IDENTIFICACIÓN DEL PROCEDIMIENTO	
OBJETIVO:	Definir los mecanismos de detección y gestión oportuna de los incidentes o problemas de TI, a través de la mesa de servicio de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Para anticipar, resolver y documentar eventos no planificados en la Entidad, que afecten la operación de las soluciones tecnológicas, los principios de confidencialidad, integridad y disponibilidad de la información.
ALCANCE:	Inicia con la validación y registro del incidente, continúa con la gestión del incidente de seguridad y/o recuperación del servicio, la definición y gestión de problemas, y finaliza con el cierre en la herramienta de gestión.
NORMAS ASOCIADAS:	Ver Normas asociados del documento en https://portalmipg.scj.gov.co

DEFINICIONES
Activo de información: (Según el Modelo de Seguridad y Privacidad de la Información MSPI): En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
Clasificación: Grado de severidad de un incidente de Seguridad de la Información.
Confidencialidad: Propiedad que garantiza que la información no sea accedida, ni sea revelada a personas, entidades o procesos no autorizados.
Diagnóstico: Estudio que se le realiza a cada caso, a fin de establecer el procedimiento a seguir para dar solución.
Disponibilidad: Principio que garantiza que la información esté accesible y utilizable cuando lo requieran las personas, entidades o procesos autorizados.
Escalar: Transferir un caso a otro especialista de la competencia que brinde el soporte adecuado.
Evento de seguridad de la información: Situación detectada en un sistema, servicio o red que indica una posible violación de la Política de Seguridad de la Información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información de la entidad.
Especialista: Profesional a quien se le designan los casos de mayor complejidad para diagnóstico y solución de acuerdo con su especialidad.

DEFINICIONES
Herramienta de gestión: Herramienta donde se documenta la información correspondiente a un incidente de seguridad de la información.
Incidente: Es toda interrupción o reducción de la calidad no planificada del servicio. La cual afecta a uno, varios o a todos los usuarios de la Entidad. Dichas fallas pueden ser reportadas por los usuarios, el equipo del servicio o por alguna herramienta de monitorización de eventos.
Incidente de seguridad de la información: Amenaza inminente a la Política de Seguridad de la Información implícita o explícita. Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del Entidad y amenazar la seguridad de la información, tales como, un acceso no autorizado o intento del mismo; uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos.
Incidente Masivo: Un evento que genera la interrupción o reducción de la calidad no planificada de un servicio misional o de apoyo que afecta a varios o todos los usuarios de la Entidad.
Incidente padre: Se determina cuando un incidente puede generar varios tickets sobre la misma incidencia. Está determinado por la actividad que afecte, crítica o no crítica, y el porcentaje de usuarios afectados.
Información: Conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia entidad o de fuentes externas) o de la fecha de elaboración.
Infraestructura: Todo el hardware, el software, las redes y las instalaciones que hacen parte de las soluciones tecnológicas de la Entidad.
Integridad: Principio que garantiza que la información sea exacta, coherente y completa desde su creación hasta su destrucción.
Problema: Se entenderá como problema cuando se presentan uno o varios incidentes en los que se desconoce su causa raíz o cuando se presenta un incidente mayor en el cual se desconoce la causa que lo genero.
Seguridad de la información: Consiste en resguardar y proteger la Confidencialidad, Integridad y Disponibilidad de la información que maneja la Entidad, mediante un conjunto de medidas preventivas y correctivas.
Ticket: Número de Registro que se informa a usuario solicitante de un servicio y al agente que atenderá dicho servicio, el cual avisa que hay una gestión en curso.

DOCUMENTOS DE REFERENCIA	
EXTERNOS	**INTERNOS**
	• Manual de Seguridad y Privacidad de la Información MA-GT-01 • Procedimiento de Gestión de Requerimientos de TI PD-GT-1 • Procedimiento de Gestión de Cambios PD-GT-2

POLITICAS DE OPERACIÓN

CONDICIONES GENERALES

1. Todo requerimiento de servicio tecnológico ingresa por la mesa de servicio por medio de los canales habilitados, donde se validará si es una solicitud o un incidente de acuerdo con lo definido en el procedimiento Gestión de Requerimientos de TI PD-GT-1.

2. La Mesa de Servicio identifica el requerimiento y determina si es un Incidente o Incidente de seguridad de la Información y de acuerdo con eso se realizará el respectivo tratamiento.

