



Firmado digitalmente por:
ERIK ALONSO PRADO VIERA
DNI:46766148 RUC:20103030791
Motivo: Soy el autor del documento
Fecha: 07/10/2026 09:28:46-0500



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: 09/10/2026 11:59:12-0500



Gerente de Administración
y Finanzas

Firmado digitalmente por:
JULIO CESAR TEMPLE
AGUILAR DNI:42302432
RUC:20103030791
Motivo: Doy V° B°
Fecha: 09/10/2026 11:33:36-0500



Devolvemos vida al planeta

Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo

Código: S3.3.IN1

Versión: 00

Fecha: 06/10/2026

Instructivo de Configuración Segura y Hardening de Activos TIC

Versión	Fecha	Control de Cambios
00	06/10/2026	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 Tecnologías 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

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: Doy V° B°
Fecha: 07/10/2026 11:01:59-0500



Especialista en Calidad
y Mejora de Procesos

Firmado digitalmente por:
DEYMER FRANK BARTUREN
HUAMAN DNI:40658546
RUC:20103030791
Motivo: Doy V° B°
Fecha: 08/10/2026 15:44:18-0500

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	---	---

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.	DISPOSICIONES ESPECÍFICAS	5
4.	ALCANCES FUNCIONALES	7
5.	REGISTROS / ANEXOS	8

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	--	--

OBJETIVO

Establecer las líneas base y requisitos mínimos de configuración segura (Hardening Baseline) aplicables a los activos y servicios tecnológicos administrados por AMSAC, con la finalidad de proteger la confidencialidad, integridad y disponibilidad de la información institucional, reducir las vulnerabilidades derivadas de configuraciones inseguras y fortalecer la postura de ciberseguridad de la organización.

I. ALCANCE

El presente lineamiento aplica a:

- Equipos de escritorio.
- Equipos portátiles.
- Servidores Windows.
- Servidores Linux.
- Equipos asignados a personal interno.
- Equipos asignados a terceros autorizados.
- Activos que almacenen, procesen o transmitan información institucional.
- Equipos de comunicaciones y seguridad de red.
- Servicios de resolución DNS.
- Servicios VPN y mecanismos de acceso remoto.
- Servicios de correo electrónico.
- Servicios de acceso a Internet y seguridad perimetral.
- Otros servicios críticos de comunicaciones administrados por AMSAC.

II. DOCUMENTOS DE REFERENCIA

- Directiva S3.1.DR1 Uso de Servicios y Recursos TIC.
- Directiva S3.1.DR2 Administración de Software
- Procedimiento S3.2.P1 Gestión de Respaldo y Recuperación.
- Procedimiento S3.2.P2 Gestión de Accesos.
- Procedimiento S3.3.P1 Gestión de Incidentes de Seguridad de la Información.
- Procedimiento S3.3.P3 Identificación y Análisis de Ciberamenazas
- Política del Sistema Integrado de Gestión.
- Norma Técnica Peruana NTP-ISO/IEC 27001
- Norma Técnica Peruana NTP-ISO/IEC 27002 -

III. VIGENCIA

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

IV. CONTENIDO

1. LÍNEA BASE DE CONFIGURACIÓN SEGURA PARA EQUIPOS DE USUARIO FINAL

1.1. Gestión de Identidades

Los equipos deberán:

- Estar unidos a Microsoft Entra ID o Active Directory.
- Utilizar únicamente cuentas corporativas autorizadas.

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	---	---

- Mantener autenticación multifactor cuando aplique.
- Aplicar el principio de mínimo privilegio.

1.2.Privilegios Administrativos

- Los usuarios finales no deberán pertenecer al grupo local Administradores.
- Las cuentas administrativas deberán estar separadas de las cuentas de usuario.
- Los privilegios administrativos deberán ser autorizados formalmente.

1.3.Contraseñas y Bloqueo de Sesión

- Longitud mínima de 12 caracteres.
- Bloqueo automático de sesión máximo a los 5 minutos de inactividad.
- Requerir autenticación para desbloqueo.

1.4.Protección Endpoint

Todo equipo deberá contar con:

- Microsoft Defender for Endpoint o Antivirus equivalente.
- Protección en tiempo real activado
- Protección en la nube activado.
- Tamper Protection.
- Protección antiransomware activado.
- Escaneos programados.

1.5. Firewall

Mantener habilitado Windows Defender Firewall para:

- Dominio.
- Red Privada.
- Red Pública.

