INFORME FINAL TRABAJO DE AUDITORÍA

Monitoreo y desempeño de los servicios TIC (disponibilidad, oportunidad) y resolutividad de requerimientos e incidentes

OFICINA DE CONTROL INTERNO

AUDITOR:
LÍDER: FRANCISCO JAVIER PINTO GONZALEZ
Lead Auditor ISO27001:2013 registro ERCA No.1001545
CISM y CISA de ISACA y
Líder en Ciberseguridad con Certiprof

REVISADO POR:
OLGA LUCIA VARGAS COBOS
JEFE OFICINA DE CONTROL INTERNO

BOGOTÁ, noviembre 2025

SECRETARÍA DISTRITAL DE SALUD

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Contenido

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Abreviaturas

- AE: Arquitectura Empresarial
- ANS: Acuerdo de Nivel de Servicio
- Checklist: Lista de verificación o chequeo
- CONPES: Consejo Nacional de Política Económica y Social
- CPU: Unidad Central de Procesamiento - Procesador
- DAFP: Departamento Administrativo de la función Publica
- HELPDESK: Soporte Técnico o Mesa de Ayuda
- ISO/IEC: norma internacional creada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC)
- NIA: Norma Internacional de Auditoría
- MECI: Modelo Estándar de Control Interno
- MINTIC: Ministerio de Tecnologías de la información y comunicaciones.
- MIPG: Modelo Integrado de Planeación y Gestión.
- MSPI: Modelo de Seguridad y Privacidad de la Información
- OCI: Oficina de control interno
- PETI: Plan estratégico de Tecnologías de la información
- POGD: Plan operativo de Gestión y Desempeño
- SEGPLAN: Sistema de Seguimiento al Plan de Desarrollo Distrital mediante los Proyectos de Inversión
- SDS: Secretaria Distrital de Salud
- TIC: Tecnologías de la Información y Comunicaciones
- WEB: Telaraña o Sitio publicado

INTRODUCCION

Las auditorias de gestión son una herramienta estratégica que las entidades utilizan para conocer el estado de los procesos y servicios, determinando su eficacia y eficiencia mediante la evaluación objetiva y metódica que permite tomar decisiones frente a las debilidades identificadas, la auditoría especifica con énfasis en riesgo a la gestión TIC en lo referente al monitoreo y desempeño de los servicios TIC (disponibilidad, oportunidad)y resolutividad de requerimientos e incidentes en la SDS, busca detectar o identificar posibles debilidades, desviaciones, errores, falencias existentes permitiendo emprender acciones de mejoramiento adecuadas y oportunas. De acuerdo con lo anterior, la evaluación se realizó mediante el instrumento de verificación (checklist) de conformidad con los requisitos seleccionados de la normatividad y legislación relacionada o aplicable.

MARCO CONCEPTUAL

La gestión de incidentes y requerimientos de servicios TIC: Es el proceso que permite restaurar o recuperar la operación normal tras una interrupción o degradación (incidentes) y atender peticiones de usuarios como consultas o asesorías (requerimientos). Su objetivo principal es minimizar el impacto en la prestación de los servicios y garantizar la satisfacción del usuario final al manejar estos eventos de manera rápida y eficiente a través de un punto centralizado como el servicio de soporte técnico (Helpdesk). Al tener un proceso estandarizado bajo un procedimiento existente, se asegura que los equipos de TI establecidos respondan de forma rápida y consistente, reduce el impacto en las operaciones, mejora la satisfacción del usuario y ayuda a prevenir futuros problemas al aprender de los incidentes actuales (lecciones aprendidas o Base de datos de conocimiento).
Es clave mencionar que, la gestión de incidentes, corresponde a cualquier evento no planeado que interrumpe o reduce la calidad de los servicios TIC y su objetivo es restaurar el servicio lo más rápido posible, con el fin de minimizar las interrupciones y el impacto en las operaciones y procesos críticos.
La Gestión de requerimientos, corresponde a la peticiones de usuarios para obtener información, asesoría o realizar cambios que no están asociados a un problema actual y su objetivo es cumplir con las necesidades de los usuarios y asegurar que los objetivos tecnológicos se alcancen, evitando errores en el proceso.
Ambas gestiones se canalizan a través del servicio de soporte técnico (Helpdesk o mesa de ayuda o línea55), que es el punto centralizado de contacto para recibir, registrar, clasificar, priorizar y dar seguimiento a las solicitudes de los usuarios.