3. Todo requerimiento debe contener como mínimo la siguiente información básica:
   - Nombre completo del usuario
   - Dependencia
   - Ubicación
   - Correo Electrónico
   - Descripción clara del evento o incidente que presenta
   - Placa del equipo de cómputo

4. En los casos donde la información básica no está completa y/o requiera ampliarse, se comunicará al usuario por el mismo medio en que se recibió para que reporte la información faltante. En caso de no recibir respuesta en los próximos dos (2) días hábiles por parte del usuario, incidente pasará a un estado completado.

POLITICAS DE OPERACIÓN

5. Todo incidente reportado a la mesa de servicio tiene asociado un número de ticket generado por la herramienta de gestión que permite su seguimiento y trazabilidad. Dicho número es informado a través de notificación automática al usuario por correo electrónico para realizar el seguimiento a la atención del incidente.

6. La mesa de servicio de la Secretaría Distrital de Seguridad Convivencia y Justicia está conformada por los siguientes niveles de atención:

NIVEL	ROL	ALCANCE
1	Agente de Mesa	Punto de contacto con el usuario, se encarga de resolver los incidentes simples y de forma remota, así como de filtrar los tickets de soporte y escalar a otros niveles que son más complejos.
2	Agente de Sitio Agente Sistemas de Información. Agente de Servicios Tecnologicos.	Grupo de técnicos de soporte que se encargan de realizar el diagnóstico y resolver los incidentes más complicados a nivel de hardware o software que necesitan de un cierto grado de conocimiento avanzado.
3	Profesional de Servicios Tecnológicos e Infraestructura Profesional de Sistemas de Información Profesional de Seguridad de la Información Profesional de Uso y Apropiación	Grupo de profesionales especialistas que tiene conocimientos específicos para diagnosticar y resolver los incidentes más complejos. Se encargan de atender los incidentes que no han podido ser resueltos por los niveles anteriores.
4	Proveedor externo prestador del servicio tecnológico	Grupo de proveedores que prestan servicios a la Entidad, se encargan de resolver los incidentes más complejos que no pueden ser solucionados directamente por los profesionales de la Dirección de Tecnologías y Sistemas de la Información.

Tabla 1. Niveles de atención mesa de servicio.

7. Todo reporte de un evento de seguridad de la información será valorado por la mesa de servicio, teniendo en cuenta la siguiente clasificación al momento de realizar la asignación del caso:

   a. **Acceso no autorizado:** Todas aquellas actividades en las que sin autorización específica o que no se encuentre dentro de las funciones, se obtiene acceso lógico o físico a un recurso o activo de información (equipo, software, red, etc.) sobre el cual no tiene permisos.

POLITICAS DE OPERACIÓN

b. **Código Malicioso:** En esta clasificación están los incidentes en donde software como virus, troyanos, RAT, Rootkit, Ransomware, gusanos y demás formas de código malicioso infectan exitosamente un recurso tecnológico de la Entidad, de tal forma que pueda corromper, alterar, modificar y/o destruir la información.

c. **Denegación de servicio:** Esta clasificación incluye los eventos que ocasionan pérdida de un servicio y la falla no es atribuible a problemas de operación normal, es decir, cuando un atacante (interno o externo a la entidad) impide a los usuarios el uso autorizado a la información o activos de información de la Entidad.

d. **Uso inapropiado de recursos tecnológicos:** Esta clasificación agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso. Comprende:

- Utilización del correo electrónico para temas como: Spam, Phishing, Hoax, cadenas de correo, ingeniería social.
- Utilización del correo electrónico y/o Internet para temas como: Contenido pornográfico, divulgación de información reservada o propia de la Entidad sin debida autorización.
- Utilización de la red para temas como: Realización de pruebas de intrusión, Scan, o vulnerabilidades, sin autorización.
- Robo, fuga, espionaje o perdida de información: Medios externos de almacenamiento y/o material impreso.

8. Todo incidente de seguridad con la información, debe ser atendido, analizado, documentado y reportado por parte del personal encargado y establecido para tal fin por parte de la Dirección de Tecnologías y Sistemas de la Información, es deber de los usuarios finales realizar los reportes sobre eventos de seguridad de la información e informar si identifican debilidades relacionadas, para lo cual deben generar los casos con los respectivos tickets de soporte a mesa de servicio para dar atención referente a seguridad de la información. Se verificará y hará seguimiento por parte del profesional de seguridad de la Información de los eventos e incidentes de seguridad de la información reportados, velando que sean comunicados y atendidos oportunamente.

9. Para la gestión de incidentes de seguridad de la información deberán tipificarse por prioridad de acuerdo con la información de la siguiente tabla:

PRIORIDAD	Descripción
Alto	El incidente alto tiene un impacto considerable (afectación total a la confidencialidad, disponibilidad o integridad) en la información y se considera crítica para la misión de la SDSCJ, esto incluye información en diferentes medios y/o sistemas críticos.

POLITICAS DE OPERACIÓN

	Estos incidentes implican una grave violación de seguridad o pueden dañar la confianza en la administración pública (pérdida de imagen institucional), o podrían afectar la seguridad física de las personas, causar una pérdida importante de recursos de la SDSCJ.
Medio	Se clasifican con este nivel aquellos eventos que puedan afectar o está afectando a los activos de información de la SDSCJ, con una valoración considerable en la triada de la información (confidencialidad, disponibilidad o integridad), lo cual puede resultar en la pérdida directa de información para la SDSCJ.
Bajo	Se clasifican con este nivel aquellos eventos que puedan ser una amenaza que afecta o está afectando a activos de información de la SDSCJ con una valoración de impacto limitado en la triada de la información (confidencialidad, disponibilidad o integridad). Su impacto debe ser nulo o insignificante para la SDSCJ.

Tabla 2. Nivel de Prioridad.

10. En caso de que el incidente de seguridad de la información se considere de prioridad alta, el profesional de seguridad de la información de la SDSCJ deberá proponer el equipo que participará en el tratamiento del incidente y este será aprobado por el Director de Tecnologías y Sistemas de la Información o quien delegue.

11. Los incidentes de seguridad de la información con prioridad Media y Baja estarán liderados por el profesional de seguridad de la información de la SDSCJ.

12. Se debe actuar para reducir los efectos reales y potenciales de un incidente de seguridad de la información, en pro de mitigar su impacto en la Entidad. Así mismo, tener en cuenta que la respuesta exacta dependerá de la naturaleza del incidente al que se enfrente. No obstante, se contemplarán las siguientes prioridades como punto de partida:
    - Proteger los activos de información pública clasificada y pública reservada, siendo los más relevantes para la Entidad los cuales deben contar con controles robustos con el fin de preservar la Confidencialidad, Integridad y Disponibilidad.
    - Proteger otra información relevante (propiedad intelectual o del ámbito directivo), dentro del entorno laboral hay otra información que también puede ser valiosa y debe ser protegida donde se dará prioridad en primer lugar a los datos más valiosos antes de pasar a otros de baja prioridad.

POLITICAS DE OPERACIÓN

- Proteger el hardware y software de la SDSCJ, lo que implica protegerlos contra pérdida y/o modificación de los archivos del sistema y contra daños físicos al hardware. Los daños en los sistemas pueden tener como consecuencia un alto tiempo de inactividad.
- Minimizar la indisponibilidad de los servicios informáticos, aunque el tiempo de producción sea muy importante en la mayoría de los entornos, el hecho de mantener los sistemas en funcionamiento durante un incidente puede tener como consecuencia problemas más graves en el futuro. Por este motivo, la minimización de la interrupción de los recursos informáticos debe ser generalmente una prioridad relativamente baja.

13. Existen varias medidas que se pueden tomar para contener el daño y minimizar el riesgo en el entorno, como mínimo, se debe llevar a cabo las siguientes acciones:
    - Evitar que los posibles atacantes conozcan las actividades que se adelanten dentro del tratamiento.
    - Comparar el impacto de dejar sin conexión los sistemas en peligro y los sistemas relacionados con el riesgo de continuar funcionando.
    - Determinar los puntos de acceso usados por posibles atacantes e implementar las medidas adecuadas para evitar futuros accesos.
    - Asegurar el cambio de las contraseñas: locales, de las cuentas de servicio y administrativas en todo el entorno.

