# Procedimiento de Gestión de Incidentes de Seguridad de la Información

| Versión | Fecha | Control de Cambios |
|---|---|---|
| 01 | 30/09/2025 | • Se actualizaron las disposiciones, actividades y alcances funcionales del procedimiento para incorporar la participación del Oficial de Seguridad y Confianza Digital y el Equipo de Respuesta ante Incidentes.<br>• Se incorporó en documentos de referencia el Reglamento de la Ley de Gobierno Digital y la Norma ISO/IEC 27035 sobre Gestión de Incidentes de Seguridad de la Información. |

| Áreas Responsables | Nombres y Cargos |
|---|---|
| **Elaborado:**<br>**Departamento de Tecnologías de la Información y Comunicaciones** | Erik Prado<br>Especialista en Redes y Comunicaciones |
| **Revisado:**<br>**Departamento de Tecnologías de la Información y Comunicaciones** | Moisés Palomino<br>Jefe de Departamento de Tecnología de la Información y Comunicaciones |
| **Homologado:**<br>**Oficina de Planeamiento y Mejora Continua** | Deymer Barturén<br>Jefe de Oficina de Planeamiento y Mejora Continua (d) y Especialista de Calidad y Mejora de Procesos |
| **Aprobado:**<br>**Gerencia de Administración y Finanzas** | Julio Temple<br>Gerente de Administración y Finanzas |

## INDICE

## I. OBJETIVO

Establecer las disposiciones y acciones para la planificación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas ante un evento o 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

- Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento de la Ley de Gobierno Digital. Capítulo III – Equipo de respuestas ante incidentes de seguridad digital. Artículo 104.
- Lineamiento del Sistema de Gestión de la Seguridad de la Información, de FONAFE.
- Manual Metodológico para la Implementación del Sistema de Gestión de Seguridad de la Información, de FONAFE.
- Norma ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.
- Norma ISO/IEC 27035 Gestión de Incidentes de Seguridad de la Información.
- Política de Seguridad, Salud en el Trabajo, Medio Ambiente, Calidad, Integridad, Anticorrupción y 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, derogándose su precedente Versión 00 de fecha 12.dic.2023.

## V. CONTENIDO

### 1. DEFINICIONES / CONSIDERACIONES

- **Equipo de respuesta ante incidentes:** Grupo especializado encargado de gestionar y mitigar incidentes de seguridad de la información dentro de una organización.
- **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.
- **Oficial de seguridad y confianza digital:** Responsable de liderar la estrategia de seguridad de la información y ciberseguridad en una organización, asegurando la protección de los activos digitales y el cumplimiento normativo. Sus funciones incluyen la gestión de riesgos, la implementación de controles de seguridad, la supervisión y respuesta ante incidentes de seguridad, y la promoción de una cultura de seguridad.
- **Usuario:** Cualquier colaborador de AMSAC que tenga acceso a la infraestructura tecnológica o sistemas de información.

### 2. DISPOSICIONES GENERALES

2.1. El Jefe de Departamento de Tecnologías de Información y Comunicaciones, como Oficial de Seguridad y Confianza Digital, 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. La Gestión de Incidentes de Seguridad de la Información comprende la planificación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas para evitar la reiteración en la ocurrencia futura de incidentes de seguridad de la información.

2.3. El Equipo de Respuesta ante Incidentes (ERI) será el encargado de recibir, analizar, registrar, gestionar y coordinar la respuesta a los incidentes de seguridad de la información, asegurando que se apliquen las medidas correctivas necesarias para minimizar su impacto en la organización.

2.4. El ERI debe garantizar la trazabilidad de la gestión de incidentes a través del formato S3.3.P1, registrando cada evento e incidente, desde su detección hasta su resolución, incluyendo evidencias, acciones correctivas y lecciones aprendidas.

2.5. El ERI debe coordinar con las áreas involucradas dentro de la organización y, cuando sea necesario, con entidades externas, como organismos reguladores y proveedores de tecnología, para asegurar una respuesta efectiva ante incidentes.

2.6. El ERI debe garantizar la confidencialidad, integridad y disponibilidad de la información relacionada con la gestión de incidentes, asegurando que solo el personal autorizado tenga acceso a los detalles y registros de los incidentes tratados.

2.7. El Departamento de Tecnología de la Información y Comunicaciones debe brindar capacitación y asistencia que requieran los usuarios o áreas usuarias de la empresa para detectar y reportar cualquier incidente de seguridad de la información.

