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 para contención del incidente de seguridad y/o recuperación del servicio, la definición y gestión de problemas, y finaliza con el análisis de satisfacción del servicio prestado.

NORMATIVIDAD
Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. **Ley 1581 de 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales. **Ley 1712 de 2014**: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública y Nacional y se dictan otras disposiciones. **Decreto 1008 de 2018**: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y Comunicaciones **Resolución 0025 de 2021**: Por la cual se adopta la Política de Seguridad y Privacidad de la Información **CONPES 3701 de 2011**: Lineamientos de política para Ciberseguridad y Ciberdefensa **CONPES 3854 de 2016**: Política Nacional de Seguridad Digital.

DOCUMENTOS DE REFERENCIA	
EXTERNOS	**INTERNOS**
• Norma Técnica NTC-ISO-IEC 27001	• Política de Seguridad y Privacidad de la Información PO-GT-1 • Manual de Seguridad y Privacidad de la Información MA-GT-01 • Procedimiento de Requerimientos de TI PD-GT-1

	• Procedimiento de gestión de cambios PD-GT-2

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. **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

DEFINICIONES

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 critica: Todo el hardware, el software, las redes y las instalaciones que hacen parte de las soluciones tecnológicas misionales 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.

POLÍTICAS 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 Gestion 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 informacion básica:

a. Nombre completo del usuario
b. Dependencia
c. Ubicación
d. Correo Electrónico
e. Descripción clara del evento o incidente que presenta
f. 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.

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 las siguientes consideraciones al momento de realizar la asignación del caso:
   - Relacionar el evento con una afectación de la integridad, disponibilidad y confidencialidad de la información.
   - Reunir información básica (Lugar, tipo de información, datos de contacto de la persona que reporta) que llevó a determinar que es un posible incidente de seguridad de la información, información que podrá ser utilizada en la investigación y/o para empezar a contener los daños y minimizar el riesgo.

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 los 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, de acuerdo con lo establecido en el numeral 5.12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN del manual de Seguridad y Privacidad de la Información, MA-GT-1

9. Un incidente de seguridad de la información podrá ser clasificado de acuerdo a la siguiente tabla:

INCIDENTE	DESCRIPCIÓN DE LA CAUSA RAIZ	EJEMPLO
Desastre Natural	Causa Natural	Terremotos, erupciones volcánicas, inundaciones huracanes, tormentas eléctricas, incendio forestal, tsunami, derrumbes.
Daño Físico	Debido a acciones físicas accidentadas en las instalaciones de la SDSCJ.	Incendio, agua, contaminación, destrucción de equipos, destrucción de medios, sustracción de equipos, sustracción de medios.
Fallas de Infraestructura	Generado por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información y los servicios sociales.	Fallas en la alimentación eléctrica, en las redes, en el aire acondicionado, fallas de hardware, etc.

tecnológica		
Malware	Causas asociadas de programas maliciosos creados y divulgados en forma intencional	Virus informáticos, gusanos de red, troyanos, botnets, entre otros.

Tabla 2. Clasificación de Incidentes de Seguridad.

10. Para la gestión de incidentes de seguridad de la información deberán tipificarse por prioridad de acuerdo con su impacto y urgencia, con relación a la información registrada en las siguientes tablas:

PRIORIDAD	ALCANCE	DESCRIPCIÓN
ALTO	El incidente de seguridad puede afectar la continuidad de la prestación de los servicios misionales y de apoyo del proceso de gestión financiera de la SDSCJ.	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. 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	El incidente de seguridad afecta un proceso de apoyo de SDSCJ, excepto el proceso de gestión financiera.	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	El incidente afecta a un funcionario o contratista, un área de colaboradores de la SDSCJ.	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 3. Descripción del nivel de prioridad de los incidentes de seguridad de la información

11. A continuación, se describe la clasificación de la prioridad de los incidentes de seguridad de la información

NIVEL DE PRIORIDAD			
IMPACTO	URGENCIA		
	Alta	Media	Baja

Alto	Alta	Alta	Media
Medio	Alta	Media	Baja
Bajo	Medio	Baja	Baja

Tabla 4. Nivel de Prioridad.

12. 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.

13. 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.

14. 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, los activos de información pública clasificada y publica reservada son los más relevantes para la entidad los cuales deben contar con controles robustos con el fin de preservar la Confidencialidad, Integridad y Disponibilidad de los mismos.
    - 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.
    - 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.

