Jefe del departamento de Tecnologías de la Información y Comunicaciones (ct)
Firmado por:
HENRY WILSON TORNERO YAYA
DNI:42896673 RUC:20103030791
IDCPE-42896673
Fecha: 09/10/2025 11:31:25-0500
Doy V° B°

Gerente de Administración y Finanzas
Firmado por:
JULIO CESAR TEMPLE AGUILAR
DNI:42302432 RUC:20103030791
IDCPE-42302432
Fecha: 09/10/2025 15:38:39-0500
Doy V° B°

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN ACTIVOS MINEROS S.A.C. 2024 - 2026

GERENCIA DE ADMINISTRACION Y FINANZAS

DEPARTAMENTO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES

Versión	Fecha	Puntos Modificados
02	07/10/2025	• Actualización de fechas para alineación con el Plan de Gobierno Digital AMSAC 2025-2027.

Responsables	Visto y Sello
Elaborado: **Departamento de Tecnología de la información y Comunicaciones**	Especialista de Redes y Comunicaciones Firmado digitalmente por: PRADO VIERA Erik Alonso FAU 20103030791 hard Motivo: Soy el autor del documento Fecha: 09/10/2025 10:39:34-0500
Revisado: **Departamento de Tecnología de la información y Comunicaciones**	
Aprobado: **Gerencia de Administración y Finanzas**	

Tabla de Contenido

I. INTRODUCCIÓN

Activos Mineros S.A.C. (en adelante AMSAC) es una empresa estatal de derecho privado bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE).

AMSAC tiene como objeto realizar actividades de remediación de pasivos ambientales mineros de alto riesgo para la salud y seguridad humana y para el ambiente, así como prestar apoyo a Proinversión en las actividades que resulten necesarias para la ejecución de los procesos de promoción de la inversión privada, supervisar el cumplimiento de las obligaciones contractuales de los inversionistas y administrar los activos y pasivos que le sean encargados por las entidades del Sector Energía y Minas, Proinversión y FONAFE, éste último titular del 100% de las acciones de AMSAC. Adicionalmente, la ejecución de encargos especiales que el Estado le asigne en el marco de las disposiciones legales que le aplican.

El presente documento es el plan de implementación de Sistema de Gestión de Seguridad de La Información (SGSI) de Activos Mineros, tiene como finalidad establecer los pasos y metodologías que se deberá seguir para implementar el SGSI basado en la norma ISO/IEC 27001:2022 según lo indicado por la Res. 003-2023 PCM/SGTD, asimismo se han establecido los puntos sugeridos por la citada norma, entre los cuales tenemos el contexto, alcance, mapa de procesos y cronograma de actividades.

II. OBJETIVOS DEL PLAN DEL SGSI

a) Preservar la confidencialidad, integridad y disponibilidad de la información que gestiona AMSAC.
b) Fortalecer la cultura de seguridad de la información en los servidores, funcionarios y colaboradores de AMSAC.
c) Asegurar el cumplimiento normativo en materia de seguridad y confianza digital.
d) Gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información.

III. MARCO LEGAL

3.1. De Seguridad de la Información

- Ley N° 27309, Ley que incorpora los delitos informáticos al código penal.
- Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y su reglamento.
- Ley N° 29733, Ley de Protección de Datos Personales y su reglamento.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Directoral N° 022-2022-INACAL/DN, que aprueba la actualización de las Normas Técnicas Peruanas, entre ellas la NTP-ISO/IEC 27001:2022, conforme al procedimiento establecido en la Ley N° 30224, reemplazo de la NTP-ISO/IEC 27001:2014.
- 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.
- Directiva 001-2023 PCM/SGTD que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital

3.2. De AMSAC

- Plan estratégico Institucional de AMSAC 2022-2026 fue aprobado mediante Acuerdo de Directorio N° 01-489-2022 del 30 de junio del 2022 y cuenta con la conformidad del sector, mediante Oficio N° 0113-2022/MINEM-VMM del 26 de julio del 2022.
- Resolución de Gerencia General 029-2019-AM/GG conformación del comité de Gobierno Digital y Designación de Oficial de Seguridad de la Información.
- Política de Seguridad de la Información 2024. Política Institucional para el fortalecimiento del Buen Gobierno Corporativo de AMSAC.

IV. PROYECTO DE IMPLEMENTACIÓN DEL SGSI

5.1. METODOLOGÍA

La metodología aplicada se fundamenta en el ciclo PDCA (Plan-Do-Check-Act), también conocido como el ciclo de Mejora Continua de Deming (ver figura 02), que guía las etapas de planificación, implementación, verificación y actuación en el SGSI. Estas

etapas están alineadas con lo establecido en la Norma Técnica 27001. Esta metodología ofrece un marco sistemático que abarca cuatro pasos esenciales, diseñados para promover la mejora continua del SGSI. Esto incluye la reducción de incidentes, el incremento de la eficacia, la resolución de problemas, y la identificación y mitigación de riesgos potenciales, entre otros aspectos.

