1. OBJETIVO:	Establecer la metodología para recibir, administrar, organizar, automatizar y responder de manera oportuna las solicitudes de incidentes y/o requerimientos tecnológicos de los usuarios de Servicios Ambientales SA ESP. **Objetivos específicos:** • Definir roles y responsabilidades dentro de TI para evaluar los incidentes y/o requerimientos tecnológicos a usuarios. • Gestionar los incidentes tecnológicos en tanto como sea posible, dentro de marcos de tiempo de acuerdo a lo establecido en los ANS (Acuerdos de Nivel de Servicios). • Determinar si un incidente genera riesgo a la seguridad de la información y mitigar sus posibles impactos. • Registrar en la mesa de ayuda (GLPI) todas las actividades ejecutadas respecto al seguimiento y solución de los incidentes y / o requerimientos reportados. • Minimizar los impactos adversos de los incidentes tecnológicos en la compañía, mediante la adecuada respuesta al incidente. • Consolidar las lecciones aprendidas que dejan los incidentes y su gestión para tomar acciones de mejora y mitigar su ocurrencia en el futuro. • Definir los mecanismos que permitan cuantificar y monitorear los tipos, prioridades y niveles, a través de una base de conocimiento y registro de incidentes y a través de los indicadores revisados en comité semanal.
2. ALCANCE:	Los términos y condiciones descritos en este documento aplican a todos los procesos, colaboradores, consultores, contratistas y proveedores de Servicios Ambientales SA ESP, que requieran atención a solicitudes y /o incidentes tecnológicos.
3. RESPONSABLE:	Ingeniero de infraestructura Colaboradores Director de infraestructura Gerente corporativo TI.

4. DEFINICIONES:

Activo: Cualquier cosa que tenga un valor de importancia relevante para la organización. Entre los activos de una organización se encuentra hardware, software, documentos electrónicos o físicos, infraestructura, servicios, personal, entre otros. El término Activo es sinónimo de Activo de Información.
Controles: Medidas de protección o salvaguardas dispuestas para reducir el nivel de riesgo. Pueden ser políticas, lineamientos, procedimientos, directrices, prácticas, estructuras de la organización, soluciones tecnológicas, entre otros.

Disponibilidad: Propiedad de garantizar que el activo de información sea accesible y utilizable en el momento que se requiera, por parte de las personas, procesos o entidades autorizada.
Impacto: Consecuencias que produce Incidente sobre la organización.
Incidente: Cualquier evento que no forma parte usual o normal de la operación diaria del proceso de negocio, que causa o puede causar una interrupción o reducción en la calidad del servicio.
Integridad: Propiedad de salvaguardar la exactitud y estado completo del activo de información, de acuerdo a los diferentes métodos de proceso a que se exponga.
Gestión de Incidentes: Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.
Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
Log's: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.
Procesamiento de Información: Es la capacidad que tiene un sistema de información de efectuar cálculos con base a una secuencia de operaciones preestablecidas y permitiendo la transformación de datos fuentes en información para ser utilizada en la toma de decisiones
Propietario: Se refiere al dueño responsable del activo de información utilizado para el desarrollo y cumplimiento de sus funciones. Está encargado de garantizar la seguridad adecuada del mismo, con base a los principios básicos de seguridad a saber: confidencialidad, integridad y disponibilidad.
Seguridad de la información: Preservación fundamental de la confidencialidad, integridad y disponibilidad del activo de información, además de otros criterios o propiedades tales como la autenticidad, no repudio, confiablidad, propiedad y/o responsabilidad, entre otros.
Sistema de Información: Es una disposición de personas, actividades o procedimientos y recursos tecnológicos integrados entre sí, para apoyar y mejorar las operaciones diarias de la organización, con la finalidad de satisfacer las necesidades de información en general y facilitar la toma de decisiones por parte de los directivos de la organización. Ejemplos aplicados: sistemas de automatización de oficina, sistemas de procesamiento de transacciones y sistemas de información de gestión.
Software: es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.
Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse en o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.
Ticket: Es un boleto digital generado por el sistema de tickets a partir de las solicitudes entrantes realizadas por los usuarios, sin importar el canal que hayan utilizado para comunicarse (correo electrónico, vía telefónica, chat o app).
Recuperación: Volver el entorno afectado a su estado natural.
Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
Vulnerabilidad: Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

