Metodología para la Implementación del Sistema de Gestión de Seguridad de la Información (SGSI)

Versión	Fecha	Control de Cambios
00	19/09/2025	• Versión inicial.

Áreas Responsables	Nombre y cargo
Elaborado: Departamento de Tecnología de Información y Comunicaciones	Moisés Palomino Jefe del Departamento de Tecnología de Información y Comunicaciones
Homologado: Oficina de Planeamiento y Mejora Continua	Deymer Barturén Especialista en Calidad y Mejora de Procesos Miguel Tito Jefe de la Oficina de Planeamiento y Mejora Continua
Revisado y aprobado: Gerencia de Administración y Finanzas	Julio Temple Gerente de Administración y Finanzas

INDICE

I. OBJETIVO

Brindar pautas, orientación y soporte para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de Activos Mineros S.A.C. (en adelante AMSAC), que sea eficaz y orientado a mejorar su desempeño en el cumplimiento de las expectativas de seguridad de la información de entidades del Estado, proveedores, clientes y otras partes interesadas pertinentes.

II. ALCANCE

Esta metodología es aplicable para los colaboradores que asumen roles y responsabilidades del SGSI y debe ser utilizada para servir como guía de implementación del SGSI en AMSAC.

III. DOCUMENTOS DE REFERENCIA

La metodología está alineada a las siguientes normativas y buenas prácticas.

- Ley N° 29733 - Ley de Protección de Datos Personales y su reglamento aprobado mediante Decreto Supremo N° 016-2024-JUS.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, su reglamento aprobado mediante Decreto Supremo N° 029-2021-PCM y modificatorias.
- Decreto Supremo N° 050-2018-PCM, que aprueba la definición de Seguridad Digital de ámbito nacional.
- Decreto de Urgencia N° 007-2020, que aprueba el marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Resolución Ministerial N° 119-2018-PCM, que crea del Comité de Gobierno Digital.
- Resolución Ministerial N° 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- Resolución de Secretaría General N° 031-2022-PCM/SG, que crea la Unidad Funcional de Confianza Digital.
- Manual Corporativo: “Manual Metodológico para la Implementación del Sistema de Gestión de Seguridad de la Información” aprobado mediante Resolución de Dirección Ejecutiva N° 029-2020/DE-FONAFE.
- NTP-ISO/IEC 27001:2022 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información, ciberseguridad y protección de la privacidad. Requisitos. 3a. Edición; aprobada por Resolución Directoral N° 022-2022-INACAL/DN.
- NTP-ISO/IEC 27002:2022 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información, ciberseguridad y protección de la privacidad. 2a. Edición; aprobada por Resolución Directoral N° 022-2022-INACAL/DN.
- NTP-ISO/IEC 27005:2022 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información, ciberseguridad y protección de la privacidad. 3a. Edición; aprobada por Resolución Directoral N° 022-2022-INACAL/DN.
- NTP-ISO 31000:2018 Gestión del Riesgo. Directrices. 2a. Edición; aprobada por Resolución Directoral N° 014-2018-INACAL/DN.

IV. VIGENCIA

Este documento entrará en vigencia a partir del primer día hábil después de la fecha de aprobación.

V. CONTENIDO

1. DEFINICIONES / CONSIDERACIONES

- **Alta Dirección**
  Denominación para identificar al órgano máximo de dirección de la organización, pudiendo ser representado por la Gerencia General y/o el Directorio.

- **Acceso**
  Actividades que brindan el acceso de los usuarios de poder localizar o usar la información documentada.

- **Activo de Información**
  Es todo aquello que es o contiene información de valor para la empresa (que incluye información de tipo datos personales) y por tanto requiere protección. Los activos están sujetos a muchos tipos de amenazas que pueden explotar sus vulnerabilidades. Se debe tener en cuenta que parte de los activos de información serán aquellos que por regulación corresponde incorporarlos como información o contenedores de información de valor para le empresa, como por ejemplo los datos personales, las tecnologías digitales, los servicios digitales y los contenidos.

- **Activos digitales**
  Es cualquier recurso que existe de forma digitalizada en el ciberespacio y que alguien puede poseer.

- **Almacenamiento**
  Actividades para que la información documentada se almacene en soportes y formatos que garanticen su disponibilidad, fiabilidad, autenticidad y preservación.

- **Amenaza**
  Es una causa potencial no deseada que daña o puede resultar en daño al sistema, a la empresa o a sus activos. Una amenaza puede ser accidental o intencional.

- **Análisis y evaluación de riesgos**
  Es el proceso por el cual los activos de información son analizados para determinar las vulnerabilidades que poseen y las amenazas a las que están expuestos, valorando el nivel de riesgo de que las amenazas exploten las vulnerabilidades.

- **Auditoría**
  Es un proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva, con el fin de determinar el grado en que se cumplen los criterios de auditoría.

- **Ciberseguridad**
  Es una práctica que garantiza la protección de los activos digitales que interactúan con el ciberespacio mediante la prevención, detección, respuesta y recuperación ante incidentes de seguridad que afecten su disponibilidad, confidencialidad o integridad.

- **Ciberespacio**
  Entorno complejo resultante de la interacción de personas, software y servicios en Internet por medio de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física.

- **CID:**
  Confidencialidad, integridad y disponibilidad.

- **Confidencialidad de la información**
  Indica que sólo acceden quienes están autorizados.

- **Consecuencia**
  Es el resultado de la ocurrencia de un evento que afecta los objetivos de la empresa.

- **Conservación**
  Son actividades realizadas para garantizar el buen estado de la información documentada a lo largo del tiempo.

- **Control**
  Es un mecanismo que sirve para fortalecer la seguridad de aquello que es valioso para la empresa.
  - **Control correctivo**: Es un control que corrige total o parcialmente el impacto de una amenaza.
  - **Control detectivo**: Es un control que detecta la ocurrencia de una amenaza. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
  - **Control preventivo**: Son aquellos controles que están involucrados dentro de los procesos y tienen como propósito evitar la ocurrencia y frecuencia de una amenaza.

- **Control de cambios**
  Son actividades para realizar el seguimiento de los cambios realizados en la información documentada.

- **Criterios de auditoría**
  Son el conjunto de políticas, procedimientos o requisitos usados como referencia frente a los cuales se evalúan las evidencias de la auditoría.

- **Datos personales**
  Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

- **Disponibilidad de la información**
  Establece que debe existir garantía de acceso cuando sea requerido.

- **Disposición**
  Son actividades asociadas con la aplicación de decisiones de transferencia, destrucción o conservación de información documentada.

- **Distribución**
  Son actividades tendientes a garantizar que la información documentada llegue a su destinatario.

- **Dueño de activo de la información**
  Es una persona, una empresa u otra parte interesada que cuente con la responsabilidad asignada y aprobada por la dirección para controlar todo el ciclo de vida de un activo. El propietario identificado no necesariamente tiene derechos de propiedad del activo.

- **Dueño del riesgo**
  Es una persona, una empresa u otra parte interesada con la responsabilidad y autoridad para administrar un riesgo.

- **Entorno digital**
  Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas.

- **Evento**

Es una ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede ser una o más instancias y puede tener varias causas, también puede consistir en algo que no sucede o puede ser referido como un "incidente" o "accidente".

- **Evento de seguridad de la información**
  Es una ocurrencia identificada de un sistema o servicio que determine una posible infracción de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que pueda ser relevante para la seguridad de la información.

- **Evidencias de la auditoría**
  Son los registros, declaraciones de hecho o cualquier otra información que son pertinentes para los criterios de auditoría y son verificables.

- **Fuente de amenaza**
  Es el elemento o conjunto de elementos que tienen el potencial de aumentar la posibilidad de ocurrencia de una amenaza.

- **Gestión de incidentes de seguridad de la información**
  Es un conjunto de procesos para preparar, detectar, analizar, contener, erradicar, recuperar y aprender de incidentes de seguridad de la información.

- **Gestión integral de riesgos**
  Es el proceso de identificación, medición, control, monitoreo, evaluación, retroalimentación y optimización de todas las situaciones que representan riesgos para la organización.

- **Gestión de la seguridad de la información**
  Es un proceso integral de gestión que permite identificar, evaluar y tratar los riesgos de seguridad de la información, en los activos de una empresa, teniendo como objetivo el aseguramiento de la confidencialidad, la integridad y la disponibilidad de la información.

- **Gobierno digital**
  Es el uso estratégico de las tecnologías digitales y datos en la administración pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño y creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

- **Hallazgos de auditoría**
  Son los resultados de la evaluación de las evidencias recopiladas de la auditoría frente a los criterios de auditoría.

- **Impacto**
  Es el nivel de afectación de la empresa o sus procesos, respecto de los distintos factores relevantes con que cuenta

- **Incidente de seguridad de la información**
  Es un evento o un conjunto de eventos no deseados o inesperados, que tienen una probabilidad significativa de comprometer los procesos de la empresa y amenazar la seguridad de la información.

- **Información documentada**
  Es la información requerida que debe ser controlada y mantenida por una empresa, incluyendo el medio en el que se encuentra. La información documentada puede estar en cualquier formato y medio y puede provenir desde cualquier fuente.

- **Integridad de la información**
  Establece que la información y su procesamiento son exactos y completos.

- **No conformidad**
  Es el incumplimiento de un requisito que puede ser identificado producto de la evaluación de los riesgos, la operación del sistema de gestión de seguridad de la información, revisiones por la Alta Dirección y la realización de auditorías.

- **Observación**
  Es un aspecto de un requisito que podría mejorarse y que no se requiere que se haga de manera inmediata.

- **Organización**
  Es la persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

- **Parte interesada**
  Es la persona o empresa que puede afectar, verse afectada por o percibirse ellos mismos como afectados por una decisión o actividad.

- **Plan de tratamiento**
  Son acciones planificadas que una vez hayan sido implementadas serán controles para hacer tratamiento a los riesgos.

- **Política de seguridad de la información**
  Es el conjunto de directrices y lineamientos que nos ayudan a garantizar la seguridad de la información en la empresa.

