Procedimiento de Seguridad de las Comunicaciones

Versión	Fecha	Control de Cambios
1	12/12/2023	• Se actualizó la descripción del procedimiento de seguridad de las comunicaciones, asegurando su alineamiento con la Política de Seguridad de la Información de AMSAC. • En documentos de referencia, se actualizó la normativa legal aplicable.

Áreas Responsables	Nombres y Cargos
Elaborado: **Departamento de Tecnología de la Información y Comunicaciones**	Henry Tornero Especialista en Sistemas de Información
Revisado: **Departamento de Tecnología de la Información y Comunicaciones**	Néstor Pisconte Jefe del Departamento de Tecnología de la 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 (e)

INDICE

I. OBJETIVO

Establecer las actividades que se deben realizar para mantener la seguridad de la información en las redes de Activos Mineros S.A.C. (en adelante AMSAC), así como asegurar que ésta sea transferida desde la empresa hacia entidades o personas externas.

II. ALCANCE

El procedimiento aplica a la red de AMSAC, incluyendo su monitoreo con el uso de internet, servidores y equipos de red.

III. DOCUMENTOS DE REFERENCIA

- Ley N° 27309, Ley que incorpora los delitos informáticos al código penal.
- Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y su reglamento.
- Ley N° 29733, Ley de Protección de Datos Personales y su reglamento.
- 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 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición.
- Política de Seguridad de la Información de AMSAC.
- Directiva S3-DR.01 "Para el Uso de los Servicios y Recursos de Tecnologías de la Información y Comunicaciones"
- Directiva S3-DR.02 "Para la Administración de Software"

IV. VIGENCIA

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

V. CONTENIDO

1. DEFINICIONES / CONSIDERACIONES

- **Firewall:** Dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente.
- **Antivirus:** Software utilizado para evitar, analizar, detectar y eliminar virus de los dispositivos.
- **LAN:** Local Área Network, son un conjunto de dispositivos conectados entre sí que comparte comunicación o enlaces con un servidor.
- **WAN:** Wide Área Network, consiste en varias redes locales unidad, aunque su ubicación física no sea la misma.
- **Trabajadores:** Se refiere a todo el personal interno que guarde relación directa con las actividades laborales realizadas en AMSAC.
- **Terceros:** Personas o grupos de personas externas a AMSAC que interactúan de alguna manera con activos e información de la empresa, tales como proveedores, contratistas, auditores, entidades de control, practicantes, entre otros.
- **Autenticidad:** Propiedad que una entidad es lo que dice ser.
- **Confidencialidad**: Principio de la seguridad de la información que busca asegurar que solo quienes estén autorizados puedan acceder a la información.
- **Integridad:** Principio de la seguridad de la información que busca asegurar que la información y sus métodos sean exactos y completos.
- **No repudio:** Capacidad para demostrar la ocurrencia de un evento o acción reclamada y sus entidades de origen.

- **P2P:** es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.
- **Log**: es el registro de los eventos y acciones sucedidas.

2. DISPOSICIONES GENERALES

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

2.2. El Especialista en Redes y Comunicaciones es el responsable de la administración, gestión y seguridad de los equipos conectados a la red de AMSAC.

2.3. Toda la gestión de recursos para garantizar la protección de las redes de comunicación de AMSAC es de responsabilidad del Jefe del Departamento de TIC. Entre estos recursos, se consideran:
- Recursos de comunicación como redes LAN, canales dedicados de datos, entre otros.
- Recursos hardware y software.
- Servicios de comunicación.

2.4. El uso de la infraestructura de red de AMSAC y sus servicios es para el intercambio de información de índole laboral. No se debe utilizar la red ni sus servicios para fines ajenos a las actividades de la empresa.

2.5. El acceso a internet por cableado o red inalámbrica se otorga de acuerdo con lo establecido en el **Procedimiento de Gestión de Accesos.**

2.6. Se permite la conexión a la red de AMSAC y sus servicios a todo el personal que, por sus funciones, deba tener acceso, mediante cableado y redes inalámbricas;

2.7. Para el trabajo remoto, se utilizará la red de conexiones VPN y se tendrá el acceso mediante las credenciales asignadas.

2.8. Se permite la conexión a la red de AMSAC a terceros para su uso en el marco de la prestación de servicios contratados por la empresa, siempre y cuando el acceso se encuentre autorizado por el Jefe del Departamento de TIC. La red inalámbrica utilizada por terceros no debe permitir conectarse a la red interna de AMSAC, ni aplicaciones o desarrollos internos.

