



Tipo de documento:
PROCEDIMIENTO

Codificación:
PR-001-2024-SUNARP-CGD

Resolución de Aprobación: **Resolución N° 125-2024-SUNARP/GG**

Fecha de emisión: **26/06/2024**

Páginas: **1/29**

PROCEDIMIENTOS PARA LA EVALUACIÓN DEL DESEMPEÑO DEL SGSI

Copia No Controlada. Es responsabilidad del usuario asegurarse que el presente documento corresponde a la versión vigente publicada en la INTRANET.

ÍNDICE

I.	OBJETIVO	3
II.	FINALIDAD	3
III.	ALCANCE	3
IV.	BASE LEGAL	3
V.	DEFINICIÓN DE TÉRMINOS Y SIGLAS	4
VI.	RESPONSABILIDADES	7
VII.	DISPOSICIONES GENERALES	7
7.1	Enfoque de la Evaluación del Desempeño	7
7.2	Evaluación del Desempeño en la Sunarp	8
VIII.	DESCRIPCIÓN DEL PROCEDIMIENTO	9
8.1	PROCESO: Seguimiento, medición, análisis y evaluación	9
8.2	PROCESO: Auditoría interna	11
8.3	PROCESO: Revisión por la Dirección	15
IX.	DISPOSICIONES COMPLEMENTARIAS	17
X.	REGISTROS	17
XI.	ANEXOS	17
	CONTROL DE CAMBIOS	18
	Anexo N° 1 Diagramas de Flujo	19
	Anexo N° 2 Formato de Lista priorizada de Necesidades de Información	22
	Anexo N° 3 Formato de Ficha de Medición	23
	Anexo N° 4 Formato de Programa Anual de Auditorías (PAA)	24
	Anexo N° 5 Formato de Plan de Auditoría Interna (PAI)	25
	Anexo N° 6 Formato de Informe de Auditoría Interna del SGSI	26
	Anexo N° 7 Perfil del Auditor Líder de Seguridad de la Información	28
	Anexo N° 8 Perfil del Auditor Interno de Seguridad de la Información	29

I. OBJETIVO

Establecer los lineamientos y actividades para el proceso de evaluación del desempeño del Sistema de Gestión de Seguridad de la Información (SGSI) de la Sede Central Sunarp.

II. FINALIDAD

Asegurar el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) y los requisitos definidos en la Norma Técnica Peruana ISO/IEC 27001:2022 de Seguridad de la información, ciberseguridad y protección de la privacidad.

III. ALCANCE

Es de obligado cumplimiento para todo el personal que preste servicios en el alcance del SGSI de la Sede Central Sunarp, de manera permanente y/o eventual bajo cualquier modalidad de contrato, incluyendo el personal de entidades externas.

IV. BASE LEGAL

- 4.1** Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital, publicada el 13 de setiembre del 2018.
- 4.2** Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, publicado el 19 de febrero de 2021.
- 4.3** Resolución Ministerial N° 119-2018-PCM que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública, publicada el 10 de mayo de 2018;
- 4.4** Resolución Ministerial N° 087-2019-PCM que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital, modificando los artículos 1 y 2 de la Resolución Ministerial N° 119-2018-PCM y dejando sin efecto los artículos 2, 5 y 5-A de la Resolución Ministerial N° 004-2016-PCM, publicada el 19 de marzo de 2019.
- 4.5** Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD que aprueba la Directiva N° 001-2023-PCM/SGTD que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital, publicada el 08 de setiembre de 2023.
- 4.6** Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, publicada el 08 de setiembre de 2023.
- 4.7** Resolución de la Superintendencia Nacional de los Registros Públicos N° 048-2022-SUNARP/SN que aprueba la actualización de la Política del Sistema Integrado de Gestión – SIG de la Superintendencia Nacional de los Registros Públicos publicada el 11 de abril del 2022.

- 4.8** Resolución de la Superintendencia Nacional de los Registros Públicos N° 099-2023-SUNARP/SN que reconfirma el Comité de Gobierno Digital de la Superintendencia Nacional de los Registros Públicos, publicada el 26 de mayo del 2023.
- 4.9** Resolución de la Gerencia General de los Registros Públicos N° 210-2022-SUNARP/GG que aprueba la Directiva DI-002-2022-UOM-OPPM, denominada “Directiva que regula la emisión de los documentos normativos de la Sunarp”, publicada el 04 de julio del 2022.
- 4.10** Marco de referencia y consulta
- a) NTP ISO/IEC 27001:2022 de Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición.
La Norma Técnica Peruana NTP-ISO/IEC 27001:2022 es la adopción nacional del estándar internacional ISO/IEC 27001:2022, por lo que en adelante se les denominará **ISO 27001**, indistintamente.
- b) NTP ISO/IEC 27002:2022 de Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición.
La Norma Técnica Peruana NTP-ISO/IEC 27002:2022 es la adopción nacional del estándar internacional ISO/IEC 27002:2022, por lo que en adelante se les denominará **ISO 27002**, indistintamente.
- c) NTP ISO/IEC 27003:2019 de Tecnología de la información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Orientación.
La Norma Técnica Peruana NTP-ISO/IEC 27003:2019 es la adopción nacional del estándar internacional ISO/IEC 27003:2017, por lo que en adelante se les denominará **ISO 27003**, indistintamente.
- d) NTP ISO/IEC 27003:2018 de Tecnología de la información. Técnicas de Seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación.
La Norma Técnica Peruana NTP-ISO/IEC 27004:2018 es la adopción nacional del estándar internacional ISO/IEC 27004:2016, por lo que en adelante se les denominará **ISO 27004**, indistintamente.

V. DEFINICIÓN DE TÉRMINOS Y SIGLAS

5.1 Definición de Términos

- a. **Acción correctiva:** Acción para eliminar la causa de una no conformidad y evitar que vuelva a ocurrir.
Nota: Existe diferencia entre corrección y acción correctiva.
- b. **Actividad:** Tarea o conjunto de tareas necesarias para realizar un proceso.
- c. **Alcance de la auditoría:** Extensión y límites de una auditoría.
Nota: El alcance de la auditoría incluye generalmente una descripción de las ubicaciones, las unidades de la organización, las actividades y los procesos.
- d. **Alta dirección:** Persona o grupo de personas que dirige y controla una organización al más alto nivel.
- e. **Auditado:** Organización, área o colaborador que es auditado.