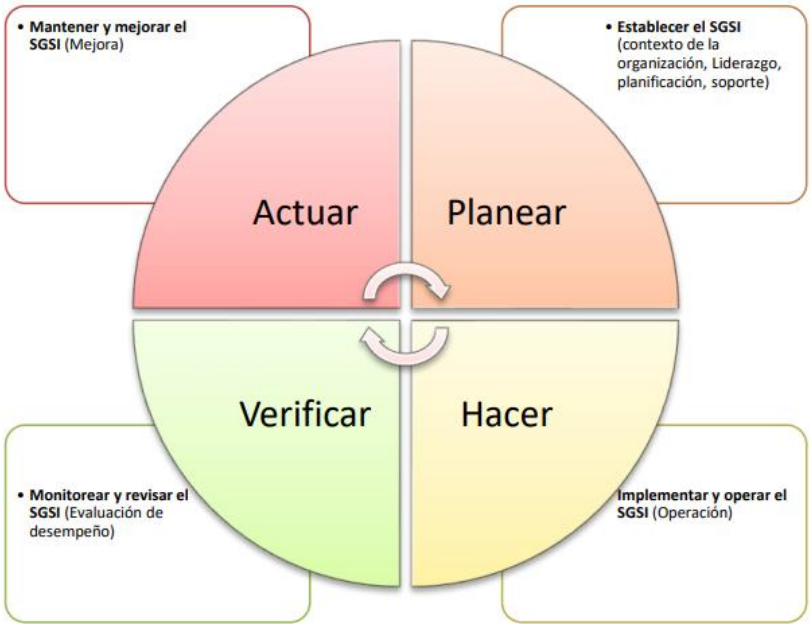

Figura 02

5.2. ALINEAMIENTO ESTRATÉGICO DEL PLAN SGSI

A continuación, se detalla el alineamiento del Plan SGSI con los del Plan Estratégico Institucional (PEI) de AMSAC:

Objetivo Estratégico del PEI 2022 - 2026	Actividad Estratégica	Objetivo del Plan SGSI
OE6. Fortalecer la gobernanza y control de gestión.	AE6.02 Implementación de nuevos mecanismos para el control de gestión en los proyectos y mejora continua.	Implementar el Sistema de Gestión de Seguridad de la Información (SGSI) bajo la Norma Técnica Peruana NTP ISO/IEC 27001:2022 en el alcance definido por AMSAC, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información. Esta implementación también fortalecerá la cultura de seguridad de la información entre los servidores, funcionarios y colaboradores de AMSAC, asegurará el cumplimiento normativo en materia de seguridad y confianza digital, y permitirá gestionar eficazmente los riesgos, eventos e incidentes de seguridad de la información.

Tabla 1

5.3. CONTEXTO DE LA ENTIDAD

AMSAC, según lo señalado en el PEI 2022 – 2026 (ver figura 01), cuenta con dos ejes principales de trabajo (actividades core): La Gestión de Proyectos de Remediación Ambiental Minera y la Gestión de Proyectos de Inversión Privada. Estas dos actividades core representan la principal fuente de generación de valor para el cumplimiento de objetivos de la institución.