- **Privacidad de los datos personales**
  Son aquellos datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto esta información no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.

- **Probabilidad**
  Es la medida de certidumbre asociada a un suceso o evento futuro.

- **Retención**
  Son las actividades realizadas para controlar el periodo de tiempo en que la información documentada estará vigente o accesible para poder ser usada.

- **Recuperación**
  Son las actividades que corresponde a la restauración de la información documentada en formato electrónico que haya sido eliminada.

- **Riesgo**
  Es un potencial daño o perjuicio para una empresa; que genera incertidumbre sobre el alcance de los objetivos de la empresa.

- **Riesgo de seguridad de la información**
  Es la probabilidad que una amenaza logre concretarse aprovechando una vulnerabilidad y generando un impacto en el acceso o disponibilidad de la información de la empresa que impide o retarda el logro de los objetivos de la empresa.

- **Riesgo residual**
  Es el nivel resultante del riesgo después de aplicar los mitigantes o controles.

- **Sistema de Gestión de Seguridad de la Información (SGSI)**
  Consiste en políticas, procedimientos, directrices, recursos y actividades, gestionados colectivamente por una empresa, con el objetivo de proteger sus activos de información. Un SGSI tiene un enfoque sistemático para establecer, implementar, operar, monitorear,

revisar, mantener y mejorar la seguridad de la información de una empresa para lograr los objetivos de negocio.

- **Seguridad de la Información**
  Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Seguridad digital**
  Es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

- **Servicio digital**
  Es aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

- **Sistema Integrado de Gestión (SIG)**
  Es un sistema de gestión que combina diversos aspectos de gestión, los cuales pueden ser: calidad, antisoborno, gestión ambiental, gestión de la seguridad y salud en el trabajo, gestión de la seguridad de la información, gestión de la continuidad del negocio, entre otros.

- **Tecnologías digitales**
  Se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

- **Tratamiento de riesgos**
  Es un proceso mediante el cual la empresa define qué estrategia va a ejecutar para abordar un riesgo.

- **Uso de la información**
  Son las actividades para el uso de la información documentada vigente y para evitar el uso de información documentada obsoleta.

- **Vulnerabilidad**
  Es la debilidad o ausencia de control que puede ser explotada por una amenaza. Son características de una vulnerabilidad el hecho de que por sí sola no causa daños y, por otro lado, si no es administrada, permitirá que una amenaza genere un daño o perjuicio.

- **Usuario**
  Individuo o grupo que se beneficia de un sistema durante su utilización.
  Nota: Los roles del usuario y del operador pueden estar asignados, simultáneamente o en secuencia en el mismo individuo u organización.

- **Validación**
  Confirmación, mediante la aportación de evidencia objetiva de que se han cumplido los requisitos para una utilización o aplicación específica prevista
  Nota: La validación en un ciclo de vida es el conjunto de actividades para asegurar y obtener confianza que un sistema es capaz de cumplir su uso previsto, las metas y los objetivos (es decir, cumplir los requisitos de las partes interesadas) en el entorno operativo.

2. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

2 .1 GENERALIDADES DEL SGSI

2.1.1 Ciclo PHVA

La metodología de implementación del SGSI, se realiza a través de un conjunto de pasos, ordenados secuencialmente y que se asocian al Ciclo de Deming - PHVA (Planear-Hacer-Verificar-Actuar) (ver figura 1).

Ciclo PHVA (Planificar – Hacer – Verificar – Actuar).

Figura 1: Ciclo de la implementación del SGSI asociados al ciclo PHVA (Planear – Hacer – Verificar – Actuar)

El Sistema de Gestión de la Seguridad de la Información según la NTP-ISO/IEC 27001:2022, considera los siguientes aspectos relevantes:

- El contexto de la organización (cláusula 4) puede variar y esto afecta a la gestión de riesgos, la operación, el desempeño y la gestión de no conformidades del sistema.
- El liderazgo (cláusula 5) no solo se necesita al inicio en la etapa de planificación; la Alta Dirección debe demostrar liderazgo para hacer las revisiones y aplicar las mejoras que se realizará en el sistema en todos los componentes que figuran en el ciclo PHVA.
- La planificación (cláusula 6) se enfoca en identificar riesgos y oportunidades; incluye la evaluación y tratamiento de riesgos de seguridad de la información y el establecimiento de objetivos medibles para mejorar la seguridad.
- El soporte (cláusula 7) está en todas las fases del SGSI debido a que, en cada componente, se requiere de recursos, personal competente, concienciación, establecimiento de los canales de comunicación y la documentación pertinente que es la base de la implementación del SGSI.
- La operación (cláusula 8) abarca la ejecución de los planes definidos; incluye la implementación de controles, la gestión de riesgos y la planificación para la respuesta a incidentes y continuidad de operaciones.
- La evaluación del desempeño (Capítulo 9) implica el seguimiento y medición de la seguridad de la información, auditorías internas periódicas y revisiones por la dirección para evaluar la eficacia del SGSI.
- La mejora (cláusula 10) busca garantizar el progreso continuo; requiere tratar no conformidades mediante acciones correctivas y optimizar el sistema de manera constante.

En la siguiente figura, se muestra el ciclo PHVA basado en la implementación de la norma ISO 27001:

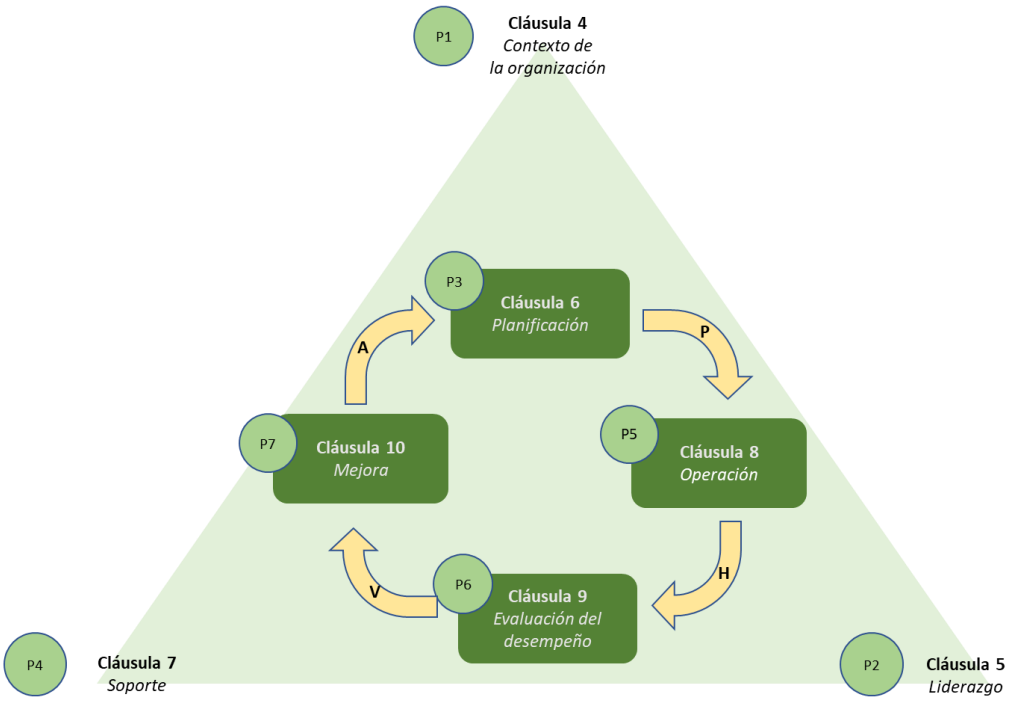

Figura 2: Ciclo PHVA de la norma ISO 27001

2.1.2 Documentación del SGSI

La NTP-ISO/IEC 27001:2022 contiene requisitos de información documentada, los mismos que se desarrollarán durante el establecimiento, operación, monitoreo y mejora del SGSI. La información documentada mínima requerida se detalla en la figura 3 (Los colores hacen referencia a los tipos de documentos).

Es importante tomar en consideración que existe un Sistema Integrado de Gestión (SIG) implementado en AMSAC, por lo tanto, la documentación del SGSI debe integrarse y alinearse al mismo. En el **Anexo 01,** se detallan los documentos del SGSI y cómo se integran con el SIG de AMSAC.

2 .2 PASOS PARA LA IMPLEMENTACIÓN DE UN SGSI

A continuación, se detallan los pasos a seguir para llevar a cabo la implementación o adecuación de un SGSI en AMSAC:

2.2.1 Paso 1: Identificar el contexto de la organización

Para identificar el contexto de la organización se recomienda ejecutar los siguientes 3 pasos:

2.2.1.1 Paso 1.1: Conocer la organización y su contexto

Permite determinar los aspectos relevantes de AMSAC y su entorno interno y externo. Entre los aspectos más importantes se encuentran: la misión y visión, las fortalezas y debilidades; las cuestiones legales, reglamentarias y contractuales; los aspectos de mercado, organizacionales, sociales y económicos, las políticas, la cultura organizacional, la estructura organizacional, los procesos y procedimientos, las funciones de software y hardware, que puedan afectar la capacidad de AMSAC para lograr los resultados esperados del SGSI. En la figura 3 se observan algunos ejemplos de los componentes del contexto.

Figura 3: Ejemplos de componentes del contexto de la organización

2.2.1.2 Paso 1.2: Identificar los requisitos de las partes interesadas

Durante la realización del análisis de contexto, se identifican las partes interesadas. (ver ejemplos en figura 4)

Es importante que se determinen:

- Las partes interesadas que sean relevantes para el SGSI; y
- Los requisitos de estas partes interesadas con respecto a la seguridad de la información.

Para ello, se recomienda realizar las siguientes actividades:

- Identificar de manera preliminar los activos de información importantes y su protección actual de la seguridad de la información.
- Identificar la visión de AMSAC y determinar el efecto futuro sobre los requerimientos de procesamiento de la información.
- Analizar las formas actuales de procesamiento de la información, sistemas de aplicaciones, redes de comunicaciones, instalaciones de las actividades y recursos de tecnologías de la información, entre otros.
- Identificar los requisitos esenciales (por ejemplo, requisitos legales y reglamentarios, obligaciones contractuales de AMSAC, normas de la industria, acuerdos entre cliente y proveedor, condiciones de seguros, entre otros).
- Identificar el nivel de concientización en seguridad de la información y a partir de esto, derivar en los requisitos de educación y entrenamiento para cada área.

