**Landing Zone de Control Tower**

**Pre-requisitos:**

* Definir la estructura de la organización que manejará Control Tower (OUs y cuentas)
* Control Tower requiere 2 correos únicos que no estén asociados a ninguna cuenta de AWS. Estos correos se asociarán a las cuentas de **Audit y Log Archive**, las cuales son mandatorias

**Pasos generales para desplegar el LZ de Control Tower**

1. Crear una cuenta de AWS y asociarla con la tarjeta de crédito
2. Acceder a la nueva cuenta y crear un usuario con permisos de administrador
3. Desde el nuevo usuario, ir a la interfaz de Control Tower y desplegar el Landing Zone, indicando las OUs adicionales que se necesitan agregar.

**Nota**: De forma mandatoria, Control Tower crea una OU llamada Security y dentro de éstas estarán dos cuentas: **Audit y Log Archive**; estos nombres se pueden modificar.

1. Personalizar el Landing Zone de Control Tower con IaC (Terraform u otro servicio), de acuerdo con el escenario del cliente:
   1. Crear las cuentas y OUs adicionales
   2. Crear la infraestructura de Networking en cada una de las cuentas
   3. En Control Tower, enrolar las cuentas y OUs creadas por Terraform: <https://docs.aws.amazon.com/controltower/latest/userguide/existing-orgs.html>

**Consideraciones generales**

* Control Tower no tiene posee ninguna API disponible o acceso programático
* La región en donde se encuentre la “consola” de Control Tower no puede cambiarse una vez configurada

**Referencias:**

<https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html>

<https://docs.aws.amazon.com/controltower/latest/userguide/setting-up.html>