Monitoreo y supervisión de redes y servicios TIC: es el proceso continuo de observar, medir y analizar el rendimiento, la disponibilidad, el estado de la red y las aplicaciones para garantizar su correcto funcionamiento, para ello se utilizan herramientas para recopilar datos como el tráfico de red, el estado de los dispositivos (servidores, routers, switches), la latencia y el uso de recursos (CPU, memoria). Su objetivo principal consiste en identificar,

detectar problemas de forma temprana, responder a ellos y optimizar el rendimiento para evitar interrupciones del servicio y mantener una buena experiencia para el usuario.

El monitoreo de los servicios (como el correo electrónico, aplicaciones WEB, entre otros), permite garantizar la disponibilidad y correcto funcionamiento de los mismos, y partir de las herramientas de monitoreo implementadas, se espera la notificación de alertas automáticas a los administradores cuando se detecta algún problema o falla.

1. OBJETIVO GENERAL DE LA AUDITORÍA (NIA 2210).

Evaluar la gestión TIC en lo referente al monitoreo y desempeño de los servicios TIC (disponibilidad, oportunidad) y resolutividad de requerimientos e incidentes, garantizar la eficacia y eficiencia de los servicios TIC y de cara a la atención del usuario final tanto Interno y externo. La evaluación se realizará con base en los componentes de control del modelo MECI: ambiente de control, actividades de control, gestión del riesgo, actividades de monitoreo e información y comunicación.

2. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA. (NIA 2210).

- Constatar que la gestión de incidentes y requerimientos se realicen de manera eficiente y con criterio de calidad.
- Verificar el estado de implementación de la gestión de servicios conforme al marco normativo y regulatorio asociado.
- Validar políticas, lineamientos, procedimientos y guías asociadas a la gestión de requerimientos e incidentes.
- Verificar la gestión de incidentes y requerimientos frente a los componentes de control: actividades de control, gestión del riesgo, actividades de monitoreo e información y comunicación (Líneas de Defensa).
- Verificar que los controles establecidos frente al riesgo identificado, minimicen las amenazas a las que está expuesta la gestión de incidentes y requerimientos.
- Identificar posibles desviaciones, debilidades o errores que pudieran existir y proponer mejoras.

3. ALCANCE DE LA AUDITORÍA. (NIA 2220).

Desde: el registro, categorización, priorización, investigación y diagnóstico,
Hasta: la resolución, recuperación y cierre del incidente o requerimiento mediante el uso de las herramientas tecnológicas implementadas y dispuestas para tal fin. Dichos pasos buscan restaurar el servicio lo más rápido posible, minimizar el impacto en el negocio y aprender de cada incidente.

Periodo a evaluar:

- Desde: 1/10/2024
- Hasta: 14/10/2025

4. CRITERIOS DE AUDITORÍA. (NIA 2210- A3).

Para el desarrollo de la presente auditoría se tuvieron en cuenta los siguientes elementos:

4.1 Internos: (políticas, normatividad, procedimientos, lineamientos)

Procedimientos, lineamientos, guías existentes, formatos:

- SDS-TIC-PR-002 - GESTIÓN DE INCIDENTES Y REQUERIMIENTOS
- SDS-TIC-LN-001 - GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC
- SDS-TIC-001 - GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA
- SDS-DFO-PR-004 - GESTIÓN DEL RIESGO EN LA SDS
- SDS-TIC-INS-005 - INSTRUCTIVO PARA GESTION DE INCIDENTES MAYORES
- SDS-TC-LN-011 - LINEAMIENTO PARA GESTION DEL CONOCIMIENTO EN LA MESA DE SERVCIOS
- SDS-TIC-FT-056 - Bitácora Incidentes Mayores
- SDS-TIC-FT-032 - Contingencia para registró de casos mesa de servicios TIC
- SDS-TIC-FT-058 - Stock de Repuestos Mesa de Servicios

