PROCEDIMIENTO

AUDITORÍA INTERNA

SGSI-PR-03

Elaborado por:	Revisado por:	Aprobado por:
.....	.....	.....
Nombre y Firma	Nombre y Firma	Nombre y Firma

1. OBJETIVO:

Establecer las pautas para la planificación, realización, seguimiento y cierre de las Auditorías Internas al Sistema de Gestión de Seguridad de la Información (SGSI).

2. ALCANCE:

Este procedimiento se aplica a todas las actividades realizadas dentro del Sistema de Gestión de Seguridad de la Información (SGSI) desde que se genera la necesidad hasta que se completa y archiva el informe de auditoría interna.

3. DOCUMENTOS ASOCIADOS:

- Programa de auditoría interna SGSI-PR-03.FO-01
- Solicitud de Acción Correctiva SGSI-PR-04.FO-01
- SGSI-PR-05.FO-01 Proyecto de Mejora
- Plan de Auditoría
- Informe de Auditoría

4. DOCUMENTOS DE REFERENCIA:

- NTP ISO/IEC 27001:2014 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.
- ISO 19001:2018 - Sistemas de gestión de la calidad.
- ISO 19011:2018 – Directrices para la auditoría de sistemas de gestión

5. DEFINICIONES Y SIGLAS:

Definiciones

5.1 Acción Correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición [27000:2016(2.19)].

5.2 Corrección: Acción de eliminar una no conformidad detectada [ISO27000:2016(2.18)]

5.3 Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría [ISO27000:2016(2.5)].

5.4 Conclusiones de Auditoría: resultado de una auditoría (3.1), tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría (3.4) [ISO19001:2018(3.5)].

5.5 Hallazgos de Auditoría: resultados de la evaluación de la evidencia de la auditoría (3.3) recopilada frente a los criterios de auditoría (3.2) [ISO19001:2018(3.4)].

5.6 No Conformidad: no cumplimiento de un requerimiento [ISO27000:2016(2.53)]

5.7 Comité de Gestión de Seguridad de la Información (CGSI): Es un Comité ejecutivo conformado por altos directivos de la entidad, designado para gestionar, supervisar, revisar e informar de manera permanente los aspectos del SGSI. El Comité es presidido por el Superintendente Nacional o su representante, tiene como coordinador al Oficial de Seguridad de la Información.

5.8 Oficial de Seguridad de la Información: Es el coordinador del Comité de Gestión de Seguridad de la Información y principal responsable operativo de la implementación del SGSI.

5.9 Usuarios del documento: Comité de Seguridad de Información, el Oficial de Seguridad de Información de SUNAT y los auditores internos.

Siglas

5.10 OFSI: Oficial de Seguridad de la Información.
5.11 CGSI: Comité de Gestión de Seguridad de la Información.
5.12 SGSI: Sistema de Gestión de Seguridad de la Información.
5.13 SUNAT: Superintendencia Nacional de Aduanas y de Administración Tributaria.
5.14 SN: Superintendente Nacional.

6. PROCEDIMIENTO:

PLANIFICACIÓN

OFSI:
1. Elabora el programa de auditoría interna de SUNAT según el formato SGSI-PR-03.01 del Anexo 1.
2. Define el criterio y metodología de la auditoría.
3. Selecciona al equipo auditor, el cual está conformado por el Auditor Líder y Auditor(es) los cuales deben cumplir con las competencias especificadas en el Anexo 1 del presente documento.
4. Informa al CGSI del contenido del mismo.

CGSI:
5. Revisa el programa de auditoría y la conformación del equipo auditor para su aprobación.
6. Si no aprueba, devuelve a OFSI con observaciones.

7. Si se aprueba, envía a OFSI para notificación a las áreas involucradas y al equipo auditor.

OFSI:

8. Envía programa de auditoría a las áreas involucradas.
9. Contacta al equipo auditor.
10. Solicita al auditor líder plan de auditoría.

EJECUCIÓN

Auditor Líder:

11. Elabora plan de auditoría y envía a OFSI para su aprobación.
12. Si OFSI aprueba, procede a efectuar la auditoría en la fecha programada.

Auditor:

13. Las evidencias de la auditoría son reunidas por los auditores mediante entrevistas, inspección, observación de actividades, revisión de documentos y registros
14. El auditor analiza las evidencias obtenidas para la determinación de conformidades, no conformidades, observaciones y oportunidades de mejora. Los hallazgos de auditoría que se definan deben contar con evidencias y ser comunicados al auditado. Sólo la información que es verificable puede constituir evidencia de la auditoría.
15. Los hallazgos de auditoría pueden ser desvirtuados por las áreas auditadas hasta antes de la reunión de cierre, siempre que se presenten los elementos necesarios que los justifiquen y hayan sido generados con anticipación a la comunicación de la realización de la auditoría. El líder del equipo auditor evalúa los elementos presentados y designa al auditor que corresponda para verificar el cumplimiento con los criterios de auditoría, caso contrario lo incluye en el informe

Auditor Líder

16. Elabora informe de auditoría.
17. Envía informe de auditoría a OFSI.

CIERRE

OFSI:

18. Programa reunión de Revisión por la Dirección para analizar con el CGSI el resultado y cierre de auditoría interna, donde se presenta el informe de auditoría.
19. Organiza con áreas involucradas plan de acción en base a los resultados de la auditoría.
20. Si como resultado de la Auditoría se generara una Solicitud de Acción Correctiva esta debe registrarse en el formato SGSI-PR-04.FO-01.
21. Si como resultado de la Auditoría se generara una oportunidad de mejora, esta debe registrarse como proyecto de mejora usando el formato SGSI-PR-05.FO-01

Áreas Involucradas:

22. Ejecutan plan de acción e informan a OFSI.

OFSI

23. Verifica la eficacia de las acciones tomadas.
24. Archiva el programa, plan e informe de auditoría.

7. CONTROL DE CAMBIOS:

Detalle	Versión	Fecha de Aprobación	Responsable
Versión inicial	01		Oficial de Seguridad de la Información

Anexo Nro. 1: Responsabilidades y Competencias para Auditar

Auditor Líder:

Responsabilidades:

- Planificar y dirigir las auditorías internas.
- Registrar el plan de auditoría interna y sus resultados en el SAGS.
- Reportar al auditado los resultados de la auditoría.

Competencias

- Que conozca la Norma ISO/IEC 27001 vigente
- Que esté familiarizado con técnicas de auditoría
- Con certificación de Auditor Líder en ISO/IEC 27001 en la versión vigente
- Haber participado en 2 auditorías como auditor y en 1 auditoría como auditor líder.

Auditor:

Responsabilidades:

- Ejecutar la auditoría que le ha sido asignada

Competencias

- Que conozca la Norma ISO/IEC 27001 vigente
- Que esté familiarizado con técnicas de auditoría
- Que haya aprobado un curso de formación de auditores internos en ISO/IEC 27001 en la versión vigente
- Haber participado en 2 auditorías como auditor bajo supervisión de un auditor líder