15. 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.
- Considerar la opción de volver a crear un sistema con discos duros nuevos (se deben eliminar los discos duros existentes y almacenarlos, ya que se pueden usar como prueba si se decide procesar a los posibles atacantes).
- Asegurar el cambio de las contraseñas: locales, de las cuentas de servicio y administrativas en todo el entorno.

16. 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).
- 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.
- Se utilizará la siguiente escala para valorar el Impacto de los incidentes de seguridad de la información en el SDSCJ:

INCIDENTE	DESCRIPCIÓN	IMPACTO	TIEMPO DE RESPUESTA
Código malicioso (Malware)	* Infección de estaciones de trabajo con código malicioso (malware). * Infección de discos de almacenamiento externo con código malicioso (malware). * Recepción y/o envío de correos electrónicos con contenido malicioso (malware).	**Crítico**	**24 horas**
Perdida o hurto de activos de información.	Perdida o hurto de componentes tecnológicos y/o activos de información (dispositivos portátiles, discos extraíbles, papeles con información confidencial, etc.).	**Crítico**	**24 horas**
Denegación del servicio de los sistemas de información	* Fallas en los canales de comunicación. * Fallas en el fluido eléctrico. * Fallas en servidores. * Saturación de recursos por ataques informáticos.	**Crítico**	**24 horas**
Fuga de información	* Envío de correo electrónico a cuentas externas con información de la Organización. * Extracción de información de la Organización usando medios de almacenamiento externo. * Divulgación de información confidencial de la compañía a personal externo. * Intentos o ejecución de Técnicas de Ingeniería Social.	**Crítico**	**24 horas**
Alteración de información	Modificación no autorizada o adulteración de información.	**Crítico**	**24 horas**
Cambios no autorizados en la plataforma tecnológica (servidores, sistemas de información, equipos de comunicación, etc.).	* Cambio de privilegios o configuraciones de usuario sin autorización previa. * Cambios en la configuración de la plataforma tecnológica sin autorización previa.	**Alto**	**48 horas**
Detección de dispositivos inalámbricos no autorizados.	* Detección de uso de redes inalámbricas generadas por medio de modem USB. * Detección de redes inalámbricas no autorizadas.	**Alto**	**48 horas**

	Acceso no autorizado	* Suplantación de usuarios en los sistemas informáticos. * Préstamo o Robo de Contraseñas. * Intrusión a sistemas de información no autorizada externa * Intrusión a sistemas de información no autorizada interna.	**Alto**	**48 horas**	
	Uso inadecuado de los recursos	* Descarga e instalación de software no autorizado. * Navegación a páginas pornográficas. * Navegación a redes sociales. * Envío de cadenas de correos electrónicos usando el correo corporativo. * Uso de herramientas que permitan saltar controles tecnológicos establecidos en la entidad.	**Medio**	**72 horas**	
	Incumplimiento político de escritorio limpio.	* El funcionario se ausenta de su puesto de trabajo sin bloquear su sesión de trabajo. * Claves de acceso a los sistemas expuestas en lugares visibles. * Información confidencial en papel sin custodia.	**Bajo**	**1 semana**	

Tabla 5. Impacto de Incidentes de Seguridad

17. Cualquier incidente que implique interrupción de algún servicio informático o afectación a un proceso de manera crítica, ya sea por el número de usuarios afectados o porque se han visto involucrados sistemas de información críticos para la SDSCJ, se debe dar una respuesta inmediata, la cual puede incluir la generación de un control de cambios para lo cual se deberá tener en cuenta las actividades del procedimiento de gestión de cambios PD-GT-2.

18. 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.).

19. 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.

20. 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 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.

PARÁMETROS DE MEDICIÓN
Matriz de indicadores

DESCRIPCIÓN DEL PROCEDIMIENTO

N°	Entrada o Insumo	Actividad	Descripción de la Actividad	Dependencia	Responsable	Punto de Control	Salida (Registro)
1	Requerimiento del usuario con el reporte	**Validar y registrar incidente**	Verificar que el requerimiento del usuario cuente con la informacion básica para registrar el incidente en la herramienta de gestión.	Dirección de Tecnologías y Sistemas de la Información	Técnico - Agente mesa de Servicio Nivel	Verificar creación del ticket	Registro del caso en la herramienta de gestión.
		Cumple con los requisitos mínimos?	**SI:** Continúa en la actividad 2 **NO:** Solicita informacion al usuario.				

2	Incidente creado en la herramienta de gestión.	**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.	Dirección de Tecnologías y Sistemas de la Información	Técnico - Agente Mesa de Servicio Nivel 1		Incidente categorizado en la herramienta de gestión.
3	Incidente registrado en la herramienta de mesa de servicio	**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.	Dirección de Tecnologías y Sistemas de la Información	Técnico - Agente Mesa de Servicio Nivel 1		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 actividad 04				
4	Incidente registrado y actualizado en	**Diagnosticar Incidente**	Realiza un diagnóstico inicial del Incidente, en	Dirección de	Técnico - Agente		Incidente actualizado en la herramienta de

	la herramienta de gestión		donde se analiza criticidad del servicio afectado, origen de la falla, prioridad de solución y posibilidades de gestión de acuerdo con la base de conocimiento	Tecnologías y Sistemas de la Información	Mesa de Servicio Nivel 1		gestión.
5	Incidente actualizado en la herramienta de gestión.	**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 problema 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 seguir el	Dirección de Tecnologías y Sistemas de la Información	Agentes de Mesa Profesionales de: Infraestructura Sistemas de Información Seguridad de la Información Uso y Apropiación Proveedores externos prestadores de servicios		Incidente actualizado en la herramienta de gestión. con la gestión y escalamiento realizado.

			procedimiento de Gestión de cambios PD-GT-2. Continua en actividad 11				
6	Incidente registrado en la herramienta	**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.	Dirección de Tecnologías y Sistemas de la Información	Profesional de Seguridad de la Información		Incidente actualizado en la herramienta de gestión.
7	Incidente actualizado en la herramienta de gestión.	**Clasificar y tipificar la prioridad del incidente de seguridad de la información**	Valida la clasificación y tipificación de acuerdo con las tablas 2,3,4 de las políticas de operación	Dirección de Tecnologías y Sistemas de la Información	Profesional de Seguridad de la Información		Incidente actualizado en la herramienta de gestión.
8	Incidente actualizado en la herramienta de gestión.	**Establecer estrategia de tratamiento del incidente de seguridad.**	Elabora con el equipo de trabajo la estrategia y los recursos (Económicos, humano, tiempo) requeridos para el tratamiento del Incidente. Si la respuesta o tratamiento del incidente requiere ejecutar un	Dirección de Tecnologías y Sistemas de la Información	Director de Tecnologías y Sistemas de la Información Profesional de Seguridad de la Información		Incidente actualizado en la herramienta de gestión.

			control de cambio, se debe diligenciar el formato F-GT-278 y seguir el procedimiento de Gestión de cambios de TIC PD-GT-2.				
9	Incidente actualizado en la herramienta de gestión.	**Recopilar y documentar evidencias**	Documenta la información necesaria del incidente y recopilar las evidencias producto de la investigación del incidente.	Dirección de Tecnologías y Sistemas de la Información	Profesional de Seguridad de la Información		Incidente actualizado en la herramienta de gestión.
10	Incidente actualizado en la herramienta de gestión.	**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. Solucionado el incidente de Seguridad de la Información.	Dirección de Tecnologías y Sistemas de la Información	Profesional de Seguridad de la Información	Validar si se requiere sensibilizar sobre medidas preventivas a implementar, para evitar la Materialización de futuros incidentes	Incidente actualizado en la herramienta de gestión.
11	Incidente actualizado en la herramienta de gestión	**Documentar en herramienta y completar caso**	Documenta detalladamente cómo se gestionó el incidente y cuáles fueron los resultados en la	Dirección de Tecnologías y Sistemas de la Información	Agentes de Mesa Profesionales de: Infraestructura Sistemas de Información		Incidente en la herramienta de gestión en estado completado. Notificación por

			herramienta de gestión. Posterior se actualiza el estado del caso como completado, automáticamente la herramienta envía la notificación del caso como completado y la encuesta de satisfacción para ser diligenciada por el usuario.		Seguridad de la Información Uso y Apropiación Proveedores externos prestadores de servicios		correo para el diligenciamiento de la encuesta de satisfacción.
12		**Identificar y Reportar posible problema**	El profesional asignado en resolver el incidente se encargará de identificar y reportar al coordinador de la mesa de servicio y al líder de servicios tecnológicos a través de correo electrónico, si el evento presentado es un posible candidato para gestionarse como problema.	Dirección de Tecnologías y Sistemas de la Información	Agentes de Mesa Profesionales de: Infraestructura Sistemas de Información Seguridad de la Información Uso y Apropiación Proveedores externos prestadores de servicios		Reporte por correo electrónico de posible problema