Normatividad específica para entidades públicas

- Decreto 1008 de 2018 - Política de Gobierno Digital.
- Guías de Gobierno Digital (MinTIC) - Guía para la Gestión y Clasificación de Incidentes de Seguridad (G.GDI.01)
- Marco de Referencia de Arquitectura Empresarial - lineamientos para la gestión de servicios de TI
- Decreto 338 de 2022, lineamientos generales en la gestión de incidentes de seguridad.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

4.2 Externos (leyes y regulaciones que apliquen)

Estándares internacionales de referencia

- ITIL (Información Technology Infrastructure Library) – Gestión de Servicio
- ISO/IEC 27001- en lo referente a la Gestión de incidentes de Seguridad
- ISO/IEC 20000: Norma internacional para la gestión de servicios de TI (ITSM)

Ejercicio basado metodológicamente en listas de chequeo a partir de los criterios seleccionados para este propósito.

5. METODOLOGÍA UTILIZADA. (NIA 2300).

La presente auditoría se desarrolló mediante mesas de trabajo presenciales con los diferentes referentes designados, verificando y constatando la conformidad de los criterios seleccionados a partir de lista de verificación elaborada. Para este propósito, se realizó la toma de casos aleatorios y análisis de la información referente a los procedimientos, registros documentales, registros de riesgos, herramientas, entre otros. Las mesas de trabajo fueron agendadas acorde a la programación establecida.

Adicionalmente el auditor tuvo en cuenta los siguientes aspectos:

- **Revisión de la documentación:** El auditor solicitó y revisó la documentación existente y relacionada con la gestión de incidentes y requerimientos, así como del monitoreo de la red y los servicios. Entre los documentos consultados se encuentran: lineamientos, procedimientos, bases de datos, registros de actas de reunión, registros de asistencia, entre otros.
- **Consultas con el personal designado:** El auditor realizó consultas específicas a los funcionarios designados.
- **Listados de verificación para los auditados:** El auditor entrego de manera anticipada las listas de verificación, la cual se trabajó en compañía de los referentes designados y personal que acompaño el ejercicio. Dichos listados serán una imagen cualitativa del estado de la gestión de incidentes y requerimientos, así como del monitoreo de la red y servicios TIC de la SDS.

6. ANÁLISIS DE INFORMACIÓN Y DE DATOS. (NIA 2320).

La presente auditoría, se llevó a cabo mediante recolección de información de diferentes fuentes, y como resultado de las diferentes mesas de trabajo realizadas, acompañadas de listas de chequeo, y verificación de diferentes documentos como es el caso de matriz de riesgos, POGD, procedimientos, lineamientos y documentos de apoyo internos e instrumentos, entre otros, que permitieron conocer los procedimientos y las prácticas utilizadas en la entidad para apoyar la gestión de incidentes y requerimientos, así como el monitoreo de la red y los servicios TIC de la SDS. En cuanto a los resultados de la evaluación, estos fueron analizados, con el fin de determinar posibles desviaciones, debilidades o falencias, evidenciando las causas que las originan y proponiendo

alternativas que permitan mitigarlos, dichos resultados serán presentados a lo largo del presente informe.

A continuación, el presenta el análisis general por componente de control MECI:

TEMAS REVISADOS	ASPECTOS VERIFICADOS
6.1 Ambiente de control: Es el conjunto de procesos y estructuras que proveen las bases para llevar a cabo el control interno a través de la organización	Contempló la revisión de las herramientas empleadas en las diferentes actividades del lineamiento, procedimiento y guía en cuestión, así como los recursos humanos, financieros y tecnológicos necesarios para la operación diaria que apoya la gestión de incidentes y requerimientos de la entidad, así como el monitoreo continuo de la red y los servicios. Es importante señalar que la gestión de incidentes y requerimientos es uno de los servicios del portafolio TIC y aplica a nivel institucional, Desde la estructura jerárquica de la entidad, y de cara a la segunda línea de defensa, se cuenta con un gobierno o liderazgo a cargo de la dirección TIC, quienes definieron, implementaron y adoptaron la buena práctica. La revisión, contempló diferentes instrumentos como son: lineamiento, procedimiento, guías, formatos ligados a los temas en cuestión. Dichos aspectos permitieron llevar a cabo una revisión integral por parte de la Oficina de Control Interno como objetivo de esta evaluación. Respecto al particular, se cuenta con listado de preguntas realizadas en cada una las mesas y en tal medida permitió constatar el cumplimiento de los criterios evaluados.
6.2 Actividades de Control (incluye la revisión de políticas de operación procedimientos , normatividad interna y externa, Plan Operativo Anual	1. Dicha fase consistió en la verificación y evaluación de los criterios establecidos en base los estándares y las buenas practicas, así como del lineamiento y procedimiento interno definido: Normatividad específica para entidades públicas y procedimientos, lineamientos y guías existentes aplicables: • Decreto 1008 de 2018 - Política de Gobierno Digital. • Guías de Gobierno Digital (MinTIC) - Guía para la Gestión y Clasificación de Incidentes de Seguridad (G.GDI.01) • Decreto 338 de 2022, lineamientos generales en la gestión de incidentes de seguridad. De cara a la política de Gobierno Digital, se emite la política específica de gestión de incidentes, la cual se enfoca en la detección, respuesta y recuperación ante incidentes de seguridad digital, con el objetivo de minimizar el impacto en los servicios y proteger la información, además de gestionar los incidentes de acuerdo a su gravedad e impacto internamente. Frente a este aspecto, la Dirección TIC, creó la “Guía para la Gestión de Incidentes de Seguridad Informática” codificada: Gui-001G_incidentes_Seg_informatica.doc, la cual establece en su numeral 4.1, los roles y responsabilidades frente al servicio, además de la diferentes fases establecidas para la gestión de incidentes que encuentran implementadas en la entidad. En cuanto al marco normativo y herramientas utilizadas, la gestión de incidentes y requerimientos de la SDS, se alinea con el Modelo de Seguridad y Privacidad de la Información (MSPI), que proporciona lineamientos para la gestión del ciclo de vida de la seguridad de la información y se alinea con la Plataforma Nacional de Notificación y Seguimiento de Incidentes de Seguridad Digital (Decreto 338 de 2022), la cual facilita el intercambio de información y el seguimiento seguro de incidentes entre las entidades y autoridades competentes, para ello se cuenta con

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

registros de boletines informativos, correos e informes de proveedores de tecnología, donde notifican las diferentes fallas, amenazas e incidentes que se reportan a nivel mundial y en la que la SDS debe analizar e implementar para prevenir posibles incidentes de seguridad.

- Marco de Referencia de Arquitectura Empresarial - lineamientos para la gestión de servicios de TI

En cuanto a la Arquitectura Empresarial (AE) para la gestión de servicios de TI en la SDS, esta se alinea al plan estratégico de la entidad y la ejecución de sus operaciones, asegurando que la tecnología actual, soporte los objetivos de la entidad de forma eficiente y segura. El enfoque de definición de la arquitectura empresarial, hizo parte de uno de los componentes del PETI año 2024, para lo cual mediante la consultoría, se generaron los siguiente entregables: dimensiones de negocio, datos, aplicaciones y tecnología, identificando brechas entre el estado actual y el futuro deseado, para gestionar y optimizar la entrega de servicios de TI, incluyendo la planificación, implementación y mejora continua.
Lo cual esta soportado mediante los entregados del contrato suscrito y que lidero uno de los especialistas de la dirección TIC.

2. La evaluación contemplo la política de Gobierno Digital y Seguridad Digital en el marco de la Resolución 705 del 11 de julio del 2025 expedida.

