



Especialista de Redes y Comunicaciones

Firmado digitalmente por:
ERIK ALONSO PRADO VIERA
DNI:46766148 RUC:20103030791
Motivo: Soy el autor del documento
Fecha: 22/09/2026 16:44:31-0500



Jefe de la Oficina de Planeamiento y Mejora Continua

Firmado digitalmente por:
MIGUEL ARMANDO TITO ASCUE
DNI:42253863 RUC:20103030791
Motivo: Doy V° B°
Fecha: 23/09/2026 15:06:25-0500



Gerente de Administración y Finanzas

Firmado digitalmente por:
JULIO CESAR TEMPLE
AGUILAR DNI:42302432
RUC:20103030791
Motivo: Doy V° B°
Fecha: 23/09/2026 13:36:24-0500



Devolvemos vida al planeta

Procedimiento para la Identificación y Análisis de Ciberamenazas

Procedimiento

Código: S3.3.P3
Versión: 01
Fecha: 22/09/2026

Procedimiento para la Identificación y Análisis de Ciberamenazas

Versión	Fecha	Control de cambios
01	22/09/2026	Numeral 4 - Se adiciona la Gestión de Análisis e Inteligencia de Amenazas: fuentes, frecuencia, análisis, evaluación de impacto, registro, reporte y evidencias.

Áreas Responsables	Nombre y cargo
Elaborado: Departamento de Tecnología de Información y Comunicaciones	Erik Prado Especialista en Redes y Comunicaciones
Revisado: Departamento de Tecnología de Información y Comunicaciones	Moisés Palomino Jefe del Departamento de Tecnología de Información y Comunicaciones
Homologado: Oficina de Planeamiento y Mejora Continua	Deymer Barturén Especialista en Calidad y Mejora de Procesos Miguel Tito Jefe de la Oficina de Planeamiento y Mejora Continua
Aprobado: Gerencia de Administración y Finanzas	Julio Temple Gerente de Administración y Finanzas

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 del departamento de Tecnologías de la Información y Comunicaciones

Firmado digitalmente por:
PALOMINO SUAREZ Moises
Reynaldo FAU 20103030791 hard
Motivo: En señal de conformidad
Fecha: 23/09/2026 08:45:09-0500



Especialista en Calidad y Mejora de Procesos

Firmado digitalmente por:
DEYMER FRANK BARTUREN
HUAMAN DNI:40658546
RUC:20103030791
Motivo: Doy V° B°
Fecha: 22/09/2026 15:21:24-0500

	Procedimiento para la Identificación y Análisis de Ciberamenazas Procedimiento	Código: S3.3.P3 Versión: 01 Fecha: 22/09/2026
---	--	--

INDICE

I.	OBJETIVO.....	3
II.	ALCANCE	3
III.	DOCUMENTOS DE REFERENCIA.....	3
IV.	VIGENCIA	3
V.	CONTENIDO.....	3
1.	DEFINICIONES / CONSIDERACIONES	3
2.	DISPOSICIONES GENERALES	4
3.	DESCRIPCIÓN	4
4.	ALCANCES FUNCIONALES.....	6
5.	REGISTROS / ANEXOS.....	7

	Procedimiento para la Identificación y Análisis de Ciberamenazas Procedimiento	Código: S3.3.P3 Versión: 01 Fecha: 22/09/2026
---	--	--

I. OBJETIVO

Establecer un procedimiento preventivo y proactivo para la identificación, análisis y gestión de ciberamenazas que puedan afectar los activos de información de Activos Mineros S.A.C. (en adelante AMSAC), con la finalidad de anticipar y mitigar riesgos antes de que se conviertan en incidentes de seguridad, permitiendo una defensa eficaz de los activos de información.

II. ALCANCE

Este procedimiento aplica a todos los activos de información, redes, sistemas y servicios tecnológicos de AMSAC, incluyendo los administrados por proveedores externos. Se enfoca en la detección temprana y el análisis de amenazas potenciales mediante monitoreo continuo y evaluación de inteligencia de amenazas.

III. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.
- Política de Seguridad, Salud en el Trabajo, Medio Ambiente, Calidad, Integridad, Anticorrupción y Seguridad de la Información de AMSAC.
- E2.3.M1 Metodología para la Gestión Integral de Riesgos, sección de riesgos de seguridad de la información.
- S3.3.P1 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

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 30/09/2025.

