ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

IPES

PROCEDIMIENTO DE ATENCIÓN DE MESA DE AYUDA E INFRAESTRUCTURA TECNOLÓGICA CON GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO
INSTITUTO PARA LA ECONOMÍA SOCIAL PES

Bogotá, MAYO 2026

Elaboró	Aprobó:	Aprobó:
Michael Brayan Pinilla Coy Contratista IPES GIRT – SDAE Alexandra Marin Parra Servidora Publica GIRT – SDAE	Hans Lwver Carlosama Alferez Profesional Especializado GIRT - SDAE Edgar Mauricio Mera Erazo Contratista SDAE	Adriana Villamizar Navarro Subdirectora de Diseño y Análisis Estratégico

Tabla de contenido

1. OBJETIVO....3
2. ALCANCE....3
3. RESPONSABLES....3
4. DEFINICIONES Y ABREVIATURAS....4
5. CONDICIONES GENERALES....6
6. DESCRIPCIÓN DEL PROCEDIMIENTO....8
7. PROTOCOLO DE ATENCIÓN DE INCIDENTES MAYORES O MASIVOS....15
8. ARTICULACIÓN CON OTROS PROCESOS....16
9. DOCUMENTOS ASOCIADOS....17
10. MARCO NORMATIVO....17

1. OBJETIVO

Establecer la metodología y los pasos para la gestión de las solicitudes e incidentes tecnológicos a través de la Mesa de Ayuda del IPES, garantizando una atención oportuna, trazable y alineada con los controles del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), en cumplimiento de los lineamientos del MSPI v5.0 de MinTIC y los controles del Anexo A de la NTC/ISO-IEC 27001:2022

2. ALCANCE

Este procedimiento aplica para todos los funcionarios y contratistas del IPES. La Mesa de Ayuda registrará todos los casos de hardware y software reportados relacionados con el soporte de los sistemas de información e infraestructura tecnológica de la entidad; los requerimientos quedarán registrados en el sistema dispuesto para ello.

Se enmarca en la política de seguridad digital del Modelo Integrado de Planeación y Gestión – MIPG, en los lineamientos del MSPI v5.0 de MinTIC, y en la Cláusula 8.1 (Planificación y control operacional) de la NTC/ISO-IEC 27001:2022. Se orienta a la gestión de la infraestructura tecnológica soportada y administrada por el proceso de Gestión de la Seguridad de la Información y Recursos Tecnológicos – PGSIRT, incluyendo la detección y escalamiento oportuno de eventos de seguridad de la información

3. RESPONSABLES

Usuario: Persona que solicita soporte ante un problema, incidente o evento tecnológico, a través de la aplicación de Mesa de Ayuda o el chat IPESencasa. Es responsable de confirmar la solución dentro de los 15 días calendario establecidos y de diligenciar la encuesta de satisfacción para el cierre formal del ticket.

Coordinador de Mesa de ayuda: Encargado de recepcionar y asignar las peticiones de soporte al grupo técnico. Monitorea los tickets "abandonados" y ejecuta el cierre administrativo y el cierre de gestión anual (1-15 de enero). En el marco del SGSPI, apoya el seguimiento a los indicadores de gestión de incidentes conforme a la Cláusula 9.1 de la NTC/ISO-IEC 27001:2022.

Agente de Mesa de ayuda: Punto de contacto principal para el registro y solución de incidentes en primera instancia. Responsable de categorizar correctamente (Incidente vs. Petición), asignar la prioridad según la matriz Impacto x Urgencia, consultar la Base de Conocimiento antes de escalar, y documentar la causa raíz o postular el caso a Gestión de Problemas. Aplica los controles A.6.8 (reporte de eventos) y A.5.25 (evaluación de eventos de seguridad) de la NTC/ISO-IEC 27001:2022.

El personal profesional / técnico de Sistemas: Gestiona los servicios asignados por el Coordinador, garantizando el soporte y la resolución de los incidentes y requerimientos en segundo nivel. Documenta las soluciones aplicadas y las lecciones aprendidas en la Base de Conocimiento.

Soporte Especializado:Tercero al que se escalan los requerimientos técnicos especializados que superan la capacidad de resolución interna. Responsable de documentar y finalizar el caso en el repositorio designado, en cumplimiento de los requisitos de seguridad establecidos contractualmente conforme al control A.5.19 de la NTC/ISO-IEC 27001:2022 (Seguridad de la información en las relaciones con proveedores).

Oficial de Seguridad de la Información: Responsable de recibir el escalamiento de eventos sospechosos que puedan catalogarse como incidentes de seguridad digital.

Evalúa el impacto, gestiona la contención y resolución del incidente, y determina si se requiere activar el Plan de Contingencia o notificar a entes externos de control. Ejerce sus funciones conforme a los controles A.5.24 (Planificación y preparación de la gestión de incidentes), A.5.26 (Respuesta a incidentes) y A.5.28 (Recolección de evidencias) de la NTC/ISO-IEC 27001:2022.

4. DEFINICIONES Y ABREVIATURAS

- **Estado del Ticket**: Indica la fase de gestión en que se encuentra una solicitud registrada en la Mesa de Ayuda. Los estados posibles son:
  - ***Nuevo*** **:** Cuando el usuario registra la solicitud en la Mesa de Ayuda.
  - **En curso asignada** **:** La solicitud ha sido asignada a un Agente de Mesa de Ayuda.
  - **En curso planificada** **:** El usuario y el Agente han acordado una fecha proyectada de atención.
  - **En espera** : El tratamiento está sujeto a un factor externo o interno (recepción de repuesto, autorización del usuario, respuesta de proveedor). Por ejemplo, el trabajo no puede continuar hasta que se reciba un repuesto, la respuesta de un proveedor o del Agente de Mesa de Ayuda está esperando la autorización del usuario para realizar algún proceso.
  - ***Resuelta*** **:** El usuario ha confirmado que el problema está resuelto.
  - ***Cerrado*** **:** El usuario diligenció la encuesta de satisfacción y el caso quedó totalmente cerrado.
- **Mesa de ayuda:** Aplicativo institucional donde quedan registrados todos los soportes solicitados al grupo técnico. Disponible en http://mesadeayuda.ipes.gov.co
- **Ticket**: Número identificador único del caso, que contiene la información del incidente o requerimiento reportado, su estado y la trazabilidad de la gestión realizada.
- **Tiempos de respuesta:** El personal de soporte técnico, tiende un tiempo de 15 minutos para contactar al usuario personalmente o vía telefónica, después de haber solicitado un servicio o soporte técnico.
- **Tiempo de solución del servicio:** Tiempo estipulado para la solución del servicio

- según el nivel de escalamiento.
    - **Tiempo de solución Nivel 1:** El personal de soporte técnico tiene entre 2 – 12 horas para solucionar el caso.
    - **Tiempo de solución Nivel 2:** El personal técnico tiene entre 2 a 24 horas para solucionar el caso.
    - **Tiempo de solución Nivel 3:** el personal técnico tiene entre 2 a 48 horas para solucionar el caso.
- **IPESencasa:** Este servicio se utiliza solo para los funcionarios que se encuentran en teletrabajo, trabajo en casa o que presentan algún problema con la VPN (conexión remota.
- **Incidente:** Se define como una desviación de la operación normal de un servicio de TI. Incluye fallas en el hardware, problemas de software, errores de red o cualquier situación que impida usar un servicio de manera efectiva.
- **Petición (o Requerimiento de Servicio):** Corresponde a solicitudes de servicios estándar (como acceso a aplicaciones, instalación de software, suministro de información) que no corresponden a una falla o error del sistema.
- **Cierre Administrativo:** Acción ejecutada por el equipo de soporte para cerrar un ticket cuando el usuario no ha confirmado la solución dentro del plazo establecido (15 días) o durante el cierre de gestión anual.
- **Solicitud Cerrada:** Estado final de un ticket que ocurre cuando el usuario confirma la solución o cuando ha transcurrido el plazo de 15 días sin respuesta.
- **Base de Datos de Conocimiento (KB):** Colección de información (artículos, manuales, soluciones previas) utilizada por los agentes para resolver incidentes de forma más eficiente y por los usuarios para autoayuda
- **Administrador DBA:** Profesional encargado de la gestión, mantenimiento y cierre técnico en base de datos de los tickets en la plataforma
- **Cierre Administrativo:** Cierre ejecutado por el equipo de soporte ante la inactividad del usuario tras un tiempo determinado.
- **Evento de seguridad de la información:** Ocurrencia identificada en un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. (Referencia: NTC/ISO-IEC 27001:2022, control A.6.8)
- **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.24)

- **Incidente tecnológico (TI):** Interrupción no planificada o degradación de la calidad de un servicio tecnológico que no necesariamente constituye un incidente de seguridad de la información. Se gestiona a través del flujo estándar de la Mesa de Ayuda.

- **Petición de servicio:** Solicitud formal de un usuario para obtener acceso a un servicio, recurso o información, o para ejecutar una tarea estándar. No implica una falla o degradación del servicio.

- **Base de Conocimiento (KB):** Repositorio institucional de soluciones documentadas, errores conocidos y lecciones aprendidas, de consulta obligatoria por parte del Agente antes de escalar un ticket. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.27)

- **Error Conocido:** Problema que tiene una causa raíz documentada y una solución temporal o definitiva registrada en la Base de Conocimiento, que permite su resolución en el primer contacto.

- **Gestión de Problemas:** Proceso orientado a identificar y eliminar la causa raíz de incidentes recurrentes, con el fin de prevenir su reaparición. Un caso se postula a Gestión de Problemas cuando la solución aplicada es temporal o cuando se detecta un patrón de recurrencia.

- **Cierre Administrativo:** Cierre de un ticket ejecutado por el Administrador o el sistema cuando el usuario no confirma ni rechaza la solución dentro de los 15 días calendario siguientes a la notificación de resolución.

- **Cierre de Gestión Anual:** Proceso ejecutado entre el 1 y el 15 de enero por el Coordinador de Mesa de Ayuda, mediante el cual se cierran masivamente los tickets que al 31 de diciembre se encuentren en estado Asignado sin movimiento, En espera, o Resuelto sin cierre formal por el usuario.

- **SGSPI:** Sistema de Gestión de Seguridad y Privacidad de la Información del IPES, alineado con el MSPI v5.0 de MinTIC y la NTC/ISO-IEC 27001:2022.

- **MSPI:** Modelo de Seguridad y Privacidad de la Información del MinTIC, marco de referencia obligatorio para las entidades del Estado colombiano.

5. CONDICIONES GENERALES

- Los servicios de soporte técnico únicamente se proporcionarán a equipos, periféricos y servicios tecnológicos que hagan parte del inventario de activos del IPES.

- Solo se atenderán casos que sean competencia del área, incluyendo:

    - Reparar, instalar y configurar equipos informáticos de la entidad.

    - Acudir a los puestos de trabajo de los usuarios y dar solución a problemas de software y/o hardware.

    - Mantener en operatividad los equipos de cómputo de la entidad..

- Todas las solicitudes de soporte deberán registrarse a través de la aplicación de

- Mesa de Ayuda o el chat IPESencasa. No se atenderán requerimientos por canales informales que no generen número de ticket.

- No se atenderán casos de ofimática básica, pues constituyen competencias propias de cada funcionario o contratista..

- En caso de cambio o formateo de equipo, se debe diligenciar el formato Lista de Chequeo para Cambio o Formateo de Equipos antes de ejecutar la acción.

- Cuando el usuario requiera copia de respaldo de su información, deberá diligenciar el formato “Solicitud de Recuperación de Información”. La custodia de la información respaldada será responsabilidad del usuario final. (Referencia: NTC/ISO-IEC 27001:2022, control A.8.13 Respaldo de la información)

- Se atenderán únicamente los requerimientos registrados mediante un consecutivo de ticket en la herramienta de Mesa de Ayuda.

- Todo ticket creado en la herramienta debe cumplir con el ciclo completo de estados definido en este procedimiento, desde la solicitud hasta su cierre formal o administrativo.

- El usuario tiene un plazo máximo de 15 días calendario para confirmar o rechazar la solución notificada. Vencido este plazo sin respuesta, el ticket se cerrará administrativamente con la nota interna correspondiente.

- Entre el 1 y el 15 de enero de cada año, el Coordinador de Mesa de Ayuda ejecutará el Cierre de Gestión Anual para los tickets que al 31 de diciembre se encuentren en estado Asignado sin movimiento, En espera, o Resuelto sin cierre formal por el usuario.

- Cuando un incidente se solucione mediante una medida temporal sin identificar la causa raíz definitiva, o cuando se detecten múltiples incidentes con la misma recurrencia, el Agente de Mesa de Ayuda deberá postular el caso a Gestión de Problemas para su investigación profunda y eliminación de la causa raíz. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.27 Aprendizaje de los incidentes de seguridad)

- Todo evento que durante la atención del ticket presente indicios de ser un incidente de seguridad de la información deberá escalarse de forma inmediata al Oficial de Seguridad de la Información, suspendiendo la atención técnica ordinaria hasta recibir instrucción de dicho funcionario. (Referencia: NTC/ISO-IEC 27001:2022, controles A.5.25 y A.5.26)

- La información generada durante la gestión de tickets, incluyendo diagnósticos, soluciones aplicadas y evidencias de incidentes, deberá tratarse conforme a los criterios de clasificación de la información definidos en el SGSPI del IPES, garantizando su confidencialidad, integridad y disponibilidad. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.12 Clasificación de la información)

- Los tiempos máximos de atención por nivel de prioridad son:

Prioridad	Criterio	Tiempos de respuesta	Tiempos de solución
Critica	Afecta a toda la entidad o	15 minutos	4 horas

	servicio misional		
Alta	Afecta a un área completa o usuario clave	1 hora	8 horas
Media	Afecta a un usuario, con workaround disponible	4 horas	2 días habiles
Baja	Solicitud estándar sin impacto operativo	8 horas	5 días habiles

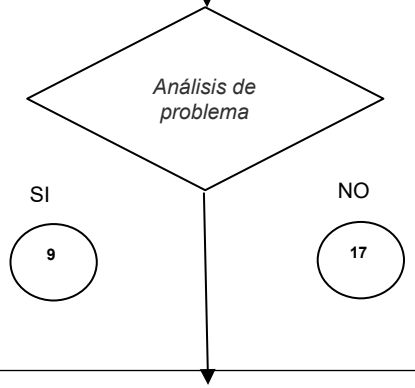
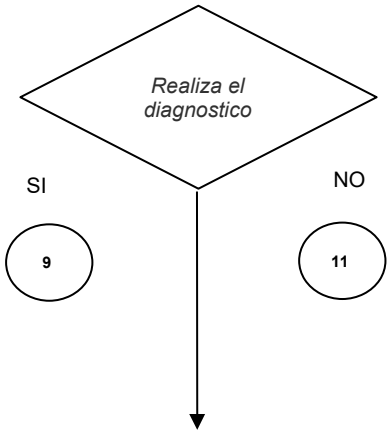
Reportes: La mesa de ayuda genera reportes estadísticos registrados en el aplicativo de mesa de ayuda, con respecto a IPESencasa se realiza un reporte en Excel, los cuales se manejan internamente en el PGSIRT.

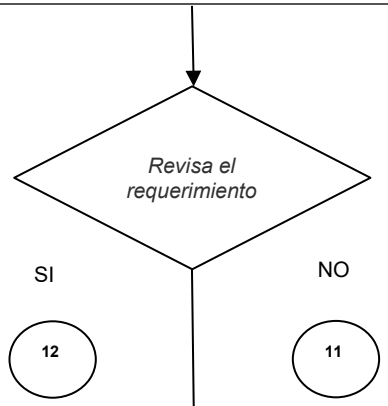
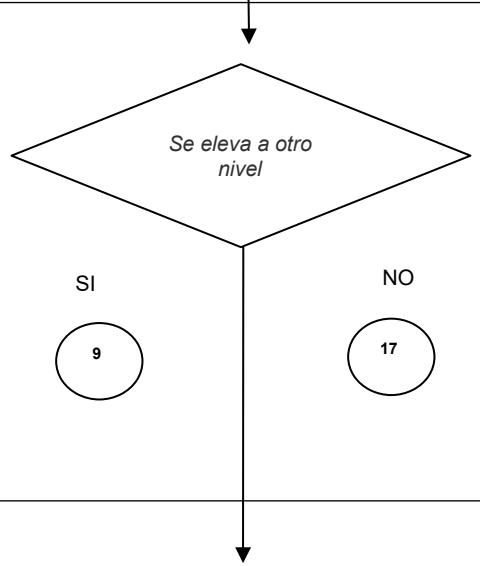
6. DESCRIPCIÓN DEL PROCEDIMIENTO

El documento contará con la siguiente tabla descriptiva:

No	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable	Punto de control	Registro
1	**INICIO**	Inicio del procedimiento			
2	Reportar la falla	El usuario registra el problema, incidente o solicitud de servicio a través de la aplicación de Mesa de Ayuda o el chat IPESencasa. El reporte debe incluir una descripción clara del problema, el equipo o sistema afectado y el impacto percibido sobre su labor. No se atenderán requerimientos reportados por canales no oficiales.	Usuario		Aplicación Mesa de Ayuda link: http://mesadeayuda.ipes.gov.co Chat IPESencasa
3	*Es Incidente o Petición?* Petición → 5 Solicitud → 4	**Petición:** Solicitud estándar de servicio. Continúa en actividad 5. **Incidente:** Falla o degradación de un servicio. Continúa en 4.	Agente de Mesa de Ayuda		
4	¿Tiene indicios de ser un evento de seguridad de la información?	El Agente evalúa si el incidente presenta alguno de los criterios de escalamiento al Oficial de Seguridad de la Información (código malicioso, ingeniería social, accesos no autorizados, pérdida de información). **SÍ:** Se escala inmediatamente al Oficial de Seguridad de la			

	Si / No 5	Información y se activa el procedimiento de Gestión de Incidentes de Seguridad. (Referencia: NTC/ISO-IEC 27001:2022, controles A.6.8 y A.5.25) **NO:** Continúa en actividad 5.			
5	Análisis y asignación por niveles.	El Agente consulta obligatoriamente la Base de Conocimiento (KB) antes de escalar el ticket. Si existe un artículo o Error Conocido que describa la falla, aplica la solución documentada de forma inmediata. Se asigna la prioridad del ticket conforme a la matriz Impacto x Urgencia y los tiempos definidos en las Condiciones Generales. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.27)	Agente de Mesa de Ayuda		
6	*¿Es un Incidente Masivo?* SI / N 7	El Agente o Coordinador evalúa si el incidente cumple criterios de masividad (impacto extenso, criticidad del servicio afectado, múltiples tickets con la misma falla en corto periodo). **SÍ:** Se activa el Protocolo de Incidentes Mayores, se crea un Ticket Padre y se vinculan los casos individuales. Se publica comunicado masivo a los usuarios. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.29 Continuidad de la seguridad de la información durante una interrupción) **NO:** Continúa el flujo normal de soporte técnico en actividad 7.	Agente de Mesa de Ayuda Coordinador		

7		Se notifica al usuario el número de ticket asignado, el estado inicial y el Agente responsable de su atención. La notificación se realiza por el mismo canal utilizado para el reporte (Mesa de Ayuda o IPESencasa). A partir de este momento comienza a correr el tiempo de atención según la prioridad asignada.	Agente de Mesa de Ayuda	No. De ticket del asignado y el estado	Aplicación Mesa de Ayuda link: http://mesadeayuda.ipes.gov.co/ Chat IPESencasa
8		El Agente analiza la solicitud y determina si está dentro del alcance de la Mesa de Ayuda. **SÍ:** Realiza el diagnóstico. Continúa en actividad 9. **NO:** Se rechaza la solicitud, se registra la justificación del rechazo en el sistema y se cierra el ticket informando al usuario. Fin del procedimiento (actividad 17).	Agente de Mesa de Ayuda	Asignación del según el nivel de atención	Aplicación Mesa de Ayuda link: http://mesadeayuda.ipes.gov.co/ Chat IPESencasa
9		El Agente asignado se desplaza al sitio o realiza atención remota según corresponda. Realiza el diagnóstico técnico y analiza si el incidente es un caso aislado o un patrón recurrente. Si durante el diagnóstico identifica indicios de evento de seguridad de la información, suspende la atención técnica y escala al Oficial de Seguridad de la Información conforme a la actividad 4. ¿Requiere escalar al siguiente nivel?	Agente de Mesa de Ayuda		Reporte aplicativo mesa de ayuda PA08-FO-008 Solicitud Recuperación de Información. FO-638 Lista Chequeo Para Cambio o Formateo De Equipos. PA08-FO-012 Formato Acompañamiento Tecnológico Eventos Institucionales

		SÍ: Continúa en actividad 10. **NO:** Continúa en actividad 12.			
10		El personal de segundo nivel ofrece soporte especializado. Si la solución implica una modificación en la infraestructura tecnológica, se suspende la solución operativa y se invoca el Procedimiento de Gestión de Cambios. Ningún cambio en infraestructura puede aplicarse sin aprobación formal previa. El Agente registra la justificación del escalamiento en el repositorio e informa al usuario el nuevo estado del ticket. (Referencia: NTC/ISO-IEC 27001:2022, control A.8.32 Gestión de cambios)	Agente de Mesa de Ayuda Segundo Nivel o Tercer Nivel		Aplicación Mesa de Ayuda link: http://mesadeayuda.ipes.gov.co/
11		El especialista o proveedor (tercer nivel) revisa y atiende el requerimiento. **SÍ se soluciona:** Documenta la solución y regresa a actividad 8 para verificación. **NO se soluciona:** Se registra el caso sin solución con la justificación correspondiente. Fin del procedimiento (actividad 16).	Agente de Mesa de Ayuda Segundo Nivel o Tercer Nivel		Aplicación Mesa de Ayuda link: http://mesadeayuda.ipes.gov.co
12		El Agente soluciona el requerimiento dentro de los tiempos establecidos	Agente de Mesa de Ayuda		Reporte aplicativo mesa de ayuda Reporte IPESencasa PA08-FO-008

	Solución del requerimiento	según la prioridad asignada. Al documentar la solución debe: Marcar el estado como "Resuelta". Indicar si la solución es definitiva o temporal. **Si es temporal:** postular el caso a Gestión de Problemas para investigación de causa raíz. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.27) **Si la solución es nueva y efectiva:** documentarla y solicitar su publicación en la Base de Conocimiento como lección aprendida.			Solicitud Recuperación de Información. FO-638 Lista Chequeo Para Cambio o Formateo De Equipos. PA08-FO-012 Formato Acompañamiento Tecnológico Eventos Institucionales
13	*Verifica y realiza pruebas* SI → 14 NO → 12	El Agente realiza las pruebas de funcionamiento necesarias para confirmar que la solución fue efectiva y que el servicio ha sido restablecido completamente. **SÍ funciona:** Continúa en actividad 14. **NO funciona:** Regresa a actividad 12.	Agente de Mesa de Ayuda	Prueba de funcionamiento de la solución	Reporte aplicativo mesa de ayuda Reporte IPESencasa PA08-FO-008 Solicitud Recuperación de Información. FO-638 Lista Chequeo Para Cambio o Formateo De Equipos. PA08-FO-012 Formato Acompañamiento Tecnológico Eventos Institucionales
14	Realizar encuesta para el cierre de la mesa de ayuda	El Agente notifica al usuario que el requerimiento ha sido atendido y le solicita confirmar la solución a través de la encuesta de satisfacción disponible en la plataforma. Se registra el estado del ticket como "Resuelta" en el repositorio. IPESencasa: se reporta por terminada la gestión al usuario por ese mismo canal.	Agente de Mesa de Ayuda	Finalización	Aplicación Mesa de Ayuda link: http://mesadeayuda.ipes.gov.co/ Chat IPESencasa

15	*Cierre por el Usuario y Cierre Administrativo*	El usuario recibe la notificación de solución y tiene 15 días calendario para confirmar o rechazar. **SÍ confirma:** El usuario diligencia la encuesta de satisfacción y el ticket pasa a estado "Cerrado". Fin del procedimiento (actividad 17). **NO responde:** El sistema o el Coordinador ejecuta el Cierre Administrativo, registrando la nota interna correspondiente. Fin del procedimiento (actividad 17).	Usuario / Agente de Mesa de Ayuda		
15	Cierre de Gestión Anual	Entre el 1 y el 15 de enero de cada año, el Coordinador de Mesa de Ayuda revisa los tickets abiertos del año anterior y ejecuta el Cierre de Gestión Anual para aquellos que al 31 de diciembre se encuentren en estado Asignado sin movimiento, En espera, o Resuelto sin cierre formal por el usuario, con excepción de los tickets de criticidad alta o asociados a proyectos en curso debidamente justificados. Los resultados del cierre anual se reportan al Oficial de Seguridad de la Información como insumo para el seguimiento del SGSPI. (Referencia: NTC/ISO-IEC 27001:2022, cláusula 9.1)	Coordinador de Mesa de ayuda		
16	**FIN**	Final del procedimiento			

7. PROTOCOLO DE ATENCIÓN DE INCIDENTES MAYORES O MASIVOS

- **Identificación y Declaración:**

  El Coordinador de Mesa de Ayuda o el Líder del proceso GIRT-SDAE son los únicos facultados para declarar un incidente masivo. La declaración procede cuando se cumple al menos uno de los siguientes criterios:

  - **Impacto extenso:** Afecta a la totalidad de los usuarios o a una sede completa de la entidad.
  - **Criticidad:** El servicio afectado es vital para la misión institucional del IPES.
  - **Recurrencia masiva:** Se detectan múltiples tickets reportando la misma falla en un periodo corto de tiempo.

  Una vez declarado el incidente masivo, se notifica de forma inmediata al Oficial de Seguridad de la Información para determinar si el evento tiene connotaciones de seguridad de la información que requieran activar el procedimiento de Gestión de Incidentes de Seguridad. (Referencia: NTC/ISO-IEC 27001:2022, controles A.5.24 y A.5.25)

- **Registro y Vinculación**

  - Se crea un Ticket Padre (Incidente Maestro) donde se centraliza toda la información técnica del incidente.
  - Todos los tickets individuales reportados por usuarios se vinculan al Ticket Padre, permitiendo su cierre simultáneo al resolver la falla principal.
  - El Ticket Padre debe contener como mínimo: descripción del incidente, servicios afectados, usuarios impactados, hora de declaración y responsable asignado.

- **Notificación y Comunicación**

  - Se publica un comunicado masivo a los usuarios informando que se presenta una falla general y que se está trabajando en su resolución. Esto evita la creación de nuevos tickets duplicados.
  - El comunicado debe incluir el canal de seguimiento y el tiempo estimado de resolución si se dispone de esa información.
  - Las actualizaciones de estado se comunican cada hora o cuando haya un cambio significativo en la gestión del incidente. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.26 Respuesta a incidentes de seguridad de la información)

- **Atención Prioritaria**

- Se asigna prioridad Crítica o Alta de forma inmediata, con los tiempos de respuesta definidos en las Condiciones Generales de este procedimiento.
- Se conforma un equipo de atención prioritaria (enjambre) con los especialistas necesarios.
- Si se requiere, el Especialista de Nivel 2 escala al Proveedor (Nivel 3) sin esperar los tiempos habituales de diagnóstico.
- Si la solución implica modificaciones en la infraestructura, se invoca el Procedimiento de Gestión de Cambios con aprobación de emergencia. (Referencia: NTC/ISO-IEC 27001:2022, control A.8.32)

- **Cierre Masivo y Reporte**

  - Una vez restablecido el servicio, se documenta la solución en el Ticket Padre y se replica automáticamente a todos los tickets hijos vinculados.
  - Se genera un Informe de Causa Raíz dentro de los 5 días hábiles siguientes al cierre del incidente.
  - Si la causa raíz no puede eliminarse de forma inmediata, el caso se postula a Gestión de Problemas para su tratamiento definitivo.
  - El informe final se remite al Oficial de Seguridad de la Información como insumo para el seguimiento del SGSPI y la mejora continua. (Referencia: NTC/ISO-IEC 27001:2022, controles A.5.27 y A.5.29)

8. ARTICULACIÓN CON OTROS PROCESOS

El presente procedimiento se articula con los siguientes procesos institucionales y del SGSPI cuando la naturaleza de la solicitud excede el alcance del soporte técnico estándar o requiere controles adicionales:

- **Gestión de Incidentes de Seguridad de la Información**

  Cuando el Agente identifica en cualquier actividad del flujo indicios de un evento de seguridad de la información, activa el procedimiento de Gestión de Incidentes de Seguridad, transfiriendo el control al Oficial de Seguridad de la Información. (Referencia: NTC/ISO-IEC 27001:2022, controles A.5.24, A.5.25 y A.5.26)

- **Gestión de Cambios**

  Cuando la solución a un requerimiento implica una modificación en la infraestructura tecnológica, se suspende la atención operativa y se invoca el Procedimiento de Gestión de Cambios. Ningún cambio puede implementarse sin aprobación formal previa. (Referencia: NTC/ISO-IEC 27001:2022, control A.8.32)

- **Gestión de Problemas**

  Cuando un incidente se resuelve con una solución temporal o se detecta un patrón de recurrencia, el caso se postula al proceso de Gestión de Problemas para la investigación y eliminación de la causa raíz. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.27

- **Gestión de Activos de Información**

Cuando durante la atención de un ticket se identifica un activo de información no registrado en el inventario, o se detecta una modificación no autorizada en un activo existente, se notifica al Oficial de Seguridad de la Información para su registro o actualización en el inventario del SGSPI. (Referencia: NTC/ISO-IEC 27001:2022, controles A.5.9 y A.5.10)

- **Gestión de Continuidad del Negocio**

  Cuando un incidente masivo afecta servicios críticos de la entidad, el Coordinador de Mesa de Ayuda notifica al Oficial de Seguridad de la Información para evaluar la activación del Plan de Continuidad del Negocio o el Plan de Contingencia institucional. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.29)

- **Gestión de Proveedores**

  Cuando el requerimiento requiere escalamiento a soporte especializado externo (tercer nivel), aplican los acuerdos de nivel de servicio y los requisitos de seguridad de la información establecidos contractualmente con el proveedor. (Referencia: NTC/ISO-IEC 27001:2022, control A.5.19)

9. DOCUMENTOS ASOCIADOS

- PA08-FO-008 Solicitud Recuperación de Información.
- FO-638 Lista Chequeo Para Cambio o Formateo De Equipos.
- PA08-FO-012 Formato Acompañamiento Tecnológico Eventos Institucionales

10. MARCO NORMATIVO

- **Normativa colombiana**

  - **Ley 1581 de 2012:** Disposiciones generales para la protección de datos personales. Aplicable al tratamiento de información personal de usuarios y funcionarios gestionada a través de los tickets de la Mesa de Ayuda.
  - **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector TIC. Marco fundamental para la Política de Seguridad Digital y Gestión de Tecnología en el Estado colombiano.
  - **Decreto 767 de 2022:** Actualiza los lineamientos de aplicación de la Política de Gobierno Digital, crucial para la estrategia de TI de las entidades públicas.
  - **Directiva Presidencial 02 de 2022:** Lineamientos para la Gestión de Incidentes de Seguridad Digital en entidades del Estado. Aplicable directamente al protocolo de escalamiento al Oficial de Seguridad de la Información.
  - **Resolución 020 de 2021 del IPES:** Por la cual se actualiza el Plan de Seguridad y Privacidad de la Información y el Plan Estratégico de Riesgos de Seguridad y Privacidad de la Información del IPES.

- **Normas técnicas distritales**

  - **NTD SIG 001:2011:** Norma Técnica Distrital del Sistema Integrado de Gestión para

las Entidades y Organismos Distritales.

- **Estándares internacionales**
  - **NTC/ISO-IEC 27001:2022:** Seguridad de la información, ciberseguridad y protección de la privacidad, Sistemas de Gestión de Seguridad de la Información.
- **Lineamientos MinTIC**
  - **MSPI v5.0:** Modelo de Seguridad y Privacidad de la Información de MinTIC, Marco de referencia obligatorio para la implementación del SGSPI en entidades del Estado colombiano. Este procedimiento se enmarca en la Fase 3 (Implementación) del MSPI.

11. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
01	10/01/2018		Elaboración del documento.
02	30/11/2021	Descripción del procedimiento	Actualización del procedimiento Descripción del procedimiento
03	01/12/21	Definiciones y abreviaturas Condiciones generales Descripción del procedimiento Documentos asociados	Concepto mesa de ayuda Reportes Puntos de control y registro Código formato
04	24/05/22	Título procedimiento Definiciones y abreviaturas Descripción del procedimiento	Se delimita procedimiento Definición y conceptos de Estados de ticket ajustados a la nueva aplicación de mesa de ayuda Cambio en registro nuevo link mesa de ayuda
05	15/06/22	Título procedimiento Responsables: Usuarios y Coordinador mesa de ayuda Definiciones y abreviaturas Descripción del procedimiento	Se delimita procedimiento Se adiciona el chat de IPESencasa Definición y conceptos de Estados de ticket ajustados a la nueva aplicación de mesa de ayuda. IPESencasa Cambio en registro nuevo link mesa de ayuda y Chat IPESencasa
06	25/05/26	Objetivo, Alcance, Responsables, Definiciones, Condiciones Generales, Descripción del procedimiento, Protocolo de Incidentes Mayores, Articulación con otros procesos, Marco Normativo	Incorporación de referencias a la NTC/ISO-IEC 27001:2022 y sus controles del Anexo A en todas las secciones del documento. Ajuste del Objetivo y Alcance para alinear con el SGSPI y el MSPI v5.0. Ampliación de Responsables con controles ISO aplicables a cada rol. Nuevas definiciones:

			evento e incidente de seguridad, Gestión de Problemas, Base de Conocimiento, Error Conocido, Cierre Administrativo, Cierre de Gestión Anual, SGSPI, MSPI. Nuevas condiciones generales: SLAs por nivel de prioridad, tratamiento de información de tickets conforme al SGSPI, escalamiento obligatorio de eventos de seguridad. Separación de la actividad 3 en dos decisiones independientes (clasificación Incidente/Petición y detección de evento de seguridad). Fortalecimiento del Protocolo de Incidentes Mayores con estructura de 5 fases. Articulación formal con 6 procesos del SGSPI. Marco Normativo reorganizado por categorías con tabla de controles ISO/IEC 27001:2022 aplicables.