PROCEDIMIENTO	Código: **S03.04.10.01**
	Versión: 01
	Vigencia:24/09/2025
Dueño del proceso: Oficina de Administración	

GESTIÓN DE ACCESO LOGICO A LOS SISTEMAS DE INFORMACIÓN

	Nombres y Apellidos	Cargo	Firma y Sello
Elaborado por:	Manuel Aguilar Cori	Oficial de Seguridad y Confianza Digital	Firmado digitalmente por: AGUILAR CORI Manuel Isidro FAU 20380799643 hard Fecha: 23/09/2025 15:16:57
	Víctor Chávez Gómez	Jefe del Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:36:12
Revisado por:	Apolinar Madrid Escobar	Jefe (dt) de la Oficina de Planeamiento y Presupuesto	Firmado digitalmente por: MADRID ESCOBAR Apolinar Junior FAU 20380799643 hard Fecha: 23/09/2025 16:39:51
Aprobado por:	Alberto Blas Ortiz	Jefe de la Oficina de Administración	

Versión	Descripción de Cambios	Fecha
01	Versión inicial	24/09/2025

1. BASE LEGAL

1.1. ISO/IEC 27001:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos” (en adelante ISO/IEC 27001).
1.2. NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos (en adelante NTP-ISO/IEC 27001).
1.3. ISO/IEC 27002 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante ISO/IEC 27002).
1.4. NTP-ISO/IEC 27002:2022 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante NTP-ISO/IEC 27002).
1.5. Versión Actualizada de la Directiva N° 02-2015-SERVIR/GPGSC Régimen Disciplinario y Procedimiento Sancionador de la Ley N° 30057, Ley del Servicio Civil.
1.6. Reglamento Interno de los Servidores Civiles - RIS de la Agencia de Promoción de la Inversión Privada – PROINVERSIÓN.
1.7. Código de Ética de la Agencia de la Promoción de la Inversión Privada PROINVERSIÓN.

2. DEFINICIONES Y SIGLAS

2.1. Definiciones

2.1.1. **Activo informático**: Cualquier tipo de hardware o software que forma parte de la plataforma tecnológica de la entidad incluyendo los sistemas informáticos o aplicativos desarrollados o adquiridos por la entidad

2.1.2. **Actualización:** Sustitución de una información contenida en un registro o archivo por otra más reciente.

2.1.3. **Área usuaria:** Dependencia que requiere la instalación de software o la adquisición de nuevo software o licencia.

2.1.4. **Ficha de usuario:** Ficha mediante la cual se crea, actualiza o desactiva la cuenta de usuario de red en el SIGA GESTOR.

2.1.5. **Usuario**: Es la persona que tiene asignado un equipo informático, cualquiera sea su condición contractual con PROINVERSION.

2.2. Siglas:

- CGTD: Comité de Gobierno y Transformación Digital.
- SGSI: Sistema de Gestión de Seguridad de la Información.
- OSCD: Oficial de Seguridad y Confianza Digital.

3. RESPONSABILIDADES

3.1. Del Especialista de Tecnologías de Información y Redes

3.1.1. Crear, modificar y suprimir acceso de usuarios a la red interna y correo electrónico de PROINVERSION.
3.1.2. Comunicar la creación, modificación y supresión de accesos otorgados.

3.2. Del Analista de Desarrollo y Portal Web

3.2.1. Crear, modificar y suprimir acceso de usuarios a los sistemas de PROINVERSION

3.3. Usuario interno de PROINVERSION

3.3.1. Verifica que las credenciales de acceso otorgadas sean las que se solicitaron

3.4. Usuario tercero

3.4.1. Personal externo de PROINVERSION a quien se le brinda accesos, se modifica y se restringe de acuerdo con las funciones realizadas

4. GENERALIDADES

4.1. Consideraciones importantes

4.1.1. Todo acceso a los equipos y servicios informáticos brindado a los usuarios debe contar previamente con la autorización del jefe o director de la unidad de organización. La autorización se realiza a través de la Ficha de usuario en el SIGA GESTOR.

4.1.2. Toda información obtenida, procesada y generada con fines institucionales es de propiedad exclusiva de PROINVERSIÓN.

4.1.3. Solo el personal encargado de la administración de copias de seguridad y el usuario responsable del mismo, pueden acceder y usar la información que está almacenada en los medios magnéticos u ópticos de respaldo.

4.1.4. El usuario es responsable directo de las acciones realizadas con los equipos y servicios informáticos que le hayan sido autorizados y asignados. En tal sentido, debe cumplir con las obligaciones de los usuarios listadas en el Anexo 4

4.1.5. El Área de TI debe informar trimestralmente sobre los accesos (altas y bajas) de los servicios informáticos al OSCD.

4.1.6. El Área de TI debe dar de baja a los accesos de los servicios informáticos de las personas que ya no cuentan con vínculo laboral o contractual con PROINVERSION, en coordinación con el Área de Personal o Logística, según corresponda

4.1.7. Para el acceso y uso adecuado de los equipos y servicios informáticos, se deben tener en cuenta las disposiciones generales establecidas en el Anexo 4 del presente documento

4.1.8. Para los usuarios con vínculo contractual, el acceso a los equipos y servicios informáticos debe encontrarse previsto en los Términos de Referencia.

4.2. Sobre los usos de servicios:

4.2.1. Uso del correo institucional

4.2.1.1. Para transmitir mensajes por correo electrónico institucional, únicamente se deben incluir a aquellas personas que, por naturaleza de su función, necesitan tomar conocimiento o tomar una acción respecto de la información comunicada.

4.2.1.2. El tráfico de envío y recepción de archivos adjuntos mediante correo electrónico institucional interna como externamente es de 25 MB, en caso dicho correo supere los 25 MB o sea enviado de forma masiva a los usuarios de la entidad, los archivos deberán enviarse a través de un enlace compartido mediante OneDrive o SharePoint de la plataforma Microsoft 365, a fin de no degradar el servicio y afectar a los demás usuarios de la red.

4.2.1.3. El uso de las opciones de confirmación de entrega y lectura deben restringirse a mensajes de alta importancia, a fin de evitar excesos de tráfico en la red.

4.2.1.4. En caso de que el usuario se encuentre fuera de la institución, puede acceder a su cuenta de correo electrónico mediante el acceso web; es importante que el usuario tenga en cuenta la seguridad y confiabilidad del equipo informático desde donde accede a fin de evitar que quede registrada la contraseña en el mismo.

4.2.1.5. Cuando un usuario deja de laborar o prestar servicios en PROINVERSION, se deshabilitará su cuenta de acceso a la red y correo electrónico.

4.2.2. Acceso y uso de la red

4.2.2.1. Los usuarios deben de tener acceso únicamente a la red y a servicios de red que hayan sido previamente autorizados.

4.2.2.2. Todo usuario de la red debe tener una cuenta única y personal con su respectivo nombre y contraseña que lo identifique en los servicios de red.

4.2.2.3. El resguardo de los archivos almacenados en los discos duros de cada computadora personal es de exclusiva responsabilidad del usuario.

4.2.3.Acceso y uso del internet

4.2.3.1. La Oficina de Administración, a través del Área de TI, se reserva el derecho de restringir o habilitar el acceso a determinados servicios de internet y páginas web, dependiendo del nivel de riesgo que dichos servicios significan para la infraestructura informática de la institución.

4.2.3.2. El director o jefe de la unidad de organización debe solicitar los accesos a los sitios de internet que se encuentren restringidos para los usuarios a cargo de su unidad, a través de un correo electrónico al Jefe de TI, quien debe evaluar si autoriza los accesos de dicha solicitud.

5. SECUENCIA DE ACTIVIDADES

Alta de usuarios

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Validar información			
1	Validar información ¿Información completa? Si: Ir a tarea 2 No: Terminar actividad	Área de TI	Especialista de Tecnologías de Información y Redes
2	Verificar tipo de usuario ¿Es usuario interno? Si: Ir a tarea 3 No: Ir a tarea 4	Área de TI	Especialista de Tecnologías de Información y Redes
Configurar acceso a la red y correo			
3	Configurar accesos de red y correo a personal interno	Área de TI	Especialista de Tecnologías de Información y Redes
4	Configurar accesos a red y correo a terceros	Área de TI	Especialista de Tecnologías de Información y Redes
5	Verificar habilitación de accesos en otros sistemas	Área de TI	Especialista de Tecnologías de Información y Redes
Validar credenciales de acceso a red y correo			
6	Comunicar de configuración de creación de accesos red y correo	Área de TI	Especialista de Tecnologías de Información y Redes
7	Validar credenciales otorgadas - interno	Áreas usuarias	Usuario interno PROINVERSION
8	Validar credenciales otorgadas - externo	Áreas usuarias	Usuario tercero