3. Así mismo, se evaluaron los procedimiento, guías y formatos codificados:
   - SDS-TIC-PR-002 GESTIÓN DE INCIDENTES
   - SDS-DFO-PR-004 - GESTIÓN DEL RIESGO EN LA SDS
   - Instructivos y documentación asociada que hacen parte del repositorio documental y que está relacionado en el procedimiento para el presente alcance, se listan a continuación:
     - SDS-TIC-LN-001 - GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC
     - SDS-TIC-001 - GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA
     - SDS-TIC-FT-056 - Bitácora Incidentes Mayores
     - SDS-TIC-FT-032 - Contingencia para registró de casos mesa de servicios TIC
     - SDS-TIC-FT-058 - Stock de Repuestos Mesa de Servicios
     - SDS-TIC-INS-005 - INSTRUCTIVO PARA GESTION DE INCIDENTES MAYORES
     - SDS-TC-LN-011 - LINEAMIENTO PARA GESTION DEL CONOCIMIENTO EN LA MESA DE SERVICIOS

Al particular, evidenciamos que:
- BITACORA INCIDENTES MAYORES - SDS-TIC-FT-056,
- ENCUESTA DE SATISFACCIÓN MESA DE SERVICIOS DE TIC - SDS-TIC-FT-038 y
- CONTINGENCIA PARA REGISTRO DE CASOS MESA DE SERVICIOS TIC - SDS-TIC-FT-032, son documentos establecidos en la operación de acuerdo a lo definido en el procedimiento de “GESTIÓN DE INCIDENTES - SDS-TIC-PR-002”, sin embargo, a la fecha de la presente evaluación, no han sido diligenciados, situación que deriva en una acción de mejora.

Por último, en lo que refiere a los siguiente documentos:

- SDS-TIC-INS-005 - INSTRUCTIVO PARA GESTION DE INCIDENTES MAYORES
- SDS-TC-LN-011 - LINEAMIENTO PARA GESTION DEL CONOCIMIENTO EN LA MESA DE SERVICIOS,
- SDS-TIC-FT-058 - Stock de Repuestos Mesa de Servicios, dichos documentos ya no existen en la base de conocimiento de isolucion, pero aún siguen relacionados en el procedimiento de "GESTIÓN DE INCIDENTES - SDS-TIC-PR-002", la presente situación, que deriva en una acción de mejora.

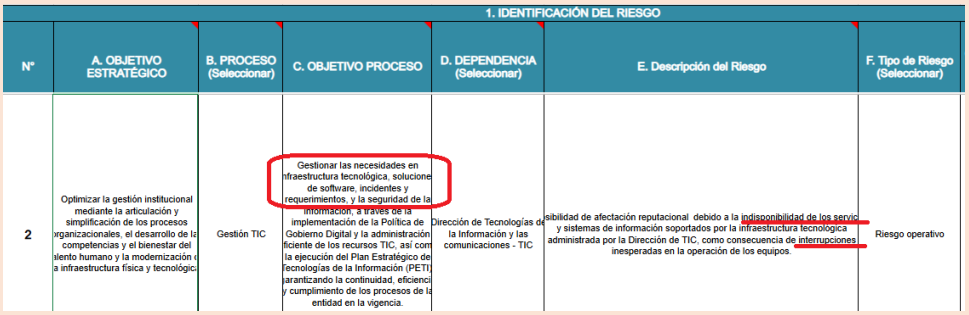
De acuerdo con lo anterior, se cuenta con el listado de preguntas realizadas en cada una las mesas y en tal medida permitió constatar el estado y avance de los criterios evaluados.

6.3 *Evaluación del Riesgo y controles (incluye análisis de contexto, riesgos relacionados identificación de controles y su operación, posibles riesgos detectados)*

Respecto a la gestión de Riesgos del proceso TIC de la SDS, si bien es cierto, la metodología actual se fundamenta en prácticas del DAFP, los riesgos de gestión identificados en la actualidad son 4, no obstante, el riesgo que apunta a contrarrestar las amenazas o vulnerabilidades propios de la gestión de incidentes y requerimientos, solo se aborda frente al riesgo Nro2, la fuente de información consultada fue la siguiente:

- Mapa_Riesgos_TIC_Def2025.xlsx
- Mz_Monitoreo_Riesgos_TIC_2025.xlsx

A continuación, comparto una captura de pantalla del documento denominado: Mapa_Riesgos_TIC_Def2025.xlsx y se resalta el riesgo nro. 2 de que tiene relación con el tema en cuestión, dicho riesgo cuenta con un plan de tratamiento que consta de 5 controles que permiten mitigar el riesgo.



