ESCUELA
POLITÉCNICA
NACIONAL

Política de Pruebas de Aceptación del Sistema

Código	Política de Pruebas de Aceptación del Sistema
Versión:	1.0.0
Fecha de la versión:	23-02-2023
Creado por:	Grupo
Aprobado por:	Líder
Nivel de confidencialidad:	Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
23/02/2023	1.0.0	Grupo	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo de esta política es establecer los procedimientos y estándares para las pruebas de aceptación del sistema, incluyendo pruebas funcionales y de seguridad fuera del entorno de operación, con el fin de garantizar la calidad y fiabilidad del sistema.

2. Política de Pruebas de Aceptación del Sistema

Se debe tomar en cuenta los siguientes procedimientos:

1. Planificación de las pruebas: Se debe elaborar un plan detallado de pruebas que incluya los objetivos de estas, las áreas del sistema que serán evaluadas, los recursos necesarios y el calendario de ejecución. El plan debe ser aprobado por el equipo de desarrollo y por los responsables de la gestión del proyecto.
2. Diseño de las pruebas: Se deben diseñar pruebas que cubran todos los aspectos funcionales y de seguridad del sistema, identificando los posibles riesgos y vulnerabilidades. Las pruebas deben ser realistas y reproducibles.
3. Ejecución de las pruebas: Las pruebas deben ser ejecutadas por personal calificado y experimentado, que siga los procedimientos y estándares establecidos. Las pruebas funcionales y de seguridad deben ser realizadas en entornos de prueba separados del entorno de operación.
4. Análisis de los resultados: Los resultados de las pruebas deben ser analizados con detalle, identificando los problemas y posibles soluciones. Se deben documentar los resultados y las decisiones tomadas.
5. Informe final: Se debe elaborar un informe final que incluya los resultados de las pruebas y las conclusiones. El informe debe ser presentado al equipo de desarrollo y a los responsables de la gestión del proyecto, para su revisión y aprobación.

Recomendaciones y lineamientos para realizar un buen plan de pruebas de seguridad:

- Se deben seguir los estándares y normas internacionales de pruebas de software.
- Las pruebas deben ser diseñadas y ejecutadas por personal calificado y experimentado.
- Las pruebas deben ser documentadas en detalle y los resultados deben ser analizados cuidadosamente.
- Se deben seguir los procedimientos y estándares establecidos en el plan de pruebas.
- Se recomienda utilizar herramientas de automatización de pruebas para aumentar la eficiencia y precisión de las pruebas.
- Se recomienda realizar pruebas de penetración para identificar posibles vulnerabilidades de seguridad.
- Se recomienda involucrar a los usuarios finales en las pruebas para asegurar que el sistema cumpla con sus requisitos y expectativas.

3. Validez y gestión de documentos

Este documento es válido hasta el año 2026.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de obligaciones de la organización que ya existían pero que no fueron identificadas.
- Cantidad o monto de multas pagadas por el no cumplimiento de obligaciones.
- Cantidad de días de atraso en el cumplimiento de la obligación.

Líder
[firma]