



## Integración AWS

<b>Control de versiones</b>	<b>2</b>
<b>Modelo de integración</b>	<b>3</b>
Autenticación y autorización (Oauth2)	3
Configuración de autenticación	3
Configuración de autorización	4
Gobierno activo	4
Nomenclatura de los grupos	5
<b>Credenciales requeridas</b>	<b>5</b>
Autenticación	5
Autorización (Oauth2)	9
Gobierno activo	11
<b>Emulación SSO vía Oauth2</b>	<b>11</b>

## Control de versiones

<b>Versión</b>	<b>Fecha de modificación</b>	<b>Responsable</b>	<b>Aprobador</b>	<b>Resumen de cambios</b>
1.0	22/11/2023	Anjana Producto	Anjana Producto	Creación del documento. Compatibilidad con la v4.5 de todos los módulos de Anjana

# Modelo de integración

## Autenticación y autorización (Oauth2)

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

### Configuración de autenticación

En la propiedad *security.authentication* se configuran los distintos proveedores de autenticación que se utilizan.

En el caso de AWS es necesario configurar las siguientes propiedades:

```
security:
  authentication:
    oidc:
      providers:
        aws:
          name: Anjana AWS
          authorize-url:
https://${security.authentication.oidc.providers.aws.domain}.auth.${security.authentication.oidc.providers.aws.region}.amazoncognito.com/login?response_type=code&client_id=${security.authentication.oidc.providers.aws.client-id}&redirect_uri=${security.authentication.oidc.providers.aws.redirect-uri}&state=STATE&scope=${security.authentication.oidc.providers.aws.scopes}
          authorize-url-portuno:
https://${security.authentication.oidc.providers.aws.domain}.auth.${security.authentication.oidc.providers.aws.region}.amazoncognito.com/login?response_type=code&client_id=${security.authentication.oidc.providers.aws.client-id}&redirect_uri=${security.authentication.oidc.providers.aws.redirect-uri-portuno}&state=STATE&scope=${security.authentication.oidc.providers.aws.scopes}
          token-url:
https://${security.authentication.oidc.providers.aws.domain}.auth.${security.authentication.oidc.providers.aws.region}.amazoncognito.com/oauth2/token
          scopes: openid+profile
          client-id: <client-id>
          client-secret: <client-secret>
          client-authentication-method: GET
          redirect-uri: https://url.anjanadata.com/anjana/authorized
```

```
    redirect-uri-portuno:
https://url.anjanadata.com/admin/authorized
    username-claim: cognito:username
    workflowType: AUTHORIZATION_CODE
    authorizeServer:
https://${security.authentication.oidc.providers.aws.domain}.auth.${security.authentication.oidc.providers.aws.region}.amazoncognito.com/oauth2/userInfo
    userNameProperty: username
    type: AWS
    region: eu-web-1
    domain: anjana-app-desarrollo
```

## Configuración de autorización

En la propiedad *security.authorization* se configuran los distintos proveedores de autorización que se utilizan.

En el caso de AWS es necesario configurar las siguientes propiedades:

```
security:
  authorization:
    oidc:
      providers:
        aws:
          providers:
            anjana-dev-app:
              poolID: eu-central-1_5oDfN6Jvv
              region: eu-central-1
              accessKey: <accessKey>
              secretKey: <secretKey>
              groupOrgUnitSeparator: "/"
              roleOrgUnitSeparator: "-"
              groupPrefix: "prefix-"
```

- *groupOrgUnitSeparator*: separador de partes de unidad organizativa en un grupo (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)  
En caso de configurar un separador distinto a '/', en el provider las OUs no se puede usar '/' como parte de un nombre de OU)
- *roleOrgUnitSeparator*: separador del rol del resto de la cadena en un grupo (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)
- *groupPrefix*: prefijo que contengan los grupos (nunca valor ""). Esta propiedad, por tanto, debe tener valor o no ser definida)

## Gobierno activo

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar elementos sobre AWS es “Tot plugin AWS IAM”.