- f. **Auditor:** Persona que lleva a cabo una auditoría.
- g. **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.
- h. **Conclusiones de la auditoría:** Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.
- i. **Conformidad:** Cumplimiento de un requisito.
- j. **Corrección:** Acción tomada para eliminar una no conformidad detectada (corrige el hecho puntual).
Ejemplo: reproceso o reclasificación.
Nota: Una corrección puede realizarse con anterioridad, simultáneamente, o después de una acción correctiva.
- k. **Criterios de auditoría:** Conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia objetiva.
Nota: Los criterios de auditoría se utilizan como una referencia frente a la cual se compara la evidencia de la auditoría.
- l. **Equipo auditor:** Uno o más personas que llevan a cabo una auditoría con el apoyo, si es necesario, de expertos técnicos.
Nota: un auditor del equipo auditor se le designa como auditor líder del mismo.
- m. **Evidencia de la auditoría:** Registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría y que es verificable.
- n. **Evidencia objetiva:** Datos que respaldan la existencia o veracidad de algo.
Nota 1: La evidencia objetiva puede obtenerse por medio de la observación, medición, ensayo o por otros medios.
Nota 2: La evidencia objetiva con fines de auditoría generalmente se compone de registros, declaraciones de hechos u otra información que son pertinentes para los criterios de auditoría y verificables.
- o. **Experto técnico:** Persona que aporta conocimientos o experiencia específicos al equipo auditor.
Nota: Un experto técnico no actúa como auditor en el equipo auditor.
- p. **Hallazgos de la auditoría:** Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.
Nota: Los hallazgos de la auditoría pueden indicar conformidad o no conformidad con los criterios de auditoría, u oportunidades de mejora.
- q. **Indicador:** Dato o conjunto de datos que ayudan a medir objetivamente la evolución de una actividad.
Es una medida asociada a una característica del resultado del bien y servicio, del proceso y del uso de los recursos; que permite a través de su medición en periodos sucesivos y por comparación con el estándar establecido, evaluar periódicamente dicha característica y verificar el cumplimiento de los objetivos evaluados.
- r. **Medición:** Acción y efecto de medir, de comparar una cantidad con su respectiva unidad, con el fin de averiguar cuantas veces la segunda está contenida en la primera.

- s. **Medida:** Expresión del resultado de una medición.
- t. **Mejora continua:** Actividad recurrente para mejorar el desempeño.

Nota: El proceso de establecer objetivos y de encontrar oportunidades para la mejora es un proceso continuo mediante el uso de hallazgos de la auditoría y de conclusiones de la auditoría, el análisis de los datos, de las revisiones por la dirección u otros medios, y generalmente conduce a una acción correctiva.
- u. **No conformidad:** Incumplimiento de un requisito.
- v. **Observación:** Situación detectada en el curso de una auditoría y apoyada por evidencias objetivas, que no representa incumplimiento de requisitos y que consiste en la identificación de aspectos puntuales por corregir.
- w. **Oportunidad de mejora:** Situación que no representa incumplimiento de requisitos pero que puede ser revisada por la institución para aumentar la capacidad de cumplir con los requisitos o mejorar la eficiencia de los mismos.
- x. **Plan de auditoría:** Descripción de las actividades y de los detalles acordados de una auditoría.
- y. **Programa de auditoría:** Conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

Nota: Un programa de auditoría incluye todas las actividades necesarias para planificar, organizar y llevar a cabo las auditorías.
- z. **Registro:** Documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas.

Nota 1: Los registros pueden utilizarse, por ejemplo, para formalizar la trazabilidad y para proporcionar evidencia de verificaciones y acciones correctivas.

Nota 2: El registro también puede estar constituido por el conjunto ordenado de documentos de la misma naturaleza que se producen en el proceso de operación del SGSI. En ese sentido, registro es sinónimo de archivo¹.

Ejemplo: El archivo de informes de auditoría.
- aa. **Seguimiento:** Verificación, supervisión, observación crítica o determinación del desarrollo de un proceso o acción.
- bb. **Suficiente:** Disponer de información relevante con adecuado nivel de detalle.
- cc. **Verificación:** Confirmación mediante la aportación de evidencia objetiva, de que se han cumplido los requisitos para una utilización o aplicación específica prevista.

5.2 Siglas:

- a. **AL** Auditor Líder (líder del equipo de auditores internos)
- b. **CGD** Comité de Gobierno Digital
- c. **OSCD** Oficial de Seguridad y Confianza Digital (o quien haga las veces)
- d. **EqA** Equipo de Auditores Internos
- e. **EqTTYM** Equipo de Trabajo Técnico y Multidisciplinario
- f. **GG** Gerencia General

¹ En concordancia con el diccionario de la Real Academia Española: <https://dle.rae.es/archivo>

- g. **SGSI** Sistema de Gestión de Seguridad de la Información
- h. **SI** Seguridad de la Información
- i. **SN** Superintendencia Nacional
- j. **SUNARP** Superintendencia Nacional de los Registros públicos
- k. **TICs** Tecnologías de la Información y Comunicación
- l. **PAA** Programa Anual de Auditorías
- m. **PAI** Plan de Auditoría Interna

VI. RESPONSABILIDADES

- 6.1** Del CGD: Es responsable de proponer acciones a la SN y a la GG sobre los aspectos de su competencia.
- 6.2** Del OSCD: Es responsable de brindar orientación técnica respecto del presente procedimiento y de informar al CGD sobre su cumplimiento.
- 6.3** De las UO involucradas en la ejecución de los procedimientos: Brindar las facilidades necesarias para su cumplimiento.

VII. DISPOSICIONES GENERALES

7.1 Enfoque de la Evaluación del Desempeño

[Referencia: ISO 27001 cláusula 9]

En la evaluación del desempeño, la norma ISO 27001 define textualmente lo siguiente:

“9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

- a) *a qué se necesita hacer seguimiento y ser medido, incluyendo procesos y controles de seguridad de la información;*
- b) *los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos. Los métodos seleccionados deberían producir resultados comparables y reproducibles para ser considerados válidos;*
- c) *cuando se debe realizar el seguimiento y medición;*
- d) *quién debe realizar el seguimiento y medición;*
- e) *cuando los resultados del seguimiento y medición deben ser analizados y evaluados;*
- f) *quién debe analizar y evaluar estos resultados.*

La información documentada debe estar disponible como evidencia de los resultados.

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

9.2 Auditoría interna

9.2.1 Generalidades

La organización debe conducir auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

- a) *está en conformidad con:*
 - 1) *los requisitos de la propia organización para su sistema de gestión de seguridad de la información; y*

- 2) los requisitos de esta Norma Técnica Peruana;
b) está eficazmente implementado y mantenido.

9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación e informes.

Cuando se establezca el (los) programa(s) de auditoría interna, la organización debe tomar en consideración la importancia de los procesos involucrados y los resultados de auditorías previas;

La organización debe:

- a) definir los criterios y el alcance de cada auditoría;
- b) seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad del proceso de auditoría;
- c) asegurar que los resultados de las auditorías se reporten a los gerentes pertinentes.

Información documentada debe estar disponible como evidencia de la implementación del (de los) programa(s) de auditoría y los resultados de la auditoría.

9.3 Revisión por la dirección

9.3.1 Generalidades

La alta dirección debe revisar el sistema de gestión de seguridad de la información de la organización a intervalos planificados para asegurar su idoneidad, adecuación y eficacia continua.

9.3.2 Entradas para la revisión por la dirección

La revisión por la dirección debe incluir consideraciones de:

- a) el estado de las acciones de las revisiones por la dirección anteriores;
- b) cambios en las cuestiones externas e internas que son pertinentes al sistema de gestión de seguridad de la información;
- c) cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información;
- d) retroalimentación sobre el desempeño de seguridad de la información, incluyendo tendencias en:
 - 1) no conformidades y acciones correctivas;
 - 2) resultados del seguimiento y medición;
 - 3) resultados de auditoría;
 - 4) cumplimiento de los objetivos de seguridad de la información;
- e) retroalimentación de partes interesadas;
- f) resultados de la evaluación de riesgo y estado del plan de tratamiento de riesgos;
- g) oportunidades para la mejora continua.