V. CONTENIDO

1. DEFINICIONES / CONSIDERACIONES

- **Activo de Información:** Es todo aquello que es o contiene información de valor para la empresa y, por tanto, requiere protección. Los activos de información están sujetos a muchos tipos de amenazas que pueden explotar sus vulnerabilidades. Se debe tener en cuenta que parte de los activos de información son aquellos que por regulación corresponde incorporarlos como información o contenedores de información de valor para la empresa, como, por ejemplo, datos personales, tecnologías digitales, servicios digitales y contenidos.
- **Amenaza:** Es una causa potencial no deseada que daña o puede resultar en daño al sistema, a la empresa o a sus activos. Una amenaza puede ser accidental o intencional.
- **Análisis y evaluación de riesgos:** Es el proceso por el cual los activos de información son analizados para determinar las vulnerabilidades que poseen y las amenazas a las que están expuestos, valorando el nivel de riesgo de que las amenazas exploten las vulnerabilidades.
- **Ciberseguridad:** Es una práctica que garantiza la protección de los activos digitales que interactúan con el ciberespacio mediante la prevención, detección, respuesta y recuperación ante incidentes de seguridad que afecten su disponibilidad, confidencialidad o integridad.
- **Ciberespacio:** Entorno complejo resultante de la interacción de personas, software y servicios en Internet por medio de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física.
- **Confidencialidad:** Principio de la seguridad de la información que busca asegurar que solo quienes estén autorizados puedan acceder a la información.

	Procedimiento para la Identificación y Análisis de Ciberamenazas Procedimiento	Código: S3.3.P3 Versión: 01 Fecha: 22/09/2026
---	--	--

- **Control:** Es un mecanismo que sirve para fortalecer la seguridad de aquel activo de información que es valioso para la empresa.
 - **Control correctivo:** Es un control que corrige total o parcialmente el impacto de una amenaza.
 - **Control detectivo:** Es un control que detecta la ocurrencia de una amenaza. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
 - **Control preventivo:** Es un control que está involucrado dentro de los procesos y tiene como propósito evitar la ocurrencia y frecuencia de una amenaza.
- **Fuente de amenaza:** Es el elemento o conjunto de elementos que tienen el potencial de aumentar la posibilidad de ocurrencia de una amenaza.
- **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.
- **Impacto:** Es el nivel de afectación de la empresa o sus procesos, respecto de los distintos factores relevantes con que cuenta.
- **Integridad:** Principio de la seguridad de la información que busca asegurar que la información y sus métodos sean exactos y completos.
- **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.
- **Plan de tratamiento:** Son acciones planificadas que una vez hayan sido implementadas serán controles para hacer tratamiento a los riesgos.
- **Privacidad de los datos personales:** Son aquellos datos personales cuya titularidad corresponde a una persona natural o persona jurídica de derecho privado, en cuanto esta información no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.
- **Probabilidad:** Es la medida de certidumbre asociada a un suceso o evento futuro.
- **Riesgo:** Es un potencial daño o perjuicio para una empresa; que genera incertidumbre sobre el alcance de los objetivos de la empresa.
- **Riesgo de seguridad de la información:** Es la probabilidad que una amenaza logre concretarse aprovechando una vulnerabilidad y generando un impacto en el acceso o disponibilidad de la información de la empresa que impide o retarda el logro de los objetivos de la empresa.

2. DISPOSICIONES GENERALES

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

3. DESCRIPCIÓN

	Procedimiento para la Identificación y Análisis de Ciberamenazas Procedimiento	Código: S3.3.P3 Versión: 01 Fecha: 22/09/2026
---	--	--