13	Reporte de posible problema	**Evaluar posible problema**	De acuerdo con el reporte se realiza evaluación de los criterios definidos en las políticas de operación con el fin de definir si se le da tratamiento como problema.				Solicitud para generación de problema.
		¿Se trata de un problema?	SI: Continúa siguiente actividad No: Continúa en la actividad 20.				
14	Solicitud para generación de problema.	**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.	Dirección de Tecnologías y Sistemas de la Información	Técnico - Agente Mesa de Servicio		Problema registrado en la herramienta
15	Problema registrado en la herramienta	**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.	Dirección de Tecnologías y Sistemas de la Información	Profesional - Coordinador de Mesa de Servicio		Convocatoria de reunión.
16		**Investigar y diagnosticar**	Analiza el problema desde los diferentes puntos de vista de cada profesional para entender el servicio o infraestructura asociadas,	Dirección de Tecnologías y	Profesionales -		Problema analizado Acta de Reunión

		causa raíz	realiza una lluvia de ideas sobre las posibles causas y la posible solución. Realiza investigación de la causa raíz en los sistemas afectados. 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.	Sistemas de la Información	Líderes delegados		Problema documentado en la herramienta de gestión
17	Problema actualizado en la herramienta de gestión.	**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.	Dirección de Tecnologías y Sistemas de la Información	Director de Tecnologías y Sistemas de la Información Profesionales - Líderes delegados		Problema documentado en la herramienta de gestión con la solución a implementar.
18	Problema documentado en la herramienta de gestión con la solución a	**Implementar solución definida en la reunión de Líderes**	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	Dirección de Tecnologías y Sistemas de la Información	Profesional: Infraestructura / Sistemas Información Seguridad de la Información/Uso y Apropiación	Verificar si la solución al problema fue exitoso respecto al escenario planteado.	Problema actualizado en la herramienta de gestión

	implementar.		cambio, se debe seguir el procedimiento de Gestión de cambios de TIC PD-GT-2.				
		¿Resolvió el problema?	**Si:** Continúa en la siguiente **No:** Retorna a la actividad número 16.				
19		**Cerrar problema**	Verifica que el problema este correctamente documentado en la herramienta de gestión y proceder al cierre de este.	Dirección de Tecnologías y Sistemas de la Información	Profesional: Servicios tecnológicos/ Infraestructura/ Sistemas Información/ Seguridad de la Información/ Uso y apropiación	Verificar que el problema quede en estado cerrado.	Problema cerrado en la herramienta de gestión
20	Notificación por correo para diligenciamiento de la encuesta de satisfacción.	**Evaluar satisfacción del servicio**	Diligenciar la encuesta de satisfacción.	Proceso que reportó el incidente	Usuario		Encuesta diligenciada por el usuario.
21	Encuesta diligenciada por el usuario.	**Analizar la evaluación de satisfacción**	Revisar y analizar los resultados de las encuestas de satisfacción	Dirección de Tecnologías y Sistemas de la	Coordinador Mesa de Servicio		Relación con los resultados de las encuestas de

			de servicio contestadas por los usuarios para determinar oportunidades de mejora. En caso de tener encuestas con resultados no satisfactorios con respecto a la solución brindada, se revisa en detalle cómo se gestionó el caso y se valida si las actividades de resolución fueron procedentes o no por parte de los agentes que gestionaron el incidente.	Información			satisfacción.
		¿La gestión realizada fue procedente?	**SI:** Se informa al solicitante por medio de correo electrónico porque la solución entregada fue procedente de acuerdo con el incidente y procedimientos establecidos. **NO:** Se cambia el estado del incidente como reapertura del mismo para continuar la gestión y dar la solución definitiva.				

CONTROL DE CAMBIOS		
No. VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**
1	30/08/2019	Documento Original
2	13/03/2020	Se ajustan logos de Alcaldía y de la Certificación ISO 9001-2015 Calidad
3	15/03/2021	Actualización del alcance, documentos de referencia, definiciones y descripción de actividades
4	21/09/2021	Actualización del logo de la Certificación ISO 9001-2015 Calidad, incorporando el numero de la certificación.
5	07/03/2023	Se unifica este procedimiento con los procedimientos Gestión de Incidentes de seguridad PD-GT-3 y Gestión de problemas PD-GT-7.

Elaboró: Diego Mauricio Usme González - Contratista - Seguridad de la Información
Francisco Javier Vargas Moncada - Profesional Universitario
Revisó: Rafael Humberto López - Contratista – Estrategia de TI
Jorge Eliecer Velásquez - Contratista – Enlace MIPG

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