9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección deben incluir decisiones relacionadas a oportunidades de mejora continua y cualquier necesidad de cambios al sistema de gestión de seguridad de la información.

La información documentada debe estar disponible como evidencia de los resultados de revisiones por parte de la dirección.”

7.2 Evaluación del Desempeño en la Sunarp

La Evaluación del Desempeño en la Sunarp está compuesto por los siguientes procesos y subprocesos:

- PROCESO: **Seguimiento, medición, análisis y evaluación**
- PROCESO: **Auditoría interna**
 - SUB PROCESO: **Programación Anual de Auditorías**
 - SUB PROCESO: **Planificación de Auditorías Internas**
 - SUB PROCESO: **Desarrollo de la Auditoría Interna**
- PROCESO: **Revisión por la dirección**

La interacción de estos procesos y subprocesos se detallan en el *Diagrama A* del Anexo N° 1.

VIII. DESCRIPCIÓN DEL PROCEDIMIENTO

8.1 PROCESO: Seguimiento, medición, análisis y evaluación

[Referencia: ISO 27004]

8.1.1 Oportunidad de Ejecución del Proceso

Este proceso se compone de tres fases, las cuales se deben ejecutar en los siguientes momentos:

- **Fase 1: Identificar:**
Esta fase se debe ejecutar con periodicidad anual, sin embargo, es posible realizar modificaciones en el momento que decida el Comité de Gobierno Digital.
- **Fase 2: Seguimiento y Medición:**
Esta fase se debe ejecutar de acuerdo a lo establecido en cada *Ficha de Medición*, sin embargo, es posible realizar modificaciones a solicitud del OSCD con aprobación del Comité de Gobierno Digital.
- **Fase 3: Análisis y Evaluación:**
Esta fase se debe ejecutar por lo menos una vez al año y antes de la Auditoría Interna.

8.1.2 Propósito

El *seguimiento* y la *medición* del SGSI se realiza para conocer y calificar el resultado de las actividades de seguridad de la información, incluida la evaluación y tratamiento de riesgos, respecto a lo planificado.

El *seguimiento*, también denominado monitoreo, determina el estado de un sistema, un proceso o una actividad, mientras que la *medición* es un proceso para determinar un valor. Por lo tanto, el seguimiento se puede lograr a través de una sucesión de mediciones similares durante un período de tiempo.

8.1.3 Documentos

De entrada		De salida	
N°	Descripción	N°	Descripción
01	Cambios en aspectos externos y/o internos que afectan el SGSI	01	Lista priorizada de Necesidades de Información
02	Información documentada del SGSI	02	Fichas de Medición
03	Fichas de Medición previas	03	Informe del Seguimiento, medición, análisis y evaluación

El formato de una *Lista priorizada de Necesidades de Información* se adjunta en el Anexo N° 2.

El formato de la *Ficha de Medición* priorizada se adjunta en el Anexo N° 3.

8.1.4 Diagrama del proceso

El flujo de las actividades se detalla en el *Diagrama B* del Anexo N° 1.

8.1.5 Actividades y Tareas

N°	Actividad	Tareas	Responsable
Fase 1: Identificar			
1.	Identificar las necesidades de información	a) Elaborar una <i>Lista preliminar de Necesidades de Información</i> y priorizarla. b) Seleccionar las Necesidades de Información que se necesita hacer seguimiento y ser medido.	OSCD
Fase 2: Seguimiento y Medición			
2.	Crear y mantener las mediciones	a) Identificar las prácticas de seguridad actuales que pueden soportar las Necesidades de Información. b) Elaborar o actualizar la <i>Ficha de Medición</i> de las <i>Necesidades de Información</i> de la lista aprobada. c) Gestionar la aprobación de las fichas de <i>Necesidades de Información</i> .	OSCD
3.	Seguimiento y medición	a) Realizar el seguimiento y medición de acuerdo con lo definido en la <i>Ficha de Medición</i> Nota: Recolectar suficientes datos para garantizar que los resultados del análisis son confiables. b) Conservar la información de los seguimientos y mediciones realizadas	Responsable(s) de cada <i>Ficha de Medición</i>
Fase 3: Análisis y Evaluación			
4.	Analizar los resultados	a) En cada <i>Ficha de Medición</i> , analizar los datos recopilados en relación con la meta para cada medición individual. b) Interpretar los resultados del análisis de datos obteniendo conclusiones iniciales basadas en dichos resultados. Nota: Todas las interpretaciones deberían tener en cuenta el contexto de las mediciones.	OSCD
5.	Evaluar el Seguimiento, medición, análisis y evaluación	a) Elaborar el <i>Informe del Seguimiento, medición, análisis y evaluación</i> .	OSCD

8.2 PROCESO: Auditoría interna

[Referencia: ISO 27001 cláusula 9.2]

8.2.1 Propósito

Las *auditorías internas* se realizan para proporcionar información sobre si el SGSI cumple con los requisitos propios de la organización para su SGSI, así como con los requisitos de ISO/IEC 27001. Los requisitos propios de la organización incluyen:

- Requisitos establecidos en la política y procedimientos de seguridad de la información;
- Requisitos producidos por el marco de referencia para establecer objetivos de seguridad de la información, incluidos los resultados del proceso de tratamiento de riesgos;
- Requisitos legales y contractuales; y
- Requisitos sobre la información documentada.

Los auditores también evalúan si el SGSI se implementa y mantiene efectivamente.

Las Auditorías Internas se deben realizar por lo menos una vez al año.

Este proceso se compone de los siguientes sub procesos:

- Programación Anual de Auditorías
- Planificación de Auditorías Internas
- Desarrollo de la Auditoría Interna

8.2.2 Documentos

De entrada		De salida	
N°	Descripción	N°	Descripción
01	Cambios en aspectos externos y/o internos que afectan el SGSI	01	Programa Anual de Auditorías (PAA)
02	Información documentada del SGSI	02	Plan de Auditoría Interna (PAI)
03	Informe del Seguimiento, medición, análisis y evaluación	03	Informe de Auditoría Interna del SGSI
04	Informes de auditorías del SGSI previas		
05	Actas de Revisión por la Dirección previas		

8.2.3 SUB PROCESO: Programación Anual de Auditorías

a) Oportunidad de Ejecución del Subproceso

Este subproceso se debe ejecutar con periodicidad anual, sin embargo, es posible realizar modificaciones a lo programado en el momento que decida el Comité de Gobierno Digital.

b) Diagrama del Subproceso

El flujo de las actividades se detalla en el *Diagrama C* del Anexo N° 1.