1. IDENTIFICACIÓN DEL RIESGO						
N°	A. OBJETIVO ESTRATÉGICO	B. PROCESO (Seleccionar)	C. OBJETIVO PROCESO	D. DEPENDENCIA (Seleccionar)	E. Descripción del Riesgo	F. Tipo de Riesgo (Seleccionar)
2	Optimizar la gestión institucional mediante la articulación y simplificación de los procesos rganizacionales, el desarrollo de la competencias y el bienestar del iento humano y la modernización a infraestructura física y tecnológica	Gestión TIC	Gestionar las necesidades en nfraestructura tecnológica, solucione de software, incidentes y requerimientos, y la seguridad de la información, a través de la implementación de la Política de Gobierno Digital y la administración ficiente de los recursos TIC, así com la ejecución del Plan Estratégico de Tecnologías de la Información (PETI arantizando la continuidad, eficienci y cumplimiento de los procesos de la entidad en la vigencia.	Dirección de Tecnologías de la Información y las comunicaciones - TIC	sibilidad de afectación reputacional debido a la indisponibilidad de los servic y sistemas de información soportados por la infraestructura tecnológica administrada por la Dirección de TIC, como consecuencia de interrupciones inesperadas en la operación de los equipos.	Riesgo operativo

Es clave mencionar que al no existir riesgos identificados para la gestión de incidentes y requerimientos, la organización queda expuesta a un aumento de problemas de cumplimiento, daños a su reputación, pérdidas financieras y sanciones legales. Por último, las consecuencias de los incidentes presentados en la operación, pueden variar desde la pérdida de datos hasta la interrupción o afectación de las operaciones, lo que resulta en un impacto en la imagen y reputación de la entidad. Si no se cuenta con un plan basado en riesgos, la respuesta ante incidentes o requerimientos puede ser lenta, desorganizada e ineficaz, lo que agrava los problemas.

Otros documentos consultados y relacionados en el repositorio documental son:

- SDS-DFO-PR-004 - GESTIÓN DEL RIESGO EN LA SDS,
- SDS-DFO-FT-035 - MAPA DE RIESGOS PARA SEGURIDAD DE LA INFORMACIÓN

	De acuerdo con lo anterior, se viene cumpliendo con la gestión de riesgos del proceso TIC, en lo referente al manejo y atención de incidentes y requerimientos de servicios en base al lineamiento, procedimiento y guía definida.
6.4 *Actividades de monitoreo (incluye las acciones que la primera y segunda línea de defensa ejercen para mitigar la ocurrencia de los riesgos sean este seguimiento al cumplimiento de políticas, actividades, directrices, metas)*	Se llevó a cabo la verificación y el resultado fue el siguiente: **Primera Línea (Autocontrol):** • El cumplimiento del lineamiento, procedimiento de gestión de incidentes y requerimientos, está en manos de cada colaborador de la entidad, dando respuesta a su vez al cumplimiento a la política de gobierno Digital y seguridad digital, así mismo, los gestores de riesgos y calidad designados, juega un papel fundamental, ya que debe impartir los conocimientos adquiridos y propiciar la cultura de seguridad y calidad con todos los colaboradores en la dependencia a la pertenece conllevando al cumplimiento de las políticas internas. • Realizan el reporte o escalamiento de incidentes y requerimientos mediante los canales de atención establecidos. • La primera línea evalúa la satisfacción del usuario frente al servicio o la atención brindada por los agentes del HelpDesk, así como determinar si la solución establecida fue eficaz. **Segunda Línea (Autoevaluación):** • La Dirección TIC, ejerce el liderazgo y gobernanza del proceso de gestión de incidentes y requerimientos de servicio, así como lleva cabo el monitoreo de la red y los servicios TIC en la entidad, y articula, direcciona todas las necesidades mediante el comité de gestión y desempeño y los comités técnicos. • La Dirección TIC, establece y adopta las metodologías del DAFP y las del ministerio de las TIC, con el fin de cada colaborador de la entidad, reporte los incidentes y requerimientos mediante los canales establecidos, adicionalmente, clasifica y prioriza la atención de los casos, en función del impacto que conllevan para la organización. • Los controles o criterios que fueron objeto de la presente evaluación, serán presentados mediante tablas a lo largo del informe, determinando cuales requisitos: “Cumplen”, cuales “No Cumplen”, y cuales adicionalmente derivan en Oportunidades de Mejora. • Si bien es cierto, la dirección del planeación institucional y calidad, estableció el procedimiento codificado SDS-DFO-PR-004 - GESTIÓN DEL RIESGO EN LA SDS y formato SDS-DFO-FT-035 - MAPA DE RIESGOS PARA SEGURIDAD DE LA INFORMACIÓN, a la fecha de la presente auditoria, resultados concretos de matrices consolidadas, resultados de monitoreo, seguimiento y resultados de tratamiento de riesgos de gestión, se encuentran en curso.
6.5 *Información y comunicación*	• Se realizo la verificación de los diferentes registros e información compartida en los repositorios establecidos, así como bases de información suministrada de las tablas de incidentes y requerimientos gestionados en el aplicativo institucional ARANDA software. • Se consultaron algunas piezas comunicativas y registros de correos que reflejan la concientización a los colaboradores en temas de gestión de incidentes y requerimientos desarrolladas en el periodo de la evaluación, No obstante, es indispensable continuar realizando las campañas de concientización, incorporando y dando a conocer lineamientos, procedimientos, guías y formatos establecidos de cara a la Gestión de incidentes y requerimientos de servicios TIC propiciando la eficacia y eficiencia del proceso. • Por último, se cuenta con registros de actas de reuniones de revisión por la dirección y comités técnicos que son escenarios para comunicar los resultados de la gestión de incidentes y requerimientos.