2.9. Los usuarios de internet en la empresa tienen las siguientes responsabilidades:

1. Accede a la red, utilizando las credenciales asignadas.
2. Mantiene, de manera confidencial, sus credenciales de acceso para el uso de internet por cable y red inalámbrica. No deben compartir las contraseñas porque son confidenciales e intransferibles.
3. Utiliza adecuadamente la red, con la finalidad de evitar congestión o degradación de los servicios asociados o que dependen de la infraestructura de red de AMSAC.
4. Asume la responsabilidad de todas las acciones que se realicen desde su cuenta de acceso a internet por cable y red inalámbrica, así como del ingreso, actualización, calidad de datos y uso de credenciales de acceso a las diferentes aplicaciones y a la red.
5. Tiene en cuenta que está prohibido transmitir cualquier material de índole sexual, discriminatorio, hostil, intimidatorio a cualquier persona o grupo de personas.
6. Tiene en cuenta que no se permite publicar información confidencial de la empresa en páginas web o redes sociales sin la autorización respectiva.
7. Hace uso del internet por cable y red inalámbrica sólo para el cumplimiento de sus funciones laborales en AMSAC.

8. Tiene en cuenta que no debe generar ningún tipo de interferencia que afecte el funcionamiento de los equipos de comunicación.

2.10. Para la seguridad de las conexiones y servicios de red, se mantiene implementado un firewall y antivirus. El tráfico hacia internet se encuentra controlado mediante firewall, el cual no permite protocolos utilizados para descargas P2P, ni el acceso a sitios no autorizados.

2.11. Se garantiza la seguridad de la red de AMSAC mediante la separación de ambientes de procesamiento de información: ambiente de desarrollo, pruebas y producción.

2.12. Los puntos de red que no estén siendo utilizados estarán deshabilitados.

2.13. Los relojes de todos los sistemas de información deben estar sincronizados a una fuente oficial de tiempo, lo que permitirá manejar registro de logs exactos en fechas y horas.

3. PROCEDIMIENTO

3.1. Gestión de seguridad de la red

Ejecutor	Actividad
3.1.1 Controles de Red	
ERC	1. Configura la red de manera automática y documentada, estableciendo valores y atributos para mantener identificadas y especificadas las características de componentes y recursos que la conforman.
	2. Conoce la distribución de red y su estado actual. Para ello, se debe tener actualizada una vez al año el diagrama de red.
	3. Establece indicadores para monitorear el servicio de red, como: • disponibilidad • tiempo de respuesta • porcentaje de tiempo en el que no ocurren errores en la entrega y transmisión de datos. • número de sesiones para un sistema o aplicación determinada. • niveles normales de rendimiento de la red. • estadísticas de uso de la red.
	5. En caso de detectar fallo en el servicio de red, procede a realizar lo siguiente: • Verificar la parte eléctrica. • Verificar el estado de los equipos activos y servidores que conforman la red. • Verificar conexiones de red. • Revisar el enrutamiento de datos. • Determinar las causas del fallo. • Aislar el fallo. • Atender y resolver el fallo presentado. • Comprobar la validez de la solución aplicada.
	6. En caso de que la solución deba implementarla un proveedor, comunica al proveedor y gestiona su aplicación. En caso contrario, continuar con el paso 8.
	7. Realiza el seguimiento a la solución aplicada por el proveedor; de ser satisfactoria, cerrar el caso.
	8. Documenta la detección, gestión y resolución aplicada ante el fallo en la bitácora de monitoreo.
	9. Informa al JDTIC los resultados obtenidos.
3.1.2 Gestión de Cambios en la red	
ERC	1. Solicita autorización del JDTIC para aplicar cambios en la red mediante el Formato S3.1.M1.F13 Cambio en la Infraestructura TIC.

Ejecutor	Actividad
JDTIC	2. Revisa y evalúa la solicitud. En caso de estar de acuerdo, aprueba la solicitud. *Continuar con el paso 3*. En caso contrario, indica al ERC el motivo de la denegatoria de la solicitud.
ERC	3. Documenta los cambios que se presenten en la red, como en configuraciones de firewall, SNMP, listas de control de acceso, actualizaciones de software, y los registra, considerando la siguiente información: • Definición del alcance • Analizar el riesgo (considerar puntos finales afectados y servicios que se podrían afectar) • Registrar pruebas y validaciones previas a la implementación • Registrar actividades, fechas y responsables de la implementación y pruebas.
	4. Informa al JDTIC los avances o el término de aplicación de los cambios.
	5. Cierra el caso.
3.1.3 Monitoreo de logs	
ERC	1. Monitorea los logs generados en los sistemas y servicios asociados a la red, así como asegura su conservación por el periodo definido, como evidencia para futuras investigaciones.
	2. Genera respaldos periódicos a los logs.
	3. Emite periódicamente reportes o informes, donde se detalle el cumplimiento de los parámetros de seguridad aplicados en la red, manteniéndolos disponibles.