c) Actividades y Tareas

N°	Actividad	Descripción	Responsable
Programación Anual de Auditorías			
1.	Elaborar el PAA (Plan anual de Auditorías)	b) Elaborar el Plan anual de Auditorías (PAA) del SGSI, para el periodo de un año, definiendo las áreas a auditar y las fechas de ejecución de las auditorías. Nota: La planificación toma en consideración el estado y la importancia de los procesos y áreas a auditar, así como los resultados de las auditorías previas.	OSCD
2.	Revisar y Evaluar PAA	a) Evaluar la propuesta y, en caso de: Aprueba el PAA del SGSI: <ul style="list-style-type: none">Se registra como acuerdo del Comité para continuar trámite en el punto 3 de este procedimiento. Desaprueba el PAA del SGSI: <ul style="list-style-type: none">Plantear las modificaciones convenientes y regresa al punto 1 de este procedimiento.	CGD
3.	Gestionar difusión del PAA	a) Gestionar la difusión interna del Programa Anual de Auditorías (PAA).	OSCD

8.2.4 SUB PROCESO: Planificación de la Auditoría Interna

a) Oportunidad de Ejecución del Subproceso

Este subproceso se debe ejecutar antes de cada Auditoría Interna programada en el *Programa Anual de Auditorías (PAA)*.

b) Diagrama del Subproceso

El flujo de las actividades se detalla en el *Diagrama D* del Anexo N° 1.

c) Actividades y Tareas

N°	Actividad	Descripción	Responsable
Planificación de la Auditoría Interna			
1.	Designar al Auditor Líder (AL)	a) Designar al Auditor Líder (AL) para que dirija el proceso de auditoría interna y las actividades del equipo auditor.	CGD

N°	Actividad	Descripción	Responsable
		Nota: de considerarlo conveniente, puede elegirse como auditor líder o encargar la ejecución de la auditoría interna a personas externas a la Institución, en todos los casos debe cumplir con el Perfil del Puesto del Auditor Líder (Véase Anexo A).	
2.	Seleccionar el Equipo Auditor (EqA)	a) Recibir la designación. b) Seleccionar a los auditores internos que van a realizar la auditoría. Los equipos formados deben estar integrados por personas que no tengan compromiso directo con la actividad a auditar. Nota: de considerarlo conveniente, puede elegirse como auditor interno a personas externas a la Institución, en todos los casos debe cumplir con el Perfil del Puesto del Auditor Interno (Véase Anexo B).	AL
3.	Elaborar el Plan de Auditoría Interna (PAI)	a) Estudiar la información documentada del SGSI correspondiente a la actividad a auditar, incluyendo los informes de auditorías anteriores y el <i>Informe de Evaluación del Desempeño de la Seguridad de la Información y la Eficacia del SGSI</i> . b) Elabora un Plan de Auditoría Interna (PAI), distribuyendo y organizando el trabajo con el Equipo Auditor (EqA). c) Comunica y remite el PAI al CGD, a los responsables de las áreas auditadas, al equipo auditor (EqA) y al OSCD, por lo menos con una semana de anticipación. d) Coordina con el OSCD la(s) fecha(s) y hora(s) de ejecución de la auditoría, a fin de asegurar su disponibilidad de los participantes durante la auditoría interna. En caso de existir inconveniente y a solicitud del responsable del área auditada, coordina la reprogramación hasta dos días antes de lo programado.	AL, EqA, CGD, OSCD
4.	Estar informado	a) Mantenerse informado sobre el PAI.	CGD, OSCD

8.2.5 SUB PROCESO: Desarrollo de la Auditoría Interna

a) Oportunidad de Ejecución del Subproceso

Este subproceso se ejecuta en los días planificados en el *Plan de Auditoría Interna (PAI)*, según lo programado en el *Programa Anual de Auditorías (PAA)*.

b) Diagrama del Subproceso

El flujo de las actividades se detalla en el *Diagrama E* del Anexo N° 1.

c) Actividades y Tareas

N°	Actividad	Descripción	Responsable
Desarrollo de la Auditoría Interna			
1.	Preparar la Auditoría Interna	a) Revisar la documentación pertinente de los procesos a auditar teniendo en consideración los resultados de auditorías previas y las cláusulas de la ISO 27001.	AL
2.	Iniciar la Auditoría	a) Realiza la Reunión de Apertura con el personal involucrado de acuerdo al Plan de Auditoría Interna establecido, confirmando los horarios, responsables y procesos a ser auditados; en caso de ser necesario, de forma excepcional y a solicitud del responsable del área auditada, modifica el Plan de Auditoría.	AL
3.	Ejecutar la Auditoría	a) Audita los procesos y/o áreas previstas haciendo uso de los criterios de auditoría definidos en el Plan de Auditoría y la información documentada del SGSI, con la finalidad de verificar la eficacia del SGSI, procediendo a recoger evidencias objetivas de las mismas a través de los siguientes medios: <ul style="list-style-type: none"> • entrevistas, • observación de actividades efectuadas, • revisión de documentos y registros. b) Para el efecto, realiza un examen por muestreo de los expedientes, registros, certificados, etc., según corresponda.	EqA
4.	Consolidar información de la Auditoría	a) Una vez finalizada la recolección de información, hallazgos y evidencias en la auditoría de campo, el EqA se reúne para analizar y evaluar lo encontrado. b) Los miembros del EqA consolidan la información y preparan sus conclusiones finales para ser presentadas a las áreas auditadas.	EqA
5.	Finalizar la Auditoría	a) El AL realiza la Reunión de Cierre de acuerdo al Plan de Auditoría Interna. b) El AL, comunica a las áreas auditadas sobre el resultado de la auditoría, explicando las no conformidades, observaciones y oportunidad de mejora encontradas.	AL, Auditados
6.	Elaborar el Informe de Auditoría Interna	a) Elaborar un Informe de Auditoría Interna, dicho informe deberá ser entregado al CGD. Nota: El AL es responsable de entregar los informes en el tiempo previsto, en caso de incumplimiento, El CGD tomará acciones pertinentes.	AL
7.	Revisar el Informe de Auditoría Interna	a) Revisar el Informe de Auditoría Interna. b) Distribuir el Informe de Auditoría a los responsables de las áreas auditadas, en la parte que les compete.	OSCD

 <small>Superintendencia Nacional de los Registros Públicos</small>	Procedimientos para la Evaluación del Desempeño del SGSI	Codificación: PR-001-2024-SUNARP-CGD
---	---	---

N°	Actividad	Descripción	Responsable
		c) Gestionar el tratamiento de las No Conformidades con los responsables de las áreas involucradas. d) Mantener informado al CGD.	
8.	Realizar seguimiento a la Auditoría Interna	a) En caso sea necesario, programar la visita de seguimiento de acuerdo con las fechas de implementación propuestas o fechas de verificación determinadas en visitas de seguimiento previas, con el objeto de verificarla adecuada implementación de las acciones correctivas o preventivas.	AL
9.	Estar informado	a) Mantenerse informado sobre el PAI.	CGD, Auditados

8.3 PROCESO: Revisión por la Dirección

[Referencia: ISO 27001 cláusula 9.3]

8.3.1 Oportunidad de Ejecución del Proceso

Este subproceso se debe ejecutar con periodicidad anual, sin embargo, es posible realizar las revisiones que el Comité de Gobierno Digital considere necesarios.

