Gerente de Administración y Finanzas (e)
Firmado digitalmente por: TEMPLE AGUILAR Julio Cesar FAU 20103030791 hard
Motivo: Doy V° B°
Fecha: 14/12/2023 17:38:38-0500

Devolvemos vida al planeta
Jefe de Departamento de Tecnologías de la Información y Comunicaciones
Firmado digitalmente por: PISCONTE PAREDES Nestor Eduardo FAU 20103030791 hard
Motivo: Doy V° B°
Fecha: 13/12/2023 11:35:24-0500

Especialista en Sistemas de Información
Firmado digitalmente por: HENRY WILSON TORNERO YAYA DNI:42896673 RUC:20103030791
Motivo: Doy V° B°
Fecha: 12/12/2023 15:28:10-0500

Procedimiento de Gestión de Incidentes de Seguridad de la Información

Versión	Fecha	Control de Cambios
00	12/12/2023	• Versión inicial.

Áreas Responsables	Nombres y Cargos
Elaborado: **Departamento de Tecnologías de la Información y Comunicaciones**	Henry Tornero Especialista en Sistemas de Información
Revisado: **Departamento de Tecnologías de la Información y Comunicaciones**	Néstor Pisconte Jefe de Departamento de Tecnología de la Información y Comunicaciones
Homologado: **Oficina de Planeamiento y Mejora Continua**	Deymer Barturén Especialista de Calidad y Mejora de Procesos Miguel Tito Jefe de Oficina de Planeamiento y Mejora Continua
Aprobado: **Gerencia de Administración y Finanzas**	Julio Temple Gerente de Administración y Finanzas (e)

Este documento es propiedad de Activos Mineros S.A.C. Queda prohibida su reproducción sin su autorización escrita. Es una copia auténtica imprimible de un documento electrónico emitido por Activos Mineros S.A.C. Es responsabilidad del usuario asegurarse que corresponde a la versión vigente publicada en la red interna y/o página web institucional.

Jefe de la Oficina de Planeamiento y Mejora Continua
Firmado digitalmente por: TITO ASCUE Miguel Armando FAU 20103030791 hard
Motivo: Doy V° B°
Fecha: 15/12/2023 11:21:22-0500

Especialista en Calidad y Mejora de Procesos
Firmado digitalmente por: BARTUREN HUAMAN Deymer Frank FAU 20103030791 hard
Motivo: Doy V° B°
Fecha: 13/12/2023 11:53:59-0500

INDICE

I. OBJETIVO

Establecer las disposiciones y acciones para reportar, atender y responder ante un incidente de seguridad de la información de Activos Mineros S.A.C. (en adelante AMSAC), con la finalidad de minimizar la pérdida de información e interrupción de servicios.

II. ALCANCE

El presente documento aplica a todos los incidentes de seguridad de la información detectados por los usuarios de los activos de información.

III. DOCUMENTOS DE REFERENCIA

- Lineamiento Corporativo: "Lineamiento del Sistema de Gestión de la Seguridad de la Información" de FONAFE.
- Manual Corporativo: "Manual Metodológico para la Implementación del Sistema de Gestión de Seguridad de la Información" de FONAFE.
- NTP ISO/IEC 27001:2022 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 3ra. Edición.
- Política de Seguridad de la Información de AMSAC.

IV. VIGENCIA

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

V. CONTENIDO

1. DEFINICIONES / CONSIDERACIONES

- **Usuario:** Cualquier colaborador de AMSAC que tenga acceso a la infraestructura tecnológica o sistemas de información.
- **Evento:** Ocurrencia identificada de un sistema, servicio o red que indica una posible ruptura de la seguridad de la información, de la política o una falla en los controles de la información, o una situación desconocida que puede ser relevante para la seguridad de AMSAC.
- **Incidente:** Evento o conjunto de eventos de seguridad, indeseados o inesperados, que tienen la probabilidad significativa de comprometer la confidencialidad, disponibilidad e integridad de la información, así como las operaciones de la empresa.
- **Mesa de ayuda:** Punto de contacto inicial para realizar el reporte o notificación de posibles incidentes de seguridad de la información.

2. DISPOSICIONES GENERALES

2.1. El Jefe de Departamento de Tecnologías de Información y Comunicaciones, como Oficial de Seguridad de la Información y dueño del proceso, es responsable de que el proceso de Gestión de Incidentes de Seguridad de la Información se efectúe cumpliendo los plazos y las disposiciones previstas en la normativa legal aplicable, los lineamientos de FONAFE y en el presente procedimiento.

2.2. El Departamento de Tecnologías de Información y Comunicaciones brindará la capacitación y el soporte a las áreas usuarias para el reporte de incidentes de seguridad de la información que puedan presentarse.

2.3. Todos los colaboradores de la empresa deben estar capacitados y preparados para reportar cualquier incidente de seguridad de la información que detecte.

