Requerimiento funcional - Gestión de Identidades

Departamento de Seguridad Informática
Dirección Nacional de Tecnología
Abril 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 / 15-04-2024	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 identidades (personas), cuentas, 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 identidad.	Los campos de información de las identidades, a obtenerse desde el Sistema de Talento Humano, deben incluir: INFORMACION GENERAL: • Cédula de Identidad • Primer Nombre • Segundo Nombre • Primer Apellido • Segundo Apellido • Fecha de ingreso • Tipo de Empleado (interno, externo) DETALLES DEL NEGOCIO: • Código de Cargo • Nombre de Cargo • Código de Unidad Administrativa • Nombre de Unidad Administrativa • Dirección (Nacional / Zonal / Distrital/Subdirección/Dirección General) • Departamento (No aplica para Directores/Subdirectores/Director General)

	INFORMACION PERSONAL: • Correo electrónico personal
Trazabilidad en las operaciones de gestión de accesos.	La solución de Gestión de Identidades debe proveer 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.
Estructura organizativa del SRI.	En la solución de Gestión de Identidades, se debe poder crear, actualizar y visualizar el árbol o diagrama de la estructura organizativa del SRI, donde se incluyan al menos los siguientes campos: • Nombre de la unidad administrativa • Código de la unidad administrativa • Código de la estructura organizacional (ADM) • Código de área del sistema de administración (ADM) • Jefe de la unidad administrativa (Nombre de la persona) • Dirección a la que pertenece (Nacional / Zonal / Distrital/ Subdirección / Dirección General) • Provincia • Ciudad • Oficina • Unidad Organizativa asociada en Directorio Activo

Perfiles de notificación	Se requiere la creación de los siguientes perfiles propios del sistema de Gestión de Identidad para ser utilizados en el envío de notificaciones por correo electrónico: • Administrador de accesos • Ingresos • Movimientos • Bajas • Jefe de unidad • Monitoreo Redes • Redes • Mesa de Servicios • Internos • Externos
Adjuntar archivos pdf	En los flujos que correspondan, el usuario solicitante debe poder adjuntar uno o varios archivos pdf con capacidad máxima de hasta 3 MB cada uno.
Almacenamiento de archivos pdf	Los archivos pdf cargados por los solicitantes deben ser almacenados en un repositorio de archivos que forme parte de la solución de Gestión de Identidades y se los debe renombrar con este formato: *CedulaAsignatario_numeroSolicitud_fecha(dd/mm/yyyy)_hora(hh:mm).pdf*

Integrar el proceso de actualización de Áreas de ADM dentro de los flujos	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 en función del código de unidad administrativa de la persona en la Acción de Personal - APA específica sobre la que se está ejecutando el flujo.
Visualización de Perfiles y Roles del personal de cada unidad administrativa	Se requiere que dentro de la interfaz web de usuario final 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.
Parametrización de los tiempos de espera en los flujos	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.
Sincronización automática en actualizaciones de identidades ADM	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.
Generación automática de requerimientos o tickets.	La integración con el sistema de requerimientos del SRI, debe permitir la creación de tickets de manera automática, de acuerdo con lo establecido en los flujos correspondientes.

Disparador de los Flujos.	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 de 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 para que sea cargada en el sistema de Gestión de Identidades. En función de la fecha “rige” que consta en las acciones de personal del sistema de Talento Humano, se dispararán los flujos correspondientes de ingresos, movimientos y bajas, respetando el orden cronológico de fecha, hora y minuto del campo de fecha de elaboración del APA. Se debe generar un proceso automático para que el sistema de Gestión de Identidades a lea las APAs todos los días (lunes a Domingo) a las 01:00 (am) y dispare los flujos correspondientes. 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.
Procesamiento de Acciones de Personal	Cuando exista más de una acción de personal para la misma persona con la misma fecha rige, se debe esperar a que la primera APA se procese completamente para procesar la siguiente, y así consecutivamente.

Matriz aclaratoria de los flujos	Se requiere que el sistema de Gestión de Identidades cumpla con las actividades especificadas en cada uno de los flujos del presente documento, en la matriz aclaratoria de cada flujo se especifican actividades relevantes que se describen a nivel técnico con mayor detalle.
Detalles funcionales de los flujos	En ciertas actividades relevantes especificadas en los flujos se detalla a nivel funcional lo que se espera para dar más claridad de dichas actividades.
Delegación de funciones	En el sistema de Gestión de Identidades deberá existir un mecanismo para que la jefatura de la unidad administrativa o el administrador de la solución puedan delegar la gestión de los accesos a otra persona de la unidad administrativa, y de esta forma el delegado pueda realizar al menos las siguientes actividades: • 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	Las notificaciones por correo electrónico serán personalizadas para cada uno de los flujos y los perfiles definidos anteriormente, la solución debe permitir que los textos puedan ser actualizados por el administrador sin que sea necesario reprogramar el flujo. Los campos y textos de las notificaciones de los flujos serán proporcionados por el SRI. Dentro de las notificaciones (donde aplique) se debe mostrar una URL para acceder al sistema de Gestión de Identidades y llevar al usuario directamente al

	menú en el cual se requiere su intervención o información a revisar.
Notificaciones para aprobadores	El sistema de Gestión de Identidades debe enviar notificaciones periódicas a los usuarios con el perfil de aprobador 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 donde intervenga uno o varios aprobadores, se considere días laborables para el tiempo máximo de espera y que este sea parametrizable desde la consola de administración de la solución.
Asignación automática de solicitudes de Gestión de Accesos	El sistema de Gestión de Identidades debe tener un mecanismo de asignación automática de las solicitudes a los usuarios que cuenten con el perfil de aprobadores, para que no sea necesaria la asignación manual.
Justificación de Solicitudes	En los flujos de solicitud de accesos iniciados por parte de las jefaturas y en las actividades de aprobación de las solicitudes por parte de los aprobadores, se debe llenar un campo de justificación de la solicitud de los accesos o de la aprobación o rechazo de los mismos, según corresponda, 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 cuentas de las identidades deberá ejecutarse de acuerdo con el estándar detallado en el Anexo 1 de este documento.
Creación de buzones de usuarios	La creación del buzón de correo electrónico de las cuentas de red deberá ejecutarse de acuerdo con el estándar detallado en el Anexo 1 de este

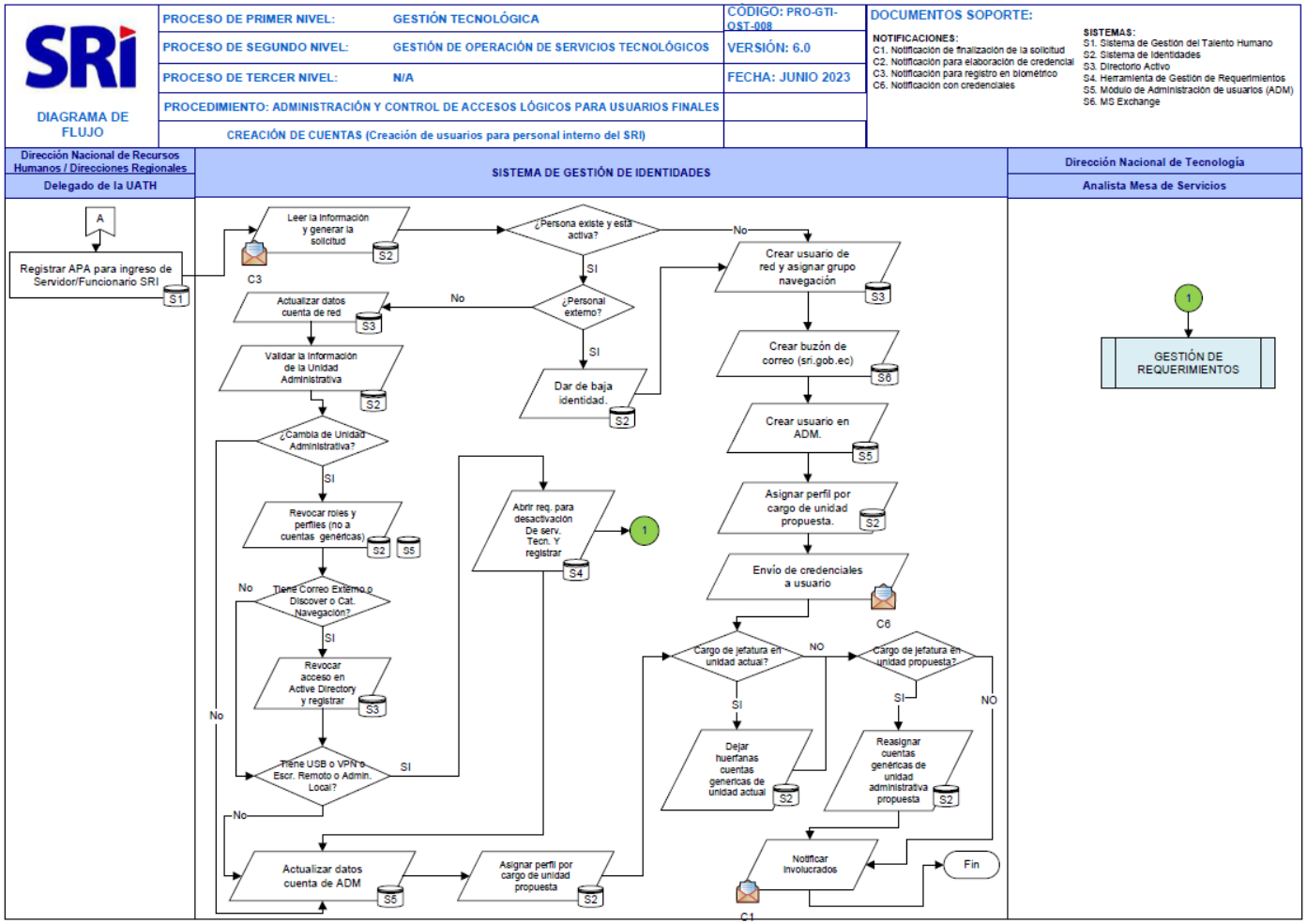
	documento.