8.3.2 Propósito

El propósito de la *Revisión por la Dirección* es garantizar la idoneidad, adecuación y eficacia continuas del SGSI. La idoneidad se refiere a la alineación continua con los objetivos de la organización. La adecuación y la eficacia se refieren a un diseño adecuado y a la integración organizativa del SGSI, así como a la implementación efectiva de procesos y controles que son llevados a cabo por el SGSI.

En este proceso, la Dirección se considera a Superintendencia Nacional y a la Gerencia General. La Dirección es la máxima responsable de la *Revisión por la Dirección*, con aportes del Comité de Gobierno Digital y, en caso se requiera, otros niveles de la organización.

Las revisiones extraordinarias del SGSI, a criterio de la Dirección, se llevarán a cabo en los siguientes casos:

- Cuando la revisión ordinaria del SGSI requiera de otra(s) revisión(es) adicional(es) debido a la complejidad o volumen de información a revisar.
- Debido a la criticidad de algún evento o incidente de seguridad, o cambios significativos que puedan afectar la efectividad o continuidad del SGSI.
- Cuando la Dirección lo considere necesario para la toma de decisiones respecto al SGSI.

8.3.3 Documentos

De entrada		De salida	
N°	Descripción	N°	Descripción

 sunarp <small>Superintendencia Nacional de los Registros Públicos</small>	Procedimientos para la Evaluación del Desempeño del SGSI	Codificación: PR-001-2024-SUNARP-CGD
--	---	---

01	Cambios en aspectos externos y/o internos que afectan el SGSI	01	Acta de Revisión por la Dirección
02	Resultados de monitoreo y medición (resumen ejecutivo)		
03	Resultados de la auditoría (resumen ejecutivo)		
04	Resultados de "Revisiones por la Dirección" previas (resumen ejecutivo)		
05	Resultados de la gestión de riesgos e incidentes (resumen ejecutivo)		

8.3.4 Diagrama del Subproceso

El flujo de las actividades se detalla en el *Diagrama F* del Anexo N° 1.

8.3.5 Actividades y Tareas

N°	Actividad	Descripción	Responsable
Preparación de la información de entrada para la revisión por la Dirección			
1.	Consolidar información de entrada	a) Durante el periodo previo a la revisión, se realiza la consolidación de la información o documentación considerada de entrada, asimismo cualquier otra información considerada relevante por los propietarios/custodios de activos de la información y otras partes interesadas.	OSCD
Planificación para la Revisión del SGSI por la Dirección			
2.	Gestionar la reunión de revisión	a) Coordina con la Dirección la revisión del SGSI, a fin de definir el lugar, fecha, hora y asistentes: miembros del comité y otros participantes convocados cuya participación sea pertinente para la reunión de revisión. b) Gestionar la convocatoria a reunión con la Dirección y demás partes interesadas para la revisión del SGSI, especificando la fecha y hora establecida.	OSCD
Desarrollo de la Revisión por la Dirección del SGSI			
3.	Iniciar la reunión	a) Llegada la fecha, hora y en el lugar establecido, iniciar la reunión de revisión del SGSI.	CGD
4.	Ejecutar la revisión	a) Analizar y evaluar el SGSI en base a la documentación de entrada, con el apoyo del OSCD y otros involucrados, para el sustento de cada uno de los puntos.	CGD
5.	Finalizar la reunión	b) Determina acuerdos y acciones a tomar para la mejora del SGSI en base a la revisión realizada.	CGD

 <small>Superintendencia Nacional de los Registros Públicos</small>	Procedimientos para la Evaluación del Desempeño del SGSI	Codificación: PR-001-2024-SUNARP-CGD
---	---	---

		c) Elaboración y firma del Acta de Revisión por la Dirección.	
--	--	---	--

IX. DISPOSICIONES COMPLEMENTARIAS

a. Propietario del documento: Comité de Gobierno Digital (CGD)

Los aspectos técnicos no contemplados en el presente Procedimiento, serán resueltos por el Comité de Gobierno Digital.

Las modificaciones o mejoras serán canalizados al Oficial de Seguridad y Confianza Digital (OSCD).

b. Clasificación del documento: USO INTERNO

c. Distribución: COPIA NO CONTROLADA (*)

X. REGISTROS

Descripción	Archivamiento	Retención
Archivo de Fichas de Medición	Repositorio del SGSI	Permanente
Archivo de Informes del Seguimiento, medición, análisis y evaluación	Repositorio del SGSI	Permanente
Archivo de Programas Anuales de Auditorías	Repositorio del SGSI	Permanente
Archivo de Planes de Auditorías Internas	Repositorio del SGSI	Permanente
Archivo de Informes de Auditorías Internas del SGSI	Repositorio del SGSI	Permanente
Archivo de Actas de Revisión por la Dirección	Repositorio del SGSI	Permanente

XI. ANEXOS

Anexo	Descripción
Anexo N° 1	Diagramas de Flujo
Anexo N° 2	Formato de Lista priorizada de Necesidades de Información
Anexo N° 3	Formato de Ficha de Medición
Anexo N° 4	Formato de Programa Anual de Auditorías (PAA)
Anexo N° 5	Formato de Plan de Auditoría Interna (PAI)
Anexo N° 6	Formato de Informe de Auditoría Interna del SGSI
Anexo N° 7	Perfil del Auditor Líder de Seguridad de la Información
Anexo N° 8	Perfil del Auditor Interno de Seguridad de la Información

CUADRO DE CONTROL DE MODIFICACIONES DEL DOCUMENTO NORMATIVO

Codificación	PR- -2024-CGD-GG
Documento Normativo	Procedimientos para la Evaluación del Desempeño del SGSI

N°	Estado	Resolución de Aprobación	Fecha de Aprobación
1	Originaria	Resolución N° ...-2024-SUNARP/GG	... / 05 /2024

Anexo N° 1 Diagramas de Flujo

Diagrama A:

Evaluación del Desempeño en la Sunarp

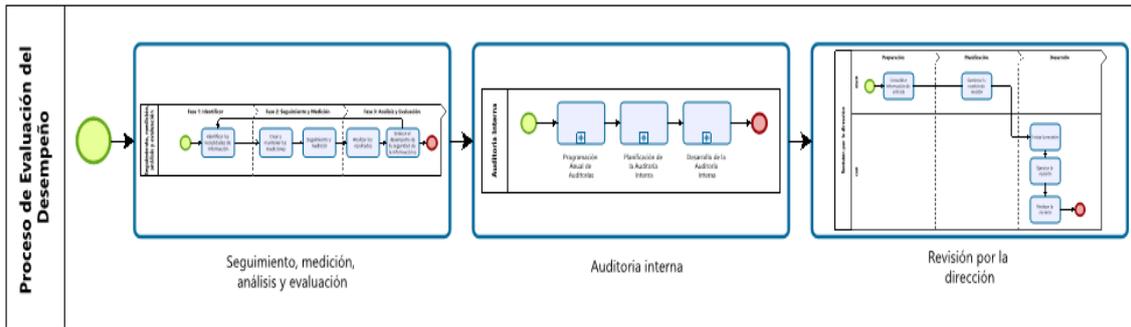


Diagrama B:

PROCESO: Seguimiento, medición, análisis y evaluación

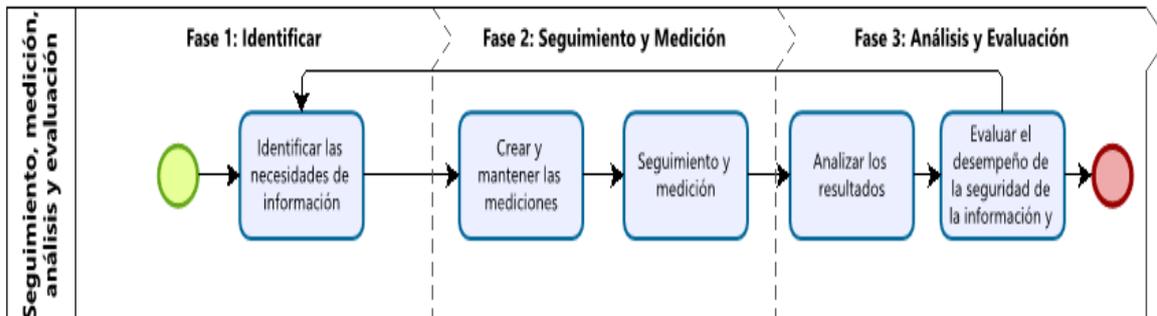


Diagrama C:

SUB PROCESO: Programación Anual de Auditorías

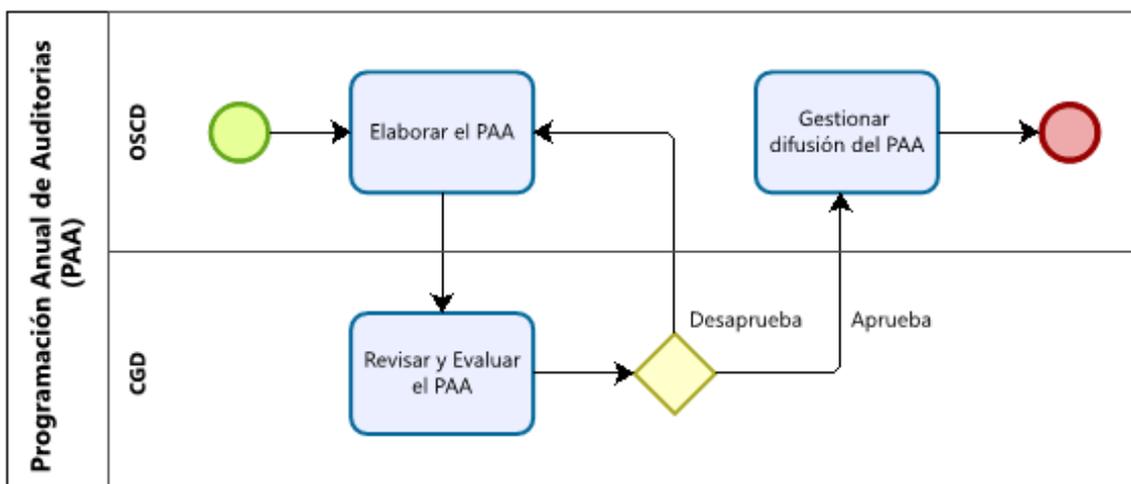


Diagrama D:

SUB PROCESO: Planificación de la Auditoría Interna

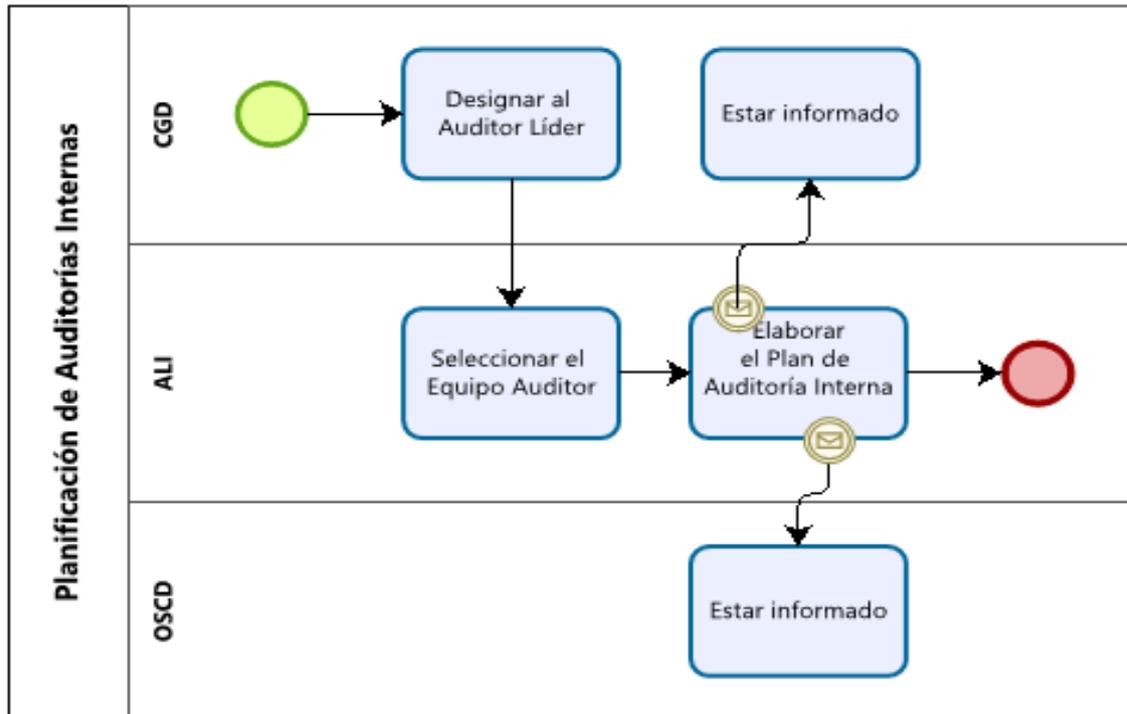


Diagrama E:

SUB PROCESO: Desarrollo de la Auditoría Interna

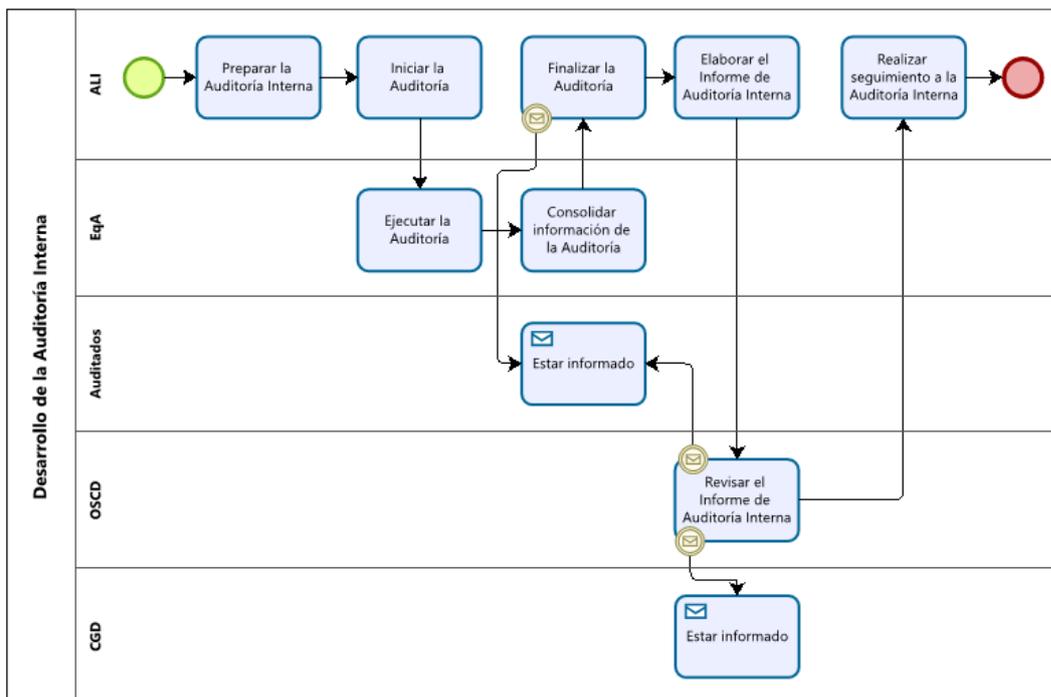
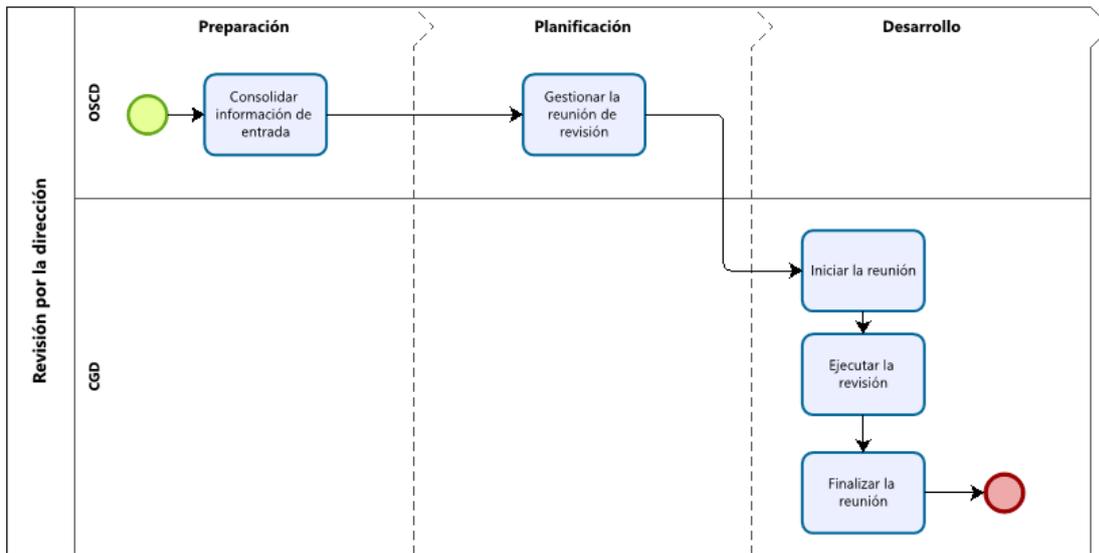


Diagrama F:

PROCESO: Revisión por la dirección



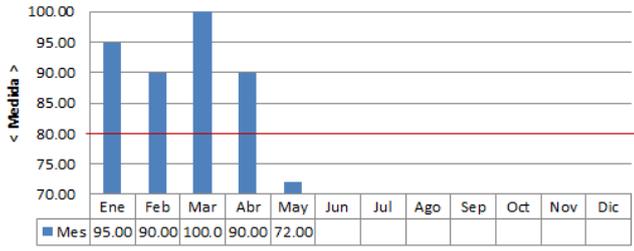
Anexo N° 2

Formato de Lista priorizada de Necesidades de Información

	SGSI-SUNARP		Código:
	Sistema de Gestión de Seguridad de la Información		Versión: v1.0
	Documento asociado: Procedimientos para la Evaluación del Desempeño del SGSI		Clasificación: USO INTERNO
Lista priorizada de Necesidades de Información			
N°	Propuesta de necesidad de medición	Control relacionado	Prioridad
1			1°
2			2°
3			3°
4			4°
5			5°
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
<i>Firmas de los participantes:</i>			

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 3 Formato de Ficha de Medición

Descriptor de información	Significado o propósito																												
SGSI-SUNARP		Código:																											
Sistema de Gestión de Seguridad de la Información		Versión:	v1.0																										
Documento asociado: Procedimientos para la Evaluación del Desempeño del SGSI		Clasificación:	USO INTERNO																										
Ficha de Medición																													
ID de medida:																													
Necesidad de información:																													
Partes responsables:																													
Revisión y aprobación:																													
Frecuencia:																													
Objetivo:			Estado																										
Meta:	>= 80%																												
Fórmula / puntuación	< 80%																												
Fecha:																													
Medida:																													
Fuente de datos:																													
Histórico de medición:	< Necesidad de Información >		Resultado en el período																										
	 <table border="1" style="margin-top: 5px; font-size: small;"> <thead> <tr> <th>Mes</th> <th>Ene</th> <th>Feb</th> <th>Mar</th> <th>Abr</th> <th>May</th> <th>Jun</th> <th>Jul</th> <th>Ago</th> <th>Sep</th> <th>Oct</th> <th>Nov</th> <th>Dic</th> </tr> </thead> <tbody> <tr> <td>Medida</td> <td>95.00</td> <td>90.00</td> <td>100.00</td> <td>90.00</td> <td>72.00</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		Mes	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Medida	95.00	90.00	100.00	90.00	72.00								72% 
	Mes	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic																
Medida	95.00	90.00	100.00	90.00	72.00																								
		Resultado acumulado																											
		89% 																											
Análisis y acciones correctivas																													
Firma partes responsables:			Fecha: __/__/2024																										
Firma revisor:			Fecha: __/__/2024																										

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 4 Formato de Programa Anual de Auditorías (PAA)

		SGSI-SUNARP Sistema de Gestión de Seguridad de la Información										Código:		
		Documento asociado: Procedimientos para la Evaluación del Desempeño del SGSI										Versión: v1.0		
												Clasificación: USO INTERNO		
Programa Anual de Auditorías (PAA)														
2024														
N° Auditoría	Tipo auditoría	Procesos	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
01-2024	Interna	Proceso 1				X						X		
		...				X						X		
		Proceso n				X						X		
01-2024	Externa	Proceso 1											X	
		...											X	
		Proceso n											X	
										Elaborado por:		Aprobado por:		
										OSCD		CGD		
										Firma:		Firma:		
										Fecha de aprobación: / /2024				

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 5 Formato de Plan de Auditoría Interna (PAI)