Configurar acceso a sistemas de información			
9	Verificar tipo de usuario para sistemas	Área de TI	Analista de Desarrollo y Portal Web
10	Configurar acceso a sistemas a usuario interno	Área de TI	Analista de Desarrollo y Portal Web
11	Configurar acceso a sistemas a usuario externo	Área de TI	Analista de Desarrollo y Portal Web
Validar credenciales de acceso a sistemas			
12	Comunicación de creación de usuarios a sistemas	Área de TI	Analista de Desarrollo y Portal Web
13	Validar credenciales a sistemas - interno	Áreas usuarias	Usuario interno PROINVERSION
14	Validar credenciales a sistemas - externo	Áreas usuarias	Usuario tercero
Cierre de requerimiento			
15	Atención de solicitud de acceso	Área de TI	Especialista de Tecnologías de Información y Redes
Fin			

Modificación de usuarios

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Validar información			
1	Validar información ¿Información completa? Si: Ir a tarea 2 No: Terminar actividad	Área de TI	Analista de Desarrollo y Portal Web
2	Seleccionar sistema al cual se modificará acceso de usuario	Área de TI	Analista de Desarrollo y Portal Web
Actualizar accesos en sistemas			
3	Actualizar perfil de acceso de usuario en sistemas	Área de TI	Analista de Desarrollo y Portal Web
Cierre de requerimiento			
4	Atención de solicitud de acceso	Área de TI	Analista de Desarrollo y Portal Web
Fin			

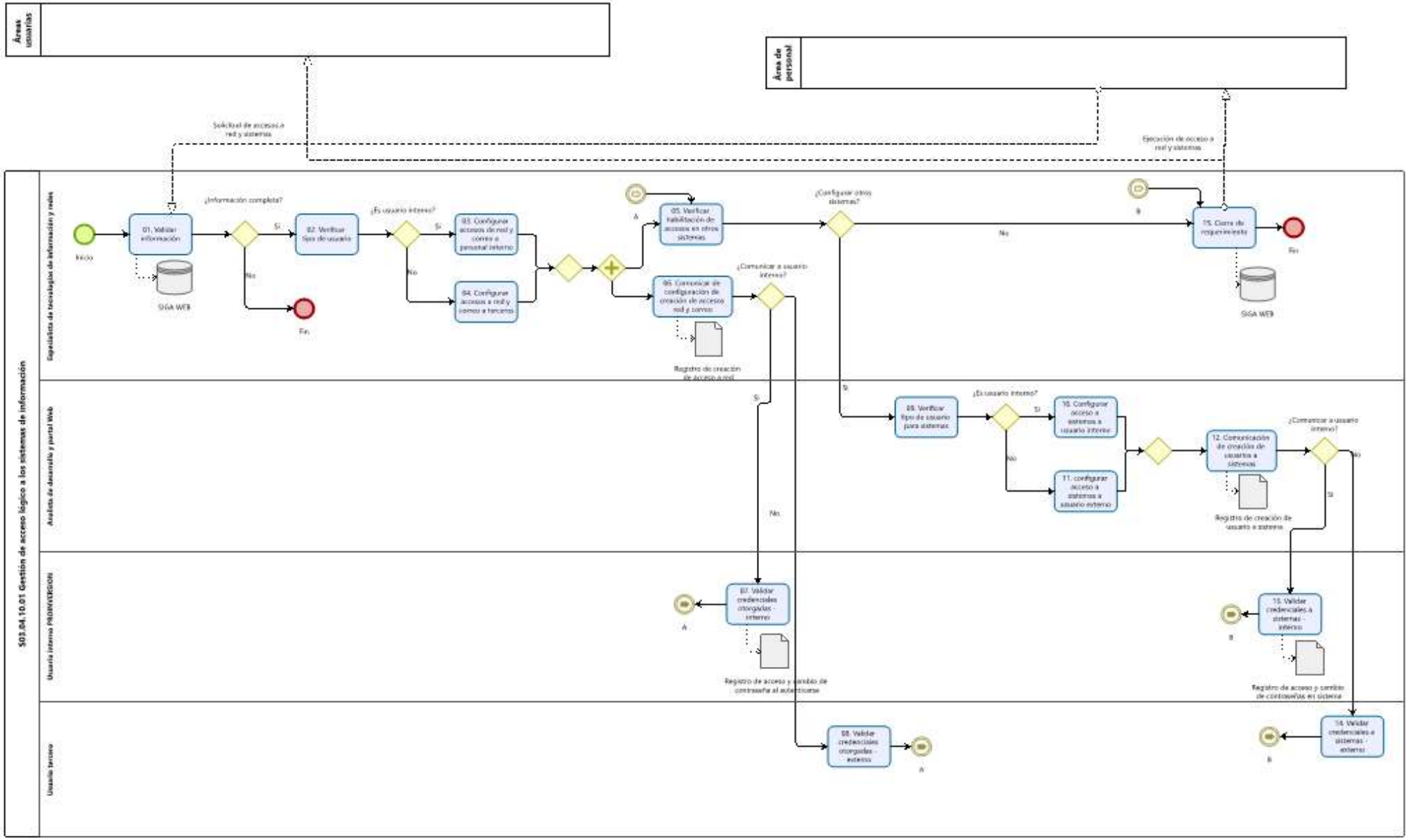
Baja de usuarios

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Validar información			
1	Validar información ¿Información completa? Si: Ir a tarea 2 No: Terminar actividad	Área de TI.	Especialista de Tecnologías de Información y Redes
2	Realizar backup de información de usuario	Área de TI.	Especialista de Tecnologías de Información y Redes
Configurar eliminación de accesos a sistemas			
3	Validar si el usuario tiene actividades pendientes en sistema	Área de TI.	Analista de Desarrollo y Portal Web
4	Eliminar cuenta de usuario en sistema	Área de TI.	Analista de Desarrollo y Portal Web
5	Coordinar cierre de actividades en sistemas	Área de TI.	Analista de Desarrollo y Portal Web
Configuración de eliminación de acceso a red y correo			
6	Configuración de eliminación de acceso a red y correo	Área de TI.	Especialista de Tecnologías de Información y Redes
Cierre de requerimiento			
7	Atención de solicitud de baja	Área de TI.	Especialista de Tecnologías de Información y Redes
Fin			

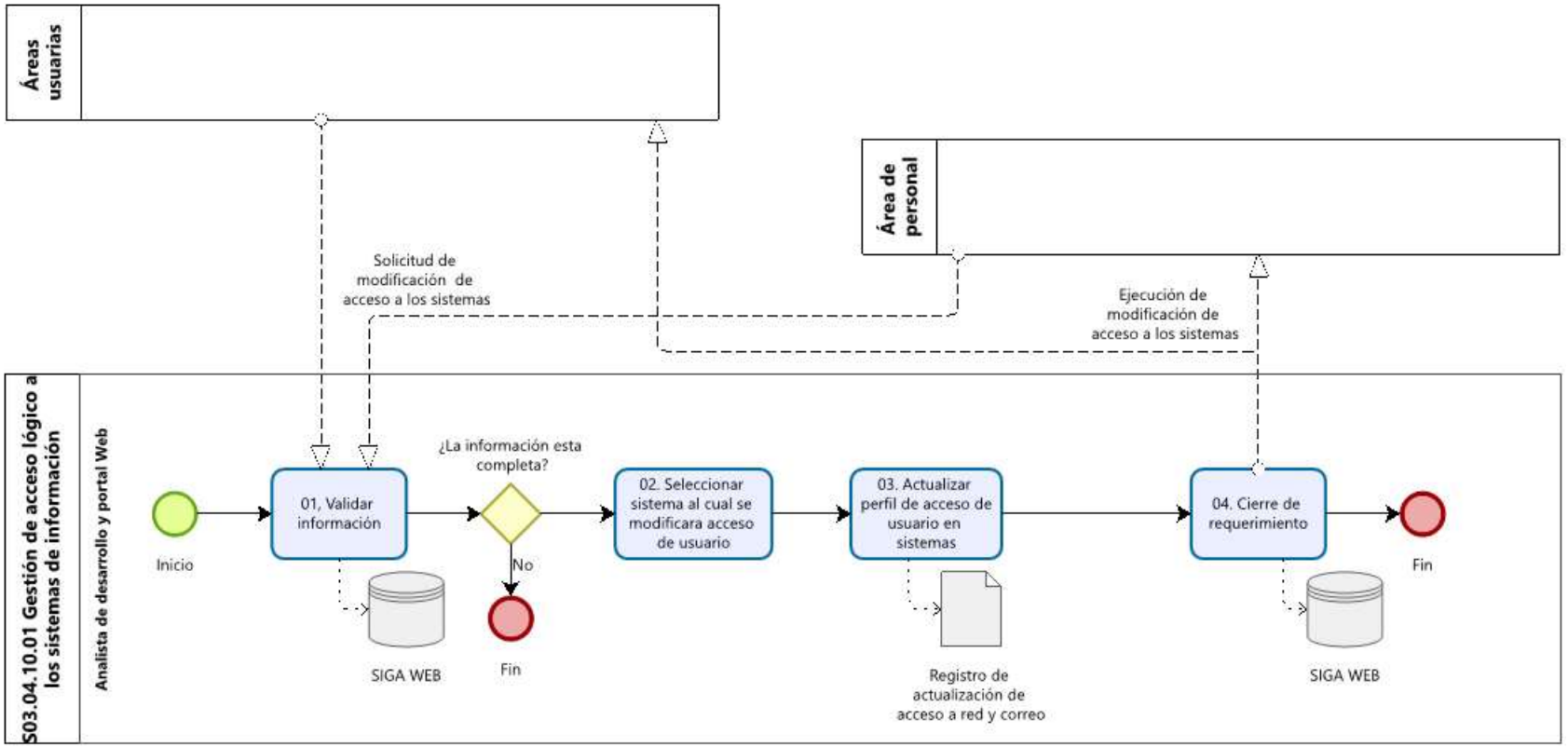
6. ANEXOS (Opcional)

6.1. Flujograma de procedimiento de acceso lógico a los sistemas de información - Alta
6.2. Flujograma de procedimiento de acceso lógico a los sistemas de información - Modificación
6.3. Flujograma de procedimiento de acceso lógico a los sistemas de información - Baja
6.4. Obligaciones de los usuarios

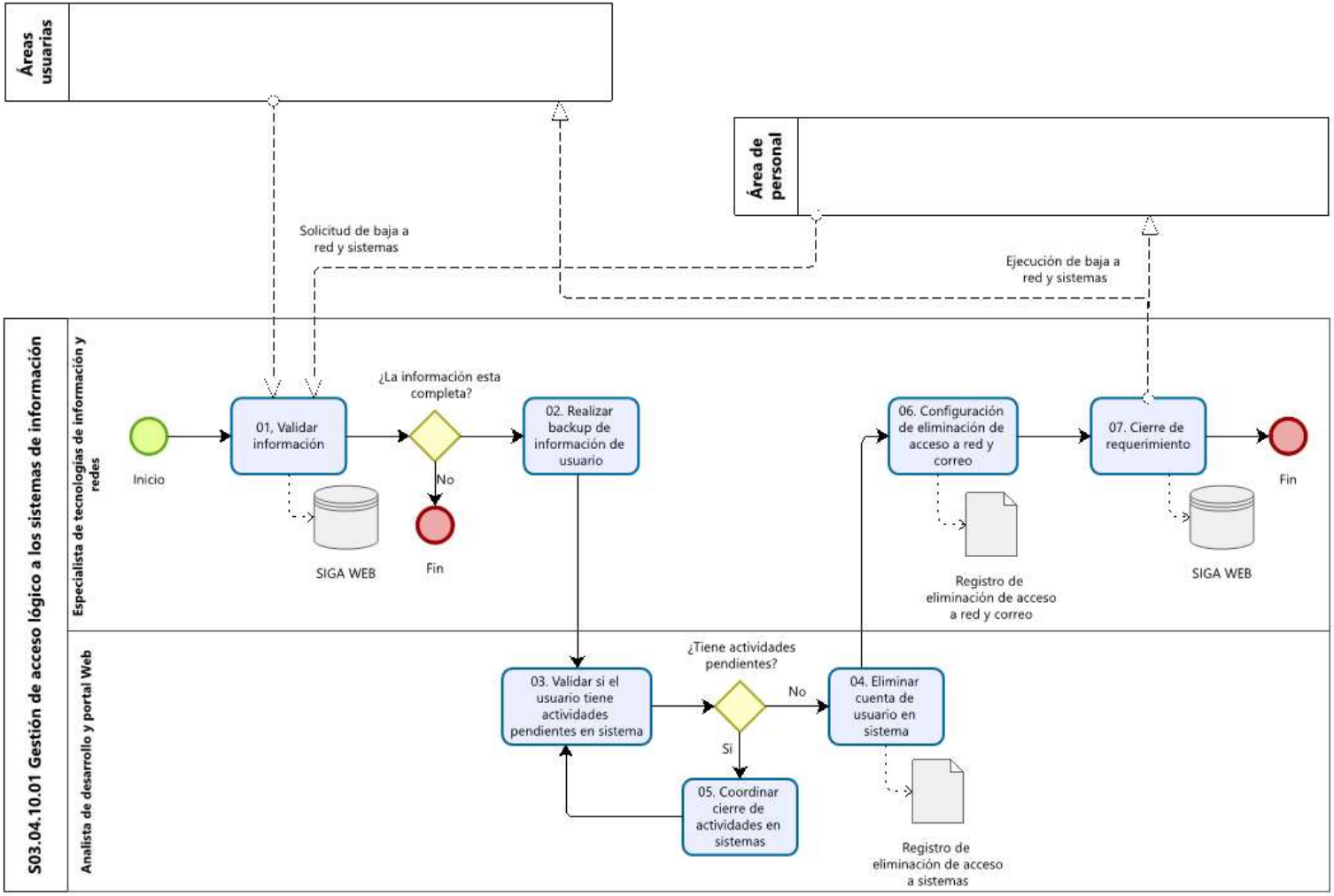
Anexo 1: Flujograma de procedimiento de gestión de acceso lógico a los sistemas de información - Alta



