1. OBJETIVO

Establecer los lineamientos de seguridad y privacidad para el control de acceso físico a las instalaciones de la Unidad para la Atención y Reparación Integral a las Víctimas - UARIV del Nivel Central, y para el control de acceso lógico a los Sistemas de información y Servicios de TI asignados a todos los funcionarios, contratistas, operadores, terceros, proveedores del (Nivel Central y Direcciones Territoriales) y/o a las Entidades Externas (Públicas o Privadas del Orden Nacional, Orden Territorial, Presencia Internacional) con el fin de preservar la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información de la Unidad para la Atención y Reparación Integral a las Víctimas - UARIV (en adelante también llamada la Entidad).

2. ALCANCE

- Ingreso físico del personal que labora con la Entidad (funcionarios, contratistas, operadores, terceros) a las instalaciones de la UARIV del Nivel Central ubicada en el Complejo San Cayetano en Bogotá D.C.

- Ingreso físico como visitante a las instalaciones de la UARIV del Nivel Central ubicada en el Complejo San Cayetano en Bogotá D.C.

- Ingreso físico de la ciudadanía a la ventanilla única de radicación para la ciudadanía de la UARIV donde realiza tramites con la Entidad ubicada en el Complejo San Cayetano en Bogotá D.C.

- Para el ingreso lógico a los Sistemas de Información para los funcionarios, contratistas, operadores, terceros, proveedores del (Nivel Central y Direcciones Territoriales) y/o a las Entidades Externas (Públicas o Privadas del Orden Nacional, Orden Territorial o Presencia Internacional) de la UARIV.

- Para el ingreso lógico a los Servicios TI para los funcionarios, contratistas, operadores, terceros y proveedores de la UARIV.

3. DEFINICIONES:

Administrador Funcional: Es el responsable de la creación, modificación, reactivación e inactivación de usuarios para el acceso a los Sistemas de Información y servicios de TI del área funcional a la que pertenece.

Administración delegada: Es el responsable de canalizar todas las solicitudes referentes a los Sistemas de Información que conforman el portafolio de servicios de la Subdirección de Atención y Asistencia Humanitaria (SAAH) en las Direcciones Territoriales de la Entidad, de igual forma aplica para la gestión del Sistema de Información **PORTAL VIVANTO**.
En ocasiones (según sea el caso) la Administración delegada puede crear el usuario y dar acceso a los Sistemas de Información.

Articulador Territorial de la SRNI: Es el interlocutor de la Subdirección Red Nacional de Información (SRNI), en las Direcciones Territoriales de la Entidad. A través del articulador se

deben canalizar todas las solicitudes referentes a los Sistemas de Información que conforman el portafolio de servicios de la SRNI.

Auditoria: Proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.

Autenticación de Usuario: Capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser.

Autorización[1]: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Ciudadanía[2]: condición que tienen las personas como habitantes de un país en la cual el ciudadano obtiene una serie de derechos civiles, políticos y sociales junto con unas obligaciones. Son las personas naturales o jurídicas que radican o consultan tramites que adelantan con la Entidad.

Confidencialidad[3]: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Unidades o procesos no autorizados.

Control de Acceso[4]: (inglés: Access control) Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.

Contratista[5]: Persona natural o jurídica que se vincula con una entidad contratante mediante la celebración de un contrato, cuya obligación es cumplir y ejecutar el objeto de este, el cual puede consistir en bienes, obras o servicios.

Colaborador Designado (Para Entidad Externa): Es la persona con la potestad otorgada por el representante legal como interlocutor con la Entidad. Aplica para los sistemas de la SRNI.
Dentro de sus funciones está: Brindar el apoyo y gestión para la suscripción de la solicitud de creación de usuarios y aceptación del acuerdo de confidencialidad con los usuarios o demás colaboradores de su Entidad a quienes se les permita el acceso a la información, y apoyar la divulgación y aplicación de los principios de veracidad, finalidad, confidencialidad, reserva, circulación restringida y salvaguarda de la información que se dispone a través del Intercambio de Información.

Colaborador Designado (Para Nivel Central y Dirección Territorial): Es el jefe inmediato o supervisor del contrato o dueño del Proceso o encargo del Proceso. aplica para los sistemas de la SRNI.

Dentro de sus funciones está: Es la encargada de firmar el "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad", aprobar la solicitud

[1] Fuente de definición https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
[2] Fuente de definición Concepto 70511 de 2015 Departamento Administrativo de la Función Pública
[3] Fuente de definición https://www.iso27000.es/sgsi.html
[4] Fuente de definición https://www.iso27000.es/sgsi.html
[5] Fuente de definición https://ansv.gov.co/es/atencion-ciudadania/glosario/contratista

para los (funcionarios, contratistas, operadores y proveedores), para el acceso a los Sistemas de Información y Servicios TI administradas por la Entidad, con el fin de ejecutar las actividades que dan cumplimiento a los objetivos Institucionales.

Delegado Interno: Es la persona asignada por el Colaborador Designado Interno cuando este no está disponible, para que realice la gestión frente a las solicitudes de acceso para los (funcionarios, contratistas, operadores y proveedores), para el acceso a los Sistemas de Información y Servicios TI administradas por la Entidad.

Directorio Activo: Mecanismo que se utiliza para gestionar y validar el acceso a los servicios y aplicaciones debido a que, en el directorio se almacena la información básica de usuarios de la Entidad, cuentas, e información de seguridad, como contraseñas.

Disponibilidad[6]: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Entidad Externa: Es un ente de persona (Natural o Jurídica) de orden nacional, territorial o con presencia internacional con las que se tiene un vínculo directo o indirecto que proporciona o recibe información para la Entidad.

Formato de solicitud de creación de usuarios y aceptación del Acuerdo de Confidencialidad: Documento en el que se especifica las herramientas a las que requiere acceso y las condiciones de manejo de la Información que se pone a disposición del usuario, con el fin de salvaguardar y restringir el uso de la información y propender por el buen manejo de los Sistemas de Información y Servicios TI.

Funcionario[7]: Un funcionario o funcionario público es aquella persona que trabaja para el Estado, desempeñando una función dentro de la Administración Pública. Estas personas se encuentran vinculadas a la función pública mediante un contrato laboral.

Integridad[8]: Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Operador[9]: Es un profesional o empresa que por encargo realiza el diseño, gestión, control y mantenimiento de algunas o todas las áreas de la cadena de suministro.

Perfil: suelen referirse a conjuntos de configuraciones y permisos asignados a un usuario o grupo de usuarios en donde tendrá unas funciones o responsabilidades asignadas. Estos perfiles definen lo que un usuario puede hacer dentro del sistema. Un perfil puede incluir varios roles. Por ejemplo: administrador, editor, analistas, usuario final.

Perfiles de Usuario[10]: Un perfil de usuario es una colección de configuraciones e información asociada con un usuario. Este se puede definir como la representación digital explícita de la

[6] Fuente de definición https://www.iso27000.es/sgsi.html
[7] Fuente de definición https://www.rankia.com/diccionario/economia/funcionario
[8] Fuente de definición https://www.iso27000.es/sgsi.html
[9] Fuente de definición https://acortar.link/eBCRqz
[10] Fuente de definición https://es.theastrologypage.com/user-profile

identidad del usuario con respecto al entorno operativo. La mayoría de los perfiles de usuario tienen un conjunto de parámetros que son obligatorios u opcionales.
El perfil de usuario permite la personalización del sistema y puede ayudarlo a personalizar ciertas funciones para sus necesidades.

Permisos: son autorizaciones específicas que se otorgan a un usuario para realizar ciertas acciones, como leer, escribir o modificar archivos o datos. Los permisos pueden ser parte de un perfil o asignados individualmente. Por ejemplo: ver, crear, editar, modificar o eliminar datos.

Proveedor: Un proveedor es a aquella persona física o jurídica que suministra profesionalmente un determinado bien o servicio a otros individuos o sociedades, como forma de actividad económica y a cambio de una contra prestación.

Sistemas de Información[11]: Conjunto de las aplicaciones y activos de tecnología donde se maneja de información.

Servicios TI: Son aquellas tecnologías que se necesitan para la gestión y transformación de la información, con la que se busca responder a las necesidades de los usuarios como: correo electrónico, telefonía, internet, servicio de almacenamiento, acceso, servicios de impresión, servicio de backup, Servidores, Base de Datos, VPN, entre otros.

Seguridad de la Información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta.

Solicitud: petición de un usuario solicitando accesos a Sistemas de Información y/o Servicios TI, asesoramiento. También es llamado Requerimiento.

Tercero: Convenios interadministrativos para practicas académicas o universidades con el fin de realizar actividades de gestión dentro de los procesos de la Entidad (pasantes).

Usuarios con privilegios: Son aquellos usuarios dentro de un sistema o red que tienen permisos especiales para realizar ciertas acciones que no están disponibles para usuarios comunes. Esto puede incluir acceso a configuraciones avanzadas, administración de usuarios, instalación de software, o la capacidad de modificar configuraciones críticas del sistema. Por ejemplo, un administrador en un sistema operativo o un "superusuario" en bases de datos.

Usuarios Generales: Son los usuarios regulares o estándar de un sistema. Su acceso y permisos están limitados a lo necesario para realizar sus tareas básicas. Por lo general, no pueden hacer cambios significativos en el sistema o red, y su alcance está diseñado para prevenir errores o actividades no autorizadas que puedan comprometer la seguridad o la estabilidad.

Visitante: Persona naturales o jurídicas que tiene un vínculo directo y/o indirecto con la Entidad, el cual ingresa por un periodo inferior a un (1) días a desarrollar actividades con los colaboradores de la Entidad.

[11] Fuente de definición https://normaiso27001.es/referencias-normativas-iso-27000/

4. ACTIVIDADES

4.1. CONTROL DE ACCESO:

El control de accesos físico y lógico es esencial para proteger recursos en entornos tanto tangibles como digitales. El control de accesos físico se centra en la regulación de la entrada a instalaciones, equipos o áreas específicas mediante mecanismos como cerraduras, tarjetas de acceso, lectores biométricos y sistemas de vigilancia. Por otro lado, el control de accesos lógico controla quién y cómo se accede a recursos digitales, como sistemas operativos, redes, aplicaciones y bases de datos, mediante autenticación y permisos específicos.

