



INEI INSTITUTO
NACIONAL DE
ESTADÍSTICA E
INFORMÁTICA

OFICINA TÉCNICA DE INFORMÁTICA

PROCEDIMIENTOS ADMINISTRATIVOS

“Procedimiento para la Auditoria Interna del SGSI”

Código: PRA-019-OTIN-2018

Versión 1.0.0

	Procedimiento Administrativo	Código: PRA-019-OTIN-2018
	PROCEDIMIENTO PARA LA AUDITORÍA INTERNA DEL SGSI	Versión: 1.0.0
		Página 2 de 12

PROCEDIMIENTO		
NOMBRE DEL PROCEDIMIENTO: PROCEDIMIENTO PARA LA AUDITORIA INTERNA DEL SGSI		
CODIGO: PRA-019-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: 19/11/2018	Fecha: 19/11/2018	Fecha:
Firma	Firma	Firma
		



 INEI INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA	Procedimiento Administrativo	Código: PRA-019-OTIN-2018
	PROCEDIMIENTO PARA LA AUDITORÍA INTERNA DEL SGSI	Versión: 1.0.0
		Página 3 de 12

TABLA DE CONTENIDO

1.	OBJETIVO.....	4
2.	ALCANCE	4
3.	REFERENCIAS	4
4.	ABREVIATURAS Y DEFINICIONES	4
5.	CONDICIONES BÁSICAS	4
6.	RESPONSABLES	5
6.1.	CISO.....	5
6.2.	DIRECTOR NACIONAL O TÉCNICO DUEÑO DEL PROCESO	5
7.	DESCRIPCIÓN DEL PROCEDIMIENTO	6
7.1.	DIAGRAMA DE FLUJO	6
7.2.	DESCRIPCIÓN DE ACTIVIDADES.....	7
8.	ANEXOS	10



	Procedimiento Administrativo	Código: PRA-019-OTIN-2018
	PROCEDIMIENTO PARA LA AUDITORÍA INTERNA DEL SGSI	Versión: 1.0.0
		Página 4 de 12

“PROCEDIMIENTO PARA LA AUDITORÍA INTERNA DEL SGSI”

1. OBJETIVO

El presente documento tiene como objetivo establecer los lineamientos y el procedimiento a seguir para la planificación, realización y cierre de auditorías internas del SGSI del Instituto Nacional de Estadística e Informática, bajo la norma NTP – ISO/IEC 27001:2014.

2. ALCANCE

El presente procedimiento está dirigido a la Dirección Nacional y/o Técnica dueña del Proceso a ser auditado, siendo fuente de consulta y aplicación para las áreas comprendidas en el alcance del SGSI.

3. REFERENCIAS

- Norma NTP-ISO/IEC 27001:2014, capítulos A.12.7.1

4. ABREVIATURAS Y DEFINICIONES

- **Auditoría:** Es la acción de verificar que un determinado hecho o circunstancia ocurra de acuerdo a lo planeado.
- **CISO:** Oficial de Seguridad de la Información
- **DDNN/TT:** Direcciones Nacionales y Técnicas
- **Hallazgo de auditoría:** Son las debilidades detectadas por el auditor. Por lo tanto, abarca los hechos y otras informaciones obtenidas que merecen ser comunicados a los funcionarios de la entidad auditada y a otras personas interesadas.
- **No conformidad:** Es cualquier incidencia o situación que se produce cuando, en la realización de una actividad, se obtiene un resultado que incumple un requisito.
- **OTA:** Oficina Técnica de Administración
- **PAA:** Programa Anual de Auditoría
- **SGSI:** Sistema de Gestión de Seguridad de Información

5. CONDICIONES BÁSICAS

- 5.1. Las auditorías internas se realizarán a fin de determinar el grado en que el SGSI se está implementando y manteniendo de manera eficaz, si cumple con los requisitos de la norma NTP-ISO/IEC 27001:2014 y con los requisitos propios de la Institución. Estas formarán parte del PAA (Ver Anexo N°1), y comunicado al Comité de Gestión de Seguridad de la Información dentro del primer trimestre de cada año.



	Procedimiento Administrativo	Código: PRA-019-OTIN-2018
	PROCEDIMIENTO PARA LA AUDITORÍA INTERNA DEL SGSI	Versión: 1.0.0
		Página 5 de 12

5.2. Para la elaboración del Programa Anual de Auditoría se debe tener en cuenta lo siguiente:

- Las auditorías internas deben realizarse a intervalos planificados (una vez por año como mínimo).
- El alcance y la frecuencia de las auditorías internas serán determinados en función de la importancia de los procesos o áreas a auditar.

