TIPOS DE PRUEBAS

Marc Triay Orfila y Mateo Ortuño Ovando

Tipos de Pruebas: Software

- Cubre el espectro completo de validación de software.
- Pruebas funcionales, estructurales y de regresión principales.
- Incluye subtipos esenciales: caja blanca y caja negra.
- Aborda automatización, seguridad e interoperabilidad cruciales.

Tipos de pruebas existentes:

- Funcionales
- Estructurales
- De regresión

FUNCIONALES

Están enfocadas en verificar requisitos

Incluyen pruebas unitarias, de integración, de sistema y de aceptación (UAT)

Abarcando desde el código individual hasta la validación final del usuario.

ESTRUCTURALES

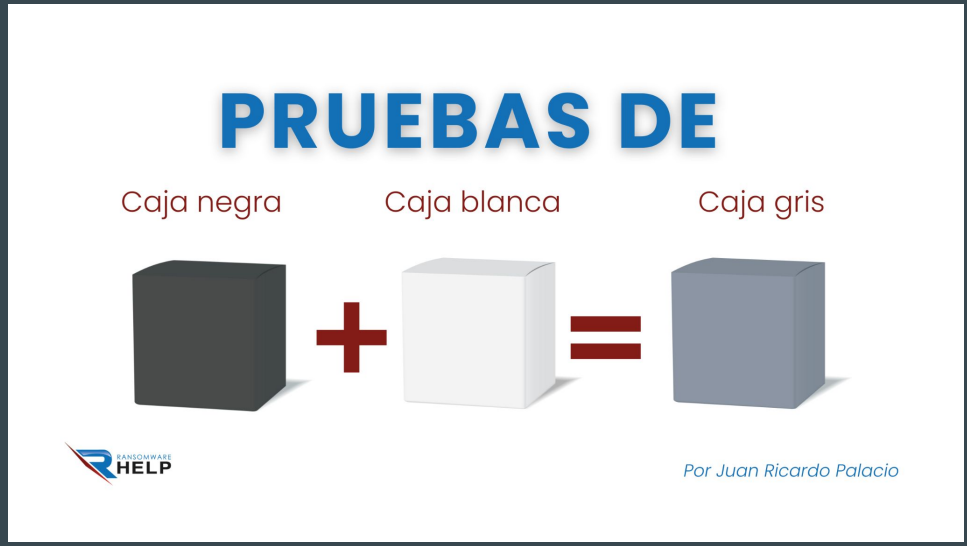
Los tipos de pruebas estructurales varían según el campo (ingeniería civil, software), pero generalmente se dividen en no destructivas (END) y destructivas, y se enfocan en evaluar la integridad, rendimiento y fallos; en software, son pruebas de caja blanca que examinan la lógica interna (cobertura de código, flujo de datos), mientras que en ingeniería civil incluyen pruebas de carga (vertical/horizontal), monitorización y ensayos de materiales para pilares, cimentaciones y edificios.

DE REGRESIÓN

Los tipos de pruebas de regresión se clasifican según su alcance y propósito, incluyendo correctivas (verificar correcciones), progresivas (validar nuevas funciones sin afectar lo antiguo), selectivas (probar solo áreas afectadas por cambios) y completas/total (re-probar todo), además de enfoques como las pruebas de integración (interacción entre componentes) o las no funcionales (rendimiento, seguridad)

Subtipos de pruebas

- Caja negra
- Caja blanca
- Pruebas automatizadas
- Pruebas de seguridad
- Pruebas de interoperabilidad



CAJA NEGRA

La **caja negra** es una metodología de pruebas que, cuando se aplica a las **pruebas funcionales** , se convierte en la técnica principal para validar que el sistema cumple con lo que el usuario espera sin mirar cómo está construido por dentro.

Generalmente son realizadas por los **ingenieros de control de calidad (QA Testers)** y los **usuarios finales** .

CAJA NEGRA

Pruebas que se enmarcan en la caja negra:

Partición de equivalencia, Análisis de valores límite, Pruebas de tabla de decisión, Pruebas de transición de estados, Pruebas de humo (Smoke Testing), Pruebas de aceptación del usuario (UAT).