3. DESCRIPCIÓN

Ejecutor	Actividad
Áreas Usuarias	1. Reporta cualquier incidente de seguridad de la información que detecte a través del sistema de gestión de incidentes, detallando lo siguiente: • Asunto del incidente • Descripción del incidente, incluyendo cómo se detectó y activos de información afectados. • Fecha y hora del incidente o del reporte. • Datos de la persona que reporta: nombres y apellidos, cargo, ubicación.
Soporte Técnico de TIC	2. Valida si se trata de un incidente de seguridad de la información, así como la categoría y criticidad del incidente considerando los Anexos N° 1 y 2. De ser necesario, requiere al usuario mayor información. Si no es un incidente de seguridad de la información, lo reclasifica para su atención correspondiente; en caso contrario, continúa el proceso.
	3. Identifica a los involucrados en el incidente y determina los activos de información afectados.
Especialista en Sistemas de Información	4. Define el plan de acciones de contención ante el incidente, en coordinación con el Jefe de TIC, y procede a su ejecución.
	5. Analiza los activos de información afectados. Puede realizarlo personal de AMSAC o subcontratar a un tercero.
	6. Evalúa las vulnerabilidades explotadas. Puede realizarlo personal de AMSAC o subcontratar a un tercero.
	7. Determina la causa raíz del incidente, a fin de prevenir la recurrencia del incidente.
	8. Define el plan de acciones correctivas para eliminar la causa raíz, en coordinación con el Jefe de TIC, incluyendo acciones de recuperación de los sistemas de información de ser necesario, y procede a su ejecución.
	9. Realiza el cierre del incidente y comunica al personal que lo reportó el resultado de la gestión realizada ante el incidente.
	10. De ser necesario, revisa y actualiza el análisis de riesgos y controles de seguridad de la información a los activos de información, en caso de que el incidente provenga de una amenaza no identificada o no tratada.
	11. Revisa periódicamente la información sobre los incidentes de seguridad de la información y las respuestas a ellos, e identifica posibles lecciones aprendidas, tendencias, patrones y oportunidades de mejora.
	12. Genera lecciones aprendidas a partir de los incidentes registrados, en coordinación con el Jefe de TIC, y las comunica a los colaboradores, con el soporte del área de Imagen Corporativa, según se requiera.
	13. Realizar acciones de mejora en la gestión de incidentes de seguridad de la información, según corresponda, en coordinación con el Jefe de TIC.

4. ALCANCES FUNCIONALES

4.1. Gerente de Administración y Finanzas

- Aprobar el presente procedimiento.

4.2. Jefe del Departamento de Tecnología de la Información y Comunicaciones, en su rol de Oficial de Seguridad de la Información

- Conducir el proceso de Gestión de Incidentes de Seguridad de la Información, cumpliendo los plazos y las disposiciones previstas en los lineamientos de FONAFE, la normativa legal aplicable y el presente procedimiento.
- Velar por el cumplimiento del presente procedimiento.
- Velar porque el procedimiento se mantenga vigente, siendo responsable de realizar revisiones y actualizaciones periódicas.

4.3. **Especialista en Sistemas de Información**

- Coordinar la ejecución de las actividades del proceso de Gestión de Incidentes de Seguridad de la Información, cumpliendo los plazos y las disposiciones previstas en los lineamientos de FONAFE, la normativa legal aplicable y en el presente procedimiento.
- Brindar la capacitación y el soporte a las áreas usuarias para la detección y reporte de incidentes de seguridad de la información.
- Evaluar, dar respuesta, efectuar el cierre, aprendizaje y mejora continua en la gestión de los incidentes de seguridad de la información.

4.4. **Áreas Usuarias**

- Reportar cualquier incidente de seguridad de la información que detecte.

5. REGISTROS / ANEXOS

- Sistema de Gestión de Incidentes.
- Anexo 1: Categorías y subcategorías de incidentes de seguridad de la información.
- Anexo 2: Nivel de criticidad de incidentes de seguridad de la información.

Anexo 1: Categorías y subcategorías de incidentes de seguridad de la información

Categoría	Subcategoría
Modificación de recurso no autorizado	Borrado de información
	Modificación de información
	Modificación, instalación o eliminación no autorizada de software
Uso inapropiado de recursos	Fuga de información
	Mal uso y abuso de los servicios tecnológicos (correo, internet, intranet)
	Pérdida de información
Código malicioso	Virus informático
	Ransoware
	Malware
Fraude	Phishing
	Suplantación

Anexo 2: Nivel de criticidad de incidentes de seguridad de la información

Nivel de Criticidad	Descripción	Ejemplos
Baja	Incidente que afecta a activos y servicios no críticos y/o pueden provocar un daño leve.	Incidente reportado con anterioridad y cuya solución se conoce. Acceso y/o divulgación de material de tipo social, comercial o que no esté autorizado por AMSAC.
Media	Incidente que afecta parcialmente a los activos y operaciones.	Compartir información sin autorización. Acceso y/o divulgación de material con contenido que atenta con la moral y las buenas costumbres.
Alta	Incidente que afecta seriamente a los activos y operaciones.	Cambios a los sistemas, hardware y/o software sin autorización. Descarga y/o uso de software no autorizado. Mal uso de los activos, información y/o recursos de la empresa.
Muy Alta	Interrupción prolongada del servicio. Impacto en varias funciones o áreas de la empresa. Afecta a uno o más sistemas críticos.	La información confidencial está gravemente comprometida. Se afecta a un considerable número de empleados o sistemas. Acceso no autorizado accidental o malicioso a los sistemas de información o de almacenamiento.