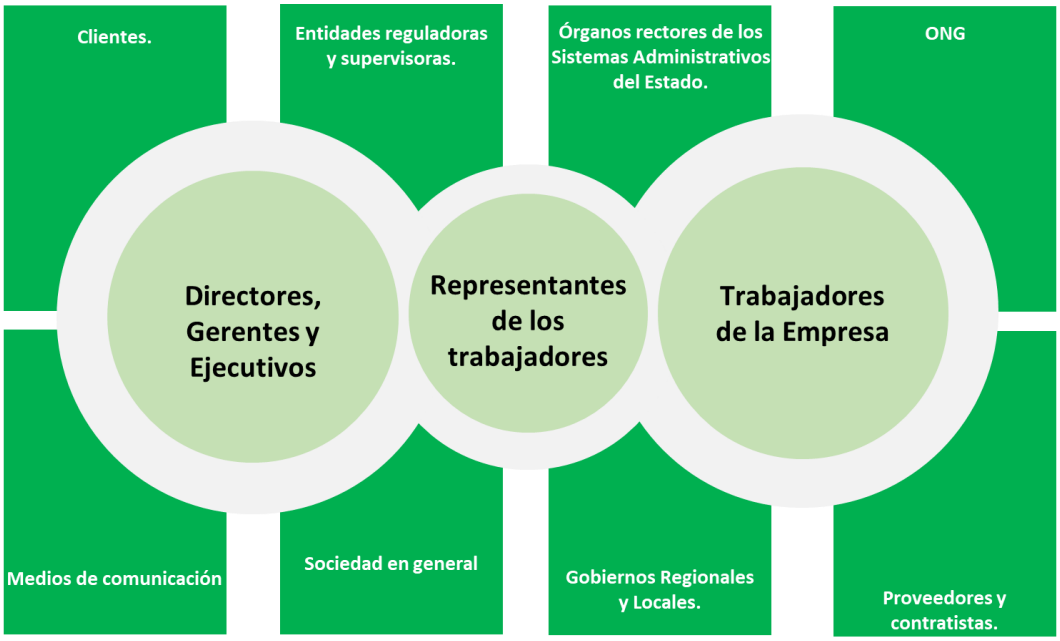

Figura 4: Ejemplo de partes interesadas

2.2.1.3 Paso 1.3: Determinar el alcance del SGSI

El alcance del SGSI es definido en términos de los procesos de AMSAC, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

Para garantizar la efectiva implementación del SGSI, el alcance es definido sobre la base de los procesos operativos, también conocidos como procesos clave o misionales, los procesos que dan soporte a los procesos clave, así como cualquier otro proceso que gestione información relevante para AMSAC, incluyendo aquellos que hacen uso de servicios de tecnologías de la información o servicios a través de los cuales se intercambia información relevante, independientemente de la naturaleza de la información (digital o de otro tipo). (ver figura 5).

Para determinar el alcance, se considera el análisis de contexto (objetivos estratégicos, valores, misión, visión, cultura organizacional, etc.), los requisitos de las partes interesadas, las interfaces y dependencias entre las actividades realizadas por AMSAC y las realizadas por otras organizaciones (proveedores y/o socios de negocio). Adicionalmente, se podrá considerar los resultados de la gestión de riesgos de seguridad de la información para evaluar el establecimiento o actualización del alcance.

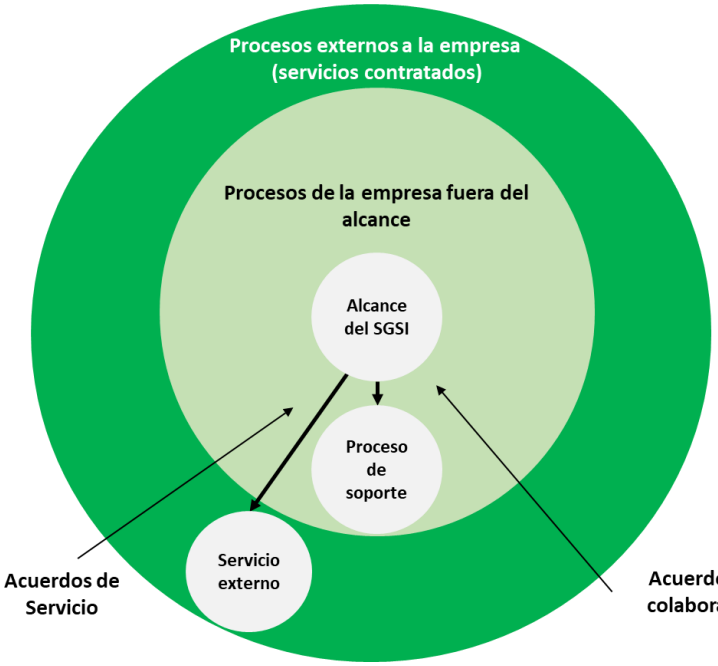

Figura 5: Relaciones entre el alcance del SGSI, los procesos internos y externos

En la figura 6, se muestran los documentos desarrollados para el SGSI en el paso 1.

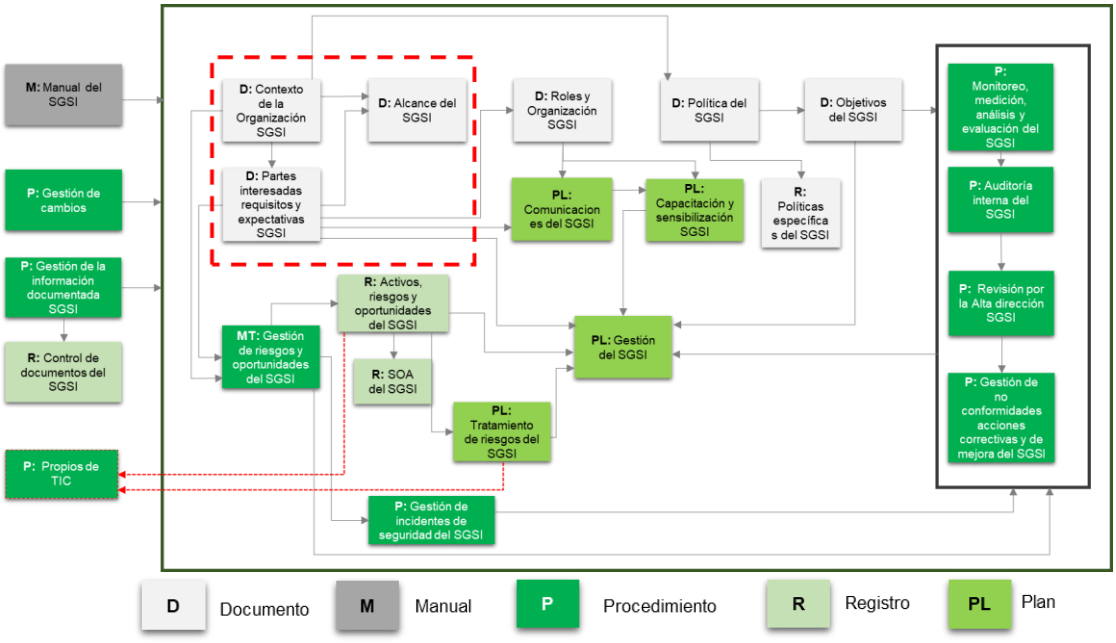

Figura 6: Documentos generados en el paso 1

- **SI:** Seguridad de la Información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **SOA:** Statement Of Applicability (Declaración de aplicabilidad).
- ◄---**:** Procedimientos que se aplican para realizar tratamiento a riesgos de SI**.**

2.2.2 Paso 2: Establecer el liderazgo

En este paso, la Alta Dirección debe brindar orientación y guía, además de comprometerse con la implementación del SGSI.
Para establecer el liderazgo, se recomienda ejecutar los siguientes pasos:

2.2.2.1 Paso 2.1: Liderazgo y compromiso

Se sugiere que la Alta Dirección demuestre su liderazgo y compromiso respecto del SGSI, para ello:

- Asegura que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y compatibles con la dirección estratégica de AMSAC.
- Asegura la integración de los requisitos del SGSI en los procesos de AMSAC.
- Asegura que los recursos necesarios para el SGSI estén disponibles.
- Comunica la importancia de una efectiva gestión de seguridad de la información que esté en conformidad con los requisitos del SGSI.
- Asegura que el SGSI logre su(s) objetivos(s) previsto(s).
- Dirige y apoya a las personas para que contribuyan con la eficacia del SGSI.
- Mantiene un compromiso con la promoción de la mejora continua.
- Apoya a otros roles relevantes de gestión de seguridad de la información para demostrar su liderazgo, tal como se aplica a sus áreas de responsabilidad.

2.2.2.2 Paso 2.2: Definir la política de seguridad de la información

Se sugiere realizar las siguientes actividades:

- Establecer, documentar, aprobar y difundir la política de seguridad de la información.
- La política de seguridad de la información será apropiada al propósito de AMSAC, incluyendo: objetivos de seguridad de la información o proporcionando un marco para fijarlos, un compromiso para satisfacer los requerimientos aplicables relacionados a seguridad de la información de las partes interesadas y un compromiso de mejora continua del SGSI.
- La política será comunicada y estará disponible dentro de AMSAC y también a las partes interesadas, según sea apropiado.
- La política estará disponible como información documentada.

2.2.2.3 Paso 2.3: Establecer los roles, responsabilidades y autoridades

Como todo sistema de gestión está gestionado y operado por personas, corresponde establecer, asignar y comunicar los roles, responsabilidades y autoridades dentro del SGSI. Esto no significa necesariamente la creación de nuevos puestos de trabajo, sino que a consideración de AMSAC, cada rol establecido puede ser relacionado con posiciones de trabajo de la estructura organizacional actual.

Dentro de los roles para el SGSI, se incluyen los siguientes:

- **El titular o un representante de la Alta Dirección**, es quien presidirá el Comité de Seguridad de la Información a fin de dirigir el gobierno, gestión y operación del SGSI, dando evidencia del liderazgo y compromiso de la Alta

Dirección de AMSAC en la implementación, mantenimiento y la mejora continua del SGSI.

- **Comité de Seguridad de la Información (CSI)**, el cual es un comité ejecutivo conformado por altos directivos de AMSAC, designado para gestionar, supervisar, revisar e informar de manera permanente los aspectos del SGSI. AMSAC debe evaluar si le corresponde aplicar la Resolución Ministerial N° 087-2019-PCM, a fin de integrar las funciones del Comité de Seguridad de la Información al Comité de Gobierno y Transformación Digital.
- **Oficial de seguridad y confianza digital**, quien es el Coordinador del CSI y principal responsable operativo de la implementación del SGSI.
- **Dueños de procesos y de riesgos**, quienes tienen la responsabilidad y autoridad para gestionar los riesgos de activos de información.
- Asimismo, se establecen los roles que apoyarán en la gestión de riesgos, quienes serán dueños de los activos y quienes los custodiarán, quienes gestionarán y ejecutarán las auditorías, entre otros.
- Este paso debe cumplirse de manera previa antes de la elaboración de documentos para la implementación del SGSI.

En la figura 7, se muestran los documentos desarrollados para el SGSI en el paso 2.

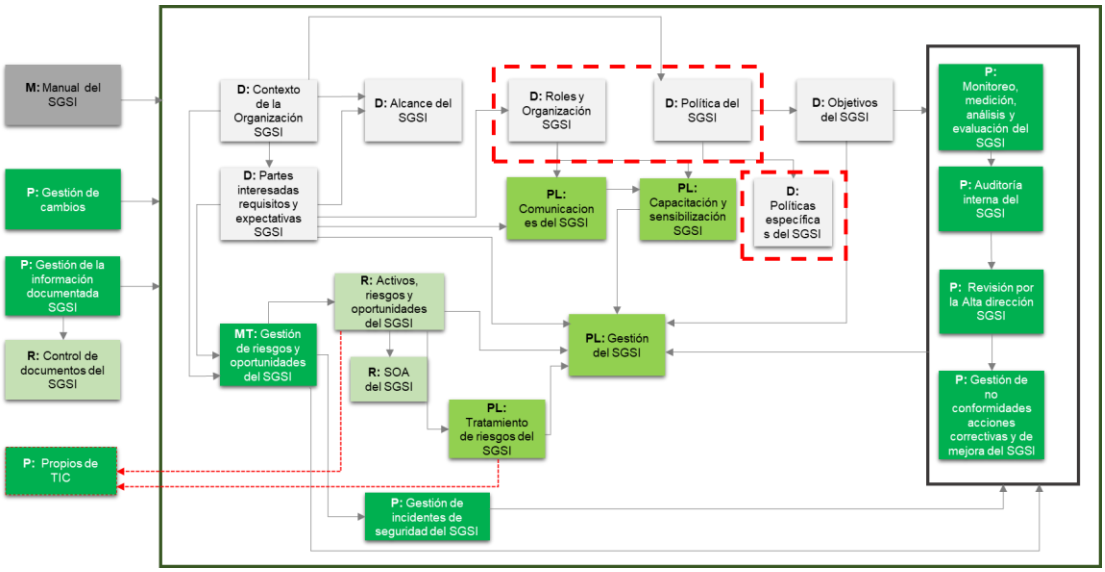

Figura 7: Documentos generados en el Paso 2

2.2.3 Paso 3: Diseñar la planificación

El desarrollo de la planificación involucra establecer qué vamos a hacer y cómo lo vamos a hacer. Un aspecto importante del cómo lo vamos a hacer es la gestión de riesgos de seguridad de la información y esta gestión será tratada como un documento independiente denominado Metodología para la gestión integral de Riesgos (código E2.3.M1 y Procedimiento de Gestión de Riesgos y Oportunidades del SIG (código E3.1.P1).

Para el diseño de la planificación, se recomienda ejecutar los siguientes pasos:

2.2.3.1 Paso 3.1: Definir la metodología de gestión de riesgos y oportunidades

Cuando se planifica el SGSI, se consideran las acciones y requisitos citados en los pasos 1.1 (Conocer el contexto de AMSAC) y 1.2 (Identificar las partes interesadas, sus requisitos de seguridad de la información y la forma para abordarlos), y se determina los riesgos y oportunidades que necesitan ser tratados. Para ello, se realiza lo siguiente:

- Asegura que el SGSI pueda lograr los resultados previstos.
- Establece medidas para prevenir, o reducir, efectos indeseados de los riesgos. Las medidas son controles que se ejecutan y planes de tratamiento para riesgos.
- Establece medidas que son planes de acción para oportunidades.
- Las medidas adoptadas para gestionar riesgos y oportunidades se integrarán e implementarán en los procesos del SGSI, así como también se evaluará su efectividad.
- Realiza la mejora continua del SGSI.

La identificación de los activos de información, el análisis, evaluación y el tratamiento de los riesgos de seguridad de la información es el flujo a seguir como parte de la metodología de gestión de riesgos para el SGSI. Para ello se debe definir cómo se llevará a cabo la gestión de los riesgos de seguridad de la información (ver figura 8) estableciendo los niveles y criterios de aceptación de riesgos de seguridad de la información. Este flujo estará alineado a la Metodología de la Gestión de Riesgos de Seguridad de la Información.

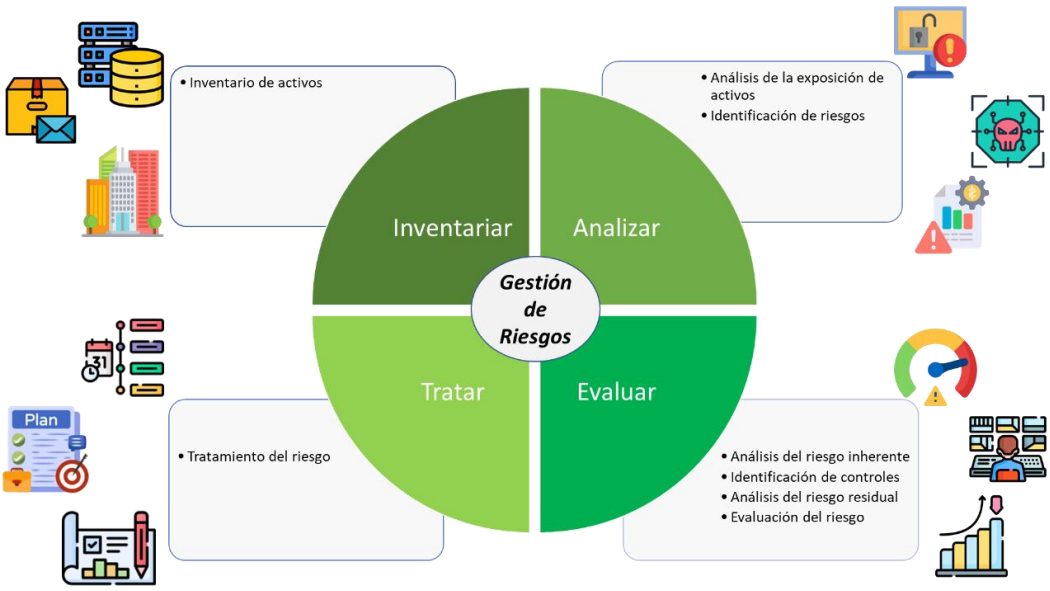

Figura 8: Metodología para la gestión de riesgos de seguridad de la información

2.2.3.2 Paso 3.2: Evaluación de los riesgos de seguridad de la información

Los riesgos se evalúan sobre los activos de la información, por ello es necesario identificar los activos de la información que forman parte del alcance del SGSI. Para ello, se sugiere realizar las siguientes actividades:

a) **Inventariar los activos de información**:

- Establecer un modelo para valorar los activos de información.
- Establecer las categorías de activos de información.
- Identificar los activos de información y sus atributos (Categoría, Ubicación Física / Lógica, Clasificación, Frecuencia de uso, Dueño del activo, Custodio).
- Priorizar los activos de información a partir de sus niveles de confidencialidad, integridad y disponibilidad.

b) **Analizar la exposición de los activos información**:

- Identificar las vulnerabilidades del activo de la información.
- Identificar las amenazas sobre los activos de información.
- Estimar cómo se afectan los activos de información (determinar los niveles de CID para el activo) por las amenazas y vulnerabilidades.

c) **Analizar y evaluar los riesgos de seguridad de la información**:

- Identificar los riesgos de seguridad de la información y detallar sus atributos (propietario del riesgo).
- Estimar el nivel de riesgo (determinar la probabilidad e impacto del nivel de riesgo inherente) que se ve afectado por las amenazas y vulnerabilidades y sin considerar los controles para su tratamiento.
- Identificar los controles actuales que permiten abordar las vulnerabilidades y amenazas a los activos de información (clasificación: organizacional, de persona, físico o tecnológico; oportunidad del control: preventivo, detectivo o correctivo; objetivo de seguridad de la información: confidencialidad, integridad y/o disponibilidad; objetivo de ciberseguridad: gobernanza, identificar, detectar, proteger, responder o recuperar; capacidades operativas, dominios de seguridad, responsable del control, grado de automatización del control y evidencia del control).
- Estimar cómo los controles afectan positivamente los activos de información (determinar los niveles de confidencialidad, integridad y/o disponibilidad mejorados, y la reducción en la probabilidad y/o impacto, así como el efecto reductor sobre el nivel de riesgo residual).
- La estimación del efecto de los controles debe ser posteriormente evaluada para confirmar el efecto sobre el riesgo residual.

2.2.3.3 Paso 3.3: Tratar los riesgos de seguridad de la información

Con la metodología de gestión de riesgos de seguridad de la información ya definida y los activos de la información que participan del SGSI inventariados, se procede a establecer el tratamiento de los riesgos. Para ello, se sugiere realizar lo siguiente:

- Indicar el tratamiento que se dará a cada riesgo.
- Determinar todos los controles que son necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información.
- Comparar los controles actuales y planes de tratamiento determinados con los controles mencionados en el Anexo A de la NTP-ISO/IEC 27001:2022 y verificar que no se ha omitido ningún control necesario.
- Identificar si dentro de los controles existe información documentada.

- Identificar si existe información documentada que refuerce los controles.
- Elaborar el plan de tratamiento de riesgos.
- Obtener la aprobación, por parte de los dueños de los riesgos, del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de la seguridad de la información.
- Disponer y controlar que se generen registros sobre las actividades de los usuarios, las excepciones y los eventos de seguridad de la información.

Posterior a la propuesta de tratamiento de riesgos se sugiere desarrollar la Declaración de Aplicabilidad (SOA por sus siglas en inglés), la cual lista los controles que se van a mantener, implementar o mejorar, y los controles que serán implementados debido a la necesidad de cumplimiento de un aspecto legal, reglamentario o contractual; así como las justificaciones de la inclusión o exclusión de los controles.

Además, se sugiere desarrollar lo siguiente:

- Estructurar el plan de tratamiento de manera que se identifique claramente cómo es que AMSAC logrará sus objetivos de seguridad de la información. AMSAC determinará: (a) qué se hará, (b) qué recursos serán requeridos, (c) quién será responsable, (d) cuándo se culminará, y (e) cómo los resultados serán evaluados.

2.2.3.4 Paso 3.4: Definir los objetivos de seguridad de la información

Se sugiere realizar las siguientes actividades:

- Establecer o actualizar objetivos de seguridad de la información a niveles y funciones relevantes. Los objetivos de seguridad de la información serán: (a) consistentes con la política de seguridad de la información, (b) medibles (si es práctico), (c) tomados en cuenta para los requisitos aplicables de seguridad de la información y resultados de la valoración y tratamiento de riesgos, (d) comunicados y (e) actualizados según sea apropiado.
- Luego de definir los objetivos de seguridad de la información, se les asignarán criterios para realizar la medición, monitoreo y comunicación del resultado de los niveles de desempeño en un objetivo. Así mismo, estos objetivos y criterios deberán actualizarse según corresponda.
- Se conservará la información documentada sobre los objetivos de seguridad de la información.

2.2.3.5 Paso 3.5: Planificar los cambios

Cuando se determine la necesidad de cambios en el SGSI, los cambios deben llevarse a cabo de manera planificada. Los cambios incluyen abordar cualquier aspecto que impacte en el SGSI y su funcionamiento, tales como proyectos, cambios normativos o regulatorios, actualización de procesos, incorporación o poner en desuso tecnologías de la información y comunicaciones, tecnologías operacionales o industriales, adquirir nuevos servicios, compartir información con terceros, entre otros.

En la figura 9 se observan los documentos desarrollados para el SGSI en el paso 3.

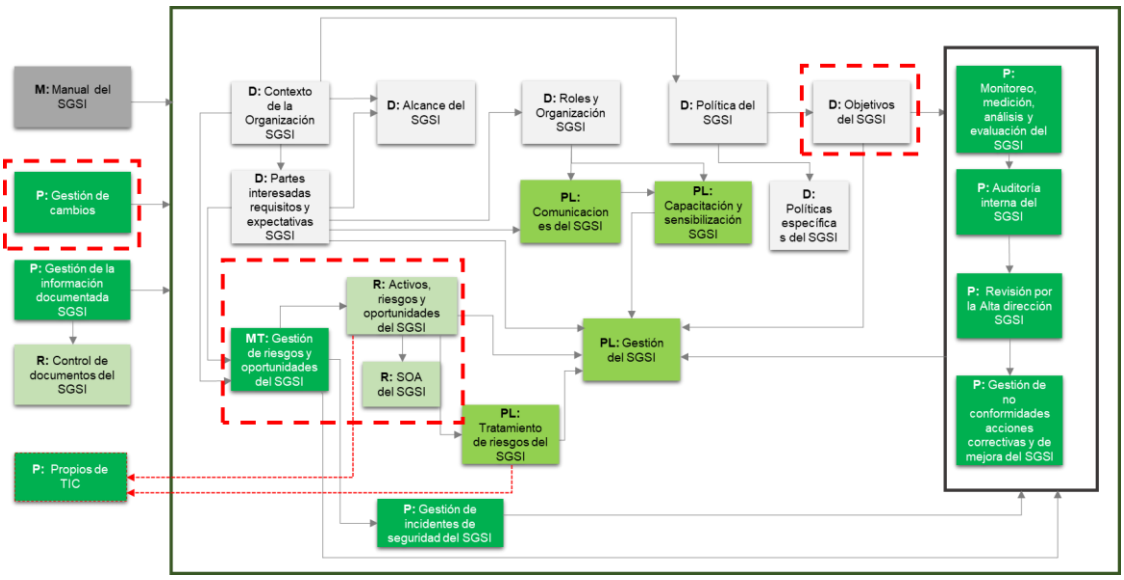

Figura 9: Documentos generados en el Paso 3

2.2.4 Paso 4: Brindar soporte

Para brindar soporte se recomienda ejecutar los siguientes pasos:

2.2.4.1 Paso 4.1 Recursos

Determinar y proporcionar los recursos necesarios para el establecimiento, operación, monitoreo y mejora continua del sistema de gestión de seguridad de la información.

2.2.4.2 Paso 4.2: Identificar y adquirir las competencias del personal

Se debe realizar las siguientes actividades:

- Determinar las competencias necesarias (educación, capacitación y /o experiencia) para los roles involucrados en el SGSI.
- Una vez determinadas las competencias necesarias, verificar que el personal asignado a cada rol cuente con las mismas (análisis de brechas en las competencias del personal).
- En caso el personal no cuente con las competencias necesarias, se planifica acciones generadoras de competencia para que el personal las adquiera. Las acciones pueden incluir, entre otras, capacitación, mentoría, reasignación o contratación de personal.
- Realizar las acciones generadoras de competencia, según lo planificado, y de manera posterior a su ejecución, AMSAC evalúa la efectividad de las mismas.
- Tener en consideración que las evidencias de las competencias pueden incluir certificados, constancias, entre otros legajos del personal, y que las evidencias de las acciones generadoras de competencia pueden incluir elementos de las capacitaciones brindadas, como listas de asistencia, entre otros registros o documentos.
- Tener disponible la evaluación de la efectividad de las acciones generadoras de competencia, es decir, deben estar disponibles como evidencia documentada.

2.2.4.3 Paso 4.3: Gestionar la concientización del personal

Es necesario brindar y reforzar conocimientos, así como validar su aplicación por parte del personal de AMSAC; para ello, se sugiere realizar como mínimo lo siguiente:

- Concientizar a los roles involucrados en la implementación, operación, monitoreo y mejora del SGSI para que interioricen los siguientes conceptos:
  - La política de seguridad de la información.
  - Los objetivos del SGSI.
  - Los roles, responsabilidades y autoridades del SGS.
  - La metodología de gestión de riesgos del SGSI.
  - Su contribución a la efectividad del SGSI, incluyendo los beneficios de un mejor desempeño de la seguridad de la información.
  - Las implicancias de no tener conformidad con los requisitos del SGSI.
- Planificar acciones generadoras de conciencia para el personal. Las acciones pueden incluir, entre otras, charlas, preparación de materiales audiovisuales, elaboración de encartes o comunicados, campañas de concientización, publicación de páginas web, entre otros.
- Realizar las acciones generadoras de conciencia según lo planificado.
- Documentar las acciones generadoras de competencia y conciencia (charlas, listas de asistencia, entre otros) de manera que estén disponibles como evidencia documentada.

2.2.4.4 Paso 4.4: Gestionar las comunicaciones del SGSI

Otro aspecto relevante es establecer cómo se lleva a cabo la gestión de las comunicaciones; para ello, se realiza lo siguiente:

- Comunica a todo el personal de AMSAC la política, los objetivos, la metodología de gestión de riesgos y los roles, responsabilidades y autoridades del SGSI, así como otros componentes del SGSI, que también serán comunicados al interior y exterior de la empresa.
- Determina la necesidad de comunicaciones internas y externas relevantes al SGSI incluyendo:
  - Qué comunicar.
  - Quién debe comunicar.
  - Cuando comunicar.
  - A quién comunicar.
  - Como comunicar.
- Realiza las comunicaciones según lo planificado.
- Observa que las evidencias de las comunicaciones estarán disponibles de manera documentada.

2.2.4.5 Paso 4.5: Gestionar la información documentada

La información generada en la implementación, operación, monitoreo y mejora del SGSI debe ser gestionada.

Al contar con un Sistema Integrado de Gestión (SIG), la gestión de la información documentada para el SGSI debe integrarse y ser realizada según lo descrito para el SIG existente. Se debe determinar la información documentada requerida para el SGSI y la determinada como necesaria para la eficacia del SGSI.

Para la gestión de la información documentada del SGSI, se sugiere ejecutar las siguientes actividades:

- Definir niveles o una estructura documentaria, dentro de las cual debe ubicarse la información documentada del SGSI. Al contar con una estructura documentaria del SIG, debe ubicarse los documentos que se generen del SGSI en esta. La estructura de documentos será de acuerdo con lo establecido en el Procedimiento de Elaboración y Control de la Información Documentada.
- Este paso debe cumplirse antes de la elaboración de cualquier documento.

El SGSI contiene la siguiente información documentada en documentos o registros que pueden denominarse como se citan o en denominaciones similares, como documentos y registros individuales o incorporados en otros documentos:

- Documentos:
  - Análisis de contexto (cap. 4.1 de ISO 27001).
  - Requisitos de las partes interesadas (cap. 4.2 de ISO 27001).
  - Alcance del SGSI (cap. 4.3 de ISO 27001).
  - Mapa de procesos de AMSAC y sus interrelaciones con el SGSI (cap. 4.4 de ISO 27001).
  - Política de seguridad de la información (cap. 5.2 y 6.2 de ISO 27001).
  - Roles, responsabilidades y autoridades del SGSI de AMSAC (cap. 5.3 de ISO 27001).
  - Metodología de gestión de riesgos y oportunidades (cap. 6.1.2 de ISO 27001).
  - Procedimiento de Gestión de Riesgos y Oportunidades del Sistema Integrado de Gestión (cap. 6.1.2 de ISO 27001).
  - Plan de tratamiento de riesgos (cap. 6.1.3 e y 8.3 de ISO 27001).
  - Objetivos de seguridad de la información (cap. 6.2 de ISO 27001).
  - Plan de capacitación y concientización (cap. 7.2 y 7.3 de ISO 27001).
  - Plan de comunicaciones del SGSI (cap. 7.4 de ISO 27001).
  - Procedimiento de elaboración y control de la información documentada (cap. 7.5 de ISO 27001).
  - Plan de operación del SGSI (cap. 8.1 de ISO 27001).
  - Procedimiento para la gestión de incidentes (cap. 8.1 de ISO 27001).
  - Procedimientos o políticas específicas que contribuyen con la implementación del SGSI (cap. 8.1 de ISO 27001).
  - Procedimiento de monitoreo, medición, análisis y evaluación (cap. 9.1 de ISO 27001).
  - Procedimiento de auditoría interna (cap. 9.2 de ISO 27001).
  - Procedimiento de revisión del SGSI por la alta dirección (cap. 9.3 de ISO 27001)
  - Procedimiento de acciones correctivas y de mejora (cap. 10.1 y 10.2 de ISO 27001).
- Registros:
  - Matriz de activos de información (cap. 6.1 de ISO 27001).
  - Matriz de oportunidades del SGSI (cap. 6.1 de ISO 27001).
  - Matriz de riesgos de seguridad de la información (cap. 6.1, 8.2 y 8.3 de ISO 27001)
  - Declaración de aplicabilidad (cap. 6.1.3 d de ISO 27001).
  - Resultados (informes o reportes) de la evaluación de riesgos (cap. 8.2 de ISO 27001).

- Registros de aprobación del plan de tratamiento y aceptación de riesgos residuales (cap. 6.1.3 de ISO 27001).
- Registros de las competencias (educación, capacitación y experiencia) de los roles del SGSI y validación de cumplimiento (cap. 7.2 de ISO 27001).
- Listas de asistencia a las capacitaciones (cap. 7.2 y 7.3 de ISO 27001)
- Registro que contiene la lista maestra de documentos internos del SGSI (cap. 7.5 de ISO 27001).
- Registro que contiene la lista maestra de documentos externos del SGSI (cap. 7.5.3 de ISO 27001).
- Registro para la gestión de eventos e incidentes de seguridad de la información (cap. 8.1 de ISO 27001).
- Resultados de seguimiento, medición, análisis y evaluación (cap. 9.1 de ISO 27001).
- Programa y plan de auditoría interna (cap. 9.2.2 de ISO 27001).
- Informe que contiene resultados de las auditorías internas (cap. 9.2 de ISO 27001).
- Informe que se remite a la Alta Dirección (cap. 9.3.2 de ISO 27001)
- Informe o acta que contiene resultados de la revisión por la Alta Dirección (cap. 9.3.3 de ISO 27001).
- Registros de no conformidades y acciones correctivas (cap. 10.1 de ISO 27001).
- Resultados de acciones correctivas (cap. 10.1 de ISO 27001).
- Registros de mejoras (cap. 10.2 de ISO 27001).

- Cuando cree o actualice la información documentada, se debe asegurar lo siguiente:
  - La identificación y la descripción apropiadas (por ejemplo, título, fecha, autor, versión del documento).
  - El formato (por ejemplo, lenguaje, versión de software, gráficos) y los medios (por ejemplo, papel, electrónico) apropiados.
  - La revisión y la aprobación apropiadas para su conveniencia y suficiencia.
- Se debe asegurar que la información documentada está disponible y adecuada para su uso, donde y cuando se necesite y que está adecuadamente protegida (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de integridad)
- Para realizar el control de la información documentada, se recomienda que AMSAC aborde las siguientes actividades: distribución, acceso, recuperación, uso, almacenamiento, conservación (incluida la conservación de la legibilidad), control de cambios, retención y disposición.
- Identificar, según sea apropiado, y controlar, la información documentada de origen externo, determinada por AMSAC como necesaria para la planificación y operación del SGSI.

En la figura 10, se muestran los documentos desarrollados para el SGSI en el paso 4.

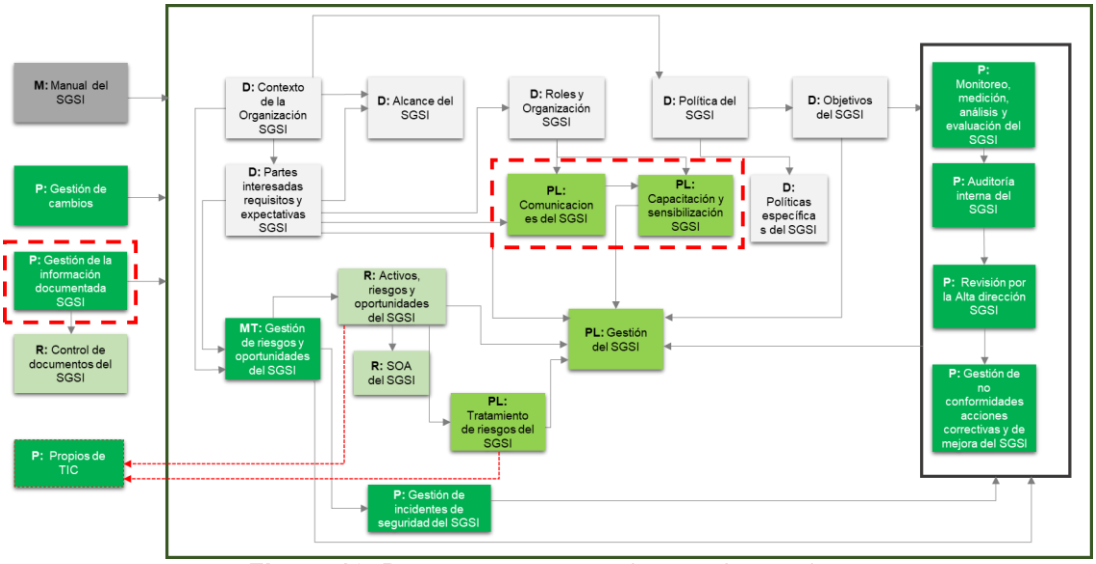

Figura 10: Documentos generados en el paso 4

2.2.5 Paso 5. Iniciar y mantener la operación

Una vez establecido el SGSI y contando con los recursos idóneos, se inicia la operación del mismo; para ello, se sugiere realizar los siguientes pasos:

2.2.5.1 Paso 5.1: Planificar y controlar la operación

Para planificar y controlar la operación, se sugiere que se ejecute lo siguiente:

- Generar un plan de actividades conducentes a cumplir los requisitos de seguridad de la información, implementar las acciones determinadas en el plan de tratamiento de riesgos y lograr los objetivos de seguridad de la información.
  - Cada actividad del plan de actividades contiene los siguientes datos:
    - ✓ Fase del SGSI a la que pertenece la actividad.
    - ✓ Descripción de la actividad.
    - ✓ Responsable de la actividad.
    - ✓ Fecha de inicio y de cumplimiento de la actividad.
    - ✓ Recursos necesarios para ejecutar la actividad.
  - Por cada recurso necesario se detalla lo siguiente:
    - ✓ Tipo de recurso (recursos humanos, infraestructura, servicios, entre otros).
    - ✓ Recurso requerido.
    - ✓ Cantidad requerida del recurso.
    - ✓ Tiempo de dedicación o uso del recurso.
    - ✓ Tipo de provisión (designación, contratación, asignación, adquisición, etc.).
  - Los recursos necesarios estarán disponibles de manera oportuna cuando sean requeridos.
- Controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario.
- Asegurar que los procesos provistos por terceros son identificados y controlados.

- Mantener información documentada en la medida necesaria para estar seguro de que los procesos se han llevado a cabo tal como fueron planificados.

2.2.5.2 Paso 5.2. Evaluar los riesgos y las oportunidades de seguridad de la información

Se evalúa los riesgos de seguridad de la información en intervalos planificados o cuando cambios significativos se propongan u ocurran, siguiendo los lineamientos de la "Metodología y/o Procedimiento para la Gestión de Riesgos y Oportunidades de Seguridad de la Información".
Se conserva la información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información y las oportunidades que plantea el establecimiento, operación y mejora del SGSI.

2.2.5.3 Paso 5.3. Hacer seguimiento al plan de tratamiento de riesgos

Se implementa y realiza el seguimiento a la ejecución del plan de tratamiento de riesgos. El modelo para desarrollar el citado plan se encuentra en la Metodología para la gestión integral de Riesgos y Procedimiento de Gestión de Riesgos y Oportunidades del SIG.
Se conserva la información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

2.2.5.4 Paso 5.4. Realizar la gestión de incidentes de seguridad de la información

Es necesario que se gestionen los incidentes de seguridad de la información de tal forma que los impactos se mantengan dentro de los márgenes tolerables para AMSAC.

La gestión de incidentes consta de las siguientes actividades:

- Detectar e informar eventos de seguridad de la información: Consiste en detectar y reportar los eventos indicando su descripción y tipo, los potenciales activos afectados o comprometidos, la fecha del evento, y si aplica, el costo asociado.
- Evaluar y tomar decisión: Consiste en evaluar el evento de seguridad de la información y decidir si se trata de un incidente de seguridad de la información.
- Dar respuestas: Consiste en generar una o varias respuestas al incidente de seguridad de la información y en la recuperación del incidente. Si se desea, también puede brindar la respuesta al evento en el caso que no haya sido clasificado como incidente. Las respuestas pueden incluir la realización de actividades que limiten la propagación de los efectos de los incidentes, la erradicación de aquello que generó el incidente, el análisis de la causa raíz que dio origen al incidente, entre otras acciones.
- Planificar la remediación de las vulnerabilidades que originaron el incidente implementando los controles necesarios para proteger los activos de información de AMSAC. Estos controles se pueden incluir para tratar riesgos existentes o nuevos riesgos que no se hayan considerado en la Matriz de riesgos de seguridad de la información.
- Identificar lecciones aprendidas: Consiste en identificar conocimiento, al que llamamos "lecciones aprendidas", ya sean mejoras en la gestión de seguridad de la información, en la gestión de riesgos o en la gestión de incidentes.

En la figura 11, se observan los documentos desarrollados para el SGSI en el paso 5.

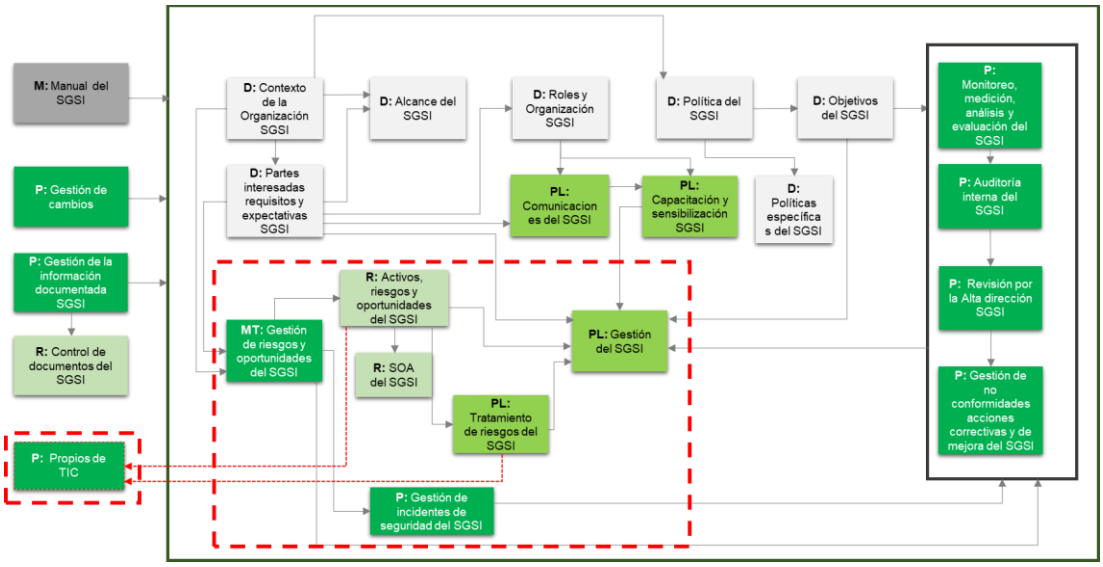

Figura 11: Documentos generados en el paso 5

2.2.6 Paso 6: Realizar la evaluación de desempeño

Desde el momento en que se ha completado un ciclo de operación del sistema de gestión de seguridad de la información, se programa y realiza la revisión periódica y permanente del SGSI por la Alta Dirección. Este proceso tiene por objetivo determinar si el SGSI está en conformidad con los requisitos del SGSI y los de la NTP-ISO/IEC 27001:2022, así como si está efectivamente implementado y mantenido.

2.2.6.1 Paso 6.1: Monitorear, medir, analizar y evaluar el SGSI

Se evalúa el desempeño de la seguridad de la información y la efectividad del SGSI, para lo cual se sugiere seguir un modelo de medición (ver figura 12), el cual representa la arquitectura base que contiene los elementos y relaciones de interdependencia para la medición.

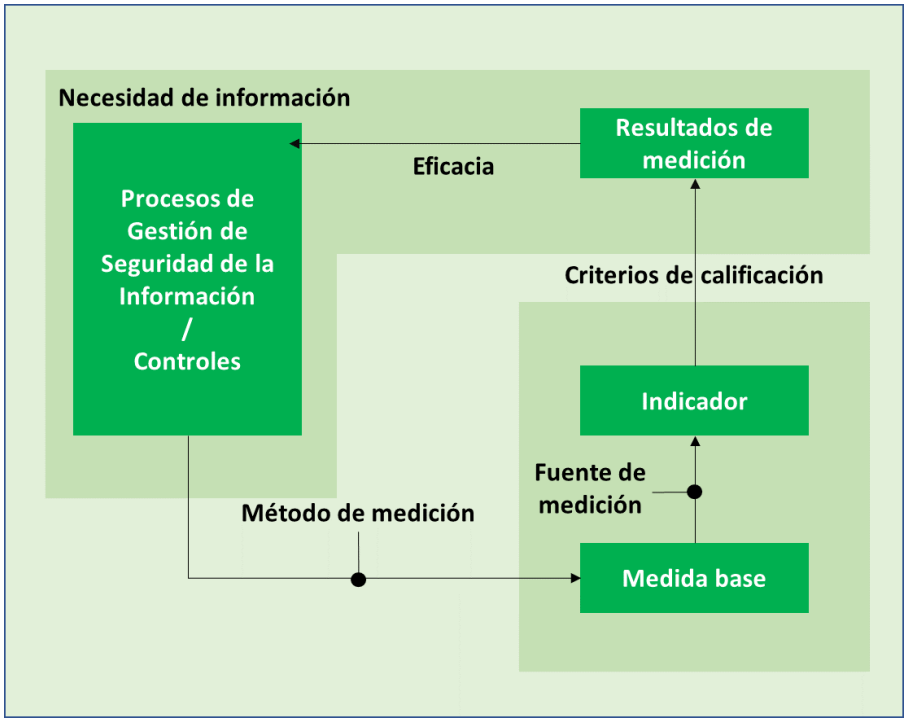

Figura 12: Modelo de medición

- Ejecutar el modelo de medición requiere de lo siguiente:
  - Identificar la necesidad de información (propósito de medición), basada en las características de los procesos o controles del SGSI.
  - Cuantificar las características a través de un método de medición a fin de obtener las medidas base. Una característica del método de medición es que determina los métodos para monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos. Los métodos seleccionados producirán resultados comparables y reproducibles para ser considerados válidos.
  - Establecer y aplicar una función de medición que hace uso de dos o más medidas base.
  - Interpretar los resultados del indicador mediante el uso de los criterios de calificación.
  - Plasmar la interpretación de los resultados del indicador en comparación con los resultados de la medición. Estos resultados proveen dirección para la toma de decisiones.
  - Determinar (a) quién va a monitorear y medir, (b) cuándo los resultados del monitoreo y medición sean analizados y evaluados, y (c) quién analizará y evaluará estos resultados.

- Tener en consideración que el proceso de medición consiste en desarrollar una herramienta que considere lo siguiente:
  - Determinar los objetivos de medición: Son los objetivos del SGSI que serán objeto de medición.
  - Desarrollar los indicadores (métricas) del SGSI: Consiste en el diseño de los indicadores alineados a los objetivos del SGSI que se usarán para medir la eficacia de los controles o procesos (cláusulas) del SGSI; así como identificar lo que necesita seguimiento y medición incluidos los procesos y controles del SGSI e identificar desviaciones en el SGSI de

manera oportuna y tratarlas en consecuencia. Estos indicadores se medirán conforme a la frecuencia y método de seguimiento y medición establecido en la herramienta; este método debe producir resultados comparables y reproducibles para que se consideren válidos.

- Recolectar y medir datos: Consiste en la recolección de datos (medidas base) y en la aplicación de funciones de medición para obtener los resultados de los indicadores. Los métodos para recolectar datos pueden involucrar varias fuentes tales como cuestionarios, entrevistas personales, resultados del análisis, evaluación y tratamiento de riesgos, reportes de auditoría interna y/o externa, registros de logs, reportes de eventos e incidentes; revisiones por la Alta Dirección previas y resultados de pruebas, como pruebas de penetración, ingeniería social, herramientas de cumplimiento y auditoría. En los roles, se determina quién deberá realizar el monitoreo y medición del SGSI.
- Reportar los resultados: Consiste en la comunicación de los resultados de los indicadores obtenidos a las partes interesadas, como la Alta Dirección y el Comité de Seguridad de la Información, con la finalidad de que se tomen decisiones con respecto a la mejora del SGSI implementado. En los roles, se determina quién reporta los resultados del SGSI.
- Analizar y evaluar los resultados: Consiste en el análisis de los resultados para identificar sus causas y consecuencias, para luego evaluarlos según los parámetros establecidos por cada indicador, lo cual servirá como insumo para la toma de decisiones. En los roles, se determina quién analiza, evalúa y comunica los resultados finales sobre el SGSI.

Los resultados del seguimiento, medición, análisis y evaluación del SGSI deberán estar disponible como información documentada.

2.2.6.2 Paso 6.2: Realizar auditoría interna

Al contar con un Sistema Integrado de Gestión (SIG), las auditorías internas para el SGSI se realizan según lo descrito en el mismo.

Para la ejecución de las auditorías internas, se sugiere realizar lo siguiente:

- Planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos e informes de planificación. Los programas de auditoría tendrán en consideración la importancia de los procesos concernientes y los resultados de auditorías previas.
- Establecer los intervalos para realizar las auditorías internas.
- Elaborar un plan de auditoría por cada auditoría programada.
- Definir los criterios y el alcance de cada auditoría.
- Desarrollar la auditoría acorde con el plan elaborado y al procedimiento de auditoría aprobado por AMSAC.
- Clasificar los hallazgos (no conformidades, oportunidades de mejora y observaciones) de auditoría como fortalezas o debilidades.
- Seleccionar a los auditores (líder e internos o externos) y conducir auditorías que aseguren la objetividad e imparcialidad del proceso de auditoría.
- Asegurar que los resultados de las auditorías se reporten a los gerentes relevantes.
- Clasificar la debilidad como observación o no conformidad.

