INSTITUTO GEOLÓGICO MINERO METALURGICO

CÓDIGO:	**VERSIÓN:**	**PÁGINAS:**	**VIGENCIA:**
SGSI.PI.01	1.00	12	31/12/2022

OFICINA DE SISTEMAS DE LA INFORMACIÓN

PLAN DE IMPLEMENTACION DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL INGEMMET

ELABORADO POR:	Ing. Rosio Curazi Yupanqui Oficial de Seguridad Digital
REVISADO POR:	Miriam Araya Carrasco Directora de la Oficina de Sistemas de la Información
APROBADO POR	Comité de Gobierno Digital Acta N°03-021-INGEMMET/CGD

Historial del Documento

Fecha de elaboración /revisión	Versión	Elaborado/ Revisado por	Naturaleza del Cambio
22/04/2021	V.1	Rosio Curazi Yupanqui. / Ing. Miriam Arara Carrasco	

Ing. MIRIAM ARAYA CARRASCO
DIRECTORA (e)
Oficina de Sistemas de Información
INGEMMET

CONTENIDO

1. INTRODUCCION

El INGEMMET tiene como objetivo, proveer servicios eficientes y eficaces en el otorgamiento de Títulos de Concesiones Mineras, su incorporación al catastro Minero y la Administración del Derecho de Vigencia y Penalidad; así como, en la investigación Geocientífica en el campo de la geología; servicios que deben estar de acuerdo a los requerimientos del cliente, los legales y reglamentario, así como a las necesidades de las partes interesadas.

Este documento describe en forma detallada el Plan de Implementación del Sistema de Gestión de Seguridad de la Información en el Instituto Geológico Minero Metalúrgico. En el documento se describen alcance del programa, actividades y metas a alcanzar en la medida que permita “la participación activa de los funcionarios, contratistas y terceros en lograr el nivel de cumplimiento adecuado de los lineamientos y requisitos de la Norma NTP ISO/IEC 27001:2014”.

La Gestión de Seguridad de la Información juega un rol importante en nuestra Institución, manifestándose a través del compromiso de la Alta dirección, en todos sus niveles jerárquicos y en el establecimiento de una estructura para la Gestión de Seguridad de la Información.

El Sistema de Gestión de Seguridad de la Información ISO/IEC 27001:2013 del INGEMMET, se aplica a los dos procesos mencionados en el primer párrafo; en la FASE I se define la implementación al proceso de “Catastro Minero Nacional y Administración de Derechos Mineros”.

2. OBJETIVO GENERAL

Implementar un Sistema de Gestión de Seguridad de la Información – SGSI que permita identificar las vulnerabilidades y amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información en el Instituto Geológico Minero Metalúrgico - INGEMMEMT.

3. ALCANCE

El presente plan aplica a todas las dependencias del Instituto Geológico Minero Metalúrgico - INGEMMET involucradas en la implementación del SGSI.

4. BASE LEGAL

4.1. Ley Nº 27658, Ley Marco de la Modernización de la Gestión del Estado.
4.2. Ley Nº 29733, Ley de Protección de Datos Personales y su reglamento, aprobado mediante Decreto Supremo Nº 003-2013.JUS.
4.3. Decreto Legislativo N°1412, Ley de Gobierno Digital
4.4. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece las tecnologías y medios electrónicos en el procedimiento administrativo.
4.5. Decreto de Urgencia N° 006-2020 que crea el Sistema Nacional De Transformación Digital.
4.6. Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
4.7. Resolución Ministerial Nº 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnologías de la Información. Técnicas de

seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da Edición. En todas las entidades integrantes del Sistema Nacional de Informática.

4.8. Decreto Supremo N° 035-2007-EM, que aprueba el Reglamento de Organización y Funciones del Instituto Geológico, Minero y Metalúrgico – INGEMMET.

4.9. Resolución Ministerial N° 087-2019-PCM publicada el 22 de marzo de 2019, se modificó el artículo 1 de la Resolución Ministerial N° 119-2018-PCM, estableciendo los integrantes debían conformar el Comité de Gobierno Digital en cada entidad, así mismo establece que toda referencia que se efectúe al Comité de Gestión de Seguridad de la Información debe entenderse realizada al Comité de Gobierno Digital.

4.10. Resolución SBS N°504-2021, que aprueba Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, modifican el reglamento de Auditoria Interna, el Reglamento de Auditoria Externa, el TUPA de la SBS, el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, el Reglamento de Riesgo Operacional, el Reglamento de Tarjetas de Crédito y Débito y el Reglamento de Operaciones con Dinero Electrónico.

4.11. Resolución Presidencial N° 076-2019-INGEMMET/PE del 24 de setiembre del 2019 que reconforma el Comité de Gobierno Digital del Instituto Geológico Minero Metalúrgico - INGEMMET, constituido por RP N° 035-2019-INGEMMET/PE.

5. GLOSARIO DE TERMINOS

5.1. **Activo de Información**: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa Información y tiene valor para la organización, como base de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la entidad, la Información como activo corporativo, puede existir de muchas formas (impresa, almacenada electrónicamente, transmitida por medios electrónicos, mostrada en videos, suministrada en una conversación, conocimiento de las personas).

5.2. **Amenazas:** fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

5.3. Análisis de riesgo: método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

5.4. **Auditoria**: proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permite determinar la extensión en que se cumplen los criterios definidos para la auditoria interna.

5.5. **Auditor en seguridad de la información:** persona con la competencia para efectuar auditorías internas de seguridad de la información.

5.6. **Control:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de la organización.

5.7. **Declaración de Aplicabilidad:** documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la entidad.

5.8. **Disponibilidad:** la información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para el uso; la no disponibilidad de la información puede resultar en pérdidas financieras de imagen y/o credibilidad ante los clientes y/o ciudadanos.

5.9. **Efectividad:** medida de impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

5.10. **Eficacia:** grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.
5.11. **Estimación de riesgo:** proceso de asignación de valores a la probabilidad e impacto de un riesgo.
5.12. **Evento de seguridad de la información**: presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc), asociada a una posible vulneración de la política de seguridad de la información.
5.13. **Evidencia de auditoria:** registro, declaración de hechos o cualquier otra información que son relevantes para los criterios de auditoria y que son verificables. La evidencia de la auditoria puede ser cuantitativa o cualitativa.
5.14. **Gestión de riesgo**: actividades coordinadas para dirigir y controlar los aspectos asociados al riesgo dentro de una organización.
5.15. **Identificación del riesgo:** proceso para encontrar, numerar y caracterizar los elementos de riesgo asociadas a la seguridad de la información.
5.16. **Impacto:** se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos de la organización.
5.17. **Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones de la organización y amenazar la seguridad de la información.
5.18. **Información:** datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.
5.19. **Integridad:** la información del MINEM debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la entidad a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen del MINEM.
5.20. **Probabilidad:** es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
5.21. **Proceso:** conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.
5.22. **Propietario de información:** es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones de acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.
5.23. **Reducción de riesgo:** acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.
5.24. **Responsabilidades:** compromisos u obligaciones del personal o grupo de trabajo.
5.25. **Riesgo:** consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la Información en os activos del MINEM.
5.26. **Riesgo en seguridad de la Información:** es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño al MINEM.

5.27. **Seguridad de la Información:** Preservación de la integridad, la confidencialidad, y la disponibilidad de la Información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. (Fuente: NTP ISO/IEC 270001:2014).
5.28. **SGSI**: Sistema de Gestión de Seguridad de la Información.
5.29. **Transferencia de riesgo:** compartir con otra de las partes la perdida (consecuencias negativas) de un riesgo.
5.30. **Tratamiento de la Información:** desarrollo de las siguientes actividades sobre la Información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.
5.31. **Tratamiento del riesgo:** proceso de selección e implementación de medidas para modificar el riesgo.
5.32. **Usuario:** cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice Información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de Información del MINEM, para propósitos propios de su labor y que tendrá el derecho manifiesto de uso dentro del inventario de Información.
5.33. **Vulnerabilidades:** debilidad de un activo de Información frente a una amenaza.
5.34. **Conformidad:** cumplimiento de un requisito.

6. DOCUMENTACIÓN DEL SGSI

Durante la implementación del Sistema de Gestión de Seguridad de la Información SGSI, se redactarán los siguientes documentos, sin perjuicio de otros que consideren pertinentes:

Nº	Norma Técnica Peruana NTP ISO/IEC 27001:2014	Documento	Descripción
1	**Clausula 7.5** Información documentada	Procedimiento para la gestión de documentos y registros	Documento que establece los lineamientos para la elaboración. Aprobación, distribución y actualización de los documentos y registros relacionados al SGSI
2	**Clausula 4.1** comprender la organización y su contexto y la **cláusula 4.2** comprender las necesidades y expectativas de las partes interesadas	Análisis de contexto y requerimiento de seguridad de las partes interesadas	Documento que establece el contexto interno y externo del Instituto Geológico Minero Metalúrgico y para asegurar que el SGSI está alineado con los objetivos institucionales y cumpla con las obligaciones legales y normativas relacionadas a la seguridad de la información.

3	**Clausula 4.3** determinar el alcance del SGSI	Alcance y límites del SGSI	Documento que define en forma precisa la ubicación, la tecnología y los activos que forman parte del alcance de la implementación del SGSI
4	**Clausula 5.1** Liderazgo y compromiso y la **Cláusula 5.2** Política.	Política y objetivos de la seguridad de la información	Documento clave que establece el marco normativo para gestionar la seguridad de la información en el Instituto Geológico Minero Metalúrgico INGEMMET.
5	**Clausula 5.3** Roles, autoridad y responsabilidad organizacionales	Roles y Responsabilidades del SGSI	Documento que define la estructura organizacional para la dirección, gestión y operación de la seguridad de la información en el Instituto Geológico Minero Metalúrgico INGEMMET.
6	**Clausula 6.1** Acciones para tratar los riesgos y las oportunidades	Metodología de la Gestión de Riesgos	Documento que describe los métodos y parámetros para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información.
7	**Clausula 6.1.2** Valoración del Riesgo de Seguridad de la Información.	Cuadro de análisis y evaluación de riesgos	Documentación resultante del análisis y la evaluación de los riesgos de seguridad de la información
8		Cuadro de tratamiento de riesgos	Documentación que establece los controles de seguridad que se deben implementar para cada riesgo inaceptable
9		Informe sobre el resultado de la gestión de riesgos y el tratamiento de los riesgos	Documento que incluye los documentos generados en el proceso de gestión de riesgos.
10	**Clausula 6.1.3** Tratamiento de riesgos de seguridad de la información.	Declaración de Aplicabilidad	Documento que contiene los controles del Anexo A de la NTP ISO/IEC 27001:2014 y justifica la inclusión o exclusión de su implementación.
11		Plan de tratamiento de riesgos	Documento que especifica un plan de trabajo priorizado de los controles que deben implementarse como resultado de la gestión de riesgos. Además de especificar los otros documentos

			que requieren para evidenciar la conformidad con la NTP ISO/IEC 27001:2014.
12	**Clausula 7.3** Concientización	Plan de Concientización en Seguridad de la Información	Documento que especifica un plan de formación en seguridad de la información.
13	**Clausula 9.1** Monitoreo, medición, análisis y evaluación.	Procedimiento de medición y monitoreo del SGSI	Documento que describe el proceso para evaluar el cumplimiento de los indicadores establecidos para el SGSI.
14	**Cláusula 9.2** Auditoria interna	Procedimiento de auditoria interna	Documento que describe como se realizara la auditoria interna y se informara el resultado de la misma.
15	**Clausula 9.**3 Revisión de la gerencia.	Procedimiento de la revisión por la gerencia	Documento que describe como se realizara la revisión por la Alta Dirección para asegurar la eficacia y efectividad del SGSI.
16	**Cláusula 10.1** No conformidades y acción correctiva	Procedimiento de acciones correctivas del SGSI	Documento que describe el proceso de implementación de las acciones correctivas y preventivas, así como los formatos a emplear.

7. ORGANIZACIÓN PARA LA IMPLEMENTACIÓN DEL SGSI

Estará a cargo del equipo implementador, organizado de la siguiente manera:

7.1. **Patrocinador:** Esta función será desempeñada por el Titular del Instituto Geológico Minero Metalúrgico

7.2. **Coordinador:** Gestionará las acciones necesarias para la implementación del SGSI y realizará las coordinaciones con los directores y/o jefes de los Órganos para la adopción de las medidas aprobadas por el Comité de Gobierno Digital. Esta función será desempeñada por el Oficial de Seguridad Digital.

7.3. **Equipo de Trabajo:** Ayudará en diversos aspectos de la implementación del SGSI, a tomar decisiones sobre diversos temas que requieren un enfoque multidisciplinario y a realizar tareas preestablecidas. Está conformado por:

7.4. **Comité de Gobierno Digital:** Conformado por funcionarios del Instituto Geológico Minero Metalúrgico, según Resolución Presidencial N°076-2019-INGEMMET/PE que reconforma el Comité de Gobierno Digital del Instituto Geológico Minero Metalúrgico - INGEMMET, constituido por R.P. N°035-2019-INGEMMET/PE.

7.5. **Coordinadores de Seguridad:** estará conformado por personal que forma parte del alcance en la implementación del SGSI, quienes coordinaran con el/la Oficial de Seguridad Digital, son el Equipo de Implementación.

8. RIESGOS IDENTIFICADOS PARA LA IMPLEMENTACIÓN DEL SGSI

La implementación del SGSI contribuye al cambio de cultura organizacional en todos los niveles de la Institución.

A continuación, se detalla los principales riesgos que se pueden identificar en la implementación del SGSI y las acciones de mitigación, a fin de lograr el éxito del mismo.

Riesgos	Acciones de Mitigación
Cambio de los funcionarios de Alta Dirección	• La Alta Dirección dará continuidad a la ejecución de los planes aprobados. • La Alta Dirección establecerá una política y objetivos de Seguridad de la Información que incluya el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información. • La Alta Dirección revisará el sistema de Gestión de Seguridad de la Información a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.
Ampliación de plazos de la ejecución del Plan, al no contar con requisitos mínimos para la implementación de la NTP ISO/IEC 27001:2014.	Que el coordinador del plan cuente con las competencias técnicas para la implementación de la NTP ISO/IEC 27001:2014. Así mismo que los miembros del comité promuevan e impulsen los documentos correspondientes.
Falta de compromiso del personal del Instituto Geológico Minero Metalúrgico respecto a importancia de la seguridad de la información.	Se deben formular y llevar a cabo actividades de concientización relacionadas a seguridad de la información en el Instituto Geológico Minero Metalúrgico, las cuales deberán ser establecidas en el plan de concientización.
Ampliación de plazos en la presentación y aprobación de documentos oficiales (evidencia legal)	El coordinador de la implementación del SGSI supervisara que todas las actividades sean realizadas dentro de los plazos definidos y solicitara a tiempo la intervención del patrocinador.

9. ACCIONES PREVIAS Y PERMANENTES

9.1. Para el inicio de la implementación del SGSI

9.1.1. **Compromiso de la Alta Dirección:** con la finalidad de respaldar al equipo y las medidas aprobadas en el Comité de Gobierno Digital.

9.1.2. **Análisis de brechas de seguridad de la Información:** con la finalidad de determinar la distancia que existe entre la organización actual de la seguridad de la información y lo establecido en la NTP ISO/IEC 27001:2014.

9.1.3. **Fortalecimiento de capacidades del coordinador del plan en los siguientes temas:**

- COBIT 5 FUNDATIONS.
- ISO 27001.
- ISO 31000.
- ISO 22301

9.2. Durante la implementación del SGSI

9.2.1. **Realización de Ethical Hacking:** en intervalos de mínimo de tres meses para determinar vulnerabilidades o intrusión a los sistemas informáticos.

9.2.2. **Auditoria informática especializada:** que permita establecer indicadores de cumplimiento y de gestión.

9.2.3. **Fortalecimiento de capacidades:** de los participantes claves en los siguientes temas:

- Seguridad de la Información.
- Ethical hacking.
- Protección de datos personales

10. HERRAMIENTAS DE APOYO AL SGSI

Todos los documentos se crearán empleando herramientas ofimáticas, dado que no se cuenta con una aplicación que automatice el Sistema de Gestión de Seguridad de la Información.

Se creará una carpeta compartida en la red local donde se almacenará las actas y los documentos generados durante la implementación del SGSI. Todos los miembros del equipo tendrán acceso a esos documentos en modo lectura. Solo el coordinador de la implementación del SGSI está autorizado a editar los datos.

Se empleará la intranet como plataforma de comunicaciones para uso interno y para desplegar la concientización de seguridad de la información.

11. METODOLOGIA

Para la implementación del SGSI se empleará la metodología PDCA (Plan-Do-Check-Act), también llamada ciclo de DEMING, que impulsa al mejoramiento continuo de procesos y consiste en los siguientes pasos:

- Planear (PLAN): Reconocer una oportunidad y planificar el cambio.
- Hacer (DO): Probar el cambio.
- Verificar (CHECK): Revisar la prueba, analizar los resultados e identificar lo aprendido.
- Actuar (ACT): tomar acción basada en las lecciones aprendidas. Si el cambio fue exitoso, incorporar lo aprendido, de lo contrario intentar un plan diferente.

12. PRESUPUESTO PARA EJECUTAR

El presupuesto para la ejecución del plan de implementación del SGSI se encuentra contemplada en el Plan Operativo Institucional.

13. CRONOGRAMA DE ACTIVIDADES

Anexo N° 01 Cronograma de actividades del Plan de Implementación del SGSI INGEMMET 2021-2022

CRONOGRAMA DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI INGEMMET 2021- 2022										
FASE/OBJETIVO	ACTIVIDADES	DETALLE DE ACTIVIDADES	2021			2022				
			May-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 ó Evaluación de documentos requeridos para el Sistema de Gestión de Seguridad de la Información.	1.Procedimiento para la gestión de documentos y registros	X							
FASE II **PLANIFICACION (PLANEAR**) desarrollar las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo.	· Evaluación del alcance del sistema de Gestión de Seguridad de la información	2. reformulación del análisis de contexto y requerimiento de seguridad de las partes interesadas. 3. reformulación del alcance y límites del SGSI.	X							
	· Declaración de la política y los objetivos de seguridad de la información.	4. reformulación de la política y objetivos de seguridad de la información. 5. reformulación de los roles y responsabilidades del SGSI.		X						
	· Definición de los criterios para la evaluación y aceptación de riesgos.	6. metodología de gestión de riesgos		X						
	· Evaluación de riesgos. · Análisis entre los riesgos identificados y las medidas correctivas existentes.	7. inventario de activos de información. 8. cuadro de análisis y evaluación de riesgos. 9. Cuadro de tratamiento de riesgos. 10. informe sobre el resultado de la gestión de riesgos y el tratamiento de los riesgos.		X						
	· Desarrollo de un plan de tratamiento de riesgos · Desarrollo de la declaración de aplicabilidad · Elaboración del plan de trabajo priorizado	11. plan de tratamiento de riesgos. 12. plan de concientización en seguridad de la información. 13. declaración de aplicabilidad 14. plan de trabajo priorizado, aprobado por los propietarios de los riesgos.		X	X					
FASE III **DESPLIEGUE (HACER)** Desplegar las actividades de implementación del SGSI	· Desarrollo de documentos y registros necesarios. · Implementación de los controles seleccionados del plan de tratamiento de riesgos. · Fortalecimiento de la gestión de incidentes	15. políticas específicas para la seguridad de la información. 16. plan de tratamiento de riesgos implementado. 17. procedimiento de gestión de incidentes de seguridad de la información. 18. plan de concientización en seguridad de la Información implementado			X	X	X			
FASE IV **REVISION (VERIFICAR)** Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la NTP ISO/IEC 27001:2014.	· Monitoreo del desempeño del SGSI	19. informe de los resultados de la medición y monitoreo del SGSI. 20. Informe de la revisión de la dirección				X	X			
	· Auditoria interna del SGSI	21. programa de auditoria interna 22. informe de los resultados de la auditoria interna					X			
FASE V **CONSOLIDACION (ACTUAR)** Implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la NTP ISO/IEC 27001:2014.	· Implementación de acciones correctivas y preventivas	23. Plan de acciones correctivas y preventivas.						X	X	
	· Desarrollo, corrección y mejora de la documentación del SGSI nueva y existente	24. informe de resultados de las acciones correctivas implementadas.						X	X	
	· Desarrollo de las actividades para evidenciar la mejora continua del SGSI	25. planes de mejora continua.						X	X	

Instituto Geológico Minero y Metalúrgico - INGEMMET - Oficina de Sistemas de Información