

Requerimiento funcional - Gestión de Identidades

Departamento de Seguridad Informática
Dirección Nacional de Tecnología
Enero 2024

Información del Documento

Resumen:	Este documento establece los requerimientos funcionales a ser implementados como parte de la adquisición de la solución de Gestión de Identidades.
Alcance del documento:	Definir los aspectos funcionales de la solución de Gestión de Identidades, y los flujos de aprobación de las operaciones de accesos lógicos a ser automatizadas.
Audiencia:	Departamento de Seguridad Informática, Departamento de Infraestructura y Operaciones, Dirección Nacional de Talento Humano.

Revisiones al Documento

Versión / Fecha	Persona	Rol	Descripción
1.0	Ing. Rafael Vintimilla	Gerente de Proyecto	Emisión inicial
1.1 / 15-07-2013	Ing. Miguel Venegas Ing. Xavier Freire Ing. Marcelo Suárez	Departamento de Seguridad Corporativa	Revisión Requerimiento Funcional
1.2 / 15-01-2024	Ing. David Mayorga	Coordinación de Seguridad Informática	Actualización de Requerimiento Funcional

Requerimiento funcional

Objetivos

- Integrar nuevas funcionalidades y requerimientos de automatización identificados como parte de la mejora continua del procedimiento de Accesos Lógicos para Usuarios Finales en el Sistema de Gestión de Identidades a adquirir.
- Corregir inconvenientes identificados en la actual solución de Gestión de Identidades para que no se presenten en la solución a adquirir.
- Disminuir el tiempo que deben dedicar los administradores del sistema actualmente implementado, debido a tareas que deben ser ejecutadas de manera manual.
- Mejorar la gestión del proceso de accesos lógicos en función de las necesidades de la Institución.

Alcance de la solución tecnológica

Dentro del Alcance

- Implementar una nueva solución de Gestión de Identidades en ambientes de desarrollo, certificación, producción y contingencia, para reemplazar la solución actual que dejó de tener soporte por parte del fabricante a partir de octubre de 2022.
- Parametrizar los flujos de trabajo definidos en este documento dentro de la nueva solución de Gestión de Identidades.
- Migrar la información de personas, identidades, roles y perfiles que al momento se alojan en la actual solución de Gestión de Identidades, a la nueva solución.

Requerimientos Generales

Entregable / Requerimiento	Funcionalidad
	Descripción de funcionalidad
Campos en la información de la persona.	<p>Los campos de información de las personas, a obtenerse desde el Sistema de Talento Humano, deben incluir:</p> <p>INFORMACION GENERAL:</p> <ul style="list-style-type: none"> • Cédula de Identidad • Nombres Completos • Primer Nombre • Segundo Nombre • Primer Apellido • Segundo Apellido • Fecha de ingreso • Tipo de Empleado (funcionario, pasante) <p>DETALLES DEL NEGOCIO:</p> <ul style="list-style-type: none"> • Código de Cargo • Nombre de Cargo • Código de Unidad Administrativa • Nombre de Unidad Administrativa • Dirección (Nacional / Zonal / Distrital) • Departamento

	<ul style="list-style-type: none"> • Coordinación <p>INFORMACION PERSONAL:</p> <ul style="list-style-type: none"> • Correo electrónico personal
<p>Trazabilidad en las operaciones de gestión de accesos.</p>	<p>La solución de Gestión de Identidades debe disponer de los registros de todas las solicitudes realizadas mediante el sistema con toda la información a detalle en cada una de ellas, así como el detalle de cada etapa de la transacción, sus aprobadores y el resultado de cada transacción.</p>
<p>Estructura organizativa del SRI.</p>	<p>En la solución de Gestión de Identidades, se debe poder crear y visualizar el árbol de la estructura organizativa del SRI, donde se incluyan al menos los siguientes campos:</p> <ul style="list-style-type: none"> • Nombre de la unidad administrativa • Código de la unidad administrativa • Código de la estructura organizacional (ADM) • Jefe de la unidad administrativa (Persona) • Dirección a la que pertenece (Nacional / Zonal / Distrital) • Provincia • Ciudad • Oficina • Unidad Organizativa del Directorio Activo asociada

Perfiles de notificación.	Se requiere la creación de los siguientes perfiles de notificación: <ul style="list-style-type: none">• Administrador de accesos• Ingresos• Movimientos• Bajas• Talento Humano Dirección Nacional• Talento Humano Zonal• Bienes Dirección Nacional• Bienes Zonal• Monitoreo Redes• Jefe• Redes• Mesa de Servicios• Persona interna• Persona externa• Pasante
Adjuntar archivos pdf.	En los flujos que correspondan, el usuario solicitante debe poder adjuntar uno o varios archivos de justificación (pdf) con capacidad máxima de hasta 5 MB cada uno.

<p>Integrar el proceso de actualización de Áreas de ADM dentro de los flujos.</p>	<p>Se requiere que en los flujos de ingresos, movimientos y bajas se realicen las tareas necesarias para la actualización de Áreas y Estructura Organizacional de ADM, según lo establecido en los flujos; esta actualización se debe ejecutar haciendo referencia a la Acción de Personal - APA específica sobre la que se está ejecutando el flujo.</p>
<p>Visualización de Perfiles y Roles del personal de cada unidad administrativa</p>	<p>Se requiere que dentro de la interfaz web de la solución de Gestión de Identidades, los jefes de cada unidad administrativa puedan visualizar los Perfiles y Roles asignados a las personas bajo su cargo y se pueda diferenciar en cada rol si proviene del perfil o es un rol asignado por excepción, y si son críticos o no.</p>
<p>Parametrización de los tiempos de espera en los flujos</p>	<p>Se requiere que los tiempos de espera en procesos de ejecución y de notificaciones de los flujos sean parametrizables por el administrador de la solución de Gestión de Identidades.</p>
<p>Sincronización automática en actualizaciones de identidades ADM</p>	<p>Se requiere que cualquier cambio en la información o asignación/revocatoria de roles relacionado a las identidades de ADM a través de la solución de Gestión de Identidades, sean sincronizados de manera automática con este sistema integrado.</p>
<p>Bajas de usuarios, temporal/definitivo</p>	<p>Se requiere que, al ser ejecutada una baja temporal o definitiva en el Sistema de Gestión de Identidades, todas las identidades, perfiles y roles asociados a la persona sean deshabilitadas temporal o definitivamente en ADM, según corresponda, de acuerdo con lo establecido en el flujo.</p>

<p>Generación automática de requerimientos o tickets.</p>	<p>La integración debe permitir la creación de requerimientos o tickets de manera automática en el sistema de requerimientos que utiliza actualmente el SRI, de acuerdo con lo establecido en los flujos correspondientes.</p>
<p>Disparador de los Flujos.</p>	<p>Los flujos de ingresos, movimientos y bajas de personal iniciarán de manera automática en función de las nuevas acciones de personal generadas en el sistema de Talento Humano, para esto el sistema de Gestión de Identidades deberá leer diariamente la tabla de acciones de personal en la base de datos del sistema de Talento Humano, la codificación de los diferentes tipos de acciones de personal y el tipo flujo que debe disparar cada una de ellas será entregada por el SRI.</p> <p>En función de la fecha “rige” que consta en las acciones de personal del sistema de Talento Humano, se dispararán los flujos de movimiento y baja. Para el flujo de ingresos este se ejecutará 1 día después de la fecha de registro de la acción de personal en el sistema de Talento Humano, sin tomar en cuenta la fecha “rige”.</p> <p>Se debe generar un proceso automático que lea las APAs todos los días (lunes a Domingo) a las 01:00 (am) y dispare los flujos correspondientes.</p> <p>En el sistema de Gestión de Identidades debe existir una tabla o matriz de acciones de personal, la cual debe ser parametrizable para futuros cambios en su codificación, descripción o flujo que debe disparar.</p>

Matriz aclaratoria de los flujos	Se requiere que el sistema de Gestión de Identidades cumpla con las actividades relacionadas en cada uno de los flujos del requerimiento funcional, en la matriz aclaratoria de cada flujo se especifican actividades que requieren un mayor detalle.
Delegación de funciones	<p>En el sistema de Gestión de Identidades deberá existir un mecanismo para que la jefatura de la unidad administrativa pueda delegar la gestión de los accesos a otra persona de su unidad para que pueda realizar al menos las siguientes actividades:</p> <ul style="list-style-type: none">• Solicitar roles o perfiles en nombre de la Jefatura ausente.• Iniciar flujos con el perfil de Jefatura.• Visualizar el estado de las solicitudes.• Cancelar o abortar solicitudes que no deben procesarse.
Notificaciones	<p>Las notificaciones serán personalizadas para cada uno de los flujos y la solución debe permitir que los textos puedan ser actualizados por el administrador sin que sea necesario reprogramar el flujo.</p> <p>Los campos y textos de las notificaciones de los flujos serán proporcionados por el SRI.</p> <p>Dentro de las notificaciones se debe mostrar una URL que al hacer click debe llevar al usuario directamente al menú en el cual se requiere su intervención o información que se requiera revisar.</p>

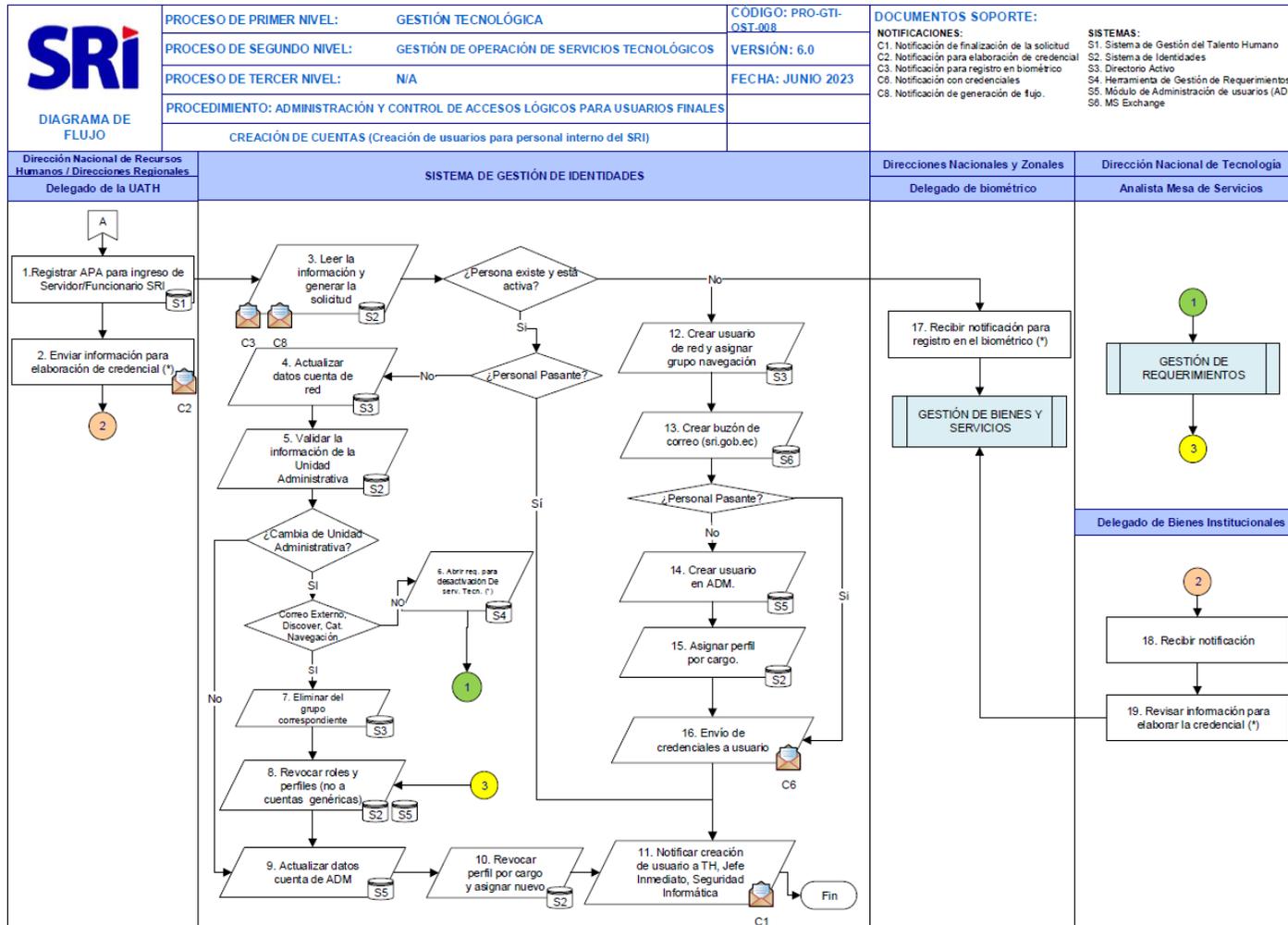
Notificaciones para aprobadores	El sistema de Gestión de Identidades debe enviar notificaciones periódicas a los aprobadores mientras se esté esperando por su interacción, el número de notificaciones debe ser parametrizable por el administrador.
Tiempo en solicitudes	Se requiere que para los flujos que dependen de un tiempo de espera o están esperando por la interacción de un aprobador, se considere días laborables para su ejecución.
Asignación de solicitudes de Gestión de Accesos	El sistema de Gestión de Identidades debe tener un mecanismo de asignación automática de las solicitudes a los aprobadores, para que no sea necesaria la asignación manual.
Justificación de Solicitudes	En los flujos de solicitud de accesos por parte de las jefaturas y en las aprobaciones de las solicitudes, los actores deben llenar un campo de justificación de los accesos solicitados, este campo debe ser obligatorio y el número de caracteres a ingresarse debe ser configurable para todos los flujos.
Creación de Cuentas de Usuarios	La creación de las identidades de las personas deberá ejecutarse de acuerdo con el estándar detallado en el Anexo 1 de este documento.
Buzones de correo electrónico	En los flujos donde exista la generación del buzón de correo estos siempre se deberán crear con el dominio @sri.gob.ec

Definición de Acción de Personal (APA): La acción de personal define el tipo de ingreso, movimiento o baja de personal y el sistema de gestión de identidades consulta la información de dichas acciones de personal en las tablas correspondientes en la base de datos del sistema de Talento Humano. Estas contienen la información de la situación actual y propuesta de la persona en función del ingreso, movimiento o baja. Para los ingresos se debe tomar la situación propuesta, para las bajas la situación actual y para los movimientos las dos.

Ejemplo de formato de notificación:

 <u>Datos de la persona creada:</u>	
Cédula de Identidad:	XXXXXXXXXXXXXX
Nombres y Apellidos:	XXXXXXXXXXXXXX
Cargo:	XXXXXXXXXXXXXX
Cuenta ADM:	XXXXXXXXXXXXXX
Cuenta Red:	XXXXXXXXXXXXXX
Unidad Administrativa:	XXXXXXXXXXXXXX
Departamento:	XXXXXXXXXXXXXX
Dirección:	XXXXXXXXXXXXXX
Jefatura Inmediata:	XXXXXXXXXXXXXX
Fecha de Ingreso:	XXXXXXXXXXXXXX
Ciudad:	XXXXXXXXXXXXXX
Oficina:	XXXXXXXXXXXXXX

1.- Creación de cuentas para personal interno del SRI



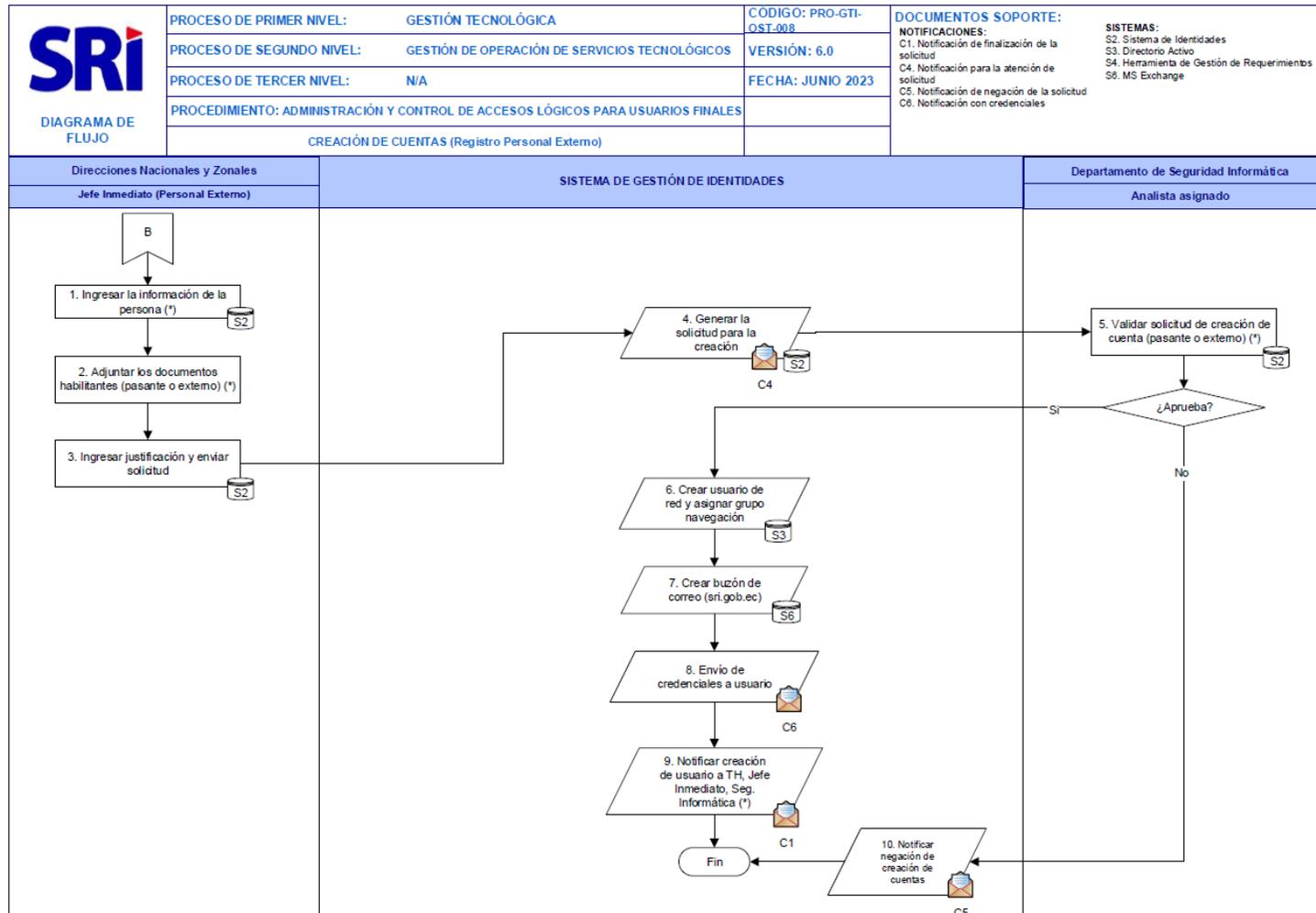
1.1.- Matriz Aclaratoria

No.	Actividad del Flujo	Instrucción Aclaratoria
Decisión	¿Tiene correo externo, discover, categoría de navegación?	<p>En el caso que cambie de unidad administrativa, debe consultar si la persona tiene activados alguno de estos servicios tecnológicos en los grupos correspondientes de Directorio Activo:</p> <ul style="list-style-type: none"> • Correo externo • Discover • Categoría de navegación diferente a la estándar.
6	Abrir requerimiento de desactivación de servicios tecnológicos	Se debe abrir un requerimiento para la desactivación de USB
7	Eliminar del grupo de AD correspondiente de los Serv. Tecn.	Eliminar al usuario de red del grupo de correo externo, discover y de todas las categorías de navegación, y agregar a la categoría de navegación estándar.
12	Crear usuario de red y asignar grupo de navegación	Se debe crear la cuenta de red con el algoritmo especificado en este documento y se debe agregar al usuario al grupo de categoría de navegación estándar.
16	Envío de credenciales a usuario	El Sistema de Gestión de Identidades debe enviar al correo electrónico personal las credenciales de sus identidades de red y ADM, no se debe copiar a nadie más este correo.
Proceso	GESTIÓN DE REQUERIMIENTOS	El Sistema de Gestión de Identidades genera requerimientos automáticos solicitando la desactivación de los servicios tecnológicos antes mencionados y los requerimientos son escalados al grupo correspondiente por parte de los actores de dicho proceso.

1.2.- Detalles funcionales del Flujo

Funcionalidad	Descripción
Ingreso de jefaturas	Cuando una persona ingresa a un puesto de jefatura se requiere: <ul style="list-style-type: none">• Se asignen automáticamente los perfiles propios del Sistema de Gestión de Identidades para que pueda tener acceso al sistema y gestionar los accesos de las personas a su cargo.• Se cambie automáticamente el jefe de todas las personas que pertenecen a la unidad administrativa correspondiente.
Ingreso de persona ya existente	En el caso de un APA que dispare el ingreso de una persona que ya existe en el sistema de Gestión de Identidades, se debe actualizar la información de persona en función de la situación propuesta de la acción de personal (APA); si no tiene cuentas, se deben crear. En el caso de que el servidor disponga de cuentas activas, el Sistema de Gestión de Identidades deberá validar automáticamente si cambia de unidad administrativa.
Ingresos sin situación Propuesta.	En el caso de existir un APA de ingreso sin situación propuesta como es el caso de las reactivaciones de usuarios, el sistema de Gestión de Identidades deberá tener un mecanismo para tomar la información de la situación actual del APA en lugar de la propuesta.

2.- Creación de cuentas para personal externo



2.1.- Matriz Aclaratoria

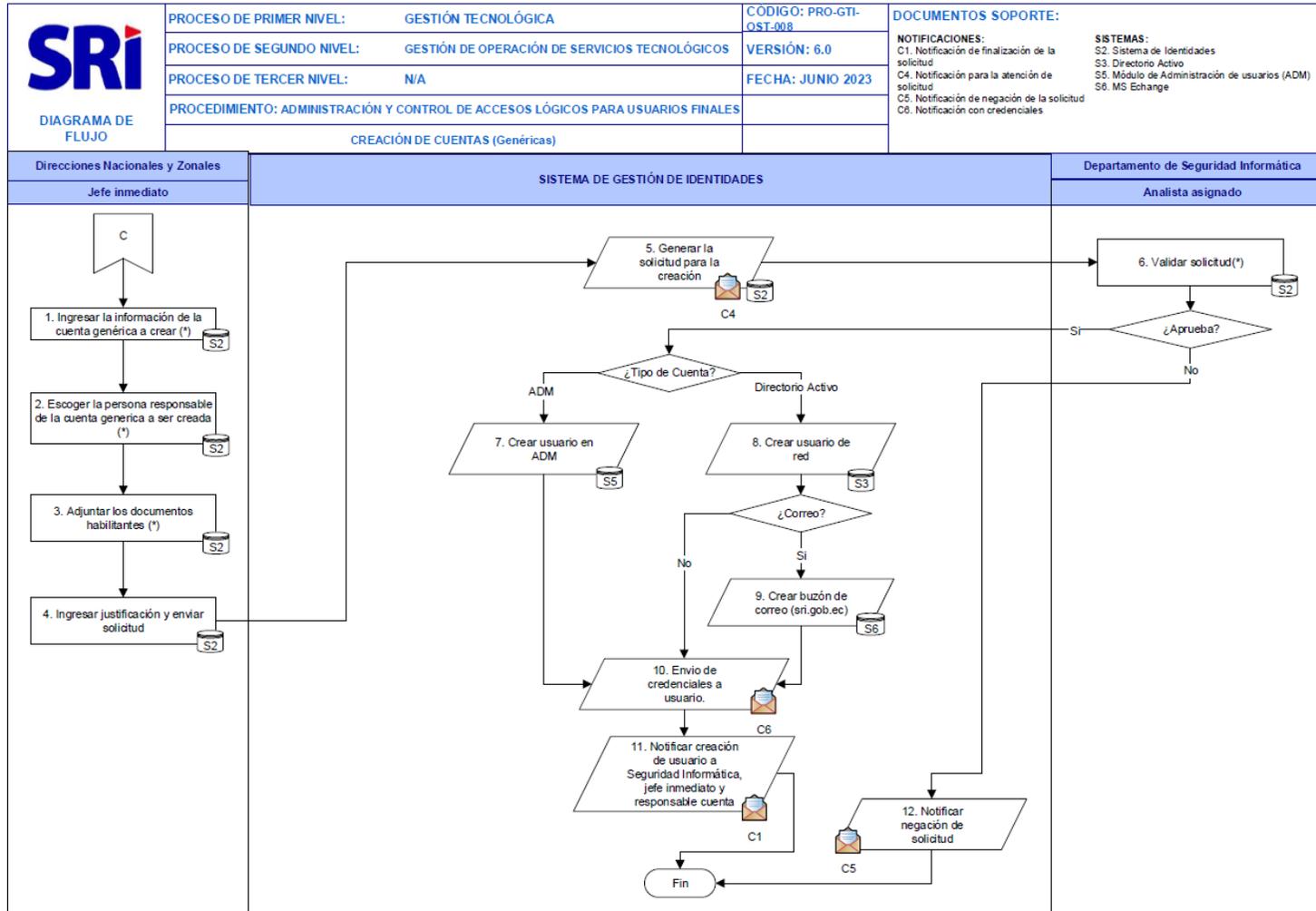
No.	Actividad del Flujo	Instrucción Aclaratoria
5	Validar solicitud de creación de cuentas	Debe permitir aprobar o rechazar la solicitud, de acuerdo con el análisis del especialista asignado sobre los adjuntos cargados y la justificación ingresada
6	Crear usuario de red y asignar grupo de navegación	Debe crear la cuenta de red y agregarla al grupo de categoría de navegación estándar.

2.2.- Detalles funcionales del Flujo.

Funcionalidad	Descripción
Ingreso de solicitud	<p>El sistema deberá presentar una primera pantalla con un formulario de datos a ingresar, se requiere que los campos obligatorios a ingresar sean los siguientes:</p> <ul style="list-style-type: none"> • Cedula de identidad • Fecha de ingreso (Fecha Inicio) • Fecha de terminación (Fecha Fin) • Apellidos y Nombres • Unidad administrativa responsable • Organización a la que pertenece

	<ul style="list-style-type: none"> • Correo electrónico personal <p>Los siguientes campos deben asignarse al personal externo automáticamente en función de la unidad administrativa responsable seleccionada:</p> <ul style="list-style-type: none"> • Nombres y apellidos de la jefatura de la unidad administrativa • Dirección • Departamento • Coordinación • Provincia • Ciudad • Oficina
<p>Fechas de vigencia</p>	<p>La fecha de inicio no puede ser anterior a la fecha actual. La fecha fin será periódicamente revisada por el Sistema de Gestión de Identidades y disparará el flujo de Bajas (Externo) en la fecha que corresponda.</p>

3.- Creación de Cuentas Genéricas



3.1.- Matriz Aclaratoria

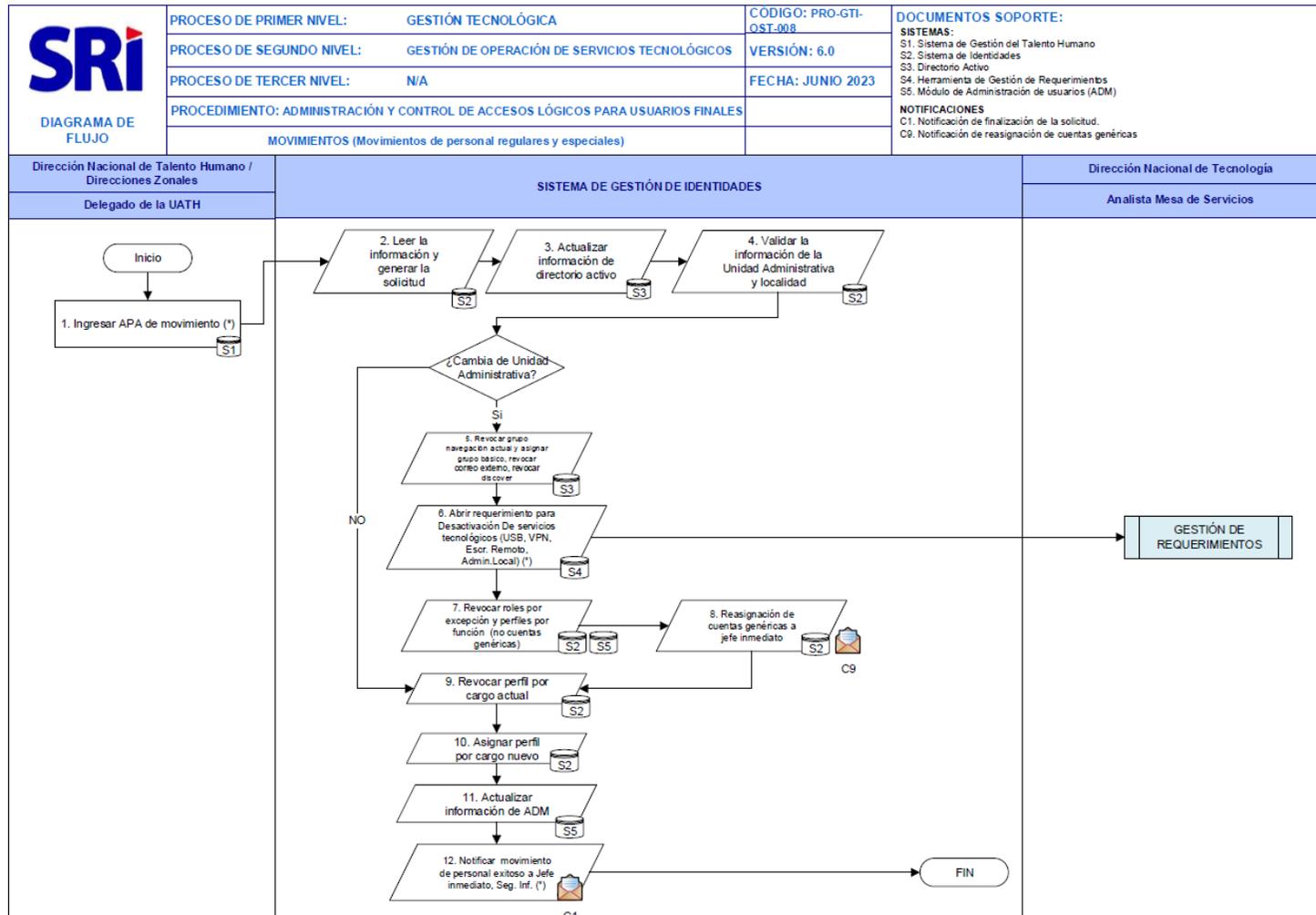
No.	Actividad del Flujo	Instrucción Aclaratoria
1	Ingresar información de la cuenta genérica a crear	Las cuentas genéricas deben tener obligatoriamente el prefijo “gen_” y se completa con el nombre que ingrese el usuario, por ejemplo: gen_ventanilla
6	Validar solicitud	Debe permitir aprobar o rechazar la solicitud, de acuerdo con el análisis del especialista asignado sobre los adjuntos cargados y la justificación ingresada.
8	Crear usuario de red	Todas las cuentas genéricas de red se crearán dentro de una Unidad Organizacional definida por el administrador del Directorio Activo.

3.2.- Detalles funcionales del Flujo

Funcionalidad	Descripción
Ingresar la información de la cuenta genérica a crear	El sistema deberá presentar una primera pantalla con un formulario de datos a ingresar, se requiere que los campos obligatorios a ingresar sean los siguientes: <ul style="list-style-type: none"> • Tipo de cuenta: ADM o red • Nombre de visualización de la cuenta (p.e.:Ventanilla Virtual) (solo en caso de escoger cuenta de red) • Nombre de la cuenta (p.e.: gen_ventanilla) • Crear buzón de correo (Solo en caso de escoger cuenta de red)

<p>Escoger la persona responsable de la cuenta genérica a ser creada</p>	<p>Se debe poder escoger la persona responsable de la cuenta genérica, entre las personas que están dentro de la unidad administrativa del jefe que realiza la solicitud.</p> <p>Los siguientes datos se asignan a la cuenta automáticamente en función del responsable seleccionado:</p> <ul style="list-style-type: none">• Cédula de Identidad del responsable• Apellidos y Nombres• Dirección• Departamento• Coordinación• Provincia• Ciudad• Oficina
--	--

4.- Movimientos de Personal



4.1.- Matriz Aclaratoria

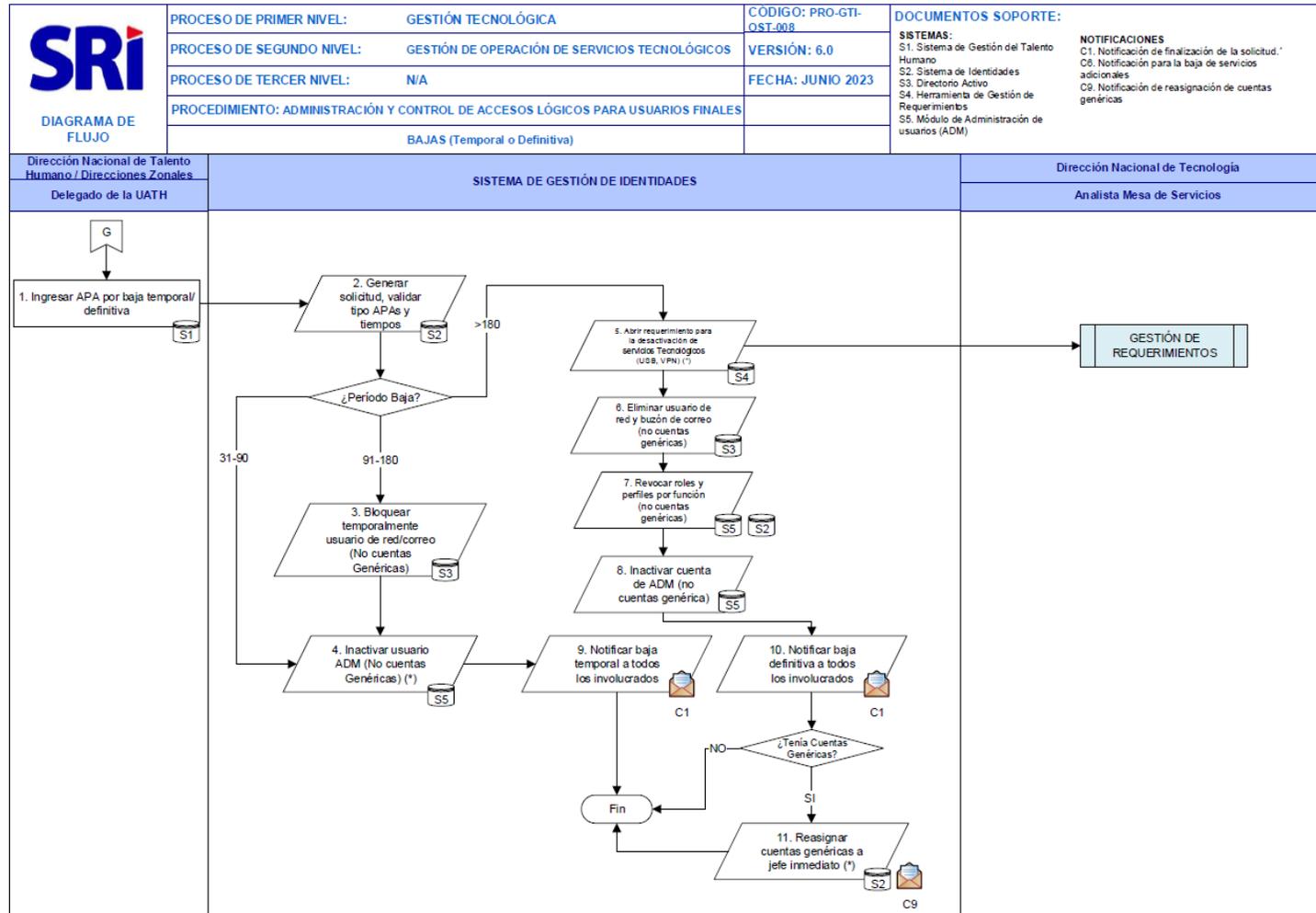
No.	Actividad del Flujo	Instrucción Aclaratoria
5	Revocar grupo de navegación actual y asignar	Se debe validar la unidad administrativa propuesta para saber
Decisión	¿Cambia de Unidad Administrativa?	Se debe ejecutar el requerimiento de cambio administrativo.
5	Notificar Movimiento de personal	Cuando exista movimiento físico en paralelo al envío de generar un requerimiento automático para actualización de buzón y configuración de PC, debe llegar una notificación a fin de que instruya al Jefe Inmediato propuesto que no se puede solicitar nuevos perfiles / roles hasta que no sea finalizado el movimiento.
8	Abrir requerimiento para actualización de buzón y configuración de PC	El Sistema de Gestión de Identidades debe generar un requerimiento automático solicitando validar, crear y configurar los buzones de correo electrónico de ser necesario, correspondiente a los servidores que sean objeto de un movimiento de personal.
9	Abrir requerimiento para la desactivación de servicios adicionales	El Sistema de Gestión de Identidades debe generar una solicitud en el Módulo de Requerimientos solicitando la revocatoria de los accesos de la persona por cambios, se requiere que se gestione la baja de servicios adicionales como: accesos USB, permisos de Firewall, Acceso VPN, licencia PGP, licencias Microsoft, reserva de direcciones IP, correo externo, internet, módem de navegación.
11	Notificar a todos los involucrados el movimiento de personal	Se debe notificar a los actores involucrados en el flujo, que fueron revocados los Perfiles Básicos Institucionales o roles por excepción que tenía el servidor que tuvo el cambio o movimiento de personal, caso contrario notificar solamente que fue finalizado el cambio / movimiento de personal.

4.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Tarea de inicio para Movimientos Especiales	Para movimientos especiales el flujo no inicia con una acción de personal, en su lugar el perfil de Recursos Humanos debe tener una opción en el Sistema de Gestión de Identidades para escoger a la persona sobre la cual se inicie el flujo. (Los movimientos especiales son movimientos que se ejecutan sin que exista una acción de personal)
Situaciones Actual y Propuesta Movimientos Especiales.	Para los movimientos especiales, al no existir una acción de personal que inicie el flujo, la situación actual será tomada de los datos de la persona en el Sistema de Gestión de Identidades, y la situación propuesta será tomada de los datos de la persona en el sistema de Recursos Humanos al momento de iniciar el flujo.
Movimientos sin situación Propuesta	En el caso de existir una acción de personal (APA) sin situación propuesta, el Sistema de Gestión de Identidades deberá tomar la información de la situación actual del APA como propuesta esta acción depende del código del APA.
Movimiento a un puesto de Jefatura	Cuando una persona se mueve a un puesto de jefatura se requiere: <ul style="list-style-type: none"> • Se asignen automáticamente los perfiles dentro del Sistema de Gestión de Identidades para que pueda cumplir las tareas de Jefe. • Se actualice automáticamente el Jefe de todas las personas que pertenecen a la Unidad Administrativa correspondiente.
Movimiento desde un puesto de Jefatura	Cuando la persona que se mueve deja un puesto de Jefatura, debe quitársele automáticamente los perfiles de jefe en los flujos de aprovisionamiento. Además se debe notificar que se ha ejecutado un movimiento de Jefatura al perfil de Administrador de accesos.
No incluir cuentas genéricas en la eliminación de roles de	Se requiere que en la tarea de revocatoria de perfiles y roles de ADM no se incluyan las cuentas genéricas que tiene a su cargo el servidor.

ADM	
Personas con más de una cuenta de ADM.	En el caso de que el servidor objeto del movimiento tenga más de una cuenta de ADM (sin tomar en cuenta genéricas), se deberán revocar todos los perfiles y roles de todas las cuentas y además se deberán, revocar y desconectar las cuentas cuyo ID sea diferente al identificador de red de Active Directory.
Integración con el Módulo de requerimientos	<p>Debe existir una integración automática con el Módulo de Requerimientos, de tal forma que el Sistema de Gestión de Identidades genere los tickets/solicitudes hacia el Módulo de Requerimientos con toda la información necesaria para que se pueda gestionar la actualización del buzón de correo, configuración de PC y solicitud de desactivación de servicios adicionales según corresponda.</p> <p>NOTA: Los servicios adicionales se refiere a: accesos USB, permisos de Firewall, Acceso VPN, licencia PGP, licencias Microsoft, reserva de direcciones IP, correo externo, internet, módem de navegación.</p>

5.- Bajas Temporales o Definitivas



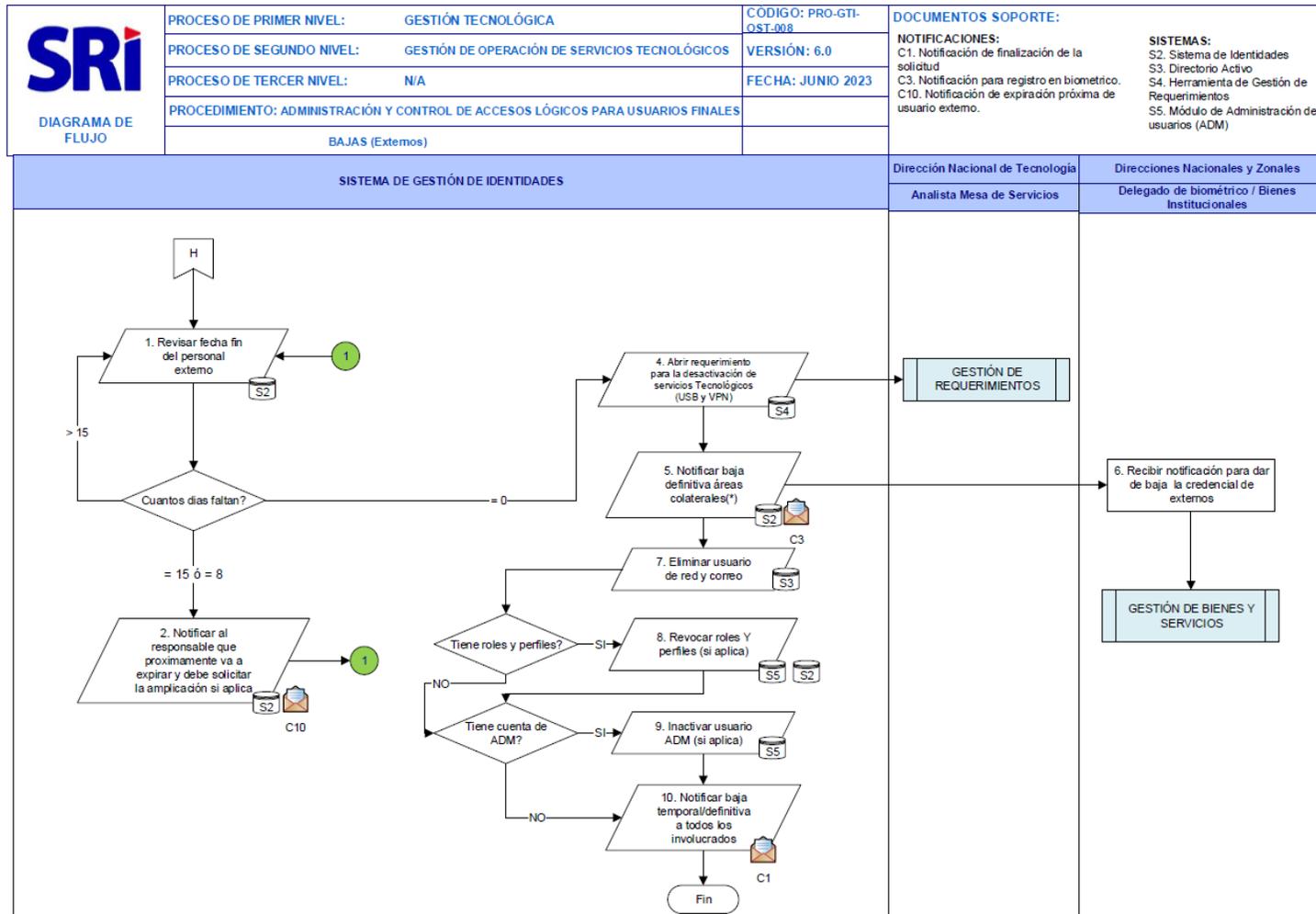
5.1.- Matriz Aclaratoria

No.	Actividad del Flujo	Instrucción Aclaratoria
Decisión	¿Periodo baja?	<p>Quando un funcionario se ausente de forma temporal por un período de 31 a 90 días se procede a la suspensión temporal de la cuenta de ADM (excepto cuentas genéricas de este sistema).</p> <p>Quando un funcionario se ausente de forma temporal por un período de 91 a 180 días se procede a la suspensión temporal de las cuentas de red y ADM.</p> <p>Quando un funcionario se ausente por un período mayor a 181 días, sea por salida temporal o definitiva, se procede con la eliminación de la cuenta de red (excepto cuentas genéricas de este sistema), eliminación del buzón de correo, revocatoria de perfiles y roles por excepción y posteriormente la inactivación de la cuenta de ADM.</p> <p>El Sistema de Gestión de Identidades valida el período de baja y la fecha de inicio y fin de la, una vez cumplido el período de baja y llegada la fecha de fin se activa automáticamente las cuentas desactivadas temporalmente (en el caso de bajas entre 31 y 180 días).</p>
Decisión	¿Tenía cuentas genéricas?	<p>El sistema debe validar si el usuario tiene cuentas genéricas (ADM y Directorio Activo), de ser así las debe reasignar al jefe inmediato.</p>

5.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
No incluir cuentas genéricas en la suspensión / eliminación.	Se requiere que en las tareas de suspensión o eliminación de cuentas de Directorio Activo y de ADM no se incluyan las cuentas genéricas que tiene a su cargo el funcionario.
Personas con más de una cuenta de ADM	En el caso de que el servidor objeto de baja definitiva tenga más de una cuenta en ADM (Sin tomar en consideración cuentas genéricas), se deberá revocar todos los perfiles y roles asignados e inactivar todas las cuentas de ADM.
Baja de usuarios temporal / definitivo	Se requiere que al ser ejecutada una baja temporal / definitiva en el Sistema de Gestión de Identidades, todas las cuentas asociadas al usuario (excepto genéricas) sean suspendidas / inactivadas según corresponda en el flujo, y la persona se revocada en el sistema de Gestión de Identidades.

6.- Bajas de Personal Externo



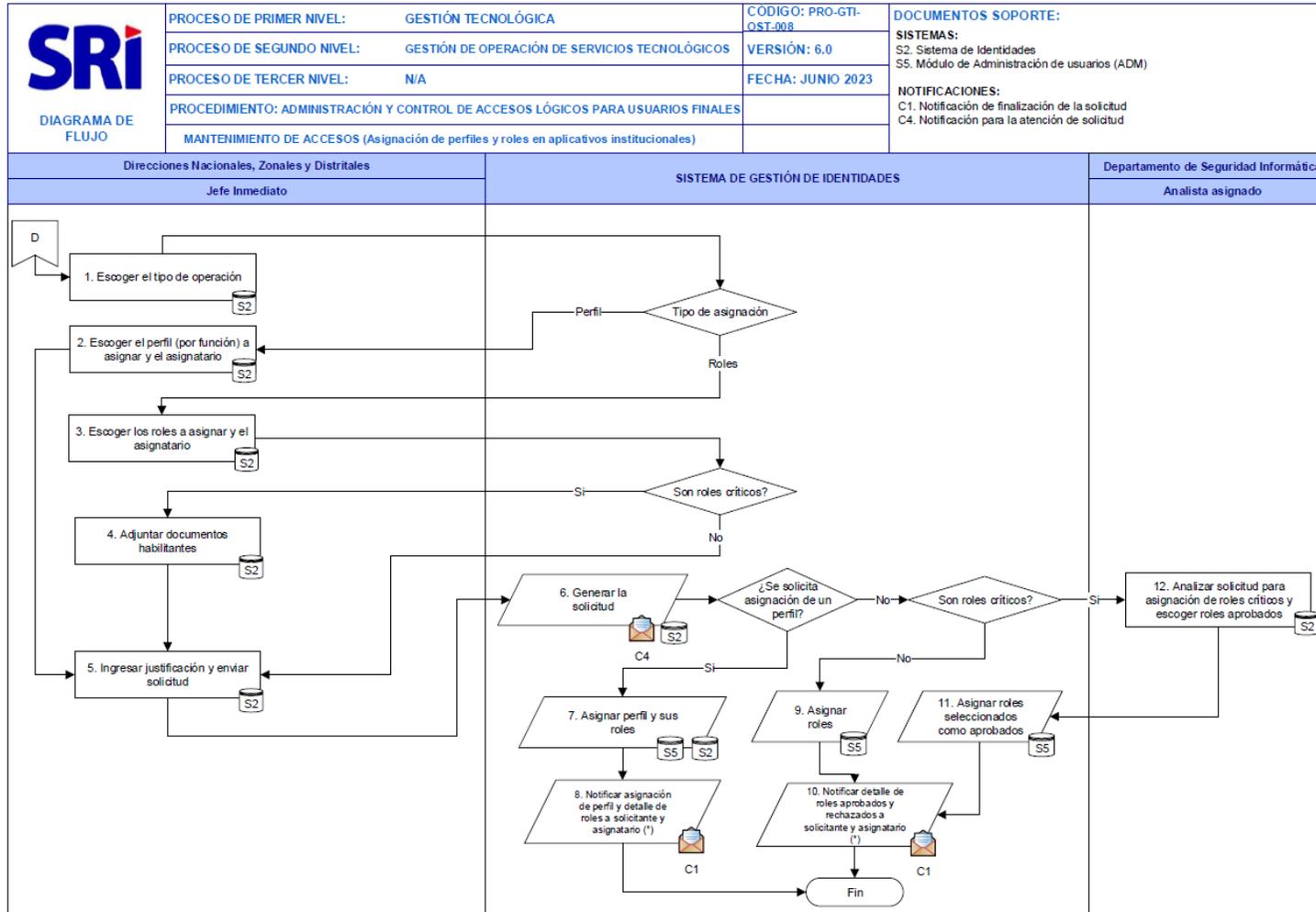
6.1.- Matriz Aclaratoria

No.	Actividad del Flujo	Instrucción Aclaratoria
1	Revisar fecha fin del personal externo	<p>El Sistema de Gestión de Identidades deberá correr un proceso diario que valide la fecha fin del personal externo:</p> <ul style="list-style-type: none"> • En caso de que falten más de 15 días para la fecha fin el proceso volverá a ejecutarse al día siguiente. • En caso de que falten 15 días para la fecha fin se enviara un correo electrónico al responsable de la cuenta a manera de recordatorio advirtiéndole que próximamente la cuenta va a expirar y debe solicitar su ampliación (si aplica). • En caso de que falten 8 días para la fecha fin se enviara un correo electrónico al responsable de la cuenta a manera de segundo recordatorio advirtiéndole que próximamente la cuenta va a expirar y debe solicitar su ampliación (si aplica). • En caso de que llegue la fecha fin se ejecutará el proceso de baja del personal externo.

6.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Revisión de la fecha fin del personal externo	El Sistema de Gestión de Identidades deberá correr un proceso diario que valide la fecha fin del personal externo.

7.- Asignación de Perfiles y Roles en Aplicativos Institucionales



7.1.- Matriz Aclaratoria

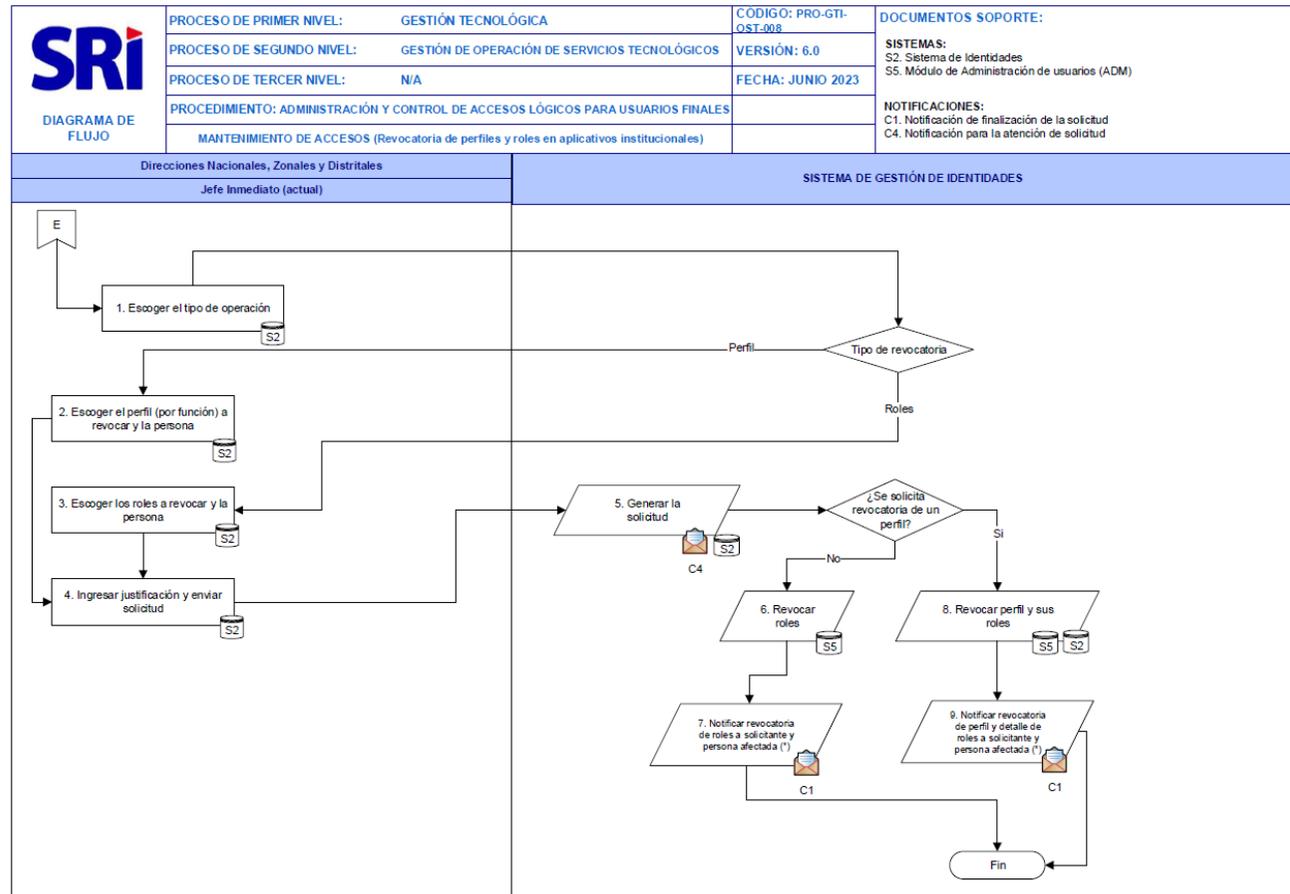
No.	Actividad del Flujo	Instrucción Aclaratoria
1	Escoger tipo de operación.	La jefatura debe escoger si lo que quiere es asignar roles o perfiles.
2	Escoger el perfil (por función) a asignar y el asignatario.	Los perfiles que se les va a presentar son los perfiles por función que pertenecen a su unidad administrativa y también el listado de personas en esa unidad administrativa.
3	Escoger los roles a asignar y el asignatario.	La jefatura debe escoger los roles a asignar y la persona a la que se solicita realizar dicha operación, el listado de personas de las que se podrá escoger son los que están dentro de la unidad administrativa a la que pertenece la jefatura solicitante.
4	Adjuntar documentos habilitantes.	En caso de que en el paso 3 se hayan escogido roles críticos se debe adjuntar los documentos de autorización en pdf.
11	Analizar solicitud para asignación de roles críticos y escoger roles aprobados	El aprobador debe analizar los documentos adjuntos que sustenten todos los roles críticos solicitados, deberá seleccionar únicamente como aprobados los roles solicitados que cumplan con los requisitos establecidos.
12	Asignar roles seleccionados como aprobados	El sistema de Gestión de Identidades deberá asignar únicamente los roles seleccionados como aprobados previamente por el aprobador en el paso 11.

7.2.- Detalles funcionales del Flujo

Funcionalidad	Descripción
Escoger el tipo de operación.	Se requiere que el sistema de Gestión de Identidades muestre una pantalla que permita al jefe solicitante escoger entre las siguientes opciones: <ul style="list-style-type: none"> • Asignación de Perfiles • Asignación de roles
Escoger el perfil (por función) a asignar y el asignatario.	Si el jefe escogió la operación de asignación de perfiles, se debe mostrar una pantalla con el listado de las personas bajo su cargo en su unidad administrativa, una vez escogida la persona (solo se puede escoger una) se debe mostrar el listado de perfiles que tiene asignados al momento y en otra sección los perfiles que no tiene asignados y están disponibles en su unidad administrativa, con su codificación, nombre y descripción. El jefe debe seleccionar uno o mas perfiles para la asignación.
Escoger los roles a asignar y el asignatario.	Si el jefe escogió la operación de asignación de roles, se debe mostrar una pantalla con el listado de las personas bajo su cargo en su unidad administrativa, una vez escogida la persona (solo se puede escoger una) se debe mostrar el listado de roles que tiene asignados al momento y en otra sección los roles que no tiene asignados y están disponibles para asignación, divididos en críticos y no críticos, y que muestre al menos la siguiente información: <ul style="list-style-type: none"> • Código de aplicación • Nombre de aplicación • Código de módulo • Nombre de módulo

	<ul style="list-style-type: none"> • Nombre de rol • Descripción del rol <p>El listado de aplicativos, roles y descripciones debe ser tomado de la base de datos de ADM.</p> <p>El jefe debe seleccionar uno o más roles para la asignación.</p>
<p>Adjuntar documentos habilitantes</p>	<p>Si el jefe seleccionó uno o varios roles críticos debe mostrar una pantalla para poder subir archivos pdf con las autorizaciones correspondientes, de acuerdo con el siguiente detalle:</p> <ul style="list-style-type: none"> • 1 campo para subir el certificado de antecedentes penales. • 1 campo para subir el record crediticio. • 1 campo para subir las autorizaciones de los responsables de aplicativos.
<p>Asignar roles seleccionados como aprobados</p>	<p>Se deben asignar únicamente los roles críticos seleccionados en el análisis de la solicitud por parte del aprobador, y adicional todos los roles no críticos solicitados.</p>

8.- Revocatoria de Perfiles y Roles en Aplicativos Institucionales



8.1.- Matriz Aclaratoria

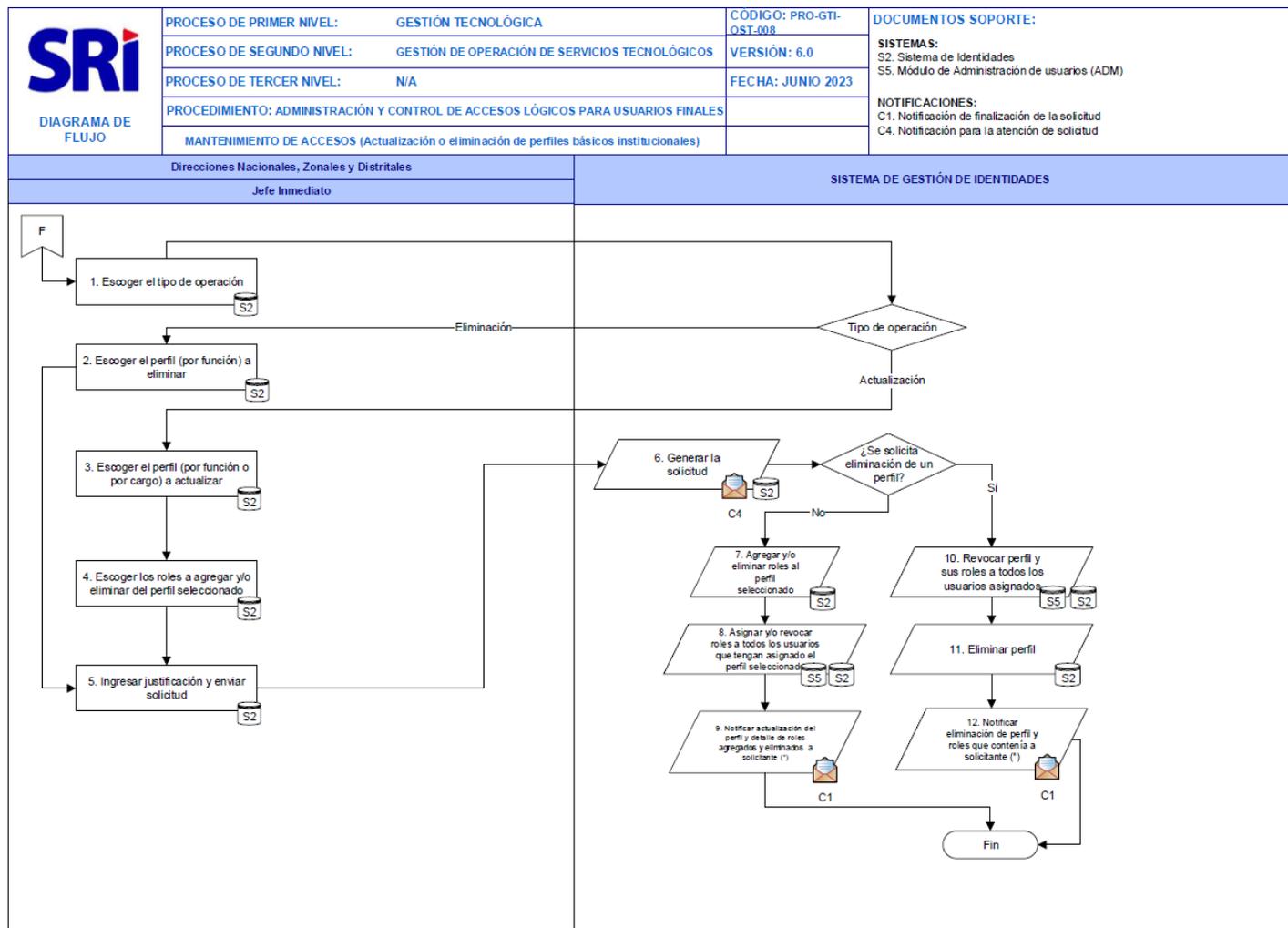
No.	Actividad del Flujo	Instrucción Aclaratoria
1	Escoger el tipo de operación.	La jefatura debe escoger si lo que quiere es revocar roles o perfiles.
2	Escoger el perfil (por función) a revocar y el asignatario.	Los perfiles que se les va a presentar son los perfiles por función que pertenecen a su unidad administrativa y también el listado de personas en esa unidad administrativa.
3	Escoger los roles a revocar y el asignatario.	La jefatura debe escoger los roles a revocar y la persona a la que se solicita realizar dicha operación, el listado de personas de las que se podrá escoger son los que están dentro de la unidad administrativa a la que pertenece la jefatura solicitante.

8.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Escoger el tipo de operación.	Se requiere que el sistema de Gestión de Identidades muestre una pantalla que permita al jefe solicitante escoger entre las siguientes opciones: <ul style="list-style-type: none"> • Revocatoria de Perfiles • Revocatoria de roles
Escoger el perfil (por función) a revocar y el asignatario.	Si el jefe escogió la operación de revocatoria de perfiles, se debe mostrar una pantalla con el listado de las personas bajo su cargo en su unidad administrativa, una vez escogida la persona

	<p>(solo se puede escoger una) se debe mostrar el listado de perfiles que tiene asignados al momento con su codificación, nombre y descripción. El jefe debe seleccionar uno o más perfiles para la revocatoria.</p>
Escoger los roles a revocar y el asignatario.	<p>Si el jefe escogió la operación de revocatoria de roles, se debe mostrar una pantalla con el listado de las personas bajo su cargo en su unidad administrativa, una vez escogida la persona (solo se puede escoger una) se debe mostrar el listado de roles que tiene asignados al momento, divididos en críticos y no críticos, y que muestre al menos la siguiente información:</p> <ul style="list-style-type: none">• Código de aplicación• Nombre de aplicación• Código de módulo• Nombre de módulo• Nombre de rol• Descripción del rol <p>El listado de aplicativos, roles y descripciones debe ser tomado de la base de datos de ADM.</p> <p>El jefe debe seleccionar uno o más roles para la revocatoria.</p>

9.- Actualización o Eliminación de Perfiles



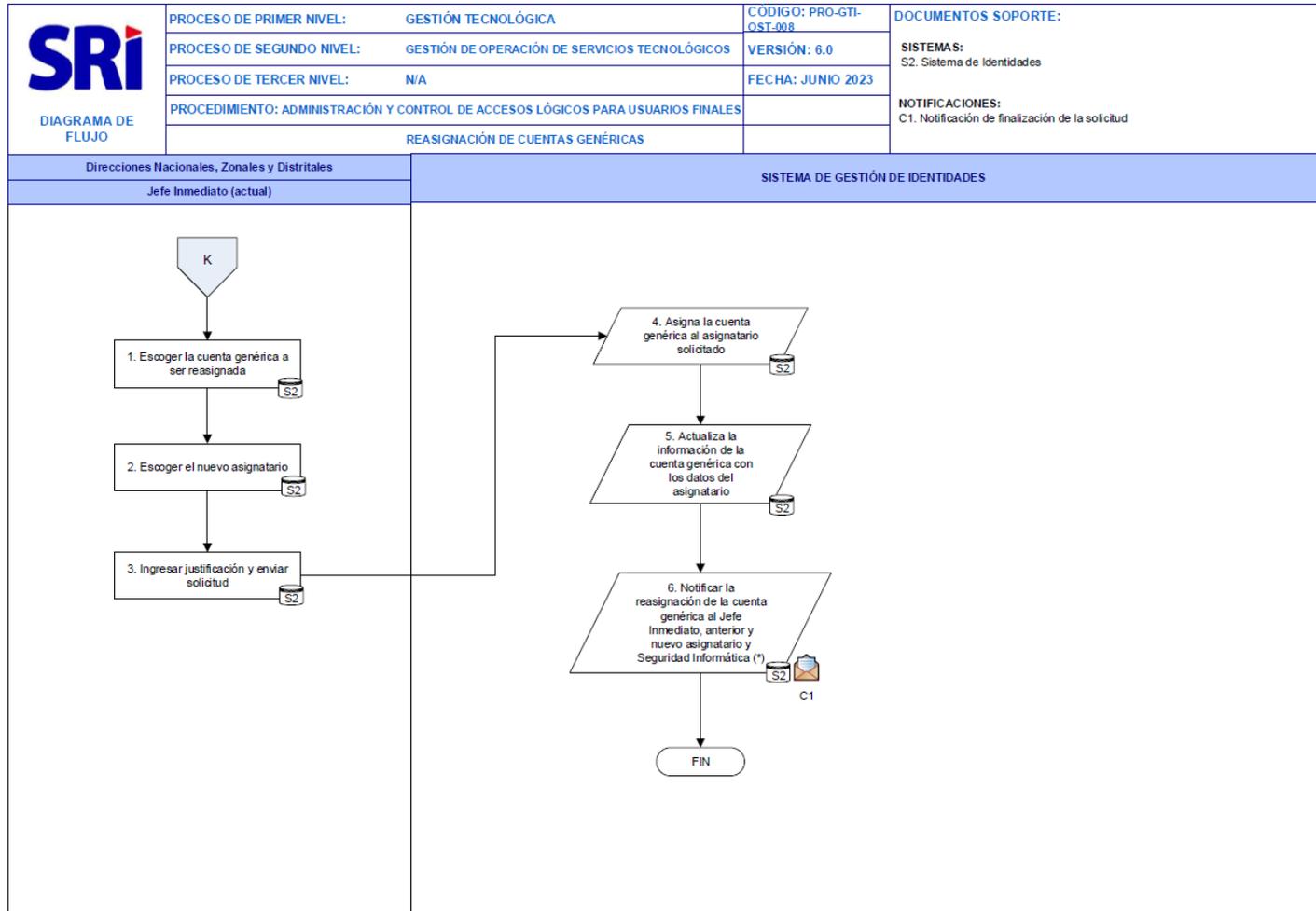
9.1.- Matriz Aclaratoria

No.	Actividad del Flujo	Instrucción Aclaratoria
1	Escoger el tipo de operación.	La jefatura debe escoger si lo que quiere es actualizar o eliminar perfiles.
2	Escoger el perfil (por función) a eliminar	Si se escogió la operación de eliminación se deben mostrar únicamente los perfiles por función creados en la unidad administrativa a la que pertenece el jefe solicitante, se podrá seleccionar solamente 1 perfil.
3	Escoger el perfil (por función o por cargo) a actualizar	Si se escogió la operación de actualizar se deben mostrar todos los perfiles (por función y por cargo) creados en la unidad administrativa a la que pertenece el jefe solicitante, se podrá seleccionar solamente 1 perfil.

9.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Exclusión de roles críticos.	Para el caso de la actualización de perfiles, se requiere que se excluyan del listado de roles disponibles para selección los roles parametrizados como críticos.
Actualización o eliminación de perfiles	<p>Para el caso de eliminación de perfiles, se debe revocar todos los roles que contenía el perfil a los usuarios que tenían dicho perfil asignado.</p> <p>Para el caso de actualización de perfiles, se debe asignar/revocar los roles seleccionados a los usuarios que tienen dicho perfil asignado.</p>

10.- Reasignación de Cuentas Genéricas



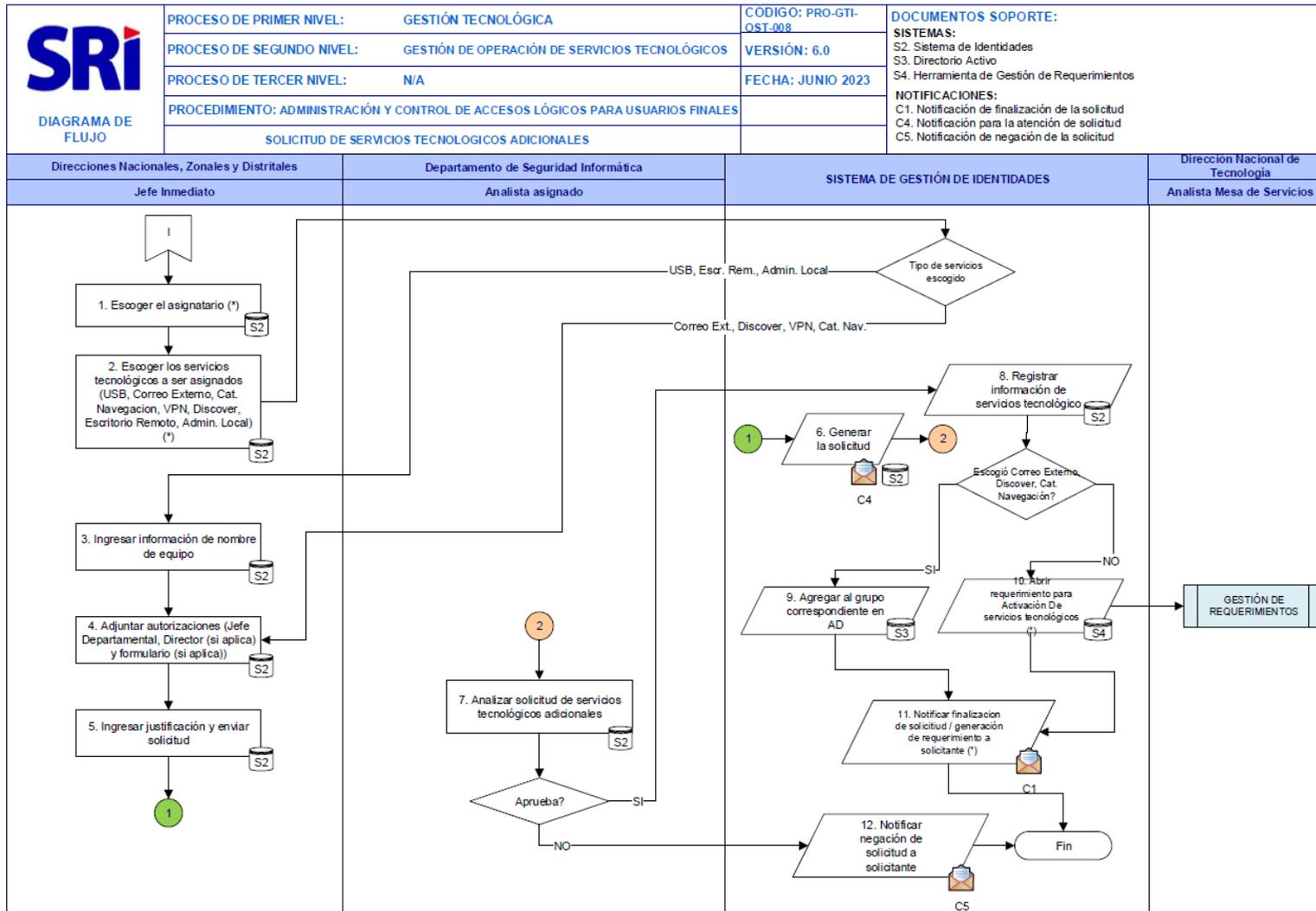
10.1.- Matriz Aclaratoria

No.	Actividad del Flujo	Instrucción Aclaratoria
1	Escoger la cuenta genérica a ser reasignada.	El Sistema de Gestión de Identidades debe mostrar una pantalla de búsqueda para poder encontrar y escoger la cuenta genérica a ser reasignada (ADM o Directorio Activo).
2	Escoger el nuevo asignatario	El Sistema de Gestión de Identidades debe mostrar una pantalla de búsqueda para poder encontrar y escoger la persona a la que va a ser reasignada la cuenta, no se podrá escoger la persona que actualmente tiene la cuenta genérica asignada.
5	Actualiza la información de la cuenta genérica con los datos del asignatario	El Sistema de Gestión de Identidades debe actualizar la información de la cuenta genérica reasignada con la información del nuevo asignatario, en los siguientes campos: Cuenta de Directorio Activo o ADM: <ul style="list-style-type: none"> • Nombres • Apellidos • Cedula No debe modificar el nombre de visualización de la cuenta, en el caso que sea cuenta de Directorio Activo.

10.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Escoger la cuenta genérica a ser reasignada	El usuario solicitante debe poder escoger la cuenta genérica (ADM o Directorio Activo)
Escoger el nuevo asignatario	El usuario solicitante debe poder escoger la persona de su unidad a la que se le va a reasignar la cuenta.
Asigna la cuenta genérica al asignatario solicitado	El sistema de Gestión de Identidades debe asignar la cuenta genérica escogida a la persona que el solicitante escogió.
Actualiza la información de la cuenta genérica con los datos del asignatario	El sistema de Gestión de Identidades debe actualizar la información de la cuenta genérica con la información del nuevo responsable.

11.- Solicitud de servicios tecnológicos adicionales



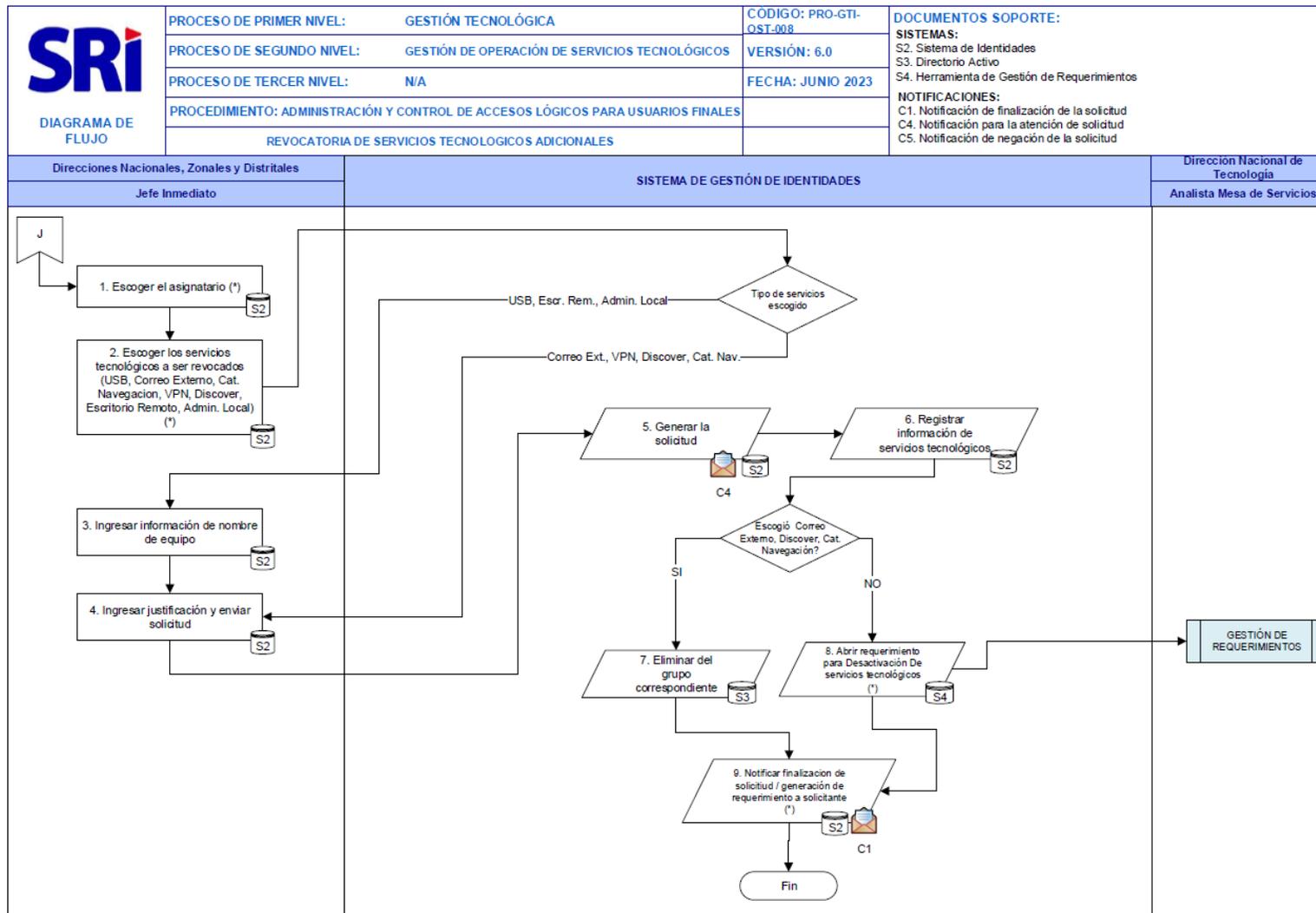
11.1.- Matriz Aclaratoria

No.	Actividad del Flujo	Instrucción Aclaratoria
1	Escoger el asignatario	El Sistema de Gestión de Identidades debe mostrar una pantalla de búsqueda para poder encontrar y escoger la persona a la que se le va a solicitar servicios tecnológicos adicionales.
2	Escoger el servicio tecnológico a ser asignado (USB, Correo Externo, Cat. Navegación, VPN, Discover, Escritorio Remoto, Admin. Local)	El Sistema de Gestión de Identidades debe mostrar una pantalla donde se podrá escoger solo 1 servicio tecnológico a ser solicitado para la persona escogida en el paso anterior.
3	Ingresar información de equipo	En caso de haber escogido USB, escritorio remoto o administrador local, el sistema de Gestión de Identidades debe mostrar una pantalla donde el solicitante debe ingresar el nombre del equipo del asignatario.
8	Registrar información de servicios tecnológicos	El sistema de Gestión de Identidades debe llevar un registro de los servicios tecnológicos adicionales aprobados para cada persona a manera de checklist, y se debe poder determinar que jefatura la solicitó, la fecha de solicitud y fecha de revocatoria de ser el caso.
9	Agregar al grupo correspondiente de AD	En caso de que el usuario solicitante escogió el servicio de correo externo, Discover o categorías de navegación, el sistema de Gestión de Identidades debe agregar el usuario de red al grupo de seguridad correspondiente, se entregará el listado de grupos a los que corresponde cada servicio.

11.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Escoger el asignatario	El usuario solicitante debe poder buscar y escoger la persona de su unidad a la que pretende solicitar los servicios tecnológicos adicionales.
Escoger los servicios tecnológicos a ser asignados (USB, Correo Externo, Cat. Navegación, VPN, Discover, Escritorio Remoto, Admin. Local)	El usuario solicitante debe poder escoger 1 servicio tecnológico adicional para la persona de su unidad seleccionada en el paso anterior.
Analizar solicitud de servicios tecnológicos adicionales	El aprobador debe analizar los documentos adjuntos que contengan las debidas autorizaciones para el servicio tecnológico solicitado y aprobar o rechazar la solicitud.

12.- Revocatoria de servicios tecnológicos adicionales



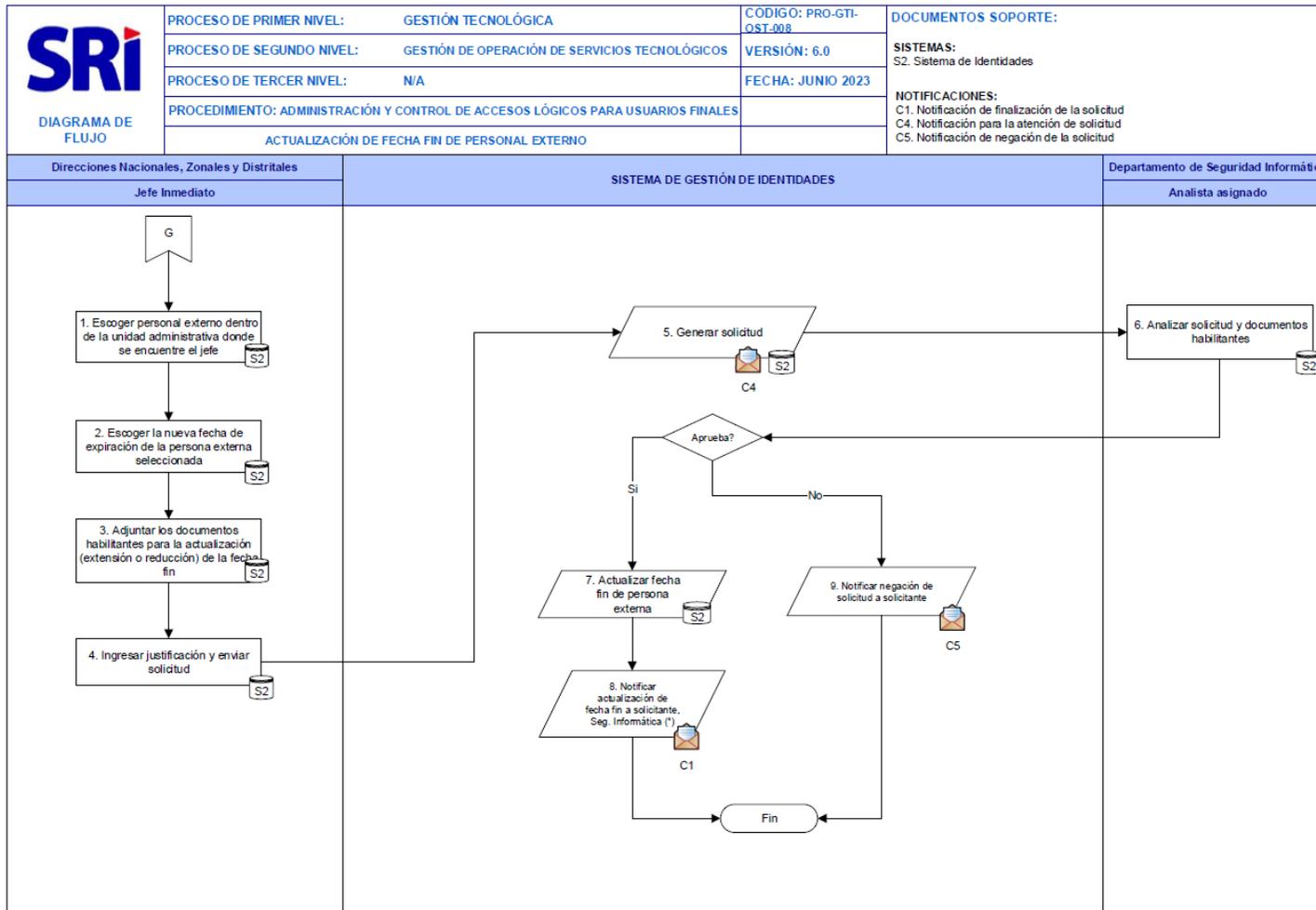
12.1.- Matriz Aclaratoria

No.	Actividad del Flujo	Instrucción Aclaratoria
1	Escoger el asignatario	El Sistema de Gestión de Identidades debe mostrar una pantalla de búsqueda para poder encontrar y escoger la persona a la que se le va a revocar servicios tecnológicos adicionales.
2	Escoger el servicio tecnológico a ser asignado (USB, Correo Externo, Cat. Navegación, VPN, Discover, Escritorio Remoto, Admin. Local)	El Sistema de Gestión de Identidades debe mostrar una pantalla donde se podrá escoger solo 1 servicio tecnológico a ser revocado para la persona escogida en el paso anterior.
3	Ingresar información de equipo	En caso de haber escogido USB, escritorio remoto o administrador local, el sistema de Gestión de Identidades debe mostrar una pantalla donde el solicitante debe ingresar el nombre del equipo del asignatario.
6	Registrar información de servicios tecnológicos	El sistema de Gestión de Identidades debe llevar un registro de los servicios tecnológicos adicionales revocados para cada persona a manera de checklist, y se debe poder determinar que jefatura la solicitó, la fecha de solicitud y fecha de revocatoria de ser el caso.
9	eliminar del grupo correspondiente	En caso de que el usuario solicitante escogió el servicio de correo externo, Discover o categorías de navegación, el sistema de Gestión de Identidades debe eliminar el usuario de red del grupo de seguridad correspondiente, se entregará el listado de grupos a los que corresponde cada servicio.

12.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Escoger el asignatario	El usuario solicitante debe poder buscar y escoger la persona de su unidad a la que pretende revocar los servicios tecnológicos adicionales.
Escoger los servicios tecnológicos a ser asignados (USB, Correo Externo, Cat. Navegación, VPN, Discover, Escritorio Remoto, Admin. Local)	El usuario solicitante debe poder escoger 1 servicio tecnológico adicional a revocar para la persona de su unidad seleccionada en el paso anterior.

13.- Actualización de fecha fin de personal externo



13.1.- Matriz Aclaratoria

No.	Actividad del Flujo	Instrucción Aclaratoria
2	Escoger la nueva fecha de expiración de la persona externa seleccionada	La fecha para escoger no puede ser menor o igual a la fecha actual
3	Adjuntar los documentos habilitantes para la actualización (extensión o reducción) de la fecha fin.	El sistema de Gestión de Identidades debe permitir subir varios archivos pdf.
7	Actualizar fecha fin de persona externa.	El sistema de Gestión de Identidades debe actualizar el campo de fecha fin de la persona externa solicitada con la fecha ingresada en el paso 2.

13.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Escoger el personal externo dentro de la unidad administrativa donde se encuentra el jefe.	El usuario solicitante debe poder buscar y escoger la persona externa de su unidad a la que pretende actualizar la fecha fin.
Escoger la nueva fecha de expiración de la persona externa seleccionada.	El usuario solicitante debe poder ver la fecha fin registrada actualmente y en otro campo ingresar la fecha actualizada mediante un campo tipo calendario.
Analizar solicitud y documentos habilitantes	El aprobador debe analizar los documentos adjuntos que contengan las debidas autorizaciones para la actualización de fecha fin solicitada y aprobar o rechazar la solicitud.

Anexo No. 1

Estándar para creación de usuarios

Cuenta funcionario / externo	Nombre Usuario
Marcelo Paúl Vinueza Espín	mpve191108
<i>(inicial primer nombre, inicial segundo nombre, inicial apellido paterno, inicial apellido materno, fecha De creación de cuenta).</i>	

El Sistema de Gestión de Identidades debe garantizar que las cuentas de red se generen considerando que existen nombres y apellidos compuestos, por ejemplo, Maria del Pilar o De La Torre, en estos casos la letra que se toma es la primera del nombre compuesto o la primera del apellido compuesto.

El Sistema de Gestión de Identidades debe garantizar que las cuentas de red se generen considerando que para usuarios con un solo nombre se tomen las dos primeras letras del nombre y no se coloque ningún dato en el campo del segundo nombre.

El Sistema de Gestión de Identidades debe garantizar que las cuentas de red se generen considerando que para usuarios con un solo apellido se tomen las dos primeras letras del apellido y no se coloque ningún dato en el campo del segundo apellido.

Algoritmo para creación de usuarios (Directorio Activo y ADM):