3.2. **Seguridad en el acceso a internet por cable y redes inalámbricas**

Ejecutor	Actividad
3.2.1 Disponibilidad del servicio	
DTIC	1. Mantiene disponible el servicio de internet para los usuarios, dentro del rango de cobertura de acceso a la red inalámbrica.
3.2.3 Monitoreo de internet	
ERC	1. Monitorea la red por razones de seguridad y rendimiento.
	2. En caso de detectar mal uso de la red, desconecta al usuario de la red.
	3. Informa al JDTIC y al usuario el caso del mal uso de la red.
	4. Genera un informe periódico sobre el uso y estado actual de la red por cable, para poner en conocimiento al JDTIC, quien a su vez lo eleva a la GAF.

3.3. **Transferencia de Información y Acuerdos de confidencialidad**

Ejecutor	Actividad
3.3.1 Acuerdo de confidencialidad del Personal de AMSAC	
Gestión Humana	1. Entrega el Acuerdo de confidencialidad de la información al personal de AMSAC.
Trabajador de AMSAC	2. Lee y suscribe el Acuerdo de confidencialidad de la información, y lo devuelve a la Oficina de Gestión Humana.
Gestión Humana	3. Archiva el Acuerdo de confidencialidad de la información suscrito por el personal de AMSAC, en un lugar seguro para evitar pérdidas o daños al documento.
Gestión Humana	4. Cuando se presente la desvinculación del personal de AMSAC, recuerda al personal saliente las responsabilidades detalladas en el Acuerdo de confidencialidad de la información suscrito al inicio de sus labores.
3.3.2 Acuerdo de confidencialidad para terceros	
Área usuaria	1. Incluye la cláusula de confidencialidad en los términos de referencia para terceros que presenten servicios a la empresa.
Administrador del contrato	2. Velar por el cumplimiento de la cláusula de confidencialidad establecida en los términos de referencia para terceros que presenten servicios a la empresa.

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**
- Conducir el proceso de Seguridad de las Comunicaciones en la empresa, cumpliendo los plazos y las disposiciones previstas en la normativa legal 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.

4.3. **Especialista en Redes y Comunicaciones**
- Supervisar y participar de la instalación y mantenimiento de la red.
- Determinar las necesidades de utilización de los servicios de red y los accesos de los usuarios a la red.
- Administrar las redes y monitorear los servicios de red.
- Identificar, diagnosticar y resolver fallos que se presenten en la red.
- Identificar, evaluar y proponer mejoras en el uso de la red.

4.4. **Jefe de Oficina de Gestión Humana**
- Velar por la suscripción de los acuerdos de confidencialidad por los trabajadores de AMSAC, así como su archivo.

4.5. **Propietario de la Información**
- Verificar que toda la información que sea transferida cuente con la autorización pertinente y de ser necesario se apliquen mecanismo de seguridad para evitar fuga de información.
- Cumplir con lo descrito en el procedimiento.

4.6. **Usuarios**
- Garantizar que toda la información que sea transferida cuente con la autorización pertinente y de ser necesario se apliquen mecanismo de seguridad para evitar fuga de información.
- Cumplir con lo establecido en el procedimiento.

5. REGISTROS / ANEXOS

- Anexo N° 1 Acuerdo de confidencialidad de la información.

Anexo 1

Acuerdo de Confidencialidad de la Información

Comparecen en la celebración del presente acuerdo, el Señor(a) **Nombres y apellidos** en su calidad de **cargo**; y, Activos Mineros S.A.C., en adelante AMSAC, representado por el(la) Señor(a) **Nombre y apellidos** en su calidad de **cargo**; quienes convienen en suscribir el presente Acuerdo de Confidencialidad al tenor de las siguientes cláusulas:

PRIMERO:

1.1 El presente acuerdo de confidencialidad se anexa y forma parte integral del contrato laboral suscrito entre las partes mencionadas

SEGUNDO:

2.1 El empleado reconoce y acepta que toda la información de AMSAC que se le proporcione es propiedad de la entidad, por lo tanto, debe ser tratada como confidencial, restringida y de carácter reservada. Se entiende como información confidencial aquella que se debe mantener en reserva solo para personal autorizado pues soporta procesos críticos de la entidad, en la cual se incluye información técnica, contables, administrativa, legal entre otra que así esté definida en la clasificación de la información.