Acuerdo de Niveles de Servicio: (siglas ANS), también conocidas por las siglas SLA (del inglés Service Level Agreement), es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.
Cambio: Modificación adicional aprobada sobre la línea base de: hardware, red, software, aplicación, ambiente, sistema, o documentación asociada.
Control de Cambio: Procedimiento para asegurar que todos los cambios están controlados, incluyendo el análisis, toma de decisiones, sujeción, aprobación, implementación y post-implementación del cambio.
Mesa de ayuda: Punto único de contacto dentro de la organización de TI, para los usuarios.
Prioridad: Secuencia con la que un problema o incidente tiene que ser resuelto, basado en impacto y urgencia.
Usuario: Persona que utiliza los servicios diarios.
GLPI: es una solución libre de gestión de servicios de tecnología de la información (ITSM), un sistema de seguimiento de incidencias y de solución de mesa de ayuda.
Colaborador: Todos los trabajadores de Servicios Ambientales SA ESP.
Requerimiento: Es una solicitud realizada por el usuario, frente a una solicitud específica y está sujeto de ser evaluado y priorizado su tiempo de atención de acuerdo a los acuerdos de niveles de servicio.
Escalamiento: Se refiere al movimiento de casos entre agentes con el fin de brindar solución a los requerimientos en el nivel de soporte técnico especializado. En el escalamiento se documentará los avances de la gestión realizada.
Infraestructura Tecnológica: Es el conjunto de hardware y software sobre el cual funcionan los diferentes servicios que se prestan; equipos de cómputo, equipos de comunicaciones, sistemas de información, impresoras, equipos de digitalización, equipos de telefonía.
Soporte 1.0: Soporte inicial, responsable de las incidencias básicas del usuario. Es el encargado de hacer el diagnóstico inicial en sitio, hacerlas configuraciones e instalaciones básicas de Sistemas Operativos, drivers, y utilitarios o de sistemas de información. La principal labor reunir toda la información del usuario y determinar la solución inmediata.
Soporte 1.5: Es el soporte que deben realizar los especialistas en un tema específico como conectividad sistemas de información, bases de datos, administración técnica de los sistemas de información.
Ingeniero de Infraestructura: De acuerdo a los cargos en TI, de desterminan; los ingenieros de soporte, auxiliares de infraestructura, estuantes SENA, estudiantes universitarios)

5. CONTENIDO

5.1 Generales

El equipo de la mesa de ayuda debe poder identificar y solucionar todos aquellos incidentes y/o requerimientos tecnológicos que se generen por la mesa de ayuda GLPI; para esto se debe contar con un personal idóneo y suficiente.

Debe poder clasificar y/o reclasificar las solicitudes de los usuarios por tipo: Incidente, Requerimiento o Cambio. Priorizando los casos según su criticidad y complejidad, cumpliendo con tiempos mínimos de espera y atención para el usuario.

Los líderes de procesos que requieran cambios a los sistemas de información, el requerimiento será evaluado por soporte de nivel 1.5, de acuerdo a la gestión de Cambio en Tecnología.

Los Colaboradores deberán conocer del proceso que se debe llevar a cabo para poder solicitar atención de los incidentes y/o requerimientos tecnológicos en la mesa de ayuda.

1.1. Gestión de incidentes tecnológicos.

- Todos los incidentes deben ser ingresado en la mesa de ayuda GLPI.

- Es responsabilidad del colaborador documentar de manera clara y detallada el incidente, de tal forma que pueda ser replicable por los ingenieros de la mesa de ayuda, esto incluye: imágenes, documentos y adjuntos, lo que permitirá mejorar la oportunidad en la resolución del incidente.
- Si un incidente reportado a la mesa de ayuda por GLPI se clasifica como incidente de seguridad de la información, este se debe atender de acuerdo a lo establecido en el procedimiento Gestión de Incidentes de seguridad de la información.
- Durante el tiempo de vida de un incidente, este puede ser asignado a diversos grupos de solución, pero permanece siempre bajo el seguimiento de la Mesa de ayuda, quien tiene bajo su responsabilidad la comunicación constante del estado del incidente al colaborador, hasta el cierre del incidente a través de la confirmación del colaborador en GLPI.

- Todos los grupos implicados en el procedimiento de atención de Incidentes tecnológicos tienen la responsabilidad de supervisar continuamente y asegurar que los incidentes y/o requerimientos sean atendidos y resueltos.
- El colaborador debe estar disponible en los tiempos especificados de acuerdo a la criticidad definida en los ANS, en caso de ser de máxima criticidad el usuario debe estar disponible en cualquier horario. Superado el tiempo del ANS sin respuesta o comunicación del usuario el ticket será cerrado.