La importancia de ambos tipos de control radica en su capacidad para salvaguardar la seguridad y privacidad de los activos, previniendo accesos no autorizados y posibles amenazas, ya sea en el ámbito físico o en el virtual. Juntos, forman una estrategia integral de seguridad que permite a las Entidad reducir riesgos, proteger información crítica y garantizar la continuidad operativa en un entorno cada vez más interconectado. Esto subraya la necesidad de implementar medidas robustas en ambos frentes para mantener una infraestructura segura y confiable.

a. Para dar inicio al presente protocolo se debe tener en cuenta los siguientes pasos para su desarrollo y estricto cumplimiento:

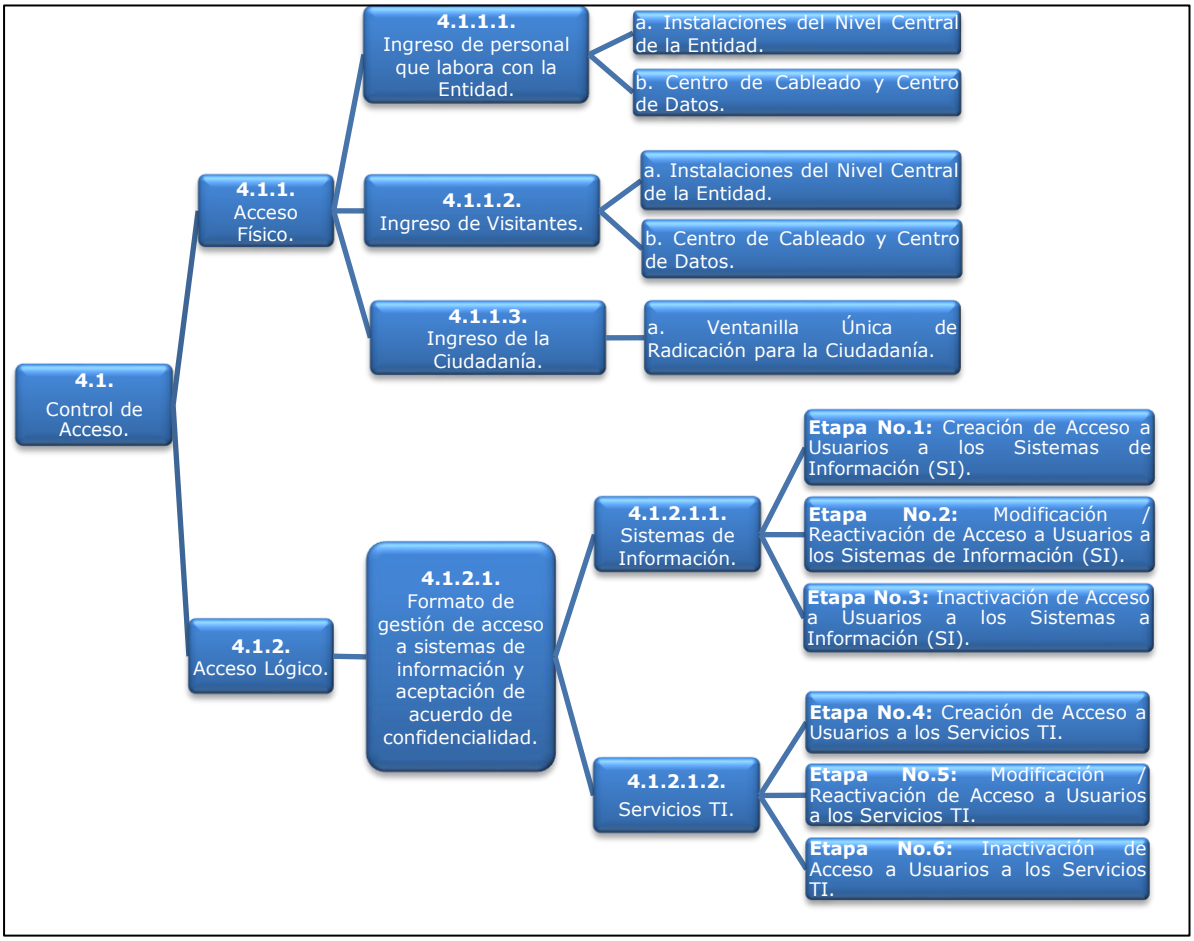


Imagen No.1 *– Desarrollo de la Gestión de Acceso a Usuarios.*

4.1.1. ACCESO FÍSICO:

Para iniciar con los accesos físicos a las instalaciones de la UARIV del Nivel Central, se deberá tener en cuenta lo siguientes pasos para la gestión y control del tránsito de personas:

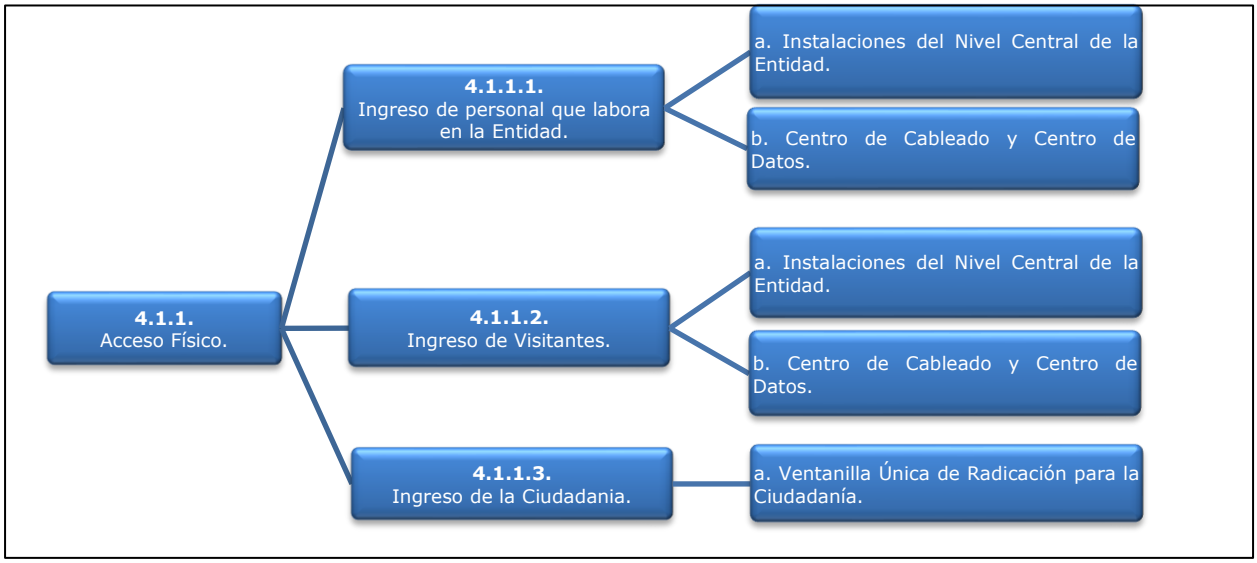


Imagen No.2 *– Acceso Físico – Nivel Central Unidad para las Víctimas.*

4.1.1.1. Ingreso Personal que labora con la Entidad:

a. Instalaciones del Nivel Central de la Entidad:

Permite gestionar y controlar el acceso en las instalaciones de la UARIV del Nivel Central de los colaboradores de la Entidad (funcionarios, contratistas, operadores, terceros) así:

- El líder del proceso o quien haga de sus veces realizara la solicitud a través del aplicativo en la Intranet: Solicitud de Autorización de Ingreso a la Sede de Nivel Nacional San Cayetano para habilitar el ingreso de los funcionarios, contratistas, operadores y terceros como personal que labora con la Entidad para que acceda de forma física a las instalaciones de UARIV del Nivel Central que se encuentra ubicado en el Complejo San Cayetano en Bogotá D.C.

- El líder del proceso o quien haga de sus veces enviara un correo a autorizacionesingreso@unidadvictimas.gov.co la cual está vinculada a una lista de distribución designada por Gestión Administrativa de la Entidad. En este correo se deberá especificar qué colaboradores tendrán ingreso permanente a las instalaciones de la Entidad en la sede de Nivel Nacional San Cayetano, incluyendo la siguiente información según corresponda:

Contratistas.	**Relacionar:** - Nombre y apellido. - Número de identificación. - Área / Dependencia / Proceso. - Piso. **Adjuntar:** - El CDP.
Operadores.	**Relacionar:** - Nombre y apellido. - Número de identificación. - Área / Dependencia / Proceso. - Piso.
Terceros.	**Relacionar:** - Nombre y apellido. - Número de identificación. - Área / Dependencia / Proceso. - Piso.
Funcionarios.	Talento humano envía la información (Nombre y apellido, Número de identificación, Área / Dependencia / Proceso).

Tabla No.1 *– Ingreso Físico Permanente.*

- Gestión Administrativa registrará en el aplicativo del Complejo San Cayetano el ingreso de forma "permanente" a los colaboradores de la Entidad. En respuesta al correo de solicitud, se enviará un mensaje con el pantallazo de la gestión realizada a las direcciones correspondientes de:

- La persona que realizo la solicitud. - Administración del Complejo San Cayetano. - Recepción San Cayetano. - Área de Seguridad. - Coordinación de vigilancia. - Monitoreo de cámaras. - Recepción de la Unidad para las Victimas. - autorizacionesingreso@unidadvictimas.gov.co

Tabla No.2 *– Notificación de la Gestión.*

Nota:

- ✓ El ingreso permanente solo se realiza por seis (6) meses por lo que se requiere volver a solicitar el acceso permanente por parte del Proceso.

- ✓ Únicamente los jefes de oficina tienen autorizado el ingreso a las Instalaciones de la Entidad después de 5:00pm.

- Para el ingreso de personal nuevo o antiguo que labore con la Entidad (funcionarios, contratistas, operadores y terceros) se requiere la firma en el "*Formato Compromiso de Confidencialidad y No Divulgación de la Información*" (firmado durante la vinculación o contratación), Este formato se encuentra relacionado en el **numeral 7. ANEXOS**.

- Cuando ingresa por primera vez, el personal que labora con la Entidad (funcionarios, contratistas, operadores y terceros) deberá anunciarse en la portería del Complejo San Cayetano en Bogotá D.C. y presentar el documento de identidad para el cotejar la información registrada en la solicitud y proceder habilitar el acceso por el torniquete del Complejo San Cayetano y los torniquetes de la recepción de la Entidad.

- El personal que labora con la Entidad (funcionarios, contratistas, operadores y terceros) deberá usar su documento de identidad o tarjeta de proximidad para el ingreso o salida por los torniquetes del Complejo San Cayetano y los torniquetes de la recepción de la Entidad.

- En caso de que los (funcionarios, contratistas, operadores y terceros) tengan dificultades para ingresar debido a problemas con la lectura de la tarjeta o documento de identidad en el torniquete del Complejo San Cayetano, deberán dirigiese a la portería del mismo Complejo con su documento de identidad o tarjeta de proximidad para reactivarla, siempre y cuando cuenten con ingreso permanente. De lo contrario deberán comunicarse con la Entidad para gestionar nuevamente el acceso.

- Cuando el personal que labora con la Entidad (funcionarios, contratistas, operadores y terceros) ingresa o sale con dispositivos electrónicos personales como (tablets, portátil, entre otros) deberá indicar y presentar el número de serie (S/N) del dispositivo en el punto de la recepción de la Entidad para el control de entrada y salida de este.

- Cuando el personal que labora con la Entidad (funcionarios, contratistas, operadores y terceros) ingresa o sale con dispositivos electrónicos de propiedad de la Entidad como (tablets, portátil, entre otros) deberá presenta memorando y/o correo electrónico de autorización avalado por el jefe inmediato y el responsable de Gestión Administrativa en el punto de la recepción de la Entidad para el control de entrada y salida de este.

b. Centro de Cableado y Centro de Datos:

Si se requiere realizar actividades como: auditorías, mantenimiento, afinamiento o configuración de los equipos, cambios de infraestructura tecnología, reparaciones físicas, aseo, entre otros, deberá:

- Estar acompañado durante su visita por el Líder del Dominio de Infraestructura TI o quien haga de sus veces de la Oficina de Tecnología de la Información (OTI).

- Registrar la entrada y salida en el formato "Bitácora de Ingreso Centro de Datos", este formato se encuentra relacionado en el **numeral 7. ANEXOS,** por el líder del Dominio de Infraestructura TI o quien haga de sus veces de la Oficina de Tecnología de la Información (OTI).

- El formato "Bitácora de Ingreso Centro de Datos" debe permanecer dentro del Centro de Cableado y Centro de Datos de forma permanente y mantener el histórico anual del mismo. Este formato se encuentra relacionado en el **numeral 7. ANEXOS**.

4.1.1.2. Ingreso a Visitantes:

a. Instalaciones del Nivel Nacional de la Entidad:

- El líder del proceso o quien haga de sus veces realizara la solicitud a través del aplicativo de la Intranet: Solicitud de Autorización de Ingreso a la Sede de Nivel Nacional San Cayetano para habilitar el ingreso de visitantes de la Entidad para que acceda de forma física a las instalaciones de la UARIV del Nivel Central que se encuentra ubicado en el Complejo San Cayetano en Bogotá D.C.

- El líder del proceso o quien haga de sus veces enviara un correo a autorizacionesingreso@unidadvictimas.gov.co la cual está vinculada a una lista de distribución designada por Gestión Administrativa de la Entidad. En este correo se deberá especificar los datos del visitante así:

Visitante	**Relacionar:** - Nombre y apellido. - Número de identificación. - Área / Dependencia / Proceso. - Piso.