Anexo 2: Flujograma de procedimiento de gestión de acceso lógico a los sistemas de información – Modificación



Anexo 3: Flujograma de procedimiento de gestión de acceso lógico a los sistemas de información – Baja



ANEXO 4
OBLIGACIONES DE LOSUSUARIOS

Gestión de Contraseñas:

Mantener la confidencialidad de las contraseñas utilizadas para el acceso a los equipos y servicios informáticos y responder por cualquier mal uso de esta.

Cambiar de manera periódica -por lo menos cada tres (3) meses-, la contraseña de acceso a la red, evitar utilizar datos fácilmente deducibles. Para ello, utilizará aquellas contraseñas mayor o igual a 8 caracteres de longitud, que combinen caracteres alfanuméricos (números, mayúsculas, minúsculas y especiales: *, $, #, &).

Memorizar la contraseña de acceso a la red evitando dejarla por escrito en el escritorio, en los equipos de cómputo o computadora portátil.

Confidencialidad y Protección de Información:

Mantener en forma reservada la información que manejen a través de los equipos y servicios informáticos. En tal sentido, no deben divulgar o difundir información de propiedad de la entidad para fines ajenos a los institucionales.

Compartir información a través de las unidades de red institucional o grupal. (P, W u otra asignada).

Actualizar, depurar y organizar la información almacenada en la unidad de red asignada al usuario (X, W, P, etc.).

Sobre los Accesos:

No ingresar o intentar acceder al correo, red, carpetas compartidas, y/o sistemas de información a los cuales no estén autorizados.

No instalar dispositivos periféricos USB u otros no autorizados. Las excepciones deberán ser solicitadas por el jefe de la unidad de organización al Jefe del Área de TI.

No instalar hardware y/o software ni modificar la configuración de los equipos informáticos de la entidad.

Sobre las Conexiones:

No conectar equipos externos vía cables o de manera inalámbrica a la red de PROINVERSION, sin autorización del Jefe del Área de TI.

No cambiar de lugar el teléfono IP del punto de red asignado.

No conectar a la red telefónica equipos que no son propiedad y/o a cargo de PROINVERSION.

No instalar ningún tipo de dispositivo electrónico que pueda ser utilizado para almacenar o captar información de voz que pueda producirse por las conversaciones telefónicas en la entidad.