# Evaluación N°4

## Ejecución práctica de pruebas de testing e informe de testeo

- Tipo: Evaluación Sumativa – Grupal
- Ponderación: 25%
- Modalidad: Práctica aplicada y análisis técnico
- Fecha de entrega: 10-12-2025 23:00 hrs Vía Plataforma

## Descripción de la Actividad

Los estudiantes deberán probar, testear y validar el prototipo de software desarrollado en la evaluación anterior.
El objetivo es verificar la calidad, confiabilidad y seguridad del sistema, mediante la ejecución de pruebas funcionales, unitarias y de seguridad, documentadas en planes de pruebas estructurados y respaldadas con evidencias de ejecución real.

Esta evaluación se centra exclusivamente en la documentación, resultados y análisis de las pruebas realizadas, no en la entrega del código fuente.

## Objetivos de Aprendizaje

- 3.1.3 Produce un prototipo de software aplicando buenas prácticas OWASP y normativa legal vigente.
- 3.1.4 Genera diagramas UML apropiados a la estructura, comportamiento o interacción del sistema, adaptando roles y metodologías.
- 3.1.5 Realiza la corrección del código a partir de los resultados de las pruebas de testing, aplicando los estándares de seguridad ISO 27000.

## Instrucciones de desarrollo

1. Diseño y ejecución de pruebas:
   - Elaboren tres planes de prueba, uno por cada tipo:
     - Pruebas funcionales: Validan el correcto funcionamiento de cada módulo o flujo principal del sistema.
     - Pruebas unitarias: Evalúan métodos, clases o componentes específicos del código.
     - Pruebas de seguridad: Comprueban validaciones de entrada, autenticación, roles, cifrado, y buenas prácticas OWASP.

- Cada plan de prueba debe incluir al menos 10 casos documentados con la siguiente estructura mínima:

| ID Prueba | Descripción | Tipo de prueba | Resultado esperado | Resultado obtenido | Estado (Aprobado / Rechazado) | Evidencia (captura o enlace) |

2. Ejecución y registro de evidencias:
   - Cada caso de prueba debe contar con una evidencia de ejecución correcta, como:
     - Captura de pantalla, consola o log del sistema.
     - Reporte generado por herramienta de testing (por ejemplo, JUnit, Postman, Selenium, Jest, etc.).
   - Las evidencias deben estar claramente etiquetadas y numeradas según el ID del plan de prueba.

3. Informe técnico (formato PDF):
   El informe debe incluir:
   - Portada con nombre del grupo, asignatura y evaluación.
   - Descripción general del sistema bajo prueba.
   - Explicación del objetivo y alcance de cada tipo de test.
   - Resumen de resultados (porcentaje de éxito/falla).
   - Principales errores detectados y acciones correctivas aplicadas.
   - Diagramas UML actualizados (clases, secuencia o actividades).
   - Referencias a OWASP e ISO 27000 utilizadas como guía de buenas prácticas.

4. Corrección y análisis:
   - En el informe, describan brevemente las mejoras o correcciones que realizaron tras las pruebas (no se entrega el código, solo el análisis de los cambios).

## Entregables

1. Informe técnico en formato PDF, que contenga:
   - Descripción del proceso de testing y análisis de resultados.
   - Diagramas UML actualizados.
   - Resumen de mejoras y conclusiones.
   - Referencias a OWASP e ISO 27000.

2. Anexo de planes de prueba ejecutados, en formato PDF o Excel:
   - Mínimo 10 pruebas por cada tipo (funcional, unitaria, seguridad).
   - Cada prueba debe incluir su evidencia de ejecución correcta.

## Rubrica de Evaluación

| Criterio | Excelente | Bueno | Básico | Insuficiente | Pts |
|---|---|---|---|---|---|
| **1. Planes de Prueba (Funcionales, Unitarias y Seguridad)** | Presenta los **3 planes de prueba**, cada uno con **≥10 casos**, completamente documentados (ID, descripción, tipo, esperado, obtenido, estado, evidencia). Redacción clara y sin omisiones. | Presenta los 3 planes, pero con pequeñas omisiones (1–2 casos incompletos o evidencia poco clara). | Planes incompletos (<10 casos por tipo) o con estructura débil; evidencias incompletas o confusas. | No presenta los 3 planes, o la estructura es incorrecta; falta la mayoría de los casos o evidencias. | **8 pts** |
| **2. Evidencias de Ejecución** | Todas las evidencias están claras, legibles, numeradas y asociadas a cada caso. Incluye capturas, logs o reportes de herramientas de testing. | Evidencias correctas, pero con algunos problemas de claridad o etiquetado. | Evidencias poco claras, sin numeración o faltantes. | Evidencias ausentes o no corresponden a los casos. | **5 pts** |
| **3. Informe Técnico en PDF** | Informe completo y profesional: incluye descripción del sistema, objetivos, alcance de pruebas, análisis cuantitativo, resumen de éxito/falla, conclusiones, UML actualizado, y referencias OWASP/ISO. | Informe adecuado, con leves omisiones (por ejemplo: falta algún diagrama o análisis numérico). | Informe incompleto o superficial; faltan varias secciones. | Informe insuficiente, sin estructura, sin análisis o sin UML. | **7 pts** |
| **4. Análisis de Resultados y Acciones Correctivas** | Identifica claramente errores, fallas y riesgos. Explica causas, impacto y acciones de mejora basadas en OWASP e ISO 27000. | Describe errores y mejoras, pero con menor profundidad o detalle. | Identificación superficial de errores y mejoras. | No identifica errores ni propone mejoras. | **3 pts** |
| **5. Diagramas UML Actualizados** | Diagramas completos, correctos y alineados a los cambios detectados durante el testing. | Diagramas correctos pero con pequeños detalles o desactualizados parcialmente. | Diagramas incompletos o con errores. | No presenta diagramas UML. | **2 pts** |