1.2. Gestión de requerimientos

- Si el requerimiento o incidente ingresado se clasifica como un cambio a los sistemas de información o infraestructura, este debe ser trasladado a soporte 1.5 para continuar con el proceso de gestión acorde a cambio, se notificará al usuario los tiempos establecidos para la entrega.

- Si el requerimiento es una solicitud de un elemento tecnológico se deben realizar las siguientes actividades:

1. El usuario debe realizar la solicitud por medio de la mesa de ayuda (GLPI), adjuntar el formato TI-RE-11 Solicitud de Recurso Tecnológico, diligenciado y firmado por el líder de proceso.
2. El ingeniero de infraestructura verificará la existencia del recurso, si no se tiene disponibilidad se atenderá mediante el GCC-M-01- manual de compras y almacén.

3. Si el recurso tecnológico está en el presupuesto anual se asignará, de lo contrario, será escaldo a la gerencia general para el proceso de aprobación.
4. El ingeniero de infraestructura recibirá el equipo y deberá registrarlo en la herramienta de control de inventarios de recursos tecnológicos.
5. El ingeniero de infraestructura entregará el recurso solicitado, mediante el formato TI-FO-05 Acta de entrega de recursos tecnológicos.

- Si el requerimiento es una solicitud de préstamo de recurso tecnológico, el ingeniero de infraestructura tendrá en cuenta lo siguiente:

1. EL colaborador debe realizar la solicitud por medio de la mesa de ayuda (GLPI).
2. El ingeniero de infraestructura deberá revisar las condiciones del equipo al momento de la entrega y devolución del mismo.
3. El ingeniero de infraestructura deberá diligenciar el formato TI-FO-07 Préstamo de Equipos e implementos.
4. Los recursos tecnológicos prestados, no pueden ser retirados de las instalaciones de la compañía sin la autorización del jefe directo.

1.3. Roles que participan en el proceso

1.3.1. Ingeniero de Infraestructura – Soporte N1:

- El nivel de soporte inicial, intenta resolver los incidentes y/o requerimientos básicos que presenten los usuarios como:
  - Inconvenientes en sistemas físicos.
  - Configuración de hardware y software.
  - Atender problemas de usuario y contraseñas.
  - Instalación de software.
  - Atender incidentes con la red de comunicaciones.
  - Atender requerimientos de recursos tecnológicos.
  - Entre otras actividades propias en la atención de la mesa de ayuda.
- Validar que todos los incidentes y/o requerimientos reportados queden registrados en la herramienta GPLI.
- Analizar, clasificar, asignar y atender los incidentes y/o requerimientos reportados.
- Documentar el seguimiento de la solución de los incidentes y/o requerimientos.
- Resolución y cierre oportuno a todos los incidentes y requerimientos tecnológicos.
- Mantener constante capacitación y sensibilización a los colaboradores, contratistas y demás partes interesadas en cuanto al reporte de incidentes y requerimientos tecnológicos de acuerdo a lo establecido en el procedimiento.
- Revisar periódicamente los reportes de los casos atendidos respecto a tiempos de atención y calidad de la solución dada, con el fin de implementar estrategias de mejora continua.
- Orientar y dar adecuado tratamiento a los incidentes y/o requerimientos detectados o reportados con el fin de reducir el impacto que este pueda tener sobre la continuidad del negocio.

- Debe hacer seguimiento al ciclo de vida de los incidentes y/o requerimientos tecnológicos reportados en la herramienta GLPI de inicio a fin.
- Vigilar que los incidentes y/o requerimientos tecnológicos de los colaboradores sean atendidos de acuerdo a los niveles de servicio.
- Controlar las actividades específicas de los ingenieros que atienden la mesa de ayuda.
- Revisar periódicamente los reportes de los casos atendidos respecto a tiempos de atención y calidad de la solución dada, con el fin de implementar estrategias de mejora continua.

1.3.2. Analista de desarrollo - soporte N1.5

- Solucionar problemas de configuración avanzada de los sistemas de información.
- Creación y actualización de perfiles a nivel de bases de datos.
- Revisión y análisis de requerimientos a cambios en los sistemas de información para asignación de desarrollo.
- Resolución de incidentes con ajustes en consultas de bases de datos.