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:

Datos de la identidad creada:	
Cédula de Identidad:	Xxxxxxxxxxxxx
Nombres y Apellidos:	Xxxxxxxxxxxxx
Cargo:	Xxxxxxxxxxxxx
Cuenta ADM:	Xxxxxxxxxxxxx
Cuenta Red:	Xxxxxxxxxxxxx
Unidad Administrativa:	Xxxxxxxxxxxxx
Departamento:	Xxxxxxxxxxxxx
Dirección:	Xxxxxxxxxxxxx
Jefatura Inmediata:	Xxxxxxxxxxxxx
Fecha de Ingreso:	Xxxxxxxxxxxxx
Ciudad:	Xxxxxxxxxxxxx
Oficina:	Xxxxxxxxxxxxx

1.- Creación de cuentas para personal interno del SRI



1.1.- Matriz Aclaratoria

Actividad del Flujo	**Instrucción Aclaratoria**
Dar de baja identidad	Se debe llamar al flujo de bajas de personal externo y realizar las actividades para dar de baja la identidad sin importar la fecha que tenga el personal externo.
¿Tiene correo externo o discover o categoría de navegación?	En el caso que cambie de unidad administrativa, debe consultar si la persona tiene activados alguno de estos servicios tecnológicos validando si el usuario de red pertenece a los grupos correspondientes de Directorio Activo: • Correo externo • Discover • Categoría de navegación diferente a la estándar
Revocar acceso en Active Directory y registrar	Eliminar al usuario de red del grupo correspondiente para: correo externo, discover, de todas las categorías de navegación y agregar a la categoría de navegación estándar, y se debe registrar la revocatoria en el inventario de servicios tecnológicos propio de la herramienta de Gestión de Identidades.
Tiene USB o VPN o Escritorio Remoto o Administrador Local?	En el caso que cambie de unidad administrativa, debe consultar si la persona tiene activados alguno o varios de estos servicios tecnológicos: • Acceso a USB • Certificado VPN • Escritorio Remoto Permiso de Administrador Local
Abrir requerimiento de desactivación de servicios tecnológicos y registrar	Se debe abrir un requerimiento por cada servicio tecnológico para la desactivación (USB, VPN, escritorio remoto o permiso de administrador local), y se debe registrar la revocatoria en el inventario de servicios tecnológicos propio de la herramienta de Gestión de Identidades.

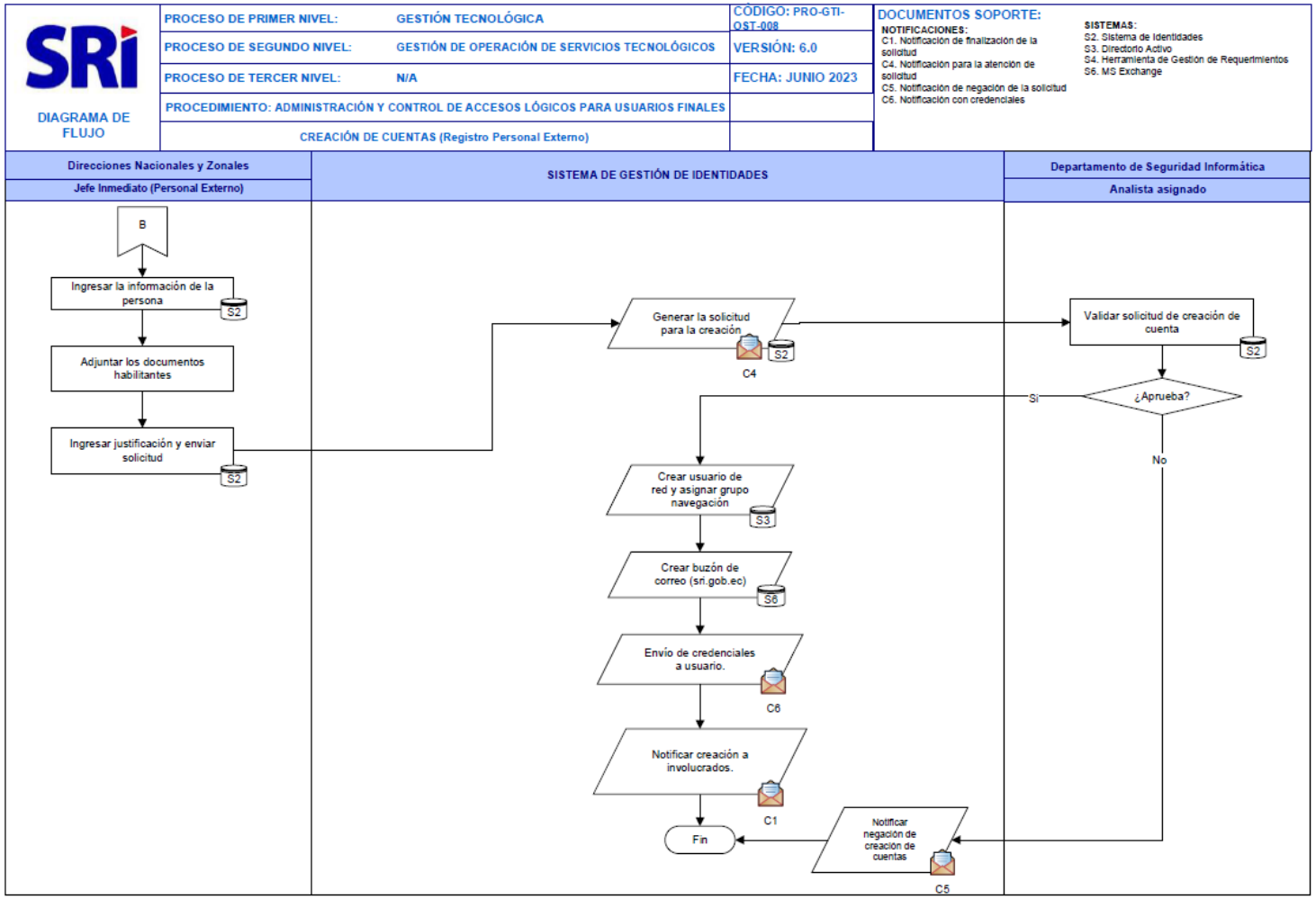
Crear usuario de red y asignar grupo de navegación	Se debe crear la cuenta de red con el algoritmo especificado en este documento y se debe agregar al usuario al grupo de categoría de navegación estándar.
Envío de credenciales a usuario	El Sistema de Gestión de Identidades debe enviar las credenciales de sus cuentas de red y ADM al correo electrónico personal, no se debe copiar a nadie más este correo.
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.
Cargo de jefatura en unidad actual?	El Sistema de Gestión de Identidades debe validar en el APA si el campo de cargo actual es de jefatura (Coordinador, Jefe Departamental, Director)
Cargo de jefatura en unidad propuesta?	El Sistema de Gestión de Identidades debe validar en el APA si el campo de cargo propuesto es de jefatura (Coordinador, Jefe Departamental, Director)

1.2.- Detalles funcionales del Flujo

Funcionalidad	Descripción
Ingreso de jefaturas	Cuando una persona ingresa a un cargo de jefatura se requiere: • 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. • Se le reasigne las cuentas genéricas de la unidad administrativa propuesta.
Ingreso de persona ya existente	En el caso de un APA que dispare el ingreso de una identidad que ya existe en el sistema de Gestión de Identidades, se debe validar si actualmente es externo, en caso de serlo se debe dar de

	baja la identidad actual para crearle una nueva, en caso de no ser externo se debe actualizar la información de las cuentas que mantiene actualmente.
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.
Notificar involucrados	Se debe notificar por correo electrónico a la persona titular del APA, al jefe inmediato y al administrador de accesos.

2.- Creación de cuentas para personal externo



2.1.- Matriz Aclaratoria

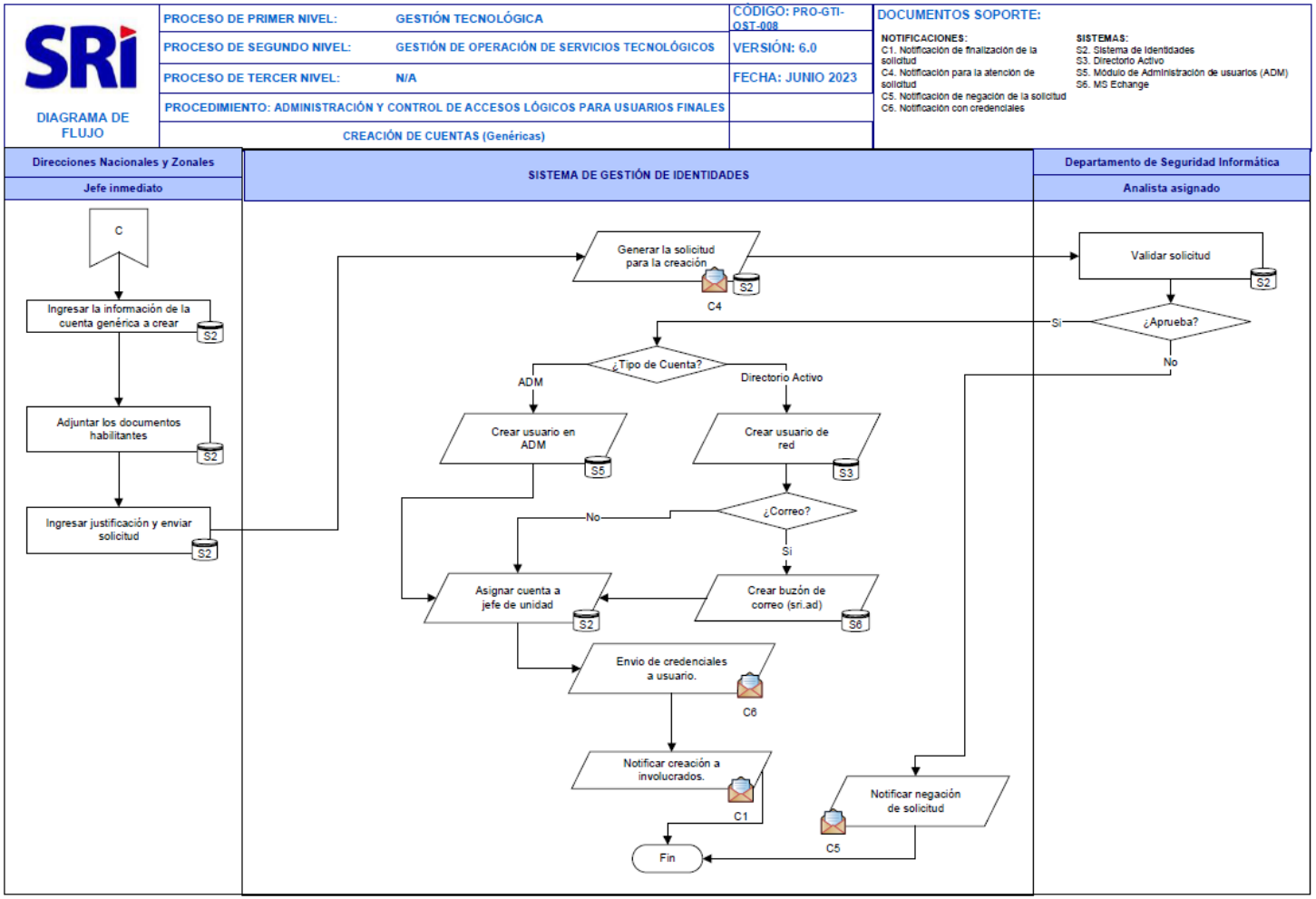
Actividad del Flujo	Instrucción Aclaratoria
Validar solicitud de creación de cuentas	Debe permitir aprobar o rechazar la solicitud, de acuerdo con el análisis del especialista asignado sobre los adjuntos cargados y la justificación ingresada
Crear usuario de red y asignar grupo de navegación	Debe crear la cuenta de red y agregarla al grupo de categoría de navegación estándar.
Envío de credenciales a usuario	El Sistema de Gestión de Identidades debe enviar las credenciales de sus cuentas de red y ADM al correo electrónico personal, no se debe copiar a nadie más este correo.

2.2.- Detalles funcionales del Flujo.

Funcionalidad	Descripción
Ingreso de solicitud	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: • Cedula de identidad • Fecha de ingreso (Fecha Inicio) • Fecha de terminación (Fecha Fin)

	• Apellidos y Nombres • Organización a la que pertenece • Correo electrónico personal Los siguientes campos deben asignarse al personal externo automáticamente en función de la unidad administrativa del solicitante: • Código de Unidad Administrativa • Nombre de Unidad Administrativa • Dirección (Nacional / Zonal / Distrital/Subdirección/Dirección General) • Departamento (No aplica para Directores/Subdirectores/Director General)
Fechas de vigencia	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.
Notificar creación a involucrados	Se debe notificar la creación de la identidad por correo electrónico al solicitante y al administrador de accesos.
Notificar negación de creación de cuentas	Se debe notificar del rechazo de la solicitud y el motivo ingresado por el avalista asignado de Seguridad Informática, al solicitante y al administrador de accesos.

3.- Creación de Cuentas Genéricas



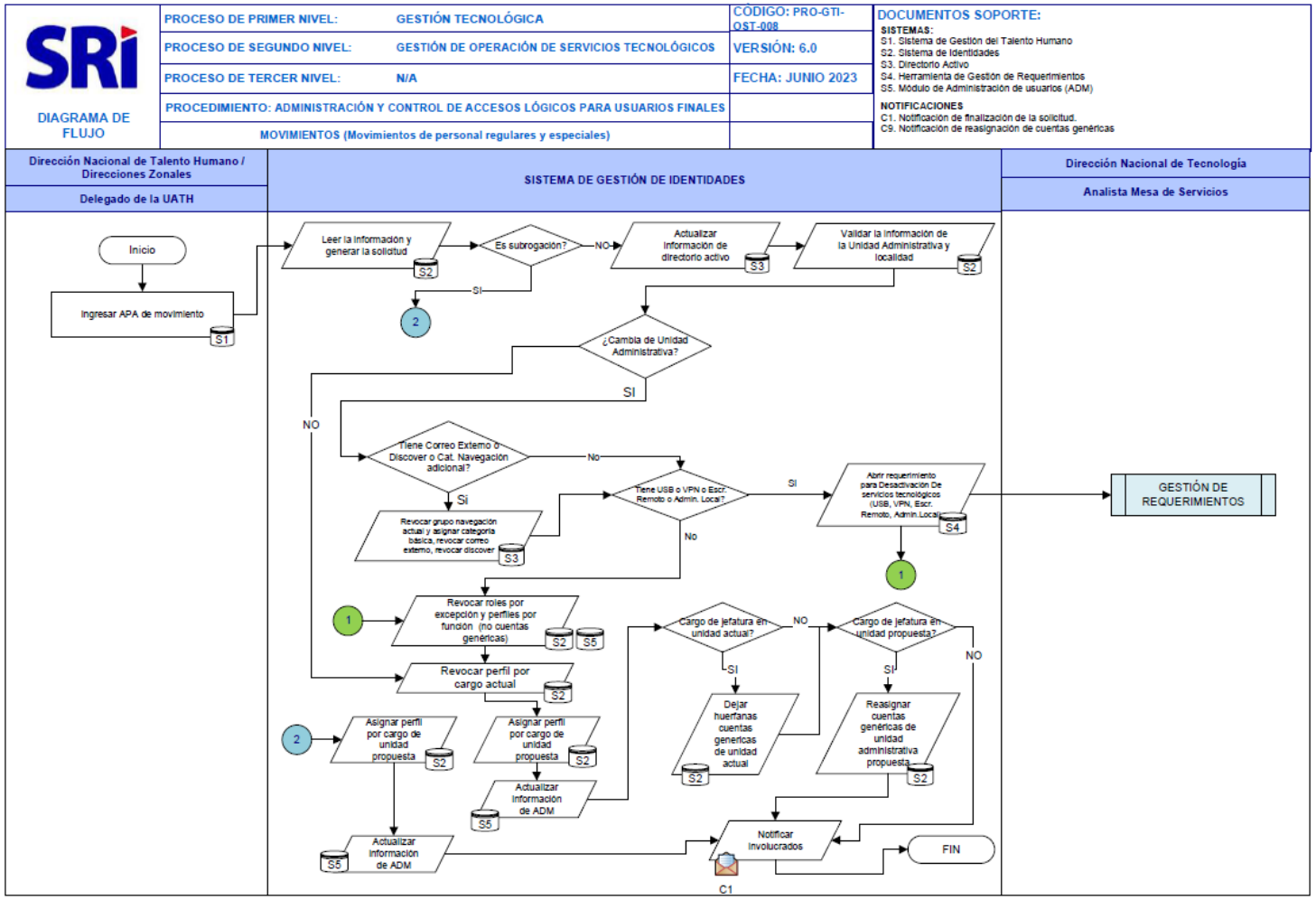
3.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
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
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.
Crear usuario de red	Todas las cuentas genéricas de red se crearán dentro de una Unidad Organizacional definida por el administrador del Directorio Activo.
Crear buzón de correo (sri.ad)	El buzón de correo debe generarse con el dominio interno sri.ad ya que se trata de cuentas genéricas.
Asignar cuenta a jefe de unidad	La cuenta genérica por crear se debe asignar al jefe actual de la unidad administrativa del solicitante.
Envío de credenciales de usuario	El Sistema de Gestión de Identidades debe enviar la credencial de la cuenta genérica al correo electrónico personal del jefe inmediato de la unidad administrativa donde se encuentra el solicitante, no se debe copiar a nadie más este correo.

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: • 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)
Asignar cuenta a jefe de unidad	Los siguientes datos se asignan a la cuenta automáticamente en función del jefe actual de la unidad administrativa: • Cédula de Identidad • Apellidos y Nombres • Dirección • Departamento • Coordinación • Provincia • Ciudad • Oficina

4.- Movimientos de Personal



4.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
¿Es subrogación?	El Sistema de Gestión de Identidades debe validar si el tipo de APA corresponde a una subrogación.
Revocar grupo de navegación actual y asignar	Se debe validar la unidad administrativa propuesta para saber
¿Cambia de Unidad Administrativa?	Se debe ejecutar el requerimiento de cambio administrativo.
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.
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.
Cargo de jefatura en unidad actual?	El Sistema de Gestión de Identidades debe validar en el APA si el campo de cargo actual es de jefatura (Coordinador, Jefe Departamental, Director)

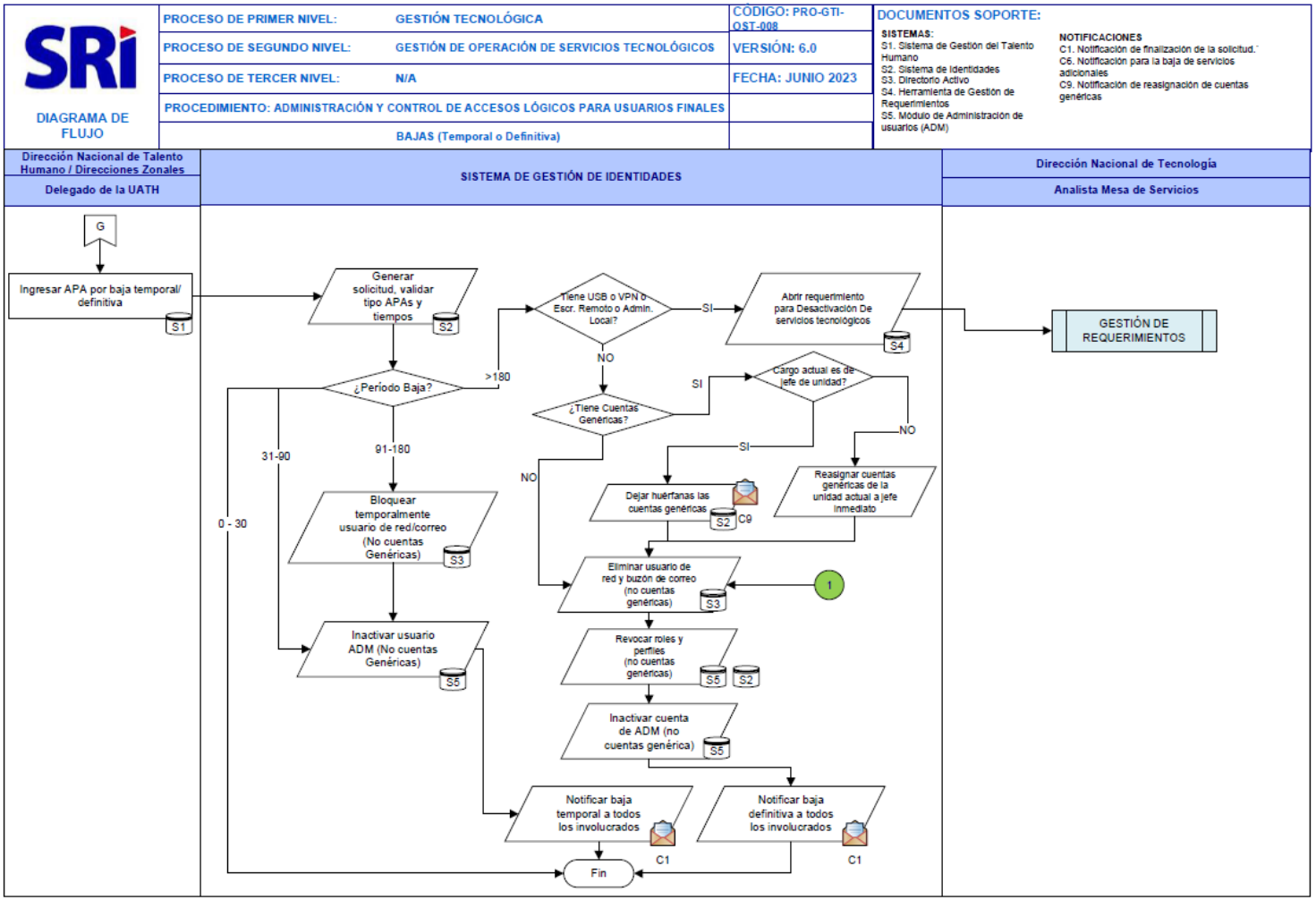
Cargo de jefatura en unidad propuesta?	El Sistema de Gestión de Identidades debe validar en el APA si el campo de cargo propuesto es de jefatura (Coordinador, Jefe Departamental, Director)
Notificar involucrados	Se debe notificar el movimiento por correo electrónico al jefe inmediato de la unidad administrativa actual y propuesta y al administrador de accesos.

4.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
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.
Movimiento a un puesto de Jefatura	Cuando una persona se mueve a un puesto de jefatura se requiere que: • Las cuentas genéricas de la unidad administrativa de la que va a ser jefe sean reasignadas a el mismo como jefe de unidad.
Movimiento desde un puesto de Jefatura	Cuando una persona se mueve desde un puesto de jefatura se requiere que: • Las cuentas genéricas que tiene asignadas se dejen huérfanas para que posteriormente sean asignadas a la persona que va a ser jefe de la unidad que deja.
No incluir cuentas genéricas en la revocatoria de roles de ADM	Se requiere que en la tarea de revocatoria de perfiles y roles de ADM no se incluyan las cuentas genéricas que tiene a cargo la persona.
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 las 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	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.

5.- Bajas Temporales o Definitivas



5.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
¿Periodo baja?	Cuando un funcionario se ausente de forma temporal por un período de 0 a 30 días no se realiza ninguna acción. Cuando 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). Cuando 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 (excepto cuentas genéricas). Cuando un funcionario se ausente por un período mayor a 181 días, sea por salida temporal o definitiva, se procede con la eliminación de la identidad y sus cuentas (excepto genéricas en caso de ser jefatura de la unidad), revocatoria de perfiles y roles por excepción y posteriormente la inactivación de la cuenta de ADM. 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).
Cargo de jefatura en unidad actual?	El Sistema de Gestión de Identidades debe validar en el APA si el campo de cargo actual es de jefatura (Coordinador, Jefe Departamental, Director)

5.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
No incluir cuentas genéricas en la inactivación o eliminación.	Se requiere que en las tareas de inactivación 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.

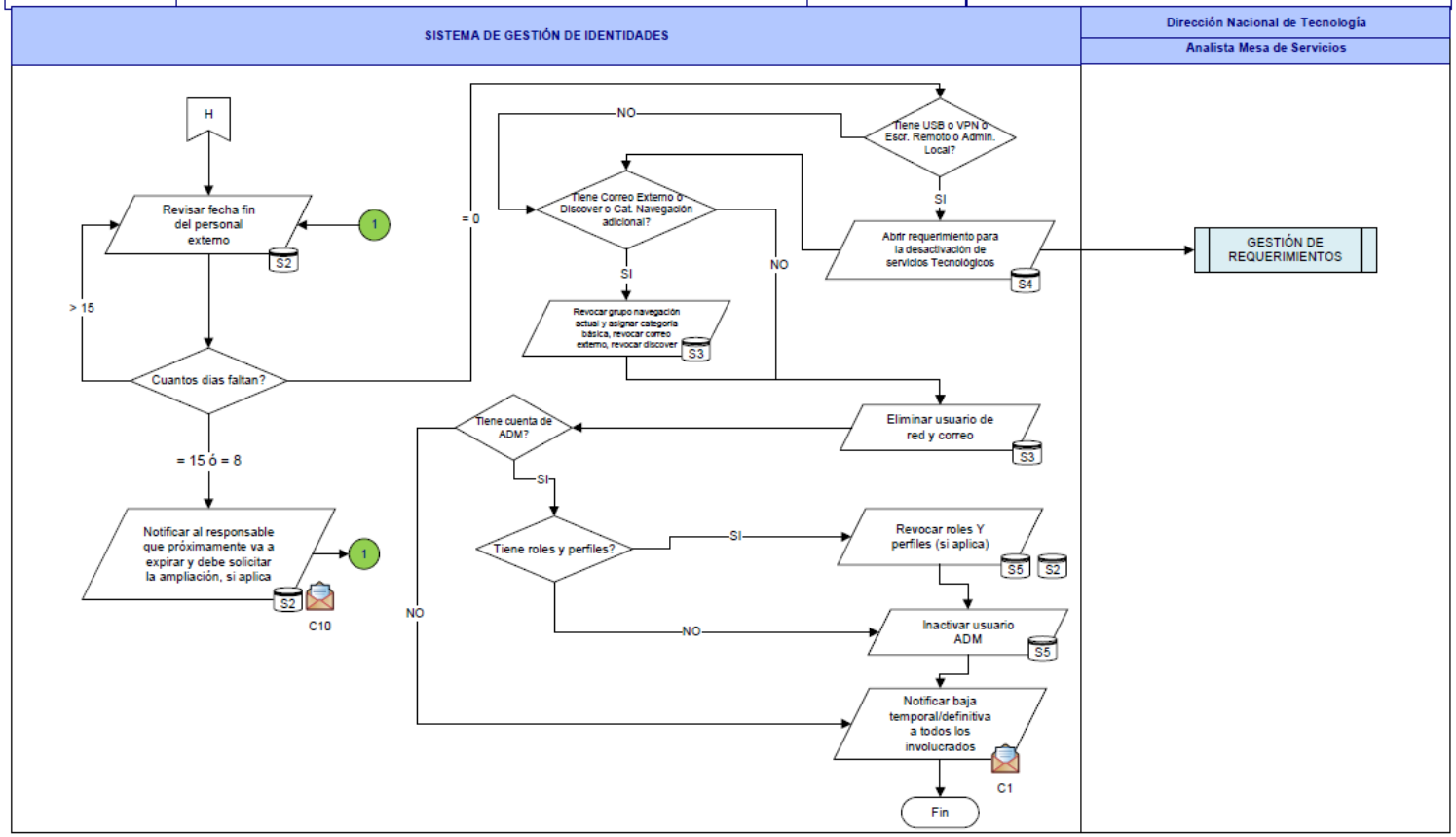
6.- Bajas de Personal Externo

SRI DIAGRAMA DE FLUJO	PROCESO DE PRIMER NIVEL:	GESTIÓN TECNOLÓGICA	CÓDIGO: PRO-GTI-OST-008
	PROCESO DE SEGUNDO NIVEL:	GESTIÓN DE OPERACIÓN DE SERVICIOS TECNOLÓGICOS	VERSIÓN: 6.0
	PROCESO DE TERCER NIVEL:	N/A	FECHA: JUNIO 2023
	PROCEDIMIENTO: ADMINISTRACIÓN Y CONTROL DE ACCESOS LÓGICOS PARA USUARIOS FINALES		
	BAJAS (Externos)		

DOCUMENTOS SOPORTE:

NOTIFICACIONES:
C1. Notificación de finalización de la solicitud
C3. Notificación para registro en biometrico.
C10. Notificación de expiración próxima de usuario externo.

SISTEMAS:
S2. Sistema de Identidades
S3. Directorio Activo
S4. Herramienta de Gestión de Requerimientos
S5. Módulo de Administración de usuarios (ADM)



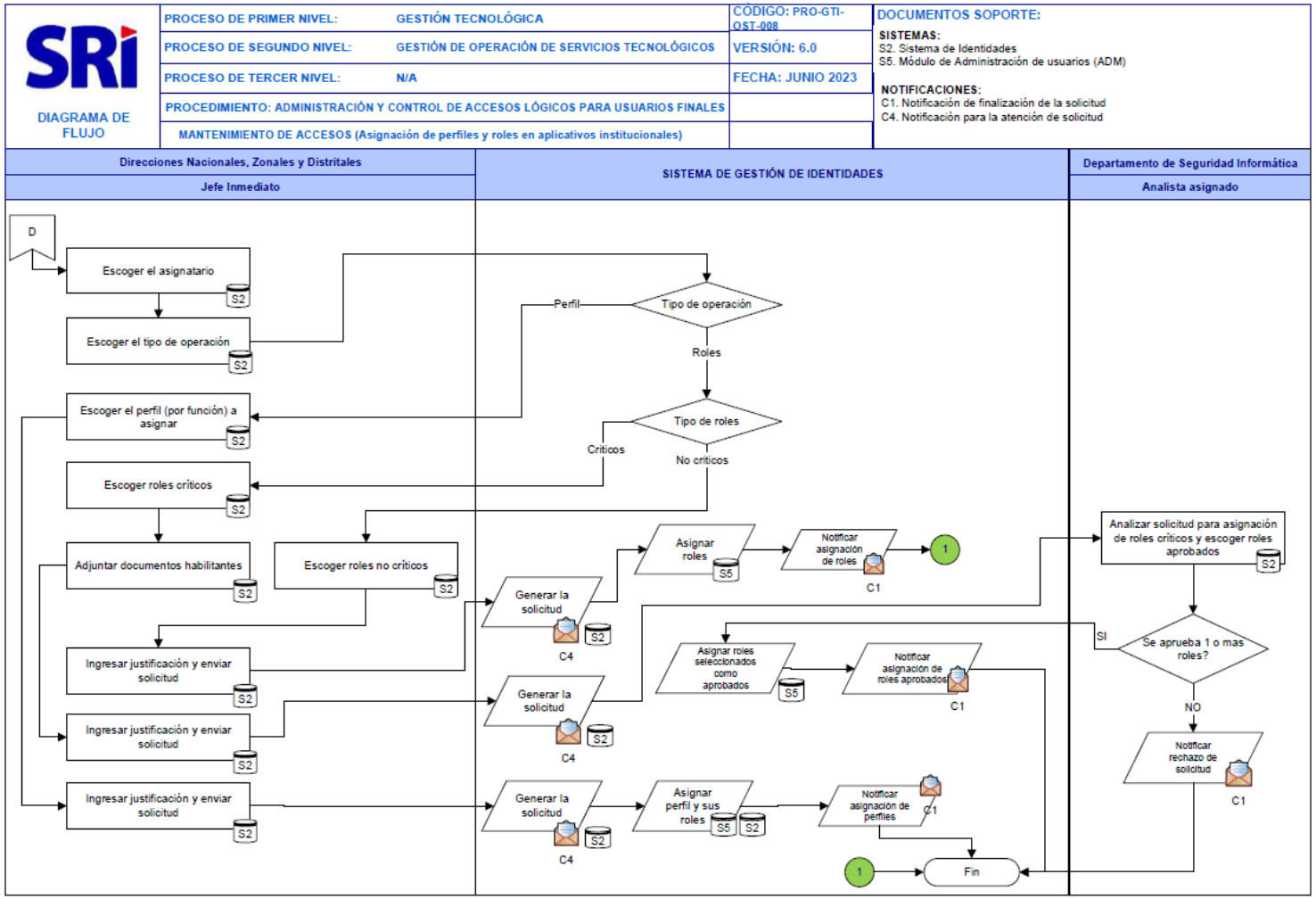
6.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
Revisar fecha fin del personal externo	El Sistema de Gestión de Identidades deberá ejecutar un proceso diario que valide la fecha fin del personal externo: • 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 primer recordatorio advirtiendo 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 advirtiendo 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.
Notificar baja temporal o definitiva a todos los involucrados	Se debe notificar la baja mediante correo electrónico al jefe de la unidad administrativa donde se encontraba la persona externa y al administrador de accesos.

7.- Asignación de Perfiles y Roles en Aplicativos Institucionales



7.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
Escoger el asignatario	La jefatura debe escoger la persona a la que se solicita realizar la 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.
Escoger el tipo de operación	La jefatura debe escoger si lo que requiere es asignar roles o perfiles.
Tipo de roles	La jefatura escoger si requiere asignar roles críticos o no críticos, en base a esta decisión se mostrará el listado correspondiente.
Escoger el perfil (por función) a asignar	Los perfiles que se les va a presentar son los perfiles por función que pertenecen a su unidad administrativa.
Escoger roles críticos	La jefatura debe escoger los roles críticos a asignar.
Escoger roles no críticos	La jefatura debe escoger los roles no críticos a asignar.
Adjuntar documentos habilitantes.	En caso de que se haya escogido la asignación de roles críticos se debe adjuntar los documentos de autorización en pdf.

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.
Asignar roles seleccionados como aprobados	El sistema de Gestión de Identidades deberá asignar únicamente los roles seleccionados como aprobados previamente por el aprobador.

7.2.- Detalles funcionales del Flujo

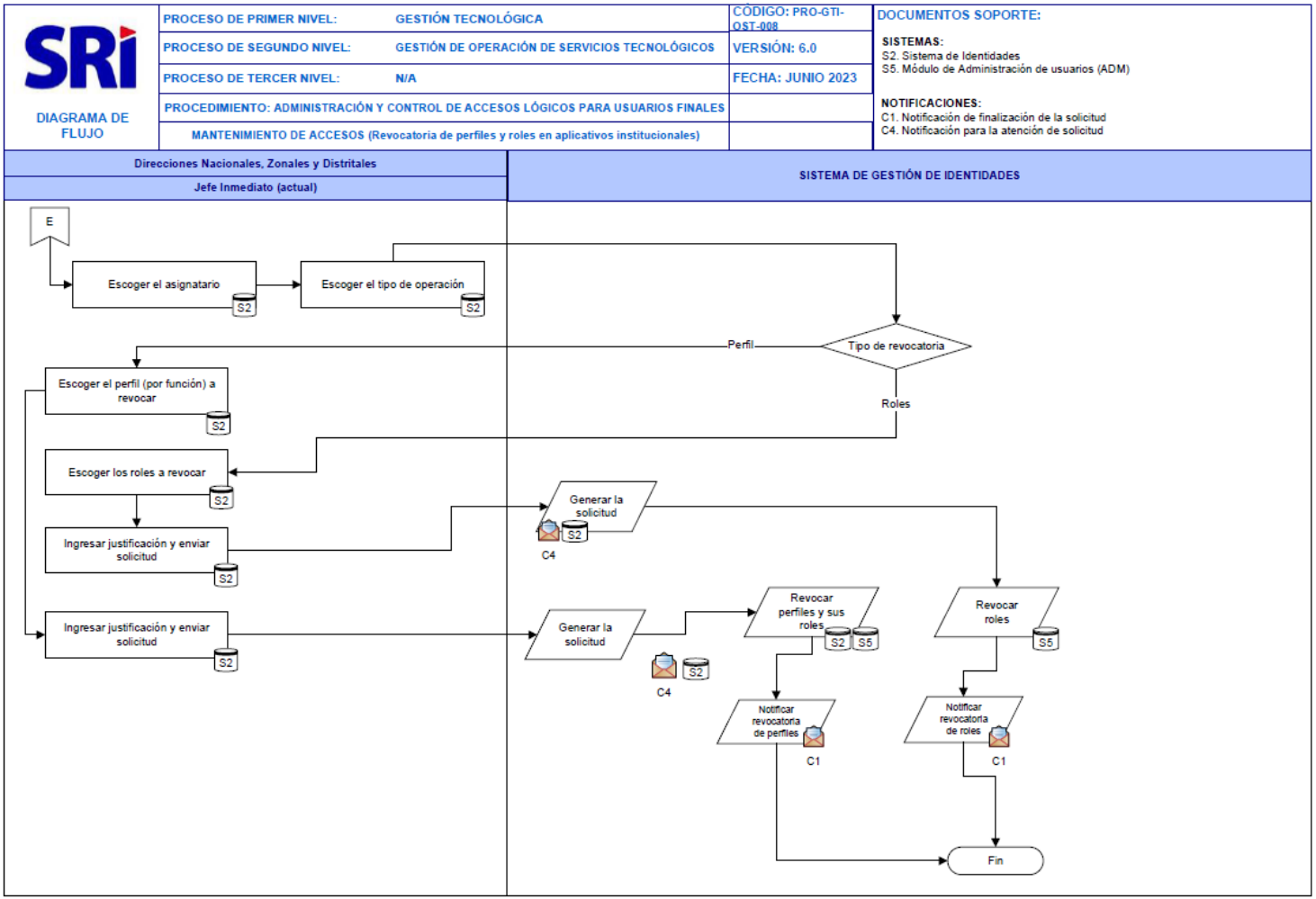
Funcionalidad	Descripción
Escoger el asignatario	Se requiere que el sistema de Gestión de Identidades muestre una pantalla con el listado de las personas a cargo de la jefatura solicitante.
Escoger el tipo de operación	Se requiere que el sistema de Gestión de Identidades muestre una pantalla que permita al jefe solicitante escoger entre las siguientes opciones: • Asignación de Perfiles • Asignación de roles
Escoger el tipo de roles	En caso de haber escogido la operación de asignación de roles, el sistema de Gestión de Identidades debe mostrar una pantalla que permita al jefe solicitante escoger entre las siguientes opciones: • Roles críticos • Roles no críticos

Escoger el perfil (por función) a asignar	Si el jefe escogió la operación de asignación de perfiles, 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 más perfiles para la asignación.
Escoger roles críticos	Si el jefe escogió la operación de asignación de roles críticos, se debe mostrar el listado de roles críticos que tiene asignados al momento el asignatario y en otra sección los roles críticos que no tiene asignados y están disponibles para asignación, y que muestre al menos la siguiente información: • Código de aplicación • Nombre de aplicación • Código de módulo • Nombre de módulo • Nombre de rol • Descripción del rol El listado de aplicativos, roles y descripciones debe ser tomado de la base de datos de ADM. El jefe debe seleccionar uno o más roles críticos para la asignación.
Escoger roles no críticos	Si el jefe escogió la operación de asignación de roles no críticos, se debe mostrar el listado de roles no críticos que tiene asignados al momento el asignatario y en otra sección los roles no críticos que no tiene asignados y están disponibles para asignación, y que muestre al menos la siguiente información:

	• Código de aplicación • Nombre de aplicación • Código de módulo • Nombre de módulo • Nombre de rol • Descripción del rol El listado de aplicativos, roles y descripciones debe ser tomado de la base de datos de ADM. El jefe debe seleccionar uno o más roles no críticos para la asignación.
Adjuntar documentos habilitantes	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: • 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 de los roles solicitados.
Asignar roles seleccionados como aprobados	Se deben asignar únicamente los roles críticos seleccionados en el análisis de la solicitud por parte del aprobador.
Notificar asignación de roles aprobados	Se debe notificar por correo electrónico los roles aprobados y asignados, al solicitante, asignatario y al administrador de accesos.
Notificar rechazo de solicitud	Se debe notificar por correo electrónico el rechazo de la solicitud y el motivo ingresado

	por el analista que gestionó la misma, al solicitante y al administrador de accesos.
Notificar asignación de perfiles	Se debe notificar por correo electrónico los perfiles asignados, al solicitante, asignatario y al administrador de accesos.

8.- Revocatoria de Perfiles y Roles en Aplicativos Institucionales



8.1.- Matriz Aclaratoria

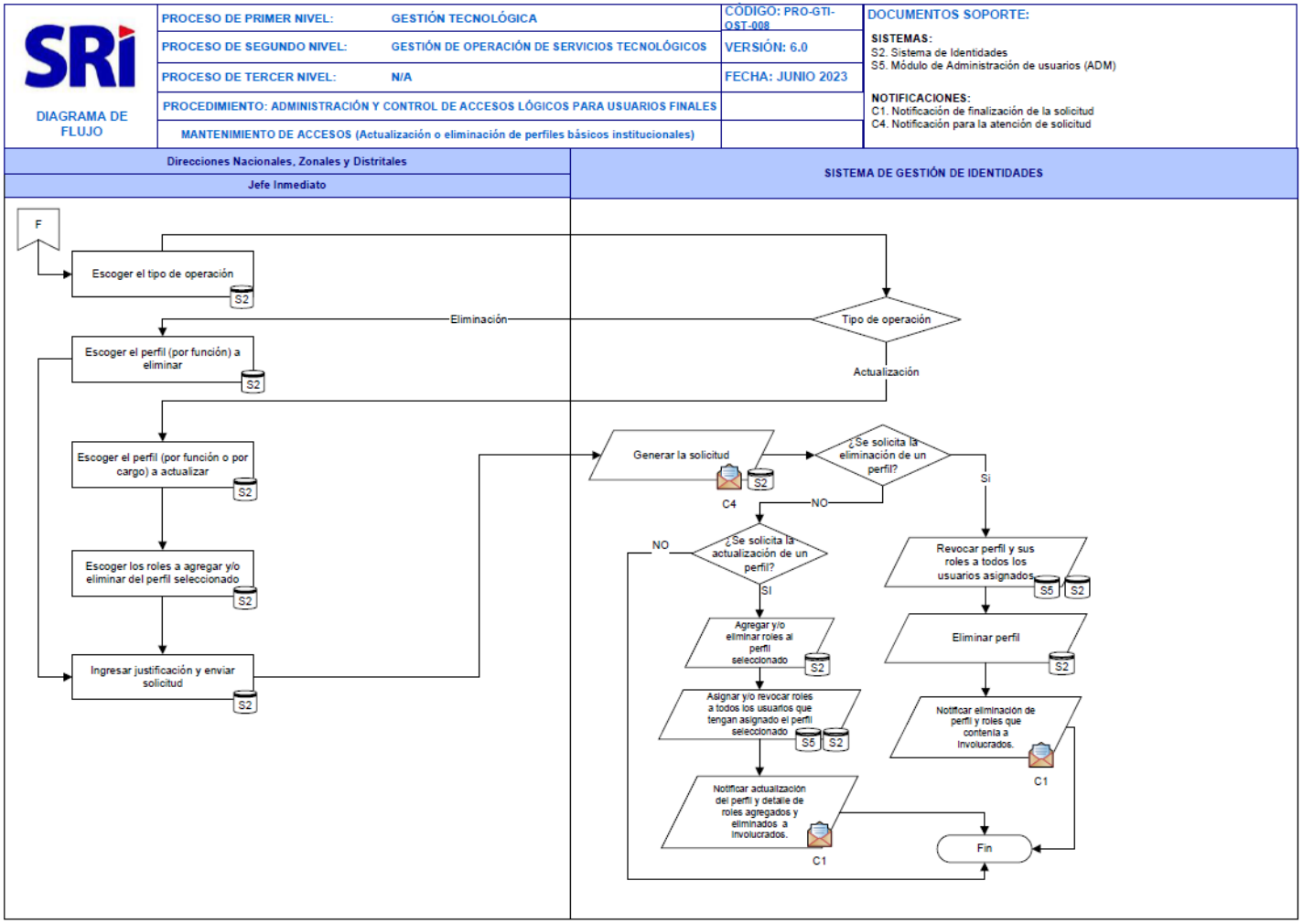
Actividad del Flujo	Instrucción Aclaratoria
Escoger el asignatario	La jefatura debe escoger la persona a la que se solicita realizar la operación, el listado de personas de las que se podrá escoger son los que están dentro de la unidad administrativa a la que pertenece la jefatura solicitante.
Escoger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

8.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Escoger el asignatario	Se requiere que el sistema de Gestión de Identidades muestre una pantalla con el listado de las personas a cargo de la jefatura solicitante.
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:

	• Revocatoria de Perfiles • Revocatoria de roles
Escoger el perfil (por función) a revocar.	Si el jefe escogió la operación de revocatoria de perfiles, se debe mostrar el listado de perfiles que tiene asignados al momento el asignatario, con su codificación, nombre y descripción. El jefe debe seleccionar uno o más perfiles para la revocatoria.
Escoger los roles a revocar.	Si el jefe escogió la operación de revocatoria de roles, se debe mostrar el listado de roles que tiene asignados al momento el asignatario, divididos en críticos y no críticos, y que muestre al menos la siguiente información: • Código de aplicación • Nombre de aplicación • Código de módulo • Nombre de módulo • Nombre de rol • Descripción del rol El listado de aplicativos, roles y descripciones debe ser tomado de la base de datos de ADM. El jefe debe seleccionar uno o más roles para la revocatoria.

9.- Actualización o Eliminación de Perfiles



9.1.- Matriz Aclaratoria

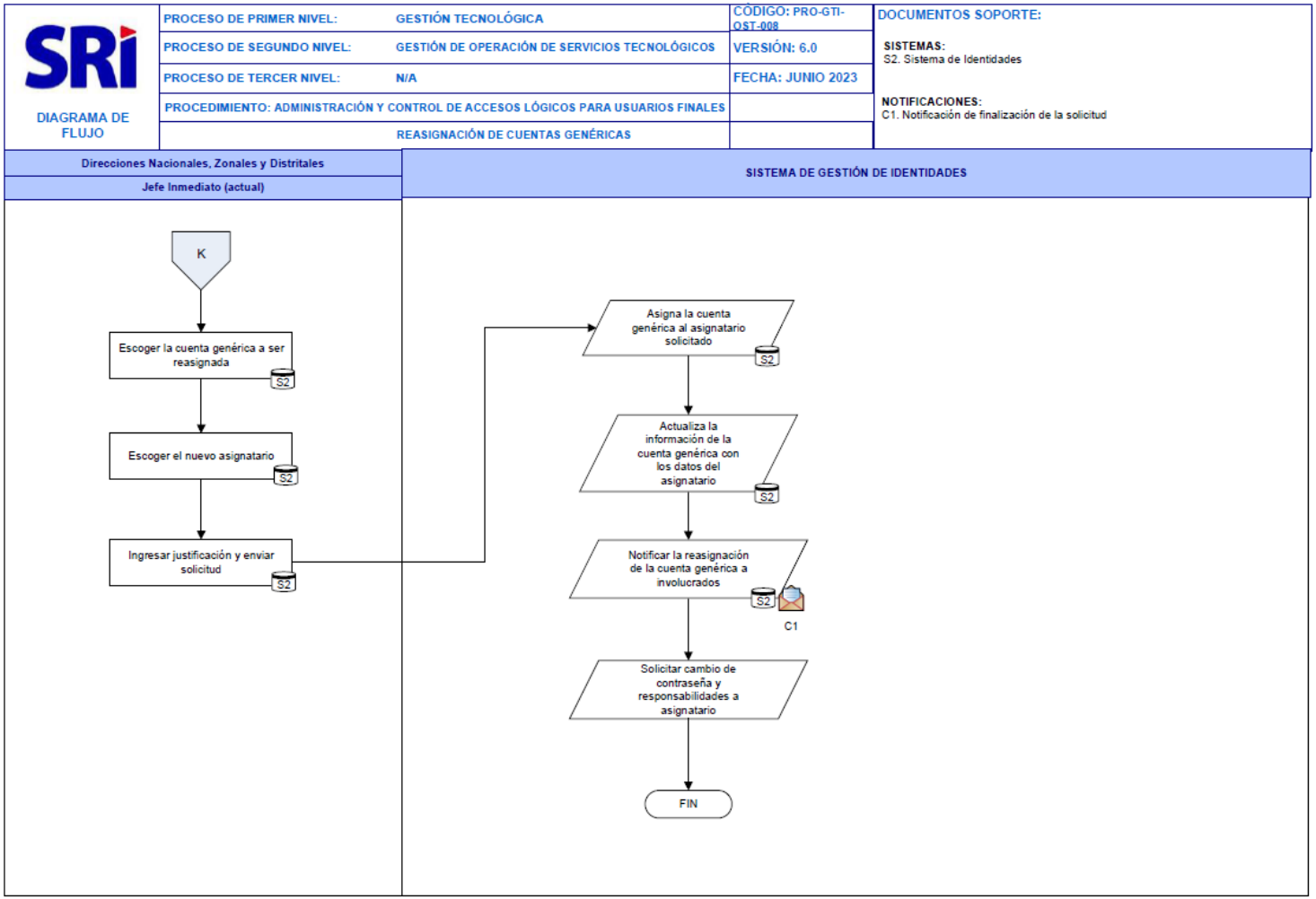
Actividad del Flujo	Instrucción Aclaratoria
Escoger el tipo de operación.	La jefatura debe escoger si lo que quiere es actualizar o eliminar perfiles.
Escoger el perfil (por función) a eliminar	Si se escogió la operación de eliminación se deben mostrar únicamente los perfiles por función creados en la unidad administrativa a la que pertenece el jefe solicitante, se podrá seleccionar solamente 1 perfil.
Escoger el perfil (por función o por cargo) a actualizar	Si se escogió la operación de actualización 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	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. Para el caso de actualización de perfiles, se debe asignar/revocar los roles seleccionados a los usuarios que tienen dicho perfil asignado.
Notificar actualización del	Se debe notificar por correo electrónico la actualización del perfil y los roles que fueron

perfil y detalle de roles agregados y eliminados, a involucrados.	agregados y revocados del mismo, al solicitante y al administrador de accesos.
Notificar eliminación de perfil y roles que contenía, a involucrados	Se debe notificar por correo electrónico la eliminación del perfil selecciones y los roles que contenía dicho perfil.

10.- Reasignación de Cuentas Genéricas



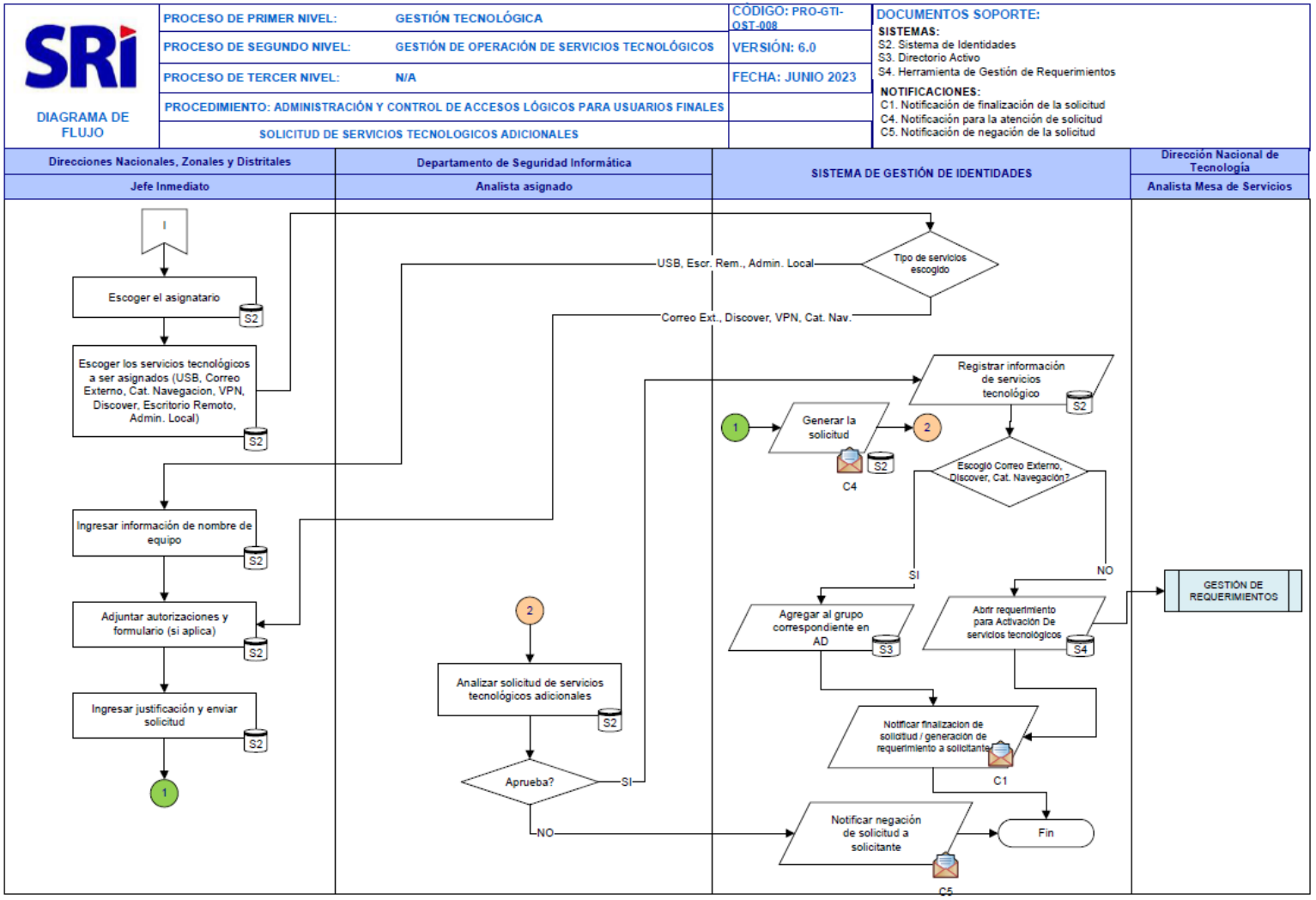
10.1.- Matriz Aclaratoria

Actividad del Flujo	**Instrucción Aclaratoria**
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).
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.
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: • 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



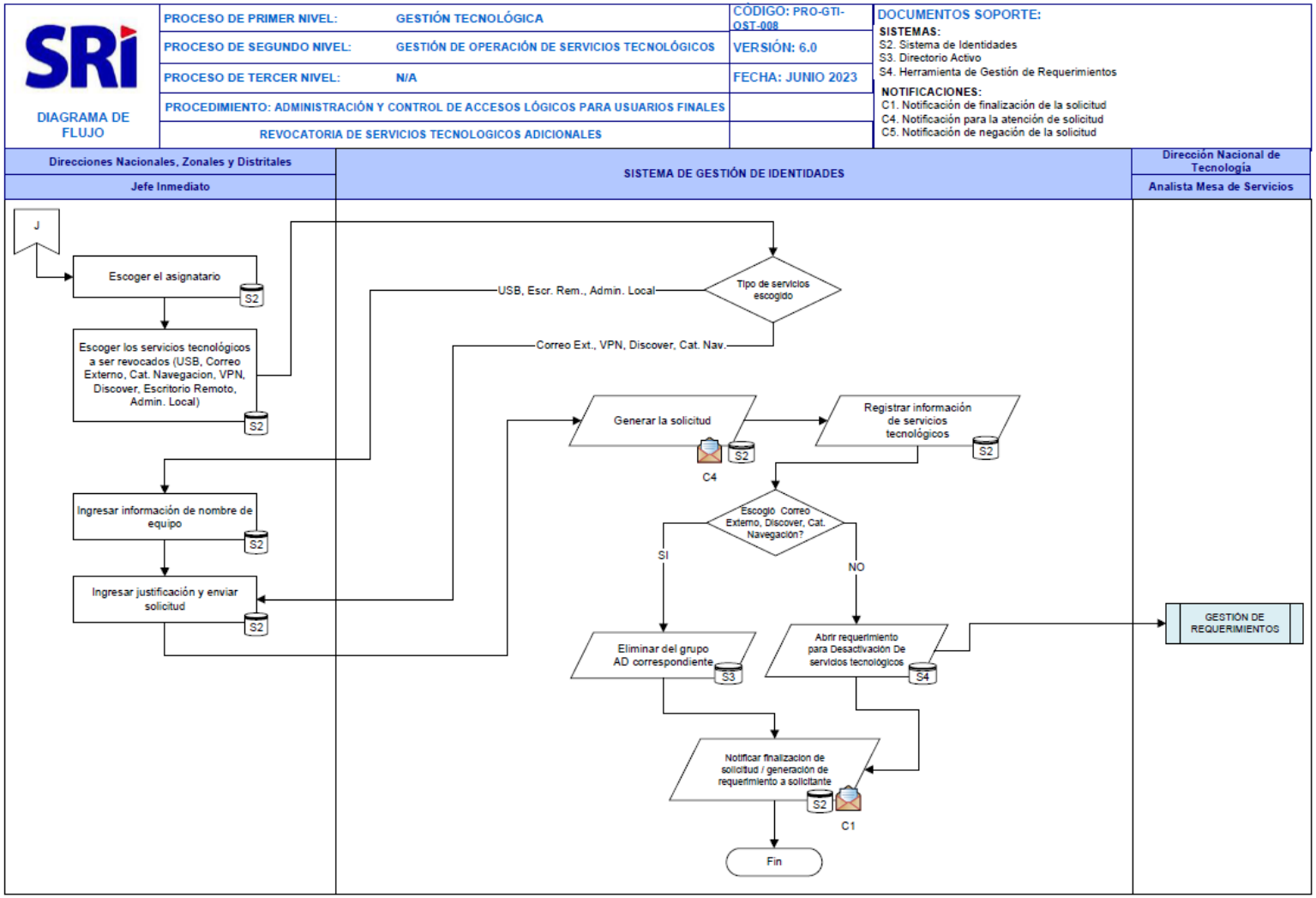
11.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
Escoger el asignatario	La jefatura debe escoger la persona a la que se solicita realizar la 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.
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.
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.
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.
Agregar al grupo correspondiente en 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.
Notificar finalización de solicitud aprobada	Se debe enviar por correo electrónico la confirmación del otorgamiento del servicio tecnológico solicitado al solicitante, asignatario y administrador de accesos.
Notificar negación de solicitud	Se debe enviar por correo electrónico el rechazo de la solicitud y el motivo ingresado por el analista que gestionó la misma, al solicitante y al administrador del accesos.

12.- Revocatoria de servicios tecnológicos adicionales



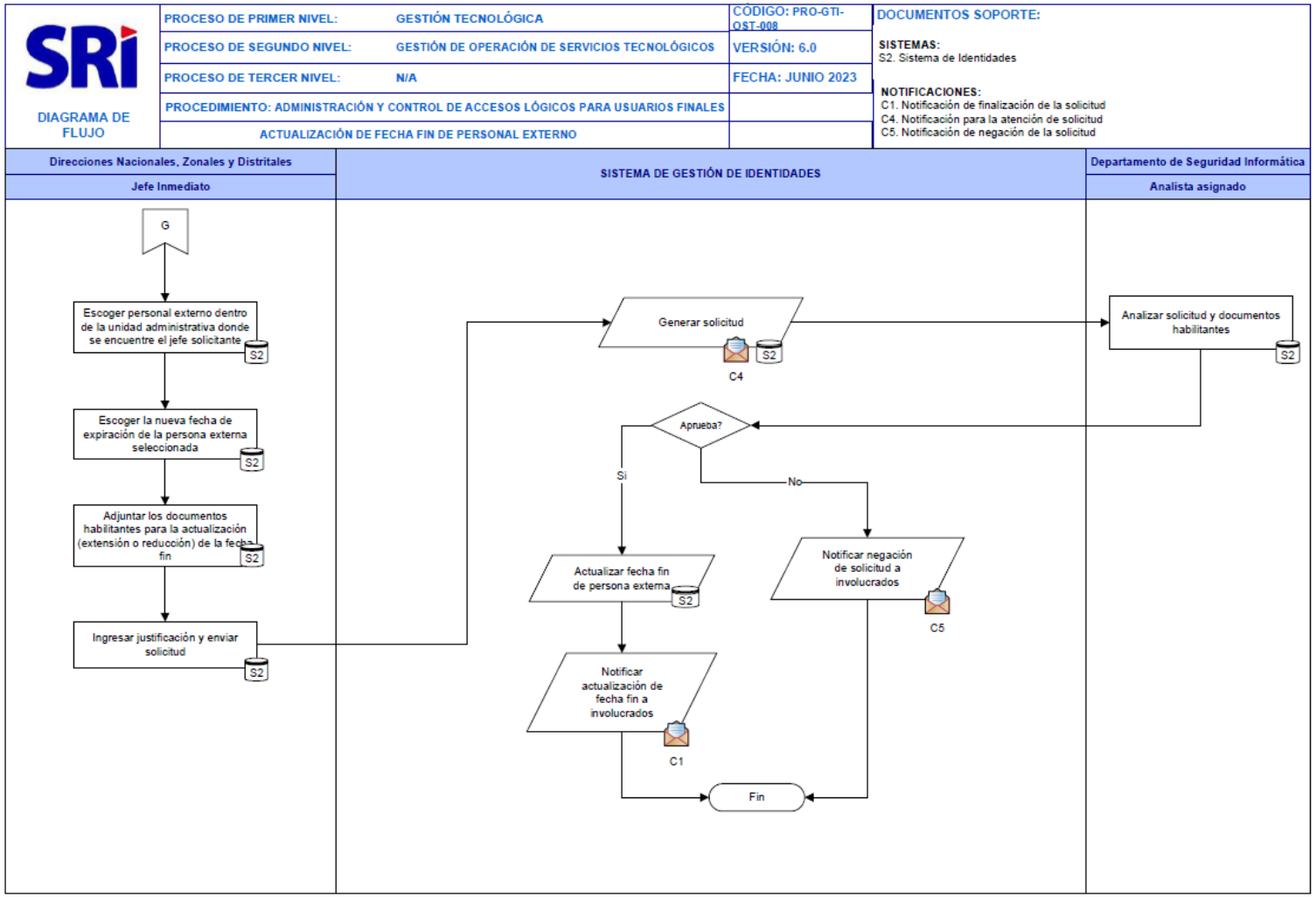
12.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
Escoger el asignatario	La jefatura debe escoger la persona a la que se solicita realizar la 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.
Escoger el servicio tecnológico a ser revocado (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.
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.
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.
Eliminar del grupo AD 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.
Notificar finalización de solicitud	Se debe enviar por correo electrónico la confirmación de la revocatoria del servicio tecnológico al solicitante, asignatario y administrador de accesos.