CAJA BLANCA

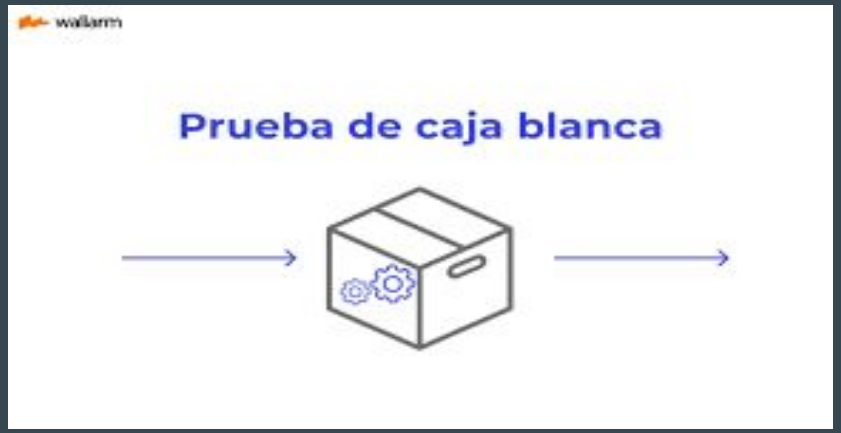
La metodología de **caja blanca** consiste en un enfoque de validación de software que examina la **estructura interna** , el código fuente y el diseño lógico de una aplicación, de la cual se encargan los desarrolladores

pertenece a tipología de pruebas estructurales

CAJA BLANCA

Pruebas que se enmarcan en la caja blanca:

Pruebas unitarias, Cobertura de sentencias (Statement Coverage), Cobertura de ramas o decisiones, Pruebas de bucles (Loop Testing), Análisis estático de código, Pruebas de flujo de datos.



PRUEBAS AUTOMATIZADAS

Las **pruebas automatizadas** son una técnica que utiliza herramientas de software especializadas y scripts para ejecutar casos de prueba de forma automática, comparando los resultados reales con los esperados sin necesidad de intervención humana constante.

Las pruebas automatizadas son **transversales** , pero su uso es más crítico en las **pruebas de regresión** .

Debido a que estas pruebas deben repetirse cada vez que el código cambia para asegurar que nada se haya roto, realizarlas manualmente sería ineficiente.

PRUEBAS AUTOMATIZADAS

Los que se encargan de realizar esta prueba son:

Ingenieros de Automatización de QA (SDET), Desarrolladores, Analistas de Negocio / QA Manuales.

Pruebas que se enmarcan en la automatización:

Pruebas Unitarias Automatizadas, Pruebas de Regresión, Pruebas de API, Pruebas de Rendimiento y Carga, Pruebas de Interfaz de Usuario (UI), Pruebas de Humo (Smoke Tests).

PRUEBAS DE SEGURIDAD

Las **pruebas de seguridad** son un conjunto de metodologías diseñadas para identificar vulnerabilidades, amenazas y riesgos en un sistema de software, con el fin de prevenir ataques externos y garantizar la protección de los datos.

Las pruebas de seguridad son predominantemente **pruebas estructurales** (en su análisis interno) y **funcionales** (en la validación de controles), pero su implementación más robusta es como **pruebas estructurales** .

se encargan en realizarla:

Hacker Ético / Especialista en Ciberseguridad, Ingenieros de DevSecOps, Analistas de Seguridad.

PRUEBAS DE SEGURIDAD

Pruebas que se enmarcan en la seguridad:

SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), Pruebas de Penetración (Pentesting), Escaneo de Vulnerabilidades, Pruebas de Autenticación y Autorización, Pruebas de Inyección (SQL, XSS).

PRUEBAS DE INTEROPERABILIDAD

Las **pruebas de interoperabilidad** tienen como objetivo verificar que el software sea capaz de comunicarse, intercambiar datos y funcionar correctamente con otros sistemas, plataformas o componentes externos.

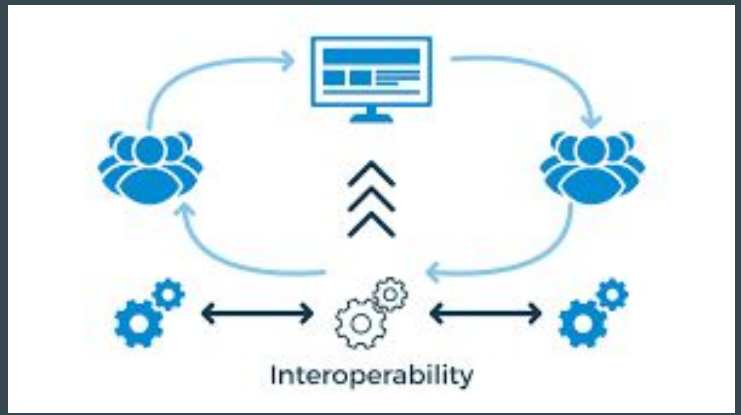
Las pruebas de interoperabilidad pertenecen a las **pruebas funcionales** .

los encargados son:

Ingenieros de QA de Integración

Arquitectos de Software

Ingenieros de DevOps



PRUEBAS DE INTEROPERABILIDAD

Pruebas que se enmarcan en la interoperabilidad:

Pruebas de API (Application Programming Interface), Pruebas de Compatibilidad de Protocolos, Pruebas de Formato de Datos, Pruebas de Interoperabilidad Semántica, Pruebas de Conectividad con Bases de Datos, Pruebas de Multiplataforma / Multicloud.