

Es una buena práctica restringir el uso de la cuenta root únicamente a operaciones críticas, por lo tanto, vamos a permitir el acceso a la actividad económica utilizando una política de IAM.

Para ello, pulsamos en **“Mi cuenta”** y hacemos *scroll* hacia abajo hasta llegar al apartado que se muestra a continuación.

▼ Acceso de los usuarios y los roles de IAM a la información de facturación

[Editar](#)

Utilice la configuración de **Active el acceso de IAM** para permitir a los usuarios y roles de IAM obtener acceso a las páginas de la consola de administración de costos y facturación. Esta configuración por sí sola no otorga a los usuarios y roles de IAM los permisos necesarios para estas páginas de la consola. Además de activar el acceso de IAM, también debe asociar las políticas de IAM necesarias a esos usuarios o roles. Para obtener más información, consulte [Conceder acceso a las herramientas e información de facturación](#).

Si esta configuración está desactivada, los usuarios y roles IAM de esta cuenta no podrán acceder a las páginas de la consola de administración de costos y facturación, incluso si tienen acceso de administrador o las políticas IAM requeridas.

La configuración de **Active el acceso de IAM** no controla el acceso a:

- Las páginas de la consola correspondientes a la detección de anomalías en los costos de AWS, la información general de los Savings Plans, el inventario de Savings Plans, la compra de Savings Plans y el carrito de Savings Plans
- La visualización de la administración de costos en la AWS Console Mobile Application
- Las APIs del SDK de administración de costos y facturación (API de AWS Cost Explorer, AWS Budgets y AWS Cost and Usage Report)

El acceso de los usuarios o los roles de IAM a la información de facturación está desactivado.

Pulsamos en **“Editar”** y marcamos la casilla **“Active el acceso de IAM”** y pulsamos sobre **“Actualizar”**

▼ Acceso de los usuarios y los roles de IAM a la información de facturación

Utilice la configuración de **Active el acceso de IAM** para permitir a los usuarios y roles de IAM obtener acceso a las páginas de la consola de administración de costos y facturación. Esta configuración por sí sola no otorga a los usuarios y roles de IAM los permisos necesarios para estas páginas de la consola. Además de activar el acceso de IAM, también debe asociar las políticas de IAM necesarias a esos usuarios o roles. Para obtener más información, consulte [Conceder acceso a las herramientas e información de facturación](#).

Si esta configuración está desactivada, los usuarios y roles IAM de esta cuenta no podrán acceder a las páginas de la consola de administración de costos y facturación, incluso si tienen acceso de administrador o las políticas IAM requeridas.

La configuración de **Active el acceso de IAM** no controla el acceso a:

- Las páginas de la consola correspondientes a la detección de anomalías en los costos de AWS, la información general de los Savings Plans, el inventario de Savings Plans, la compra de Savings Plans y el carrito de Savings Plans
- La visualización de la administración de costos en la AWS Console Mobile Application
- Las APIs del SDK de administración de costos y facturación (API de AWS Cost Explorer, AWS Budgets y AWS Cost and Usage Report)

☒ **Active el acceso de IAM**

Actualizar

Cancelar

Importante: En la parte inferior de la página tienes las opciones para cerrar tu cuenta de AWS en el caso de que no quieras seguir utilizándola después de las clases y quieras asegurarte de que no se realizan cobros a tu cuenta.

▼ Cerrar la cuenta

☐ Comprendo que, si hago clic en esta casilla, cerraré mi cuenta de AWS. Esto le indica a AWS mi voluntad de terminar el acuerdo de cliente o cualquier otro acuerdo con AWS que rija mi cuenta, únicamente con respecto a esa cuenta de AWS.

El uso mensual de determinados servicios de AWS se calcula y factura al principio del mes siguiente. Si he utilizado estos tipos de servicio durante un mes, al principio del mes siguiente recibiré una factura por el uso realizado antes de la terminación de mi cuenta. Además, si poseo suscripciones activas (como una instancia reservada que opté por pagar en cuotas mensuales), incluso después de haber cerrado mi cuenta, es posible que se siga facturando la suscripción hasta que esta caduque o se venda de acuerdo con las condiciones que la rigen.

Reconozco que tengo la posibilidad de volver a abrir mi cuenta de AWS únicamente dentro de los 90 días posteriores al cierre (“Período de poscierre”). Si vuelvo a abrirla durante el Período de poscierre, es posible que se me cobre por los servicios de AWS que no hayan terminado antes de cerrar la cuenta. Si vuelvo a abrir la cuenta de AWS, acepto que se apliquen los mismos términos para regir el acceso a los servicios de AWS y su uso mediante esta cuenta de AWS.

Si decido no volver a abrir la cuenta de AWS después del Período de poscierre, se eliminará cualquier contenido que quede en ella. Para obtener más información, consulte la [página Cierre de cuentas de Amazon Web Services](#).

☐ Comprendo que, una vez pasado el Período de poscierre, ya no podré volver a abrir la cuenta cerrada.

☐ Comprendo que, una vez pasado el Período de poscierre, ya no podré acceder a la consola de facturación para descargar las facturas anteriores y las facturas de impuestos. Si desea descargar alguna de las declaraciones, puede hacerlo aquí. Seleccione el mes y amplíe la sección del resumen para descargar los documentos relativos a los pagos de impuestos o las facturas.

☐ Comprendo que, una vez pasado el Período de poscierre, ya no podré crear una nueva cuenta de AWS con la dirección de email asociada actualmente a esta cuenta.

Si desea actualizar su dirección de email, siga las instrucciones que aparecen aquí.

Cerrar la cuenta

2. Seguridad de la cuenta de AWS

Vamos a continuar con la seguridad de nuestra cuenta de AWS y para ello, vamos a comenzar realizando algunos cambios sobre el servicio *IAM (Identity and Access Management)*

En la barra de búsqueda escribimos **“IAM”** y pulsamos sobre el servicio.



Lo primero que vemos al acceder al panel de IAM es una alerta de seguridad que nos indica que no tenemos activado el múltiple factor de autenticación (MFA). Pulsamos sobre **“Agregar MFA”**.

Panel de IAM

Recomendaciones de seguridad 1

- ⚠ Agregar MFA para el usuario raíz**
Habilite la autenticación multifactor (MFA) para el usuario raíz para mejorar la seguridad de esta cuenta.
- ✅ El usuario raíz no tiene claves de acceso activas**
El uso de claves de acceso asociadas a un usuario de IAM en lugar del usuario raíz mejora la seguridad.

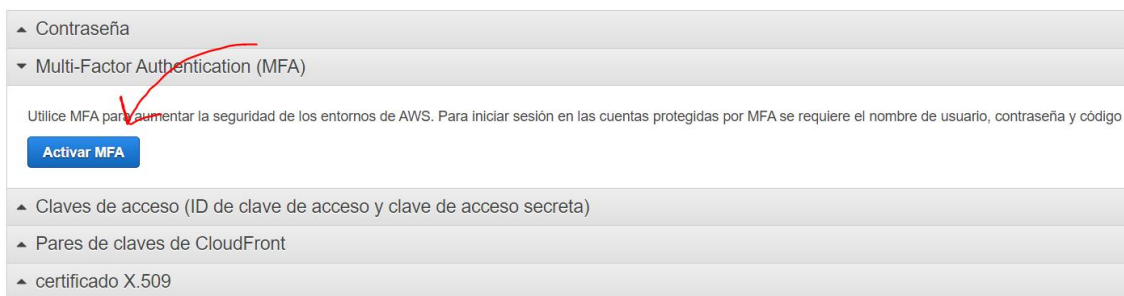
[Agregar MFA](#)

Recursos de IAM

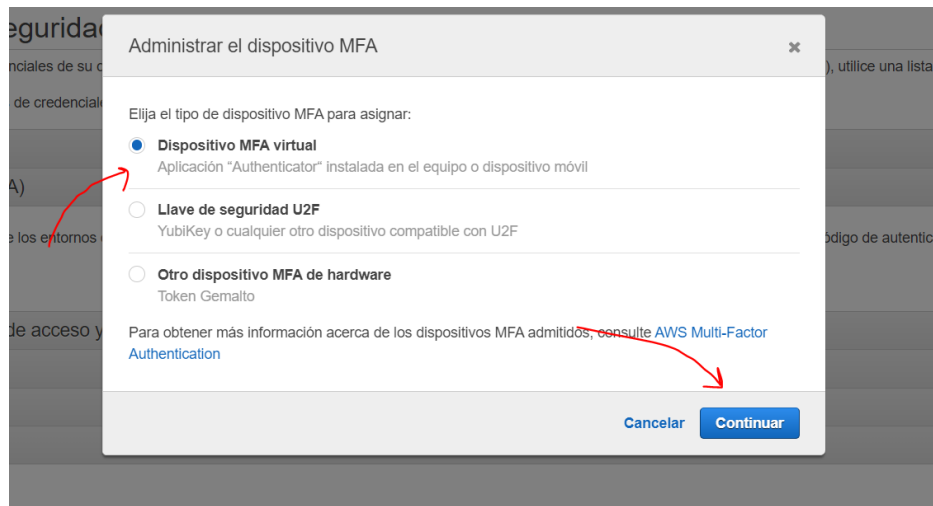
Grupos de usuarios	Usuarios	Roles	Políticas	Proveedores de identidad
0	0	2	0	0

[Novedades](#)

En la ventana que aparece, pulsamos sobre **“Activar MFA”**



Como podemos observar, AWS soporta diferentes tipos de autenticación de múltiple factor, en nuestro caso seleccionamos **“Dispositivo MFA virtual”** y pulsamos en **“continuar”**



Utiliza una aplicación de autenticación para leer el QR que se muestra en pantalla. Entre las aplicaciones más conocidas para soportar este tipo de MFA se encuentran: *Google Authenticator* y *Microsoft Authenticator*.

Tras leer el código QR automáticamente debería aparecer un código en la aplicación que debemos introducir en los cuadros de texto.

A screenshot of a web form for MFA verification. At the top, there is a text input field. Below it, the text "También puede escribir la clave secreta. [Mostrar la clave secreta](#)" is displayed. Below this is a section header "3. Escriba dos códigos de MFA consecutivos a continuación". Under this header, there are two rows. The first row is labeled "Código de MFA 1" and has a text input field. The second row is labeled "Código de MFA 2" and also has a text input field.

Tras introducir los dos códigos OTP (*One Time Password*) debería mostrarse un mensaje indicando que nuestra cuenta tiene el MFA configurado.

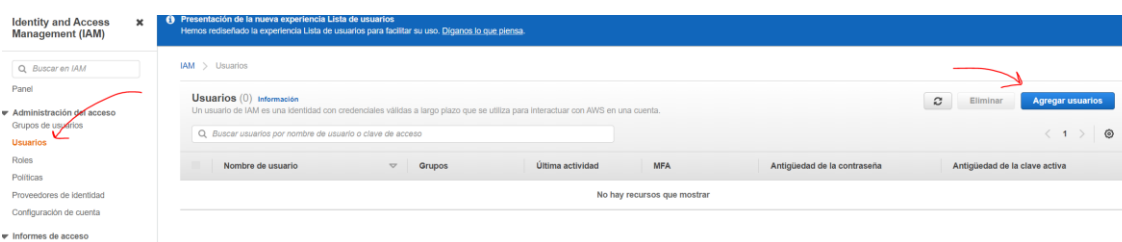


3. Creación de un usuario de AWS

Tal y como se comentaba anteriormente, la cuenta root solo debe utilizarse para actividades críticas, esto es debido a que tiene privilegios para realizar cualquier tipo de acción sobre la cuenta de AWS.

Para evitar utilizar la cuenta de root para nuestra actividad diaria, vamos a crear otro usuario dentro de nuestro entorno de AWS con el que accederemos habitualmente.

Para ello, dentro del panel de IAM pulsamos sobre usuarios y después sobre **“Agregar usuarios”**.



Introducimos un nombre para el usuario, por ejemplo, **“TESTUSER”** y activamos la opción **“Contraseña: acceso a la consola de administración de AWS”** y **“Contraseña personalizada”**.

Introducimos una contraseña robusta y desactivamos la opción **“Requerir el restablecimiento de contraseña”**. Pulsamos en **“Siguiente: Permisos”**

Establecer los detalles del usuario

Puede añadir varios usuarios a la vez con los mismos permisos y el mismo tipo de acceso. [Más información](#)

Nombre de usuario*

[+ Añadir otro usuario](#)

Seleccionar el tipo de acceso de AWS

Seleccione cómo estos usuarios accederán principalmente a AWS. Si elige únicamente el acceso mediante programación, NO evitará que los usuarios accedan a la consola por medio de un rol asumido. Las claves de acceso y las contraseñas generadas automáticamente se proporcionan en el último paso. [Más información](#)

- Seleccione el tipo de credenciales de AWS*
- ☐ **Clave de acceso: acceso mediante programación**
Habilita una **ID de clave de acceso** y una **clave de acceso secreta** para el SDK, la CLI y la API de AWS, además de otras herramientas de desarrollo.
 - ☒ **Contraseña: acceso a la consola de administración de AWS**
Habilita una **contraseña** que permite a los usuarios iniciar sesión en la consola de administración de AWS.

Contraseña de la consola*


- ☐ Contraseña generada automáticamente
- ☒ Contraseña personalizada

☐ Mostrar contraseña


Requerir el restablecimiento de contraseña ☐ El usuario debe crear una contraseña nueva en el próximo inicio de sesión
Los usuarios obtienen automáticamente la política [IAMUserChangePassword](#) que les permite cambiar su propia contraseña.

En la nueva pantalla que aparece, pulsamos sobre **“Crear un grupo”**.


▼ Establecer permisos



Añadir un usuario al grupo



Copiar permisos de un usuario existente



Asociar directamente las políticas existentes

Introducción a los grupos

Aún no ha creado ningún grupo. El uso de grupos es una práctica recomendada para administrar los permisos de los usuarios por funciones de trabajo, el acceso a los servicios de AWS o sus permisos personalizados. Empezar por crear un grupo. [Más información](#)

Crear un grupo

Introducimos un nombre para el grupo, por ejemplo **“Console-Admin”** y seleccionamos el permiso **“AdministratorAccess”**. Pulsamos sobre **“Crear un grupo”**.

Crear un grupo

Crear un grupo y seleccione las políticas que desea asociar a este. El uso de grupos es una práctica recomendada para administrar los permisos de los usuarios por funciones de trabajo, el acceso a los servicios de AWS o sus permisos personalizados. [Más información](#)

Nombre de grupo:

Crear una política **Actualizar**

Filtros: políticas

Nombre de la política	Tipo	Utilizado como	Descripción
<input checked="" type="checkbox"/> AdministratorAccess	Función de trabajo	Ninguna	Provides full access to AWS services and resources.
<input type="checkbox"/> AdministratorAccess-Amplify	Administrado por AWS	Ninguna	Grants account administrative permissions while explicitly allowing direct access to resources needed by Amplify applications.
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	Administrado por AWS	Ninguna	Grants account administrative permissions. Explicitly allows developers and administrators to gain direct access to resources they n...
<input type="checkbox"/> AlexaForBusinessDeviceSetup	Administrado por AWS	Ninguna	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/> AlexaForBusinessFullAccess	Administrado por AWS	Ninguna	Grants full access to AlexaForBusiness resources and access to related AWS Services
<input type="checkbox"/> AlexaForBusinessGatewayExecution	Administrado por AWS	Ninguna	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/> AlexaForBusinessLifesizeDelegatedAccessPolicy	Administrado por AWS	Ninguna	Provide access to Lifesize AWS devices
<input type="checkbox"/> AlexaForBusinessPolyDelegatedAccessPolicy	Administrado por AWS	Ninguna	Provide access to Poly A/Vs devices
<input type="checkbox"/> AlexaForBusinessReadOnlyAccess	Administrado por AWS	Ninguna	Provide read only access to AlexaForBusiness services
<input type="checkbox"/> AmazonAPIGatewayAdministrate...	Administración por AWS	Ninguna	Provides full access to create/delete APIs in Amazon API Gateway via the AWS Management Console

Cancelar **Crear un grupo**

Asegúrate de que **“Console-Admin”** esta seleccionado y pulsa sobre **“Siguiente: Etiquetas”**

Añadir un usuario al grupo

Crear un grupo Actualizar

Buscar Mostrando 1 resultado

Grupo	Políticas asociadas
<input checked="" type="checkbox"/> Console-Admin	AdministratorAccess

Establecer un límite de permisos

Cancelar Anterior **Siguiente: Etiquetas**

Pulsamos **“Siguiente: Revisar”** sin añadir ninguna etiqueta. Finalmente, revisamos que todos los datos son correctos y pulsamos sobre **“Crear un usuario”**.

Revisar

Revise las opciones que ha elegido. Después de crear el usuario, puede ver y descargar la contraseña y la clave de acceso generadas automáticamente.

Detalles del usuario

Nombre de usuario	TESTUSER
Tipo de acceso de AWS	Acceso a la consola de administración de AWS: con contraseña
Tipo de contraseña de la consola	Personalizado
Requerir el restablecimiento de contraseña	No
Límite de permisos	No se ha establecido un límite de permisos

Resumen de permisos

El usuario que se muestra más arriba se añadirá a los grupos siguientes.

Tipo	Nombre
Grupo	Console-Admin

Etiquetas

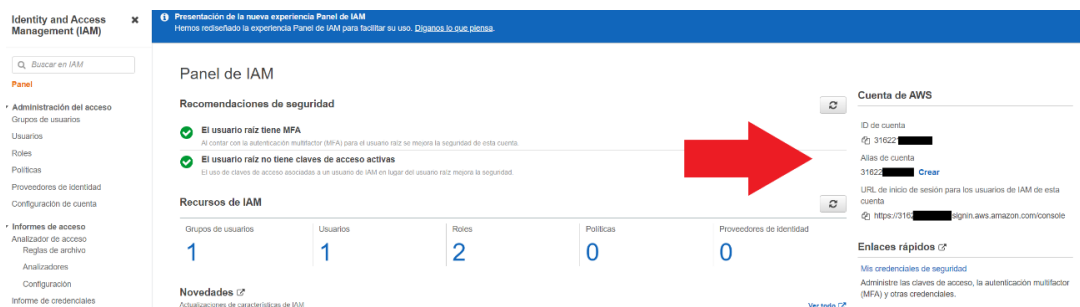
No se han añadido etiquetas.

Cancelar Anterior **Crear un usuario**

4. Alias para la cuenta de AWS

En lugar utilizar el ID de cuenta para acceder a la consola de administración de AWS, vamos a configurar un alias.

En el panel de IAM, pulsamos sobre **“Crear”** en la esquina superior derecha.



En el cuadro de texto introducimos un alias. El alias debe ser único, por ejemplo ***“testuser-[Iniciales de tu nombre]”***

Una vez hecho esto ya tenemos todo listo para comenzar. Cerramos sesión de la cuenta y volvemos a iniciar sesión.

En el inicio de sesión, seleccionamos **“Usuario de IAM”** e introducimos el alias de la cuenta.

Iniciar sesión

☐ **Usuario raíz**
 Propietario de la cuenta que realiza tareas que requieren acceso ilimitado. [Más información](#)

☒ **Usuario de IAM**
 Usuario de una cuenta que realiza tareas diarias. [Más información](#)

ID de cuenta (12 dígitos) o alias de cuenta

Siguiente

Al continuar, acepta el [Contrato de cliente de AWS](#) u otro acuerdo para los servicios de AWS y el [Aviso de privacidad](#). Este sitio utiliza cookies esenciales. Consulte nuestro [Aviso de cookies](#) para obtener más información.

¿Es nuevo en AWS?

Crear una cuenta de AWS

Después, introducimos el nombre de usuario (“**TESTUSER**”) y la contraseña que establecimos en los pasos anteriores y pulsamos sobre “**Iniciar Sesión**”.

Para terminar, podemos añadir MFA para la cuenta TESTUSER de la misma forma que hicimos para el usuario root.

The screenshot shows the 'Panel de IAM' (IAM Panel) interface. On the left is a sidebar with navigation links: 'Panel', 'Administración del acceso' (Groups of users, Users, Roles, Policies, Identity Providers, Account configuration), and 'Informes de acceso' (Access analyzer, Rules of access, Analyzers, Configuration, Credential report, Organization activity, Service control policies (SCP)).

The main content area has a blue header with a message: 'Presentación de la nueva experiencia Panel de IAM. Hemos rediseñado la experiencia Panel de IAM para facilitar su uso. Díganos lo que piensa.' Below this is the 'Panel de IAM' title and a 'Recomendaciones de seguridad' (Security recommendations) section with 1 item. The first recommendation is a green checkmark: 'El usuario raíz tiene MFA' (The root user has MFA), with a sub-note: 'Al contar con la autenticación multifactor (MFA) para el usuario raíz se mejora la seguridad de esta cuenta.' The second recommendation is a red warning triangle: 'Agregue MFA para usted' (Add MFA for you), with a sub-note: 'Agregue autenticación multifactor (MFA) para usted y mejore la seguridad de esta cuenta.' A red arrow points to the 'Agregar MFA' button next to this recommendation. The third recommendation is a green checkmark: 'El usuario TESTUSER no tiene claves de acceso activas que no hayan sido utilizadas durante más de un año.' (The TESTUSER user does not have active access keys that have not been used for more than a year), with a sub-note: 'La desactivación o la eliminación de claves de acceso no utilizadas mejora la seguridad.'

Below the recommendations is the 'Recursos de IAM' (IAM Resources) section, which displays a table of counts:

Grupos de usuarios	Usuarios	Roles	Políticas	Proveedores de identidad
1	1	2	0	0

At the bottom, there is a 'Novedades' (News) section with a link to 'Actualizaciones de características de IAM' (IAM feature updates) and a 'Ver todo' (View all) link.