1.3.3. Colaboradores y contratistas

- Deben tomar conciencia de su responsabilidad de reportar eventos y debilidades tan pronto como sea posible a la mesa de servicios.
- Recibir las capacitaciones y participar en las campañas de sensibilización que se realicen al interior de la compañía.
- Reportar oportunamente los incidentes o eventos y cualquier comportamiento anormal que se presente en la Compañía o en sus activos.

1.3.4. Ingeniero de Desarrollo

- Revisión, alcance e impactos de requerimientos de desarrollo para nuevos sistemas de información, de acuerdo a lo estipulado en gestión de cambio.
- Atención de requerimientos de mejoras en los sistemas de información de la empresa.
- Atención a incidentes en los sistemas de información que requieran ajustes en el código fuente.

1.3.5. Director de Infraestructura

- Revisión periódica de la gestión de mesa de ayuda.
- Revisión y análisis de los indicadores de gestión, junto con los ingenieros de infraestructura.

1.3.6. Gerente Corporativo TI

- Revisión y aprobación de los requerimientos de los recursos tecnológicos.
- Revisar, medir los indicadores de la gestión de la mesa de ayuda.

1.4. Tipo de Incidentes

- Entre los tipos de incidentes se puede tener en cuenta los siguientes:

- Daño de Hardware.
- Daño de Software.
- Requerimiento de Hardware.
- Requerimiento de Software.
- Daño de impresora.
- Daño físico de Celular.
- Daño lógico de Celular.

1.5. Tipo de Requerimientos (REQ).

Entre los tipos de requerimientos se puede tener en cuenta los siguientes:

- Requerimiento o reposición de recursos tecnológicos (equipo de cómputo, celular, impresoras, entre otros)
- Cambio o mejora a los sistemas de información.
- Creación de cuentas de usuarios a sistemas de información.
- Asignación de privilegios a usuarios.
- Solicitudes de accesos a sistemas de información.
- Requerimientos para apoyar eventos o reuniones.
- Cambios (RFC)
- Traslado de equipos.
- Restablecimiento de Contraseñas.
- Actualizaciones de software.

Clasificación del evento de acuerdo a la criticidad del incidente o requerimiento a fin de darle el tratamiento adecuado:

Nivel	Descripción
Incidencia o Requerimiento Nivel 1	Interrumpe seriamente la operación de la compañía, el incidente puede tener velocidad significativa/rápida en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo.
Incidencia o Requerimiento Nivel 2	Interrumpe en un periodo corto de tiempo los procesos generales de la compañía, el incidente/evento compromete un activo importante.

Incidencia o Requerimiento Nivel 3	No interrumpe los procesos generales de la compañía, el incidente/requerimiento, se detecta y puede controlar fácilmente con recursos existentes en la compañía.
Incidencia o Requerimiento Nivel 4	No interrumpe, ni afecta los procesos de la compañía, el incidente/requerimiento es una novedad que puede atenderse con recursos internos o externos.

Tabla 1. Niveles de criticidad del evento/incidente

La mesa de ayuda, debe conocer la siguiente tabla de acuerdo de niveles de servicio a fin de darle el tratamiento adecuado.

Relevancia	Incidente	Requerimiento
Muy alta	Se debe atender y/o solucionar en los 100 minutos siguientes de ser reportado.	Se debe solucionar en las 24 horas siguientes de ser reportado.
Alta	Se debe atender y/o solucionar en las 8 horas hábiles siguientes de ser reportado.	Se debe solucionar en las 72 horas siguientes de ser reportado.
Media	Se debe atender y/o solucionar en las 24 horas siguientes de ser reportado.	Se debe solucionar en los 7 días siguientes de ser reportado.
Baja	Se debe atender y/o solucionar en las 48 horas siguientes de ser reportado.	Se debe solucionar en los 15 días siguientes de ser reportado.

Tabla 2. Tiempos de Solución

1.6. Características específicas de atención al usuario

- Si un colaborador, contratista y demás partes interesadas, identifica que está teniendo un incidente o necesita realizar un requerimiento, debe reportar al proceso de TI a través de los siguientes canales de atención:
  - GLPI (Herramienta en línea de gestión de tickets)
  - https://glpi.datint.co:8200
  - Correo electrónico del ingeniero de soporte

- El reporte de cada incidente y/o requerimiento independiente del medio por que se reciba, debe quedar registrado por el usuario en la herramienta de GLPI, donde se podrá realizar seguimiento y cierre con la solución por parte de TI.
- Al registrar el incidente o requerimiento se debe incluir fecha, hora y descripción del evento.