SGSI-SUNARP		Código:		
Sistema de Gestión de Seguridad de la Información		Versión: v1.0		
Documento asociado: Procedimientos para la Evaluación del Desempeño del SGSI		Clasificación: USO INTERNO		
Plan de Auditoría Interna (PAI)				
PLAN DE AUDITORÍA INTERNA DEL SGSI				
1. Auditoría Interna N°:	01-2024			
2. Fecha(s) de ejecución:	dd/mm/aaa			
3. Lugar(es):				
4. Objetivo:				
5. Criterios de la auditoría:				
6. Alcance:				
7. Equipo Auditor:				
Auditor(a) Líder	Auditor(a) Interno(a)	Área a la que pertenece		
Auditor	Auditor interno 1			
	...			
	Auditor interno n			
DETALLE DEL PLAN DE AUDITORÍA INTERNA				
Primer Día < fecha dd/mm/aaaa >				
Área	Contacto	Aspectos / requisitos a evaluar	Auditor	Hora
Reunión de apertura				08:00 am a 08:30 am
Receso para almorzar				12:30 am a 13:30 pm
Reunión de cierre				16:30 am a 17:00 pm
			Elaborado por:	Aprobado por:
			Auditor Líder	CGD
			Firma:	Firma:
			Fecha de aprobación: / /2024	

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 6 Formato de Informe de Auditoría Interna del SGSI

SGSI-SUNARP		Código:
Sistema de Gestión de Seguridad de la Información		Versión: v1.0
Documento asociado: Procedimientos para la Evaluación del Desempeño del SGSI		Clasificación: USO INTERNO
Informe de Auditoría Interna		
PLAN DE AUDITORÍA INTERNA DEL SGSI		
1. Auditoría Interna N°:	01-2024	
2. Fecha(s) de ejecución:	dd/mm/aaa	
3. Lugar(es):		
4. Objetivo:		
5. Criterios de la auditoría:		
6. Alcance:		
7. Equipo Auditor:		
Auditor(a) Líder	Auditor(a) Interno(a)	Área a la que pertenece
Auditor	Auditor interno 1	
	...	
	Auditor interno n	
RESUMEN DE LA AUDITORÍA INTERNA		
Numero de No Conformidades:		
Número de Observaciones:		
Aspectos positivos:		
Oportunidades de mejora:		
Recomendaciones:		
Elaborado por:		Aprobado por:
Auditor Líder		CGD
Firma:		Firma:
Fecha: ___/___/2024		

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Informe de Auditoría Interna en detalle

A continuación, se muestra el resultado de la auditoría interna del SGSI de la sunarp por cada cláusula de la norma y por cada dominio del Anexo A:

4. CONTEXTO DE LA ORGANIZACIÓN

5. LIDERAZGO

6. PLANEACIÓN

7. SOPORTE

8. OPERACIÓN

9. EVALUACIÓN DEL DESEMPEÑO

10. MEJORA

Anexo A

ANEXO A: 5. CONTROLES ORGANIZACIONALES

ANEXO A: 6. CONTROLES DE PERSONAS

ANEXO A: 7. CONTROLES FÍSICOS

ANEXO A: 8. CONTROLES TECNOLÓGICOS

Nota: Imagen referencial, por favor utilizar el archivo editable de este formato.

Anexo N° 7

Perfil del Auditor Líder de Seguridad de la Información

1. Función:

El Auditor Líder planifica y gestiona las auditorías internas al Sistema de Gestión de la Seguridad de la Información (SGSI) conforme al Programa Anual de Auditorías (PAA), Plan de Auditorías Internas (PAI) y a los requerimientos específicos para la realización eficiente y eficaz de las auditorías.

Reporta al Presidente del Comité de Gobierno Digital (CGD).

Tiene autoridad para realizar la revisión documental y de campo para verificar el cumplimiento normativo del SGSI.

2. Perfil²:

Formación : Profesional titulado

Especialización : Curso de Auditor Líder ISO 27001.

Curso de Auditor Interno ISO 27001.

Experiencia : Personal de la Sunarp con más de cinco años en la institución.

Experiencia mayor de dos años en auditorías.

3. Habilidades:

Personales³ : Ético, de mentalidad abierta, diplomático, observador, perceptivo, versátil, tenaz, decidido, seguro de sí mismo, firme, abierto a la mejora, colaborador, destreza verbal y escrita.

Liderazgo : Capacidad para organizar, dirigir, orientar y establecer relaciones interpersonales armoniosas con el equipo auditor

Dirección : Representar al equipo auditor.

Capacidad para gestionar el proceso de auditoría, la incertidumbre, analizar problemas, prevenir y resolver conflictos.

Negociación.

Planeación : Integración de planes y programas a corto, mediano y largo plazo.

Organización : Organización del Trabajo.

Interpretación de estructuras organizacionales.

Control : Análisis e interpretación de los resultados de los programas y proyectos.

Análisis, interpretación y supervisión de la aplicación del marco normativo de la Institución.

4. Responsabilidades:

Las responsabilidades del Auditor Líder se encuentran detallados en el documento “*Manual de Roles y Responsabilidades para la Seguridad de la Información*”.

² Cuando el personal no cumpla con la competencia declarada en el presente documento, será necesario emprender las acciones o proporcionar los cursos correspondientes, incluyendo la experiencia en auditorías.

³ Basado en la ISO 19011, Directrices para la auditoría de los sistemas de gestión.

Anexo N° 8

Perfil del Auditor Interno de Seguridad de la Información

1. Función:

El Auditor Interno participa activamente en la planificación, preparación y ejecución de las auditorías internas al Sistema de Gestión de la Seguridad de la Información (SGSI) conforme al Plan de Auditorías Internas (PAI) y a los requerimientos específicos.

Reporta al Auditor Líder de Seguridad de la Información.

Tiene autoridad para realizar la revisión documental y de campo para verificar el cumplimiento normativo del SGSI.

2. Perfil⁴:

Formación : Profesional titulado

Especialización : Curso de Auditor Interno ISO 27001.

Experiencia : Personal de la Sunarp con más de tres años en la institución.
Experiencia mayor de un año en auditorías.

3. Habilidades:

Personales⁵ : Ético, de mentalidad abierta, diplomático, observador, perceptivo, versátil, tenaz, decidido, seguro de sí mismo, firme, abierto a la mejora, colaborador.

Liderazgo, capacidad para establecer relaciones interpersonales y de equipo, destreza verbal y escrita.

Planeación : Integración de planes y programas a corto, mediano y largo plazo.

Organización : Organización del Trabajo.
Interpretación de estructuras organizacionales.

Dirección : Análisis de problemas.
Manejo de conflictos.
Negociación.

Control : Análisis e interpretación de los resultados de los programas y proyectos.
Análisis, interpretación y supervisión de la aplicación del marco normativo de la Institución.

4. Responsabilidades:

Las responsabilidades del Auditor Interno se encuentran detallados en el documento "*Manual de Roles y Responsabilidades para la Seguridad de la Información*".

⁴ Cuando el personal no cumpla con la competencia declarada en el presente documento, será necesario emprender las acciones o proporcionar los cursos correspondientes, incluyendo la experiencia en auditorías.

⁵ Basado en la ISO 19011, Directrices para la auditoría de los sistemas de gestión.