Tabla No.3 *– Ingreso Físico Visitantes.*

Nota:

- ✓ El ingreso de visitante está en una franja de 8:00am a 5:00pm.
- ✓ Los visitantes deberán indicar en la recepción de la portería que ya no van a volver a ingresar más a las instalaciones del a Entidad.
- ✓ Se enviará un correo al solicitante cuando el visitante ingresa y sale del Complejo de San Cayetano.
- ✓ Después de su registro de salida del visitante por los torniquetes del Complejo San Cayetano y que sean las 5:00pm del día del ingreso del visitante este será desactivado. Si requiere volver a ingresar deberá realizarse la solicitud como se indicó en el **"numeral 4.1.1.2. del literal a"** del presente protocolo. En los casos particulares donde el visitante requiere ingresar de manera consecutiva durante la semana, se deberá registrar la renovación semanalmente.

- Para el ingreso físico de visitantes **NO** se requiere diligenciar el *"Formato Compromiso de Confidencialidad y No Divulgación de la Información"*.

- El visitante se debe anunciar portería del Complejo San Cayetano en Bogotá D.C. y presentar el documento de identidad para el cotejar la información registrada en la solicitud y proceder al registro para su ingreso.

- El visitante deberá usar su documento de identidad para el ingreso por los torniquetes del Complejo San Cayetano y los torniquetes de la recepción de la Entidad.

- Si el visitante ingresar dispositivos electrónicos como (tablets, portátil, entre otros) deberá indicar y mostrar el número de serie (S/N) del dispositivo en el punto de la recepción de la Entidad.

- Cuando el visitante salga de la Entidad, deberá presentar el dispositivo electrónico y mostrar el número de serie (S/N) del dispositivo en el punto de la recepción de la Entidad para que sea de salida de este.

b. Centro de Cableado y Centro de Datos:

Si el visitante requiere realizar actividades como: (auditorías, mantenimiento, afinamiento o configuración de los equipos, cambios de infraestructura tecnología, reparaciones físicas, aseo, entre otros) deberá:

- Estar acompañado durante su visita y permanecía por el Líder del Dominio de infraestructura TI o quien haga de sus veces de la Oficina de Tecnología de la Información (OTI).

- Registrar la entrada y salida en el formato "Bitácora de Ingreso Centro de Datos".

- El formato "Bitácora de Ingreso Centro de Datos" debe permanecer dentro del Centro de Cableado y Centro de Datos de forma permanente y mantener el histórico anual del mismo. Este formato se encuentra relacionado en el **numeral 7. ANEXOS** del presente documento.

4.1.1.3. Punto de Atención al Ciudadano:

a. Ventanilla Única de Radicación para la Ciudadanía:

- Para el ingreso de la Ciudadanía **NO** se requiere diligenciar el Compromiso de Confidencialidad y No Divulgación de la Información.

- El Ciudadano que realiza tramites con la Entidad, deberá presentar el documento de identidad en la portería del Complejo San Cayetano en Bogotá D.C. para que sea registrado.

- El Ciudadano deberá usar su documento de identidad para el ingreso por los torniquetes del Complejo y será acompañado por el guarda de seguridad de la Entidad hasta el punto de atención al ciudadano de la Entidad "Ventanilla de Radicaciones".

- Después de su registro de salida del Ciudadano por los torniquetes del Complejo San Cayetano, se desactivará el acceso. Si requiere ingresar nuevamente deberá realizar el trámite indicado en el presente **numeral**.

4.1.2. ACCESO LÓGICO:

La gestión de acceso lógico apoya a la adecuada creación de cuentas de usuario y niveles de privilegio, lo cual es fundamental para preservar la Confidencialidad, Integridad y

Disponibilidad de los activos de información. A continuación, se presentan unas directrices por dominio pertenecientes a la OTI:

Sistemas de Información:

- Se debe ejecutar el presente protocolo para obtener credenciales de acceso para los ambientes de pruebas y producción.

- Los usuarios que sean requeridos para el consumo de Servicios Web deben ser creados a nombre de la aplicación o Sistema de Información que consume el servicio y el responsable de la cuenta es el administrador funcional del Sistema de Información que consume el servicio.

- Cada Administrador Funcional del Sistema de Información debe definir y mantener actualizado ante el Sistema de Gestión de Seguridad de la Información, el delegado interno para la generación de solicitudes de creación de usuarios.

- Para obtener más información sobre la creación de acceso, modificación, reactivación e inactivación en los Sistemas de Información, consulte el **numeral 4.1.2.2.** del presente documento.

- Ningún usuario puede ser genérico, excepto aquellos utilizados para integraciones con Sistemas de Información como: Servicios Web o Web Services.

- Para los operadores que cuenten con acceso a Sistemas de información **no deberán tener usuario genérico** porque comprometen la Seguridad de la Información.

Excepciones:

- Para los Sistemas de Información que utilizan Servicios Web y requieren credenciales para su integración, se deben **usar únicamente en este caso usuarios genéricos**, con el fin de no afectar la operación. Por esta razón, este usuario debe tener un responsable asignado como, por ejemplo, el Líder del Proceso.

- Para los Sistemas de Información en ambientes de prueba, se podrán utilizar únicamente "usuarios genéricos" para actividades relacionadas con pruebas de versión, corrección de errores reportados y/o mejoras.

Servicios TI:

- Se debe ejecutar el **"Procedimiento Gestión de Servicios e Infraestructura Tecnológica",** este formato se encuentra relacionado en el **numeral 7. ANEXOS** del presente documento. Aplicando los instructivos según sea el caso para obtener credenciales de acceso tales como: (servidores, base de datos, repositorio de información, VPN, entre otros). Para el caso de VPN se deberá realizar la solicitud a través de la **"APP Solicitud VPN"** la cual se encuentra en los aplicativos específicos en la Intranet.

- Para obtener más información sobre la creación de acceso, modificación, reactivación e inactivación de los Servicios TI, consulte el **numeral 4.1.2.2.**

Para garantizar una gestión eficiente y segura de los accesos lógicos a los Sistemas de Información y/o Servicios TI de la Entidad, es crucial seguir una serie de pasos estratégicos.

- En primer lugar, se debe establecer un proceso de autenticación sólido, basado en credenciales seguras, "autenticación multifactor" y políticas de acceso definida por roles.

- Además, la implementación de mecanismos de monitoreo continuo permitirá la detección temprana de amenazas o accesos no autorizados, facilitando una respuesta oportuna ante posibles incidentes de seguridad.

- Asimismo, la administración de accesos debe adaptarse a las dinámicas y necesidades operativas y a los cambios estructurales de la Entidad.

- Es recomendable mantener un registro detallado de los accesos otorgados y realizar auditorías periódicas para identificar posibles vulnerabilidades.

- Además, fomentar una cultura de seguridad de la información mediante capacitaciones constantes sobre buenas prácticas, al igual que el cumplimiento normativo interno, contribuirá significativamente a la protección de los datos y a la optimización del uso de los recursos tecnológicos.

A continuación, se presenta el flujo de las actividades para los accesos lógicos:

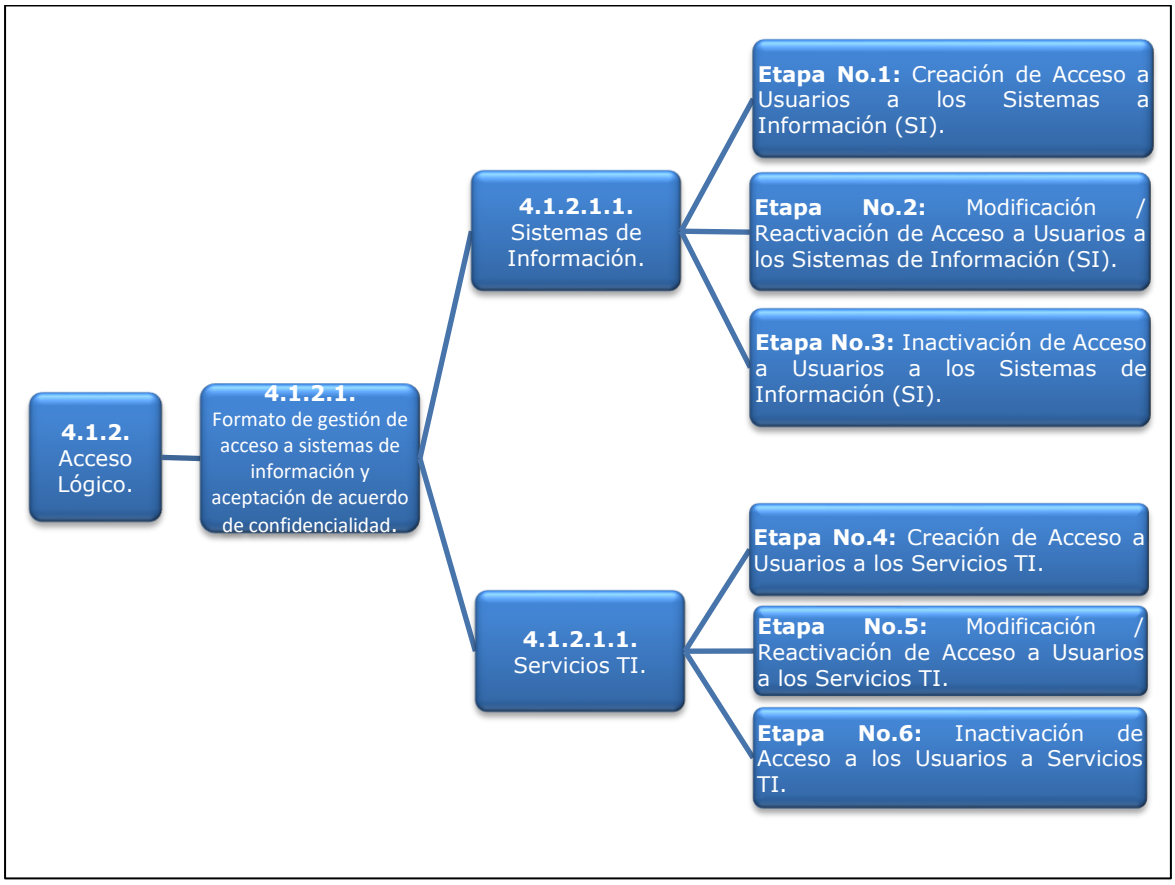


Imagen No.3 *– Acceso Lógico.*

4.1.2.1. Solicitud de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad:

El formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad debe ser diligenciado y firmado como requisito fundamental para la creación y asignación de credenciales de acceso en los Sistemas de Información (SI) de la Entidad, incluyendo funcionarios, contratistas, operadores, terceros y proveedores, así como en los procesos de articulación con **entidades públicas o privadas** que actúen como **usuarios externos**. Su implementación contribuye al cumplimiento de las políticas de seguridad de la información y a la prevención de accesos **NO** autorizados, fugas o mal uso de datos sensibles.