1.6. Gestión de Actualizaciones

- Instalación automática de actualizaciones de seguridad.
- Gestión centralizada mediante Microsoft Intune o herramienta autorizada.
- Aplicación prioritaria de parches críticos.

1.7. Gestión de Vulnerabilidades

- Monitoreo continuo mediante herramientas corporativas.
- Corrección de vulnerabilidades críticas dentro del plazo definido por TIC.
- Generación de reportes periódicos de cumplimiento.

1.8. Cifrado de Información

- BitLocker habilitado.
- Claves de recuperación almacenadas en Microsoft Entra ID.
- Cifrado obligatorio para equipos portátiles.

1.9. Dispositivos USB

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	---	---

- Bloqueo por defecto de dispositivos extraíbles.
- Habilitación únicamente mediante autorización formal.
- Registro y monitoreo de excepciones.

1.10. Instalación de Software

- Solo software autorizado por TIC.
- Prohibida la instalación por parte del usuario.
- Prohibido software sin licenciamiento.

1.11. Navegación y Correo

- Protección antiphishing habilitada.
- Protección antispam habilitada.
- Restricción de descargas desde sitios no autorizados.

1.12. Acceso Remoto

- Uso obligatorio de VPN corporativa.
- Acceso únicamente desde dispositivos administrados.
- Aplicación de acceso condicional.

1.13. Registro y Monitoreo

Registrar como mínimo:

- Inicio y cierre de sesión.
- Instalación de software.
- Cambios de privilegios.
- Eventos de seguridad.
- Conexión de dispositivos externos.

1.14. Cifrado de Información

Los dispositivos administrados deberán permitir:

- Bloqueo remoto.
- Restablecimiento remoto.
- Borrado remoto.

1.15. Gestión mediante Microsoft Intune

Todos los equipos corporativos deberán contar con las siguientes políticas:

- Política de cumplimiento
- Línea Base de Seguridad
- Política de Seguridad de Dispositivo Final (Endpoint)
- Política de cifrado BitLocker
- Política de Antivirus
- Política de Firewall
- Política de Actualizaciones de Windows.

2. LÍNEA BASE DE HARDENING PARA SERVIDORES WINDOWS

2.1. Gestión de Identidades

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	---	---

- Integración con Active Directory o Entra ID cuando corresponda.
- Uso de cuentas nominativas.
- Aplicación del principio de mínimo privilegio.

2.2. Cuentas Administrativas

- Separación de cuentas administrativas y operativas.
- Restricción de administradores locales.
- Revisión periódica de privilegios.

2.3. Acceso Remoto

- RDP únicamente para personal autorizado.
- Restricción mediante VPN o segmentación de red.
- Prohibido exponer RDP a Internet.

2.4. Servicios y Roles

- Mantener únicamente servicios requeridos.
- Deshabilitar componentes innecesarios.
- Revisar periódicamente servicios habilitados.

2.5. Protección Endpoint

- Microsoft Defender o XDR equivalente activo.
- Protección en tiempo real.
- Protección antimanipulación.
- Actualización automática de firmas.

2.6. Firewall

- Firewall habilitado permanentemente.
- Puertos abiertos únicamente por necesidad operativa documentada.

2.7. Gestión de Parches

- Aplicación de actualizaciones de seguridad.
- Registro de actualizaciones implementadas.

2.8. Auditoría

Registrar:

- Inicio y cierre de sesión.
- Elevación de privilegios.
- Cambios de configuración.
- Instalación de software.
- Eventos críticos del sistema.

2.9. Cifrado

- Cifrado de discos cuando almacenen información sensible.
- Protección de claves de recuperación.

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	---	---

3. LÍNEA BASE DE HARDENING PARA SERVIDORES LINUX

Aplica para:

- Red Hat Enterprise Linux.
- Ubuntu Server.
- Otras distribuciones autorizadas.

3.1. Gestión de Usuarios

- Cuentas nominativas.
- Eliminación de cuentas obsoletas.
- Aplicación del principio de mínimo privilegio

3.2. Usuario Root

- Deshabilitar acceso remoto directo del usuario root.
- Utilizar sudo para tareas administrativas.

3.3. Servicio SSH

- Uso de protocolo seguro.
- Restricción de usuarios autorizados.
- Limitación de intentos fallidos de autenticación.
- Restricción de acceso desde redes autorizadas.