Una vez realizado el análisis de la información obtenida, resultado de las mesas de trabajo realizadas, se obtienen los siguientes resultados:

Resultados de la evaluación mediante lista de chequeo: El ejercicio mediante lista de chequeo, contempló la evaluación de 34 criterios para el frente de gestión de incidentes y requerimientos y contemplo 22 criterios para el frente de monitoreo de la red y servicios TIC, criterios establecidos en base al código de buenas prácticas mundial, adicionalmente y se evaluaron los procedimientos y guías existentes relacionadas.

Nota: El detalle de la evaluación realizada con cada uno de los criterios, hace parte de los papeles de trabajo utilizados, así mismo se cuenta con las grabaciones obtenidas que soportan el ejercicio con evidencia digital.

A continuación, mediante tablas agrupadas, se presentan los criterios evaluados y los resultados obtenidos de conformidad con el alcance establecido por parte del auditor:

Convenciones de la tabla: Color Verde: Cumple, Color Rojo: No cumple y Color Azul: Oportunidad de mejora

Componente1: Evaluación a la gestión de incidentes y requerimientos de servicios TIC

Fases o etapas de la gestión	Cumple	No Cumple	Total general
1. Preparación y prevención	5		5
2. Identificación e investigación	5	1	6
3. Contención y erradicación		1	1
4. Recuperación y cierre	2		2
5. Comunicación con el usuario	3		3
6. Recuperación y cierre	1		1
7. Análisis post-incidente y mejora continua	3	1	4
8. Revisión y métricas	7	3	10
9. Gestión de requerimientos	2		2
Total general	28	6	34

Tabla1: Resultados por fases o etapas

La Tabla1, resume el resultado de la evaluación realizada de cara a las 9 fases o etapas de la gestión de incidentes y requerimientos de los Servicios TIC, para lo cual hubo una selección de 34 criterios de los cuales, 28 criterios “Cumplen”, mientras que 6 de los criterios evaluados “No Cumplen”, para los cuales se decreta una no-conformidad y requerirá de una acción correctiva inmediata. Por último, identificamos doce (12) de los criterios evaluados que presentan una debilidad y en consecuencia, será indispensable definir un plan de mejoramiento que permita fortalecer y afianzar cada uno de estos aspectos.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Fases o etapas de la gestión	Oportunidad de Mejora	Total general
1. Preparación y prevención	2	5
2. Identificación e investigación	3	6
3. Contención y erradicación		1
4. Recuperación y cierre		2
5. Comunicación con el usuario		3
6. Recuperación y cierre	1	1
7. Análisis post-incidente y mejora continua	2	4
8. Revisión y métricas	4	10
9. Gestión de requerimientos		2
Total general	12	34

Tabla2: Resultados de oportunidades de mejora

La tabla 1 y 2, permite presentar el resultado de las oportunidades de mejora identificadas en cada una de las fases, sin embargo, es importante precisar que algunos de los criterios evaluados que desde la óptica del auditor “cumplen”, es necesario emprender una oportunidad de mejora para fortalecer dicho control.