TERCERO:

3.1. El empleado se obliga a mantener en reserva la información que se le sea entregada por cualquier medio electrónico o físico para el desarrollo de su trabajo.
3.2. El empleado se obliga a no divulgar información en ningún medio de comunicación, redes sociales, o el internet en general información que sea de propiedad de AMSAC.
3.3. El empleado se obliga a no copiar, ni reproducir parcial o totalmente información confidencial sin autorización del Propietario de la Información.
3.4. El empleado se obliga a devolver toda la información que se le ha entregado y que ha generado durante su relación laboral con AMSAC.
3.5. El empleado ha sido informado y acepta que cualquier información, documento, comunicación (física o digital); o mensaje de datos enviado por éste, refleja directa o indirectamente la imagen de AMSAC, entiende y acepta que la entidad debe adoptar las medidas necesarias para evitar daños en su imagen y fugas de información.
3.6. El empleado se obliga a responder por daños y perjuicios, en caso de incumplimientos a la confidencialidad y reserva de la información que maneja en sus labores diarias, así como por los costos y gastos que se generen en caso de demandas, reclamos por incumplimiento a la confidencialidad de la información.
3.7. El empleado ha sido informado, comprende y acepta que las plataformas tecnológicas, la red de datos y comunicaciones, y demás recursos asociados con las tecnologías de información de la entidad son de propiedad de AMSAC.
3.8. El empleado se compromete a usar los recursos de información y tecnológicos de AMSAC de manera legal, profesional y apegada al código de ética.
3.9. El empleado ha sido informado y acepta que conoce el contenido de la Política de Seguridad de la Información y se adhiere a la misma sin restricciones.
3.10. El empleado conoce y acepta que AMSAC como medida de protección ejecutará actividades de respaldo de la información de la entidad de manera manual o automática, a fin de mantener la misma en los repositorios de la entidad, pudiendo en estos procesos, por efecto de la dificultad de discriminación automática, respaldar también la información de carácter personal.
3.11. AMSAC no está obligado a respaldar y preservar la información personal, por lo que, el Empleado deberá tomar las medidas que creyere pertinentes, para que dicha información no sea considerada en los procesos de respaldo institucionales.
3.12. El empleado conoce que AMSAC podrá realizar los procesos de control sobre la información institucional bajo su custodia y recursos tecnológicos asignados a él, que garanticen el buen uso y manejo de estos, cuando lo estime pertinente.

CUARTO

4.1. El empleado autoriza expresamente AMSAC que, en caso de investigación preliminar debidamente autorizada, se abra, retenga y examine la correspondencia virtual identificada como datos personales, contenida en la cuenta de correo electrónico bajo los dominios “amsac.pe”, asignados al Empleado por parte del EMPRESA para el cumplimiento de sus funciones laborales
4.2. El empleado autoriza AMSAC expresamente que, en caso de investigación preliminar debidamente autorizada; se abra, retenga y examine la información identificada como personal, contenida en los recursos tecnológicos asignados a él por parte de la empresa para el cumplimiento de sus funciones laborales.

4.3. En ambos casos, se deberá hacer conocer al Empleado respecto del proceso de investigación preliminar previamente autorizado por **nombre y apellido** de quien autoriza, en el que se le indicará los motivos de ésta, de manera que pueda ejercer su derecho a la defensa y exigir se guarde el secreto de los asuntos ajenos al hecho que motiven dicho análisis.

QUINTO

5.1. El empleado declara que conoce las responsabilidades y sanciones a las que está expuesto por incumplimiento y transgresión de la Política de Seguridad de Información, políticas y procedimientos anexos a esta, del presente Acuerdo de Confidencialidad, sin perjuicio de las responsabilidades civiles o penales a que hubiere lugar en virtud de la Ley.

SEXTO

6.1. Los compromisos establecidos en el presente Acuerdo de Confidencialidad tendrán vigencia durante el tiempo que el empleado esté vinculado laboralmente a AMSAC y posterior al término de las tareas, servicios o actividades tendrá una vigencia de dos años.

Se firma como constancia y aceptación de que el contenido del presente Acuerdo de confidencialidad de la información ha sido comunicado, conocido y aceptado por las partes y que se comprometen a su cumplimiento.

Las partes firman por duplicado el presente documento a los …… días del mes de ……..... de 20……

Empleado	AMSAC
Firma: ……	Firma: ……
Nombres y apellidos: DNI N°:	Nombres y apellidos: DNI N°: