GESTÓN DE PRUEBAS FUNCIONALES, TÉCNICAS Y DE SEGURIDAD

DIRECCIÓN DE GESTIÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD
SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

Noviembre de 2026

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

CONTENIDO

1 INTRODUCCIÓN 3
2 OBJETIVO 3
3 ALCANCE 3
4 NORMATIVIDAD 4
4.1 Normatividad externa 4
4.2 Referentes técnicos 4
4.3 Documentos institucionales relacionados 4
5 DEFINICIONES 5
6 PRINCIPIOS RECTORES 6
7 METODOLOGÍA PARA LA GESTIÓN DE PRUEBAS 6
7.1 Criterios para la selección y aplicación de pruebas 6
7.2 Tipos de pruebas 7
7.3 Fases de la gestión de pruebas 8
7.4 Preparación de ambientes y datos de prueba 9
7.5 Gestión de hallazgos y criterios de aceptación 9
7.6 Técnicas y herramientas de apoyo 9
7.7 Integración con prácticas DevSecOps 10
7.8 Roles y responsabilidades 11
8 ENTREGABLES DE LA GESTIÓN DE PRUEBAS 11
HISTORIAL DE CAMBIOS 12

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

1 INTRODUCCIÓN

La creciente dependencia de los procesos institucionales respecto de las soluciones tecnológicas, el aumento de las integraciones y servicios digitales, la evolución de las arquitecturas de software y la necesidad de proteger la información institucional demandan mecanismos de aseguramiento de calidad cada vez más consistentes y trazables.

La diversidad de requerimientos funcionales y no funcionales, tecnologías, datos, interfaces y componentes de seguridad hace necesario fortalecer las prácticas de verificación y validación antes de liberar cambios o nuevas soluciones, reduciendo la probabilidad de fallas, vulnerabilidades, afectaciones a la continuidad operativa y reprocesos durante la operación.

En este contexto, la Agencia Nacional de Tierras requiere criterios técnicos y operativos comunes que permitan ejecutar las pruebas de manera proporcional a la criticidad, alcance y riesgos de cada iniciativa, articulando la calidad del software con la arquitectura institucional, la seguridad y privacidad de la información, la interoperabilidad y la mejora continua.

2 OBJETIVO

Establecer la metodología técnica y operativa para planificar, diseñar, preparar, ejecutar, documentar, gestionar y cerrar las pruebas funcionales, técnicas y de seguridad aplicables a las soluciones tecnológicas de la Agencia Nacional de Tierras, con el fin de verificar el cumplimiento de los requerimientos y criterios de aceptación, identificar y tratar oportunamente hallazgos y vulnerabilidades, y generar evidencias trazables que soporten la aceptación de la solución y su eventual paso a producción, mediante la aplicación de prácticas de aseguramiento de calidad, arquitectura, seguridad y privacidad de la información y, cuando aplique, automatización y DevSecOps.

3 ALCANCE

Este instructivo aplica a los sistemas de información, aplicaciones, servicios digitales, integraciones, interfaces, APIs y demás componentes de software desarrollados, modificados, adquiridos o mantenidos por la Agencia Nacional de Tierras, incluyendo sistemas de información tradicionales y sistemas de información geográfica.

Aplica a desarrollos internos o inhouse y a soluciones construidas o implementadas por proveedores o contratistas, así como a iniciativas nuevas, evolutivas, correctivas, adaptativas o de integración. Comprende desde la definición de la estrategia y el plan de pruebas hasta el cierre del ciclo de validación, incluyendo el diseño de casos, preparación de ambientes y datos, ejecución, registro y tratamiento de hallazgos, reejecución, pruebas de regresión, aceptación funcional y consolidación de evidencias.

La profundidad y combinación de las pruebas deberá determinarse de acuerdo con la naturaleza, criticidad, arquitectura, exposición, volumen de información, integraciones, requisitos de seguridad y privacidad y nivel de riesgo de la solución, sin perjuicio de los controles mínimos establecidos en los instrumentos institucionales aplicables.

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

4 NORMATIVIDAD

4.1 Normatividad externa

- Ley Estatutaria 1581 de 2012: Disposiciones generales para la protección de datos personales.
- Ley 1341 de 2009: Define principios y organización de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia.
- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 767 de 2022: Establece los lineamientos generales de la Política de Gobierno Digital.
- Decreto 1263 de 2022: Define lineamientos para la Transformación Digital Pública.

4.2 Referentes técnicos

- ISO/IEC 25010: Modelo de calidad para productos de software y sistemas.
- ISO/IEC 27001 e ISO/IEC 27002: Referentes para la gestión de seguridad de la información y sus controles.
- OWASP Top 10 y OWASP ASVS: Referentes para identificación y verificación de riesgos de seguridad en aplicaciones.

4.3 Documentos institucionales relacionados

- GINFO-Política-006 Política General de Tecnologías de la Información y las Comunicaciones (TIC).
- GINFO-L-001 Lineamientos para la Gestión del Ciclo de Vida de Sistemas de Información.
- GINFO-P-003 Construcción de Software.
- GINFO-I-032 Gestión de Requerimientos Funcionales y No Funcionales.
- GINFO-G-015 Guía del Plan de Pruebas de Software.
- GINFO-G-020 Framework Tecnológico para los Sistemas de Información Institucional.
- GINFO-F-033 Lista de Chequeo Paso a Producción Sistemas de Información.
- GINFO-F-046 Levantamiento y Análisis de Requerimientos.
- GINFO-F-048 Historia de Usuario.
- GINFO-F-050 Acta de Aceptación Funcional para la Transferencia de Soluciones de Terceros.
- Política institucional vigente de seguridad y privacidad de la información.
- Lineamientos institucionales vigentes de Arquitectura Empresarial, seguridad de la información, administración de bases de datos, datos e interoperabilidad y accesibilidad.

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

5 DEFINICIONES

- **Ambiente de pruebas:** Entorno controlado y separado del ambiente productivo en el que se ejecutan validaciones funcionales, técnicas, de integración, rendimiento o seguridad.
- **Caso de prueba:** Conjunto documentado de condiciones, datos de entrada, pasos de ejecución y resultados esperados utilizado para verificar un requerimiento o comportamiento específico de la solución.
- **Criterio de aceptación:** Condición verificable que debe cumplirse para considerar satisfactorio un requerimiento, funcionalidad, componente o entrega.
- **DAST (Dynamic Application Security Testing):** Análisis dinámico de seguridad aplicado sobre una solución en ejecución para identificar vulnerabilidades observables durante su funcionamiento.
- **DevSecOps:** Enfoque que integra desarrollo, seguridad y operaciones durante el ciclo de vida del software, promoviendo controles y validaciones de seguridad continuas y, cuando sea posible, automatizadas.
- **Evidencia de prueba:** Registro verificable que demuestra la ejecución y resultado de un caso o escenario de prueba, como capturas, registros de eventos, archivos de salida, reportes o resultados generados por herramientas.
- **Hallazgo:** Falla, defecto, vulnerabilidad, desviación o incumplimiento identificado durante una prueba respecto de un requerimiento, criterio de aceptación, estándar o control aplicable.
- **Informe de resultados de pruebas:** Documento o registro consolidado que presenta el alcance ejecutado, resultados, hallazgos, estado de aceptación, riesgos y recomendaciones derivados del ciclo de pruebas.
- **OWASP:** Open Worldwide Application Security Project, comunidad y conjunto de referentes técnicos orientados al fortalecimiento de la seguridad de aplicaciones.
- **Plan de pruebas:** Instrumento que define alcance, objetivos, tipos de prueba, ambientes, datos, recursos, responsabilidades, cronograma, criterios de entrada y salida y evidencias requeridas para un ciclo de pruebas.
- **Plataforma institucional de gestión de requerimientos y desarrollo:** Herramienta autorizada por la entidad para registrar, planificar, hacer seguimiento y conservar evidencias de requerimientos, actividades, pruebas, hallazgos y cambios asociados al ciclo de vida del software.
- **Prueba automatizada:** Prueba ejecutada mediante scripts, pipelines o herramientas que permiten validar de forma repetible una condición con mínima intervención manual.
- **Prueba de aceptación de usuario (UAT):** Validación realizada con participación de la dependencia funcional o usuarios designados para confirmar que la solución satisface los requerimientos y criterios de aceptación acordados.
- **Prueba de regresión:** Validación orientada a confirmar que una corrección, ajuste o nueva funcionalidad no afectó comportamientos previamente aprobados.
- **Prueba de seguridad:** Validación orientada a identificar vulnerabilidades, configuraciones inseguras o incumplimientos que puedan comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información y los servicios.
- **Prueba funcional:** Validación del comportamiento de la solución frente a los requerimientos funcionales, reglas de negocio y criterios de aceptación definidos.