- En la evaluación del incidente se debe identificar los activos afectados, cual es alcance del mismo, que pronóstico tiene de expansión, así como los daños potenciales o reales que se generen.
- En la medida que haya tiempo y recursos, el equipo de mesa de ayuda debe adelantar las actividades que tiendan para dar solución pronta al incidente o requerimiento.
- Se deben tener en cuenta los siguientes factores para la atención de incidentes o requerimientos:

a. Daño potencial de recursos a causa del incidente.
b. Necesidad de preservación de la evidencia.
c. Tiempo y recursos necesarios para poner en práctica la solución.
d. Efectividad de la solución.
e. Duración de las medidas a tomar.
f. Criticidad de los sistemas afectados.
g. Posibles implicaciones Legales.

- Se debe dar un correcto manejo a los datos y evidencias recolectadas, los cuales deben ser almacenados en la herramienta de GLPI para futuras investigaciones e implementación de controles preventivos o de mejoramiento.

- Se debe tener en cuenta para definir y decidir las estrategias de erradicación los siguientes factores:

a. Tiempo y Recursos necesarios para poner en práctica la estrategia.
b. Efectividad de la solución.
c. Pérdida económica.
d. Posibles implicaciones legales.
e. Relación costo-beneficio de la solución.
f. Experiencias anteriores.
g. Identificación de los procedimientos de cada sistema operativo comprometido.
h. Identificación de usuarios o servicios comprometidos.

- Al realizar el análisis post-incidente se debe garantizar el correcto manejo de las lecciones aprendidas, de la siguiente manera:

a. Periódicamente los ingenieros de infraestructura o quienes hagan sus veces se reunirán a fin de analizar los eventos e incidentes presentados durante el periodo.
b. Buscar definir esquemas más efectivos para responder ante situaciones que afecten la infraestructura de la compañia.
c. Realización de capacitaciones a los colaboradores de la compañia en lo relacionado a incidentes y requerimientos.
d. Analizar los hechos y tomar decisiones.
e. Programar reuniones con los procesos de negocio impactados de comun acuerdo, en estas se deben identificar estadisticas y patrones que permitan mejorar el servicio.

1.7. Matriz de Escalamiento

Con el objetivo de generar los escalamientos pertinentes, se establece la siguiente matriz de escalamiento, de acuerdo a esta podrá ser atendido de manera interna o a través de un proveedor la atención a los usuarios así:

MATRIZ DE ESCALAMIENTO			
	INGENIERO	**CORREO**	**TELEFONO**
NIVEL 1	**MIGUEL PEROZO**	miguel.perozo@serambiental.com	3023641410
NIVEL 2	**GIOVANNY GALEANO** **MARIO PINTO**	giovanny.galeano@aseoregional.com mario.pinto@aseoregional.com	3184908962 3163027108
NIVEL 3	**JHON MARTINEZ** **ALFREDO RAMOS**	john.martinez@aseoregional.com alfredo.ramos@aseoregional.com	3153046372 3124208999

1.8. Disponibilidad de Aplicaciones

- Las aplicaciones se miden de acuerdo a su disponibilidad y criticidad, esto está directamente relacionado a las jornadas laborales establecidas para cada área.

MATRIZ DE DISPONIBILIDAD MENSUAL			
APLICACIÓN	**% DISPONIBILIDAD**	**ESQUEMA**	**BACKUP**
AIDA	99,749	24x7	DIARIO
SIOR - ARQ	98,0	9x5	DIARIO
GESTOR DOCUMENTAL	98,0	9x5	DIARIO
GLPI	98,0	24x7	DIARIO
NOVASOFT	98,0	9x5	DIARIO
PAGINA WEB	99,749	24x7	DIARIO
PROMOSO	98,0	9x5	DIARIO
SCP	98,0	9x5	DIARIO
SGH	98,0	9x5	DIARIO
SGI	98,0	9x5	DIARIO
SIESA	98,0	9x5	DIARIO
SIGAB	99,749	24x7	DIARIO
SIREDE	98,0	9X5	DIARIO
SISCOMBAS	98,0	24x7	SEMANAL
SUITE CRM	98,0	9x5	DIARIO
TESORERIA	98,0	9X5	DIARIO
VPN	99,749	24x7	MENSUAL

