

PLAN DE DESPLIEGUE

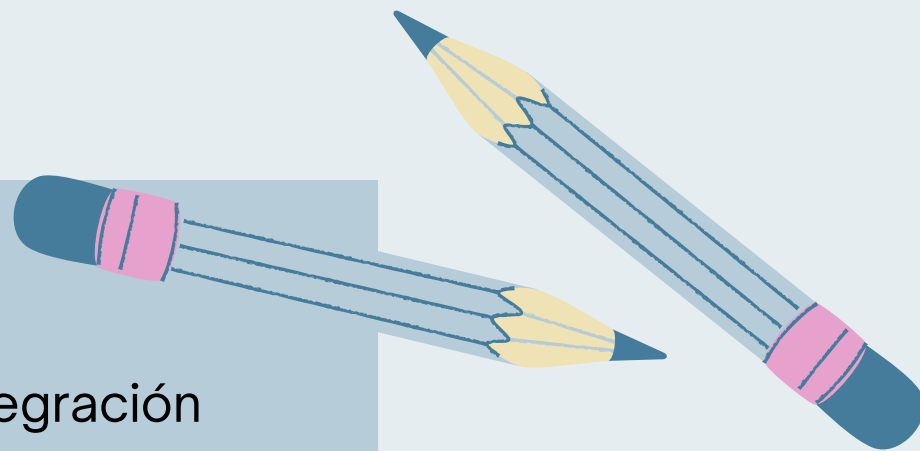
Es el “plan de acción” que permite pasar una nueva versión del software desde el entorno de desarrollo hasta el entorno real (producción) de manera segura, controlada y reproducible.

INTRODUCCIÓN

Empresa proveedora de sensores IoT para medir temperatura y humedad en plantas industriales. Se necesita desplegar nuevos firmwares para corregir bugs y mejorar algoritmos de medición. El gran riesgo esta en la falla de una actualización, los dispositivos puede quedar inutilizable (brick) y enviar un técnico físicamente sería muy costoso.

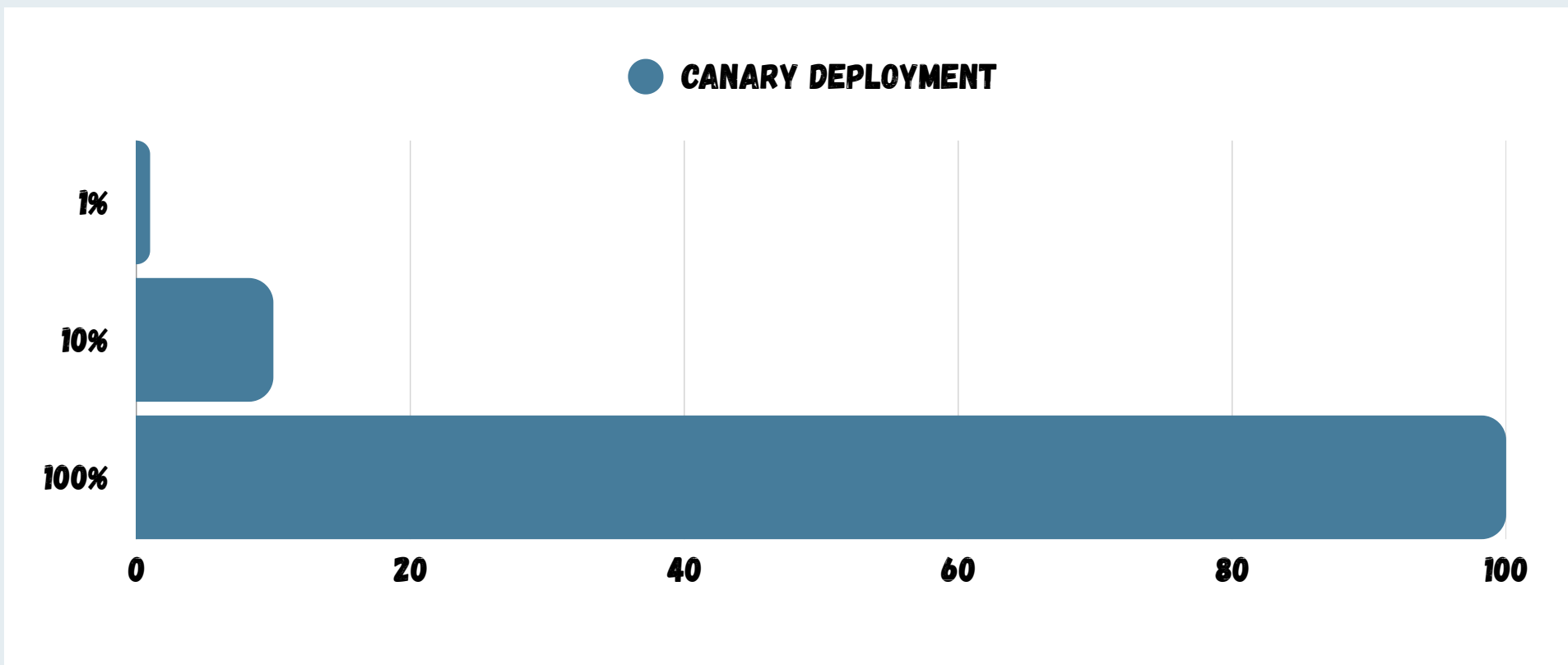
OBJETIVO

El objetivo es presentar un plan de despliegue para el escenario descrito. En el cual se dé respuesta a los ítems planteados en los lineamentos para trabajos de investigación de la catedra.



METODOLOGIA

- Se implementa un pipeline CI/CD con integración continua, pruebas automáticas, firma digital y publicación segura.
- Despliegue progresivo (Canario 1% → 10% → 100%) para reducir riesgos.
- Rollback automático mediante partición dual.
- Canal de descarga protegido con cifrado TLS.
- Telemetría post-despliegue para verificar el correcto funcionamiento.



RESULTADOS ESPERADOS

- Reducción máxima en intervenciones físicas de personal técnico.
- Asegurar disponibilidad, 0% brick.
- 100 % de trazabilidad de versiones (SCM)
- Mayor confiabilidad del sistema
- Optimización del consumo de red
- Cumplimiento de protocolos de seguridad



CONCLUSION

En un entorno industrial con conectividad limitada y alta criticidad operativa, el despliegue remoto de firmware representa un desafío importante para mantener la confiabilidad del sistema.

El despliegue OTA progresivo con rollback automático y verificación criptográfica permite actualizar sensores IoT distribuidos sin detener la producción. La estrategia reducirá costos de mantenimiento, garantizara seguridad e integridad del firmware y asegurará continuidad operativa en plantas con conectividad limitada.



ASPECTOS TECNICOS

Ítem	Detalle Implementado
Entorno de destino	Sensores IoT distribuidos en plantas con conectividad variable.
Metodo de despliegue y tipo de despliegue	OTA (over the air) + canario 1% inicial.
Infraestructura requerida	Servidor de firmware, gateways locales, colas MQTT/CoAP.
Artefacto (software)	Firmware v2.4 – rollback posible a v2.3.
Cómo se instala	Servidor OTA → MQTT→ Sensor IoT → Descarga partición B → Verificación TLS / Firma digital → Reinicio y activación → Rollback
Dependencias	Biblioteca de drivers, stack de comunicación MQTT/REST, y gestor de firmware dual-partition.
Roles involucrados	DevOps, QA tester, Equipo de Desarrollo
Horario de despliegue	Ventana: 02:00–04:00 AM / menor actividad operativa

ASPECTOS ORGANIZATIVOS

Procesos para e despliegue del producto	<ul style="list-style-type: none">Planificación del desplieguePruebas pre-despliegueDespliegueVerificación post-despliegue → rollback automaticoCierre y documentación
Relación DevOps – Despliegue de Productos	Radica en la automatización y control del proceso OTA: el equipo DevOps gestiona el pipeline CI/CD y la seguridad para asegurar actualizaciones remotas confiables, trazables y con capacidad de rollback en los sensores IoT.
Relación SCM – Despliegue de Productos	<ul style="list-style-type: none">Mantiene el registro exacto de versiones del firmwarePermite volver a una versión anteriorControla las dependencias y configuraciones asociadas
Relación prácticas continuas – Despliegue de Productos	Las prácticas continuas CI/CD facilitan la planificación de despliegues, permiten automatizar el proceso, incluyendo la configuración de pruebas automatizadas, la configuración de entornos y el despliegue en producción.
Seguridad en el despliegue de productos	una actualización maliciosa o corrupta podría dañar los dispositivos, por lo que seguridad implica un aspecto crítico. Resuelto mediante Firma digital del firmware, Cifrado TLS en la transmisión, Rollback automático
Plan de rollback / contingencia	Reversión inmediata a versión previa (partición backup).