🔐 AWS Lambda + Aurora con Secrets Manager

Guía simplificada para desarrolladores junior

⚠️ ¿Por qué NO usar contraseñas en el código?

- ✗ **Inseguro:** Las contraseñas quedan expuestas en el código
- ✗ **Difícil de mantener:** Cambiar una contraseña requiere modificar y redesplegar todo
- ✗ **No cumple normas:** Viola estándares como PCI DSS y HIPAA

✅ La Solución: AWS Secrets Manager

- ✓ **Cifrado automático:** Tus contraseñas están protegidas con AWS KMS
- ✓ **Acceso controlado:** Solo quien debe puede acceder
- ✓ **Rotación automática:** Cambia contraseñas sin tocar el código
- ✓ **Gestión centralizada:** Un solo lugar para todos tus secretos

🔄 ¿Cómo Funciona?

1. **Se activa Lambda**
   Un evento (API, cronograma, etc.) ejecuta tu función Lambda
2. **Lambda asume un rol IAM**
   Automáticamente obtiene permisos para actuar
3. **Solicita las credenciales**
   Lambda pide al Secrets Manager las contraseñas de la base de datos
4. **Secrets Manager valida y entrega**
   Verifica permisos y devuelve las credenciales descifradas
5. **Conexión a Aurora**
   Lambda usa las credenciales para conectarse a la base de datos
6. **Procesa y guarda datos**
   Ejecuta la consulta y guarda resultados (ej: en S3)

🛠️ Pasos de Implementación

📦 A. Guardar Secreto

- → Ir a Secrets Manager
- → Seleccionar "Store a new secret"
- → Elegir "RDS database credentials"
- → Ingresar usuario y contraseña
- → Darle un nombre (ej: prod/aurora/credentials)
- → Activar rotación automática (recomendado)

🔑 B. Configurar Rol IAM

- → Crear rol para Lambda
- → Agregar política de confianza para Lambda
- → Dar permiso para leer el secreto
- → Agregar permisos para VPC y logs
- → Principio: menor privilegio posible

💻 C. Escribir Código

- → Usar variables de entorno para el nombre del secreto
- → Obtener secreto con boto3 (Python)
- → Manejar errores con try/except
- → Cerrar conexiones siempre (finally)
- → NUNCA poner contraseñas en el código

⚙️ D. Configurar Lambda

- → Subir código empaquetado (.zip)
- → Asignar el rol IAM creado
- → Configurar variables de entorno
- → Conectar a la misma VPC que Aurora
- → Configurar grupos de seguridad

📚 Fuentes de Información

1. Doppler - Lambda Secrets Manager Guide
2. AWS Docs - Lambda with Secrets Manager
3. AWS Docs - Retrieving Secrets in Lambda
4. Apiiro - Hardcoded Secrets Glossary
5. Checkmarx - Exposed Secrets Prevention