Ejecutor	Actividad
Identificación Proactiva de Ciberamenazas	
Usuarios o áreas usuarias	1. Reportan actividades sospechosas o intentos de ataque.
Especialista de Sistemas de Información	2. Coordina la recopilación y análisis de inteligencia de amenazas. 3. Consulta bases de datos de inteligencia de amenazas (MITRE ATT&CK, CIS, FIRST, proveedores de seguridad). 4. Evalúa registros de actividad sospechosa en aplicaciones y bases de datos.
Especialista de Redes y Comunicaciones	5. Monitorea eventos en firewalls, SIEM, sistemas IDS/IPS y reportes de proveedores.
Análisis Preventivo de Ciberamenazas	
Especialista de Sistemas de Información	6. Ejecuta pruebas de seguridad en aplicaciones (SAST, DAST).
Especialista de Redes y Comunicaciones	7. Analiza los logs de tráfico de la red y correlaciona los eventos sospechosos. 8. Comunica al Especialista de Sistemas de Información de más ciberamenazas identificadas.
Especialista de Sistemas de Información	9. Evalúa el impacto y probabilidad de las ciberamenazas y vulnerabilidades identificadas. 10. Determina y evalúa el riesgo de ciberamenazas según la E2.3.M1 Metodología para la Gestión Integral de Riesgos, en lo correspondiente a riesgos de seguridad de la información. 11. Determina controles aplicables al riesgo.
Jefe del Departamento de Tecnología de la Información y Comunicaciones	12. Valida la evaluación de amenazas y riesgos, el plan de tratamiento y las acciones correctivas necesarias.
Medidas Preventivas y Mitigación	
Especialista de Redes y Comunicaciones	13. Coordina la aplicación de reglas de mitigación en firewalls y SIEM.
Especialista de Sistemas de Información	14. Supervisa la aplicación de parches y actualizaciones de seguridad. 15. Refuerza controles de acceso y corrige configuraciones inseguras en aplicaciones. 16. Documenta la amenaza en el S3.3.P3.F1 Registro de Identificación de Ciberamenazas .
Jefe del Departamento de Tecnología de la Información y Comunicaciones	17. Valida el S3.3.P3.F1 Registro de Identificación de Ciberamenazas y pone en conocimiento al Gerente de Administración y Finanzas si es necesario.
Reporte y Seguimiento	
Especialista de Sistemas de Información	18. Genera el S3.3.P3.F2 Reporte de Ciberamenazas y Acciones Correctivas .
Especialista de Redes y Comunicaciones	19. Mantiene un monitoreo reforzado en los activos de información que podrían ser afectados.
Especialista de Sistemas de Información	20. Revisa periódicamente las amenazas registradas para detectar patrones o tendencias.
Jefe del Departamento de	21. Valida el informe final y aplica el S3.3.P1 Procedimiento de Gestión de Incidentes de Seguridad de la Información si la amenaza escala.

	Procedimiento para la Identificación y Análisis de Ciberamenazas Procedimiento	Código: S3.3.P3 Versión: 01 Fecha: 22/09/2026
---	--	---

Ejecutor	Actividad
Tecnología de la Información y Comunicaciones	

4. Gestión de Inteligencia y Análisis de Ciberamenazas

4.1. Fuentes de Inteligencia:

Se deben revisar las siguientes fuentes:

1. Reportes CNSD (PCM)
2. Reportes Cato Networks
3. Microsoft Security (Threat Intelligence)
4. SIEM AMSAC

4.2. Frecuencia:

- Semanal: Recopilación y análisis
- Mensual: Reporte consolidado

4.3. Procedimiento:

4.3.1 Recopilación

- Acceder a cada fuente definida
 - Descargar o registrar información relevante

4.3.2 Análisis

- Identificar:
 - Tipos de amenazas
 - Vulnerabilidades asociadas
 - Tendencias
- Evaluar aplicabilidad a AMSAC

4.3.3 Evaluación de impacto

- Clasificar impacto:
 - Alto / Medio / Bajo
- Determinar sistemas afectados

4.3.4 Registro

- Almacenar evidencias en SharePoint:
 - Carpeta: ISO 27001 / A.5.7 Inteligencia de Amenazas

4.3.5 Reporte mensual

- Consolidar información relevante
 - Incluir:
 1. Resumen ejecutivo
 2. Top amenazas
 3. Impacto
 4. Recomendaciones

4.4. Evidencias:

- Reportes descargados
- Registro semana
- Reporte mensual
- Carpeta SharePoint

5. ALCANCES FUNCIONALES

5.1. Gerente de Administración y Finanzas

- Aprobar el presente procedimiento.

	Procedimiento para la Identificación y Análisis de Ciberamenazas Procedimiento	Código: S3.3.P3 Versión: 01 Fecha: 22/09/2026
---	---	--

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

- Conducir el proceso de Identificación y Análisis de Ciberamenazas, 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.
- Aprobar reportes de amenazas y coordinar acciones preventivas.

5.3. Especialista en Sistemas de Información

- Coordinar la identificación de ciberamenazas y evaluar su impacto.
- Gestionar inteligencia de ciberamenazas.
- Implementar medidas preventivas de seguridad en aplicaciones y servicios.
- Identificar oportunidades de actualización del presente procedimiento.

5.4. Especialista de Redes y Comunicaciones

- Analizar tráfico sospechoso, gestionar firewalls y aplicar o gestionar la aplicación de controles de mitigación.
- Identificar oportunidades de actualización del presente procedimiento.

5.5. Usuarios y Áreas usuarias

- Reportar actividades sospechosas y colaborar con el monitoreo de ciberamenazas.

6. REGISTROS / ANEXOS

- Formato S3.3.P3.F1 Registro de Identificación de Ciberamenazas.
- Formato S3.3.P3.F2 Reporte de Ciberamenazas y Acciones Correctivas.