INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TÉCNICA DE INFORMÁTICA

POLÍTICAS

"POLÍTICA PARA EL DESARROLLO SEGURO DE LOS SISTEMAS DE INFORMACIÓN"

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA
Oficina Técnica de Informática
ELMER PEREZ ESPINOZA

Código: POL-004-OTIN-2018
Versión 1.0.0

POLÍTICA		
NOMBRE DE LA POLÍTICA: POLÍTICA PARA EL DESARROLLO SEGURO DE LOS SISTEMAS DE INFORMACIÓN		
CODIGO: POL-004-OTIN-2018		**VERSION:** 1.0.0
PROCESO AL QUE PERTENECE: Gestión de Programas y Proyectos de TI		
Elaborado por: Unidad Funcional de Calidad, Procesos y Seguridad de la Información	**Coordinado con:** Unidad Funcional de Transformación Digital	**Aprobado por:** Director Técnico de la Oficina Técnica de Informática
Nombre: Ing. Katherine Montenegro Julcapoma	**Nombre:** Ing. Verónica Tejeda León	**Nombre:** Ing. CIP Manuel Matos Alvarado
Fecha: 17/10/2018	**Fecha:** 17/10/2018	**Fecha:** 22 OCT 2018
Firma	**Firma**	**Firma**
INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA V°B° Oficina Técnica de Informática Katherine Montenegro Julcapoma - INEI -		Ing. CIP Manuel Amador Matos Alvarado Director Técnico Oficina Técnica de Informática

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Oficina Técnica de Informática ELMER PEREZ ESPINOZA

TABLA DE CONTENIDO

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA
Oficina Técnica de Informática
ELMER PEREZ ESPINOZA

"POLÍTICÁ PARA EL DESARROLLO SEGURO DE LOS SISTEMAS DE INFORMACIÓN"

1. OBJETIVO

El presente documento tiene como objetivo definir las reglas básicas para el desarrollo seguro de software y sistemas de información en el Instituto Nacional de Estadística e Informática (INEI).

2. ALCANCE

La presente política se aplica al desarrollo y mantenimiento de todos los servicios, arquitectura, software y sistemas de información que forman parte del Sistema de gestión de seguridad de la información (SGSI) del INEI.

3. REFERENCIAS

- Norma NTP-ISO/IEC 27001:2014, capítulos A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1
- Metodología de Gestión de Riesgos
- Política General de Seguridad de la Información

4. ABREVIATURAS Y DEFINICIONES

Las siguientes abreviaturas y definiciones son aplicables para el propósito de este procedimiento:

- ✓ **OTIN:** Oficina Técnica de Informática
- ✓ **POO:** Programación Orientada a Objetos
- ✓ **SGSI:** Sistema de Gestión de Seguridad de la Información
- ✓ **Ataque man in the middle:** Es un ataque en el que el atacante adquiere la capacidad de leer, insertar y modificar a voluntad.
- ✓ **Sistema de Información:** Es un conjunto de elementos interrelacionados con el propósito de prestar atención a las demandas de información de una organización, para elevar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones. (Peña, 2006). Por lo que abarca aplicativos de escritorio y web, archivos APK, softwares, aplicaciones, otros.

5. DESARROLLO Y MANTENIMIENTO SEGURO

5.1. Evaluación de riesgos para el proceso de desarrollo de software

- ✓ Todos los Jefes de Unidad y de Proyectos que desarrollan sistemas de información deben incluir, dentro del Cronograma del Proyecto, el tiempo que se va a emplear para las pruebas de los mismos.
- ✓ La Unidad de Calidad, Procesos y Seguridad de la Información debe realizar la evaluación de las vulnerabilidades técnicas de los sistemas de información a utilizarse en el INEI antes de que éstos sean puestos en Producción.
- ✓ Al introducir una nueva tecnología para el desarrollo de los sistemas de información, se debe realizar una evaluación de los riesgos de seguridad que podría generar su implementación.
- ✓ Se debe implementar la seguridad en el ciclo de vida de desarrollo de un sistema de información, integrando las actividades de seguridad:

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA
Oficina Técnica de Informática
ELMER PEREZ ESPINOZA

a) Los requisitos de seguridad, deben ser definidos al inicio de un proyecto por los Jefes de Proyectos respectivamente.
b) Se debe realizar una revisión de la arquitectura para confirmar que sea segura, esta actividad la debe realizar la Unidad Funcional de Infraestructura Tecnológica.
c) Se debe contar con una metodología de análisis de riesgos y amenazas.
d) Se debe realizar un análisis estático es decir evaluar el software sin ejecutarlo.
e) Los programadores deben realizar una revisión del código fuente y las personas encargadas del testing de las aplicaciones deben registrar las actividades de pruebas de seguridad, penetración dentro de un Plan de Pruebas.

5.2. Asegurar el ambiente de desarrollo

- ✓ Para la generación el ambiente de desarrollo, el Jefe de Proyecto debe identificar los requerimientos de seguridad internos y externos para el desarrollo del proyecto y remitirlos a la Unidad Funcional de Infraestructura Tecnológica de la Oficina Técnica de Informática para poder implementarlos.
- ✓ El ambiente de desarrollo debe encontrarse separado de los ambientes de prueba y producción.
- ✓ Se restringirá el acceso al ambiente de desarrollo para evitar accesos o cambios no autorizados.
- ✓ De ser necesario, el Jefe de Proyecto podrá solicitar la generación de la copia de seguridad del proyecto que se encuentra desarrollando; esta solicitud debe ser remitida al Director Técnico de la Oficina Técnica de Informática encontrándose debidamente justificada.

5.3. Principios de ingeniería segura

- ✓ Se deben aplicar los siguientes principios de ingeniería segura de sistemas de información tanto para el desarrollo de nuevos sistemas como para el mantenimiento de los ya existentes:

a) Nombramiento de las variables:

Camel Case: Se debe de escribir una palabra donde su primera letra está en minúsculas, y la primera letra de las subsiguientes palabras en mayúsculas. Ejemplo: nombreVendedor

b) Programación:

Programación Orientada a Objetos (POO): Paradigma de programación que busca que nuestra forma de programar sea más cercana a la forma como nos relacionamos en nuestro día a día. El nombre de "Orientado a Objetos" se debe a que nuestro código creará objetos que se encargarán de manipular los datos de entrada para así obtener datos de salida. Estos objetos tendrán propiedades y métodos.

c) Diccionario de datos

Se debe desarrollar durante el análisis de flujo de datos y debe contener las características lógicas y puntuales de los datos que se van a utilizar en el sistema que se programa, incluyendo nombre, descripción, alias, contenido y organización

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA
Oficina Técnica de Informática
ELMER PEREZ ESPINOZA

identificando los procesos donde se emplean los datos y los sitios donde se necesita el acceso inmediato a la información.

d) **Metodología de desarrollo:**

Se empleará una metodología basada en la Metodología Ágil Scrum, definiendo un conjunto de prácticas y roles, que puedan tomarse como punto de partida para definir el proceso de desarrollo que se ejecutará durante los proyectos.

e) **Técnicas de autenticación de usuarios**

El usuario y la contraseña: Simple, robusto, incluso rústico, su más grande defecto es que el nivel de seguridad depende directamente de la complejidad de la contraseña.

f) **Control de sesión segura**

Se seguirá la NIST SP800-53, que sugiere cinco controles relacionados con la administración de sesiones:

i. **Control de sesión concurrente:** El sistema de información limitará el número de sesiones simultáneas para cada cuenta definida por la organización y / o tipo de cuenta (usuario privilegiado, usuario no privilegiado, dominio, aplicación específica)
ii. **Bloqueo de sesión:** El sistema de información impedirá un mayor acceso al sistema iniciando un bloqueo de sesión después de un período de tiempo de inactividad (definido por la organización) o al recibir una solicitud de un usuario; y retendrá el bloqueo de la sesión hasta que el usuario restablezca el acceso mediante los procedimientos de identificación y autenticación establecidos.
III. **Terminación de la sesión:** El sistema de información finalizará automáticamente una sesión de usuario después de un periodo de inactividad mayor a 5 minutos.
iv. **Auditoria de sesión:** El sistema de información proporcionará a los usuarios autorizados la capacidad de seleccionar una sesión de usuario para capturar / grabar o ver / escuchar las acciones realizadas en sesión auditada.
v. **Autenticidad de sesión:** El sistema de información protegerá la autenticidad de las sesiones de comunicaciones, la protección de la autenticidad incluye, por ejemplo, la protección contra ataques de man in the middle / secuestro de sesiones y la inserción de información falsa en las sesiones.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Oficina Técnica de Informática ELMER PEREZ ESPINOZA

g) **Validación de datos**

Como mecanismo de seguridad se pueden implementar las alertas a través de mensajes, indicando al usuario el error en los datos ingresados, evitando que los usuarios introduzcan datos no válidos.

✓ Los estándares mínimos de seguridad que todo sistema de información debe cumplir son los siguientes:

a) **Integridad:** La modificación de los datos por personas autorizadas debe quedar registrada, asegurando su precisión y confiabilidad.

b) **Confidencialidad:** Los datos sólo deben ser legibles para las personas autorizadas; la información no debe divulgarse a personas, entidades o procesos no autorizados.

c) **Disponibilidad:** La información ha de estar disponible para las personas, procesos o aplicaciones que deban acceder a ella en el momento en el que lo requieran.

d) **Autenticación:** El generador de la información, o el que acceda o la edite, ha de estar perfectamente identificado en todo momento, de forma unívoca e inequívoca.
Adicionalmente se tiene que considerar que, de acuerdo al grado de confidencialidad de la información, se debe agregar una nueva manera de ingresar al sistema de información (doble autenticación).

e) **Irrefutabilidad (No-Rechazo o No-Repudio)** Imposibilidad, para una persona usuaria, programa o proceso, de negar (rechazar) la autoría de una acción.

5.4. Requerimientos de seguridad

Al adquirir nuevos sistemas de información o al desarrollar o cambiar los vigentes, el Jefe de Proyecto debe documentar los requerimientos de seguridad indicando:

- ✓ **Nombre del sistema de información**
- ✓ **Versión del sistema de información existente.**
  En caso de que se haya adquirido un nuevo sistema de información, se escribirá "Nuevo sistema de información"
- ✓ **Especificación funcional del sistema de información.**
  Es la descripción de qué debería generar el sistema (qué sirve como dato de entrada, cómo se procesa, cuál es el dato de salida); su capacidad, rendimiento, diseño de la interfaz de usuario, etc.
- ✓ **Controles automáticos necesarios.**
  Son los controles del sistema de información; por ejemplo, cómo evitar el acceso no autorizado, los controles para el uso de claves y demás mecanismos de autenticación, requerimientos para copias de seguridad, controles para acceso remoto, requerimientos para llevar registros, cómo se transfieren de manera segura los datos, los mecanismos para verificar la integridad de los datos, los mecanismos de control para enviar y/o recibir datos, garantizar un alto nivel de disponibilidad del sistema, cómo se reportan los errores, controles para garantizar la continuidad del negocio, etc.
- ✓ **Especificaciones**
  Identificar aquellos requerimientos funcionales que tendrán impacto en los aspectos de seguridad de la aplicación (requerimientos de compliance con normativas locales o internacionales), tipo de información que se transmitirá o procesará (información pública o confidencial, datos personales, datos financieros, contraseñas, datos de pago electrónico, etc.).

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Jefa Técnica de Informática ELMER PEREZ ESPINOZA

5.5. Requerimientos de seguridad relacionados con redes públicas

El equipo de desarrollo, liderado por su Jefe de Proyecto debe coordinar con el Administrador Web para implementar controles que eviten:

- ✓ El direccionamiento erróneo.
- ✓ La transmisión de datos incompletos.
- ✓ La modificación no autorizada de datos.
- ✓ La duplicación de datos.
- ✓ La divulgación no autorizada de datos.
- ✓ La denegación de servicios

5.6. Verificación y prueba de la implementación de los requerimientos de seguridad

- ✓ El equipo de desarrollo debe realizar pruebas unitarias de los sistemas de información que desarrollan.
- ✓ Para garantizar un mejor resultado en las pruebas, adicional a las pruebas que realiza el equipo de desarrollo, la Unidad de Calidad, procesos y Seguridad de la Información ejecutará el testing de los sistemas de información.
- ✓ La Unidad de Calidad, procesos y Seguridad de la Información debe definir la metodología, las responsabilidades y los plazos para verificar si se cumplieron todos los requerimientos de la Especificación de requerimientos de seguridad y si el sistema está listo para producción.
- ✓ La Unidad de Calidad, procesos y Seguridad de la Información debe incluir revisiones de seguridad del código fuente con evaluaciones/herramientas utilizando Pruebas de Seguridad de Análisis Estático (Evaluación sin ejecutar el código) y revisiones de seguridad en aplicaciones con Pruebas de Seguridad de Análisis Dinámico (Evaluación ejecutando el código).

5.7. Repositorio

- ✓ Se debe aplicar el Procedimiento Administrativo para el Control de versiones y pase a Producción de los Aplicativos Desarrollados en la OTIN.
- ✓ Las fuentes de cada sistema de información deben almacenarse en un único directorio el cual puede ser un sistema de archivos en un disco duro, un banco de datos, un ordenador o un servidor.
- ✓ Debe existir un único usuario responsable de este repositorio centralizado de todo el código, facilitando las tareas administrativas y reduciendo flexibilidad; todas las decisiones fuertes (como crear una nueva rama) necesitarán la aprobación del responsable.
- ✓ Este repositorio debe contener el historial de versiones de todos los elementos gestionados.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA
Oficina Técnica de Informática
ELMER PEREZ ESPINOZA

5.8. Control de Versiones

- ✓ Se debe usar un sistema de control de versiones que autentifique y registre el miembro del equipo asociado con todos los cambios que se realice en el código base, todos los archivos de configuración y compilación.
- ✓ El sistema de control de versiones que se emplee debe disponer de un repositorio, que contenga el conjunto de información gestionada por el sistema.

- ✓ El control de versiones debe registrar los cambios realizados sobre un archivo o conjunto de archivos permitiendo recuperar versiones específicas más adelante.

5.9. Protección de datos de prueba

- ✓ El Equipo de Desarrollo debe considerar que los datos de carácter personal no deben ser usados como datos de prueba ya que se expondría al riesgo de la difusión de estos.
- ✓ El Jefe de Proyecto tiene la potestad de autorizar el uso de datos de carácter personal bajo responsabilidad; sin embargo, se debe implementar medidas de protección necesaria para estos datos de prueba.

5.10. Capacitación necesaria en seguridad

El Jefe de Proyecto debe identificar:

- ✓ El nivel de las habilidades y conocimientos en Seguridad necesarios para el proceso de desarrollo en un Sistema de Información.
- ✓ La Oficina Técnica de Informática debe elaborar cada año un Plan de capacitación y concienciación de ser necesario.
- ✓ A los trabajadores nuevos a quienes se le debe capacitar. Y a aquellos trabajadores quienes necesitan reforzar sus conocimientos.

6. Validez y gestión de documentos

El presente documento es válido desde el momento de su aprobación, el propietario de este documento es la Oficina Técnica de Informática, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

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

- ✓ Cantidad de incidentes que surgen por fallas en los controles de seguridad creados en los sistemas.
- ✓ Cuando se encuentren nuevas maneras de realizar el desarrollo seguro y se adapten a la forma de trabajo en la institución.
- ✓ Cuando hay cambios en la normatividad (nueva ley) dada por el estado, las cuales afecten el documento, se debe actualizar adaptándolo a esta nueva norma.

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA
Oficina Técnica de Informática
ELMER PEREZ ESPINOZA