14. Teniendo en cuenta que el tratamiento y la respuesta de cada incidente de seguridad de información depende de su naturaleza, se tendrá una respuesta diferente de acuerdo con los siguientes parámetros:

    - Una solución efectiva: La gestión del incidente logró remediar los servicios o activos afectados por el incidente.
    - Una solución que relaciona un cambio: La gestión del incidente logró remediar los servicios o activos afectados por el incidente, no obstante, el incidente puede replicarse, siendo necesario ejecutar un cambio para evitar reincidencia.
    - La valoración del incidente de seguridad de la información se realizará por el gestor de incidentes de seguridad de la SDSCJ para determinar los impactos y/o costos que afectan a la SDSCJ. El daño y los costos del incidente constituirán una prueba importante y necesaria si decide emprender acciones legales. Entre ellos, se pueden contar los siguientes:
    - Consecuencias asociadas a la pérdida de información tipificada como pública reservada.
    - Consecuencias legales.
    - Consecuencias laborales por el análisis de las infracciones, la reinstalación del software y la recuperación de datos.
    - Consecuencias en el tiempo de inactividad de los sistemas (por ejemplo, pérdida de productividad de los funcionarios y/o contratistas, sustitución del hardware, del software y de otras propiedades).

POLITICAS DE OPERACIÓN

- Consecuencias relacionadas con la reparación y posible actualización de las medidas de seguridad físicas dañadas o ineficaces (cierres, paredes, cajas, etc.).
- Consecuencias relacionadas con la imagen del proceso afectado por un incidente. Otros daños derivados, como la pérdida de la reputación o de la confianza de la ciudadanía.
- Valoración del impacto del incidente de seguridad de la información.

15. La valoración del incidente de seguridad de la información se realizará por el profesional de seguridad de la información de la SDSCJ para determinar los impactos y/o costos que afectan a la SDSCJ. El daño y los costos del incidente constituirán una prueba importante y necesaria si decide emprender acciones legales. Entre ellos, se pueden contar los siguientes:

- Consecuencias asociadas a la pérdida de información tipificada como pública reservada.
- Consecuencias legales.
- Consecuencias laborales por el análisis de las infracciones, la reinstalación del software y la recuperación de datos.
- Consecuencias en el tiempo de inactividad de los sistemas (por ejemplo, pérdida de productividad de los funcionarios y/o contratistas, sustitución del hardware, del software y de otras propiedades).
- Consecuencias relacionadas con la reparación y posible actualización de las medidas de seguridad físicas dañadas o ineficaces (cierres, paredes, cajas, etc.).

16. En el evento de que algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Entidad, haya sido vulnerado o comprometido, el profesional de seguridad debe reportar al ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) por medio de correo electrónico a: contacto@colcert.gov.co, de acuerdo con el P*rotocolo de Gestión de Incidentes de la Información para el Distrito Capital.*

17. Criterios para la definición de un problema:

- Incidentes con causa raíz desconocida: Incidentes que se presentan en la operación los cuales pueden ser solucionados restableciendo el servicio, pero se desconoce su causa raíz por lo que se puede volver a presentar.
- Recurrencia de incidentes: Cuando se presentan repetidos incidentes que generan la misma afectación de servicio.
- Incidente mayor: Consecuencia de incidente de gran impacto.

18. Categorías de definición de problemas:
- Análisis de tendencias: Gestión proactiva de problemas en la que se revisan los registros de incidentes para encontrar patrones o

POLITICAS DE OPERACIÓN
tendencias que pueden indicar la presencia de errores en las soluciones tecnológicas de la Entidad. • Incidente mayor: Consecuencia de incidente de gran impacto • Postulado por la operación: En la mayoría de los casos es una gestión reactiva, por el registro de un incidente del cual no se conozca su causa raíz o de problemas ya materializados en el servicio de TI. 19. En la ejecución del procedimiento se contempla lo establecido en el Manual de Seguridad y Privacidad de la Información, MA-GT-01

DESCRIPCIÓN DEL PROCEDIMIENTO					
ID	**AC***	**Actividad**	**DESCRIPCIÓN (CÓMO)**	**Responsable**	**Salida (Registro)**
1	X	Validar y registrar incidente	Verifica que el requerimiento del usuario cuente con la información básica para registrar el incidente en la herramienta de gestión. Tener en cuenta lo establecido en la política de operación N. 3 del procedimiento.	Técnico - Agente mesa de Servicio Nivel 1 / Dirección de Tecnología y Sistemas de la Información.	Registro del caso en la herramienta de gestión.
		¿Cumple con los requisitos mínimos?	**SI:** Continúa en la siguiente actividad. **NO:** Solicita información al usuario.		
2		Categorizar el Incidente	Según el tipo de evento se categoriza en la herramienta de gestión de acuerdo con el catálogo de servicios. **Nota.** Si se trata de un incidente masivo, validar si ya existe un incidente padre para relacionarlo. Si aún no está registrado el caso padre, se debe marcar este incidente como padre, para relacionar los demás que se generen.	Técnico - Agente Mesa de Servicio Nivel 1 / Dirección de Tecnología y Sistemas de la Información.	Incidente categorizado en la herramienta de gestión.

3		Clasificar y Asignar	Según el tipo de incidente se clasifica en la herramienta de gestión de acuerdo con el catálogo de servicios, y se asigna al responsable correspondiente.	Técnico - Agente Mesa de Servicio Nivel 1 / Dirección de Tecnología y Sistemas de la Información.	Incidente registrado y actualizado en la herramienta de mesa de servicio
		¿Es un posible incidente de seguridad?	**SI:** Continúa en la actividad 6 **NO:** Continúa en la siguiente actividad.		
4		Diagnosticar Incidente	Realiza un diagnóstico inicial del Incidente, en donde se analiza criticidad del servicio afectado, origen de la falla, prioridad de solución y posibilidades de gestión.	Técnico - Agente Mesa de Servicio Nivel 1 / Dirección de Tecnología y Sistemas de la Información.	Incidente actualizado en la herramienta de gestión.
5		Resolver Incidente	De acuerdo con el diagnóstico inicial se realiza el soporte de primer nivel, en cual se gestiona el incidente en forma remota siempre que por la naturaleza del incidente sea posible. Si la solución del incidente no está al alcance del primer nivel, escala al siguiente de acuerdo con los niveles registrados en las políticas de operación, para así dar solución y restablecer el servicio. Existen casos en que para aplicar las actividades que permitan restablecer el servicio es necesario realizar un cambio, por lo que se debe continuar el procedimiento de Gestión de cambios PD-GT-2. **Continua en actividad 11**	Agentes de Mesa/ Profesionales de Infraestructura, Servicios Tecnológicos, Sistemas de Información, Seguridad de la Información, Uso y Apropiación, Proveedores externos prestadores de servicios. / Dirección de Tecnología y Sistemas de la Información.	Incidente actualizado en la herramienta de gestión, con la gestión y escalamiento realizado.

6	X	Validar incidente de seguridad de la información.	Valida que el evento reportado corresponda a un incidente de seguridad de la información, para esto el Profesional de Seguridad de la Información realizará una segunda validación de acuerdo con las condiciones del caso reportado. Se actualiza la herramienta de gestión	Profesional de Seguridad de la Información / Dirección de Tecnología y Sistemas de la Información.	Incidente actualizado en la herramienta de gestión.
7		Clasificar y tipificar la prioridad del incidente de seguridad de la información	Clasifica y tipifica el incidente de acuerdo con las políticas de operación. Se actualiza la herramienta de gestión	Profesional de Seguridad de la Información / Dirección de Tecnología y Sistemas de la Información.	Incidente actualizado en la herramienta de gestión.
8		Establecer estrategia de tratamiento del incidente de seguridad.	Definir la estrategia y los recursos (económicos, humano, tiempo) requeridos para el tratamiento del incidente de seguridad con el profesional o profesionales, de acuerdo a la prioridad y a lo definido en las políticas de operación respectivas. Si la respuesta o tratamiento del incidente requiere ejecutar un control de cambio, se debe diligenciar el formato de gestión de cambios F-GT-278 y seguir el procedimiento de Gestión de cambios de TIC PD-GT-2.	Director de Tecnologías y Sistemas de la Información. / Profesional de Seguridad de la Información. / Dirección de Tecnología y Sistemas de la Información.	Incidente actualizado en la herramienta de gestión. Gestión de cambios (cuando se requiera)
9		Recopilar y documentar evidencias	Documenta la información necesaria del incidente y recopilar las evidencias producto de la investigación del incidente. Se actualiza la herramienta de gestión	Profesional de Seguridad de la Información / Dirección de Tecnología y Sistemas de la Información.	Incidente actualizado en la herramienta de gestión.
10		Resolver el incidente de seguridad de la información	Da la respectiva solución al incidente luego de la gestión realizada por el Profesional de Seguridad de la Información y/o equipo de trabajo asignado. Se actualiza la herramienta de gestión	Profesional de Seguridad de la Información /	Incidente actualizado en la herramienta de gestión.

				Dirección de Tecnología y Sistemas de la Información.	
11		Documentar en herramienta y completar caso	Documenta detalladamente cómo se gestionó el incidente y cuáles fueron los resultados en la herramienta de gestión. Posterior se actualiza el estado del caso como resuelto, automáticamente la herramienta envía a través de correo electrónico la notificación del caso como completado y la encuesta de satisfacción para ser diligenciada por el usuario.	Agentes de Mesa/ Profesionales de Infraestructura, Servicios Tecnológicos, Sistemas de Información, Seguridad de la Información, Uso y Apropiación, Proveedores externos prestadores de servicios. / Dirección de Tecnología y Sistemas de la Información.	Incidente en la herramienta de gestión en estado completado. Notificación por correo para el diligenciamiento de la encuesta de satisfacción.
12		Identificar y analizar posible problema	Una vez gestionados los incidentes, se podrán identificar posibles problemas así: 1.El profesional asignado en resolver el incidente se encargará de identificar y reportar, si el evento presentado es un posible candidato para gestionarse como problema. 2.El coordinador de la mesa de servicios, evaluando el comportamiento y el historial de incidentes registrados en la herramienta de gestión, puede reportar un evento como posible candidato a problema. Se realiza evaluación de los criterios definidos en las políticas de operación con el fin de definir si se le da tratamiento como problema.	Agentes de Mesa/ Profesionales de Infraestructura, Servicios Tecnológicos, Sistemas de Información, Seguridad de la Información, Uso y Apropiación, Proveedores externos prestadores de servicios. / Dirección de Tecnología y Sistemas de la Información.	Posible problema.

		¿Se trata de un problema?	**SI:** Continúa en la siguiente actividad **NO:** Fin de procedimiento		
13		Registrar problema en herramienta de gestión	Registra el problema en la herramienta de gestión. Dependiendo de la criticidad del servicio afectado y del impacto causado, se le debe asignar una prioridad al Problema.	Técnico - Agente Mesa de Servicio / Dirección de Tecnología y Sistemas de la Información.	Problema registrado en la herramienta
14		Convocar reunión para gestionar el problema	Convoca al equipo de trabajo de especialistas, lideres o partes interesadas para la gestión del problema registrado en la herramienta de gestión.	Profesional responsable del problema / Dirección de Tecnología y Sistemas de la Información.	Soporte de Convocatoria de reunión cargado en la herramienta.
15		Investigar y diagnosticar causa raíz	Realiza reunión donde se analiza el problema desde los diferentes puntos de vista de cada profesional para entender el servicio o infraestructura asociadas, realiza una lluvia de ideas sobre las posibles causas y la posible solución. Realiza investigación de la causa raíz en los sistemas afectados. Se deja registro en el formato Acta de reunión F-FI-1380 Esta actividad puede requerir investigación de la causa por medio de la apertura de casos con proveedores, hacer los escalamientos funcionales y/o jerárquicos necesarios.	Profesional responsable del problema/ Dirección de Tecnología y Sistemas de la Información.	Problema analizado Acta de Reunión Problema documentado en la herramienta de gestión cargando acta de reunión
16		Definir Solución del problema	Define y planifica con el equipo de trabajo las actividades que se ejecutarán para abordar la solución definitiva y/o aquellas que sean preventivas o de mejora y documentarlo en la herramienta de gestión.	Profesional responsable del problema/ Dirección de Tecnología y Sistemas de la Información.	Problema documentado en la herramienta de gestión con la solución a implementar.

17		Implementar solución	Implementa y gestiona la solución definida de acuerdo con los tiempos, actividades y objetivos planeados para alcanzar la solución. Si la solución del problema requiere ejecutar un control de cambio, se debe seguir el procedimiento de Gestión de cambios de TIC PD-GT-2. Se actualiza la herramienta de Gestión	Profesional responsable del problema/ Dirección de Tecnología y Sistemas de la Información.	Problema actualizado en la herramienta de gestión
		¿Resolvió el problema?	**SI:** Continúa en la siguiente actividad. **NO:** Regresa a la actividad número 15.		
18		Cerrar problema	Verifica que el problema este correctamente documentado en la herramienta de gestión y proceder al cierre de este.	Profesional responsable del problema/ Dirección de Tecnología y Sistemas de la Información.	Problema cerrado en la herramienta de gestión.
			FIN DEL PROCEDIMIENTO		

*AC: marque con una X si la actividad corresponde a una actividad de control.

Elaboró: Diego Mauricio Usme Gonzalez – Contratista SDSCJ

Francisco Vargas Moncada– Profesional Universitario 219-18

Revisó: Jairo Alonso Bohórquez Blanco – Profesional Especializado 222-27

Jorge Eliecer Velásquez Perilla – Contratista SDSCJ.

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - https://portalmipg.scj.gov.co