## Nomenclatura de los grupos

El nombre del grupo debe contener el alias de la unidad organizativa y el rol que aplica a dicha unidad organizativa.

Un ejemplo de un nombre de un grupo sería : HQ/Legal-architect , donde HQ/Legal es el alias de la unidad organizativa y architect el rol<sup>1</sup>.

Como se puede observar hay dos separadores:

- El separador de jerarquía de la unidad organizativa: '/' , cuyo valor es configurable gracias a la propiedad del yml: roles.separator-organizational-unit.
- El separador de la unidad organizativa y el rol: '-' , cuyo valor es configurable gracias a la propiedad del yml: roles.separator-role.

## Credenciales requeridas

La credencial puede ser única aglutinando los permisos de ambas, pero se recomienda mantenerlas por separado de cara a facilitar la monitorización y auditoría de la actividad ejercida por las mismas.

## Autenticación

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

Es necesario registrar un grupo de usuarios en el servicio Amazon Cognito con las siguientes propiedades.

---

<sup>1</sup> Independientemente de los separadores usados en los repositorios de identidades el producto normalizará al formato estándar, por lo que en la configuración del producto ha de usarse siempre los separadores “/” y “-” para conformar el alias, por ejemplo “UO/UO..../UO-role”.



The screenshot shows the Amazon Cognito service page. At the top, there is a navigation bar with the AWS logo, a search bar containing the text "Buscar servicios, características, productos del", and a dropdown menu for "Irlanda". Below the navigation bar, the Cognito logo is centered, followed by the heading "Amazon Cognito". A paragraph of text explains that Amazon Cognito offers user and identity groups. Below this text are two blue buttons: "Administrar grupos de usuarios" and "Administrar grupos de identidades". The page is divided into two columns. The left column features an icon of two people with a plus sign, the heading "Añadir la funcionalidad de inscripción e inicio de sesión", and a short paragraph. The right column features an icon of a computer monitor with a lock, the heading "Conceda acceso a sus usuarios a los servicios de AWS", and a short paragraph.

aws Servicios  [Alt+S] Irlanda Soporte

## Amazon Cognito

Amazon Cognito ofrece grupos de usuarios y de identidades. Los grupos de usuarios son directorios de usuarios que proporcionan a los usuarios de las aplicaciones opciones para inscribirse e iniciar sesión. Los grupos de identidades proporcionan las credenciales de AWS para conceder a los usuarios acceso a otros servicios de AWS.

[Administrar grupos de usuarios](#) [Administrar grupos de identidades](#)



### Añadir la funcionalidad de inscripción e inicio de sesión

Los grupos de usuarios de Cognito le permiten añadir de forma fácil y segura la funcionalidad de inscripción e inicio de sesión a sus



### Conceda acceso a sus usuarios a los servicios de AWS

Los grupos de identidades de Cognito permiten que su aplicación obtenga credenciales temporales para que usuarios invitados anónimo

En el apartado “Clientes de aplicación” se obtienen las credenciales que más tarde hay que indicar en la configuración de Zeus.

aws Servicios  [Alt+S] Soporte

Grupos de usuarios | Identidades federadas

## anjana-app-desarrollo

Configuración general

- Usuarios y grupos
- Atributos
- Políticas
- MFA y verificaciones
- Seguridad avanzada
- Personalizaciones de mensaje
- Etiquetas
- Dispositivos
- Clientes de aplicación
- Desencadenadores
- Análisis

Integración de aplicaciones

- Configuración del cliente de aplicación
- Nombre del dominio
- Personalización de la interfaz de usuario
- Servidores de recursos

Federación

- Proveedores de identidades
- Mapeo de atributos

### ¿Qué clientes de aplicación tendrán acceso a este grupo de usuarios?

Los clientes de aplicación que añada recibirán un ID único y una clave secreta opcional para obtener acceso a este grupo de usuarios.

