Secretario de Directorio (e)

Firmado digitalmente por: LECAROS JIMENEZ Oscar Guillermo FAU 20103030791 hard
Motivo: Soy el autor del documento
Fecha: 27/11/2023 14:56:50-0500

Devolvemos vida al planeta

ACTIVOS MINEROS S.A.C.

T.S.D. N° 031-2023

EL SECRETARIO DEL DIRECTORIO DE LA EMPRESA ACTIVOS MINEROS S.A.C., de conformidad con el artículo 23° del Reglamento de Organización y Funciones – ROF;

CERTIFICA:

Que, en la Sesión de Directorio No Presencial Nº 523-2023-AM de fecha 24 de noviembre del año 2023, realizada bajo la Presidencia del Ing. Karl Maslo, contando con el quórum reglamentario, el Directorio adoptó el Acuerdo que corre en Acta, cuyo texto es el siguiente:

APROBACIÓN DE LA ACTUALIZACIÓN DE LAS POLÍTICAS INSTITUCIONALES DE AMSAC.

ACUERDO DE DIRECTORIO Nº 01-523-2023

VISTOS: El Resumen Ejecutivo N° 011-2023-GG de la Gerencia General, el Informe N° 008-2023-GG/OPMC de la Oficina de Planeamiento y Mejora Continua, el Informe Legal N° 099-2023-GL de la Gerencia Legal, y **OIDA** la exposición del Gerente General (e) quien hizo suyos los documentos puestos a consideración del Colegiado;

El Directorio luego de una breve deliberación y por unanimidad:

ACORDÓ:

1. Aprobar la actualización de la Política de Gestión Documental, presentada por la Administración.

2. Aprobar la Política de Innovación, presentada por la Administración.

3. Disponer su inclusión en el Compendio de Políticas Institucionales de AMSAC, versión 8, la que estará conformada por 17 Políticas para el fortalecimiento del Buen Gobierno Corporativo

   - Política de Auditoría
   - Política de Gestión Integral de Riesgos
   - Política de Cumplimiento Normativo y de Obligaciones y Compromisos
   - Política de Prevención y Solución de Conflictos
   - Política de Información y Comunicación
   - Política de Responsabilidad Social Corporativa
   - Política de Inversiones en Proyectos de Remediación Ambiental Minera
   - Política de Innovación
   - Política de Seguridad y Salud en el Trabajo, Medio Ambiente, Calidad, Antifraude y Anticorrupción
   - Política de Seguridad de la Información
   - Política de Gestión Documental

- Política de Gestión Humana
- Política Remunerativa
- Política de Participación de Agentes Externos
- Política Contable
- Política de Dividendos
- Política de Endeudamiento

4. Encargar a la Gerencia General disponer las acciones conducentes a la implementación del presente acuerdo.

5. Dispensar el presente acuerdo de la lectura y aprobación del Acta.

Lima, 27 de noviembre de 2023

FIRMADO DIGITALMENTE

Oscar Lecaros Jiménez
Secretario de Directorio (e)

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Objeto

EL objeto de la Política de Seguridad de la información es establecer los lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información.

2. Alcance

La Política de Seguridad de la Información se aplica a la totalidad de procesos de Activos Mineros (AMSAC), lo cuales son ejecutados por:

- Trabajadores de AMSAC
- Terceros con vínculo contractual con AMSAC.

3. Base Normativa

- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos 2ª. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Decreto Supremo N° 043-2003-PCM, Aprueban TUO de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- Lineamiento Corporativo: Lineamiento del Sistema de Gestión de la Seguridad de la Información, aprobado mediante Resolución de Dirección Ejecutiva N° 029-2020/DE-FONAFE de 26.abr.2020.
- 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 de 26.abr.2020.
- Resolución de Gerencia General 029-2019-AM/GG Conformación del Comité de Gobierno Digital y Designación de Oficial de Seguridad de la información de AMSAC.
- Resolución Ministerial N° 087-2019 PCM Conformación y Funciones del Comité de Gobierno Digital.

4. Glosario de Términos

- **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.

