

 Devolvemos vida al planeta	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	--

Procedimiento de Gestión de Accesos

Versión	Fecha	Control de Cambios
05	06/10/2026	• Numeral 3.7. Se incorporó la gestión de accesos privilegiados, incluyendo las actividades de solicitud, evaluación, aprobación, asignación, registro, revisión periódica, modificación, suspensión y retiro. Se amplió el alcance del procedimiento a privilegios administrativos sobre infraestructura tecnológica, sistemas de información, servicios en nube, grupos administrativos, sitios SharePoint y demás recursos TIC críticos. • Numeral 4. Se actualizaron las referencias y responsabilidades relacionadas con la gestión y revisión de accesos conforme a la NTP ISO/IEC 27001. • Numeral 5. Se incorporó el formato S3.2.P2.F6 "Registro de Accesos Privilegiados".

Áreas Responsables	Nombres y cargos
Elaborado: Departamento de Tecnologías de la Información y Comunicaciones	Henry Tórnero Especialista en Sistemas de Información
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.

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	3
3.	DESCRIPCIÓN	4
4.	ALCANCES FUNCIONALES	12
5.	REGISTROS / ANEXOS.....	13

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	---

I. OBJETIVO

Establecer las actividades para la solicitud, evaluación, aprobación, asignación, modificación, revisión y retiro de los accesos a aplicaciones, servicios, infraestructura y demás recursos TIC de AMSAC, incluyendo la gestión de accesos privilegiados, con la finalidad de prevenir accesos no autorizados y proteger la confidencialidad, integridad y disponibilidad de la información.

II. ALCANCE

- El presente procedimiento es de aplicación obligatoria a las áreas, personal interno, personal externo y demás partes que intervengan en la solicitud, aprobación, asignación, modificación, revisión o retiro de accesos a los recursos TIC de AMSAC.

Comprende la gestión del ciclo de vida de los accesos de usuarios y accesos privilegiados sobre aplicaciones, sistemas de información, infraestructura tecnológica, servidores, dispositivos de red y seguridad, bases de datos, servicios y plataformas en nube, sitios SharePoint y demás recursos TIC administrados o utilizados por AMSAC.

III. DOCUMENTOS DE REFERENCIA

- Directiva Corporativa de Gestión Empresarial de FONAFE.
- NTP ISO/IEC 27001 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 3ra. Edición
- Norma ISO 9001 Sistema de Gestión de la Calidad – Requisitos.
- Directiva S3.1.DR1 Uso de Servicios y Recursos de Tecnologías de la Información y Comunicaciones.
- Directiva S3.1.DR2 Administración de Software.

IV. VIGENCIA

Este documento entrará en vigencia a partir del primer día hábil después de la fecha de aprobación, derogándose su precedente Versión 04, de fecha 09.jun.2024.

V. CONTENIDO

1. DEFINICIONES / CONSIDERACIONES

Ver documento S3-GT.01 Glosario de Términos del Dpto. de Tecnologías de Información y Comunicaciones.

- Acceso privilegiado:** Derecho, rol, perfil o permiso que permite realizar funciones administrativas, de configuración, gestión, modificación o control sobre recursos TIC, superiores a las disponibles para un usuario estándar.
- Cuenta privilegiada:** Cuenta destinada a realizar funciones administrativas o técnicas que requieren permisos elevados sobre uno o más recursos TIC.
- Recurso TIC crítico:** Sistema, servicio, plataforma, aplicación, infraestructura o componente tecnológico cuya indisponibilidad, alteración, exposición o acceso no autorizado pueda generar un impacto significativo para AMSAC.

2. DISPOSICIONES GENERALES

- El Jefe del Departamento de Tecnología de la Información y Comunicaciones, como dueño del proceso, es responsable que el proceso de Gestión de Accesos se efectúe cumpliendo los plazos y las disposiciones previstas en la normativa legal y el presente procedimiento.
- La Oficina de Gestión Humana o el área usuaria que lo requiera, según corresponda, pueden solicitar al Departamento de Tecnología de la Información y Comunicaciones el alta y baja de usuario o cambio de perfiles de acceso a los servicios informáticos de AMSAC, conforme a lo establecido en las directivas de TIC y el presente procedimiento.