**ID de cliente de aplicación**

**Clave secreta de cliente de aplicación**

**Actualizar el vencimiento del token**

días y  minutos

*Deben estar comprendidos entre 60 minutos y 3650 días*

**Vencimiento del token de acceso**

días y  minutos

*Deben estar comprendidos entre 5 minutos y 1 día. No pueden ser mayores que el vencimiento del token de actualización.*

### How do you want your end users to sign in?

You can choose to have users sign in with an email address, phone number, username or preferred username plus their password. [Learn more.](#)

**Username** - Users can use a username and optionally multiple alternatives to sign up and sign in.

- Also allow sign in with verified email address
- Also allow sign in with verified phone number
- Also allow sign in with preferred username (a username that your users can change)

**Email address or phone number** - Users can use an email address or phone number as their "username" to sign up and sign in.

- Allow email addresses
- Allow phone numbers
- Allow both email addresses and phone numbers (users can choose one)

You can choose to enable case insensitivity on the username input for the selected sign-in option. For example, when this option is selected, the users can sign in using either "username" or "Username".

(Recommended) Enable case insensitivity for username input

### Which standard attributes do you want to require?

All of the standard attributes can be used for user profiles, but the attributes you select will be required for sign up. You will not be able to change these requirements after the pool is created. If you select an attribute to be an alias, users will be able to sign-in using that value or their username. [Learn more about attributes.](#)

Required	Attribute	Required	Attribute
<input type="checkbox"/>	address	<input type="checkbox"/>	nickname
<input type="checkbox"/>	birthdate	<input type="checkbox"/>	phone number
<input checked="" type="checkbox"/>	email	<input type="checkbox"/>	picture
<input type="checkbox"/>	family name	<input type="checkbox"/>	preferred username
<input type="checkbox"/>	gender	<input type="checkbox"/>	profile
<input type="checkbox"/>	given name	<input type="checkbox"/>	zoneinfo
<input type="checkbox"/>	locale	<input type="checkbox"/>	updated at
<input type="checkbox"/>	middle name	<input type="checkbox"/>	website
<input type="checkbox"/>	name		