13.- Actualización de fecha fin de personal externo



13.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
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
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.
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.

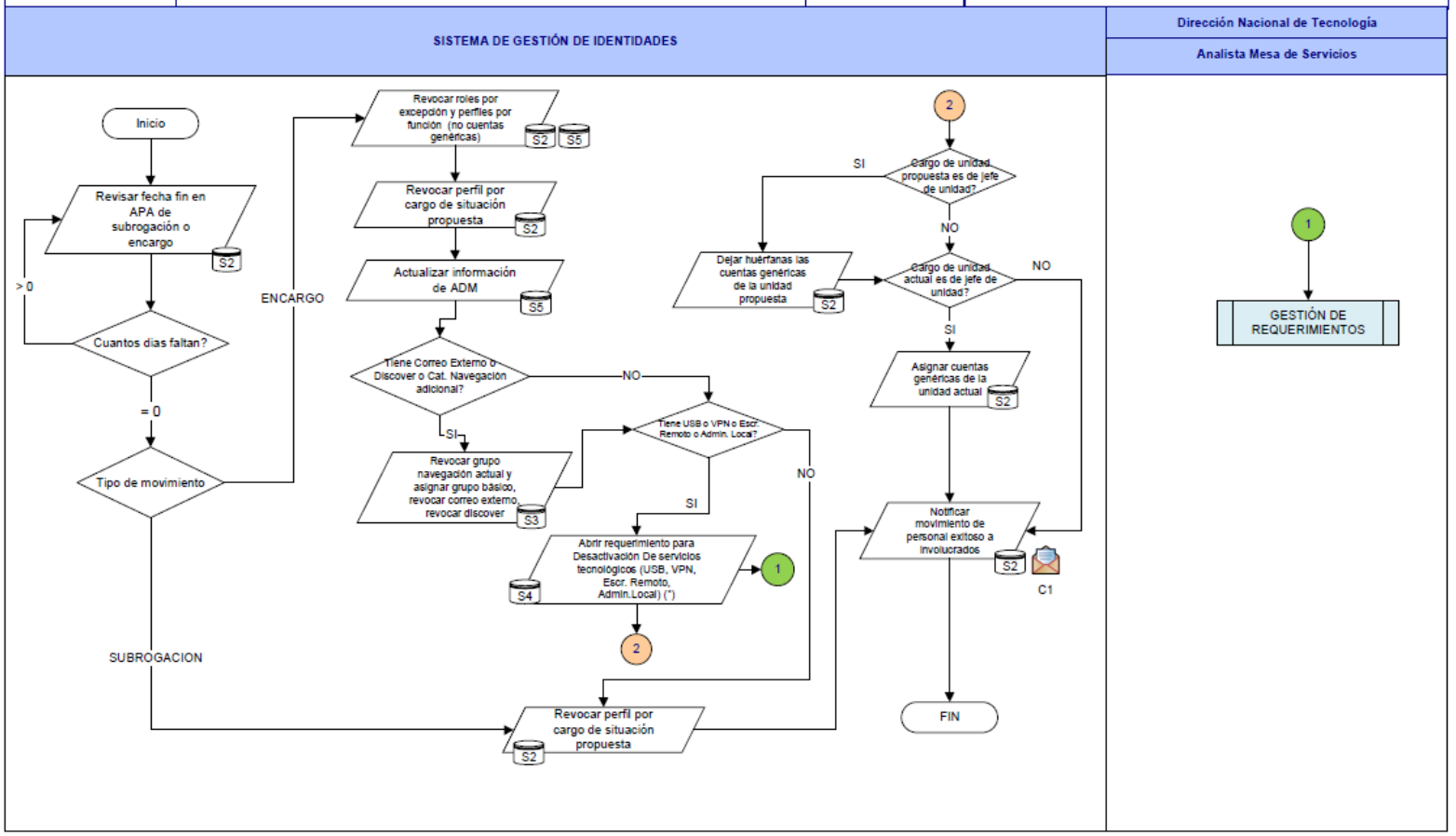
13.2.- Detalles Funcionales del Flujo

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.

Notificar actualización de fecha fin	Se debe enviar por correo electrónico la confirmación de actualización de fecha fin al solicitante, asignatario y administrador de accesos.
Notificar negación de solicitud	Se debe enviar por correo electrónico el rechazo de la solicitud y el motivo ingresado por el analista que gestionó la misma, al solicitante y administrador de accesos.

14.- Terminaciones de subrogaciones y encargos

DIAGRAMA DE FLUJO	PROCESO DE PRIMER NIVEL: GESTIÓN TECNOLÓGICA	CÓDIGO: PRO-GTI-OST-008	DOCUMENTOS SOPORTE:
	PROCESO DE SEGUNDO NIVEL: GESTIÓN DE OPERACIÓN DE SERVICIOS TECNOLÓGICOS	VERSIÓN: 6.0	SISTEMAS: S1. Sistema de Gestión del Talento Humano S2. Sistema de Identidades S3. Directorio Activo S4. Herramienta de Gestión de Requerimientos S5. Módulo de Administración de usuarios (ADM) NOTIFICACIONES C1. Notificación de finalización de la solicitud. C8. Notificación de generación de flujo. C9. Notificación de reasignación de cuentas genéricas
	PROCESO DE TERCER NIVEL: N/A	FECHA: JUNIO 2023	
	PROCEDIMIENTO: ADMINISTRACIÓN Y CONTROL DE ACCESOS LÓGICOS PARA USUARIOS FINALES		
	TERMINACIONES DE SUBROGACIONES Y ENCARGOS		



14.1.- Matriz Aclaratoria

Actividad del Flujo	Instrucción Aclaratoria
Revisar fecha fin en APA de subrogación o encargo	El sistema de Gestión de Identidades debe tener un mecanismo que lea diariamente la fecha fin de las APAs de subrogación y encargo.
¿Cuántos días faltan?	Si la fecha fin del APA es mayor a la fecha actual debe seguir revisando la fecha el día siguiente. Si la fecha fin del APA en igual o menor a la fecha actual el flujo continúa.
Tipo de movimiento	El sistema de Gestión de Identidades debe validar si el APA es de subrogación o encargo, la codificación de dichos tipos de APA será entregada por el SRI.
Revocar perfil por cargo de situación propuesta	El sistema de Gestión de Identidades debe revocar el perfil por cargo de la unidad administrativa propuesta indicada en el APA.

14.2.- Detalles Funcionales del Flujo

Funcionalidad	Descripción
Cargo de unidad propuesta	Si el cargo propuesto del APA es de jefatura (Coordinador, Jefe Departamental o Director) el sistema de Gestión de Identidades debe dejar huérfanas las cuentas genéricas que en ese momento tenga asignado el usuario,
Cargo de unidad actual	Si el cargo actual del APA es de jefatura (Coordinador, Jefe Departamental o Director) el sistema de Gestión de Identidades debe asignar las cuentas genéricas de la unidad administrativa actual del APA al usuario.

Anexo No. 1

Estándar para creación de usuarios

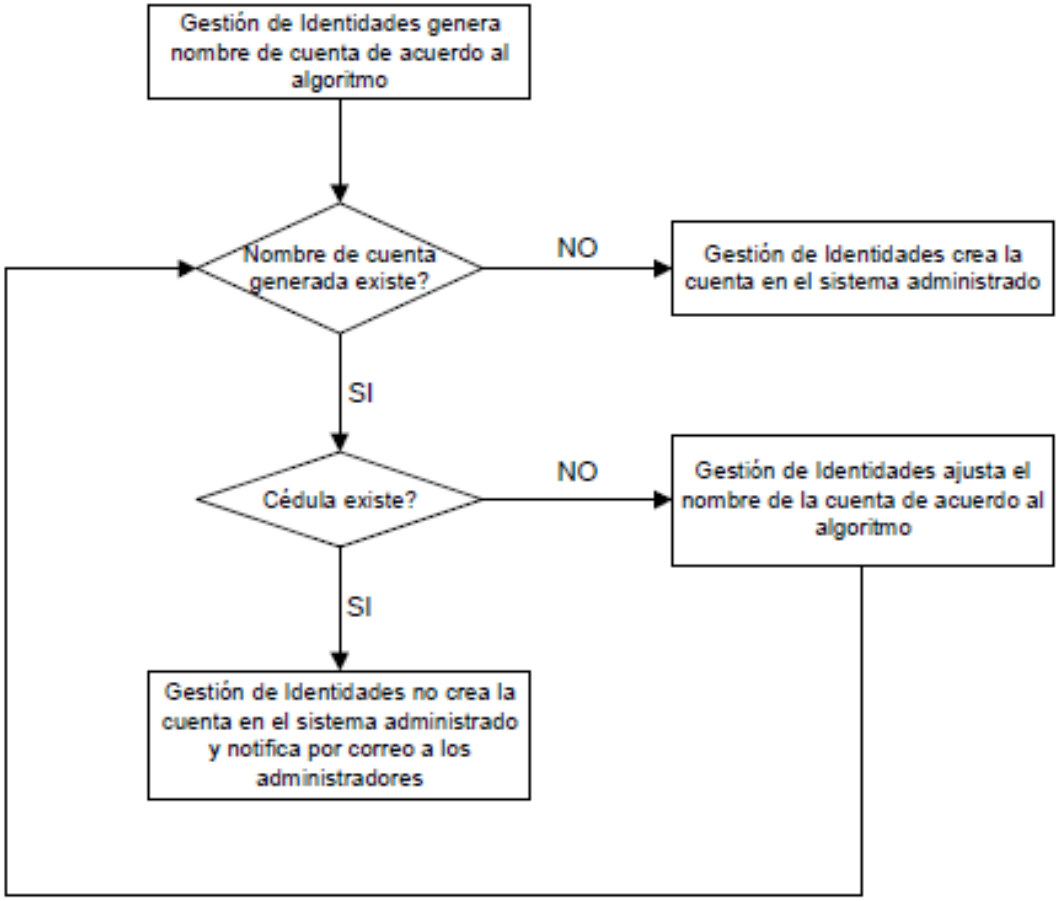
Cuenta funcionario / externo	Nombre Usuario
Marcelo **P**aúl **V**inueza **E**spín	mpve191108
(inicial primer nombre, inicial segundo nombre, inicial apellido paterno, inicial apellido materno, fecha De creación de cuenta).	

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):



Algoritmo para creación de buzones de correo: