

 Devolvemos vida al planeta	Procedimiento de Gestión y Monitoreo de Logs Procedimiento	Código: S3.3.P4 Versión: 00 Fecha: 22/09/2026
---	--	---

Procedimiento de Gestión y Monitoreo de Logs

Versión	Fecha	Control de Cambios
00	22/09/2026	• Versión inicial.

Áreas Responsables	Nombres y Cargos
Elaborado: Departamento de Tecnologías de la Información y Comunicaciones	Erik Prado Especialista en Redes y Comunicaciones
Revisado: Departamento de Tecnologías de la Información y Comunicaciones	Moisés Palomino 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

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.

	Procedimiento de Gestión y Monitoreo de Logs Procedimiento	Código: S3.3.P4 Versión: 00 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.	DESCRIPCION	4
4.	ALCANCES FUNCIONALES	6
5.	REGISTROS / ANEXOS	7

	Procedimiento de Gestión y Monitoreo de Logs Procedimiento	Código: S3.3.P4 Versión: 00 Fecha: 22/09/2026
---	---	--

I. OBJETIVO

Establecer las actividades, controles operativos y lineamientos técnicos para la generación, almacenamiento, protección, retención y revisión periódica de los registros de eventos (logs) de los sistemas de información e infraestructura tecnológica de Activos Mineros S.A.C. (AMSAC), con la finalidad de garantizar la trazabilidad, facilitar la detección de anomalías y respaldar la investigación de incidentes de seguridad de la información, en cumplimiento del control 8.15 de la norma ISO/IEC 27002.

II. ALCANCE

El presente procedimiento aplica a todos los activos de información críticos (hardware, software, servicios en la nube y redes) listados y clasificados formalmente en la Matriz de Activos de Información del DTIC vigente de AMSAC.

III. DOCUMENTOS DE REFERENCIA

- Ley N° 29733, Ley de protección de Datos Personales y modificatorias.
- Política de Seguridad, Salud en el Trabajo, Medio Ambiente, Calidad, Integridad, Anticorrupción y Seguridad de la Información de AMSAC.
- Directiva S3.1.DR1 Uso de los Servicios y Recursos de Tecnología de la Información y Comunicaciones.
- Código de Ética y Conducta de AMSAC.
- Norma Técnica Peruana NTP-ISO/IEC 27001 — Sistemas de gestión de seguridad de la información - Requisitos.
- Norma Técnica Peruana NTP-ISO/IEC 27002, control 8.15 sobre registros de eventos.
- Matriz de Activos de Información del DTIC vigente 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

- 1.1. Log (Registro de Evento):** Archivo o registro de base de datos que contiene información detallada sobre eventos ocurridos en un sistema operativo, aplicación, servidor o equipo de red.
- 1.2. Evento Crítico:** Acción o suceso en los sistemas de información que puede impactar la confidencialidad, integridad o disponibilidad de los activos (ej. inicios de sesión fallidos, escalamiento de privilegios).
- 1.3. NTP (Network Time Protocol):** Protocolo de red diseñado para sincronizar los relojes de los equipos informáticos a través de una red de datos.
- 1.4. Custodio de Activo:** Persona responsable de la gestión operativa, mantenimiento y salvaguarda de un activo de información, conforme se detalla en la Matriz de Activos de Información del DTIC de AMSAC.
- 1.5. Retención en Línea (Hot Storage):** Almacenamiento de logs de rápido acceso en plataformas nativas para consultas inmediatas (mínimo 90 días).

	Procedimiento de Gestión y Monitoreo de Logs Procedimiento	Código: S3.3.P4 Versión: 00 Fecha: 22/09/2026
---	---	--

1.6.Retención Histórica (Cold Storage): Almacenamiento a largo plazo de los logs exportados para cumplir con requisitos de auditoría o forenses (1 año).

2. DISPOSICIONES GENERALES

- 2.1. El Jefe del Departamento de Tecnologías de la Información y Comunicaciones, como dueño del proceso, es responsable de que la gestión de logs cumpla las disposiciones establecidas en las políticas, directivas y procedimientos internos, así como la normativa aplicable.
- 2.2. Todos los componentes de infraestructura y software inventariados como críticos deben tener habilitada la generación obligatoria de registros de auditoría.
- 2.3. La identificación del alcance de los sistemas a auditar se alinea de forma estricta con los custodios designados en la **Matriz de Activos de Información del DTIC**.
- 2.4. Los administradores de sistemas y redes no deben tener permisos de modificación o eliminación sobre los repositorios donde se centralizan los logs históricos, asegurando el principio de segregación de funciones.
- 2.5. La zona horaria estándar configurada en todos los componentes de AMSAC para el registro de eventos es **UTC -5 (Lima, Perú)**.

3. DESCRIPCION

3.1. Sincronización de Relojes

Ejecutor	Actividad
Especialista de Redes y Comunicaciones	1. Configurar los Controladores de Dominio principales según la Matriz de activos de información del DTIC, para que sincronicen su hora automáticamente con un servidor de hora confiable de Internet (ej. time.windows.com). 2. Configurar todas las estaciones de trabajo y servidores miembros del dominio para sincronizar su hora con el Controlador de Dominio. 3. Configurar los equipos de red y firewalls para sincronizar la hora directamente mediante protocolo NTP hacia un servidor de estrato superior confiable, estableciendo la zona horaria UTC -5.

3.2. Configuración y Generación de Registros Críticos

Ejecutor	Actividad
Especialista de Sistemas de Información	1. Capa de Aplicación: Habilitar el registro de eventos vinculados a la creación de usuarios, cambios de perfiles y fallas críticas, abarcando exclusivamente los sistemas internos que se encuentren bajo su custodia según la Matriz de Activos de Información del DTIC.

	Procedimiento de Gestión y Monitoreo de Logs Procedimiento	Código: S3.3.P4 Versión: 00 Fecha: 22/09/2026
---	---	--

Especialista de Redes y Comunicaciones	2. Autenticación y Nube: Habilitar en Microsoft Entra ID y servidores locales el registro de inicios de sesión exitosos y fallidos, bloqueos de cuenta y cambios de contraseñas de los activos Microsoft a su cargo según la Matriz de Activos de Información del DTIC. 3. Gestión de Privilegios y Datos: Configurar el registro de creación/eliminación de usuarios en el entorno Microsoft y activar la auditoría unificada en Microsoft Purview / SharePoint Online para rastrear accesos o modificaciones masivas. 4. Seguridad de Red e Infraestructura: Habilitar en el Firewall y equipos de borde el registro de tráfico bloqueado, conexiones VPN y actividades anómalas. Asimismo, habilitar los logs de Sistema Operativo para los servidores físicos y virtuales bajo su custodia.
--	--

3.3. Monitoreo Automatizado y Alertas

Ejecutor	Actividad
Especialista de Sistemas de Información	1. Desarrollar e implementar alertas y notificaciones ante fallas críticas o eventos de seguridad específicos de los sistemas internos y bases de datos bajo su custodia. Toda alerta clasificada como un evento real de seguridad debe documentarse en el Formato S3.3.P4.F2 "Bitácora de Incidentes y Alertas Automatizadas".
Especialista de Redes y Comunicaciones	2. Desarrollar e implementar flujos automatizados (ej. mediante Power Automate o scripts) que interactúen con las APIs de Entra ID / M365 para el envío inmediato de notificaciones ante eventos críticos en la nube. 3. Configurar el envío automático de alertas desde el Firewall o consola de seguridad perimetral ante la detección de ataques. Registrar la mitigación de los ataques relevantes en el Formato S3.3.P4.F2 "Bitácora de Incidentes y Alertas Automatizadas".
Ambos Especialistas	4. Validar de forma trimestral que los scripts de automatización y flujos de alerta de sus respectivas plataformas (Sistemas e

	Procedimiento de Gestión y Monitoreo de Logs Procedimiento	Código: S3.3.P4 Versión: 00 Fecha: 22/09/2026
---	--	---

	Infraestructura/Microsoft) se estén ejecutando correctamente.
--	---

3.4. Respaldo, Retención y Revisión Manual

Ejecutor	Actividad
Especialista de Redes y Comunicaciones	1. Asegurar que los registros operativos de sus plataformas administradas se mantengan disponibles en la consola nativa (Hot Storage) por un mínimo de 90 días. 2. Ejecutar la exportación programada de los logs críticos hacia un repositorio de almacenamiento seguro (Cold Storage) configurado con permisos de solo lectura, manteniéndolos por 1 año. 3. Realizar una revisión manual (semanal o mensual) de los tableros de seguridad (Dashboards) de sus sistemas correspondientes para identificar patrones anómalos. Al finalizar, generar y suscribir el Formato S3.3.P4.F1 " Reporte de Revisión Mensual de Eventos de Seguridad".
Especialista de Sistemas de Información	4. Realizar una revisión manual (semanal o mensual) de los registros de auditoría de los aplicativos internos asignados a su custodia según la Matriz de Activos de Información del DTIC. Al finalizar la revisión, documentar los hallazgos suscribiendo el Formato S3.3.P4.F1 " Reporte de Revisión Mensual de Eventos de Seguridad".
Jefe del Departamento de Tecnología de la Información y Comunicaciones	5. Validar y firmar el Formato S3.3.P4.F1 " Reporte de Revisión Mensual de Eventos de Seguridad" presentado por los especialistas. 6. Autorizar formalmente la liberación o eliminación de registros históricos que hayan superado el tiempo de retención normativo de 1 año.

4. ALCANCES FUNCIONALES

4.1. Gerente de Administración y Finanzas

- Aprobar el presente procedimiento y disponer los recursos necesarios para la implementación de herramientas de monitoreo o almacenamiento de logs en la nube.

4.2. Jefe del Departamento de Tecnologías de la Información y Comunicaciones

	Procedimiento de Gestión y Monitoreo de Logs Procedimiento	Código: S3.3.P4 Versión: 00 Fecha: 22/09/2026
---	--	--

- Conducir el proceso de Gestión y Monitoreo de Logs, cumpliendo las disposiciones establecidas en la Norma ISO/IEC 27001 y el presente procedimiento.
- Aprobar los cambios en las configuraciones de auditoría.
- Revisar los reportes periódicos de eventos y gestionar la respuesta ante posibles incidentes escalados.

4.3. Especialista de Sistemas de Información

- Configurar y gestionar la generación de logs, políticas de auditoría y retención en los sistemas de información y aplicativos internos bajo su custodia según la **Matriz de Activos de Información del DTIC** (ej. STD, SGPAM, ERP Spring, SAFNET, PIMA).
- Desarrollar y mantener los mecanismos automatizados de alerta para los eventos críticos de los sistemas y bases de datos bajo su responsabilidad.

4.4. Especialista de Redes y Comunicaciones

- Configurar y gestionar la generación de logs, políticas de auditoría y retención en las plataformas de identidad, nube y colaboración (Microsoft Entra ID, Active Directory, Microsoft 365, Correo electrónico), así como en los equipos de red, firewalls, servidores y plataformas de virtualización bajo su custodia según la **Matriz de Activos de Información del DTIC**.
- Desarrollar y mantener los mecanismos automatizados de alerta (Power Automate, PowerShell) para el entorno Microsoft.
- Mantener y revisar los sistemas de detección de intrusos y alertas de tráfico anómalo.
- Garantizar la sincronización de tiempo (NTP) en los controladores de dominio, servidores de infraestructura y equipos de comunicaciones.

4.5. Oficial de Seguridad y Confianza Digital

- Analizar los reportes de logs ante la materialización de un incidente de seguridad.
- Auditar periódicamente el cumplimiento del presente procedimiento.

5. REGISTROS / ANEXOS

- Formato S3.3.P4.F1 "Reporte de Revisión Mensual de Eventos de Seguridad".
- Formato S3.3.P4.F2 "Bitácora de Incidentes y Alertas Automatizadas".