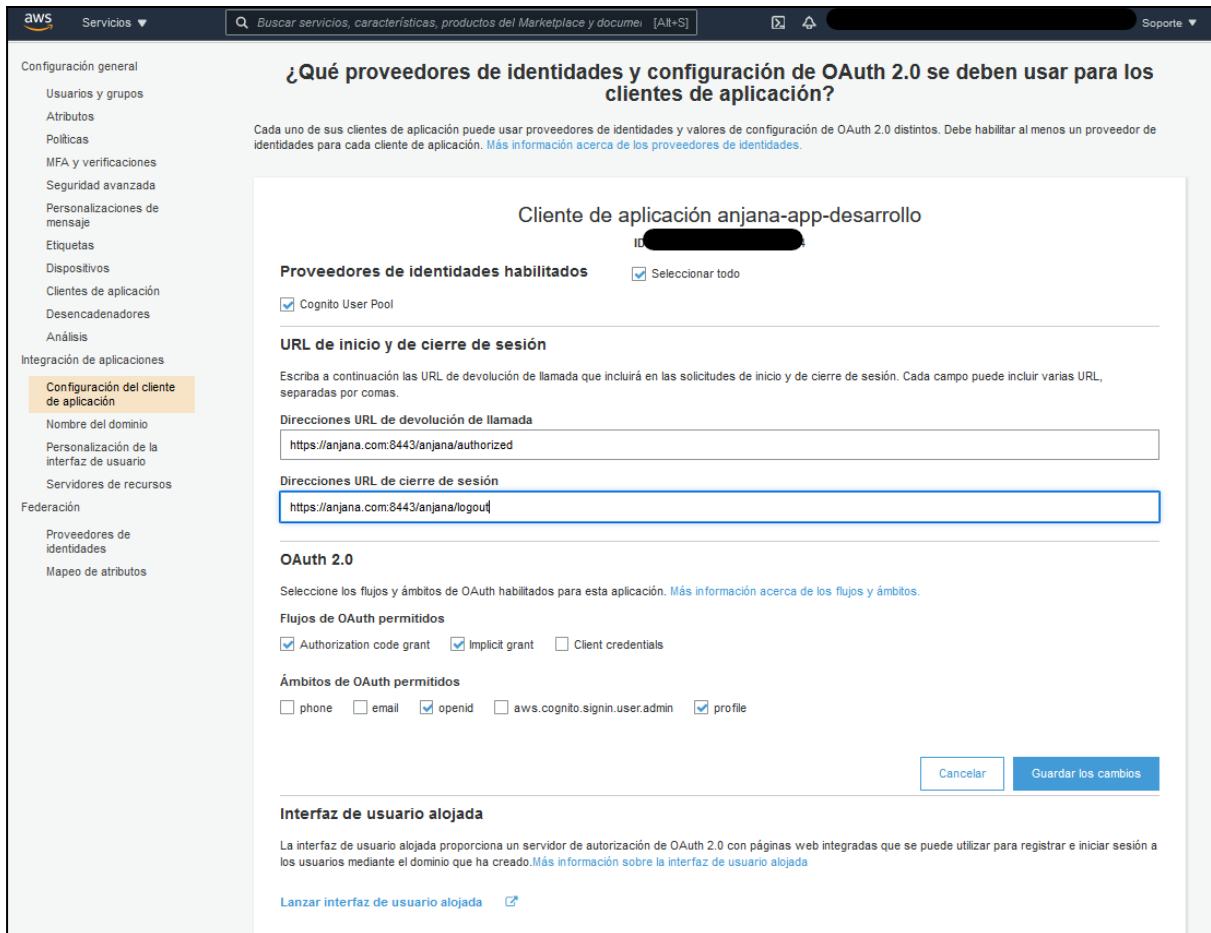
### Do you want to add custom attributes?

Enter the name and select the type and settings for custom attributes.



En el apartado “Configuración del cliente de aplicación” se configuran las url acorde al nombre de dominio que enrute hasta el frontal de Anjana Data, es necesario dar de alta:

- https://<host>:<port>/anjana/authorized
- https://<host>:<port>/anjana/login
- https://<host>:<port>/anjana/logout



**¿Qué proveedores de identidades y configuración de OAuth 2.0 se deben usar para los clientes de aplicación?**

Cada uno de sus clientes de aplicación puede usar proveedores de identidades y valores de configuración de OAuth 2.0 distintos. Debe habilitar al menos un proveedor de identidades para cada cliente de aplicación. [Más información acerca de los proveedores de identidades.](#)

**Cliente de aplicación anjana-app-desarrollo**

**Proveedores de identidades habilitados**  Seleccionar todo

Cognito User Pool

**URL de inicio y de cierre de sesión**

Escriba a continuación las URL de devolución de llamada que incluirá en las solicitudes de inicio y de cierre de sesión. Cada campo puede incluir varias URL, separadas por comas.

**Direcciones URL de devolución de llamada**

**Direcciones URL de cierre de sesión**

**OAuth 2.0**

Seleccione los flujos y ámbitos de OAuth habilitados para esta aplicación. [Más información acerca de los flujos y ámbitos.](#)

**Flujos de OAuth permitidos**

Authorization code grant  Implicit grant  Client credentials

**Ámbitos de OAuth permitidos**

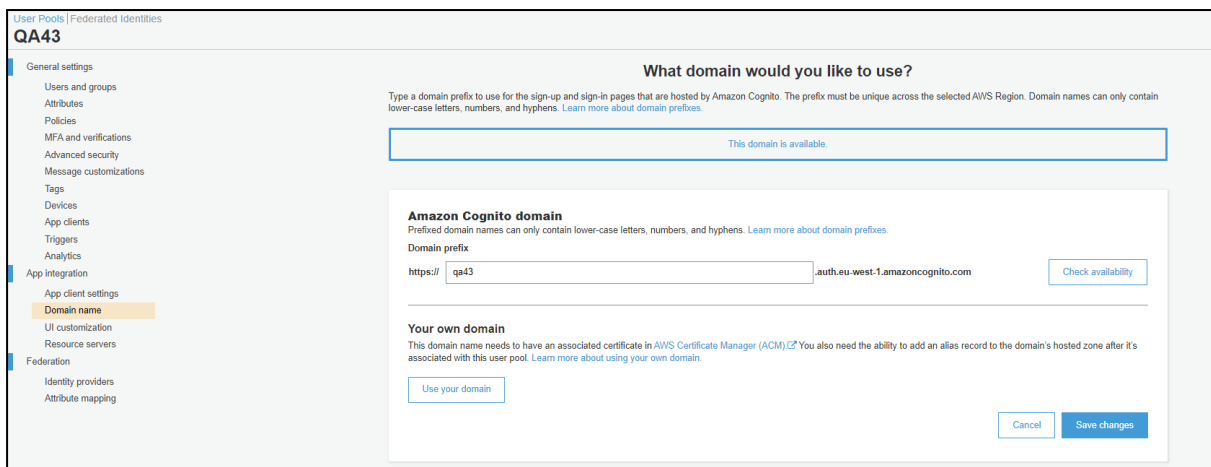
phone  email  openid  aws.cognito.signin.user.admin  profile

**Interfaz de usuario alojada**

La interfaz de usuario alojada proporciona un servidor de autorización de OAuth 2.0 con páginas web integradas que se puede utilizar para registrar e iniciar sesión a los usuarios mediante el dominio que ha creado. [Más información sobre la interfaz de usuario alojada](#)

[Lanzar interfaz de usuario alojada](#)

También, en el apartado de nombre del dominio se debe rellenar el nombre del pool, en minúsculas.



**QA43**

**What domain would you like to use?**

Type a domain prefix to use for the sign-up and sign-in pages that are hosted by Amazon Cognito. The prefix must be unique across the selected AWS Region. Domain names can only contain lower-case letters, numbers, and hyphens. [Learn more about domain prefixes.](#)

**Amazon Cognito domain**

Prefixed domain names can only contain lower-case letters, numbers, and hyphens. [Learn more about domain prefixes.](#)

Domain prefix  
 https://  .auth.eu-west-1.amazoncognito.com

**Your own domain**

This domain name needs to have an associated certificate in [AWS Certificate Manager \(ACM\)](#). You also need the ability to add an alias record to the domain's hosted zone after it's associated with this user pool. [Learn more about using your own domain.](#)

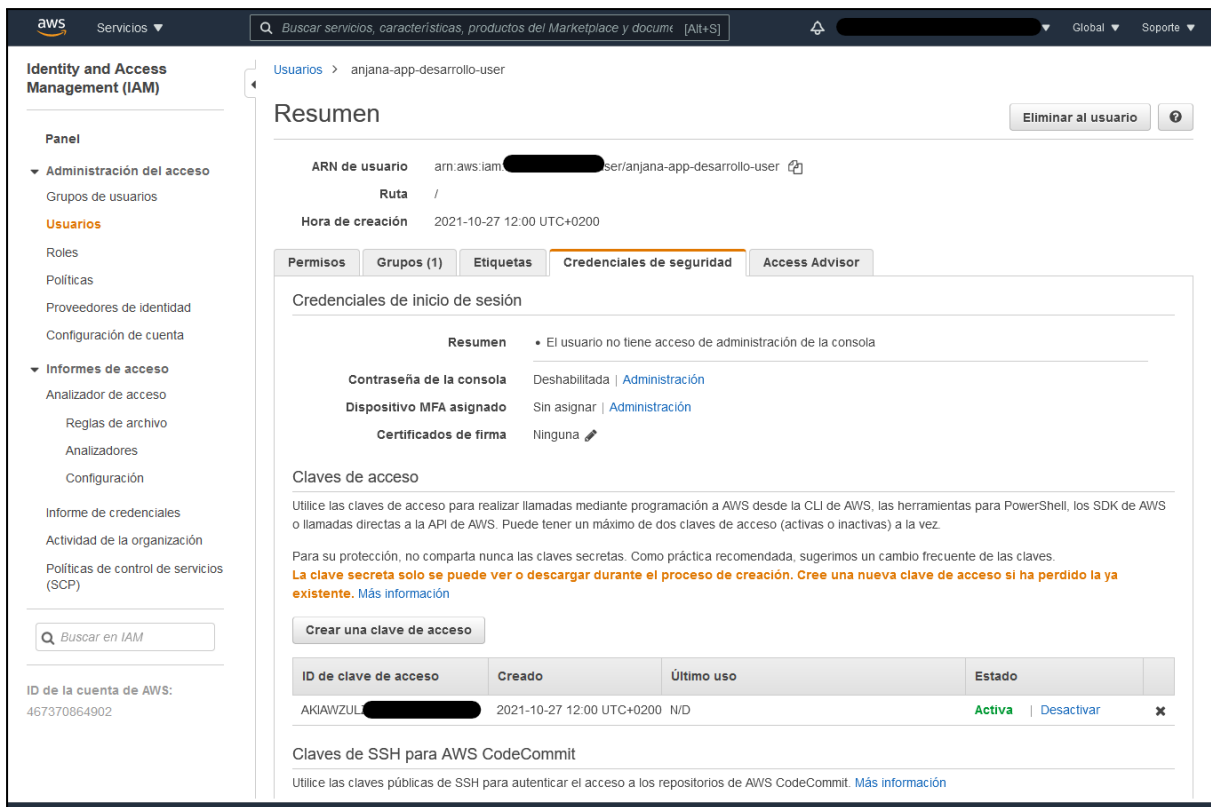
## Autorización (Oauth2)

La funcionalidad está directamente embebida en el microservicio de gestión de autenticación y autorización Zeus, se habilita y configura mediante el fichero de configuración de dicho microservicio.

En el servicio de Cognito User Pools de Amazon son necesarios los siguientes permisos AdminListGroupForUser, AdminGetUser, ListUsers, listGroups y ListUsersInGroup.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "cognito-idp:ListUsersInGroup",
        "cognito-idp:ListGroups",
        "cognito-idp:AdminListGroupForUser",
        "cognito-idp:AdminGetUser",
        "cognito-idp:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

En la configuración de Zeus para autorización se indican las credenciales creadas en el apartado de “Credenciales de seguridad” de la ficha del usuario.



**Resumen**

ARN de usuario: `arn:aws:iam::[redacted]:user/anjana-app-desarrollo-user`

Ruta: `/`

Hora de creación: 2021-10-27 12:00 UTC+0200

**Credenciales de seguridad**

**Credenciales de inicio de sesión**

**Resumen**

- El usuario no tiene acceso de administración de la consola

**Contraseña de la consola**: Deshabilitada | [Administración](#)

**Dispositivo MFA asignado**: Sin asignar | [Administración](#)

**Certificados de firma**: Ninguna [✎](#)

**Claves de acceso**

Utilice las claves de acceso para realizar llamadas mediante programación a AWS desde la CLI de AWS, las herramientas para PowerShell, los SDK de AWS o llamadas directas a la API de AWS. Puede tener un máximo de dos claves de acceso (activas o inactivas) a la vez.

Para su protección, no comparta nunca las claves secretas. Como práctica recomendada, sugerimos un cambio frecuente de las claves. **La clave secreta solo se puede ver o descargar durante el proceso de creación. Cree una nueva clave de acceso si ha perdido la ya existente.** [Más información](#)

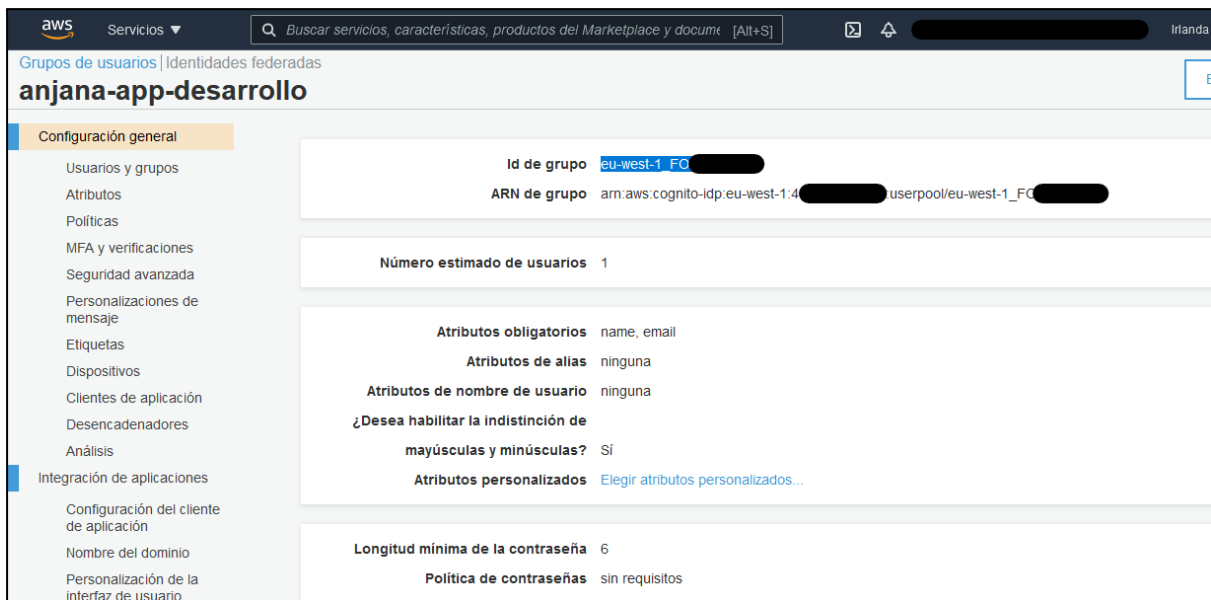
[Crear una clave de acceso](#)

ID de clave de acceso	Creado	Último uso	Estado
AKIAWZUL[redacted]	2021-10-27 12:00 UTC+0200	N/D	Activa   <a href="#">Desactivar</a>   <a href="#">✕</a>

**Claves de SSH para AWS CodeCommit**

Utilice las claves públicas de SSH para autenticar el acceso a los repositorios de AWS CodeCommit. [Más información](#)

El valor poolID se puede encontrar en el grupo de usuarios creado en Amazon Cognito.



**Configuración general**

**Id de grupo**: eu-west-1\_FC[redacted]

**ARN de grupo**: `arn:aws:cognito-idp:eu-west-1:4[redacted]:userpool/eu-west-1_FC[redacted]`

**Número estimado de usuarios**: 1

**Atributos obligatorios**: name, email

**Atributos de alias**: ninguna

**Atributos de nombre de usuario**: ninguna

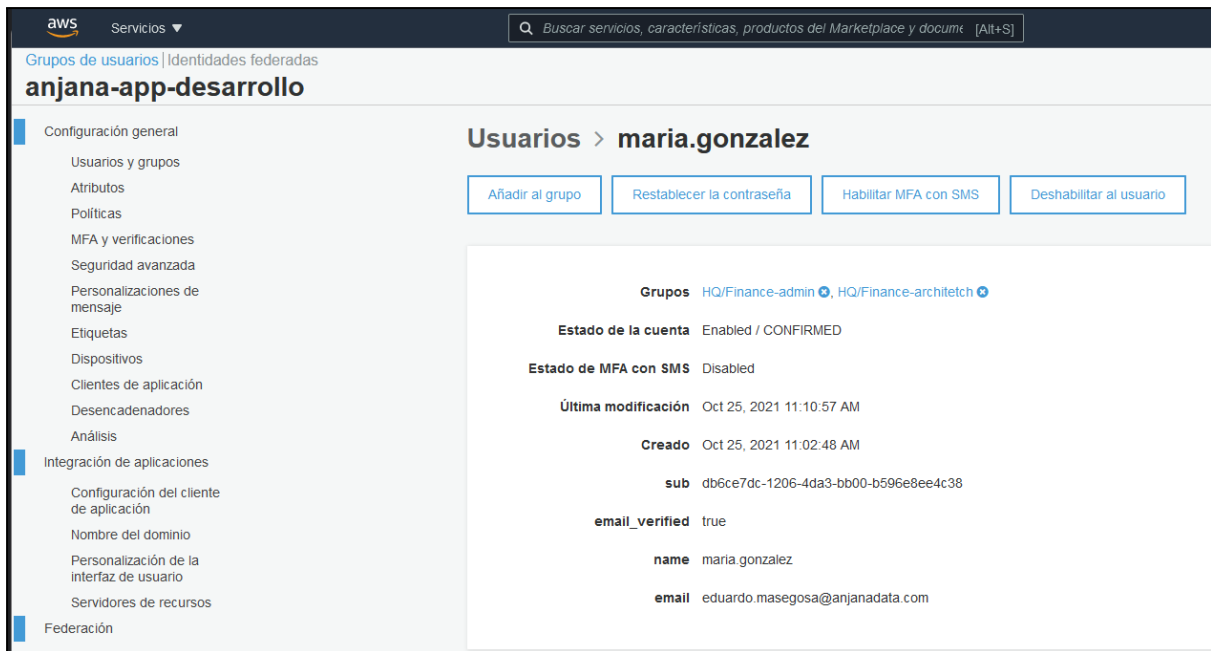
**¿Desea habilitar la indistinción de mayúsculas y minúsculas?**: Sí

**Atributos personalizados**: [Elegir atributos personalizados...](#)

**Longitud mínima de la contraseña**: 6

**Política de contraseñas**: sin requisitos

El usuario y sus membresías deben darse en el grupo de usuarios creado en Cognito.



The screenshot shows the AWS IAM console interface. At the top, there's a search bar and the text "Grupos de usuarios | Identidades federadas". Below that, the page title is "anjana-app-desarrollo". On the left, there's a navigation menu with categories like "Configuración general", "Integración de aplicaciones", and "Federación". The main content area is titled "Usuarios > maria.gonzalez". It features four action buttons: "Añadir al grupo", "Restablecer la contraseña", "Habilitar MFA con SMS", and "Deshabilitar al usuario". Below these buttons, the user's details are displayed in a structured format:

- Grupos:** HQ/Finance-admin, HQ/Finance-architect
- Estado de la cuenta:** Enabled / CONFIRMED
- Estado de MFA con SMS:** Disabled
- Última modificación:** Oct 25, 2021 11:10:57 AM
- Creado:** Oct 25, 2021 11:02:48 AM
- sub:** db6ce7dc-1206-4da3-bb00-b596e8ee4c38
- email\_verified:** true
- name:** maria.gonzalez
- email:** eduardo.masegosa@anjanadata.com

## Gobierno activo

El plugin a desplegar el cual realizará la parte de las tareas de gobierno activo que tengan que provisionar elementos sobre AWS es "Tot plugin AWS IAM", en su documentación queda descrita la credencial requerida.

## Emulación SSO vía Oauth2

El protocolo Oauth2 observa la autenticación transparente en caso de que sea posible, para lo cual solo es necesario redirigir al usuario a <https://<host>/anjana/login?provider=<identificador de provider en zeus>>, si el usuario ya está logado en dicho provider y las políticas configuradas en dicho provider hacen que no se requiera validar nuevamente la credencial, el usuario será autenticado en Anjana Data de forma totalmente transparente.