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	---

- 2.3. Los accesos privilegiados deberán asignarse únicamente cuando exista una necesidad operativa debidamente justificada, aplicando los principios de mínimo privilegio, necesidad de conocer y segregación de funciones.
- 2.4. Todo acceso privilegiado deberá contar con autorización previa del Jefe del Departamento de TIC antes de su asignación, salvo situaciones de contingencia debidamente justificadas y regularizadas posteriormente conforme a los mecanismos establecidos por AMSAC.
- 2.5. Las solicitudes y autorizaciones podrán sustentarse mediante los formatos del presente procedimiento, SIGAP, memorandos u otros mecanismos formales establecidos por AMSAC, debiendo mantenerse evidencia que permita demostrar la solicitud y autorización del privilegio otorgado.
- 2.6. Los accesos privilegiados deberán registrarse en el formato S3.2.P2.F6 “Registro de Accesos Privilegiados” y estarán sujetos a revisión periódica.

3. DESCRIPCIÓN

Ejecutor	Actividad
3.1. Gestión de solicitudes de Alta de Usuario	
Gestión Humana	1. El Especialista en Desarrollo de Personal solicita el alta del usuario con el sustento pertinente usando el formato S3.2.P2.F1 “Solicitud de Alta, Baja de Usuario o Cambio de perfil” al Jefe del Departamento de TIC.
Área usuaria	2. En caso de personal externo con contrato u orden de servicio vigente, la Gerencia, Jefatura y/o Supervisión del área solicita el alta del usuario con el sustento pertinente usando el formato S3.2.P2.F1 “Solicitud de Alta, Baja de Usuario, Cambio de perfil o Uso de Aplicaciones” al Jefe del Departamento de TIC.
Especialista de Redes y Comunicaciones	3. Verifica en la solicitud de alta de usuario: a) Que los datos del usuario y solicitante son correctos. b) Que el requerimiento esté conforme a las directivas de TIC y a la Matriz de Perfiles de Usuario de Recursos TIC (S3.2.P2.F5), se encuentre sustentado y tenga el visto bueno de la Supervisión, Jefatura y/o Gerencia del área.
Jefe del Departamento de TIC	4. Evalúa y aprueba la solicitud en caso sea procedente. 5. En caso de que NO proceda; comunica al área usuaria el motivo de la denegatoria de la solicitud vía correo electrónico, culminando así este proceso.
Especialista de Redes y Comunicaciones	6. Crea el usuario según estándar de nomenclatura y configura el perfil que le corresponde acorde a la Matriz de Perfiles de Usuario de Recursos de TIC (S3.2.P2.F5) y la vigencia del usuario dependiendo de la fecha de término del contrato del personal interno o externo, de ser el caso.
	7. Configura los accesos siguiendo las instrucciones de creación de accesos para el “correo electrónico institucional”, “internet”, “impresión / escaneo”, “telefonía fija (código de llamadas)”, “telefonía móvil”, “unidad de red o en la nube”.



Devolvemos vida al planeta

Procedimiento de Gestión de Accesos

Procedimiento

Código: S3.2.P2

Versión: 05

Fecha: 06/10/2026

Ejecutor	Actividad
	Nota: Instrucciones para la creación de accesos. Para la creación del “correo electrónico institucional”, se debe tener en cuenta lo siguiente: 1. Identificar el usuario y crear el buzón de correo o mailbox en servidor de correos según perfil de usuario que corresponda. Dependiendo del perfil de usuario, se definirá la limitación de espacio y las restricciones del uso del buzón de correo. 2. Dependiendo de los accesos autorizados para el usuario, realizar configuraciones, como enviar/recibir correos electrónicos externos. 3. Configurar el acceso en la computadora del usuario. Para la creación del acceso al “internet”, se debe tener en cuenta lo siguiente: 1. Revisar los enlaces de comunicaciones para el servicio de internet, con el fin de verificar que se puede habilitar el acceso a internet al usuario. 2. Configurar el acceso a internet al usuario según el perfil que corresponda. Dependiendo del perfil del usuario, se filtra contenido y se aplican políticas de seguridad. 3. Configurar el acceso en la computadora del usuario. Para la creación del acceso a la “impresión / escaneo” se debe tener en cuenta lo siguiente: 1. Identificar el usuario de red. 2. Configurar el usuario de red para acceder a la impresora y/o scanner requerido según el perfil que le corresponda. 3. Configurar el acceso en la computadora personal de usuario, definiendo la carpeta donde se guardarán automáticamente los documentos escaneados dependiendo del perfil que fue asignado. Para la creación del acceso a la “telefonía fija (código de llamada)” se debe tener en cuenta lo siguiente: 1. Crear el código para hacer llamadas según el perfil que le corresponda al usuario. 2. En caso sea necesario, entregar un teléfono fijo siguiendo con las actividades de asignación de equipo informático. Para la creación del acceso a la “telefonía móvil” se debe tener en cuenta lo siguiente: 1. Asignar el plan de datos y minutos y el modelo de teléfono según el cuadro de asignación que se define y aprueba cada año como parte de la renovación anual del contrato de telefonía móvil. 2. Entregar un teléfono móvil siguiendo las actividades de asignación de equipo informático. Para la creación del acceso a la “unidad de red o en la nube”, se debe tener en cuenta lo siguiente: 1. Identificar el usuario de red o en la nube y verificar que unidad de red este activa. Ejemplo de unidad de red: carpeta compartida. 2. Configurar el acceso a unidad de red según el perfil que corresponda. Por ejemplo, dependiendo del perfil, el usuario sólo podrá tener acceso de lectura en la carpeta compartida. 3. Configurar el acceso en la computadora del usuario.

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	--

Ejecutor	Actividad
	Para todos los casos de creación, se coordinará con el usuario para realizar las pruebas de funcionamiento.
Especialista de Sistemas de Información	8. Configura el usuario en la aplicación requerida acorde a la “Matriz de Perfiles de Usuario de Recursos de TIC” (S3.2.P2.F5).
Especialista de Redes y Comunicaciones	9. Comunica que la solicitud de alta ha sido atendida a la Oficina de Gestión Humana o al área usuaria, según corresponda.
	10. Brindar inducción al usuario sobre los accesos configurados haciendo referencia a manuales de usuario correspondientes. De ser necesario, coordina con el usuario responsable del sistema para que le brinde inducción al usuario sobre uso de aplicación.
Área Usuaria	11. Verifica la funcionalidad de los accesos solicitados.
3.2. Gestión de solicitudes de Cambio de perfil de usuario	
Gestión Humana	1. En caso de encargaturas y delegación de funciones, el Especialista en Administración de Personal realiza directamente la actualización del perfil del usuario en el ERP Spring, acorde al documento que aprueba la encargatura o delegación de funciones; culminando así este proceso.
	2. En caso de rotación de personal, el Especialista en Desarrollo de Personal solicita el cambio del perfil del usuario con el sustento pertinente usando el formato S3.2.P2.F1 “Solicitud de Alta, Baja de Usuario o Cambio de perfil” al Jefe del Departamento de TIC.
Área usuaria	3. La Gerencia, Jefatura y/o Supervisor del área solicita el cambio de perfil (por ejemplo, cambio en niveles de acceso) utilizando el formato S3.2.P2.F1 “Solicitud de Alta, Baja de Usuario o Cambio de perfil” al Jefe del Departamento de TIC.
Especialista de Redes y Comunicaciones	4. Verifica en la solicitud de cambio de perfil de usuario: a) Que los datos del usuario y solicitante son correctos. b) Que el requerimiento esté conforme a las políticas y directivas de TIC y a la Matriz de Perfiles de Usuario de Recursos TIC (S3.2.P2.F5), se encuentre sustentado y tenga el visto bueno de la Supervisión, Jefatura y/o Gerencia del área.
	5. Evalúa y aprueba la solicitud en caso sea procedente.

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	---

Ejecutor	Actividad
Jefe del Departamento de TIC	6. En caso de que NO proceda; comunicar al área usuaria el motivo de la denegatoria de la solicitud vía correo electrónico, culminando así este proceso.
Especialista de Redes y Comunicaciones	7. Configura los accesos requeridos siguiendo las instrucciones de modificación de accesos para el “correo electrónico institucional”, “internet”, “impresión / escaneo”, “telefonía fija (código de llamadas)”, “unidad de red o en la nube”, acorde a la “Matriz de Perfiles de Usuario de Recursos de TIC (S3.2.P2.F5).
	Nota: Instrucciones para la modificación de accesos: Para la modificación del “correo electrónico institucional” se debe tener en cuenta lo siguiente: 1. Identificar la cuenta de correo. 2. Realizar las modificaciones requeridas a la cuenta. Ejemplos de modificación: Envío o recepción de emails externos, reenvío de correo, ampliación del tamaño de archivos adjuntos a los correos electrónicos, normalmente la cuota es 10MB. 3. Configurar acceso en computadora del usuario. Para la modificación del acceso al “internet” se debe tener en cuenta lo siguiente: 1. Identificar el perfil de acceso a internet que fue asignado al usuario. 2. Realizar las modificaciones requeridas al perfil correspondiente o se cambia de perfil según sea necesario. Ejemplo de modificación: ampliar el acceso a páginas web. Para la modificación del acceso a la “impresión / escaneo” se debe tener en cuenta lo siguiente: 1. Identificar el usuario que tiene acceso a la impresora y/o scanner. 2. Realizar las modificaciones requeridas. Ejemplo de modificación: dar acceso a envío de documentos escaneados a correo electrónico. Para la modificación del acceso a la “telefonía fija (código de llamada)” se debe tener en cuenta lo siguiente: 1. Identificar el código de llamadas asignado a usuario. 2. Realizar las modificaciones requeridas a configuración de código asignado. Ejemplo de modificación: dar acceso a llamadas a teléfono celular. Para la modificación del acceso a la “unidad de red o en la nube” se debe tener en cuenta lo siguiente: 1. Identificar el usuario de red y unidad de red o en la nube. 2. Realizar las modificaciones del acceso a la unidad de red requeridas. Ejemplo de modificación: ampliar a permisos de escritura en carpeta compartida. 3. Configurar el acceso en la computadora de usuario de ser necesario. Para todos los casos de modificación se coordinará con el usuario para realizar las pruebas de funcionamiento.
	8. En caso de que el usuario tenga accesos a los sistemas de información de AMSAC, coordina con el Especialista en Sistemas de Información para realizar los ajustes necesarios.
	9. Comunica que la solicitud de cambio de perfil ha sido atendida al área usuaria.

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	---

Ejecutor	Actividad
	10. Brinda inducción al usuario sobre los accesos configurados haciendo referencia a manuales de usuario correspondientes.
Área Usuaría	11. Verifica que el cambio de perfil esté acorde a lo solicitado.
3.3. Gestión de solicitudes de Baja de Usuario	
Gestión Humana	1. El Especialista en Administración de Personal solicita la baja del usuario con el sustento pertinente usando el formato S3.2.P2.F1 "Solicitud de Alta Baja de Usuario o Cambio de perfil" al Jefe del Departamento de TIC.
Área usuaria	2. En caso de finalización del servicio de personal externo antes del plazo previsto, la Jefatura y/o Gerencia del área puede solicitar la baja del usuario con el sustento pertinente usando el formato S3.2.P2.F1 "Solicitud de Alta, Baja de Usuario o Cambio de perfil" al Jefe del Departamento de TIC.
Especialista de Redes y Comunicaciones	3. Verifica en la solicitud de baja de usuario: a) que los datos del usuario son correctos. b) que el requerimiento esté conforme a las políticas y directivas de TIC y a la "Matriz de Perfiles de Usuario de Recursos TIC" (S3.2.P2.F5), esté sustentado y tenga el visto bueno de la Supervisión, Jefatura y/o Gerencia del área.
Jefe del Departamento de TIC	4. Evalúa y aprueba la solicitud en caso sea procedente.
	5. En caso de que NO proceda; comunica al área usuaria el motivo de la denegatoria de la solicitud vía correo electrónico, culminando así este proceso.
Especialista de Redes y Comunicaciones	6. Da de baja al usuario siguiendo las instrucciones de baja de accesos para el "correo electrónico institucional", "internet", "impresión / escaneo", "telefonía fija (código de llamadas)", "telefonía móvil", "unidad de red o en la nube".
	Nota: Instrucciones para la baja de accesos de usuarios Para la baja del "correo electrónico institucional" se debe tener en cuenta lo siguiente: 1. Identificar la cuenta de correo. 2. Hacer copia de respaldo a mailbox correspondiente y configurar reenvío de correos según perfil de usuario. 3. Deshabilitar cuenta de correo. Para la baja del acceso al "internet" se debe tener en cuenta lo siguiente: 1. Identificar el perfil de acceso a internet que fue asignado al usuario 2. Deshabilitar el acceso a internet del usuario. Para la baja del acceso a la "impresión / escaneo" se debe tener en cuenta lo siguiente: 1. Identificar el usuario que tiene acceso a la impresora y/o scanner. 2. Deshabilitar el acceso a impresora y/o scanner. Para la baja del acceso a la "telefonía fija (código de llamada)" se debe tener en cuenta lo siguiente: 1. Identificar el código de llamadas asignado a usuario. 2. En caso sea necesario, recoger teléfono fijo asignado siguiendo las actividades de devolución de equipo informático. 3. Deshabilitar el código asignado. Para la baja del acceso a la "telefonía móvil" se debe tener en cuenta lo siguiente: 1. Solicitar la devolución de teléfono móvil asignado al usuario siguiendo con las actividades de devolución de equipo informático.

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	---

Ejecutor	Actividad
	2. Borrar la data del usuario en el teléfono móvil devuelto. 3. Inactivar la línea telefónica. Para la baja del acceso a la “unidad de red o en la nube” se debe tener en cuenta lo siguiente: 1. Identificar el usuario de red y unidad de red o en la nube. 2. Deshabilitar el acceso a unidad de red.
Especialista de Sistemas de Información	7. Da de baja al usuario en las aplicaciones de la empresa acorde a la Matriz de Perfiles de Usuario de Recursos TIC (S3.2.P2.F5).
Especialista de Redes y Comunicaciones	8. Comunica que la solicitud de baja de usuario ha sido atendida a la Oficina de Gestión Humana o al área usuaria, según corresponda.
3.4. Seguimiento de accesos de usuarios	
Especialista de Redes y Comunicaciones	1. En concordancia con el apartado A.9.2.5 de la ISO 27001, hace seguimiento del uso de los accesos configurados para cada usuario, con la finalidad de verificar que cumple con el perfil asignado e identificar abusos de acceso, accesos no autorizados, uso inapropiado de accesos.
	2. Captura evidencia de algún caso de uso inapropiado de accesos descritos en las directivas de TIC.
Especialista de Sistemas de Información	3. hace seguimiento al uso de los accesos configurados para cada usuario de los sistemas de información de la empresa, con la finalidad de verificar que cumple con el perfil asignado e identificar abusos de acceso, accesos no autorizados, uso inapropiado de accesos.
	4. Captura evidencia de algún caso de uso inapropiado de accesos descritos en las directivas de TIC.
3.5. Depuración de usuarios	
Especialista de Redes y Comunicaciones	1. Al fin de cada mes, verifica en el Directorio Activo aquellos usuarios que no acceden a la Red de Activos Mineros durante los últimos tres meses.
	2. Inactiva las cuentas de los usuarios que pasaron más de 3 meses sin ser utilizados.
	3. Realiza un listado de usuarios inactivados, considerando los nombres y apellidos, cargo, usuario de red y fecha de último acceso, y lo remite al Jefe de TIC.
Especialista de Sistemas de Información	4. Al fin de cada mes, verifica en el maestro de usuarios del ERP aquellos usuarios que no acceden al sistema durante los últimos tres meses.
	5. Inactiva las cuentas de los usuarios que pasaron más de 3 meses sin ser utilizados.
	6. Realiza un listado de usuarios inactivados, considerando los nombres y apellidos, cargos, usuario de red y fecha de último acceso, y lo remite al Jefe de TIC.
Jefe del Departamento de TIC	7. Consolida y remite a las áreas respectivas los listados de usuarios inactivados elaborados por el Especialista en Redes y Comunicaciones y el Especialista en Sistemas de Información, para su conocimiento.
3.6. Exoneración de Restricción de TIC	
Área Usuaria	1. Solicita la exoneración de restricción de TIC, como páginas web o dispositivos de almacenamiento externo, mediante el llenado del formato S3.2.P2.F3 “Exoneración de restricción de TIC” , indicando los datos del solicitante, tipo de exoneración, justificación y periodo de vigencia, y remitiendo el formato visado por el gerente, jefe o supervisor del área al Departamento de TIC.

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	---

Ejecutor	Actividad
Especialista de Redes y Comunicaciones	2. Recibe la solicitud validada, revisa la información y verifica que la justificación se encuentre conforme a las políticas y directivas de seguridad de la información de la empresa.
Jefe del Departamento de TIC	3. Evalúa la solicitud de exoneración de restricción, determinando su aprobación o rechazo. De aprobarse, firma en la sección de autorización del DTIC del formato.
Especialista de Redes y Comunicaciones	4. Configura y habilita el acceso solicitado, ya sea de forma temporal o permanente, implementando los controles de seguridad necesarios.
	5. Informa al usuario sobre la habilitación del acceso solicitado.
3.7. Gestión de Accesos Privilegiados*	
Área Usuaria / Departamento de TIC	1. Identifica la necesidad de asignar un acceso privilegiado y presenta la solicitud mediante el mecanismo formal aplicable, indicando como mínimo el usuario, recurso TIC, rol o privilegio requerido, justificación y vigencia solicitada. 2. Para accesos privilegiados relacionados con aplicaciones o servicios en nube que actualmente sean autorizados mediante memorando, dicho documento constituirá el sustento formal de la solicitud y deberá conservarse como evidencia.
Especialista de Redes y Comunicaciones / Especialista de Sistemas de Información	3. Evalúa la solicitud según el ámbito de su competencia y verifica: a) Identidad del usuario y solicitante. b) Necesidad operativa y justificación. c) Correspondencia del privilegio con las funciones realizadas. d) Aplicación del principio de mínimo privilegio. e) Vigencia solicitada. f) Posibles conflictos de segregación de funciones. g) Criticidad del recurso sobre el cual se solicita el privilegio.
Jefe del Departamento de TIC	4. Evalúa la solicitud y determina su aprobación o rechazo. 5. En caso de aprobación, autoriza expresamente el nivel de privilegio y, cuando corresponda, su periodo de vigencia. 6. En caso de rechazo, comunica al solicitante el motivo de la denegatoria.
Especialista de Redes y Comunicaciones / Especialista de Sistemas de Información	7. Asigna el acceso privilegiado conforme al ámbito de su competencia y al nivel expresamente autorizado. 8. Cuando tecnológicamente resulte aplicable, la administración deberá efectuarse mediante cuentas nominativas diferenciadas de las cuentas utilizadas para actividades cotidianas. 9. Registra el acceso asignado en el formato S3.2.P2.F6 “Registro de Accesos Privilegiados” .
3.7.1. Accesos privilegiados temporales y de terceros	
Área Usuaria / Departamento de TIC	1. Los accesos privilegiados requeridos por personal externo, proveedores o terceros deberán estar debidamente justificados y autorizados, y limitarse exclusivamente a los recursos, funciones y actividades necesarias para la prestación del servicio o actividad autorizada.
Jefe del Departamento de TIC	2. Evalúa y aprueba, cuando corresponda, la asignación del acceso privilegiado, considerando el nivel de privilegio requerido y su periodo de vigencia.
Especialista de Redes y Comunicaciones / Especialista de Sistemas de Información	3. Los accesos privilegiados de carácter temporal, incluyendo los otorgados a terceros o proveedores para actividades específicas de soporte, mantenimiento, implementación o configuración, deberán contar con una fecha o periodo de vigencia determinado y ser retirados una vez concluida la actividad o vencido el plazo autorizado.

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	---

Ejecutor	Actividad
	4. La asignación, vigencia y posterior retiro del acceso deberán registrarse en el formato S3.2.P2.F6 “Registro de Accesos Privilegiados” , conservándose la evidencia correspondiente. 5. Cuando por razones técnicas u operativas se requiera mantener un acceso privilegiado de un tercero por un periodo prolongado, su necesidad deberá ser validada durante las revisiones periódicas de accesos privilegiados.
3.7.2. Revisión periódica de Accesos Privilegiados	
Especialista de Redes y Comunicaciones / Especialista de Sistemas de Información	1. Como mínimo trimestralmente, realiza la revisión de los accesos privilegiados correspondientes a los recursos TIC bajo su administración, utilizando el formato S3.2.P2.F6 “Registro de Accesos Privilegiados” . a) Vigencia del usuario o cuenta. b) Necesidad actual del privilegio. c) Correspondencia con las funciones asignadas. d) Nivel de privilegio concedido. e) Vigencia de la autorización. f) Cumplimiento del principio de mínimo privilegio. g) Existencia de privilegios innecesarios o incompatibles.
	2. El resultado deberá clasificarse, según corresponda, como: Mantener / Modificar / Suspender / Retirar.
Jefe del Departamento de TIC	3. Revisa los resultados de la evaluación periódica y dispone las acciones que correspondan respecto de los accesos identificados.
3.7.3. Modificación, suspensión o retiro de Accesos Privilegiados	
Gestión Humana / Área usuaria / DTIC	1. Comunica oportunamente los cambios que puedan modificar la necesidad del acceso privilegiado, incluyendo cambio de funciones, rotación, cese, finalización contractual o vencimiento de autorizaciones temporales.
Especialista de Redes y Comunicaciones / Especialista de Sistemas de Información	2. Procede a modificar, suspender o retirar el privilegio cuando: • desaparezca la necesidad operativa; • cambien las funciones del usuario; • finalice la relación laboral o contractual; • venza el período autorizado; • la revisión periódica determine que el privilegio no resulta necesario; • se identifique un riesgo o incidente de seguridad que requiera la revocación.
	3. La acción ejecutada deberá registrarse en el formato S3.2.P2.F6 “Registro de Acceso Privilegiado” , consignando la fecha, acción realizada y responsable de ejecución.

*Nota: La gestión de accesos privilegiados comprende, según corresponda:

- cuentas administrativas de sistemas operativos y servidores;
- grupos administrativos de dominio o directorio;
- administradores de dispositivos de comunicaciones y seguridad;
- roles administrativos de servicios y plataformas en nube;
- administradores de aplicaciones y sistemas de información;
- administradores y propietarios de sitios SharePoint;

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	---	---

- administradores de bases de datos;
- cuentas de servicio con privilegios elevados;
- accesos administrativos de terceros y proveedores;
- otros roles o perfiles con capacidad de administrar, configurar o modificar recursos TIC críticos.

4. ALCANCES FUNCIONALES

4.1. Gerente de Administración y Finanzas

- Aprobar el presente documento.

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

- Conducir el proceso de Gestión de Accesos, cumpliendo los plazos y las disposiciones previstas en los lineamientos de FONAFE, la norma ISO 27001, la normativa legal aplicable 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 su difusión.
- Evaluar y aprobar o rechazar solicitudes de acceso presentadas por las áreas usuarias conforme a lo establecido en el presente procedimiento.
- Evaluar y aprobar o rechazar las solicitudes de accesos privilegiados.
- Revisar los resultados de las evaluaciones periódicas de accesos privilegiados y disponer las acciones correspondientes.

4.3. Especialista en Redes y Comunicaciones

- Coordinar con el Especialista de Sistemas de Información para elaborar y elevar el presente documento a Jefe del Departamento de TIC.
- Cumplir con las actividades relacionadas al alta/baja de usuario y modificación de perfil señaladas en el presente documento.
- Coordinar con el Especialista de Sistemas de Información para monitorear los accesos de los usuarios.
- Verificar el cumplimiento de políticas y directivas de seguridad de la información en las solicitudes de exoneración de restricción de dispositivos de almacenamiento externo y desbloqueo de páginas web.
- Configurar el acceso a dispositivos de almacenamiento externo o páginas web, aplicando los controles de seguridad necesarios.
- Administrar los accesos privilegiados correspondientes a infraestructura tecnológica, servicios en nube, comunicaciones y demás recursos bajo su competencia.
- Mantener actualizado el Registro de Accesos Privilegiados correspondiente a los recursos bajo su administración y ejecutar su revisión periódica.
- Ejecutar la modificación, suspensión o retiro de privilegios cuando corresponda.
- Identificar oportunidades de actualización del procedimiento.

4.4. Especialista de Sistemas de Información

- Cumplir con las actividades relacionadas al acceso a aplicaciones señaladas en el presente documento.
- Administrar los accesos privilegiados de aplicaciones, sistemas de información y demás recursos bajo su competencia.
- Mantener actualizado el Registro de Accesos Privilegiados correspondiente y participar en su revisión periódica.
- Ejecutar la modificación, suspensión o retiro de los privilegios correspondientes a sistemas y aplicaciones.
- Identificar oportunidades de actualización del procedimiento.

4.5. Oficina de Gestión Humana

- Solicitar el alta y baja de usuarios de los colaboradores de la empresa.

	Procedimiento de Gestión de Accesos Procedimiento	Código: S3.2.P2 Versión: 05 Fecha: 06/10/2026
---	--	--

4.6. Área usuaria

- Solicitar el alta de usuario para personal externo que presta servicio a la empresa, así como el cambio de perfil del personal a su cargo.
- Solicitar la exoneración de restricciones de dispositivos de almacenamiento externo, así como el desbloqueo de páginas web.
- Comunicar cualquier cambio en las funciones, necesidad operativa o vigencia que pueda requerir la modificación o retiro de accesos privilegiados previamente solicitados.

4.7. Gerentes, Jefes o Supervisor de Área

- Validar las solicitudes de exoneración de restricción de dispositivos de almacenamiento externo y de desbloqueo de páginas web presentadas por el área usuaria.

5. REGISTROS / ANEXOS

- Formato S3.2.P2.F1 Solicitud de Alta, Baja de Usuario o Cambio de perfil.
- Formato S3.2.P2.F3 Exoneración de Restricción de TIC.
- Formato S3.2.P2.F5 Matriz de Perfiles de Usuario de Recursos TIC.
- Formato S3.2.P2.F6 Registro de Accesos Privilegiados.