AUDITORÍA A LA SEGURIDAD DE LA INFORMACIÓN

Procedimiento: PR-OTI-005

Versión: 01

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Elaborado por: José Antonio Chacón Calderón Director Oficina de Tecnologías de la Información y la Comunicación **Dueño del proceso**	**Firma:** Firma Digital Senamhi Firmado digitalmente por CHACON CALDERON Jose Antonio FAU 20131366028 soft Motivo: Soy el autor del documento Fecha: 11.11.2020 13:12:35 -05:00
Revisado por: Sonia Huamán Lozano Directora Unidad de Modernización y Gestión de la Calidad Laiter Luis García Tueros Director Oficina de Asesoría Jurídica	**Firma:** Firma Digital Senamhi Firmado digitalmente por SILVA OLIVER Nora Isabel FAU 20131366028 soft Motivo: Soy el autor del documento Fecha: 13.11.2020 16:21:01 -05:00 Firma Digital Senamhi Firmado digitalmente por ARTEAGA ARCE Daniel Alberto FAU 20131366028 hard Motivo: Soy el autor del documento Fecha: 17.11.2020 09:49:21 -05:00
Aprobado por: José Percy Barrón López Gerente General Gerencia General	**Firma:** Firma Digital Senamhi Firmado digitalmente por BARRON LOPEZ Jose Percy FAU 20131366028 soft Motivo: Soy el autor del documento Fecha: 17.11.2020 10:37:33 -05:00

INDICE

1. OBJETIVO

Gestionar las actividades para la planificación y ejecución de las auditorías de seguridad de la información en el Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI, con la finalidad de evaluar el cumplimiento de los requisitos que establece el estándar nacional e internacional sobre la seguridad de la información, garantizando la confidencialidad, disponibilidad e integridad de la información institucional.

2. ALCANCE

El presente procedimiento es de aplicación y cumplimiento obligatorio para los funcionarios y servidores públicos del SENAMHI que manejen información.

3. BASE LEGAL

3.1 Ley N° 24031, Ley del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI, modificado por la Ley N° 27188.
3.2 Decreto Supremo N° 003-2016-MINAM, que aprueba el Reglamento de Organización y Funciones del SENAMHI.
3.3 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, y sus modificatorias
3.4 Resolución Jefatural N° 090-95-INEI, que aprueba la Directiva N° 008-95-INEI/SJI, “Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública”.
3.5 Ley N° 29733, Ley de Protección de Datos Personales.
3.6 Ley N° 30096, Ley de Delitos Informáticos.
3.7 Resolución Jefatural N° 386-2002-INEI, que aprueba la Directiva N° 016-2002-INEI/DTNP "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública".
3.8 Resolución Ministerial N°004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Requisitos. 2da.Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

4. DEFINICIONES Y SIGLAS

4.1 Activo de información
Cualquier elemento físico, tecnológico o intangible que se genera, procesa o almacena información y tiene valor para la institución, como base de datos, archivos, programas, manuales, equipos de comunicaciones.

4.2 Análisis de Riesgos
Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

4.3 Alcance de la Auditoría
Extensión y límites de una auditoría.

4.4 Auditor
Persona que analiza y comprueba el cumplimiento de los requisitos conforme al estándar internacional y requisitos nacionales e institucionales.

4.5 Auditoría

Proceso sistemático, independiente y documentado para obtener evidencia de la auditoría y evaluarlas de manera objetiva, con el fin de determinar el grado en que se cumplen los criterios de auditoría.

4.6 Control

Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos del SENAMHI.

4.7 Criterios de auditoría

Conjunto de políticas, procedimientos o requisitos utilizados como una referencia a la cual se compara la evidencia de la auditoria.

4.8 Plan de auditoría

Descripción de las actividades y de detalles de una auditoría.

4.9 Seguridad de la información

Consiste en la preservación de su confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de la institución.

4.10 Siglas

TI: Tecnologías de la Información
SistGD: Sistema de Gestión Documental

5. RESPONSABILIDADES

5.1 Oficina de Tecnologías de la Información y la Comunicación – OTI

5.1.1 Actualizar y formular propuestas de optimización y mejora del presente procedimiento, en el marco de las normas legales correspondientes y las medidas de racionalidad y austeridad en el uso de los recursos públicos.

5.1.2 Revisar y aprobar la propuesta de Plan de Auditoría interna elaborada por el/la Especialista de seguridad de la información.

5.1.3 Remitir la información requerida para la ejecución de la auditoría externa.

6. GENERALIDADES

La auditoría de seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información institucional.

6.1. Fases de la Auditoría de seguridad de la información

6.1.1. Planificación de la auditoría interna

Consiste en la programación de auditoría, elaboración y aprobación del Plan de auditoría, el cual debe ser aprobado por el/la Director/a de la OTI.

El plan de auditoría interna debe tener el siguiente contenido:

a) Objeto del plan de auditoría.
b) Alcance del plan.
c) Metodología y criterios para la elaboración de reportes.
d) El nombre del auditor interno, la asignación de sus responsabilidades y funciones.
e) Cronograma de actividades.

6.1.2. Ejecución de la auditoría interna

La ejecución de la auditoría interna permite determinar si los objetivos, controles, procesos y procedimientos de la seguridad de la información se encuentran conforme a lo siguiente:

- Los requisitos que establece el estándar internacional sobre seguridad de la información.
- Requisitos establecidos internamente por la institución; lineamientos internos sobre la seguridad de la información.

La auditoría interna se inicia con una reunión de apertura, con la participación del/la Director/a de la OTI, los/las coordinadores/as de la OTI y la/el especialista de seguridad de la información asignado como auditor/a presentando la metodología, los tiempos y recursos que serán utilizados, se recopila información de los Órganos y Unidades, incluyendo de la Oficina de Tecnologías de la Información y la Comunicación - OTI, posteriormente se realiza un análisis de los siguientes aspectos:

- **Análisis y valorización de activos:** Análisis de los activos de información de la institución.
- **Evaluación de riesgos:** Evaluación de vulnerabilidad, amenazas y riesgos de información y su criticidad.
- **Análisis de elementos de seguridad física**: Videovigilancia, control de accesos, protección contra incendios, etc.
- **Análisis de disponibilidad de infraestructuras y servicios de TI:** Análisis de cualquier elemento que ponga en riesgo la disponibilidad de los servicios.
- **Auditoría de procesos de seguridad:** Análisis a los procesos de seguridad y gestión de TI definidos en la institución y el grado de cumplimiento de los estándares, verifica la existencia de y cumplimento de documentos de seguridad.
- **Hacking ético:** Analiza la penetración en redes y sistemas, tanto desde el exterior como el interior de la red.

Ejecutada la auditoría interna, se elabora un informe de auditoría interna detallando las observaciones y recomendaciones ante posibles vulnerabilidades encontradas. En el mencionado informe de auditoría interna debe indicarse lo siguiente:

- Tipo y descripción de vulnerabilidad
- Sistemas o procesos afectados

- Observaciones y recomendaciones sobre implementación de medidas preventivas y/o correctivas.

6.1.3. Ejecución de la Auditoría externa

Es realizada por una entidad externa. En este caso, es el/la Especialista en Seguridad de la Información quien se encarga de identificar y recopilar la información requerida por la auditoría externa. El/la Director/a de la OTI remite la información solicitada al/la auditor/a externo/a, previo visto bueno del/la Coordinador/a de la OTI.

6.1.4. Control de la auditoría

En esta última fase, se implementa las medidas preventivas o correctivas a las observaciones y recomendaciones mencionadas en el informe de auditoría interna o externa, posteriormente son validadas mediante un seguimiento con la finalidad de asegurar la integridad de los controles de seguridad aplicados, permitiendo la confidencialidad, disponibilidad e integridad de la información institucional.

7. DESARROLLO

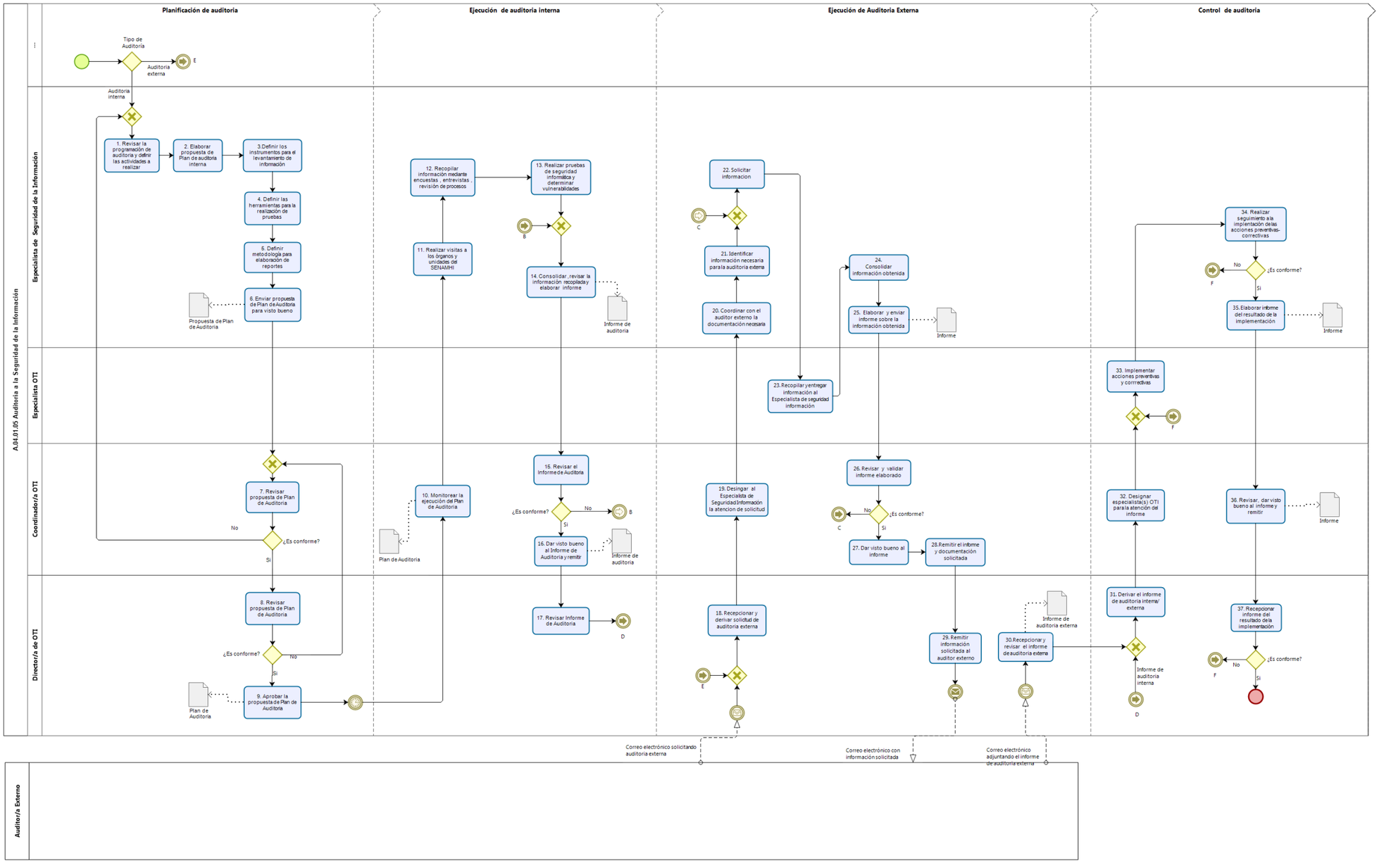
7.1. Requisitos del inicio del procedimiento

Descripción del requisito	Fuente
Programación de auditoria	Oficina de Tecnologías de la Información y la Comunicación

7.2. Proceso relacionado

Todos los procesos identificados en el inventario de procesos vigente.

7.3 Diagrama de flujo



7.3. Descripción de las actividades

N°	Descripción	Órgano/ Unidad	Responsable	Registros
Planificación de auditoría				
	¿Tipo de auditoría? **Auditoría Interna: Continuar con la Actividad N° 1** **Auditoría Externa: Continuar con la Actividad N° 18**	– – –	– – –	– – –
1	Revisar la programación de auditoria y definir las actividades a realizar.	OTI	Especialista de Seguridad de la Información	– – –
2	Elaborar propuesta del plan de auditoría interna.	OTI	Especialista de Seguridad de la Información	– – –
3	Definir los instrumentos para el levantamiento de información.	OTI	Especialista de Seguridad de la Información	– – –
4	Definir las herramientas para la realización de pruebas.	OTI	Especialista de Seguridad de la Información	– – –
5	Definir la metodología para elaboración de reportes.	OTI	Especialista de Seguridad de la Información	– – –
6	Enviar propuesta de plan de auditoría interna para visto bueno al/la Coordinador/a de la OTI.	OTI	Especialista de Seguridad de la Información	Propuesta de Plan de Auditoría interna
7	Revisar propuesta de Plan de auditoría interna. **¿Es conforme?** **Si: Continuar con la Actividad N° 8** **No: Reiniciar desde la Actividad N° 1**	OTI	Coordinador/a de la OTI	– – –
8	Revisar propuesta de plan de auditoría. **¿Es conforme?** **Si: Continuar con la Actividad N° 9** **No: Reiniciar desde la Actividad N° 7**	OTI	Director/a de la OTI	– – –
9	Aprobar la propuesta de Plan de auditoría interna	OTI	Director/a de la OTI	Plan de Auditoría Interna aprobado
Ejecución de auditoría interna				
10	Monitorear la ejecución del Plan de auditoría interna.	OTI	Coordinador/a de la OTI	Plan de Auditoría interna

N°	Descripción	Órgano/ Unidad	Responsable	Registros
11	Realizar visitas a los órganos y unidades del SENAMHI de acuerdo al alcance de la auditoría interna.	OTI	Especialista de Seguridad de la Información	– – –
12	Recopilar información mediante encuestas, entrevistas, revisión de procesos de TI.	OTI	Especialista de Seguridad de la Información	– – –
13	Realizar pruebas de seguridad informática y determinar vulnerabilidades.	OTI	Especialista de Seguridad de la Información	– – –
14	Consolidar, revisar la información recopilar y elaborar informe.	OTI	Especialista de Seguridad de la Información	Informe de auditoría interna
15	Revisar el Informe de auditoría interna. **¿Es conforme?** **Si: Continuar con la Actividad N° 16** **No: Continuar con la Actividad N° 14**	OTI	Coordinador/a de la OTI	– – –
16	Dar visto bueno al Informe de auditoría y remitir al/la Director/a de la OTI.	OTI	Coordinador/a de la OTI	Informe de auditoría interna SistGD
17	Revisar Informe de auditoría interna y continuar con la Actividad N° 31.	OTI	Director/a de la OTI	– – –
Ejecución de auditoría Externa				
18	Recepcionar y derivar solicitud de información de la auditoría externa.	OTI	Director/a de la OTI	Solicitud de información de la auditoría externa (SistGD y/o correo electrónico)
19	Designar al/la Especialista de Seguridad de la Información para la atención de solicitud.	OTI	Coordinador/a de la OTI	– – –
20	Coordinar con el/la Auditor/a externo la documentación necesaria para la ejecución de la auditoría externa.	OTI	Especialista de seguridad de la información	– – –
21	Identificar información necesaria para la auditoría externa.	OTI	Especialista de seguridad de la información	– – –
22	Solicitar información al/la Especialista de la OTI.	OTI	Especialista de seguridad de la información	– – –
23	Recopilar y entregar información al/la Especialista de seguridad información.	OTI	Especialista de la OTI	– – –
24	Consolidar información obtenida.	OTI	Especialista de seguridad de la información	– – –

N°	Descripción	Órgano/ Unidad	Responsable	Registros
25	Elaborar y enviar informe sobre la información obtenida al/la Coordinador/a de la OTI mediante SistGD.	OTI	Especialista de seguridad de la información	Informe
26	Revisar y validar informe elaborado por el/la Especialista de seguridad de la información. **¿Es conforme?** **Si: Continuar con la Actividad N° 27** **No: Reiniciar con la actividad N° 22**	OTI	Coordinador/a de la OTI	– – –
27	Dar visto bueno al informe.	OTI	Coordinador/a de la OTI	– – –
28	Remitir el informe y documentación solicitada al/la Director/a de la OTI.	OTI	Coordinador/a de la OTI	– – –
29	Remitir información solicitada al auditor externo y **finalizar.**	OTI	Director/a de la OTI	Información solicitada (SistGD y/o correo electrónico)
30	Recepcionar y revisar el informe de auditoría externa.	OTI	Director/a de la OTI	Informe de auditoría externa
Control de auditoría				
31	Derivar el informe de auditoría interna o externa al/la Coordinador/a de la OTI, mediante SistGD y/o correo electrónico.	OTI	Director/a de la OTI	Informe de auditoría interna Informe de auditoría externa
32	Designar al/los Especialista(s) OTI para la atención del informe de auditoría.	OTI	Coordinador/a de la OTI	– – –
33	Implementar medidas preventivas y/o correctivas en atención del informe de auditoría.	OTI	Especialista de la OTI	– – –
34	Realizar seguimiento a la implementación de las acciones preventivas y/o correctivas. **¿Es conforme?** **Si: Continuar con la Actividad N° 35** **No: Reiniciar con la Actividad N° 33**	OTI	Especialista de Seguridad de la Información	– – –
35	Elaborar y remitir el informe del resultado de la implementación mediante SistGD y/o correo electrónico.		Especialista de Seguridad de la Información	Informe
36	Revisar, dar visto bueno al informe y remitir al/la Director/a de la OTI.	OTI	Coordinador/a de la OTI	

N°	Descripción	Órgano/ Unidad	Responsable	Registros
37	Recepcionar informe del resultado de la implementación **¿Es conforme?** **Si: Finaliza** **No: Reiniciar con la Actividad N° 33**	OTI	Director/a de la OTI	_ _ _

8. REGISTROS

Denominación	Código
Plan de auditoría Interna	S/C
Informe de auditoría interna	S/C
Informe de auditoría externa	S/C
Informe	S/C
Documentación del SistGD	S/C
Correo electrónico	S/C

9. TABLA HISTÓRICA DE CAMBIOS

Versión	Fecha	Detalle de cambios
01	--	Versión inicial