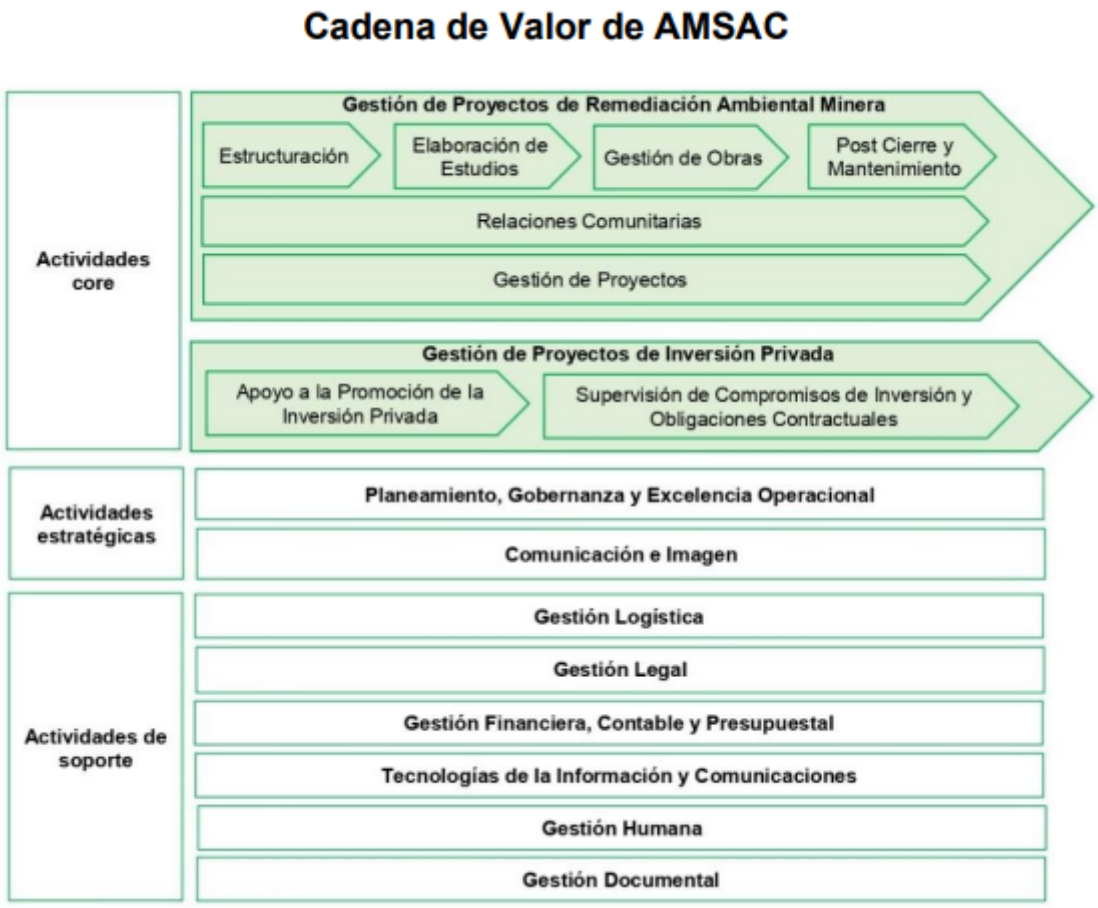

Figura 01

Fuente: PEI 2022-2026 AMSAC

5.3.1. Gestión de proyectos de remediación ambiental:

Los pasivos ambientales mineros corresponden a antiguas unidades mineras abandonadas o a aquellas donde no se han identificado a los responsables. Los pasivos ambientales mineros (PAM) son inicialmente catalogados y priorizados por la Dirección General de Minería (DGM) del Ministerio de Energía y Minas (MINEM) y, posteriormente, son encomendados a AMSAC.

5.3.2. Gestión de proyectos de inversión privada:

AMSAC asume la responsabilidad de velar por el cumplimiento estricto de las obligaciones contractuales establecidas en cada uno de los contratos derivados de los procesos de inversión privada que son asignados por Proinversión. Estos compromisos incluyen la contraprestación en favor del Estado, los compromisos de inversión, la conservación de activos y la vigencia de garantías.

5.4. PARTES INTERESADAS

Resulta de vital importancia contar con gestión de interesados del SGSI, ello reforzará el cumplimiento de las actividades y metas definidas. Los grupos de interés internos de AMSAC se circunscriben al Directorio de la empresa, los Gerentes y colaboradores.
Los principales grupos de interés externos a AMSAC se listan en la tabla siguiente:

N°	Grupos de Interés	Descripción
1	FONAFE	Corporación estatal que planifica, dirige, financia y controla la gestión de 34 empresas públicas incluyendo a AMSAC.
3	PCM	Presidencia del Consejo de Ministros, es una institución del Gobierno de Perú que tiene la responsabilidad de coordinar las políticas del Poder Ejecutivo y supervisar la administración pública.

Tabla 2

5.5. ALCANCE DEL SGSI

En alineación con el análisis contextual de la institución y teniendo en cuenta las necesidades y expectativas de las partes interesadas, tal como se detallan en la matriz de priorización de procesos del Anexo N° 1, se ha definido que el alcance del SGSI abarcará los siguientes procesos críticos: 1) Estructuración, 2) Elaboración de Estudios, 3) Gestión de Obras, 4) Post Cierre y Mantenimiento y 5) Relaciones Comunitarias. Estos procesos han sido identificados como prioritarios en función de su relevancia estratégica para la organización (ver Tabla 3).

Proceso Nivel 0	Código	Proceso Nivel 1	Dueño de Proceso
Gestión de Proyectos de	O1.1	Estructuración	Jefe de Departamento de Ingeniería de Proyectos
	O1.2	Elaboración de Estudios	Jefe de Departamento de Ingeniería de Proyectos

Remediación Ambiental Minera	O1.3	Gestión de Obras	Jefe de Departamento de Gestión de Obras
	O1.4	Post Cierre y Mantenimiento	Jefe de Departamento de Post Cierre y Mantenimiento
	O1.5	Relaciones Comunitarias	Supervisor de Relaciones Comunitarias

Tabla 3

5.6. ESTADO ACTUAL DE SEGURIDAD DE LA INFORMACIÓN EN AMSAC

En AMSAC, la seguridad de la información es un pilar fundamental de nuestra operación. Como prioridad estratégica, nos aseguramos de que todos los niveles de la organización estén alineados con las mejores prácticas de seguridad, garantizando la protección rigurosa de la confidencialidad, integridad y disponibilidad de nuestra información. Este compromiso fortalece nuestra capacidad para innovar y crecer en un entorno seguro y confiable.

En esa línea de acción, el Departamento de Tecnologías de Información y Comunicaciones (DTIC) se encuentra implementando un conjunto de medidas de seguridad informática diseñadas para mitigar los riesgos y proteger nuestros activos de información contra posibles ataques informáticos, entre los más importantes:

5.6.1. Seguridad Perimetral:

- Se ha actualizado las reglas de control de acceso externo, limitando el tráfico entrante exclusivamente a direcciones IP conocidas y geográficamente ubicadas en Perú, mediante listas de control de acceso (ACLs) en los firewalls perimetrales.
- Se ha realizado una auditoría exhaustiva de la configuración de puertos TCP/UDP en los dispositivos de borde, asegurando que únicamente los puertos necesarios para servicios críticos estén abiertos, y que no existan puertos no estándar o de administración expuestos a Internet. Se ha cerrado cualquier puerto no autorizado para evitar potenciales vectores de ataque.
- Se ha implementado un sistema de autenticación multifactor (MFA) robusto, integrando un segundo factor de autenticación basado en tokens para el acceso a la red interna a través de la VPN de AMSAC, asegurando así un control más

estricto sobre las sesiones remotas y reduciendo el riesgo de acceso no autorizado.

Estas medidas han mitigado de manera significativa el riesgo de accesos no autorizados y han reducido la superficie de ataque, al minimizar la exposición de los recursos críticos de la red a amenazas externas. Además, al implementar controles de acceso más estrictos y mecanismos de autenticación avanzados, se ha fortalecido la seguridad perimetral, asegurando un entorno más resiliente frente a intentos de intrusión y ataques dirigidos.

5.6.2. Acciones en Identidad:

- Se ha implementado la autenticación multifactor (MFA) en todos los sistemas informáticos, incluyendo correo electrónico, VPN, dispositivos móviles y aplicaciones corporativas, añadiendo una capa adicional de seguridad que requiere la verificación de identidad a través de múltiples factores antes de conceder el acceso.
- Se ha establecido un sistema de registro y gestión de dispositivos corporativos (laptops y teléfonos móviles) que acceden a los recursos empresariales, garantizando la protección de los datos sensibles y fortaleciendo los controles para prevenir fugas de información y accesos no autorizados. Este registro incluye políticas de conformidad y monitoreo continuo para asegurar que solo dispositivos autorizados y seguros puedan interactuar con la red corporativa.

Estas medidas han robustecido significativamente la autenticación y reforzado la protección contra accesos no autorizados a los recursos corporativos, asegurando que solo usuarios y dispositivos verificados puedan interactuar con los sistemas críticos de la empresa.

5.6.3. Acciones sobre Servidores:

- Se ha implementado un proceso de validación periódica de los backups automáticos, asegurando la integridad y disponibilidad de los datos respaldados, junto con la provisión de almacenamiento redundante en la nube para mayor capacidad y seguridad de la información crítica.
- Se ha llevado a cabo la remediación de las vulnerabilidades identificadas durante la auditoría de Ethical Hacking anual realizada por AMSAC, aplicando parches, configuraciones de seguridad mejoradas y otras medidas correctivas para cerrar posibles vectores de ataque.

Estas acciones han incrementado la resiliencia de nuestros sistemas, fortaleciendo la continuidad operativa y reduciendo de manera efectiva los riesgos asociados con vulnerabilidades no corregidas.

5.6.4. Acciones en Correo Electrónico y Antivirus:

- Refuerzo de las políticas de seguridad de correo electrónico, incluyendo anti-spam avanzado, protección anti-phishing, y detección proactiva de malware, mejorando la capacidad de filtrado y bloqueo de amenazas antes de que lleguen a los usuarios.
- Implementación de análisis preventivo de enlaces en tiempo real, que inspecciona y verifica la seguridad de los enlaces (URLs) antes de que los usuarios accedan a ellos, mitigando el riesgo de ataques de phishing y sitios web maliciosos.
- Despliegue de un sistema antivirus EDR (Endpoint Detection and Response) con capacidades avanzadas de monitoreo y respuesta en tiempo real, permitiendo la detección rápida y la contención automática de amenazas en los endpoints corporativos.