MATRIZ DE DISPONIBILIDAD MENSUAL			
APLICACIÓN	**% DISPONIBILIDAD**	**ESQUEMA**	**BACKUP**
ZIMBRA	98,0	24x7	DIARIO

1.9. Métricas de proceso

MÉTRICA DE GESTIÓN			
PERIODO	**TIEMPOS DE ATENCIÓN A SOLICITUDES**	**% ATENCION**	**META**
MENSUAL	Casos cerrados dentro de los tiempos establecidos en los ANS	# de Casos Atendidos con cumplimientos ANS en el Mes.	>95

2. Buenas prácticas de Seguridad de la Información

- Es responsabilidad del colaborador el buen manejo, uso y confidencialidad del usuario y contraseña asignados, y de la información a la cual se tenga acceso.
- Es responsabilidad del colaborador ingresar a los sistemas de información y a la red corporativa únicamente con su usuario y contraseña no está autorizado a autenticarse como administrador local.
- Es responsabilidad del colaborador la administración de su usuario y contraseña dado que es de uso personal e intransferible.
- Es responsabilidad de los ingenieros de infraestructura mantener actualizado el estado de los usuarios, asegurando que el proceso de gestión humana informe las novedades relacionadas con los colaboradores.
- El líder o dueño del proceso debe ser el responsable para la solicitud de asignación de los permisos y perfiles de los usuarios sobre los sistemas de información de acuerdo con el cargo y roles desempeñados.
- Es responsabilidad de los ingenieros de infraestructura verificar que el perfil de cada usuario activo en las aplicaciones este acorde con lo establecido en la matriz de roles y accesos, esta labor se realizará con una periodicidad de cada 90 días.
- Como evidencia de esta revisión se dejará registro en la bitácora.
- En la creación y modificación de usuarios, la asignación de derechos debe realizarse de acuerdo con las matrices de roles y perfiles definidas.
- Los usuarios creados y asignados a cada colaborador activos deben ser únicos e irrepetibles.
- No se deben usar nombres genéricos para crear usuarios en cualquier sistema de información de la organización, a no ser que ya estas cuentas se encuentren creadas con anticipación y se usen para efectos legales externos como los utilizados para recibir información de la empresa como (notificaciones, requerimientos, PQR. Etc.).
- Solo se deben crear y asignar usuarios a colaboradores que estén activos en la organización, en ninguna circunstancia se permite el uso de usuarios temporales creados en los sistemas de información con nombres y privilegios de usuarios que no existen. Exceptuando solicitudes que lo requieran y sean aprobadas por la gerencia de TI. La creación de cuentas y usuarios de administradores para ambientes, dominio y plataformas solo puede ser ejecutada por el proceso de tecnología.

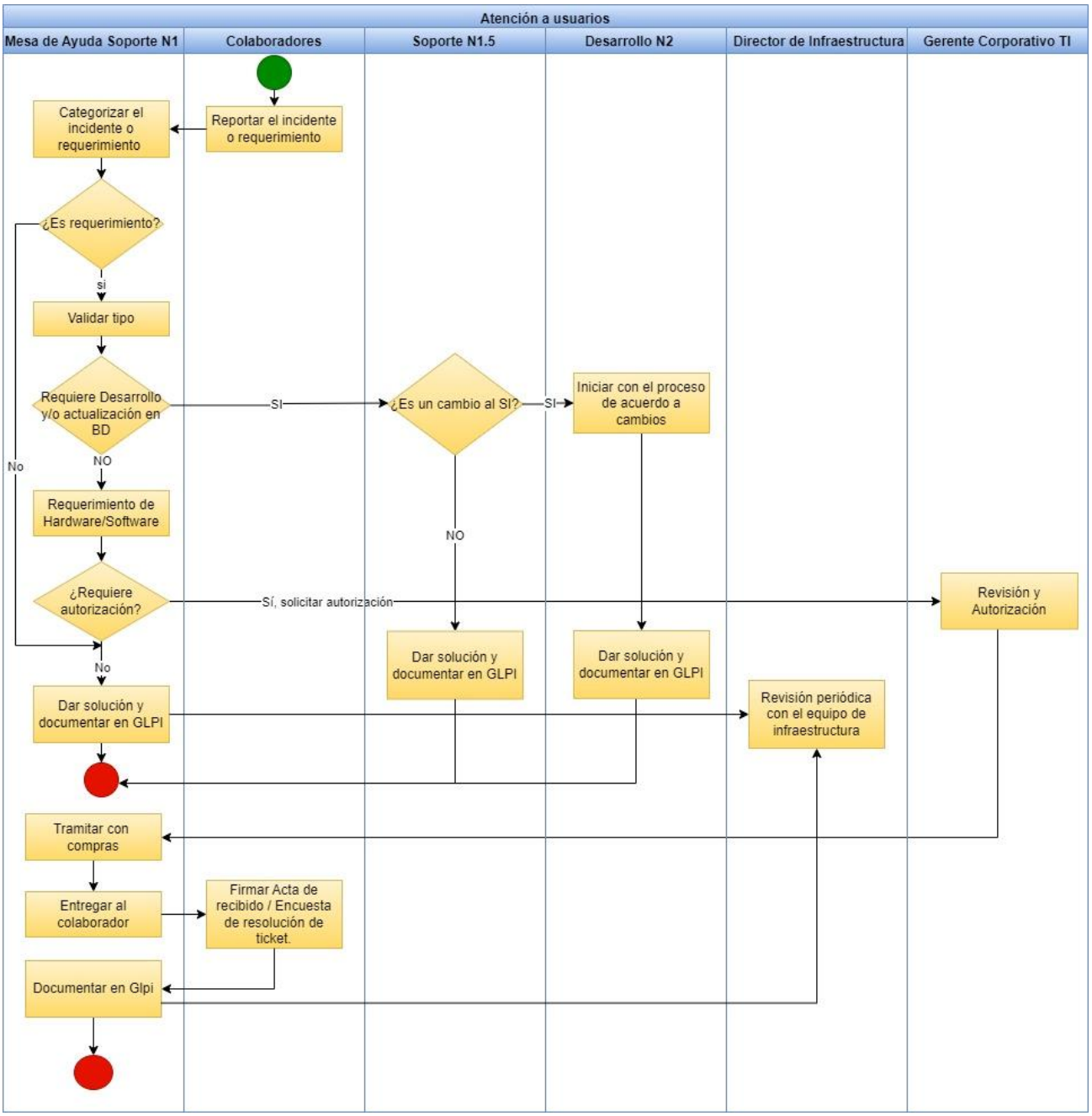
- Ningún proceso ajeno a tecnología debe manipular o hacer modificaciones sobre usuarios existentes.
- Es responsabilidad del proceso de tecnología la administración y la ejecución en la asignación de derechos de acuerdo con las matrices establecidas para cada uno de los sistemas de información a los colaboradores de la organización.
- Para solicitar la creación de una cuenta de correo de proceso, el líder de proceso debe diligenciar el formato de solicitud de recurso tecnológico TI-RE-11, crear un requerimiento en la herramienta de solicitudes tecnológicas y adjuntar el formato diligenciado

El proceso de tecnología debe realizar validación del uso de las cuentas de correo de proceso cada 3 meses, para realizar depuración de las cuentas que no se presenten actividad.

La solicitud se debe generar por medio del formato TI-RE-11 y con un tiempo mínimo de 1 día hábil antes del ingreso del colaborador.

La solicitud o cambio de permisos se debe generar por medio de un ticket de GLPI, generado por el líder del proceso.

Para la inactivación de usuarios críticos (Líder de proceso o de alto impacto) la gerencia de gestión humana remitirá correo electrónico de notificación de retiro, este será desactivado de manera inmediata.



6. ANEXOS

TI-RE-11 FORMATO SOLICITUD DE RECURSOS TECNOLOGICOS
TI-FO-07 PRESTAMOS DE EQUIPOS O IMPLEMENTOS
TI-FO-05 ACTA DE ENTREGA DE RECURSOS TECNOLÓGICOS.

HISTORIAL DE CAMBIOS

Versión N°	Fecha	Elaborado/Modificado por	Descripción del cambio
01	01/07/2021	Coordinador de TI	Versión Original
02	23/04/2024	Coordinador de TI	Se ajustan los roles y perfiles que participan en el proceso de atención de usuarios. Se ajusta el flujograma. Se elimina el ítem documentos relacionados. Se actualiza el indicador para medir la atención al usuario

Elaboró: Coordinador de TI	**Revisó:** Director de Infraestructura
Aprobó: Gerente de TI	

COPIA CONTROLADA: **SI:** ☐ **NO**