- **Amenaza:** causa de un potencial incidente no deseado, el cual puede ocasionar daño a un sistema y/o organización
- **Confidencialidad**: Principio de la seguridad de la información que busca asegurar que solo quienes estén autorizados puedan acceder a la información.
- **Controles:** Medidas o actividades adoptadas para mitigar el impacto y/o reducir la probabilidad de ocurrencia de los riesgos.
- **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.
- **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.
- **Riesgo de Seguridad de la información:** Condición que supone una posible amenaza o vulnerabilidad que pueda afectar a la seguridad de la información.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

5. Cumplimiento y conformidad

El cumplimiento de la Política de Seguridad de la Información es obligatorio. Ningún trabajador y tercero que mantenga vínculo contractual con AMSAC, está exento del cumplimiento de estas políticas. Si un individuo u organización viola las siguientes disposiciones, por negligencia o intencionalmente, AMSAC tomará las medidas correspondientes, tales como acciones administrativas, laborales, disciplinarias, legales, u otras.

Estos lineamientos de Seguridad guardan conformidad con la “NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos 2ª. Edición”.

6. Roles y Responsabilidades

Todo el personal de AMSAC es responsable de conocer, cumplir y hacer cumplir la Política de Seguridad de la Información, lineamientos, procedimientos y estándares asociados a esta y aquello específicamente relacionados con su área de competencia. Dentro de este contexto, se distinguen los siguientes niveles de responsabilidad:

a. Directorio:

- Aprobar la Política de Seguridad de la Información.
- Evaluar el cumplimiento de la Política de Seguridad de la Información.

b. Gerencia General:

- Brindar y comprometer apoyo a todo nivel para el cumplimiento de los objetivos de la gestión de seguridad de la información cautelando la confidencialidad, integridad y disponibilidad de la información.

c. Comité de Gobierno Digital:

- Revisar y proponer al Directorio las modificaciones de la Política y los documentos asociados, producto de la revisión del grado de efectividad de los controles de seguridad implementados; del análisis de cambios significativos en los riesgos que podrían afectar a los recursos de información; y del análisis del impacto de los incidentes relativos a la seguridad reportados
- Recomendar e impulsar acciones en pro de la implementación de soluciones tecnológicas, estándares y buenas prácticas cuyos propósitos cautelen la preservación de la Seguridad de la información.
- Apoyarse en la asesoría de especialistas, internos o externos, cuando sea preciso, buscando cumplir con los requisitos de la normativa vigente y optimizar resultados.

d. Oficial de Seguridad de la Información:

- Coordinar las acciones del Comité de Gobierno Digital e impulsar la implementación y cumplimiento de la Política y demás controles asociados a la NTP-ISO/IEC 27001:2014
- Supervisar permanentemente todos los aspectos inherentes a la política, asegurando que las metas de seguridad sean cubiertas, identificando y manejando los no cumplimientos, e informando al Comité de Gobierno Digital y al personal involucrado de las acciones de seguridad gestionadas.
- Definir y proponer acciones vinculadas a la protección de amenazas y reducción de riesgos de seguridad de la información ante el comité de Gobierno digital.
- Asegurar mecanismos de protección de los activos de información, sin desmedro de la responsabilidad de los trabajadores sobre la información que administran.
- Difundir la Política de Seguridad de la Información en todos sus niveles.
- Proponer acciones ante el Comité de Gobierno Digital para el cambio, mejora y/o adecuaciones de la Política de Seguridad de la Información, la documentación y actualización del análisis de riesgos e impacto de los incidentes relativos a la Seguridad de la Información.
- Proponer y hacer de conocimiento del Comité de Gobierno Digital las iniciativas y programas de acción en pro de la implementación de soluciones tecnológicas, estándares y buenas prácticas cuyos propósitos cautelen la preservación de la Seguridad de la información.

e. Gerencias y Jefaturas:

- Brindar apoyo visible en la gestión de iniciativas de seguridad de la información.
- Revisar preventivamente el cumplimiento de los controles de seguridad de sus áreas e informar al Oficial de seguridad de la información de la ocurrencia de vulnerabilidades o amenazas que pudieran afectar la seguridad de la empresa.

f. Trabajadores:

- Clasificar la información de la cual son responsables de acuerdo a su grado

de sensibilidad y criticidad; y documentar y mantener actualizada esta clasificación definiendo quienes tienen permisos de acceso por sus funciones y competencia.
- Proteger la información y recursos bajo su custodia que sean propiedad de la empresa, y hacer un uso adecuado de estos, alineado a los procedimientos establecidos para cada puesto de trabajo con la política de seguridad de la información y sus documentos asociados.

7. Lineamientos

7.1 Lineamiento de clasificación de la información

AMSAC garantiza la implementación de mecanismos de control de la información contenida en forma impresa o escrita en papel, almacenada electrónicamente, transmitida por algún medio electrónico, o de conocimiento específico del personal involucrado. Así mismo clasifica la información considerando los siguientes criterios:

- Confidencial: la que se encuentra regulada en las excepciones contenidas en el artículo 17° del Decreto Supremo N° 043-2003-PCM "Aprueban TUO de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública."
- Restringido: referido a niveles medios de confidencialidad, definidos por el propietario de la información y/o la Gerencia correspondiente.
- Uso interno: aquella información con un nivel bajo de confidencialidad, utilizada de manera ordinaria por personal de AMSAC.
- Público: la que es accesible al personal de AMSAC y de uso externo.

7.2 Lineamiento de fomento de cultura de seguridad de información

AMSAC fomenta el desarrollo de una cultura de seguridad de la información, a través de la formación de sus trabajadores en temas relacionados al impacto ante eventos e incidentes de seguridad, ataques, acciones que predispongan a un estado de vulnerabilidad, amenazas, riesgos y su tratamiento, teniendo presente los lineamientos, normativas y procedimientos de seguridad establecidas en la empresa; supervisando que se cumplan las buenas prácticas en seguridad; y realizando acciones de sensibilización para los trabajadores y personal tercero que realiza actividades dentro de su ámbito.

7.3 Lineamiento de seguridad física y ambiental

AMSAC toma acciones con el propósito de preservar la seguridad física y ambiental minimizando riesgos de daños e interferencias a la información y operaciones.

Asimismo, propone medidas para evitar incidentes que pueda menoscabar los activos físicos y de información, mediante el establecimiento de perímetros de seguridad los cuales permitan:

- Prevenir e impedir accesos no autorizados, daños e interferencia en las instalaciones e información.
- Proteger el equipamiento de procesamiento de información, así como los activos de cómputo.
- Controlar los factores ambientales que podrían perjudicar el funcionamiento del equipamiento que procesa y almacena la información de la empresa
- Salvaguardar la información y la continuidad de las operaciones.

7.4 Lineamiento de control de acceso

AMSAC implementa mecanismos de identificación y autenticación para el acceso a sus instalaciones, información, uso de sus capacidades, recursos e infraestructura, así mismo se reserva el derecho de revocar el privilegio de acceso a la información y a las tecnologías que la soportan en caso se identifique un mal uso del mismo.

7.5 Lineamiento de gestión de los incidentes de seguridad

Todo Trabajador de AMSAC, debe alertar de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en los lineamientos de seguridad de la información. El responsable inmediato superior deberá analizar cada caso, consultarlo y reportarlo al Oficial de Seguridad de la Información de manera que se adopten las medidas correspondientes para evitar su repetición.

7.6 Lineamiento para el soporte de las operaciones

AMSAC garantiza y asegura el soporte tecnológico de los procesos de la empresa, implementando soluciones ante contingencias acordes con los avances y especialización en el campo de la seguridad de la información.

AMSAC garantiza y asegura una permanente capacitación y asesorías para el personal encargado de la implementación y sostenimiento de la Seguridad de la información.

7.7 Lineamiento para la gestión de los recursos y servicios informáticos e infraestructura de red

AMSAC proporciona y asegura el aprovisionamiento de un catálogo de servicios de Tecnologías de la Información y Comunicaciones para sus operaciones, tales como: equipamiento de cómputo, impresión, internet, correo electrónico, telefonía fija y móvil, sistemas de información, licencias de software, entre otros, los cuales permiten hacer tratamiento y almacenamiento de la información de forma eficiente.

AMSAC monitorea de forma constante la infraestructura y servicios de red que presta, implementando las herramientas que le permitan detectar, prevenir y recuperarse del ataque y vulnerabilidades que puedan encontrarse en la plataforma tecnológica

AMSAC establece esquemas de mantenimiento para toda su plataforma tecnológica que deberá ser cumplido dentro de determinadas fechas programadas.

7.8 Lineamiento de continuidad de operaciones

AMSAC implementa mecanismos de disponibilidad y respaldo ante eventuales contingencias con la infraestructura de operaciones de cómputo y comunicaciones, garantizando la restauración del servicio informático en el más corto plazo posible.