## 3. PROCEDIMIENTO

| Ejecutor | Actividad |
|---|---|
| **Oficial de Seguridad y Confianza Digital** | **Planificación:**<br>1. Establece un equipo de respuesta ante incidentes capacitado que brindará apoyo y proporcionará soluciones ante cualquier evento o incidente que pudiera afectar la seguridad de la información.<br><br>Los equipos de respuesta ante incidentes se pueden apoyar en terceros. |
| **Usuario o áreas usuarias (trabajador de la empresa, proveedor u otro)** | **Detección:**<br>2. Reporta cualquier incidente de seguridad de la información que detecte al correo electrónico del Equipo de Respuesta Ante Incidentes con copia al Oficial de Seguridad y Confianza Digital, indicando lo siguiente:<br>• Datos del usuario (nombres y apellidos y cargo).<br>• Descripción del incidente (qué ocurrió, cuándo, cómo, quién lo originó y por qué sucedió, de ser posible). |
| **Equipo de Respuesta ante Incidentes** | **Análisis:**<br>3. Evalúa el incidente de seguridad de la información y su causa raíz.<br><br>Se evalúa más de una causa raíz que pudo haber originado el incidente. |
| | 4. Clasifica los incidentes según la categoría y subcategoría establecida en el “Registro de incidentes de seguridad de la información”. |
| | 5. Evalúa la criticidad que tiene el incidente sobre AMSAC: baja, media, alta y muy alta. |
| | 6. Designa al personal encargado de resolver el incidente, que puede ser alguien dentro del equipo de respuesta ante incidentes o de otra área en caso se requiera. |
| | **Contención:**<br>7. Planifica las acciones de contención del incidente para evitar su propagación, incluyendo plazos. |

| Ejecutor | Actividad |
|---|---|
| | 8. Difunde y asigna las acciones de contención del incidente, así como brinda la orientación necesaria. |
| | 9. Ejecuta las acciones de contención del incidente dentro de los plazos previstos. |
| | 10. Valida que las acciones de contención hayan sido eficaces. |
| | **Erradicación:**<br>11. Planifica las acciones de erradicación del incidente, incluyendo plazos. |
| | 12. Difunde y asigna las acciones de erradicación del incidente, así como brinda la orientación necesaria. |
| | 13. Ejecuta las acciones de erradicación del incidente dentro de los plazos previstos. |
| | 14. Valida que las acciones de erradicación hayan sido eficaces. |
| | **Recuperación:**<br>15. Planifica las acciones de recuperación de los activos de información afectados, incluyendo plazos. |
| | 16. Difunde y asigna las actividades de recuperación de los activos de información, así como brinda la orientación necesaria. |
| | 17. Ejecuta las acciones de recuperación de los activos de información dentro de los plazos planificados. |
| | 18. Valida que las acciones de recuperación hayan sido eficaces. |
| **Oficial de Seguridad y Confianza Digital** | 19. Emite un informe con el detalle de los incidentes de seguridad de la información y eventos detectados y remediados. |
| **Equipo de Respuesta ante Incidentes** | **Lecciones aprendidas:**<br>20. Determina lecciones aprendidas a partir de los informes y registros de los incidentes de seguridad de la información ocurridos, para que se tomen en cuenta ante la ocurrencia de un incidente similar. |

## 4. ALCANCES FUNCIONALES

### 4.1. Gerente de Administración y Finanzas

- Aprobar el presente procedimiento.

### 4.2. Oficial de Seguridad y Confianza Digital

- Conducir el proceso de la Gestión de Incidentes de Seguridad de la Información, cumpliendo los plazos y las disposiciones establecidas en la normativa legal aplicable, los lineamientos de FONAFE 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, así como de la difusión y conocimiento del mismo por parte del equipo de trabajo y áreas vinculadas.
- Brindar capacitación y asistencia a los usuarios o áreas usuarias para la detección y reporte de incidentes de seguridad de la información.

### 4.3. Equipo de Respuesta ante Incidentes

- Identificar, clasificar y priorizar incidentes de seguridad que afecten a los activos de información, basándose en su gravedad e impacto potencial en las operaciones de la empresa.

- Evaluar, dar respuesta, efectuar el cierre, lecciones aprendidas y mejora continua en la gestión de los incidentes de seguridad de la información.
- Identificar oportunidades de actualización del presente procedimiento.

4.4. **Usuarios o Áreas usuarias**

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

## 5. REGISTROS / ANEXOS

- Formato S3.3.P1 Registro de Incidentes de Seguridad de la Información.