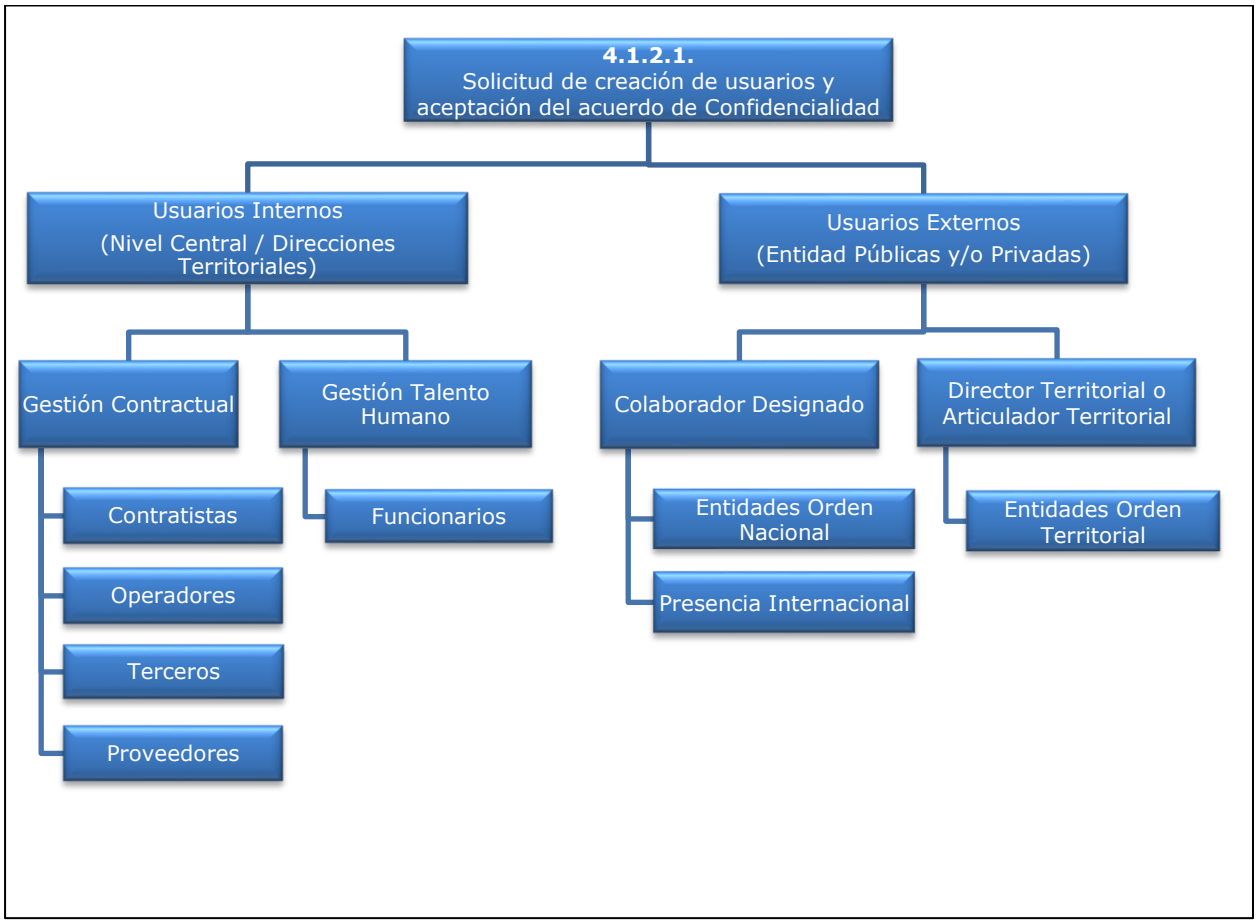


Imagen No.4 *- Acceso Lógico – Acuerdo de Confidencialidad.*

En conclusión:

a. El diligenciamiento del "Formato de Gestión de Acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad" es de estricto cumplimiento para todos los usuarios internos y externos con quien se tenga un vínculo directo e indirecto con la Entidad.

b. Puede ser diligenciada de forma física y/o digital y/o a través de una herramienta que se definida para tal fin.

c. En un mismo "Formato de Gestión de Acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad" se pueden asociar uno o varios Sistemas de Información. Estos accesos para los Sistemas de Información deben ser solicitados uno a uno por cada Sistema de Información mediante la creación de un caso en la Herramienta de Gestión de la Entidad o el canal designado para tal fin.

d. En dicho formato se deben relacionar lo siguiente:

Lista de herramientas:	Se relacionar los Sistemas de Información y/o Servicios TI.
Modulo:	Se especifica el módulo(s) del Sistema de Información al cual accederá el usuario, cuando aplique según sea el caso. Algunos pueden ser: consulta individual, sistema unificado de cifras, reportes, consultas generales, etc. **Nota**: Para SGV (Sistema de Gestión para las Víctimas) y SM (Subsistencia Mínima) este campo es opcional, en caso de resolver inquietudes consultar con el delegado interno.
Perfil:	Se definen los perfiles que estén autorizados para ese rol asignado al usuario dentro del Sistema de Información y/o Servicios TI. (Cuando aplique según sea el caso).
Observaciones / Permisos / Actividad:	Se especifica las acciones que el usuario puede realizar dentro del Sistema de Información y/o Servicio TI. (Cuando aplique según sea el caso). **Nota**: Para SGV (Sistema de Gestión para las Víctimas) y SM (Subsistencia Mínima) este campo es opcional, en caso de resolver inquietudes consultar con el delegado interno.
Horario:	Se define el tiempo en los que el usuario puede acceder a los Sistemas de Información. (Cuando aplique según sea el caso). **Nota**: Para relacionar el horario consulte el Manual del Sistema de Información al que requiere permisos.

***Tabla No.4** – Detalle del "Acuerdo de Confidencialidad".*

e. El "Formato de Gestión de Acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad" para los proveedores se debe realizar únicamente para los casos en que requiera un usuario de conexión para:
   - Afinamiento y/o configuración de las herramientas de infraestructura TI.
   - Herramientas de gestión adquiridas.
   - Desarrollos externos adquiridos.
   - Entre otros.

f. El "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad" debe estar firmado por el usuario titular y el Colaborador Designado/Enlace Unidad o Articulador director/Enlace Territorial, y este debe verificar los siguientes criterios:
   - Que se cuenten con todos los campos registrados.
   - Que los Sistemas de Información solicitados sean acordes a las necesidades del usuario.
   - Que los perfiles asociados estén acorde a los módulos en caso de que se requiera.

g. Así mismo, el mencionado formato debe estar firmado por:

Solicitud y aceptación del acuerdo de Confidencialidad	Usuario Titular	Firma del Aprobador o Autorizador
Usuarios Internos	**Nivel Central:** • Funcionarios. • Contratistas. • Operadores. • Terceros. • Proveedores (según sea el caso).	**Colaborador designado:** Jefe inmediato o supervisor de contrato o dueño del Proceso o encargado del Proceso del Nivel Central. **Nota:** para concederse el acceso a los Sistemas de Información se deberá verificar el diligenciamiento del formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad.
	Dirección Territorial: • Funcionarios. • Contratistas. • Operadores.	**Articulador Territorial:** Director Territorial o Articulador Territorial. **Nota:** para concederse el acceso a los Sistemas de Información se deberá verificar el diligenciamiento del formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad.
Usuarios Externos	**Entidades Externas Públicas o Privadas:** • Del Orden Nacional. • Presencia Internacional.	**Colaborador Designado:** Para las Entidades de Orden Nacional / Presencia Internacional. **Nota para Consulados:** Deben estar con validadas por la Subdirección de Valoración y Registro (SVR) quien, valida la información registrada en la toma de la declaración tramitada por el ministerio público, consulados y cancillerías en el exterior.
	Entidades Externas Públicas o Privadas: • Del Orden Territorial.	Director Territorial o Articulador Territorial firmará los acuerdos del enlace Municipal de Víctimas para acceso a SGV.

Tabla No.5 *– Firmas del "Acuerdo de Confidencialidad".*

h. Se debe tener en cuenta los siguientes lineamientos de Gestión Documental para el almacenamiento, custodia y vigencia de las solicitudes diligenciadas mediante el "Formato de Gestión de Acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad" así:

Formato de Gestión de Acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad			
	Almacenamiento	**Custodia**	**Vigencia**
Físicos.	Las solicitudes de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad deben estar almacenados en el expediente, del contrato celebrado con terceros o el expediente del contratista o historia laboral del funcionario. • **Historias laborales:** En la carpeta de los funcionarios. • **Contratos:** En la carpeta de los contratistas. • **Convenios interadministrativos y/o interinstitucionales de la red:** En la carpeta de los convenios. • **Operadores:** En la carpeta de los operadores. En caso de externos, la custodia física debe gestionarla la dependencia que estableció el acuerdo de intercambio de información en articulación con el Grupo de Gestión Documental.	La Solicitud de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad son custodiados por el responsable de cada uno de los expedientes de: • Historias laborales. • Contratos. • Convenios. • Operadores.	La Solicitud de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad tienen vigencia de almacenamiento de acuerdo con la Serie Documental a la que corresponda cada expediente, el cual es indicado en la Tabla de Retención Documental **(TRD)**.
Digitales	Las solicitudes de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad deben estar almacenados en **ArchiDHU** de acuerdo con el tipo de vinculación que se tenga con la entidad. • Historias laborales: En la carpeta de los funcionarios. • Contratos: En la carpeta de los contratistas. • Convenios interadministrativos y/o interinstitucionales de la red: En la carpeta de los convenios. • Operadores: En la carpeta de los operadores. • El histórico individual de las solicitudes de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad o los históricos "Acuerdos de Confidencialidad" diligenciados previo a la oficialización del presente protocolo se mantiene en el **PORTAL VIVANTO, SGV, INDEMNIZA y MAARIV**.	• Las solicitudes de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad son custodiadas por Gestión Documental que administra el Sistema de Información **ArchiDHU** (Cuando se cuente con interoperabilidad según se el caso). • Cuando se crea el caso en la Herramienta de Gestión de la Mesa de Ayuda de Servicios Tecnológicos, se carga "la solicitud de creación de usuarios y aceptación del acuerdo de Confidencialidad" y demás documentos para la solicitud.	Las solicitudes de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad tienen vigencia de almacenamiento de acuerdo con la Serie Documental a la que corresponda cada expediente, el cual es indicado en la Tabla de Retención Documental **(TRD)**.
Herramienta Tecnológica.	Los Acuerdos de Confidencialidad (históricos) y las nuevas solicitudes de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad son custodiados por Gestión Documental que administra el Sistema de Información **ArchiDHU** (Cuando se cuente con interoperabilidad según se el caso).	Los Acuerdos de Confidencialidad son custodiados por Gestión Documental que administra el Sistema de Información **ArchiDHU** (Cuando se cuente con interoperabilidad según se el caso).	Los Acuerdos de Confidencialidad tienen vigencia de almacenamiento de acuerdo con la Serie Documental a la que corresponda cada expediente, el cual es indicado en la Tabla de Retención Documental **(TRD)**.

Tabla No.6 *– Almacenamiento, custodia y vigencia de los Acuerdos de Confidencialidad.*

Nota: Adicional a la solicitud de gestión de acceso a Sistemas de Información y aceptación del acuerdo de Confidencialidad, que se diligencia en el marco del presente protocolo, los funcionarios, Contratistas y Personal vinculado por Operador deben firmar Compromiso de Confidencialidad y No Divulgación de la Información durante la vinculación o contratación. Para esto, se establece el "*Formato Compromiso de Confidencialidad*", este formato se encuentra relacionado en el **numeral 7. ANEXOS** del presente documento.

4.1.2.1.1. Sistemas de Información:

Para tramitar una solicitud de acceso a los Sistemas de Información se deberá contar primero con el trámite indicado en el **numeral 4.1.2.1. solicitud de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad** del presente documento.

Solicitudes:

- Para concederse el acceso a los Sistemas de Información se deberá verifica el diligenciamiento del formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad.

- Las solicitudes del Nivel Central que requiera permisos de acceso a los Sistemas de Información del **PORTAL VIVANTO** deben venir con visto bueno y revisadas previamente por (Colaborador Designado (Para Entidad Externa) y/o Colaborador Designado (Para Nivel Central y Dirección Territorial) de la Subdirección Red Nacional de Información (SRNI).

- La Subdirección Red Nacional de Información (SRNI) enviará de forma trimestral a los jefes de áreas o enlaces que administra los Sistemas de Información, el listado de colaboradores designados con el fin de que se mantenga la información actualizada. (cuando se presente algún cambio antes del periodo del reporte deberá informarse). De igual forma las demás áreas deberán realizar el mismo reporte.

- Para las Entidades Públicas o Privada del (Orden Nacional / Orden Territorial / Presencia Internacional) requiere que:

  a. Las solicitudes sean realizadas por el colaborador designado, con la información del funcionario de la Entidad Externa que solicita el acceso al sistema de información.
  b. Las solicitudes de Entidades Externas del Nivel Nacional con Presencia Territorial deben ser escaladas por el Colaborador Designado y no desde el Director/Articulador Territorial.
  c. Las solicitudes que son tramitadas por el Ministerio Público, Consulados y Cancillerías en el exterior para otorgar usuarios a través de la herramienta de "toma en línea", en el cual se genera la declaración, son validadas por la Subdirección de Valoración y Registro (SVR).

NOTA:

- Para efectuar la solicitud de acceso a los Sistemas de Información se deberá registrar un caso en la Mesa de Servicios tecnológicos a través de la Herramienta de Gestión definida por la Entidad.

- Para las solicitudes de Usuarios Externos Entidad (Públicas y/o Privadas) de Orden Nacional / Orden Territorial / Presencia Internacional, será el articulador que creará los casos en la Herramienta de Gestión de la Entidad. (Ver el Procedimiento de Gestión de Servicios e Infraestructura Tecnológica).

- Para las solicitudes de acceso a SM (Subsistencia Mínima) y SGV (Sistema de Gestión para las Víctimas), deberán ser enviadas al correo adminsaah@unidadvictimas.gov.co donde se realiza la verificación de que cumplan todos los requisitos antes de ser creada la solicitud del caso en la Mesa de Servicios tecnológicos a través de la Herramienta de Gestión definida por la Entidad.

- Para la creación de usuarios en Vivanto, por parte de usuarios externos, la Entidad tercera debe tener un documento político legal y/o documento técnico para intercambio de información.

Crear el caso para Sistemas de Información:

Se debe registrar en la Mesa de Servicios tecnológicos a través de la Herramienta de Gestión para solicitudes de acceso a los Sistemas de Información (según la necesidad). Remitirse al Procedimiento de Gestión de Servicios e Infraestructura Tecnológica:

- ✓ Creación de acceso a usuario.
- ✓ Modificación y reactivación de acceso a usuario.
- ✓ Inactivación de acceso a usuario.

A continuación, se detallan los responsables para la creación de caso:

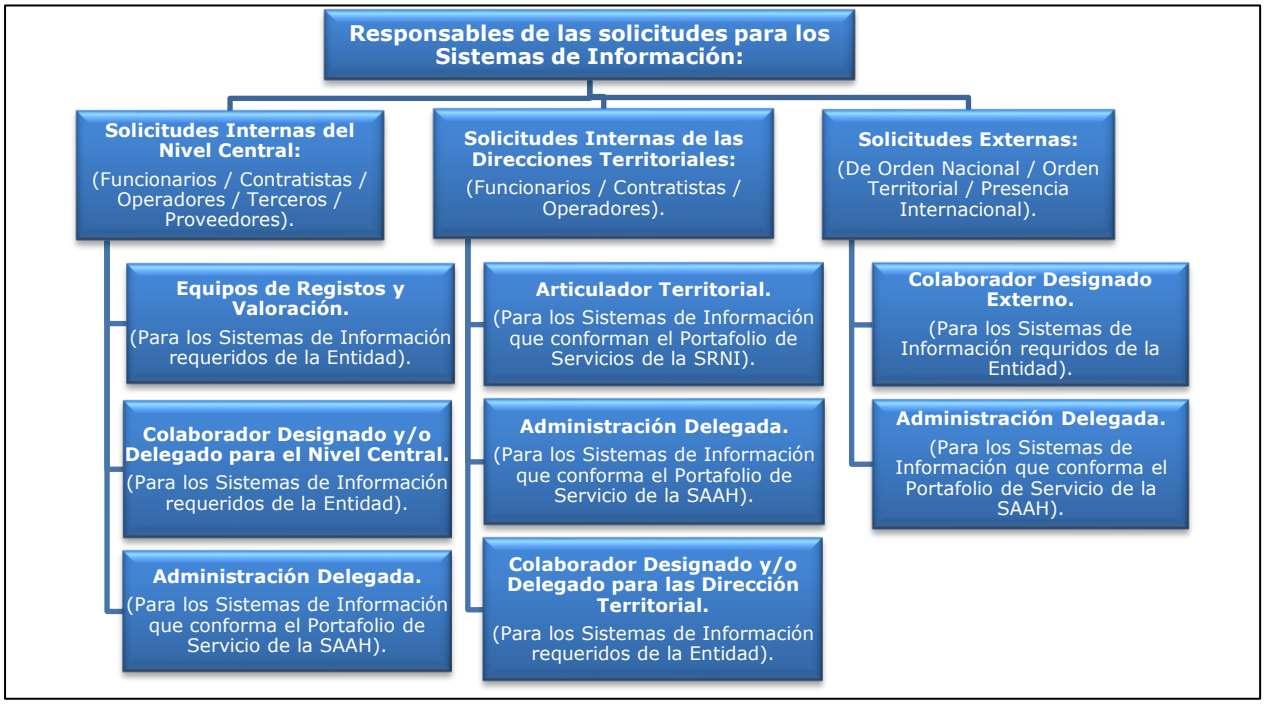


Imagen No.5 *– Responsable de la creación del caso para la solicitud para las fases.*

NOTA:

- Cabe resaltar, que para los usuarios internos (Nivel Central / Direcciones Territoriales) la solicitud se realiza desde el jefe del grupo o dependencia para funcionarios y Contratistas.

- Cabe resaltar, que para los operadores (Nivel Nacional / Dirección Territorial) la solicitud la debe realizar el supervisor del contrato.

Para crear el caso se debe tener en cuenta las siguientes recomendaciones para la creación, modificación, reactivación o inactivación).

Solicitud	Indicaciones
Creación de acceso a usuario.	• **Adjuntar:** (Cuando aplique) la Matriz en (Formato listado-personas-v1.xlsx) con la relación de todas las solicitudes, dado que permite corroborar información que se encuentra en los formatos diligenciados de solicitud de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad con el fin de minimizar errores. • **Adjuntar:** El "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad" relacionados en la Matriz de Excel indicada anteriormente. (En formato PDF). • **Adjuntar:** (Cuando aplique) para el Sistema RUV - Toma en Línea, para los personeros se deberá unificar en un (solo archivo PDF) el Formato de Autorización Firma y el Acta de Posesión. **Nota:** 1. Remitirse al Procedimiento de Gestión de servicios e infraestructura tecnológica para la generación para la creación de casos de Mesa de Ayuda para generar la solicitud de credenciales de acceso en Sistemas de Información (Cuando aplique). 2. Se recomienda tener en cuenta las indicaciones que se encuentran: a. En los manuales de los Sistemas de Información. b. La información que se encuentra en la **Etapa No.1** del presente documento.
Modificación de acceso usuario.	• **Adjuntar:** nuevo "Formato de Gestión de Acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad" en donde se registren los Sistemas de Información que requieren modificación en cuanto a módulo o perfil requerido. (En formato PDF) y la Matriz en Formato Excel (Formato listado-personas-v1.xlsx) (Cuando aplique) en donde se relaciona los Acuerdos, dado que permite corroborar la información que se encuentra en los "Acuerdos de Confidencialidad" con el fin de minimizar errores. • **Adjuntar:** (Cuando aplique) para el Sistema RUV - Toma en Línea, para los personeros se deberá unificar en un (solo archivo PDF) el Formato de Autorización Firma y el Acta de Posesión. **Nota:** 1. Remitirse al Procedimiento de Gestión de Servicios e Infraestructura Tecnológica para la creación de casos de Mesa de Ayuda para generar la solicitud de modificación del permiso de acceso Sistemas de Información (Cuando aplique). 2. Se recomienda tener en cuenta las indicaciones que se encuentran: a. En los manuales de los Sistemas de Información b. La información que se encuentra en la **Etapa No.2** del presente documento.
Reactivación de acceso usuario.	Se solicita el numero cedula, nombre y apellido y la justificación por la inactivación. **Ejemplos para reactivación:** Contraseñas erradas, tiempo sin acceso al Sistemas de Información, entre otros. **Nota:** 1. Debe crear solicitud a través de la Mesa de Servicios Tecnológicos. Procedimiento de Gestión de Servicios e Infraestructura Tecnológica. (Cuando aplique). 2. Se recomienda tener en cuenta las indicaciones que se encuentran en la **Etapa No.2** del presente protocolo.
Inactivación de acceso usuario.	• **Adjuntar:** el archivo de Excel (Formato listado-personas-v1.xlsx) con la relación de usuarios con las novedades de inactivación (solicitudes masivas). **Nota:** 1. Creación de solicitud de inactivación en Aranda. Remitirse al Procedimiento Gestión de Servicios e Infraestructura Tecnológica, para la creación de solicitudes de inactivación y creación de tickets o casos de la Mesa de Servicios Tecnológicos, asignados a los administradores funcionales de sistemas de información.

	2. Las solicitudes de inactivación de usuarios podrán remitirse por correo electrónico a los administradores funcionales de sistemas de información. 3. Respecto a funcionarios: La inactivación permanente o temporal debe realizarse a partir de las novedades que sean informadas por el Grupo de Gestión del Talento Humano, incluyendo: a. Desvinculación de personal b. Vacaciones c. Licencias no remuneradas d. Comisiones de servicio e. Incapacidad médica extendida f. Suspensión disciplinaria g. Traslados de personal 4. Se recomienda tener en cuenta las indicaciones que se encuentran: a. La información que se encuentra en la **Etapa No.3** del presente protocolo. 5. Se podrán inactivar usuarios de manera temporal o permanente según el caso, a partir de presunto uso irregular o anómalo que se identifique desde el monitoreo interno de uso de sistemas de información. En esta situación, se solicitará al usuario involucrado la correspondiente justificación del presunto uso irregular o anómalo. En caso de contar con una justificación satisfactoria, se procederá a realizar la reactivación del usuario. a. En caso de requerirse investigación[12] (Grupo Contra Fraude o por autoridades competentes) las credenciales de acceso involucradas se mantendrán inactivas. La reactivación de las credenciales de acceso del usuario involucrado dependerá del cierre y conclusión de la investigación. En este escenario, si la entidad Externa requiere tener acceso al sistema de información, el colaborador designado deberá solicitar el acceso para otro usuario.

Tabla No.7 *– Indicaciones para la creación del caso para los Sistemas de Información.*

NOTA: Se deberá unificar en un solo archivo (En formato PDF) el "Formato de Gestión de Acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad" y la Fotocopia de Cédula, razón por la cual se recomienda revisar los requerimientos para la creación de usuarios del Sistema de Información al cual requiere acceso que se encuentra en el **numeral 7. ANEXOS** del presente protocolo.

Etapas para Acceso lógico a los Sistemas de Información:

A continuación, se detallan las etapas para la creación, modificación, reactivación e inactivación de acceso a los Sistemas de Información:

Etapas	Usuario Interno		Usuario Externo Entidad Públicas y/o Privadas		
Etapa No.1 Creación de Acceso a Sistemas de Información.	Nivel Central	Dirección Territorial	Orden Nacional	Orden Territorial	Presencia Internacional
Etapa No.2 Modificación y/o Reactivación de Acceso a Sistemas de Información.	Nivel Central	Dirección Territorial	Orden Nacional	Orden Territorial	Presencia Internacional
Etapa No.3 Inactivación de Acceso a Sistemas de Información.	Nivel Central	Dirección Territorial	Orden Nacional	Orden Territorial	Presencia Internacional

Tabla No.8 – Etapas para el Acceso Lógico a los Sistemas de Información.

[12] La determinación de inicio de investigación se realizará por parte del Grupo Antifraude de la Oficina Asesora Jurídica, a partir del seguimiento del uso de los sistemas de información.

Etapa No.1:

Creación de Acceso a Usuarios a los Sistemas de Información.
Revisar los tipos de usuarios que le aplican para la creación de acceso para los Sistemas de Información:

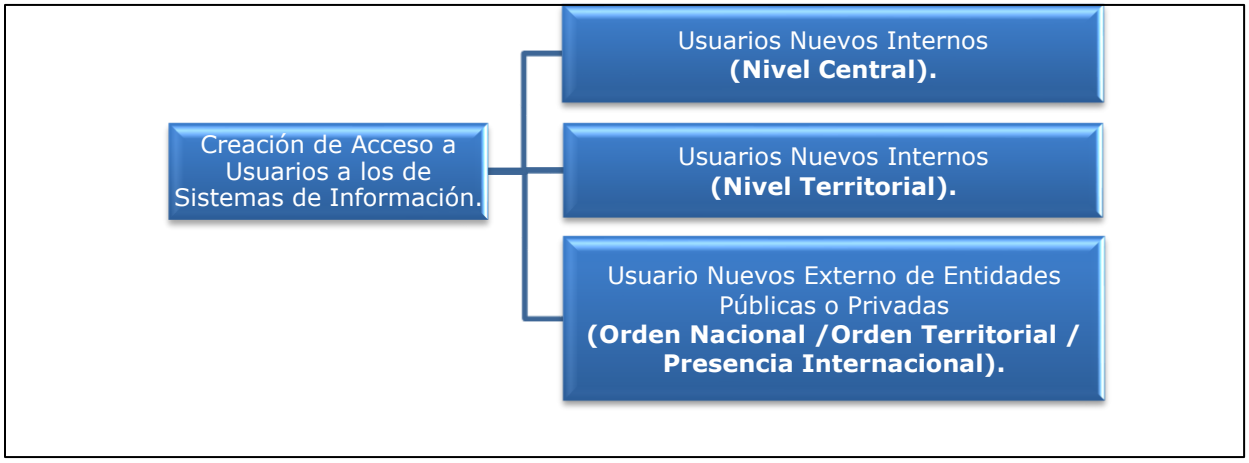


Imagen No.6 *– Tipos de Usuarios para Creación de Acceso a los Sistemas de Información.*

Los casos se asignarán al Administrador Funcional y/o Administrador delegado (según sea el caso) para que realice la creación de usuarios en los Sistemas de Información y proceda a dar los accesos de acuerdo con las especificaciones detalladas en la creación del caso en la Herramienta de Gestión y los archivos adjuntos.

El Administrador Funcional:

a. Crea el usuario para el acceso a los Sistemas de Información que se relacionaron en el "Formato de Gestión de acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad" y verifica que se cumplan con las indicaciones consignadas en el mismo.

b. Si el usuario existe y requiere modificar o reactivar el acceso a los Sistemas de Información, deberá pasar a la **Etapa No.2** del presente protocolo.

c. Si el usuario existe y requiere inactivar el acceso a los Sistemas de Información, deberá pasar a la **Etapa No.3** del presente protocolo.

NOTA:
Se recomienda tener en cuenta las indicaciones que se encuentran en los manuales de los Sistemas de información involucrados en la solicitud.

Aspectos adicionales para tener en cuenta para el Acceso a los Sistemas de Información:

a. Si ya se cuentan con un "Formato de Gestión de acceso a Sistemas de Información y aceptación de Acuerdo de Confidencialidad" y requieren incorporar un nuevo acceso como:

- Lista de herramientas.
- Módulos.
- Perfil.
- Observaciones/Permisos.
- Horario.
- Otros Sistemas de Información.

Deberá ir a la **Etapa No.2** donde se especifica más detalles para los Sistemas de Información.

b. Para el caso particular del **PORTAL VIVANTO** no se puede dar acceso a la vigencia superiores a un (1) año, salvo cuando la fecha de solicitud de acceso se encuentre entre 1 de diciembre y el 31 de diciembre para que se pueda dar acceso en la vigencia actual y/o la siguiente vigencia.

c. Se verifica si el usuario fue creado para el acceso a los Sistema de Información y cumple con las especificaciones detalladas en el "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad".

d. Se suministrará "El Usuario y Contraseña" al correo registrado en los adjuntos que se encuentra en el caso generado en la Herramienta de Gestión. La persona que crea el acceso deberá documentar las actividades realizada en la herramienta de Gestión.

e. Para **SGV**, el Sistema de Información enviará de forma automática el usuario y contraseña al correo registrado en el "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad". Cuando ingresa por primera vez el Sistema de Información obliga a cambiar la contraseña asignada.

NOTA:
El usuario tiene la responsabilidad de cambiar la contraseña asignada cuando ingrese por primera vez al Sistema de Información, aplicando la Política de Contraseña y dar cumplimiento a las Políticas de Seguridad de la información definidas por la Entidad.

Etapa No.2:

Modificación / Reactivación de Acceso a Usuarios a los Sistemas de Información.

1. Escenarios de Modificación de Acceso a Usuario a los Sistemas de Información:

Revisar los siguientes escenarios para modificación de accesos a usuarios para los Sistemas de Información:

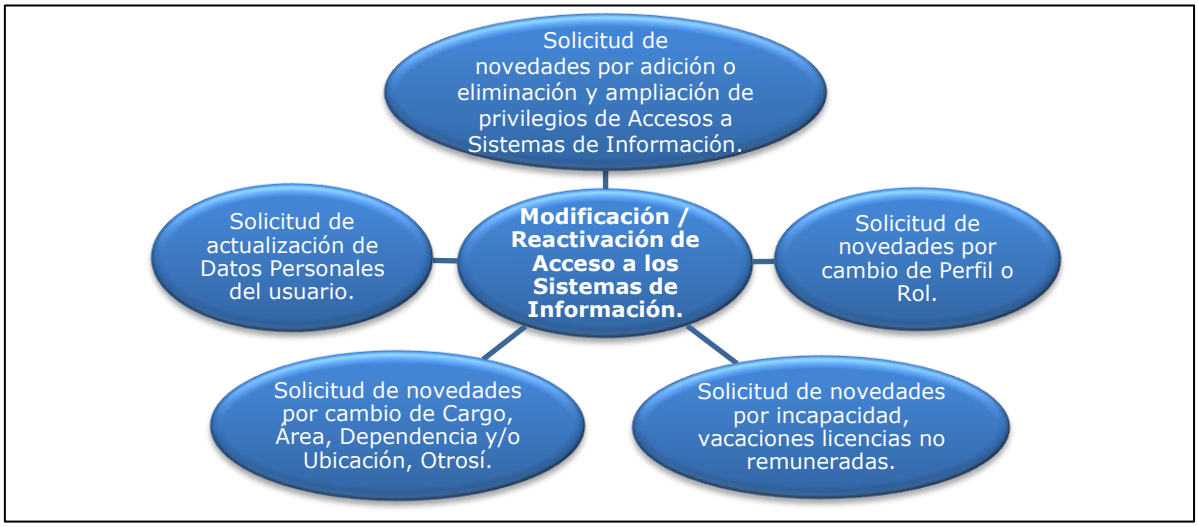


Imagen No.7 *-Escenarios para la Modificación de Acceso a los Sistemas de Información.*

a. Para todos los escenarios de modificación de acceso a usuario para los Sistemas de Información, se debe diligenciar nuevamente el "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad". En este nuevo acuerdo se deben especificar todos los cambios de acceso a los Sistemas de Información y listar los accesos que deben mantenerse.

b. Esta información será verificada y validada por Colaborador Designado Interno o Colaborador Designado Externo; con el fin de que estos permisos sean actualizados por parte de los Administradores Funcionales de los Sistemas de Información.

NOTA:

- ✓ Se deberá unificar en un solo archivo (En formato PDF) el "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad" y la Fotocopia de Cédula.

- ✓ Se recomienda revisar en el **numeral 7. ANEXOS** del presente documento si requiere más información para el Acceso a los Sistemas de Información que están solicitando.

- ✓ En caso de otro si o prórroga del contrato con Operadores de la UARIV, la extensión del tiempo de la ejecución del contrato aplicará a la fecha de vigencia de las solicitudes de gestión de acceso y aceptación de acuerdo de confidencialidad para el personal involucrado.

2. Escenarios de Reactivación de Acceso a Usuarios a los Sistemas de Información:

Revisar los siguientes escenarios para reactivación de accesos a usuarios para los Sistemas de Información.

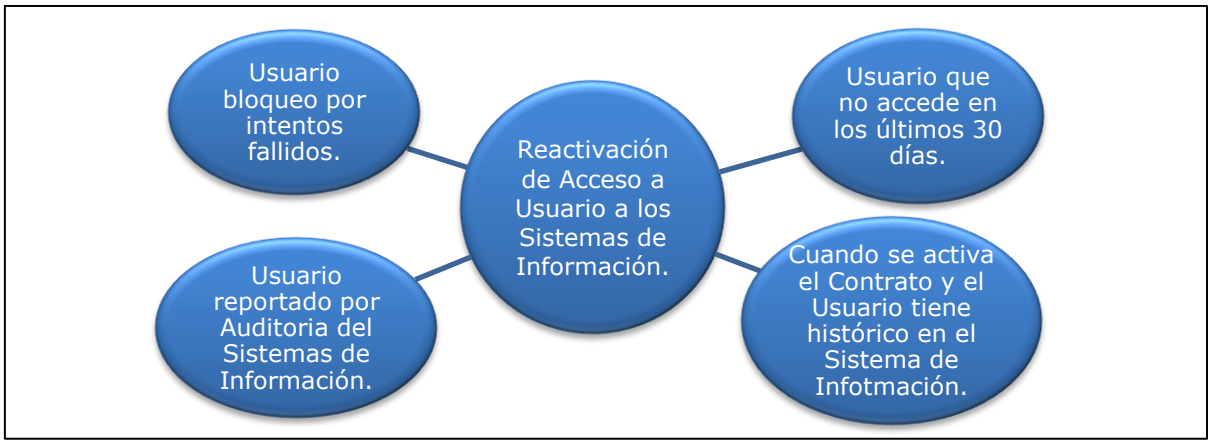


Imagen No.8 -Reactivación de Acceso a Usuario para los Sistemas de Información.

a. Para los escenarios de reactivación de: (Reportados por auditoria, bloqueo por intentos fallidos y no acceder a los últimos 30 días) para los Sistemas de Información, **NO** debe volver a diligenciar el "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad".

b. Para el escenario de reactivación de acceso cuando se active un nuevo contrato y el usuario tenga histórico en el Sistema de información **SI** se deberá diligenciar un "formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad".

c. Para la solicitud de la reactivación de acceso a los Sistemas de Información **VIVANTO**, deberá crear el caso en la Mesa de Servicios Tecnológicos a través de la Herramienta de Gestión de la Entidad, por el responsable que se indica en la **Imagen No.5** del presente protocolo y se deberá tener en cuenta lo siguiente.

Cuando la solicitud es para reactivación individual:	Se requiere que, en la descripción del caso, se detalle los datos del usuario sobre el cual se requiere la gestión: • Numero de cedula. • Nombre y apellidos. • Justificación de la reactivación.

Cuando la solicitud es para reactivación masiva (superior a 20 usuarios):	No es necesario agregar los datos del usuario en el campo descripción. Se debe adjuntar el archivo (Excel) con la relación de los usuarios que se deben reactivar.

Tabla No.9 *– Indicaciones para crear caso de Reactivación de Acceso a los Sistemas de Información.*

NOTA:

- ✓ Cuando aplique se suministrará "El Usuario y Contraseña" al correo registrado en el caso reportado en la Herramienta de Gestión y se deberá documentar las actividades realizadas en la misma herramienta.
- ✓ El usuario tiene la responsabilidad de cambiar la contraseña asignada cuando ingrese al Sistema de Información, aplicando la Política de Contraseña con el fin dar cumplimiento a las Políticas de Seguridad de la información definidas por la Entidad.

Etapa No.3:

Inactivación de Acceso a Usuarios a los Sistemas de Información.