Estas mejoras han reducido significativamente la recepción de correos electrónicos maliciosos y disminuido el riesgo de ataques cibernéticos contra nuestros recursos corporativos. Además, se han llevado a cabo capacitaciones para los usuarios sobre las nuevas políticas de seguridad implementadas, enfocadas en concientizar sobre las amenazas más recientes y fomentar las mejores prácticas en seguridad de la información, asegurando una mayor defensa proactiva a nivel organizacional.

A pesar de haberse implementado estas acciones, la adopción e implementación del SGSI nos proporcionará beneficios adicionales, mejorando aún más nuestra capacidad para proteger los activos de información, gestionar los riesgos de manera proactiva y mantener un entorno de seguridad alineado con las mejores prácticas internacionales.

5.7. CRONOGRAMA DE ACTIVIDADES

Una vez definido el alcance del Plan SGSI, se ha desarrollado un cronograma detallado que incluye las fases correspondientes y la asignación de responsables para cada actividad, como se presenta en el Anexo N° 2. Este cronograma está diseñado para asegurar la implementación ordenada y efectiva del SGSI, garantizando que cada etapa

del proceso sea ejecutada dentro de los plazos establecidos y con la participación de los actores clave.

5.8. RECURSOS Y PRESUPUESTO

La ejecución del Plan SGSI requiere la asignación precisa de recursos y presupuesto, desglosados de la siguiente manera:

a) **Personal:**

- Oficial de Seguridad y Confianza Digital: Responsable de liderar el Plan SGSI, desempeñado por el Jefe del Departamento de Tecnologías de la Información y Comunicaciones (DTIC).
- Equipo de trabajo del SGSI: Conformado por miembros del equipo DTIC, encargados de las actividades diarias de implementación y seguimiento del SGSI.
- Equipo especializado en SGSI: Servicios contratados a terceros con experiencia en seguridad de la información, responsables de tareas técnicas avanzadas y auditorías.

b) **Presupuesto:**

El presupuesto requerido contempla los recursos necesarios para la ejecución del Plan, ello incluye al personal interno dedicado al desarrollo y seguimiento del SGSI, así como las contrataciones de servicios externos necesarios para garantizar la implementación y mantenimiento de los controles del SGSI.

En la Tabla 4 se muestra el presupuesto para la ejecución de Plan SGSI:

N°	Bien o Servicio	Tipo	Inicio de servicio	Costo Referencial			Total
				2024	2025	2026	
1	Contratación del servicio de Implementación del SGSI	Externo	Setiembre 2024 a Junio 2025	S/70,000	S/40,000	S/0.00	S/100,000
2	Adquisición de Herramientas Informáticas de Seguridad de la Información	Externo	Octubre 2025 a Julio 2026	S/0.00	S/30,000	S/40,000	S/40,000
4	Auditoría Interna del SGSI	Externo	Enero 2026 a Junio 2026	S/0.00	S/0.00	S/40,000	S/40,000
3	Certificación en ISO 27001	Externo	Setiembre 2026 a Diciembre 2026	S/0.00	S/0.00	S/40,000	S/40,000
TOTAL				S/70,000	S/70,000	S/120,000	S/260,000

Tabla 4

5.9. MONITOREO Y EVALUACIÓN

Una vez aprobado el presente plan, el Oficial de Seguridad y Confianza Digital supervisará el cumplimiento de las actividades planificadas según el cronograma detallado en el Anexo 2. Además, elaborará un informe semestral dirigido al Comité de Gobierno y Transformación Digital de AMSAC, en el que se indicará el nivel de avance en la implementación del SGSI.

Anexo 1 – Matriz de priorización de priorización de procesos.

	Matriz de Priorización de Procesos	Código: E3.1.1.P2.F6 Versión: 04 Fecha: 20-12-2022

	FACTOR DE CRITICIDAD CRITERIO DE PRIORIZACIÓN		15%	15%	20%	10%	10%	10%	15%	5%	
	INVENTARIO DE PROCESOS		**CRITERIO 1:** Materialidad (Baja 0; Media 1; Alta 2)	**CRITERIO 2:** Expectativas de la Alta Dirección y el Directorio (Poca importancia 0; Mediana importancia 1;Alta importancia 2)	**CRITERIO 3:** Impacto en objetivos estratégicos (Baja contribución 0; Contribuye parcialmente 1; Contribuye totalmente 2)	**CRITERIO 4:** Complejidad de las operaciones (Proceso con operaciones no complejas 0; Parcialmente complejas 1; Muy complejas 2)	**CRITERIO 5:** Volumen de las operaciones (nivel bajo de volumen de operaciones 0; Nivel medio de volumen de operaciones 1; Nivel alto de volumen de operaciones 2)	**CRITERIO 6:** Nivel de automatización (Brecha poco significativa con relación al nivel de automatización deseada 0; Brecha significativa 1; Brecha muy significativa 2)	**CRITERIO 7:** Importancia en la continuidad del negocio (Bajo impacto en la continuidad del negocio 0; Mediano impacto 1; Alto impacto 2)	**CRITERIO 8:** Desempeño del personal (Brecha poco significativa con relación al nivel deseado 0; Brecha significativa 1; Brecha muy significativa 2)	RESULTADO (Promedio del resultado de todos los criterios)
TIPO	PROCESO NIVEL 0	PROCESO NIVEL 1									
Core	O1. Gestión de Proyectos de Remediación Ambiental Minera	O1.2. Elaboración de Estudios	2	2	2	2	2	2	2	2	2.00
Core	O1. Gestión de Proyectos de Remediación Ambiental Minera	O1.3. Gestión de Obras	2	2	2	2	2	2	2	2	2.00
Core	O1. Gestión de Proyectos de Remediación Ambiental Minera	O1.4. Post Cierre y Mantenimiento	2	2	2	2	2	2	2	2	2.00
Soporte	S4. Gestión Logística	S4.1. Gestión de las Contrataciones	2	2	2	1	2	2	2	2	1.90
Core	O1. Gestión de Proyectos de Remediación Ambiental Minera	O1.1. Estructuración	2	2	2	2	1	2	2	1	1.85
Core	O1. Gestión de Proyectos de Remediación Ambiental Minera	O1.5. Relaciones Comunitarias	2	2	2	2	1	2	2	1	1.85
Core	O2. Gestión de Proyectos de Inversión Privada	O2.2. Supervisión de Compromisos de Inversión y Obligaciones Contractuales en Minería	2	2	2	2	1	2	2	0	1.80
Core	O2. Gestión de Proyectos de Inversión	O2.3. Supervisión de Obligaciones	2	2	2	2	1	2	2	0	1.80

	Privada	Contractuales en Generación Eléctrica									
Soporte	S2. Gestión Financiera, Contable y Presupuestal	S2.1. Gestión Financiera	2	2	2	1	2	1	2	1	1.75
Estratégico	E4. Imagen Institucional	E4.1. Gestión de las Comunicaciones	2	2	2	1	1	1	2	1	1.65
Soporte	S2. Gestión Financiera, Contable y Presupuestal	S2.3. Gestión Presupuestal e Inversiones	2	2	2	1	1	1	2	1	1.65
Estratégico	E1. Planeamiento	E1.1. Planeamiento Institucional	2	2	2	1	1	2	1	0	1.55
Core	O1. Gestión de Proyectos de Remediación Ambiental Minera	O1.6. Gestión de Proyectos	2	2	2	1	1	1	1	1	1.50
Soporte	S5. Gestión Humana	S5.2. Desarrollo personal	2	2	1	1	1	1	1	1	1.30
Estratégico	E2. Gobernanza	E2.1. Gobierno Corporativo	1	2	2	1	1	1	1	0	1.30
Por Encargo	N1. Gestión de Proyectos Especiales	N1.1. Comercialización de Oro	2	2	1	1	1	1	1	0	1.25
Core	O2. Gestión de Proyectos de Inversión Privada	O2.1. Apoyo a la Promoción de la Inversión Privada	1	2	1	1	1	1	2	0	1.25
Soporte	S3. Tecnologías de Información y Comunicaciones	S3.1. Gestión de Desarrollo y Mantenimiento de Software	2	1	0	1	2	1	2	1	1.20
Soporte	S5. Gestión Humana	S5.1. Gestión del Personal	1	1	2	1	1	1	1	1	1.20
Estratégico	E2. Gobernanza	E2.3. Gestión de Riesgos	1	2	1	1	1	1	1	1	1.15
Estratégico	E2. Gobernanza	E2.4. Gestión de Cumplimiento	1	2	1	1	1	1	1	1	1.15
Soporte	S1. Gestión Legal	S1.1. Solución de Controversias	2	2	0	1	1	1	1	1	1.10
Soporte	S3. Tecnologías de Información y Comunicaciones	S3.2. Gestión de Infraestructura Tecnológica	2	1	0	1	1	1	2	1	1.10

