EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE MORELIA
"José María Morelos y Pavón"

INSTITUTO TECNOLÓGICO DE MORELIA

INGENIERÍA EN SISTEMAS COMPUTACIONALES

TALLER

DE

SISTEMAS OPERATIVOS

PROFESORA:

BRENDA GUADALUPE GONZALEZ MARTINEZ

MANTENIMIENTO

"Plan de mantenimiento"

ALEJOS SORIA SALVADOR

GRUPO: **"A"**

MORELIA, MICHOACÁN

FECHA DE ENTREGA: 13/10/2025

Contenido

Plan de mantenimiento servidor Ubuntu

1. Medidas de Seguridad Fundamentales (Configuración Inicial)

Estas acciones deben realizarse **una sola vez** durante la configuración inicial del servidor. Son la base sobre la que se construye todo lo demás.

- **Firewall de Nube (Cloud Firewall):** Antes de que el servidor reciba tráfico, configúralo en el panel de DigitalOcean. Es tu primera línea de defensa.
    - **Reglas de entrada:** Permite tráfico **solo** en los puertos estrictamente necesarios:
        - **SSH (Puerto 22):** Limítalo solo a tu dirección IP o la de tu oficina, no a todo el mundo.
        - **HTTP (Puerto 80):** Abierto a todo el mundo.
        - **HTTPS (Puerto 443):** Abierto a todo el mundo.
    - **Reglas de salida:** Generalmente se pueden dejar abiertas para que el servidor pueda descargar actualizaciones.
- **Configuración del Servidor (Ubuntu):**
    - **No usar el usuario root:** Crea un usuario administrador con privilegios sudo y deshabilita el login de root por SSH.
    - **Autenticación por Clave SSH:** Deshabilita la autenticación por contraseña y utiliza exclusivamente claves SSH. Es mucho más seguro.
    - **Instalar Fail2ban:** Este servicio monitorea los logs y banea automáticamente las IPs que intentan ataques de fuerza bruta contra SSH u otros servicios.
    - **UFW (Uncomplicated Firewall):** Activa también el firewall local como una segunda capa de defensa.
- **Seguridad de la Aplicación (Flask):**
    - **Variables de Entorno: Nunca** escribas contraseñas, claves de API o tokens directamente en el código. Utiliza un archivo .env (incluido en .gitignore) para gestionar esta información sensible.
    - **Actualizar Dependencias:** Mantén las librerías de Python (Flask, sus extensiones, etc.) actualizadas para protegerte de vulnerabilidades conocidas.

2. Plan de Mantenimiento Preventivo (Acciones Programadas)

Son las tareas recurrentes para mantener el servidor sano y evitar problemas.

Diarias

- **Verificación de Backups Automáticos:** DigitalOcean ofrece backups automáticos a nivel de Droplet. **Confirma cada día desde el panel que el backup del día anterior se completó exitosamente.** Un backup fallido es un riesgo enorme.

Semanales

- **Actualización de Paquetes del Sistema:** Conéctate por SSH y actualiza todos los paquetes de Ubuntu. Esto aplica parches de seguridad críticos.
- **Revisión de Logs del Sistema y Aplicación:** Busca patrones de errores inusuales en los logs del sistema (journalctl), del servidor web (Nginx/Gunicorn) y de tu aplicación Flask.
- **Monitoreo de Recursos:** Revisa las gráficas de uso de **CPU, RAM y Disco** en el panel de DigitalOcean. Busca picos inesperados o una tendencia de crecimiento constante que pueda indicar un problema de rendimiento o la necesidad de ampliar el Droplet.

Mensuales

- **Prueba de Restauración de Backups:** Esta es una tarea **crítica**. Crea un nuevo Droplet a partir de tu último backup para **verificar que la restauración funciona** y que tanto la aplicación como la base de datos se levantan correctamente. Un backup no probado no es confiable.
- **Revisión de Espacio en Disco:** Asegúrate de que tienes suficiente espacio libre, especialmente si tu aplicación o base de datos generan muchos archivos o logs.
- **Optimización de la Base de Datos:** Ejecuta tareas de mantenimiento en tu base de datos (por ejemplo, VACUUM en PostgreSQL) para mantener su rendimiento óptimo.

Trimestrales

- **Auditoría de Acceso:** Revisa quién tiene acceso SSH al servidor y elimina las claves (~/.ssh/authorized_keys) de personas que ya no necesiten acceso.
- **Revisión de Reglas del Firewall:** Confirma que las reglas del Firewall (tanto en DigitalOcean como en UFW) siguen siendo las correctas y no se ha abierto ningún puerto innecesario.

3. Plan de Mantenimiento Correctivo (Respuesta a Incidentes)

Este es el protocolo a seguir cuando algo falla. El objetivo es restaurar el servicio lo más rápido posible y de forma segura.

Incidente: La Aplicación Web no Responde o Muestra un Error 500

1. **Diagnóstico Inmediato (Primeros 5 minutos):**
    - **¿El servidor está en línea?** Intenta conectarte por SSH. Si no puedes, usa la **Consola de Recuperación** desde el panel de DigitalOcean. Revisa el uso de CPU/RAM desde el panel; un uso del 100% puede ser la causa.
    - **Revisa el estado del servicio.** Una vez dentro, verifica si los procesos de tu aplicación (Gunicorn/uWSGI) y de la base de datos están corriendo.
    - **Consulta los logs.** Esta es tu principal fuente de información. Revisa los últimos errores.
2. **Acciones de Contención Rápida:**
    - **Reiniciar el servicio:** A menudo, un simple reinicio de la aplicación soluciona problemas temporales.
    - **Reiniciar el Droplet:** Si el servidor está colgado por un problema de recursos, un reinicio desde el panel de DigitalOcean puede ser la solución más rápida para restaurar el servicio mientras investigas la causa.
3. **Recuperación Mayor (Plan "B"):**
    - **Restaurar desde un Snapshot:** Si el problema es grave (un borrado accidental, una actualización fallida que rompió el sistema), la forma más rápida y segura de recuperarse es **restaurar el Droplet a partir del último backup automático de DigitalOcean**. Esto reemplazará tu servidor con una copia funcional de la noche anterior. Perderás los datos generados desde el último backup, pero el servicio volverá a estar en línea.
4. **Análisis Post-Incidente:**
    - Una vez que el servicio esté restaurado, **investiga la causa raíz** del problema usando los logs. ¿Fue un pico de tráfico? ¿Una mala consulta a la base de datos? ¿Falta de memoria?
    - **Documenta el problema y la solución.** Esto te ayudará a prevenir que vuelva a ocurrir y a solucionarlo más rápido en el futuro.