Imagen No.9 *- Escenarios para Inactivación de Acceso a los Sistemas de Información.*

1. **Para los Usuarios Internos del Nivel Central o Dirección Territorial (funcionarios, contratistas, operadores, terceros y proveedores):**

   a. El Colaborador Designado Interno o delegado Interno deberá reportar la novedad mediante la creación del caso en la Mesa de Servicios Tecnológicos a través de la Herramienta de Gestión de la Entidad (cuando aplique), e indicar el motivo de la inactivación.
   b. Para las solicitudes de inactivación de acceso a **SGV** (Sistema de Gestión para las Víctimas) y **SM** (Subsistencia Mínima) deberán ser enviadas al correo adminsaah@unidadvictimas.gov.co y ser registrada en la Herramienta de Gestión de Mesa de Servicio.
   c. Para las solicitudes de inactivación de acceso a **INDEMNIZA** deberán ser enviadas al correo indemniza@unidadvictimas.gov.co y ser registrada en la Herramienta de Gestión de Mesa de Servicio.
   d. Aquí se enumeran algunos motivos por los cuales los **usuarios internos** pueden ser inactivados en los Sistemas de Información (Cuando aplique):
      - El 31 de diciembre de cada año se desactivan los usuarios internos (contratistas, operadores, terceros y proveedores).
      - Cuando finaliza el Acuerdo de Confidencialidad.
      - Cuando reportan novedades relacionadas con los escenarios de inactivación indicados en la imagen No.9 del presente documento.
      - Cuando se tramite el **PAZ** y **SALVO** por:

Desvinculación Laboral:	• Funcionarios.
Terminación de Contrato:	• Contratistas. • Operadores. • Proveedores.
Terminación Convenio Interadministrativo:	• Terceros.

Tabla No.10 *– Tramite de Paz y Salvo.*

NOTA:
Adicional a estos motivos de inactivación, se realizará de manera automática la inactivación de acceso al Sistema de Información cuando lleva más de (30) días sin hacer uso de los Sistemas de Información.

2. **Para los Usuarios Externos de Entidades Públicas o Privadas (Orden Nacional, Orden Territorial y Presencia Internacional):**

   a. Para el caso de usuarios asociados al PORTAL VIVANTO, Se debe realizar por parte del Articulador Designado y/o Colaborador del Nivel Central o Territorial, el reporte de la novedad mediante la creación del caso en la Mesa de Servicios Tecnológicos a través de la Herramienta de Gestión de la Entidad, e indicar el motivo de la inactivación.

   b. Aquí se enumeran algunos motivos por los cuales los **usuarios externos** pueden ser inactivados en los Sistemas de Información (Cuando aplique):
      - El 31 de diciembre de cada año se desactivan los usuarios externos.
      - Cuando finaliza el Acuerdo de Confidencialidad.

- Cuando reportan novedades relacionadas con los escenarios de inactivación.
- Por análisis de registros de auditoría sobre el usuario.
- Cuando la **ENTIDAD EXTERNA** reporta novedades relacionadas con inactivación al Articulador Designado y/o Colaborador del Nivel Central o Territorial.

NOTA:
Adicional a estos motivos de inactivación, se realizará de manera automática la inactivación de acceso al Sistema de Información cuando lleva más de (30) días sin hacer uso de los Sistemas de Información.

4.1.2.1.2. Servicios TI:

Para tramitar una solicitud de acceso a los Servicios TI (cuando aplique), se deberá realizar primero el trámite indicado en el **numeral 4.1.2.1 Solicitud de gestión de acceso a sistemas de información y aceptación del acuerdo de Confidencialidad** del presente protocolo; en caso contrario continuar con el proceso.

Solicitudes:
Para las solicitudes de accesos y permisos a los Servicios TI se deberá consulta el "Procedimiento de Gestión Servicios e Infraestructura Tecnológica". A continuación, se listan algunos de los Servicios TI:

- Servidores de aplicación.
- Servidores de Base de Datos.
- Almacenamiento OneDrive y SharePoint.
- Buzones de Correo.
- Servicios de Telefonía IP.
- Servicios de VPN.
- Otros.

Nota:
Se deberá tener en cuenta los instructivos relacionados con la solicitud de acceso a los Servicios TI, de acuerdo con el "Procedimiento de Gestión Servicios e Infraestructura Tecnológica".

Imagen No.10 *– Instructivos Relacionados con Solicitud de Acceso a los Servicios TI.*

Crear del caso para Servicios TI:
Para crear el caso se deberá registrar en la Mesa de Servicios Tecnológicos a través de la Herramienta de Gestión para las solicitudes de los Servicios TI, para lo cual deberá consultar el Procedimiento de Gestión de Servicios e Infraestructura Tecnológica.

NOTA:
Se recomienda revisar los instructivos relacionados con el procedimiento.

Etapas para Acceso lógico a los Servicios TI:

A continuación, se detallan las etapas para la creación, modificación, reactivación e inactivación de acceso a los Servicios TI.

Etapas	Usuario Interno	
Etapa No.4 Creación de Acceso a Servicios TI.	Nivel Central	Dirección Territorial
Etapa No.5 Modificación y/o Reactivación de Acceso a Servicios TI.	Nivel Central	Dirección Territorial
Etapa No.6 Inactivación de Acceso a Servicios TI.	Nivel Central	Dirección Territorial

Tabla No.11 *– Etapas para el Acceso Lógico a los Servicios TI.*

Etapa No.4:
Creación de Acceso a Usuarios a los Servicios TI.
Revisar los tipos de usuarios que le aplican para la creación de acceso para los Servicios TI.

Etapa No.5:
Modificación / Reactivación de Acceso a Usuarios a los Servicios TI.

1. **Escenarios de Modificación de Acceso a Usuarios a los Servicios TI:** Se deberá tener en cuenta los siguientes escenarios para modificación de accesos a usuarios para los Servicios TI.

Imagen No.11 *-Escenarios para la Modificación de Acceso a los Servicios TI.*

2. **Escenarios de Reactivación de Acceso a Usuarios a los Servicios TI:** Se deberá tener en cuenta los siguientes escenarios para la reactivación de acceso a usuarios para los Servicios TI.

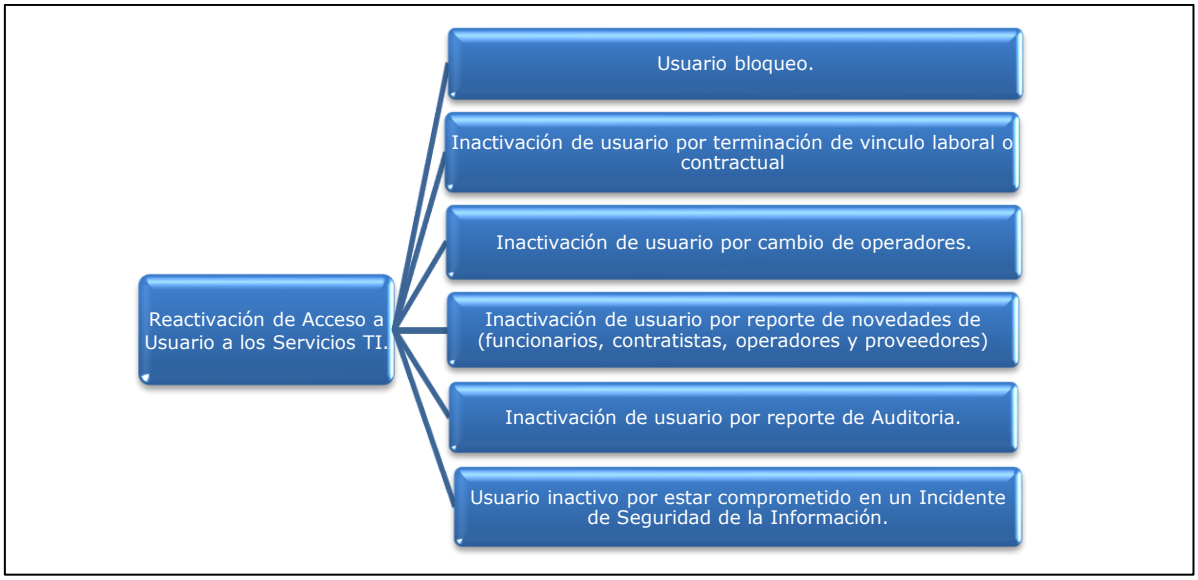


Imagen No.12 *-Escenarios para Reactivación de Acceso a Usuario a los Servicios TI.*

Etapa No.6:

Inactivación de Acceso a Usuarios a los Servicios TI.

Se deberá tener en cuenta los escenarios para inactivación de usuarios para Servicios TI:

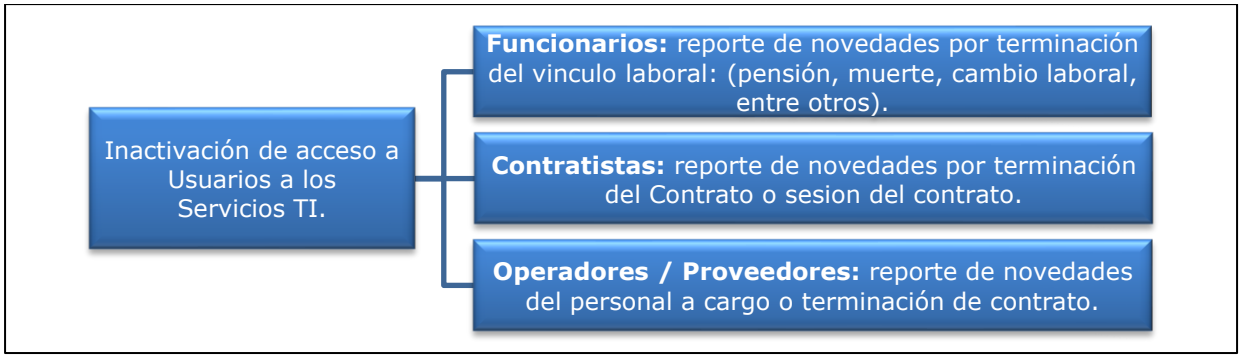


Imagen No.13 *- Escenarios para Inactivación de Acceso a Usuarios a los Servicios TI.*

5. RECOMENDACIONES:

a. Para fortalecer el control de autenticación de usuarios internos y externos de los Sistemas de Información según sea el caso debe:

- Aplicar el Doble Factor de Autenticación para fortalecer la validación de identidad de usuarios.

- Los administradores de los Sistemas de Información deben realizar monitoreo periódico del uso, con el fin de identificar comportamientos no habituales; para lo cual deberán evaluar y determinar si el comportamiento no habitual requiere de inactivación temporal o permanente para el acceso a los Sistemas de Información de la Unidad.

b. Para fortalecer el control de autenticación de usuarios internos de los Servicios TI según sea el caso debe: Aplicar el Doble Factor de Autenticación para fortalecer la validación de identidad de usuarios.

c. Para el acceso a la información se debe tener en cuenta: La información Sensible y/o Confidencial solo podrá ser autorizada por el líder de la dependencia que lo administra y es responsable de la información para su consulta y uso. Para el caso de los datos personales como:

- Fecha de expedición de documento de identidad, datos personales de población víctima, origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros.

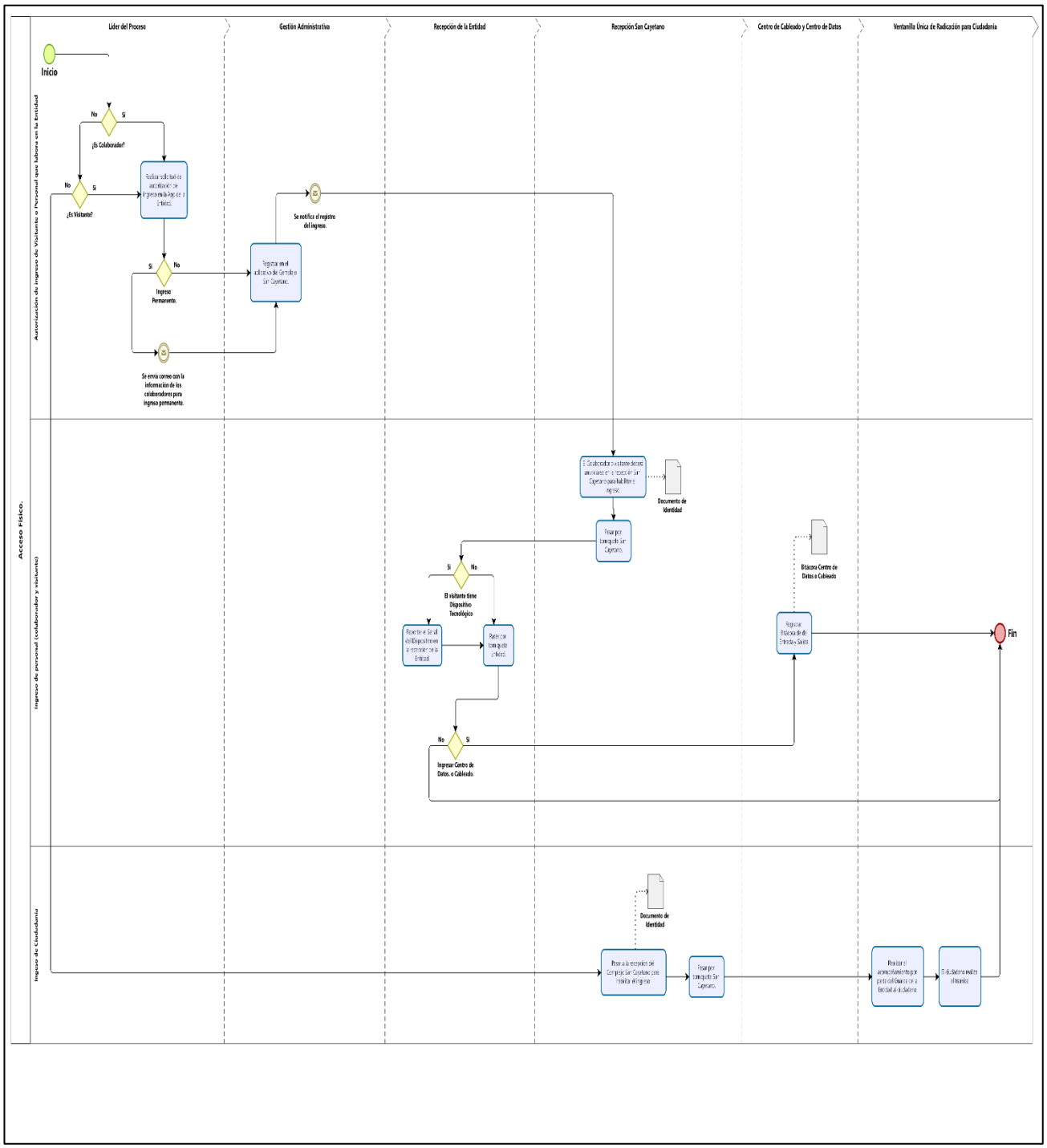
Nota: Deben contar con previa autorización de la Oficina Asesora Jurídica y/o del Oficial de Protección de Datos y/o quien haga de sus veces de acuerdo con su competencia dentro de la Entidad.

d. Vigencia de Acceso: La vigencia para los accesos a Sistemas de Información y/o Servicios TI aplica para:

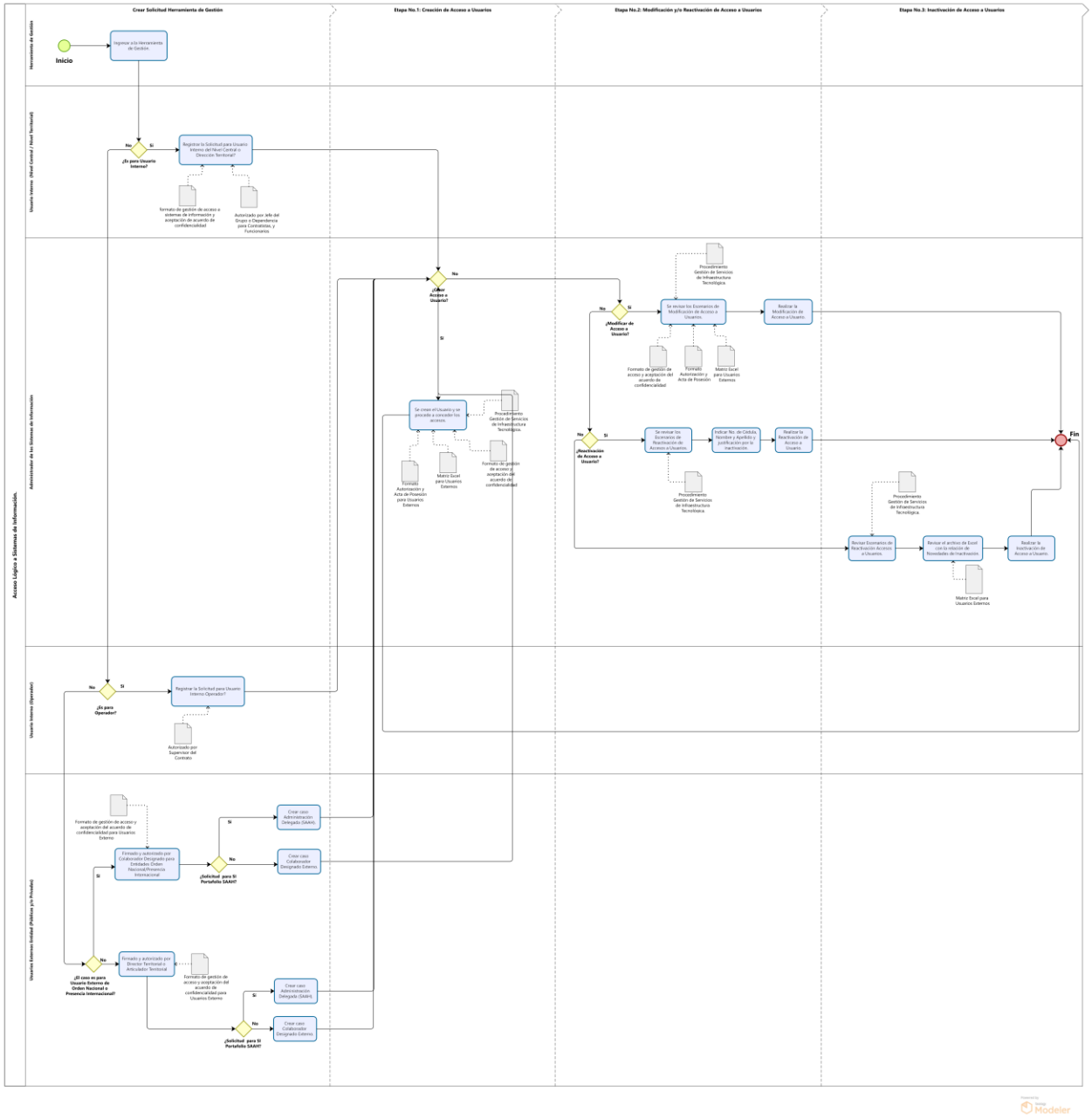
- La duración definida en la fecha de terminación del contrato, incluidas sus prórrogas.
- La terminación de la vinculación laboral o contractual.
- La vinculación del usuario señalada en el "Formato de aceptación del lineamiento de Confidencialidad de usuario de aplicativos, herramientas o información de la Unidad para la Atención y Reparación Integral a las Víctimas".

6. FLUJO DE ACTIVIDADES:

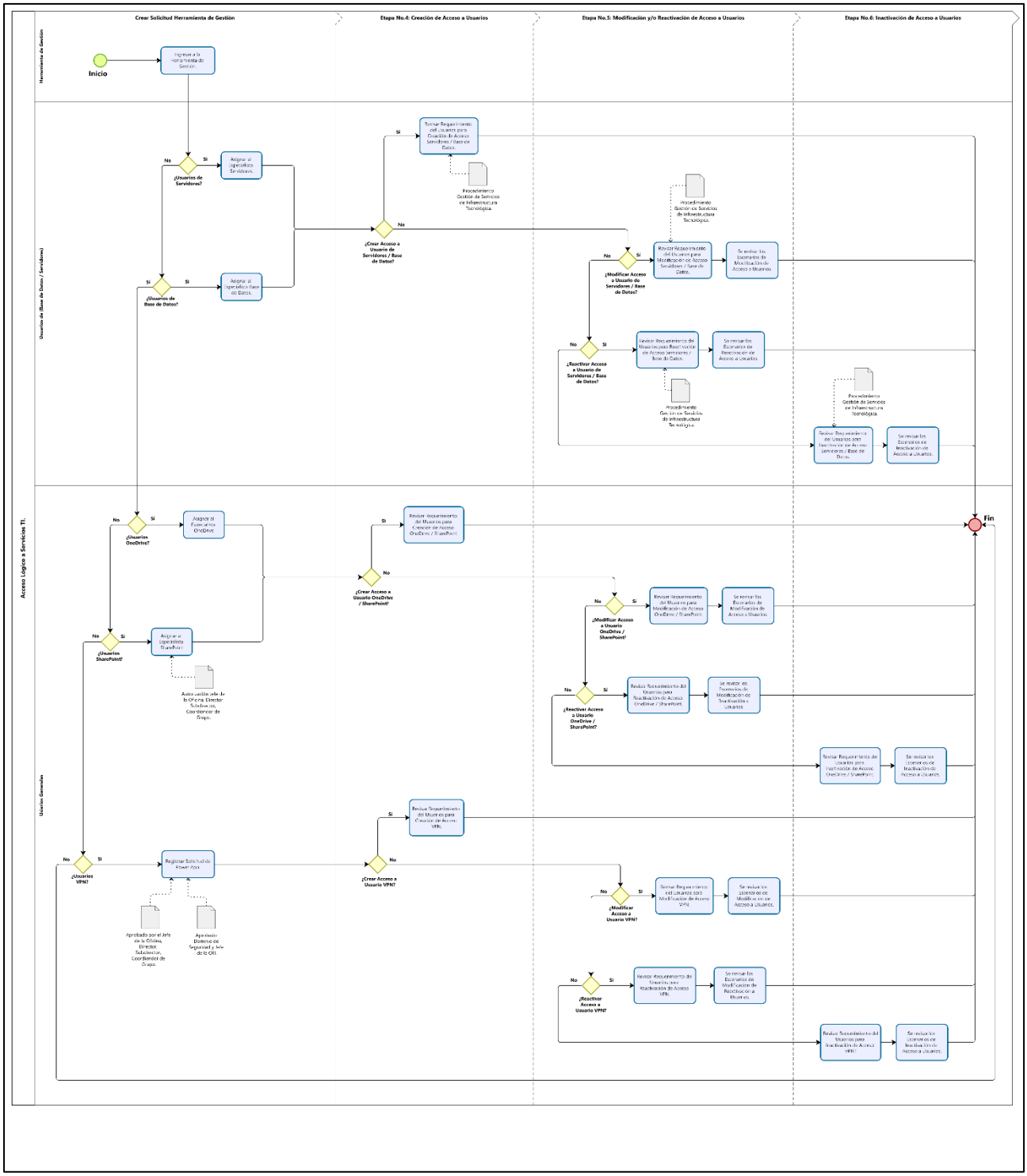
6.1. ACCESO FÍSICO.



6.2. ACCESO FÍSICO – SISTEMAS DE INFORMACIÓN (SI).



6.3. ACCESO FÍSICO – SERVICIOS TI.



7. ANEXOS

- **Anexo 1**. Formato de gestión de acceso a sistemas de información y aceptación de acuerdo de confidencialidad.
- **Anexo 2**. Formato Listado Personas v1.
- **Anexo 3**. Formato de Usuarios Autorizados para el Acceso a Sistemas de Información
- **Anexo 4**. Instructivo Soporte Mesa de Servicios.
- **Anexo 5**. Procedimiento Gestión de Servicios e Infraestructura Tecnológica.
- **Anexo 6.** Formato Compromiso de Confidencialidad y No Divulgación de la Información

8. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	20/11/2025	Creación de documento.