INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

LINEAMIENTOS PARA LA EJECUCIÓN DEL TESTING

Versión:	1.0.0
Fecha de la versión:	05/11/2018
Elaborado por:	Juan Luis Jr Vargas Mayurí
Revisado por:	Arlett Agüero Vargas
Aprobado por:	Ing. CIP Manuel Matos Alvarado

1. OBJETIVOS

Establecer los lineamientos para la ejecución de las pruebas de los sistemas y aplicativos desarrollados en el INEI, a ser realizado por el personal a cargo de Testing de la Unidad de Calidad, Procesos y Seguridad de la Información, en adelante UCAPSI.

2. RESPONSABLE DEL CUMPLIMIENTO

El Jefe de la UCAPSI, y personal a cargo de Testing, son responsables de seguir con los lineamientos descritos en el presente documento.

3. LINEAMIENTOS

3.1. LINEAMIENTO GENERAL

Considerando las etapas de Preparación y Ejecución del Testing, el personal a cargo de realizar las pruebas de los sistemas al no contar con el tiempo para la ejecución del testing y muchas veces al no haberse incluido el proceso de Testing en el cronograma del proyecto, no siempre se pueden ejecutar las pruebas establecidas en este lineamiento, por ello el jefe de la UCAPSI o el personal de Testing de la OTIN deberá ponerse de acuerdo de antemano con el equipo encargado del desarrollo sobre el tiempo disponible que tendrán para realizar el testing, asimismo debido a esta falta de tiempo el equipo de Testing hace uso del enfoque de caja negra el cual se limita a la revisión de las funcionalidades del sistema y la codificación es algo transparente.

3.2. LINEAMIENTO ESPECÍFICO

3.2.1. MÉTODO USADO PARA TESTING

El método usado para el Testing de las aplicaciones será: Caja Negra, el cual consiste en la revisión de la funcionalidad del sistema, haciendo uso de un INPUT (entrada) se revisa el OUTPUT (salida), si el OUTPUT corresponde al resultado esperado, entonces la funcionalidad es correcta.

3.2.2. TIPOS DE PRUEBA

Así mismo dentro de las Funcionales, el tipo de prueba que se ejecutan son las siguientes:

- Pruebas Exploratorias: Este tipo de prueba se suele ejecutar a menudo debido que los sistemas desarrollados en el INEI no suelen crear su documentación, por ello se explora el sistema con el fin de comprender la funcionalidad del sistema.
- Pruebas de Regresión: Este tipo de prueba se ejecuta debido a los constantes cambios que suele haber durante el desarrollo del software y después del desarrollo del software (luego del cierre del proyecto).
- Pruebas de Integración: Este tipo de prueba se ejecutan si el sistema interactúa o depende de otro sistema, actualmente en el INEI se integran diversos sistemas con múltiples lenguajes de programación y Bases de Datos, en este caso los desarrolladores deberán de mencionar si el sistema

tiene una integración con otro en su documentación o en el peor de los casos por correo o verbalmente, dato que será incluido en el informe del Testing.

- Pruebas de Aceptación: este tipo de prueba se utiliza al realizar el Testing de las aplicaciones, ya que debido a que se usa el enfoque de prueba de Caja Negra es fundamental revisar la funcionalidad del sistema.

3.2.3. HERRAMIENTAS

Actualmente las herramientas utilizadas por el personal de Testing son las siguientes:

- OWASP: Herramienta para escanear vulnerabilidades.
- SQLMAP: Herramienta para ejecutar pruebas de inyección SQL.
- NMAP: Herramienta para escanear puertos y encontrar vulnerabilidades a nivel de RED.
- JMETER: Herramientas para crear y ejecutar Pruebas de rendimiento en aplicaciones Web.
- POWER BI: Herramienta que permite crear dashboard, se usa para mejorar los reportes del JMETER.

3.2.4. PREPARACIÓN

a. Todo software que sea desarrollado por personal del INEI antes de ser publicado deberá pasar a la UCAPSI para ser testeado por el personal a cargo de Testing de la OTIN, excepto que en caso de carácter urgente el Director Técnico de OTIN autorice el pase a producción y el proyecto asuma la responsabilidad de los futuros incidentes que ocurran con el sistema presentando su debida justificación. Otro caso por el cual se podría pasar el sistema a producción sin ser testeado, es que el proyecto asuma la responsabilidad de los futuros incidentes que ocurran con el sistema, presentando su debida justificación para lo cual el proceso de Testing se realiza en paralelo.

b. Es necesario conocer el funcionamiento del sistema, por ello el personal a cargo de realizar el testing analizarán los documentos (manual de sistema, requerimientos funcionales, manual de usuario u otro documento que contenga los mismos fines de informar los requerimientos o funcionalidades del sistema) que el Jefe de Proyecto les proporcionen del sistema caso contrario se requerirá socializar con el equipo encargado del desarrollo del proyecto.

c. Para actualizaciones de sistemas, el Jefe del proyecto debe remitir el documento de Control de Cambios (ANEXO 01) con el fin que el equipo de testing tenga conocimiento del cambio que se ha ejecutado, inclusive cuando requieran el pase a producción sin ser testeado bajo responsabilidad del proyecto, para que el testing pueda realizarse en paralelo al pase a producción.

d. El Testing debe ejecutarse en ambientes de QA, de no poderse excepcionalmente se deberá de analizar y coordinar con los responsables del proyecto para ejecutarse en los ambientes de desarrollo, producción o Local justificando dicha acción ante el DT de la OTIN.

3.2.5. EJECUCIÓN

3.2.5.1. PRUEBAS FUNCIONALES

a. Es necesario revisar la página principal del sistema, la cual suele ser una presentación del sistema o un Login. Tanto el titulo como la descripción del sistema debe hacer referencia al sistema proporcionado.
b. En todo tipo de sistema se deberá de revisar la ortografía del sistema, dando más énfasis en los menús de navegación, títulos, encabezados de tablas que suelen tener mayor probabilidad de error ortográfico por parte de los desarrolladores.
c. Se deberá de revisar por medio de la consola del browser que no falte ningún elemento en las páginas o sistemas web debido a que al enviarse las fuentes puede no incluirse algunos elementos como imágenes, fuentes (fonts), estilos (css) o puede existir un mal direccionamiento de los elementos.
d. Se deberá de revisar que el sistema sea totalmente responsivo (que la visualización del sistema se aprecie sin la necesidad de hacer zoom en dispositivos de diferentes resoluciones y que su navegabilidad solo sea verticalmente).
e. Cuando el sistema es responsivo se suele ocultar ciertos elementos de la página, se deberá de analizar si estos objetos son fundamentales o no, o qué otros elementos deben ser ocultados.

3.2.5.1.1. PÁGINAS INFORMATIVAS

a. En el caso de ser solo una página informativa, que no posee login (Ingreso al sistema) ni ninguna interacción con la BD, se tendrá que revisar cada una de las vistas (sea por medio del menú de navegación, enlaces o imágenes hipervinculadas) y opciones de la página.
b. En caso que el sistema tenga alguna interacción con la BD, se deberá de revisar cómo se invoca estos datos con el fin de prevenir una posible inyección.

3.2.5.1.2. SISTEMAS INFORMATICOS

a. Validar los roles y perfiles según sus permisos, descritos en la documentación proporcionada por el jefe de proyecto o desarrolladores del sistema.
b. Validar la autenticación login, accesos y permisos con un usuario aleatorio de cada rol y perfil que será proporcionados por el jefe del proyecto o los desarrolladores.
c. Validar que el sistema no permita saltarse el login del sistema haciendo uso de un URL interna del sistema sin tener actica una sesión del login.
d. Validar que en la página de logeo en los campos de usuario y la contraseña no haya valores por defecto (vacío).
e. Validar que el sistema muestre un mensaje "USUARIO/CONTRASEÑA INCORRECTO" al ingresar en los campos usuario y contraseña los siguientes valores:

'	1=1	'1=1	'1=1'	A=A	'A=A	'A=A'	'1'='1'	'A'='A'	'& 'a'='a'

Si el sistema muestra algún mensaje "error de ODBC" entonces existe una gran posibilidad de que pueda ser inyectable, el personal de Testing deberá reportar al jefe de proyecto o desarrolladores sobre esta incidencia y luego ejecutar las pruebas de inyección SQL.

f. Durante la prueba en todo momento se deberá de verificar la URL de browser y corroborar que no se esté mostrando ningún parámetro, de ser el caso que se muestre un parámetro se deberá de incluir en el reporte de incidencias, más aún si se trata de un ID.

g. Para el caso de variación de un formulario de ingreso de datos, se deberá de validar cada uno de los campos que en el formulario se presente, para ello hacer uso de la siguiente tabla de validación.

<table>
<tr><th>TIPO DE CAMPO</th><th>VALIDACIÓN</th></tr>
<tr><td>Texto</td><td>Se deberá de validar que el sistema solo permita ingresar los caracteres que se requieran, de no ser necesarios se deberá de reportar. CARACTERES ESPECIALES:
<table>
<tr><td>'</td><td>{</td><td>}</td><td>[</td><td>]</td><td>,</td><td>;</td><td><</td><td>></td></tr>
<tr><td>/</td><td>*</td><td>-</td><td>+</td><td>.</td><td>-</td><td>_</td><td>¡</td><td>""</td></tr>
<tr><td>(</td><td>)</td><td>\</td><td>%</td><td>$</td><td>#</td><td></td><td></td><td>Etc.</td></tr>
</table>
Si es un sistema de captura de datos y monitoreo, al ingresar los siguientes comandos y guardarlos:
<h1>QA</h1>
<script>alert("QA")</script>
"><h1>QA</h1>
Para Luego entrar al módulo de monitoreo, si estos comandos se ejecutan en el módulo de monitoreo entonces el sistema es vulnerable a ataques XSS, exactamente CROSS SITE SCRIPTIN y deberá ser reportado a los desarrolladores como una incidencia de Grado Alta. "Generalmente esto suele ocurrir cuando se reportan en un dataTable"</td></tr>
</table>

TIPO DE CAMPO	VALIDACIÓN
	En caso que sea un formulario de guardar y editar, se deberá de grabar y actualizar, para comprobar esta vulnerabilidad. También tendrá que validarse el tamaño de longitud de campo.
FECHA	Validar que se cumpla la regla correspondiente a las fechas según el requerimiento (condicionales, reglas de flujo), se deberá de probar que no permita ingresar cualquier otro tipo de dato que no sea el correspondiente al formato de fecha (dd/mm/aaaa), validar los rangos de fecha si el requerimiento lo solicita, verificar si la fecha y hora capturadas son local o del servidor. De no ser la fecha del servidor deberá ser reportado excepto que lo amerite porque al estar consultándose cada intervalo de tiempo con el servidor representa un consumo de recursos.
NUMÉRICO	Validar que el sistema no permita ingresar otros tipos de caracteres distintos al numérico, se tendrá que revisar si es lógico o si se requiera el ingreso de números negativos. También la longitud del campo.
BLOQUEADO	En el caso que, un formulario de Guardar y Editar, muestre un campo Bloqueado se deberá de corroborar si se está enviando o no este campo, ya que puede ser posible su edición por medio de la consola. De ser el caso deberá de reportarse.

h. Al guardar la información de un formulario deberá de validarse qué parámetros se están enviando en la consola del Browser, verificar que no se esté mandando ninguna consulta a la BD directamente o algún procedimiento.

i. verificar los campos que se bloquean, desbloquean o habiliten por condiciones o reglas de flujo, según indique los requerimientos.

j. Si el sistema genera un PDF o Excel, se deberá verificar si este documento cumple la estructura requerida, normalmente los sistemas que muestran reporte en sus módulos, se basan en la estructura del dataTable para generar el formato.

k. En el caso que el sistema presente la funcionalidad de cargar archivos, sea Excel, XML u otro formato, se deberá de probar que el sistema solo permita subir los archivos del tipo requerido más no otros tipos. En el caso que eso suceda se deberá de reportar como una incidencia de grado ALTA.

l. Al probarse alguna funcionalidad del sistema que interactúe con la BD y demore más de 2 segundos esto también deberá de incluirse en el reporte de incidencias, existe un gran

posibilidad que esto pueda causar perdida de datos debido al cuello de botella (cola de solicitudes en espera de respuesta por parte del servidor) si es que posee demasiado concurrencia.

m. Verificar el evento de deslogeo del sistema, ya que algunas veces no permite el deslogearse o también apunte a otra página de login de otro sistema.

3.2.5.2. NO FUNCIONAL

a. Si el sistema tiene un requerimiento de deslogeo por inactividad programado en X minutos o segundos, se deberá de validar este requerimiento.
b. Si el sistema posee el requerimiento de recargarse cada X minutos o segundos, se deberá de efectuar un análisis de qué tan pesada es la actualización de esa sección del sistema.
c. Si se ha encontrado indicio de Vulnerabilidades se deberá de ejecutar las pruebas no funcionales e informar sobre esta incidencia.
    - Respecto a las pruebas de inyección que corresponde las pruebas de intrusión se deberá de crear el script de inyección y ejecutarse en el SQLMAP
    - También deberá de ejecutarse un escaneo de puertos mediante el NMAP, en el caso de encontrarse puertos abiertos estos se deberán de someter a las pruebas de intrusión usando la herramienta METASPLOIT.
d. Si se ha encontrado indicio de cuellos de botellas se deberá de ejecutar las pruebas de rendimiento e informar sobre la incidencia. Este tipo de pruebas solo se suelen realizar si es solicitado. Dentro de las pruebas de rendimiento se tendrá que seguir los siguientes pasos:
    - Mapear todos los componentes a probar (pueden ser todos los elementos de un sistema, consultas a la BD, o servicios).
    - Para capturar los elementos a probar se deberá de crear un servidor proxy dentro de JMETER.
    - Una vez capturado los elementos se deberá de elaborar el Plan de Pruebas en el JMETER, teniendo en cuenta que cada grupo de Hilos suele representar a un módulo.
    - Los usuarios virtuales y tiempo a simular se deberán de coordinar con los encargados del proyecto para estimar estas cantidades.
    - Para ejecutar las Pruebas de Rendimiento se deberá de coordinar con los administradores Web, de BD y de Redes, con el fin de establecer una hora de ejecución y tomar las medidas de seguridad pertinentes.
    - Una vez ejecutada las pruebas se generará un archivo CSV el cual se deberá de tratar e interpretar para ser reportado.

3.2.6. RESULTADOS

Mantener un registro detallado de las pruebas que se realizan. Luego de completadas las pruebas, enumerar los errores y redactar un informe para que los programadores y jefes de proyectos puedan implementar posteriormente.

CONTROL DE VERSIONES					
Versión	***Hecho por***	***Revisado por***	***Aprobado por***	***Fecha***	***Motivo***

SOLICITUD DE CAMBIO

CÓDIGO Y NOMBRE DEL PROYECTO	CÓDIGO DE LA SOLICITUD DE CAMBIO

DEFINICIÓN DEL PROBLEMA O SITUACIÓN ACTUAL: *DEFINA Y ACOTE EL PROBLEMA QUE SE VA A RESOLVER, DISTINGUIENDO EL PROBLEMA DE SUS CAUSAS, Y DE SUS CONSECUENCIAS.*

DESCRIPCIÓN DETALLADA DEL CAMBIO SOLICITADO: *ESPECIFIQUE CON CLARIDAD EL CAMBIO SOLICITADO, PRECISANDO EL QUÉ, QUIÉN, CÓMO, CUÁNDO Y DÓNDE.*

RAZÓN POR LA QUE SE SOLICITA EL CAMBIO: *ESPECIFIQUE CON CLARIDAD PORQUE MOTIVOS O RAZONES SOLICITA EL CAMBIO, PORQUE MOTIVOS ELIGE ESTE CURSO DE ACCIÓN Y NO OTRO ALTERNATIVO, Y QUÉ SUCEDERÍA SI EL CAMBIO NO SE REALIZA.*

EFECTOS EN EL PROYECTO: *DEFINIR EL EFECTO DEL CAMBIO SOLICITADO A CORTO O LARGO PLAZO EN EL ALCANCE DEL PROYECTO.*

EN EL CORTO PLAZO	***EN EL LARGO PLAZO***

EFECTOS EN OTROS PROYECTOS, PROGRAMAS, PORTAFOLIOS U OPERACIONES INTERNAS

EFECTOS EXTRA EMPRESARIALES EN CLIENTES, MERCADOS, PROVEEDORES, GOBIERNO, ETC.

OBSERVACIONES Y COMENTARIOS ADICIONALES

REVISIÓN DEL COMITÉ DE CONTROL DE CAMBIOS

FECHA DE REVISIÓN	
EFECTUADA POR	
RESULTADOS DE REVISIÓN (APROBADA/RECHAZADA)	
RESPONSABLE DE APLICAR/INFORMAR	
OBSERVACIONES ESPECIALES	

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA - INEI - V° B° Oficina Ejecutiva de Desarrollo de Sistemas - OTIN Bertha Arcondo Huanaco

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TECNICA DE INFORMATICA

INFORME NRO. XXX – 2018/OTIN-JVM

Para : [Jefe Responsable UCAPSI]

De : [Tester de OTIN]

Fecha : [Fecha de emisión del reporte]

Asunto : [Asunto]

Tengo el agrado de dirigirme a usted a fin de remitirle el reporte de las pruebas realizadas al [Nombre del sistema].

Las pruebas fueron efectuadas por el personal de QA a cargo:

- [Nombre del Tester 1]
- [Nombre del Tester 2]

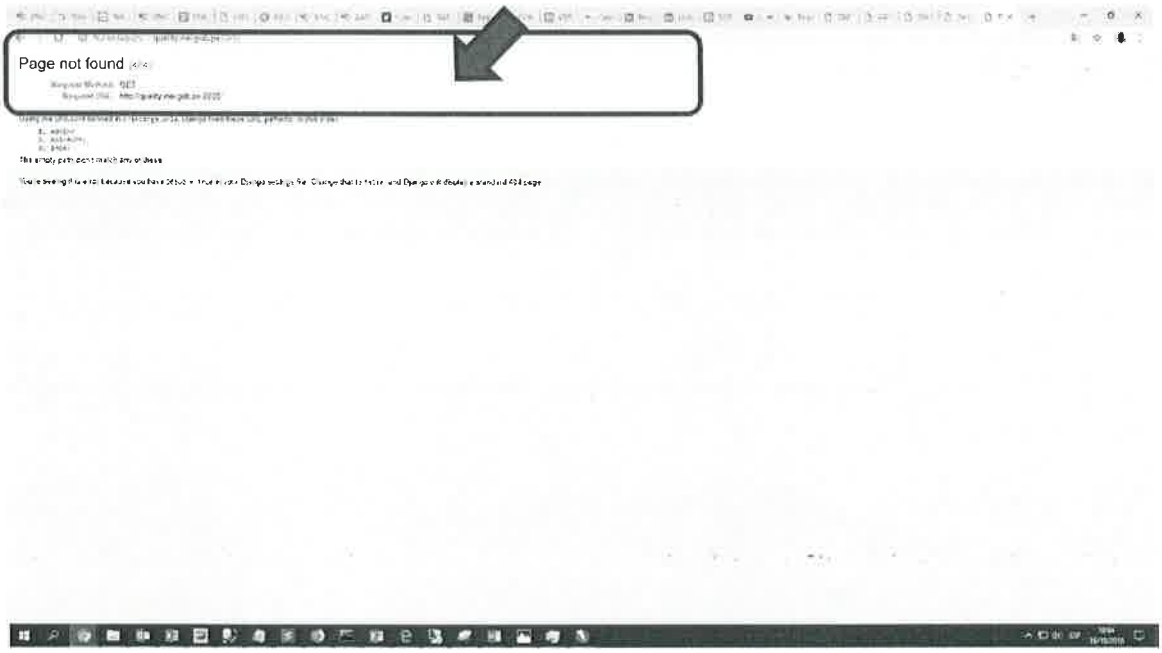
RESUMEN:

	Incidencia de grado Alta, Debe ser Atendido
	Incidencia de Grado Medio, debe ser Atendido
	Incidencia de Grado Bajo, son incidencias de poco impacto o recomendaciones

	Incidencia en estado Atendido que ya fue Atendida, resuelta o Justificada
	Incidencia en estado Pendiente

Nro	GRADO	INCIDENCIA	EVIDENCIA	ESTADO
1	ALTO	[Descripción detallada de la incidencia]	Evidencia_01_1 Evidencia_01_2	PENDIENTE
2	MEDIO	[Descripción detallada de la incidencia]	Evidencia_02_1	PENDIENTE
3	BAJO	[Descripción detallada de la incidencia]	Evidencia_03_1	PENDIENTE
4	MEDIO	[Descripción detallada de la incidencia]	Evidencia_04_1 Evidencia_04_2	ATENDIDO

Evidencia_01_1



INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA
V° B°
Oficina Ejecutiva de Desarrollo de Sistemas - OTDS
Bertha Arcando Huanaco