Soporte	S5. Gestión Humana	S5.4. Gestión del Bienestar	1	1	2	1	1	1	0	1	1.05
Soporte	S5. Gestión Humana	S5.3. Gestión de la Compensación	1	1	1	1	1	1	1	1	1.00
Estratégico	E2. Gobernanza	E2.2. Sistema de Control Interno	1	2	1	1	1	1	0	1	1.00
Estratégico	E3. Gestión de la Excelencia Operacional	E3.2. Sistemas de Gestión	1	1	1	1	1	1	1	0	0.95
Soporte	S2. Gestión Financiera, Contable y Presupuestal	S2.2. Gestión Contable	2	1	0	1	1	1	1	1	0.95
Soporte	S1. Gestión Legal	S1.3. Soporte Legal	1	2	0	1	1	1	1	1	0.95
Soporte	S6. Gestión Documental	S6.1. Gestión de Trámite Documentario	1	1	0	1	1	2	1	2	0.95
Soporte	S1. Gestión Legal	S1.2. Gestión del Directorio	1	2	0	1	1	1	1	0	0.90
Estratégico	E3. Gestión de la Excelencia Operacional	E3.1. Administración del Sistema Integrado de Gestión	1	1	1	1	1	1	0	0	0.80
Soporte	S4. Gestión Logística	S4.3. Control Patrimonial	2	1	0	1	1	1	0	1	0.80
Soporte	S6. Gestión Documental	S6.2. Gestión de Archivo	1	1	0	1	1	2	0	2	0.80
Soporte	S4. Gestión Logística	S4.2. Gestión de Servicios Generales	1	1	0	1	1	1	0	1	0.65
									Resultado Promedio		**1.32**

Fuente: PEI 2022-2026

Anexo 2 - Cronograma de actividades

Fase	Objetivo	Actividades	Entregable	2024		2025				2026			
				Jul - Set	Oct - dic	Ene - Mar	Abr - Jun	Jul - Set	Oct - Dic	Ene - Mar	Abr - Jun	Jul - Set	Oct - Dic
FASE I ORGANIZACIÓN	Desarrollar las actividades principales para la dirección e inicio de la implementación del SGSI.	Desarrollo del Plan del Sistema de Gestión de Seguridad de la Información (Plan SGSI)	Aprobación del Plan SGSI en AMSAC	X									
		Aprobación del Plan SGSI	Publicación del Plan en plataforma de la Secretaría de Gobierno y Transformación Digital	X									
FASE II PLANIFICACIÓN (PLANEAR)	Desarrollar las actividades de planificación requeridas por la norma ISO 27001:2022 de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo.	Formulación del alcance del Sistema de Gestión de Seguridad de la Información.	Identificación de Procesos Misionales críticos en AMSAC	X									
		Declaración de la política y los objetivos de seguridad de la información.	Objetivos de Seguridad de la Información alineados a los Objetivos Institucionales		X								
		Definición de los criterios para la evaluación y aceptación de riesgos.	Revisión y actualización de Metodología de Gestión de Riesgos y Oportunidades de AMSAC		X								

Fase	Objetivo	Actividades	Entregable	2024		2025				2026			
				Jul - Set	Oct - dic	Ene - Mar	Abr - Jun	Jul - Set	Oct - Dic	Ene - Mar	Abr - Jun	Jul - Set	Oct - Dic
		Análisis y evaluación de los riesgos identificados y de las medidas correctivas existentes.	Matrices de Riesgos y Oportunidades del SGSI		X								
		Desarrollo de un plan de tratamiento integral de riesgos.	Plan de tratamiento de riesgos y oportunidades			X							
		Desarrollo de la declaración de aplicabilidad de acuerdo con el alcance del SGSI.	Matriz de aplicabilidad de los controles del SGSI			X							
		Elaboración del plan de trabajo priorizado.	Documento del Plan de trabajo priorizado			X							
FASE III DESPLIEGUE (HACER)	Desplegar las actividades de implementación del SGSI	Desarrollo de documentos y registros necesarios.	Documentos y registros de actividades de implementación del SGSI			X							
		Implementación de los controles seleccionados del plan de tratamiento de riesgos.	Registro de controles implementados del plan de tratamiento de riesgos				X						
		Fortalecimiento de la gestión de incidentes.	Procedimiento mejorado para la gestión de eventos					X	X				

Fase	Objetivo	Actividades	Entregable	2024		2025				2026			
				Jul - Set	Oct - dic	Ene - Mar	Abr - Jun	Jul - Set	Oct - Dic	Ene - Mar	Abr - Jun	Jul - Set	Oct - Dic
			e incidentes de Seguridad de la Información										
FASE IV REVISIÓN (VERIFICAR)	Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la NTP ISO/EC 27001:2022	Auditoría interna del SGSI	Informe de Auditoría Interna y Actualización del Procedimiento de Auditoría Interna de AMSAC.							X			
		Monitoreo del desempeño del SGSI	Informe de Revisión por la Dirección del desempeño del SGSI.								X		
FASE V CONSOLIDACIÓN (ACTUAR)	Implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la NTP ISO/IEC 27001:2022	Implementación de acciones correctivas y preventivas	Reporte de seguimiento de hallazgos de auditoría, incluyendo registro de acciones correctivas y preventivas.									X	
		Desarrollo, corrección y mejora de la documentación del SGSI nueva y existente	Documentación corregida o mejorada del SGSI.									X	
		Desarrollo de las actividades para evidenciar la mejora continua del SGSI	Matriz de Oportunidades del SGSI y un Plan de Mejora Continua.									X	

Fase	Objetivo	Actividades	Entregable	2024		2025				2026			
				Jul - Set	Oct - dic	Ene - Mar	Abr - Jun	Jul - Set	Oct - Dic	Ene - Mar	Abr - Jun	Jul - Set	Oct - Dic
FASE VI	Certificación en ISO 27001	Certificar los procesos misionales presentes en el alcance del SGSI con la norma ISO 27001.	Certificado ISO 27001									X	X

Nota: El presente cronograma ha sido elaborado utilizando la metodología PHVA (Planificar – Hacer – Verificar – Actuar)

TERMINOS Y DEFINICIONES

- **Activos:** Son los bienes que tienen valor para la organización y están constituidos por los siguientes tipos:
    a) **De información:** bases de datos, archivos, contratos y acuerdos, documentación de sistema, información de investigación, manuales de usuario, material de entrenamiento, procedimientos operacionales o de soporte, planes de continuidad de operaciones, registros de auditoría, e información de archivo.
    b) **De Software:** aplicaciones, sistemas informáticos, herramientas de desarrollo y utilidades.
    c) **Físicos:** equipos de cómputo, equipos de comunicaciones, medios removibles, medios portátiles y otros.
    d) **Servicios:** servicios computacionales y de comunicación con la utilización de recursos informáticos.
    e) **Personas:** incluyendo sus calificaciones, competencias y experiencia.
    f) **Intangibles:** como reputación e imagen de la entidad.
- **Almacenamiento:** Actividades para que la información documentada se almacene en soportes y formatos que garanticen su disponibilidad, fiabilidad, autenticidad y preservación
- **Amenaza:** causa de un potencial incidente no deseado, el cual puede ocasionar daño a un sistema y/u organización.
- **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.
- **Clientes:** Organización o persona que recibe un bien, servicio, producto o idea. Para AMSAC, los clientes son: las comunidades locales, el Ministerio de Energía y Minas (MINEM), el Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE) y la Agencia de Promoción de la Inversión Privada (PROINVERSIÓN).
- **Confianza digital:** Es el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas,

entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la transformación digital y la economía digital.

- **Comité de Gobierno y Transformación Digital:** es el mecanismo de gobernanza a nivel institucional para el gobierno y transformación digital en las entidades de la administración pública, responsable de liderar y dirigir el proceso de transformación digital en la entidad.
- **Confidencialidad:** Principio de la seguridad de la información que busca asegurar que solo quienes estén autorizados puedan acceder a la información.
- **Conservación**: Son actividades realizadas para garantizar el buen estado de la información documentada a lo largo del tiempo.
- **Controles:** Medidas o actividades adoptadas para mitigar el impacto y/o reducir la probabilidad de ocurrencia de los riesgos.
- **Custodio de activo de información:** Es el responsable del cumplimiento de las políticas de seguridad en los activos de información bajo su tutela.
- **Disponibilidad:** Principio de la seguridad de la información que busca asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieren.
- **Dueño de Proceso**: Persona formalmente identificada para asumir la responsabilidad global de proceso y, por lo tanto, cuenta con las atribuciones y el poder de decisión necesario como para garantizar que el proceso sea efectivo.
- **Economía digital:** Es la innovación y transformación de la economía basada en el uso estratégico de las tecnologías digitales, redes de datos o comunicación y plataformas digitales. Produce beneficios económicos para la sociedad.
- **Evento de seguridad de información:** Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.
- **Incidente de seguridad de información:** Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de la entidad y de amenazar la seguridad de la información.
- **Integridad:** Principio de la seguridad de la información que busca asegurar que la información y sus métodos sean exactos y completos.

- **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.
- **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.
- **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.
- **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.
- **Oficial de Seguridad y Confianza Digital:** Rol responsable de coordinar la implementación, operación, mantenimiento y mejora continua del SGSI en la entidad.
- **Política:** Conjunto de directrices y lineamientos que nos ayudan a garantizar la seguridad de la información en la empresa
- **Riesgo de Seguridad de la información**: Condición que supone una posible amenaza o vulnerabilidad que pueda afectar a la seguridad de la información.
- **Riesgo residual:** Es el nivel resultante del riesgo después de aplicar los mitigantes o controles
- **Seguridad de la Información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Seguridad digital:** Es la 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.
- **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, gestión ambiental, gestión de la seguridad y salud en el trabajo, gestión de la seguridad de la información, gestión de la continuidad del negocio, antisoborno, entre otros.
- **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.
- **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.
- **Transformación Digital:** es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intenso de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.
- **Tratamiento de riesgos:** Es un proceso mediante el cual la empresa define qué estrategia va a ejecutar para abordar un riesgo.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.