6. RESPONSABLES

6.1. CISO

El CISO del INEI es el responsable de:

- Velar por el cumplimiento de lo dispuesto en este procedimiento.
- Gestionar el PAA para el SGSI.
- Elaborar y socializar el PAA preliminar con el Director Nacional y/o Técnico dueño del proceso a auditar de la Institución antes de su presentación al Secretario General para su aprobación.
- Comunicar a las partes pertinentes la aprobación, modificación, avance y resultados del PAA.
- Asegurar la implementación del PAA, incluyendo el establecimiento de los objetivos, el alcance y los criterios de auditoría de las auditorías individuales y la selección del Equipo Auditor y del Auditor Líder.
- Hacer seguimiento, revisar y mejorar del PAA.
- Asegurar que se gestionen y mantengan los registros apropiados del PAA.

6.2. DIRECTOR NACIONAL O TÉCNICO DUEÑO DEL PROCESO

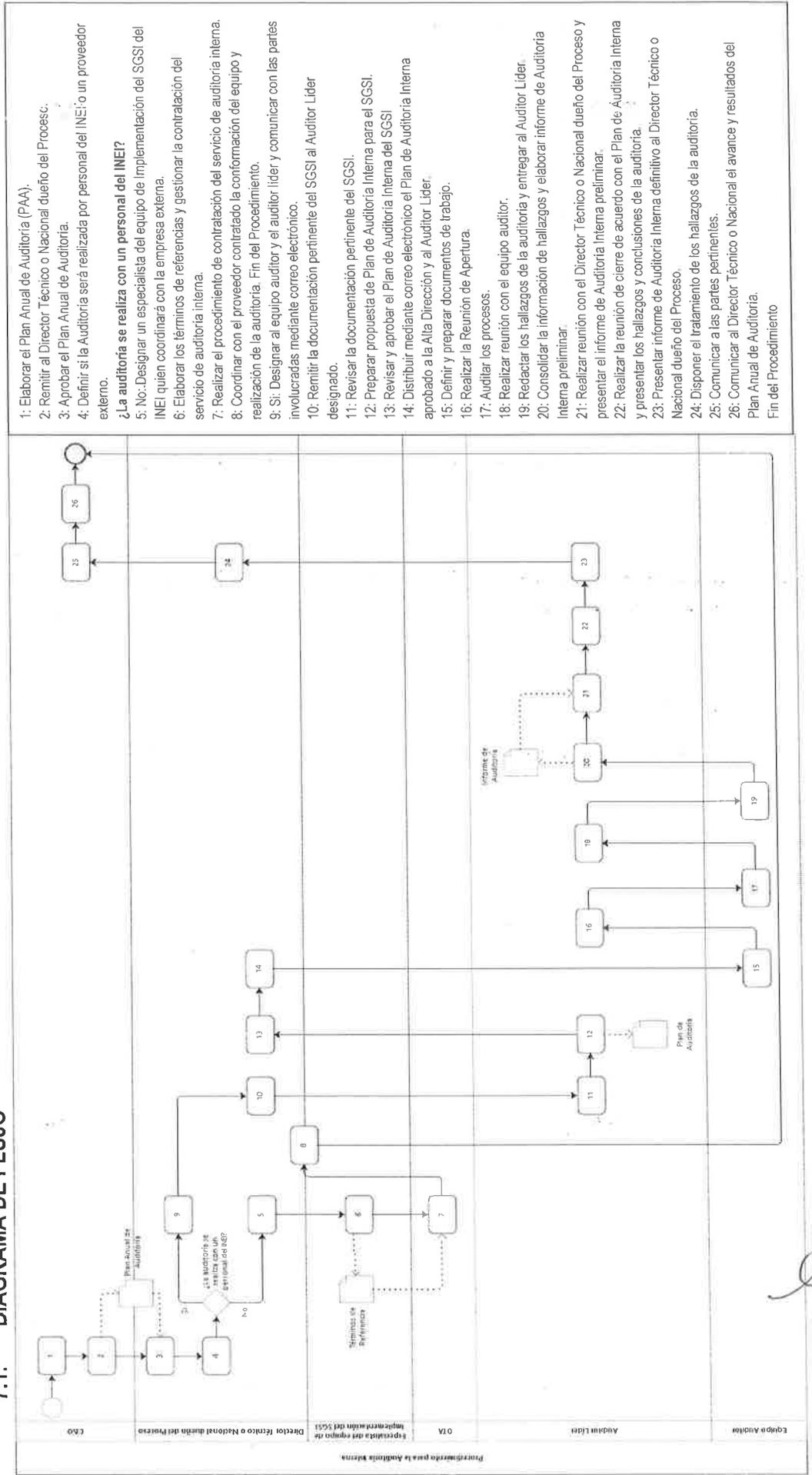
El Director Nacional o Técnico es el responsable de:

- Poner a disposición del equipo auditor los medios necesarios y requeridos para realizar la auditoría.
- Facilitar el acceso a las instalaciones y documentos relevantes para la auditoría.
- Cooperar con los auditores para asegurar el éxito de la auditoría.
- Tomar las acciones correctivas necesarias sin demora injustificada para eliminar las no conformidades detectadas durante la auditoría y sus causas.
- Determinar y gestionar los recursos necesarios para la implementación del PAA.



7. DESCRIPCIÓN DEL PROCEDIMIENTO

7.1. DIAGRAMA DE FLUJO




	Procedimiento Administrativo	Código: PRA-019-OTIN-2018
	PROCEDIMIENTO PARA LA AUDITORÍA INTERNA DEL SGSI	Versión: 1.0.0
		Página 7 de 12

7.2. DESCRIPCIÓN DE ACTIVIDADES

N°	Responsable	Actividades
Inicio del Procedimiento		
1	CISO	Elaborar el Plan Anual de Auditoría (PAA) para el Sistema de Gestión de Seguridad de la Información.
2	CISO	Remitir el PAA al Director Técnico o Nacional dueño del Proceso para su aprobación.
3	Director Técnico o Nacional dueño del Proceso	Aprobar el PAA y comunicar a las partes pertinentes.
4	Director Técnico o Nacional dueño del Proceso	Definir si la Auditoría será realizada por personal del INEI o un proveedor externo.
		¿La auditoría se realiza con un personal de INEI?
5	Director Técnico o Nacional dueño del Proceso	No: Designar un especialista del equipo de Implementación del SGSI para la elaboración de los términos de referencia y gestión de la contratación del servicio de auditoría interna.
6	Especialista del equipo de Implementación del SGSI	Elaborar los términos de referencias y gestiona la contratación de servicio de auditoría interna ante OTA, en coordinación con el Director Técnico o Nacional dueño del Proceso.
7	OTA	Realizar el procedimiento de contratación del servicio auditoría interna, según normatividad vigente.
8	Director Técnico o Nacional dueño del Proceso// Especialista del equipo de Implementación del SGSI	Coordinar con el proveedor contratado la conformación del equipo auditor (inclusive Auditor Líder) y comunicar a las partes involucradas mediante correo electrónico la contratación del servicio y la conformación del equipo. Fin del Procedimiento
9	Director Técnico o Nacional dueño del Proceso	Si: Designar al equipo auditor y el auditor líder que realizará la auditoría interna y comunicar con las partes involucradas mediante correo electrónico. Continuar con la Actividad N° 7.
10	Director Técnico o	Remitir la documentación pertinente del SGSI al Auditor Líder designado para la auditoría interna.

