CONTENIDO

[1. Objetivo 2](#_Toc8331)

[2. Alcance 2](#_Toc16812)

[3. Política 2](#_Toc11498)

[4. Elaboración y aprobación 3](#_Toc13884)

[5. Historial de cambios 3](#_Toc21584)

# Objetivo

Contar con una política general para el correcto seguimiento diario de las tareas requeridas para garantizar una disponibilidad del 99% 24/7 de la plataforma.

# Alcance

Abarca a todos los activos ubicados en proveedores de recursos en la nube como AWS y Digital Ocean.

# Política

* 1. Se deberá acceder todos los días a las 9:00 a.m. a la cuenta de AWS y verificar que el costo diario se encuentre entre los parámetros requeridos.
  2. Se deberá eliminar inmediatamente y reportar a AWS si se encontró algún recurso que no haya sido creado por el equipo de operación de la organización.
  3. Se deberá cambiar y actualizar en la bóveda de contraseñas, la contraseña se acceso a AWS si aplica el punto anterior.
  4. Se deberá acceder todos los días a las 9:30 a.m. a la cuenta de Digital Ocean y verificar que el costo diario se encuentra entre los parámetros requeridos.
  5. Se deberá eliminar inmediatamente y reportar a Digital Ocean si se encontró algún recurso que no haya sido creado por el equipo de operación de la organización.
  6. Se deberá cambiar y actualizar en la bóveda de contraseñas, la contraseña se acceso a Digital Ocean si aplica el punto anterior.
  7. Se deberá acceder vía SSH todos los días al Droplet en Digital Ocean llamado PRODUCTION-DATABASE y verificar que este aún tenga espacio disponible en disco duro.
  8. Se deberá acceder vía SSH al Droplet en Digital Ocean llamado PRODUCTION-DATABASE y verificar con el comando docker ps que esté se encuentre activo.
  9. En caso de que el servicio de base de datos no se encuentre activo, se deberá ejecutar el comando docker start mariadb1 para inicializar la base de datos.
  10. Se deberá acceder a todos los droplets o instancias en el transcurso del día y verificar que toda aplicación sea funcional, accediendo a ella a modo usuario y a modo servicio que en la mayoría de los casos es ejecutar el comando docker ps.
  11. Se deberá verificar diario que los VPN’s se encuentren con un tunel establecido y activo, esto se realiza utilizando el comando ipsec statusall
  12. Se deberán realizar respaldos en sitio siguiente la política de respaldo ubicada en el archivo TI - SGSI - 04 - Política de Respaldo.

# 4. Elaboración y aprobación

| **Nombre y Cargo** | **Fecha** | **Rol** |
| --- | --- | --- |
| Alfredo José Bolio Domínguez | 02/02/2022 | Elaboró y aprobó |

# 5. Historial de cambios

| **Revisión** | **Descripción del cambio** | **Responsable** | **Fecha** |
| --- | --- | --- | --- |
| 01 | Creación de documento | Alfredo José Bolio Domínguez | 02/02/2022 |