- Documentar los resultados de la auditoría.
- Retener información documentada como evidencia del (de los) programa(s) de auditoría y los resultados de cada auditoría.

La evidencia de la implementación del programa de auditoría, la ejecución del plan de auditoría y los resultados de la auditoría, deberá estar disponible como información documentada.

2.2.6.3 Paso 6.3: Ejecutar la revisión por la Alta Dirección

Al contar con un Sistema Integrado de Gestión (SIG), la revisión por la Alta Dirección se realiza a intervalos planificados según lo descrito en el mismo.

Para la revisión por la Alta Dirección, se sugiere tomar en cuenta lo siguiente:

- Revisar el SGSI en intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.
- Incluir las siguientes entradas:
  - El estado de las acciones con relación a las revisiones anteriores por parte de la Alta Dirección.
  - Cambios en asuntos externos e internos que son pertinentes al SGSI.
  - Retroalimentación sobre el desempeño de seguridad de la información, incluyendo tendencias en:
    - ✓ No conformidades y acciones correctivas.
    - ✓ Resultados del monitoreo y medición.
    - ✓ Resultados de auditoría interna.
    - ✓ Cumplimiento de los objetivos de seguridad de la información.
  - Retroalimentación de las partes interesadas.
  - Resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos de seguridad de la información.
  - Oportunidades para la mejora continua (mejoras).
  - Revisión de acciones nuevas o en curso
- Los productos de la revisión por la Alta Dirección incluyen decisiones relacionadas a oportunidades de mejora continua (mejoras) y cualquier necesidad de cambios al SGSI.
- Conservar la información documentada como evidencia de los resultados de las revisiones por parte de la Alta Dirección. Estos resultados pueden presentarse en informes o actas conforme a lo establecido en los roles del SGSI.

En la figura 13 se observan los documentos desarrollados para el SGSI en el paso 6.

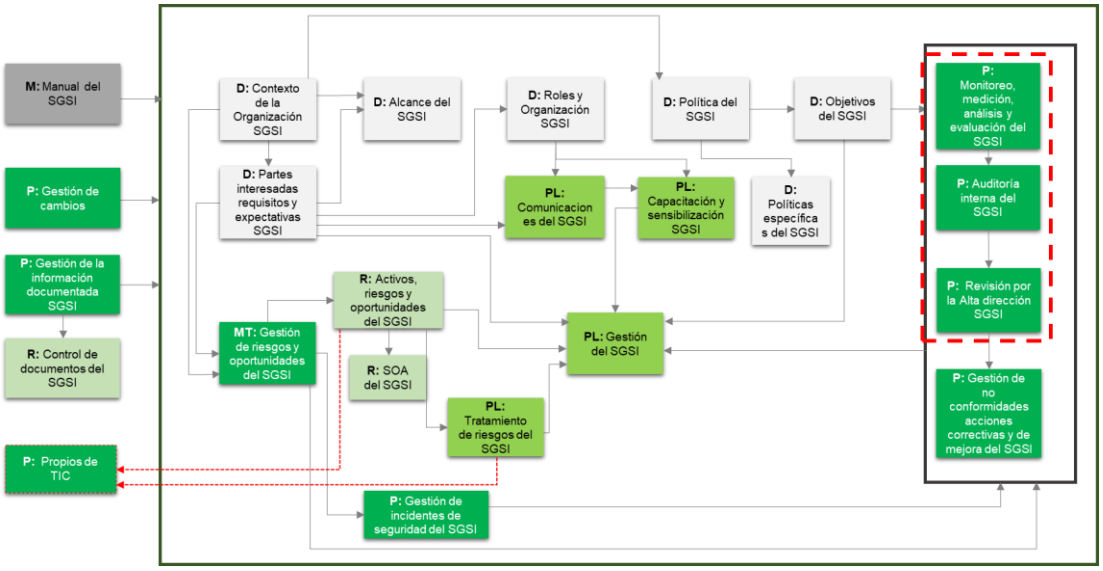

Figura 13: Documentos generados en el paso 6

2.2.7 Paso 7: Identificar y aplicar las correcciones y mejoras

Al contar con un Sistema Integrado de Gestión (SIG), las correcciones y mejoras se realizan según lo descrito en el mismo.

Los sistemas de gestión no son infalibles o perfectos, además el contexto para el cual fueron desarrollados es cambiante, por lo cual, producto de la implementación, operación y monitoreo del SGSI encontraremos posibles no conformidades por corregir y oportunidades de mejora por desarrollar. Para ello, se sugiere ejecutar lo siguiente:

2.2.7.1 Paso 7.1. Identificar no conformidades y desarrollar acciones correctivas

Cuando ocurre una no conformidad, se toma acción para controlarla y corregirla, así como ocuparse de las consecuencias. Esta acción es denominada acción correctiva, la cual elimina las causas de la no conformidad con el fin de que no recurra u ocurra en otro lugar. Se determina si existen no conformidades similares o si podrían ocurrir potencialmente. La acción correctiva podría involucrar cambios en el SGSI. Luego de que la acción correctiva sea implementada, se revisa la efectividad de la misma. Para ello, se define un proceso que debe tener en cuenta lo siguiente:

- Describir los siguientes datos por cada acción correctiva:
  - Fecha, origen y descripción de la solicitud de acción correctiva.
  - Análisis de causa de la no conformidad.
  - Fecha programada.
  - Evidencias.
  - Actividades a realizar y los responsables de ejecutar las mismas.
- Identificar la fuente que originó una no conformidad; entre las principales fuentes que originan una no conformidad, se tiene:
  - Gestión de riesgos y oportunidades de seguridad de la información.
  - Gestión de cambios significativos en relación a la seguridad de la información.
  - Resultados y/o decisiones de las revisiones por la Alta Dirección.
  - Resultados de auditorías internas o externas.
  - Resultados del monitoreo, medición, análisis y evaluación.

- Gestión de incidentes de seguridad de la información.
- Hallazgos de personal.

- Implementar cualquier acción necesaria.
- Revisar la efectividad de cualquier acción correctiva tomada.
- Hacer cambios al SGSI, si fuera necesario.
- Contar con información documentada como evidencia de la naturaleza de las no conformidades y cualquier acción subsiguiente tomada; y de los resultados de cualquier acción correctiva.

2.2.7.2 Paso 7.2. Ejecutar la mejora continua

El SGSI irá perfeccionándose en el tiempo, ajustándose a los cambios empresariales, cambios en las tecnologías, cambios externos y los cambios del SGSI. A continuación, se detalla de manera específica los cambios a supervisar:

Empresariales	Tecnologías	Externos	SGSI
- Misión - Objetivos empresariales - Presupuestos y recursos financieros - Nuevos productos y servicios - Cambios en el personal	- Hardware - Software - Procedimientos y políticas específicas de TI - Procesos de TI - Servicios de TI	- Leyes y reglamentaciones aplicables - Necesidades y preocupaciones de los clientes y proveedores - Proveedores - Cambios en el entorno (por ejemplo: nuevos competidores)	- Política del SGSI - Nuevos escenarios de riesgo - Cambios en los procedimientos - Resultados de los ejercicios y pruebas - Resultados de auditorías internas y externas

Tabla 1 – Factores de cambio

El Oficial de seguridad y confianza digital es la responsable de ejecutar la mejora continua del SGSI.

Esta mejora continua debe ser permanente a fin de mantener actualizado el SGSI ante la existencia de cambios relevantes en el entorno, tamaño, complejidad, operaciones, estrategia y otros factores que impacten en la mejora de procesos, servicios y en los objetivos de AMSAC.

En la figura 14 se observan los documentos desarrollados para el SGSI en el paso 7.

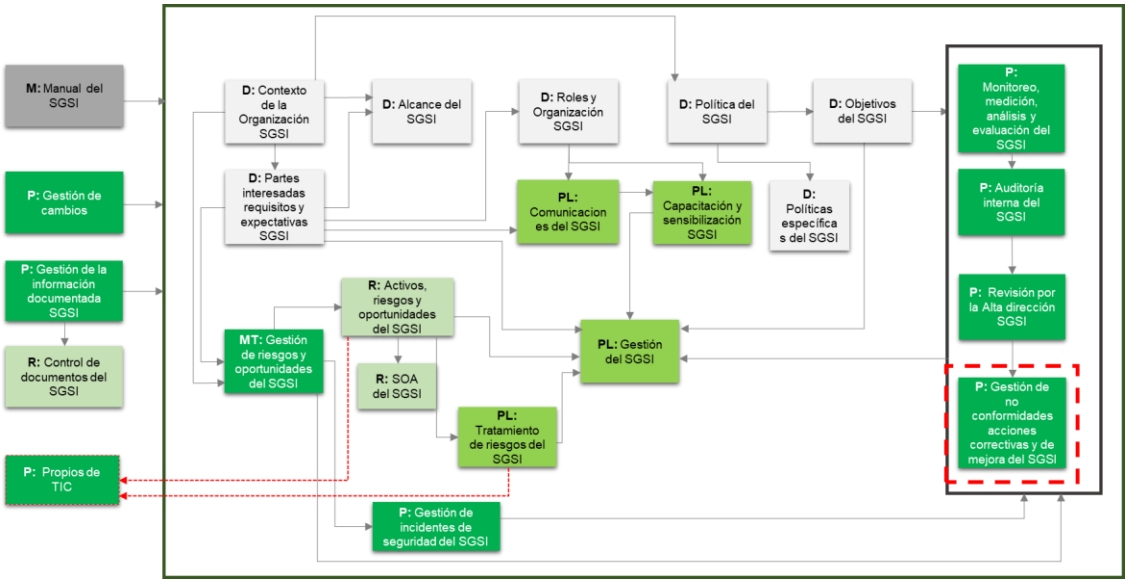

Figura 14: Documentos generados en el paso 7

3. ALCANCES FUNCIONALES DE LOS ROLES Y RESPONSABILIDADES

Los roles y las responsabilidades identificados en el documento de "Roles, responsabilidades y competencias para el SGSI".

4. REGISTRO / ANEXOS

- Anexo 01 - Documentos integrados del SGSI.