ESCUELA
POLITÉCNICA
NACIONAL

Política de Pruebas de Seguridad del Sistema

Código	Política de Pruebas de Seguridad 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 un plan de pruebas de seguridad para evaluar la seguridad de nuestro sistema.

2. Política de Pruebas de Seguridad del Sistema

Se debe tomar en cuenta los siguientes procedimientos:

1. Definir el alcance de las pruebas, identificando los componentes y sistemas que se van a evaluar.
2. Identificar los riesgos y amenazas a los que está expuesto el sistema, estableciendo un análisis de vulnerabilidades.
3. Diseñar los casos de prueba, en los que se definan los objetivos de cada prueba y los pasos a seguir para su ejecución.
4. Ejecutar las pruebas, registrando los resultados y las incidencias encontradas.
5. Evaluar los resultados de las pruebas y establecer medidas correctivas en caso de ser necesario.

Es importante realizar las pruebas de seguridad de forma periódica y cada vez que se realicen cambios importantes en el sistema. Además, se deben utilizar herramientas de seguridad para automatizar las pruebas y garantizar una evaluación más rigurosa.

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

- Identificar los activos críticos y definir los objetivos de seguridad que se quieren lograr.
- Identificar las amenazas y vulnerabilidades del sistema para priorizar las pruebas de seguridad.
- Establecer un equipo de pruebas de seguridad con expertos en seguridad y conocimiento técnico.
- Definir los tipos de pruebas de seguridad que se van a realizar (penetración, análisis de vulnerabilidades, pruebas de intrusión, etc.).
- Establecer los criterios de aceptación para determinar si los resultados de las pruebas de seguridad son satisfactorios.
- Establecer un plan de contingencia en caso de que se detecten fallas de seguridad durante las pruebas.
- Establecer un plan de seguimiento para garantizar que las fallas detectadas sean corregidas.
- Realizar pruebas de seguridad de manera regular para asegurarse de que se mantengan los niveles de seguridad adecuados.
- Documentar todas las actividades relacionadas con las pruebas de seguridad, incluyendo los resultados de las pruebas, los procedimientos utilizados, y las medidas tomadas para remediar las fallas.
- Garantizar que los resultados de las pruebas de seguridad se compartan con los miembros relevantes de la organización, para que puedan tomar medidas apropiadas.

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]