

PLANTILLA — PLAN DE IMPLEMENTACIÓN / DESPLIEGUE

Portada

- **Proyecto/Sistema:**
- **Versión del documento:**
- **Fecha:**
- **Responsable:**
- **Ambiente objetivo:** (QA / Staging / Producción)

Control de versiones

Versión	Fecha	Autor	Descripción del cambio
1.0			

1. Introducción

(Explica brevemente el propósito del plan: describir cómo se implementará/desplegará el sistema en el ambiente objetivo, minimizando riesgos y asegurando continuidad operativa.)

2. Objetivo

Definir el procedimiento técnico y organizativo para ejecutar el despliegue del sistema, asegurando:

- disponibilidad del servicio,
- integridad de datos,
- control de cambios,
- validación posterior al despliegue.

3. Alcance

3.1 Incluye

- Preparación del ambiente (servidor, BD, variables)
- Instalación/despliegue de backend y frontend
- Configuración de servicios
- Migración/carga inicial de datos (si aplica)
- Validación post-despliegue (smoke test)
- Plan de reversión (rollback)

3.2 No incluye

- Mejoras funcionales del software

- Desarrollo de nuevas características
- Pruebas de rendimiento avanzadas (si no aplica)

4. Roles y responsabilidades

Rol	Nombre	Responsabilidad
Líder de despliegue		Coordina el despliegue
Dev Backend		Publicación de API
Dev Frontend		Publicación UI
DBA / Responsable BD		Migraciones y respaldos
QA		Validación post-despliegue
Dueño del producto		Aprobación final

5. Requisitos previos

5.1 Requisitos de infraestructura

- Servidor / VM / Hosting:
- IP / DNS / Dominio:
- Certificado SSL (si aplica):
- Acceso SSH/RDP:

5.2 Requisitos de software

- Sistema operativo:
- Runtime: (Python/Node/.NET/etc.)
- Motor de BD:
- Servidor web/reverse proxy: (Nginx/Apache/IIS)
- Contenedores: (Docker/Kubernetes, si aplica)

5.3 Accesos necesarios

- Repositorio (GitHub/GitLab):
- Servidor de despliegue:
- Base de datos:
- Panel cloud: (Azure/AWS/GCP, si aplica)

6. Arquitectura de despliegue (resumen)

Componentes a desplegar:

- Frontend:

- Backend/API:
- Base de datos:
- Almacenamiento multimedia (si aplica):
- Servicios externos (si aplica):

Puertos y servicios

Servicio	Puerto	Protocolo	Observación
Frontend		HTTP/HTTPS	
Backend		HTTP/HTTPS	
DB		TCP	

7. Estrategia de despliegue

Seleccionar una estrategia:

- **Despliegue directo:** actualización en el mismo servidor.
- **Blue/Green:** dos ambientes alternos.
- **Rolling update:** actualización gradual.
- **Canary:** despliegue controlado a una parte de usuarios.

Estrategia elegida:

Justificación:

8. Planificación del despliegue

8.1 Fecha y ventana de despliegue

- **Fecha:**
- **Hora inicio:**
- **Hora fin estimada:**
- **Ventana aprobada por:**

8.2 Checklist previo

- ☐ Código aprobado en rama principal (main/master)
- ☐ Merge realizado y estable
- ☐ Compilación/build exitoso
- ☐ Pruebas aprobadas (mínimo smoke/regresión)
- ☐ Backups realizados
- ☐ Variables de entorno listas

- ☐ Plan de rollback definido

9. Procedimiento de implementación/despliegue (Paso a paso)

9.1 Preparación del entorno

1. Verificar disponibilidad del servidor y recursos.
2. Confirmar conexión y permisos de acceso.
3. Validar que el ambiente objetivo esté correcto (QA/Prod).

9.2 Respaldo (Backup)

Objetivo: garantizar recuperación ante fallos.

Acciones:

1. Generar backup de base de datos:
 - Nombre del archivo:
 - Ubicación:
2. Respalidar archivos multimedia (si aplica):
3. Respalidar configuraciones (Nginx/IIS/.env):

9.3 Despliegue de Backend (API)

1. Descargar la última versión del repositorio:
 - rama/tag:
2. Instalar dependencias:
 - comandos:
3. Aplicar migraciones de base de datos:
 - comandos:
4. Configurar variables de entorno:
 - .env / settings / secrets
5. Reiniciar servicio backend:
 - systemctl / pm2 / docker restart / IIS reset
6. Verificar endpoint de salud:
 - /health o /api/status

9.4 Despliegue de Frontend (UI)

1. Compilar proyecto frontend:
 - comando:

2. Publicar build en servidor:
 - ruta:
3. Configurar URL del backend/API:
 - variables / config
4. Reiniciar servicio frontend (si aplica)
5. Validar acceso por navegador:
 - URL:

9.5 Configuración de servidor web (si aplica)

1. Configurar reverse proxy (Nginx/Apache/IIS).
2. Habilitar HTTPS con certificado SSL.
3. Verificar redirecciones y rutas.

10. Pruebas posteriores al despliegue (Smoke Test)

Objetivo: confirmar que el sistema funciona después de implementar.

Checklist:

- ☐ Acceso al sistema (login)
- ☐ Navegación principal
- ☐ Consulta de datos
- ☐ Creación/actualización (si aplica)
- ☐ Reportes/Dashboard
- ☐ Verificación de logs sin errores críticos

Resultado: (Aprobado / No aprobado)

Observaciones:

11. Plan de rollback (reversión)

Objetivo: restaurar el sistema en caso de fallo.

Criterios para aplicar rollback:

- Error crítico impide el uso
- Caída del servicio prolongada
- Pérdida/corrupción de datos
- Fallo en validación post-despliegue

Procedimiento de rollback:

1. Detener el servicio actual.
2. Restaurar versión anterior (tag/release).
3. Restaurar backup de base de datos (si aplica).
4. Reiniciar servicios.
5. Ejecutar smoke test nuevamente.

12. Riesgos y mitigación

Riesgo	Impacto	Probabilidad	Mitigación
Fallo en migraciones	Alto	Media	Backup + validar migraciones en QA
Configuración incorrecta	Alto	Media	Checklist + doble revisión
Caída del servicio	Alto	Baja	Ventana + rollback listo

13. Evidencias del despliegue

- Capturas de:
 - consola de despliegue
 - servicios activos
 - sistema funcionando
 - pruebas smoke test
- Logs relevantes:
 - ruta / archivo log

14. Cierre y aprobación

Estado final del despliegue: (Exitoso / Fallido / Exitoso con observaciones)

Observaciones finales:

Nombre	Rol	Firma	Fecha
	Líder de despliegue		
	QA		
	Responsable del sistema		