N°	Responsable	Actividades
	Nacional dueño del Proceso	
11	Auditor Líder	Revisar la documentación pertinente del SGSI a fin de reunir información para preparar las actividades de auditoría, así como establecer una visión general del grado de la documentación del sistema que permita detectar posibles carencias.
12	Auditor Líder	Preparar propuesta de Plan de Auditoría Interna (Ver Anexo N°2) para el SGSI, en coordinación con el Director Técnico o Nacional dueño del Proceso y los auditores internos, de acuerdo al PAA correspondiente.
13	Director Técnico o Nacional dueño del Proceso	Revisar y aprobar el Plan de Auditoría Interna del SGSI, según corresponda.
14	Director Técnico o Nacional dueño del Proceso	Distribuir mediante correo electrónico el Plan de Auditoría Interna aprobado a la Alta Dirección y al Auditor Líder.
15	Equipo Auditor	Definir y prepara documentos de trabajo, según sea necesario, para referencia y registro de evidencias de la auditoría.
16	Auditor Líder	Realizar la Reunión de Apertura con el personal involucrado de acuerdo al Plan de Auditoría Interna aprobado.
17	Equipo Auditor	Auditar los procesos, de acuerdo con el Plan de Auditoría Interna, obteniendo evidencias objetivas de los hallazgos y dar la retroalimentación a los auditados con respecto a las evidencias encontradas.
18	Auditor Líder	Realizar reunión de enlace con el equipo auditor, de acuerdo con el Plan de auditoría Interna aprobada.
19	Equipo Auditor	Redactar los hallazgos de la auditoría y entregar al Auditor Líder.
20	Auditor Líder	Consolidar la información de hallazgos y elaborar informe de Auditoría Interna preliminar, de acuerdo con el formato establecido (Ver Anexo N°3), con la colaboración del Equipo Auditor.
21	Auditor Líder	Realizar reunión con el Director Técnico o Nacional dueño del Proceso y presentar el informe de Auditoría Interna preliminar.
22	Auditor Líder	Realizar la reunión de cierre de acuerdo con el Plan de Auditoría Interna y presentar los hallazgos y conclusiones de la auditoría.
23	Auditor Líder	Presentar informe de Auditoría Interna definitivo al Director Técnico o Nacional dueño del Proceso.
24	Director Técnico o Nacional dueño del Proceso	Disponer el tratamiento de los hallazgos de la auditoría señalados en el informe de Auditoría Interna.
25	CISO	Comunicar los hallazgos de la auditoría a las partes pertinentes para el tratamiento y levantamiento de las no conformidades.

	Procedimiento Administrativo	Código: PRA-019-OTIN-2018
	PROCEDIMIENTO PARA LA AUDITORÍA INTERNA DEL SGSI	Versión: 1.0.0
		Página 9 de 12

N°	Responsable	Actividades
26	CISO	Comunicar al Director Técnico o Nacional el avance del levantamiento de las no conformidades y los resultados del Plan Anual de Auditoría.
Fin del procedimiento		

Anexo N° 2

PLAN DE AUDITORÍA INTERNA

I. DATOS DE LA AUDITORÍA INTERNA			
1.1. N° de Auditoría		1.2. Norma de referencia	

II. OBJETIVO DE LA AUDITORÍA INTERNA

III. ALCANCE DE LA AUDITORÍA INTERNA

IV. EQUIPO AUDITOR	
4.1. Auditor Líder	
4.2. Auditores Internos	
4.3. Auditores en formación	

V. INVITADOS	
5.1. Expertos Técnicos	
5.2. Observadores	

VI. PLAN DE AUDITORÍA						
Fecha	Hora	Auditor	Proceso / Área	Criterios de Auditoría		Auditado
				Claúsula / Control	Documentación	
			Reunión de Apertura			
			Reunión de Cierre			

VII. APROBACIÓN DEL PLAN DE AUDITORÍA	
Elaborado por:	Aprobado por:
Nombres, cargo y firma Fecha: ___/___/___	Nombres, cargo y firma Fecha: ___/___/___

Anexo N° 3

INFORME DE AUDITORÍA INTERNA

Fecha: dd/mm/aaaa

I. DATOS DE LA AUDITORÍA INTERNA			
1.1. N° de Auditoría		1.2. Norma de referencia	
1.3. Fecha de Auditoría	Del dd/mm/aaaa al dd/mm/aaaa		
1.4. Lugar de Auditoría			

II. OBJETIVO DE LA AUDITORÍA INTERNA

III. ALCANCE DE LA AUDITORÍA INTERNA <i>(Señalar las exclusiones reportadas de ser el caso)</i>

IV. EQUIPO AUDITOR	
4.1. Auditor Líder	
4.2. Auditores Internos	
4.3. Auditores en formación	

V. INVITADOS	
5.1. Expertos Técnicos	
5.2. Observadores	

VI. FORTALEZAS Y DEBILIDADES	
Fortalezas	Debilidades
<i>(Agregar los guiones que sena necesarios)</i>	

VI. RESULTADOS DE LA AUDITORÍA INTERNA				
No conformidades: _____			Oportunidades de mejora: _____	
No Conformidades				
N°	Área / Proceso	Descripción	Responsable	Auditor
<i>(Agregar las filas que sean necesarias)</i>				
<i>(Agregar las filas que sean necesarias)</i>				
Oportunidades de Mejora				
N°	Área / Proceso	Descripción	Responsable	Auditor
<i>(Agregar las filas que sean necesarias)</i>				

VI. CONCLUSIONES DE LA AUDITORÍA INTERNA
<i>(Agregar los guiones que sean necesarias)</i>