1. OBJETIVO

Definir los lineamientos y actividades para la gestión de incidentes de servicios TIC, con el propósito de restablecer la operación normal del servicio lo antes posible, reduciendo el impacto en los usuarios y asegurando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS), conforme a la práctica de Gestión de Incidentes establecida en ITIL 4.

2. ALCANCE

El presente procedimiento aplica a la gestión de los incidentes relacionados con los servicios TIC de la Superintendencia de Sociedades. Inicia con el reporte y registro del incidente a través de los canales oficiales o de la herramienta institucional de Gestión de Servicios TIC por parte del usuario.

Incluye las actividades de identificación, registro, clasificación, priorización, diagnóstico inicial, escalamiento, investigación y diagnóstico, resolución, restauración del servicio, validación de la solución, notificación al usuario, evaluación del servicio mediante encuesta de satisfacción y cierre del incidente.

Este procedimiento cubre los incidentes que afecten o puedan afectar los servicios tecnológicos, sistemas de información, infraestructura tecnológica y demás activos administrados por la Dirección de Tecnologías de la Información y las Comunicaciones -DTIC.

3. DEFINICIONES

ANS – Acuerdo de Nivel de Servicio: Acuerdo documentado entre el proveedor de servicios TIC y el cliente que define los niveles de servicio esperados, incluyendo tiempos de respuesta y resolución de incidentes según su prioridad.

Aranda Device Management (ADM): Solución de gestión unificada de activos de TI que permite administrar, monitorear y controlar de forma centralizada los dispositivos tecnológicos de la organización, mediante funcionalidades de inventario de hardware y software, control remoto, distribución y actualización de aplicaciones, gestión de licenciamiento, aplicación de políticas y generación de reportes, contribuyendo al control y soporte de la infraestructura tecnológica institucional.

Base de Conocimiento: Repositorio institucional que almacena información estructurada sobre incidentes resueltos, soluciones documentadas, errores conocidos y buenas prácticas, con el fin de apoyar el diagnóstico y resolución ágil de incidentes.

CST – Centro de Servicios Tecnológicos: Área de la Dirección de Tecnología de la Superintendencia de Sociedades responsable de actuar como punto único de contacto para la recepción, registro, seguimiento y gestión de incidentes y solicitudes de servicios TIC.

Error Conocido: Problema que ha sido analizado, pero no resuelto definitivamente. Se documenta en la Base de Conocimiento junto con soluciones temporales disponibles para agilizar la atención de incidentes relacionados.

Escalamiento: Proceso mediante el cual un incidente se transfiere a un nivel superior de soporte técnico o jerárquico cuando el nivel actual no puede resolverlo dentro de los tiempos o capacidades establecidas. Puede ser funcional (técnico) o jerárquico (administrativo).

Herramienta ITSM - Herramienta institucional de Gestión de Servicios TIC: utilizada para el registro, seguimiento, gestión y cierre de incidentes, solicitudes de servicio y demás registros del proceso.

Incidente: Interrupción no planificada de un servicio TIC, reducción en la calidad de un servicio TIC o falla de un elemento de configuración que aún no ha afectado el servicio, pero que puede impactar su operación. La gestión de incidentes tiene como objetivo restablecer la operación normal del servicio en el menor tiempo posible, minimizando el impacto en la operación de la Superintendencia de Sociedades.

Incidente de Seguridad de la Información: Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información institucional, incluyendo accesos no autorizados, uso indebido, alteración, divulgación o destrucción de la información, o cualquier violación a las políticas de seguridad de la información de la Superintendencia de Sociedades.

Incidente Mayor: Incidente con el nivel más alto de impacto y prioridad, que genera una interrupción significativa en los servicios tecnológicos, afecta un servicio crítico o impacta a un número considerable de usuarios, comprometiendo la continuidad de la operación institucional y requiriendo atención prioritaria e inmediata.

Incidente Recurrente: Incidente que se presenta de forma repetitiva bajo las mismas o similares condiciones, afectando un servicio TIC, y que puede indicar la existencia de una causa raíz no resuelta.

Solución Temporal (Workaround): Medida que reduce o elimina el impacto de un incidente o problema para el cual aún no se dispone de una solución definitiva. Permite restaurar el servicio mientras se trabaja en la resolución permanente.

4. DOCUMENTOS DE REFERENCIA

- ITIL® 4 Foundation – PeopleCert / AXELOS
  Marco de buenas prácticas para la gestión de servicios de TI, especialmente en las prácticas de Gestión de Incidentes, Gestión de Solicitudes de Servicio, Gestión del Conocimiento y Gestión de Niveles de Servicio.
- ISO/IEC 20000-1: Norma internacional para sistemas de gestión de servicios de TI, compatible con los principios de ITIL 4.
- ISO/IEC27001:2022:
  Estándar internacional desarrollado por ISO e IEC que proporciona un marco pa ra establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI).
- GIN-PO-001 Documento de Políticas del SGI
- GIN-PO-003 Políticas de Seguridad y Privacidad de la Información del SGSI
- GTI-PR-024- Operación Centro de Servicios Tecnológicos
- GTI-GU-006_GestionIncidentes
- Catálogo de Servicios TIC – Superintendencia de Sociedades.
- Matriz de Escalamiento CST – Dirección de Tecnología.

5. CONDICIONES GENERALES

5.1. Principios del Procedimiento

El presente procedimiento se fundamenta en los siguientes principios de ITIL 4:

- Enfocarse en el valor: Toda actividad debe orientarse a minimizar el impacto del incidente y a restaurar el servicio en el menor tiempo posible.
- Colaboración y visibilidad: Los roles involucrados deben comunicarse de forma oportuna y mantener actualizada la herramienta ITSM en todas las etapas del ciclo de vida del incidente.
- Pensar y trabajar de forma holística: La gestión de incidentes debe integrarse con las prácticas de Gestión de Problemas, Gestión de Cambios, Gestión del Conocimiento y Gestión de Niveles de Servicio.
- Optimizar y automatizar: Se deben aprovechar las capacidades de automatización de la herramienta ITSM para la clasificación, escalamiento, notificaciones y cierre de incidentes.
- Mejora continua: Los resultados del proceso deben ser revisados periódicamente para identificar oportunidades de mejora.

5.2. Registro y trazabilidad

- Todos los incidentes reportados por los usuarios deben ser registrados en la herramienta institucional ITSM, garantizando su trazabilidad completa desde el reporte hasta el cierre.
- Cada incidente registrado recibirá un número único de identificación para su seguimiento.
- El análisis preliminar del incidente debe incluir la consulta de la Base de Conocimiento institucional y una vez disponible, a la CMDB, para identificar posibles soluciones documentadas o el elemento de configuración afectado.
- Cuando se identifiquen incidentes duplicados, se deberá registrar el incidente más reciente en estado "Anulado" y asociarlo al incidente original, con el fin de evitar reprocesos y garantizar la trazabilidad del incidente principal.

5.3. Clasificación y Priorización

A todos los incidentes se les debe asignar una prioridad basada en la combinación del impacto (número de usuarios o servicios afectados) y la urgencia (velocidad con la que el negocio requiere la resolución). Se definen los siguientes niveles de prioridad:

PRIORIDAD	IMPACTO	URGENCIA	TIEMPO DE ATENCIÓN	TIEMPO DE SOLUCIÓN
Crítica *	Más de 10 usuarios / múltiples dependencias / servicios misionales o core	Inmediata – operación institucional comprometida	30 minutos	120 minutos
Alta	5–10 usuarios / servicios institucionales importantes (GeDeSS, VPN, correo)	Alta – impacta la operación de la entidad	60 minutos	180 minutos
Media	2–5 usuarios / aplicaciones ofimáticas, sistemas administrativos, impresoras	Media – no interrumpe completamente la operación	90 minutos	240 minutos

Baja	1 usuario / baja criticidad (estaciones de trabajo, periféricos, puntos de red)	Baja – no impacta la operación institucional	120 minutos	300 minutos

*Ejemplos de este tipo de incidentes incluyen fallas en aplicaciones misionales o sistemas Core, bases de datos institucionales, servicio de correo electrónico institucional, Directorio Activo, infraestructura de red (switch core), servicios de seguridad perimetral (firewall), servicios de conectividad, portales web institucionales, servicios financieros y, en general, cualquier servicio tecnológico corporativo que soporte la operación institucional y los servicios ciudadanos.

Nota: Los tiempos de atención y solución descritos corresponden a la parametrización actual definida en la herramienta institucional de gestión de servicios (Aranda), conforme a los ANS establecidos por la Dirección de Tecnología."

5.4. Notificaciones Automáticas

La herramienta institucional de Gestión de Servicios TIC enviará notificaciones automáticas (estas notificaciones tienen como finalidad alertar sobre el vencimiento próximo del tiempo de atención, con el fin de garantizar el cumplimiento de los niveles de servicio establecidos) desde el correo electrónico del Centro de Servicios Tecnológicos (servicios.tecnologicos@supersociedades.gov.co) a los grupos solucionadores y demás instancias responsables, conforme a los porcentajes de tiempo transcurrido del Acuerdo de Nivel de Servicio (ANS):

Notificación al 50%	Notificación al 75%	Notificación al 100%
Especialista asignado, Coordinador del Grupo.	Especialista asignado, Coordinador del Grupo, Supervisor del contrato.	Especialista asignado, Coordinador del Grupo, supervisor del contrato, director.

5.5. Gestión de Incidentes Relacionados y Recurrentes

- Cuando múltiples incidentes reportados correspondan a una misma afectación o causa común, se deberá crear o identificar un caso principal (caso padre) y asociar los demás casos como casos relacionados o casos hijos en la herramienta ITSM.

- El caso padre será gestionado por el grupo solucionador correspondiente y concentrará el seguimiento técnico del evento. Las actualizaciones y comunicaciones masivas relacionadas con el incidente serán realizadas por el Nivel 2 del CST mediante los canales institucionales definidos.

- Los casos hijos deberán mantenerse asociados al caso principal con el fin de garantizar la trazabilidad, evitar reprocesos y facilitar la comunicación masiva a los usuarios afectados. El cierre del caso padre generará automáticamente el cierre de los casos hijos asociados en la herramienta ITSM.

- Los incidentes identificados como recurrentes deberán ser gestionados mediante la práctica de Gestión de Problemas, con el propósito de analizar su causa raíz y establecer acciones que eviten su repetición y mejoren la estabilidad de los servicios TIC.

- La herramienta ITSM realizará el cierre automático del incidente cuando el usuario no diligencie la encuesta de satisfacción dentro de los cuatro (4) días calendario posteriores a su notificación.

- Los incidentes mayores o masivos deberán clasificarse con prioridad Crítica y seguirán el flujo de Gestión de Incidentes Mayores definido en la sección B del procedimiento.

5.6. Incidentes de Seguridad de la Información

Los incidentes de seguridad de la información deberán ser gestionados conforme a lo establecido en la GTI-GU-006_GestionIncidentes_y los lineamientos institucionales de Seguridad de la Información. Se consideran incidentes de seguridad, entre otros, los siguientes eventos:

- Pérdida, robo o extravío de información clasificada o reservada alojada en cualquier componente de la infraestructura tecnológica de la Entidad.
- Alteración, modificación o eliminación no autorizada de información confidencial o datos personales almacenados en los sistemas de información o dispositivos tecnológicos institucionales.
- Instalación, ejecución o uso de software o aplicaciones no autorizadas en los equipos o dispositivos tecnológicos de la Entidad.
- Interrupción no autorizada o prolongada de servicios tecnológicos, sistemas de información o servicios de red institucionales.
- Incumplimiento de las políticas, normas o lineamientos de seguridad de la información establecidos por la Superintendencia de Sociedades.
- Identificación de vulnerabilidades técnicas en software, sistemas operativos, aplicaciones, dispositivos de red, servidores, estaciones de trabajo o dispositivos móviles que puedan comprometer la seguridad de la información.
- Infección de dispositivos tecnológicos por código malicioso, incluyendo virus, gusanos, troyanos, ransomware u otros tipos de malware.

- Ataques informáticos dirigidos a la infraestructura tecnológica, red corporativa, sistemas de información o aplicaciones web institucionales.
- Pérdida, robo o extravío de activos tecnológicos institucionales que contengan información de la Entidad y que puedan representar un riesgo para la seguridad de la información.

5.7. Roles y Responsabilidades

Rol	Responsabilidad
Usuario del CST	• Registrar incidentes o solicitudes a través del Portal de Servicios o canales definidos. • Proporcionar información clara y completa para la atención del caso. • Hacer seguimiento al estado de sus solicitudes en la herramienta ITSM. • Atender el llamado del personal del CST en caso de requerir validaciones o conexión remota. • Validar la solución implementada por el Centro de Servicios Tecnológicos. • Calificar la encuesta de satisfacción del servicio dentro del tiempo establecido.
Agente de contacto CST	• Registrar y/o gestionar los incidentes y requerimientos recibidos por los diferentes canales de atención (Correo, Teléfono y Portal de Servicios), de manera oportuna. • Registrar, clasificar y categorizar incidentes y solicitudes en la herramienta ITSM. • Garantizar una comunicación clara con los usuarios y registrar la información necesaria para la atención de los casos. • Realizar el escalamiento de los incidentes y requerimientos al siguiente nivel, de acuerdo con la Matriz de Escalamiento CST. • Mantener informado al usuario sobre el estado de su solicitud.

Solucionadores – Soporte Nivel 1 CST	• Atender y gestionar oportunamente los incidentes y solicitudes recibidos a través de los canales oficiales, registrándolos en la herramienta ITSM y brindando soporte presencial y/o remoto conforme a los ANS establecidos. • Analizar, diagnosticar y resolver los incidentes y requerimientos asignados, garantizando su atención dentro de los tiempos establecidos en los Acuerdos de Nivel de Servicio (ANS). • Gestionar, cuando aplique, los incidentes y/o requerimientos ante el proveedor o fabricante correspondiente, realizando el seguimiento y actualizando oportunamente el estado en la herramienta de gestión ITSM. • Registrar, documentar y mantener actualizada la información del incidente o requerimiento en la herramienta ITSM, garantizando la trazabilidad y manteniendo informado al usuario. • Monitorear el estado y progreso de los casos asignados hasta su solución y cierre. • Ejecutar las actividades necesarias para dar trámite y solución a los incidentes y requerimientos. • Participar en las actividades de mejora continua del servicio y de los procesos del Centro de Servicios Tecnológicos. • Contribuir a la actualización y alimentación de la Base de Conocimiento, documentando las soluciones implementadas.

Solucionadores – Soporte Nivel 2 y 3 CST	• Atender y gestionar oportunamente los incidentes y solicitudes recibidos a través de los canales oficiales, registrándolos en la herramienta ITSM y brindando soporte presencial y/o remoto conforme a los ANS establecidos • Analizar, diagnosticar y resolver los incidentes y requerimientos asignados, garantizando su atención dentro de los tiempos establecidos en los Acuerdos de Nivel de Servicio (ANS). • Gestionar, cuando aplique, los incidentes y/o requerimientos ante el proveedor o fabricante correspondiente, realizando el seguimiento y actualizando oportunamente el estado en la herramienta de gestión ITSM. • Registrar, documentar y mantener actualizada la información del incidente o requerimiento en la herramienta ITSM, garantizando la trazabilidad y manteniendo informado al usuario. • Monitorear el estado y progreso de los casos asignados hasta su solución y cierre. • Ejecutar las actividades necesarias para dar trámite y solución a los incidentes y requerimientos. • Participar en las actividades de mejora continua del servicio y de los procesos del Centro de Servicios Tecnológicos. • Contribuir a la actualización y alimentación de la Base de Conocimiento, documentando las soluciones implementadas. • Proporcionar soporte técnico y funcional a los usuarios en el uso de los sistemas misionales, tales como GeDeSS, SIGS, Expediente Digital, BPM, Baranda Virtual, soluciones de inteligencia artificial y el Módulo de Insolvencia, entre otros, garantizando la continuidad operativa y el adecuado funcionamiento de los servicios tecnológicos.

Coordinador Mesa de Servicios – CST	• Supervisar la operación del Centro de Servicios Tecnológicos, garantizando la adecuada gestión de incidentes, requerimientos y solicitudes de servicio, conforme a los procedimientos y Acuerdos de Nivel de Servicio (ANS) establecidos. • Coordinar, asignar y realizar seguimiento a las actividades del equipo de soporte y demás recursos que intervienen en la operación, asegurando una atención oportuna, eficiente y de alta calidad. • Monitorear el estado y la gestión de los casos registrados en la herramienta ITSM, garantizando su correcta atención, actualización y cierre. • Asegurar la correcta ejecución de los procesos de Gestión de Incidentes y Requerimientos, conforme a las buenas prácticas y lineamientos definidos por la entidad. • Gestionar el seguimiento al backlog del Centro de Servicios Tecnológicos, promoviendo su control y reducción. • Monitorear el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) y realizar seguimiento a los niveles de satisfacción de los usuarios, promoviendo acciones de mejora cuando aplique. • Consolidar, revisar y presentar los informes de gestión, reportes, indicadores, estadísticas y demás información relacionada con la operación del servicio, conforme a la periodicidad y condiciones establecidas por la entidad. • Velar por la calidad del servicio prestado por el Centro de Servicios Tecnológicos, promoviendo la mejora continua de los procesos y la satisfacción de los usuarios.

Coordinador Mesa de Servicios – CST/Gestor de Incidentes	• Gestionar y supervisar la eficiencia y efectividad del proceso de Gestión de Incidentes de Servicios TIC, garantizando su adecuada ejecución conforme a los lineamientos definidos por la Dirección de Tecnología. • Asegurar que los incidentes sean gestionados correctamente durante todo su ciclo de vida, desde su registro hasta su resolución y cierre, garantizando la trazabilidad y el cumplimiento de los Acuerdos de Nivel de Servicio (ANS). • Asegurar que los incidentes sean gestionados correctamente durante todo su ciclo de vida, desde su registro hasta su resolución y cierre, garantizando la trazabilidad y el cumplimiento de los Acuerdos de Nivel de Servicio (ANS). • Coordinar la integración del proceso de Gestión de Incidentes con los demás procesos de gestión de servicios TIC, tales como Gestión de Problemas, Gestión de Cambios y Gestión de Requerimientos. • Generar, analizar y reportar los indicadores y métricas del proceso, con el fin de evaluar su desempeño y fortalecer la calidad del servicio • Apoyar al Centro de Servicios Tecnológicos (CST) y a los grupos solucionadores en la gestión de escalamientos funcionales y jerárquicos, cuando sea requerido. • Coordinar y gestionar el esquema de comunicación de los incidentes mayores, garantizando la notificación oportuna a los usuarios afectados, grupos técnicos y partes interesadas, hasta el restablecimiento del servicio.
Coordinador Mesa de Servicios – CST/ Gestor de Incidentes	• Definir y mantener las políticas, lineamientos y estándares del proceso de Gestión de Incidentes. • Asegurar el seguimiento, control y mejora continua del proceso y sus indicadores. • Velar por el cumplimiento del propósito del proceso y proponer acciones de mejora cuando sea necesario.
Solucionador – Soporte Nivel 1/Gestor de Calidad	• Recibir y analizar las inconformidades reportadas por los usuarios a través de las encuestas de satisfacción o los diferentes canales de atención (correo, Teléfono, Portal de Servicios). • Realizar seguimiento a las inconformidades reportadas por los usuarios o identificadas durante la operación del servicio, incluyendo los casos reabiertos en estado "Devolución por Calidad", con el fin de fortalecer la calidad de la atención y garantizar una solución efectiva al usuario. • En conjunto con los grupos solucionadores, proponer acciones de mejora relacionadas con la atención, documentación y gestión de incidentes y requerimientos.

5.8. Indicadores del Proceso

Para el seguimiento y control del procedimiento se definen los siguientes indicadores de medición:

Nombre del indicador	Fórmula	Meta	Responsable	Frecuencia	Propósito
Porcentaje de incidentes atendidos	(Número total de incidentes atendidos / Número total de incidentes registrados) × 100	**>=90%**	Gestor de Incidentes/ Coordinador CST	Mensual	Medir cumplimiento de tiempos de atención

6. PROCEDIMIENTO

A. Gestión de Incidentes

No.	Actividad	Responsable	Punto de Control	Registro
1	**Registrar Solicitud:** El usuario reporta una interrupción o degradación de un servicio TIC a través de los canales oficiales (Portal de Servicios, correo electrónico, línea telefónica). El agente CST registra el incidente en la herramienta ITSM asignando un número único de identificación.	Usuario / Agente CST	No Aplica	Correo Electrónico / línea telefónica 911/ Herramienta de Gestión ITSM
2	**Validar y Clasificar Solicitud:** Verificar que la solicitud corresponda al catálogo de servicios TIC y clasificarla correctamente como incidente o solicitud de servicio. Si corresponde a un	Agente CST/ Coordinador CST	X	Herramienta de Gestión ITSM

No.	Actividad	Responsable	Punto de Control	Registro
	requerimiento gestionar conforme al procedimiento de Gestión de Requerimientos. Si no está en catálogo orientar al usuario hacia el canal o dependencia correspondiente. Si es duplicado o incorrecto. Anular con justificación (solo coordinador CST o Agente de Calidad)			
3	**Categorizar y Priorizar:** Clasificar el incidente conforme al Catálogo de Servicios TIC. Asignar la prioridad (Crítica, Alta, Media, Baja) según la combinación de impacto y urgencia, conforme a los ANS definidos. Verificar en la Base de Conocimiento y CMDB si existe información relevante del elemento de configuración afectado.	Agente CST	Verificar asignación correcta de prioridad según impacto y urgencia	Herramienta de Gestión ITSM
4	**Realizar diagnóstico inicial:** Analizar los síntomas y el alcance del incidente. Consultar la Base de Conocimiento y los errores conocidos documentados. Si existe una solución documentada, aplicarla directamente. Si es posible resolver en Nivel 1, proceder a la resolución. Si no es posible, escalar al nivel correspondiente.	Agente CST (Nivel 1 / Nivel 2)	Verificar consulta de Base de Conocimiento antes de escalar	Herramienta de Gestión ITSM
5	**Verificar si es un Incidente Mayor:** Determinar si el incidente corresponde a un Incidente Mayor según los criterios de impacto definidos por la Entidad (afectación	Agente CST (Nivel 2)	Verificar criterios de clasificación como Incidente Mayor	Herramienta de Gestión ITSM

No.	Actividad	Responsable	Punto de Control	Registro
	crítica, múltiples usuarios o dependencias, servicios misionales). Si es Incidente Mayor, activar el flujo B de Gestión de Incidentes Mayores			
6	**Escalar incidente:** La Herramienta de Gestión ITSM asigna automáticamente el incidente al grupo solucionador correspondiente, conforme a las reglas de asignación y matriz de escalamiento definidas por la Dirección de Tecnología.	Agente CST	No Aplica	Herramienta de Gestión ITSM
7	**Verificar si es un incidente de seguridad:** El grupo solucionador valida si el incidente corresponde a un incidente de seguridad de la información. Si aplica, se notifica al responsable y se gestiona conforme a la GTI-GU-006_GestionIncidentes	Solucionador/ Responsable Seguridad	Verificar criterios de clasificación como incidente de seguridad	Herramienta de Gestión ITSM
8	**Investigar y Diagnosticar**: El grupo solucionador realiza análisis técnico profundo del incidente. Identifica la causa probable, evalúa el alcance total del impacto y determina la solución más adecuada (definitiva o temporal/workaround). Documenta hallazgos en la herramienta ITSM.	Grupo Solucionador	No Aplica	Herramienta de Gestión ITSM
9	**Aplicar Solución (Temporal O Definitiva):** Ejecutar las acciones necesarias para restablecer el servicio afectado. Si se aplica una	Grupo Solucionador	No Aplica	Herramienta de Gestión ITSM

No.	Actividad	Responsable	Punto de Control	Registro
	solución temporal (workaround), documentarla claramente en la herramienta ITSM e indicar que se requiere solución definitiva. Si se requiere un cambio para la solución definitiva, coordinar con el procedimiento de Gestión de Cambios en ambiente productivo. Verificar el restablecimiento del servicio.			
10	**Documentar Solución En Base De Conocimiento**: Registrar la solución implementada en la Base de Conocimiento institucional para facilitar la resolución de incidentes similares en el futuro. Incluir síntomas, diagnóstico, solución aplicada y, si aplica, solución temporal utilizada.	Grupo Solucionador	No Aplica	Herramienta de Gestión ITSM
11	**Notificar solución y enviar encuesta:** La herramienta notifica al usuario la solución del incidente y envía la encuesta de satisfacción para evaluar la calidad del servicio.	Herramienta de Gestión ITSM	No Aplica	Herramienta de Gestión ITSM
12	**Gestionar inconformidad (si aplica):** Cuando la evaluación del servicio no sea satisfactoria, el incidente deberá reabrirse en estado "Devolución por Calidad". Se gestionan nuevamente las acciones de resolución, documentando los pasos adicionales y asegurando la trazabilidad del caso hasta garantizar la solución efectiva.	Herramienta de Gestión ITSM / Agente CST (Nivel 1)/ Gestor de Calidad	X	Herramienta de Gestión ITSM

No.	Actividad	Responsable	Punto de Control	Registro
13	**Cerrar el incidente:** El incidente es cerrado automáticamente cuando el usuario diligencia la encuesta de satisfacción de forma positiva o cuando transcurren cuatro (4) días calendario sin respuesta del usuario. Se registra el estado final y se garantiza la trazabilidad completa del caso.	Herramienta de Gestión ITSM	No Aplica	Herramienta de Gestión ITSM
B. Gestión incidentes mayores				
14	**Declarar y notificar Incidente Mayor:** Declarar formalmente el Incidente Mayor. El Nivel 2 del CST realizará la comunicación masiva a los usuarios de la Entidad sobre la indisponibilidad del servicio y el estado de la gestión, mediante las plantillas establecidas y a través del buzón de correo asignado al CST. Informar a la Dirección de Tecnología.	Coordinador CST / Agente CST (Nivel 2)	No Aplica	Correo Electrónico
15	**Convocar equipo técnico especializado:** Activar y convocar al equipo técnico responsable del servicio afectado para atención prioritaria. El equipo debe estar integrado por los responsables técnicos de los servicios comprometidos y coordinado por la Dirección de Tecnología.	Equipo Solucionador de Incidentes Mayores	No Aplica	Correo Electrónico
16	**Analizar, diagnosticar y aplicar solución**: Verificar si existe una solución documentada en la Base de	Equipo Solucionador de Incidentes Mayores	No Aplica	Herramienta de Gestión ITSM

No.	Actividad	Responsable	Punto de Control	Registro
	Conocimiento. Realizar análisis técnico y diagnóstico para identificar la causa del incidente. Aplicar solución temporal (workaround) inmediata para restaurar el servicio. Actualizar continuamente el estado y avances en la herramienta ITSM para garantizar comunicación oportuna al CST y usuarios.			
17	**Notificar restablecimiento del servicio**: Una vez restablecido el servicio informar al CST la restauración, el Nivel 2 del CST realizará la notificación de restablecimiento a los usuarios de la Entidad mediante las plantillas establecidas y a través del buzón de correo asignado al CST, informando la disponibilidad del servicio.	Equipo Solucionador de Incidentes Mayores Coordinador CST / Agente CST (Nivel 2)	X	Herramienta de Gestión ITSM
18	**Realizar Revisión Post-Incidente:** Dentro de los cinco (5) días hábiles siguientes al cierre del Incidente Mayor, el equipo técnico y el Coordinador CST realizan la revisión post-incidente. Se documentan: cronología del incidente, impacto, acciones ejecutadas, efectividad de la respuesta y lecciones aprendidas. El informe se comparte con la Dirección de Tecnología.	Coordinador CST / Equipo Técnico	No Aplica	Correo electrónico
19	**Postular A Gestión De Problemas:** El Incidente Mayor y los incidentes	Coordinador CST	x	Herramienta de Gestión ITSM

No.	Actividad	Responsable	Punto de Control	Registro
	recurrentes son postulados formalmente al proceso de Gestión de Problemas para el análisis de causa raíz y el establecimiento de soluciones definitivas que prevengan la recurrencia.			
FIN DEL PROCEDIMIENTO				

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
01	30/06/2026.	Versión inicial.

Elaboró	Revisó	Aprobó
Nombre: Leidy Dayanny Molano Cogollo Cargo: Agente Técnico Fecha: 30/05/2026	Nombre: Jhoan Manuel Espinosa Montilla Cargo: Coordinador de CST Fecha: 30/05/2026	Nombre: Ricardo Ríos Rosales Cargo: director de Tecnología de la información y las comunicaciones Fecha:20/06/2026