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

- **Prueba técnica:** Validación de aspectos no funcionales o tecnológicos como integración, rendimiento, carga, estabilidad, compatibilidad, integridad de datos, observabilidad o comportamiento de infraestructura.
- **Reejecución:** Nueva ejecución de un caso de prueba previamente fallido después de aplicar una corrección, con el fin de verificar la solución del hallazgo.
- **SAST (Static Application Security Testing):** Análisis estático de seguridad realizado sobre código fuente o artefactos sin ejecutar la aplicación, orientado a identificar debilidades de seguridad de forma temprana.
- **Trazabilidad de pruebas:** Capacidad de relacionar requerimientos, casos de prueba, resultados, hallazgos, correcciones, reejecuciones, aprobaciones y evidencias durante el ciclo de validación.

6 PRINCIPIOS RECTORES

- **Orientación a la calidad:** Las pruebas deberán verificar de manera objetiva el cumplimiento de los requerimientos funcionales y no funcionales y contribuir a la estabilidad y sostenibilidad de la solución.
- **Seguridad y privacidad integradas:** La validación de controles de seguridad y privacidad deberá incorporarse desde etapas tempranas y mantenerse de manera proporcional al riesgo durante el ciclo de pruebas.
- **Trazabilidad:** Los casos, resultados, hallazgos, correcciones y aprobaciones deberán relacionarse con los requerimientos y conservarse en los repositorios institucionales definidos.
- **Independencia y objetividad:** Cuando la criticidad o naturaleza de la solución lo requiera, las validaciones deberán contar con participación de actores diferentes a quienes realizaron la construcción del componente probado.
- **Interoperabilidad y compatibilidad:** Las soluciones deberán ser verificadas respecto de sus integraciones, interfaces, dependencias y compatibilidad con la arquitectura y los ambientes tecnológicos institucionales.
- **Proporcionalidad basada en riesgo:** El alcance y profundidad de las pruebas deberá definirse según criticidad, impacto, exposición, datos tratados, complejidad e historial de cambios de la solución.
- **Automatización y repetibilidad:** Se promoverá la automatización de pruebas repetitivas y controles técnicos cuando genere valor, permita detectar fallas tempranas y facilite la ejecución consistente de regresiones.
- **Mejora continua:** Los resultados y lecciones aprendidas deberán retroalimentar la construcción, arquitectura, seguridad, requerimientos y prácticas de prueba de futuras iniciativas.

7 METODOLOGÍA PARA LA GESTIÓN DE PRUEBAS

La gestión de pruebas deberá integrarse con el ciclo de vida definido institucionalmente y con el procedimiento GINFO-P-003 Construcción de Software. La ejecución podrá adaptarse a enfoques ágiles, tradicionales o híbridos, manteniendo en todos los casos la trazabilidad entre requerimientos, criterios de aceptación, casos de prueba, resultados, hallazgos y evidencias.

7.1 Criterios para la selección y aplicación de pruebas

La selección de los tipos de pruebas y su profundidad deberá realizarse durante la planeación, considerando como mínimo:

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

- Criticidad e impacto de la solución sobre los procesos institucionales.
- Naturaleza del cambio: nuevo desarrollo, evolución, corrección, integración, actualización tecnológica o configuración.
- Arquitectura, componentes, integraciones, dependencias y ambientes involucrados.
- Volumen, sensibilidad y clasificación de la información procesada.
- Requisitos de seguridad, privacidad, interoperabilidad, accesibilidad y rendimiento.
- Exposición de la solución a Internet, usuarios externos o servicios de terceros.
- Historial de incidentes, defectos o vulnerabilidades de la solución.
- Criterios de aceptación definidos en GINFO-I-032 y en los instrumentos de requerimientos aplicables.

Como mínimo, todo cambio funcional deberá contar con pruebas funcionales y de regresión proporcionales a su impacto; toda solución con integraciones deberá validar la interoperabilidad; y toda solución deberá considerar controles de seguridad acordes con su nivel de riesgo. Las pruebas de rendimiento, carga, accesibilidad, compatibilidad o penetración controlada se ejecutarán cuando la naturaleza y criticidad de la solución lo requieran.

7.2 Tipos de pruebas

Tipo de prueba	Propósito
Pruebas unitarias	Validan componentes individuales de código y deben ejecutarse antes de liberar una construcción hacia ambientes formales de prueba.
Pruebas de integración	Verifican la interacción entre módulos, servicios, APIs, bases de datos, componentes externos e interfaces.
Pruebas funcionales	Comprueban reglas de negocio, flujos, validaciones y resultados esperados conforme a requerimientos y criterios de aceptación.
Pruebas de aceptación de usuario (UAT)	Confirman con la dependencia funcional o usuarios designados que la solución satisface las necesidades y condiciones acordadas.
Pruebas de regresión	Verifican que los cambios no afecten funcionalidades previamente aprobadas.
Pruebas de rendimiento	Evalúan tiempos de respuesta, consumo de recursos, estabilidad y comportamiento frente a objetivos definidos.
Pruebas de carga y estrés	Evalúan el comportamiento bajo demanda concurrente, volúmenes altos o condiciones superiores a la operación esperada, cuando aplique.
Pruebas de compatibilidad	Validan funcionamiento en plataformas, navegadores, dispositivos, versiones o componentes soportados institucionalmente.
Pruebas de interoperabilidad	Verifican intercambio de información, contratos de servicios, formatos, integridad y manejo de errores entre sistemas.
Pruebas de integridad y calidad de datos	Validan consistencia, completitud, transformación, migración y reglas aplicables a la información procesada.
Pruebas de usabilidad y accesibilidad	Evalúan facilidad de uso, comprensión, navegación y cumplimiento de criterios de accesibilidad aplicables.
Pruebas de seguridad	Incluyen, según riesgo, validaciones de autenticación, autorización, sesiones, cifrado, configuración, análisis de vulnerabilidades, SAST, DAST, dependencias y pruebas de penetración controladas.

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

7.3 Fases de la gestión de pruebas

1) Planear las pruebas: Definir objetivos, alcance, tipos de prueba, responsables, cronograma, criterios de entrada y salida, ambientes, datos, herramientas y evidencias. El plan deberá alinearse con GINFO-G-015 Guía del Plan de Pruebas de Software.
2) Diseñar casos y escenarios: Construir los casos de prueba a partir de requerimientos funcionales y no funcionales aprobados, incluyendo condiciones previas, datos, pasos, resultados esperados y criterios de aceptación. Se deberán contemplar escenarios positivos, negativos, alternos y de error cuando correspondan.
3) Preparar ambientes y datos: Verificar disponibilidad y configuración del ambiente, servicios, integraciones, perfiles, datos y demás condiciones necesarias para ejecutar las pruebas de forma controlada y sin comprometer información sensible.
4) Ejecutar las pruebas: Realizar las validaciones planificadas, comparar resultados reales frente a los esperados y conservar evidencia suficiente, verificable y trazable.
5) Registrar y gestionar hallazgos: Documentar los defectos, vulnerabilidades o desviaciones identificados, asignar severidad y prioridad, establecer responsables y hacer seguimiento hasta su corrección, tratamiento o aceptación formal del riesgo cuando corresponda.
6) Reejecutar y validar: Ejecutar nuevamente los casos afectados por correcciones y realizar pruebas de regresión proporcionales al impacto para verificar que el ajuste sea efectivo y no genere afectaciones colaterales.
7) Cerrar el ciclo de pruebas: Consolidar resultados, evidencias, hallazgos resueltos y pendientes, riesgos residuales, aceptación funcional y lecciones aprendidas. El cierre deberá soportar la decisión de continuar o no hacia el paso a producción.



La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

7.4 Preparación de ambientes y datos de prueba

- Los ambientes de prueba deberán estar separados del ambiente productivo y contar con configuraciones controladas, trazables y coherentes con la arquitectura de la solución.
- Los accesos deberán asignarse bajo principio de mínimo privilegio y limitarse a las personas y servicios requeridos para la ejecución de las pruebas.
- Los datos de prueba deberán ser simulados o anonimizados cuando sea posible. El uso de información real, personal, reservada o sensible requerirá autorización y controles institucionales de protección, enmascaramiento y custodia.
- Las pruebas que puedan afectar disponibilidad, integraciones, capacidad o seguridad deberán ejecutarse en ambientes controlados y bajo coordinación con las dependencias técnicas responsables.
- Las pruebas de penetración o actividades que impliquen explotación controlada de vulnerabilidades deberán contar con autorización previa, alcance definido y medidas para evitar impactos sobre otros servicios o información institucional.
- Deberán conservarse evidencias de versión desplegada, configuración relevante, fecha de prueba y datos utilizados cuando estos elementos sean necesarios para reproducir el resultado.

7.5 Gestión de hallazgos y criterios de aceptación

Todo hallazgo deberá registrarse en la plataforma institucional definida (actualmente Azure DevVops), relacionándolo con el requerimiento, caso de prueba o componente afectado. El registro deberá incluir como mínimo descripción, evidencia, severidad, prioridad, responsable de atención, estado y resultado de la validación posterior. (Los hallazgos no deberán gestionarse en hojas de cálculo ni en archivos aislados)

La severidad podrá clasificarse como crítica, alta, media o baja considerando impacto funcional, técnico, de seguridad, privacidad, disponibilidad e integridad de la información. Los criterios específicos de priorización podrán complementarse con los lineamientos de seguridad y gestión de riesgos vigentes.

Los hallazgos críticos o altos que comprometan requisitos esenciales, seguridad, integridad de datos o continuidad deberán ser tratados antes del paso a producción. Cuando subsista un riesgo residual, su aceptación deberá quedar formalmente documentada por la instancia competente de acuerdo con los lineamientos institucionales aplicables.

Una solución podrá considerarse aprobada para continuar al paso a producción cuando se hayan ejecutado las pruebas definidas, se cumplan los criterios de aceptación, los hallazgos bloqueantes estén cerrados o tratados, exista evidencia suficiente y se cuente con las validaciones técnicas y funcionales requeridas. La Lista de Chequeo Paso a Producción GINFO-F-033 deberá utilizarse cuando corresponda.

7.6 Técnicas y herramientas de apoyo

Las herramientas utilizadas deberán estar autorizadas por la entidad y ser compatibles con la arquitectura, los controles de seguridad y las condiciones del proyecto. La selección no deberá generar dependencia innecesaria de una tecnología específica y podrá ajustarse según las capacidades institucionales.

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

Uso	Tipo de herramienta	Aplicación
Gestión y trazabilidad	Plataforma institucional de gestión de requerimientos y desarrollo	Registrar casos, resultados, hallazgos, tareas, evidencias y estados del ciclo de prueba.
Automatización funcional y API	Herramientas autorizadas de automatización de interfaz y servicios	Ejecutar validaciones repetibles, regresiones y pruebas de contratos de servicios.
Carga y rendimiento	Herramientas autorizadas de generación de carga y medición	Medir tiempos de respuesta, concurrencia, consumo de recursos y estabilidad.
Análisis estático y dependencias	Herramientas SAST y análisis de composición de software autorizadas	Detectar debilidades en código, dependencias vulnerables y prácticas inseguras.
Análisis dinámico	Herramientas DAST y escaneo autorizado	Identificar vulnerabilidades sobre aplicaciones en ejecución.
Integración continua	Pipelines institucionales de construcción y despliegue	Automatizar pruebas y controles asociados a cambios de código y entregas.
Evidencias técnicas	Repositorios institucionales y reportes generados por herramientas	Conservar resultados de forma trazable, versionada y disponible para revisión.

7.7 Integración con prácticas DevSecOps

Cuando el modelo de desarrollo y las capacidades tecnológicas lo permitan, las pruebas deberán integrarse de forma continua a los procesos de construcción y despliegue, con el propósito de detectar defectos y riesgos de seguridad de manera temprana. La automatización deberá complementar, y no sustituir, las validaciones funcionales, técnicas y de aceptación que requieran análisis humano.

- Ejecutar pruebas unitarias y de integración como parte de los procesos de integración continua.
- Incorporar análisis de calidad, SAST y revisión de dependencias antes de promover una versión a ambientes posteriores.
- Utilizar las herramientas automatizadas de seguridad de aplicaciones para detectar vulnerabilidades en distintas fases del desarrollo de software que la SSIT defina como institucionales y registre en el GINFO-G-020 Framework Tecnológico para los Sistemas de Información Institucional, para consolidar resultados comparables entre proyectos.
- Ejecutar pruebas automatizadas de API, interfaz y regresión sobre ambientes intermedios cuando aplique.
- Aplicar análisis dinámico y controles de configuración en ambientes de prueba o preproducción autorizados.
- Gestionar secretos, credenciales y variables de configuración mediante mecanismos institucionales seguros, evitando su incorporación al código fuente.
- Mantener trazabilidad entre la versión del código, resultados de pruebas, hallazgos y artefactos desplegados.
- Definir umbrales o controles de calidad que permitan detener una promoción cuando existan incumplimientos críticos.

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

7.8 Roles y responsabilidades

Actor	Responsabilidades principales
Subdirección de Sistemas de Información de Tierras	Coordinar la estrategia de pruebas, validar el alcance técnico, asegurar la trazabilidad, revisar resultados y articular las decisiones relacionadas con aceptación y paso a producción.
Dependencia solicitante o funcional	Definir y validar criterios de aceptación, participar en pruebas funcionales y UAT, confirmar reglas de negocio y emitir la aceptación o las observaciones correspondientes.
Responsables de desarrollo	Ejecutar pruebas unitarias y de integración, corregir hallazgos, apoyar automatización y suministrar artefactos y evidencias técnicas requeridas.
Responsables de arquitectura e infraestructura	Validar condiciones de ambiente, compatibilidad, integraciones, capacidad, configuración y demás aspectos técnicos requeridos para las pruebas.
Responsables de seguridad de la información	Definir o validar los controles y pruebas de seguridad aplicables según riesgo, analizar hallazgos relevantes y orientar su tratamiento.
Proveedor o contratista	Cuando el desarrollo sea tercerizado, ejecutar y documentar las pruebas que le correspondan contractualmente, entregar evidencias, corregir hallazgos y atender las validaciones de la ANT sin sustituir la aceptación institucional.
Responsable de pruebas o rol equivalente	Diseñar casos, ejecutar o coordinar validaciones, registrar resultados y hallazgos, realizar reejecuciones y consolidar el informe de pruebas, de acuerdo con la organización definida para cada iniciativa.

8 ENTREGABLES DE LA GESTIÓN DE PRUEBAS

Los entregables deberán generarse de acuerdo con la naturaleza y alcance de la iniciativa y conservarse en los repositorios institucionales definidos, manteniendo su relación con los requerimientos, versiones y decisiones del proyecto. Como mínimo se deberán considerar los siguientes:

- **Plan de pruebas:** Define alcance, tipos de prueba, ambientes, datos, cronograma, responsabilidades, criterios de entrada y salida, herramientas y evidencias. Deberá elaborarse conforme a GINFO-G-015.
- **Casos y escenarios de prueba:** Documentan condiciones iniciales, datos, pasos, resultados esperados, criterios de aceptación y resultado de ejecución.
- **Registro de evidencias:** Conserva soportes verificables de la ejecución, como capturas, registros de eventos, archivos, reportes o resultados de herramientas.
- **Registro de hallazgos y seguimiento:** Permite rastrear defectos, vulnerabilidades o incumplimientos desde su identificación hasta su corrección, validación o tratamiento formal.
- **Informe de resultados de pruebas:** Consolida alcance ejecutado, estado de casos, hallazgos, riesgos residuales, cumplimiento de criterios y recomendación de aceptación o rechazo.
- **Evidencia de aceptación funcional:** Registra la validación de la dependencia funcional o usuarios designados. Para soluciones de terceros podrá complementarse con GINFO-F-050 cuando aplique.
- **Evidencias de seguridad y técnicas:** Incluyen reportes de análisis, resultados de rendimiento, integraciones, seguridad, accesibilidad u otras pruebas especializadas requeridas por la solución.
- **Lecciones aprendidas:** Registra aprendizajes, oportunidades de automatización, defectos recurrentes y acciones de mejora para ciclos posteriores.

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

Los resultados y evidencias de pruebas constituyen insumos para las actividades de aceptación, despliegue y paso a producción establecidas en GINFO-P-003 Construcción de Software y deberán mantenerse disponibles para seguimiento, auditoría y mejora continua.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
06/03/2026	01	Creación inicial del instructivo para estandarizar la gestión de pruebas funcionales, técnicas y de seguridad de los sistemas de información.
13/11/2026	02	Se actualiza integralmente el instructivo para armonizarlo con los lineamientos institucionales vigentes del ciclo de vida de sistemas de información y la Gestión de la Información Documentada. Se fortalecen los criterios, tipos y fases de prueba, la gestión de ambientes, datos y hallazgos, las prácticas DevSecOps, los roles y entregables, incorporando de manera transversal arquitectura, seguridad, privacidad, trazabilidad y criterios aplicables a desarrollos internos y tercerizados.

APROBACIÓN				
	NOMBRE	**CARGO**	**FIRMA**	**FECHA**
ELABORÓ	Jerson Eguis Berrio	Contratista – Subdirección de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	25/08/2026
REVISÓ	Liliam Cárdenas Diaz	Contratista – Subdirección de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	11/09/2026
APROBÓ	Adriana María Bolaños Méndez	Subdirectora de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	13/11/2026

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia.

La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.