3.4. Gestión de Parches

- Mantener actualizado el sistema operativo.
- Aplicar actualizaciones de seguridad oportunamente.

3.5. Firewall

Implementar y administrar:

- firewalld.
- nftables.
- iptables.

Según la distribución utilizada.

3.6. Servicios

- Deshabilitar servicios innecesarios.
- Mantener únicamente puertos autorizados.

3.7. Auditoría

Mantener registros de:

- Inicio y cierre de sesión.
- Uso de sudo.
- Cambio de configuraciones.
- Creación o eliminación de usuarios.
- Eventos de seguridad.

3.8. Protección Antimalware

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	--	--

Mantener una Solución Antimalware:

- Microsoft Defender for Linux o Solución EDR aprobada por AMSAC.

3.9. Sincronización de Tiempo

Los servidores deberán utilizar de acuerdo al sistema operativo alguno de estos servicios de sincronización de tiempo:

- NTP.
- Chrony.
- Servicios de sincronización autorizados.

3.10. Respaldo y Recuperación

- Respaldo automático conforme a la política de backups.
- Pruebas periódicas de recuperación.
- Conservación de evidencias de ejecución.

4. LÍNEA BASE DE CONFIGURACIÓN SEGURA PARA SERVICIOS CRÍTICOS DE RED

4.1. Servicio DNS

El servicio DNS utilizado por AMSAC deberá:

- Contar con mecanismos de protección y filtrado frente a dominios maliciosos, phishing, malware y otras amenazas conocidas.
- Aplicar políticas o categorías de bloqueo definidas por el Departamento de TIC.
- Mantener mecanismos de registro, monitoreo y alertamiento sobre eventos relevantes de seguridad.
- Utilizar únicamente servidores o servicios DNS autorizados por el Departamento de TIC en los entornos institucionales donde técnicamente corresponda.
- Restringir las modificaciones de las políticas y configuraciones DNS al personal autorizado.
- Mantener controladas y documentadas las excepciones a las políticas de filtrado.
- Revisar periódicamente las políticas y configuraciones de seguridad aplicadas.

4.2. Servicio VPN y acceso remoto

Los servicios de acceso remoto deberán:

- Utilizar exclusivamente soluciones VPN o mecanismos de acceso remoto autorizados por el Departamento de TIC.
- Requerir autenticación mediante cuentas institucionales autorizadas.
- Utilizar autenticación multifactor cuando la tecnología lo permita.
- Limitar el acceso a usuarios, dispositivos, redes y recursos previamente autorizados.
- Aplicar los principios de mínimo privilegio y necesidad de acceso.
- Mantener registros de conexiones, desconexiones, intentos fallidos y otros eventos relevantes disponibles en la plataforma.

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	---	---

- Restringir la administración y modificación de la configuración VPN al personal autorizado.
- Revisar periódicamente usuarios, grupos, permisos y políticas asociadas al acceso remoto.
- Retirar o modificar oportunamente los accesos cuando desaparezca la necesidad que justificó su asignación.
- Mantener actualizados los componentes utilizados para proporcionar el servicio.

4.3. Servicio de correo electrónico

El servicio de correo electrónico institucional deberá:

- Contar con mecanismos de protección contra malware, spam, phishing y otras amenazas asociadas al correo electrónico.
- Mantener políticas de análisis y protección de archivos adjuntos y vínculos cuando la tecnología utilizada lo permita.
- Aplicar mecanismos para identificar, bloquear, poner en cuarentena o alertar sobre mensajes considerados riesgosos.
- Requerir los mecanismos de autenticación definidos por AMSAC, incluyendo autenticación multifactor cuando corresponda.
- Mantener registro y monitoreo de alertas y eventos relevantes de seguridad.
- Restringir la administración de las políticas de seguridad del correo electrónico al personal autorizado.
- Revisar periódicamente las configuraciones y políticas de protección implementadas.
- Gestionar los eventos detectados de acuerdo con los procedimientos de seguridad e incidentes establecidos por AMSAC.

4.4. Internet y Seguridad Perimetral

Los servicios de acceso a Internet deberán:

- Mantener mecanismos de seguridad perimetral o controles equivalentes para inspeccionar y controlar las comunicaciones.
- Restringir servicios, aplicaciones, categorías, destinos o comunicaciones identificadas como riesgosas o no autorizadas por AMSAC.
- Aplicar filtrado de navegación conforme a las políticas institucionales.
- Mantener mecanismos de protección frente a amenazas provenientes de redes externas.
- Registrar y monitorear eventos relevantes de seguridad asociados al tráfico de Internet.
- Restringir la administración de las políticas y reglas de seguridad al personal autorizado.
- Mantener controladas las excepciones a las políticas de bloqueo.
- Revisar periódicamente las políticas de seguridad implementadas y su necesidad operativa.

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	--	--

Verificación de Configuración Segura de Servicios de Red:

- El Departamento de TIC deberá verificar periódicamente el cumplimiento de las configuraciones de seguridad establecidas para los servicios críticos de red y adicionalmente cuando se produzcan cambios significativos en las plataformas, infraestructura o riesgos asociados.
- Las revisiones deberán considerar, según corresponda, las políticas habilitadas, configuraciones de autenticación y acceso, mecanismos de protección, registros de eventos, alertas y excepciones configuradas.
- Las desviaciones identificadas deberán ser evaluadas y corregidas o gestionadas mediante el mecanismo de excepciones establecido en el presente instructivo.
- Los resultados de las verificaciones deberán conservarse como evidencia mediante reportes, capturas de configuración, registros de plataforma, actas de revisión u otros mecanismos disponibles.

5. GESTIÓN DE EXCEPCIONES

Toda excepción a la presente línea base deberá:

- Encontrarse técnicamente sustentada.
- Ser evaluada por el Departamento de TIC.
- Ser aprobada por el Oficial de Confianza y Seguridad Digital.
- Contar con controles compensatorios.
- Mantener una vigencia definida.
- Ser revisada periódicamente.

6. VERIFICACIÓN DEL CUMPLIMIENTO

El cumplimiento del presente lineamiento será evaluado mediante:

- Microsoft Intune.
- Microsoft Defender.
- SIEM Wazuh o equivalente.
- Auditorías internas.
- Revisiones técnicas periódicas.
- Evaluaciones de vulnerabilidades.
- Pruebas de penetración cuando corresponda.
- Plataformas de seguridad y monitoreo de red.
- Consolas de protección DNS y acceso seguro.
- Plataformas de administración VPN.
- Consolas de seguridad del correo electrónico.
- Firewalls y soluciones de seguridad perimetral.
- Reportes o registros de revisión de configuraciones.

Los incumplimientos detectados deberán registrarse y gestionarse conforme a los procedimientos de gestión de incidentes, gestión de riesgos o gestión de vulnerabilidades de AMSAC.

	Instructivo de Configuración Segura y Hardening de Activos TIC Instructivo	Código: S3.3.IN1 Versión: 00 Fecha: 06/10/2026
---	--	--

7. ALCANCES FUNCIONALES

6.1. Gerente de Administración y Finanzas

- Aprobar el presente documento.

6.2. Departamento de TIC

- Definir técnicamente y mantener las líneas base de configuración segura.
- Implementar o supervisar las configuraciones establecidas mediante las herramientas autorizadas.
- Verificar periódicamente su cumplimiento.
- Registrar y gestionar las desviaciones identificadas.
- Proponer las excepciones técnicamente justificadas.

6.3. Oficial de Seguridad y Confianza Digital

- Verificar que las líneas base se encuentren alineadas con los requisitos del SGSI.
- Evaluar los riesgos de seguridad asociados a excepciones.
- Revisar y aprobar, cuando corresponda, las excepciones propuestas.
- Verificar el cumplimiento de los controles en el marco de las actividades de seguimiento del SGSI.

6.4. Personal de AMSAC

- Utilizar los activos conforme a las configuraciones establecidas.
- No modificar ni deshabilitar controles de seguridad implementados por TIC.
- Reportar incidentes o anomalías detectadas.

8. REGISTROS / ANEXOS

Como evidencia de cumplimiento podrán utilizarse:

- Reportes de cumplimiento de Microsoft Intune.
- Reportes de Microsoft Defender.
- Reportes de Wazuh.
- Actas de revisión de configuraciones.
- Registros de excepciones aprobadas.
- Informes de auditoría interna.
- Informes de evaluación de vulnerabilidades.
- Reportes o evidencias de configuración de protección DNS.
- Registros de accesos y configuración VPN.
- Reportes de seguridad del correo electrónico.
- Reportes de seguridad perimetral y filtrado de Internet.
- Evidencias de revisión periódica de servicios críticos de red.