INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TÉCNICA DE INFORMÁTICA

"METODOLOGÍA PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS TIC"

Código: MET-001-OTIN-2018
Versión 1.0.0

POLÍTICA		
NOMBRE DE LA POLÍTICA: METODOLOGÍA PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS TIC		
CODIGO: MET-001-OTIN-2018		**VERSION:** 1.0.0
PROCESO AL QUE PERTENECE: Gestión de la Seguridad		
Elaborado por: Unidad Funcional de Calidad, Procesos y Seguridad de la Información	**Coordinado con:** Unidad Funcional de Calidad, Procesos y Seguridad de la Información	**Aprobado por:** Director Técnico de la Oficina Técnica de Informática
Nombre: Ing. Katherine Montenegro Julcapoma	**Nombre:** Ing. Arlett Agüero Vargas	**Nombre:** Ing. CIP Manuel Matos Alvarado
Fecha: 19/12/2018	**Fecha:** 21/12/18	**Fecha:** 21 DIC 2018
Firma	**Firma**	**Firma**
		Ing. CIP Manuel Amador Matos Alvarado Director Técnico Oficina Técnica de Informática

TABLA DE CONTENIDO

"SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS TIC"

1. OBJETIVO GENERAL

El objetivo del presente documento es considerar dentro de la Gestión de Proyectos el componente de Seguridad de la Información evitando posibles vulnerabilidades que afecten la confidencialidad, disponibilidad e integridad de la información procesada en los proyectos institucionales tomando como base la NTP-ISO/IEC 27001:2014 y en base al numeral 6.2 Organización de la seguridad de la información de la Política de Seguridad de la Información.

2. FINALIDAD

Garantizar la seguridad de la Información en la gestión de proyectos TIC del INEI, gestionando apropiadamente las herramientas existentes en la institución para que la información se encuentre protegida. También generar los documentos necesarios para que el personal a cargo de la Gestión de Proyectos administre y soporte adecuadamente el modelo propuesto y los mecanismos implementados.

3. ALCANCE

Este documento está dirigido a los Jefes de Proyectos de las diferentes dependencias que desarrollan y gestionan proyectos TIC en el INEI.

Para el alcance se tendrá en consideración lo siguiente:

- Análisis de riesgos de los activos de información que intervienen en el Proyecto
- Pruebas de Ingeniera Social
- Plan de capacitación sobre SGSI
- Construcción de la matriz de riesgos
- Revisión y desarrollo de políticas y procedimientos de seguridad
- Aseguramiento de componentes críticos

4. DOCUMENTOS DE REFERENCIA

- Política de seguridad de la información
- Norma ISO/IEC 27001:2014, capítulo A.6.1.5
- Lista de requisitos legales, normativos, contractuales y de otras índoles relacionadas con la Seguridad de la Información.
- Ley N° 29733 Protección de datos personales.
- Metodología para el Desarrollo de Software
- Política para el Desarrollo Seguro de los Sistemas de Información (MM/Nº 037-2018-INEI/OTIN)
- Procedimiento administrativo para el inicio de proyectos en la OTIN (MM/Nº 025-2018-INEI/OTIN)

- Componentes que todo proyecto de la OTIN debe tener (MM/Nº 028-2018-INEI/OTIN)

5. ABREVIATURAS Y DEFINICIONES

Las siguientes abreviaturas son aplicables para el propósito de este documento:

- SGSI: Sistema de Gestión de Seguridad de la Información
- OTIN: Oficina Técnica de Informática
- Riesgo: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la organización.
- UCAPSI: Unidad Funcional de Calidad, Procesos y Seguridad de la Información de la OTIN.
- Vulnerabilidad: En un sistema informático es un punto o aspecto susceptible de ser atacado o de dañar su seguridad; representan las debilidades o aspectos falibles o atacables en el sistema informático y califican el nivel de riesgo del mismo.

6. OBJETIVOS ESPECÍFICOS

- Se implementarán bajo normas, mejores prácticas, y requerimientos de seguridad, un control de la Seguridad de la Información en la Gestión de Proyectos TIC.
- Se realizarán un diagnóstico de la situación actual entorno al ambiente de Seguridad de la Información.
- Se establecerá la metodología y los procedimientos necesarios para incluir la Seguridad de la Información dentro de los proyectos TIC.
- Se mejorarán e implementarán nuevas medidas de seguridad sobre los activos de información, los procesos y los sistemas que permiten brindar los servicios de la institución.

7. DISPOSICIONES GENERALES

7.1. Todo Proyecto TIC, al momento de su planificación deberá considerar el componente de seguridad de la información el cual abarca:

- El personal encargado de realizar el testing a las aplicaciones
- La Etapa del testing, que es el tiempo de ejecución para las pruebas de las aplicaciones.
- Los requisitos funcionales y no funcionales de Seguridad de la Información.
- La Seguridad de la Información para la información sensible y datos personales

7.2. Se deberá crear conciencia del valor de la seguridad de la información para generar compromiso en su implementación en los proyectos TIC para ello el Jefe de la Unidad Funcional de Calidad, Procesos y Seguridad de la Información socializará y/o difundirán boletines TIC de seguridad de la Información.

7.3. Se desarrollarán y validarán líneas base de seguridad acorde a nuestra infraestructura y regulaciones nacionales. Ver Anexo 1.

7.4. Se tendrá en cuenta la flexibilidad justificada para ofrecer controles alternativos para minimizar los riesgos relacionados con la seguridad de la información.

8. DISPOSICIONES ESPECÍFICAS

8.1. Es responsabilidad de la Oficina Técnica de Informática, a través de la Unidad Funcional de Calidad, Procesos y Seguridad de la Información, velar por el cumplimiento de la presente metodología en los proyectos TIC institucionales.

8.2. El Jefe de Proyecto por parte de la OTIN, deberá:

- Coordinar y supervisar cada una de las fases de desarrollo del Proyecto; además de solicitar a los programadores o generar la documentación necesaria a fin de dar cumplimiento con los requisitos de seguridad de la información.
- Mejorar e implementar, de corresponder, nuevas medidas de seguridad sobre los activos de la información, los procesos y los sistemas que permiten brindar servicios.
- Elaborar los documentos necesarios que permitan gestionar de manera segura el flujo de información derivado de los diferentes procesos.
- Identificar y comunicar al Jefe de la Unidad Funcional de Infraestructura TIC los requerimientos de normativas, servicios o software que sean necesarios implementar para mejorar y garantizar la confidencialidad, integridad y disponibilidad de la seguridad de la información.
- Documentar los casos de éxito y las lecciones aprendidas para futuros proyectos y comunicarlos al Director Técnico de la OTIN.

8.3. El Equipo del proyecto elaborará la documentación necesaria (requisitos funcionales y no funcionales) de los Sistemas de Información desarrollados teniendo en cuenta lo proporcionado por las Direcciones Nacionales y Técnicas.

8.4. El equipo de programadores del proyecto desarrollará las aplicaciones manteniendo un estándar de desarrollo seguro de sistemas de información, establecido en la Política de Desarrollo Seguro de la OTIN.

8.5. La Unidad funcional de Calidad, Procesos y Seguridad de la Información deberá:

- Verificar los pilares de seguridad de la información en los activos y los procesos que se encuentran inmersos en el desarrollo de los proyectos TIC.
- Realizar el testing funcional y no funcional de las aplicaciones desarrolladas.
- Mantener un Plan de Pruebas y registro de las incidencias encontradas al realizarlas de acuerdo a la Metodología para el Desarrollo de Software de OTIN.

9. ESTRUCTURA DE LA METODOLOGÍA

La Seguridad de la Información debe estar presente en las Fases del desarrollo de los Proyectos TIC, a continuación se listan los aportes relacionados a la Seguridad de la Información en cada una de ellas.

FASE	APORTE
PLANIFICACIÓN	• Alinean expectativas • Identifican los recursos necesarios • Identifican los posibles riesgos
ANÁLISIS DE REQUERIMIENTOS	• Definicion de una strategia de seguridad apropiada • Identificación y clasificación de activos • Identificación de regulaciones, políticas aplicables, riesgos, etc.
DISEÑO	• Aportes conceptuales y técnicos para proteger el software y la información que procesa • Capacidad para resistir ataques de ciberdelincuentes • Minimizan vulnerabilidades
DESARROLLO	• Implementación de una linea base de seguridad de la información • Se cuenta con definiciones específicas de seguridad provenientes de la etapa de diseño.

PRUEBAS	• Pruebas funcionales
	• Pruebas no funcionales:
	  • Pruebas de stress
	  • Pruebas de seguridad

PUESTA EN PRODUCCIÓN	• Seguridad Operativa • Implementación de controles • Estandarización de procedimientos

10. IMPLEMENTACION DE LA METODOLOGÍA

10.1. FASE PLANIFICACIÓN DEL PROYECTO

- En la Planificación del Proyecto, el Analista identificará los activos de información digitales claves que estarán involucrados en el desarrollo del Sistema de Información, alineándose a la Metodología para el Desarrollo de software de la OTIN.
- Se identificarán los recursos necesarios, así como los posibles riesgos que el proyecto pueda originar de acuerdo a la Metodología para la Gestión de Riesgos.

- Asimismo, la UCAPSI revisará las responsabilidades legales que tiene el INEI con el tratamiento de la información que realiza (incluyendo los grupos de interés que podrían verse afectados) de acuerdo a la Ley de Protección de Datos Personales.
- Se identificará el nivel de sensibilidad y las necesidades de seguridad que el sistema de información requiere, para posteriormente ser establecidos y expuestos en la reunión de Kick – Off de acuerdo a la Ley de Protección de Datos Personales.
- El Jefe de Proyecto de la OTIN deberá establecer el estándar de cuidado necesario y suficiente para atender los retos propios del desarrollo de los sistemas, atendiendo las exigencias de los entes de control y las expectativas de las Direcciones Nacionales y Técnicas usuarias.

10.2. FASE ANÁLISIS DE REQUERIMIENTOS

- La Unidad Funcional de Calidad, procesos y Seguridad de la Información mantendrá un catálogo de normas donde se encuentren las directrices que debe seguir el INEI en materia TIC, incluyendo las que seguirá el software resultante de la implementación del proyecto. En este catálogo se incluirá:
  - ✓ Políticas de seguimiento, revisión, normativas, técnicas de programación, metodologías.
  - ✓ Políticas de seguridad del INEI.
  - ✓ Directrices de planificación, gestión de cambios y gestión de calidad
- El jefe de proyecto deberá obtener información detallada de los usuarios acerca de los requisitos que el sistema de información debe cumplir referente a seguridad y disponibilidad del sistema.
- El jefe de proyecto identificará las prioridades de los requisitos funcionales y no funcionales del sistema de información.
- El jefe de proyecto clasificará los activos de información que estarán involucrados en el desarrollo del Sistema de Información considerando los niveles de clasificación de la Información que se encuentran en la Política de clasificación, manejo y difusión de la información en la OTIN.

10.3. FASE DISEÑO

- Dentro del modelo lógico de datos, el Analista o Jefe del Proyecto determinará:
  - ✓ Número máximo de ocurrencias
  - ✓ Tipo y frecuencia de acceso
  - ✓ Características de seguridad, confidencialidad, disponibilidad y demás que sean consideradas como relevantes

- El Analista o Jefe de Proyecto deberá designar dentro del grupo de programadores a quien verifique que se eviten redundancias, inconsistencias y grupos repetidos. Caso contrario esta responsabilidad recaerá sobre el Analista o Jefe de Proyecto mismo.
- Se realizará un plan de migración de datos desde otros sistemas para la carga de información, de requerirlo el sistema.
- Dentro de la descripción de las interfaces, el Analista o Jefe de Proyecto deberá especificar los requisitos de seguridad y las validaciones.

10.4. FASE DESARROLLO

- Dentro de la arquitectura del sistema se definirán los requisitos de seguridad y control de acceso diseñando procedimientos para el acceso al sistema, mantenimiento y confidencialidad de datos, control y registro de accesos al sistema, copias de seguridad y recuperación de datos.
- Los Jefes de Proyecto de la OTIN dentro de las especificaciones del entorno de desarrollo de software deberán incluir los requisitos de operación y seguridad del sistema.
- El Analista del sistema o quien haga sus veces definirá los procedimientos de migración y carga inicial, referidos a la seguridad, preparación, carga de datos, verificación y comprobación de la integridad de la información al finalizar la migración y/o carga de datos.
- Deberá seguirse la Política para el Desarrollo Seguro de Sistemas de Información de la OTIN.

10.5. FASE PRUEBAS

- Dentro del Plan de pruebas se considerará el entorno que se requiere para la realización de pruebas del sistema, teniendo en cuenta el entorno tecnológico, sus restricciones, requisitos de operación y seguridad, herramientas de prueba, planificación de capacidades y procedimientos relativos a la promoción entre entornos, emergencia y recuperación.
- Acorde con las características del diseño del sistema, se implantarán verificaciones de acuerdo a los niveles de prueba que se establezcan, de tal forma que sean aplicables a grupos de componentes y cubran aspectos funcionales y no funcionales que aseguren el buen funcionamiento del sistema.
- Se realizará el Plan de pruebas de acuerdo a los perfiles establecidos en los requerimientos del Sistema y sus funciones; además se estimará el tiempo para la ejecución de cada prueba.

10.6. FASE PUESTA EN PRODUCCIÓN

- Se tomará en cuenta, para la puesta en producción del sistema, los requisitos y procedimientos contemplados en el desarrollo del sistema.
- Se verificará que la infraestructura necesaria para configurar el entorno se encuentre disponible.
- Se instalarán todos los componentes del nuevo sistema (producto software) de acuerdo al plan de implantación, al desarrollo del sistema y a las normas y estándares nacionales aplicables.
- Se indicará la frecuencia para la realización de las copias de seguridad (backup).