A partir del capítulo del Componente1 de la página 15, se listan y detallan los diferentes hallazgos representados en (No-conformidades y Oportunidades de mejora) que fueron resultado de la evaluación realizada y para los cuales será que los responsables tomen las acciones de mejora pertinentes para subsanar y lograr que la entidad cumplan con estos aspectos o criterios en el mediano o largo plazo.

Componente2: Evaluación al Monitoreo de la red y los Servicios TIC

Criterios Evaluados	Cumple	No Cumple
¿Existen herramientas implementadas para la supervisión (ej. Zabbix, Nagios, SolarWinds, PRTG, etc.).?	1	
¿Las herramientas generan alertas automáticas en caso de falla o degradación?	1	
¿Se comparan los resultados con los SLA definidos?		1
¿Se detectan desviaciones o incumplimientos?	1	
¿Se encuentra documentado el plan de monitoreo con roles, responsabilidades y herramientas?		1
¿Se evalúa la capacidad actual vs. demanda proyectada?	1	
¿Se generan informes de desempeño por periodo (diario, mensual, trimestral)?	1	
¿Se ha determinado la frecuencia del monitoreo (en tiempo real, diario, semanal, etc.)?	1	
¿Se han definido los objetivos del monitoreo (disponibilidad, capacidad, desempeño, seguridad, etc.)?	1	
¿Se han establecido los indicadores clave de desempeño (KPI) y niveles de servicio (SLA/OLA)?		1
¿Se han identificado los servicios TIC críticos a monitorear?	1	
¿Se mantiene un registro histórico de los datos de monitoreo?	1	
¿Se mide el porcentaje de disponibilidad de cada servicio TIC?	1	
¿Se miden los tiempos de respuesta de aplicaciones y servicios?	1	
¿Se monitorea Infraestructura clave (Aplicaciones y bases de datos)?	1	
¿Se monitorea Infraestructura clave (Seguridad)?	1	
¿Se monitorea Infraestructura clave (Servicios en la nube y virtualización)?	1	
¿Se monitorea Infraestructura clave (servidores, redes, almacenamiento)?	1	
¿Se registran y analizan los tiempos de inactividad (downtime)?	1	
¿Se revisa la experiencia del usuario final (tiempo de carga, latencia, errores)?	1	
¿Se revisan tendencias de uso de recursos (CPU, memoria, almacenamiento, ancho de banda)?	1	
¿Se verifican los mecanismos de respaldo y redundancia de los sistemas monitoreados?	1	
Total general	19	3

Tabla 3: Resultados x Criterios

La tabla 2, resume la evaluación realizada frente al código de buenas prácticas y comprendió la selección de 22 criterios, al observar la tabla, podemos constatar que, existen 19 criterios que de acuerdo con la evaluación “Cumplen”, mientras que tres (3) de los

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

criterios evaluados “no cumplen” para los cuales se decreta una no-conformidad y requerirá de una acción correctiva inmediata. Por último, identificamos 4 de los criterios evaluados que “cumplen”, no obstante, desde la óptica del auditor presentan una debilidad y en consecuencia, será indispensable definir un plan de mejoramiento que permita fortalecer y afianzar cada uno de estos aspectos. Es clave mencionar que varios de estos hallazgos presentados, se unifican o consolidan para abordar la acción de mejora.

A continuación, mediante tablas se presentan los resultados de la evaluación y se refleja el estado de cada uno de los criterios en base a la identificación de la pregunta establecida:

Criterios Evaluados	Oportunidad de Mejora
¿Existen herramientas implementadas para la supervisión (ej. Zabbix, Nagios, SolarWinds, PRTG, etc.).?	
¿Las herramientas generan alertas automáticas en caso de falla o degradación?	1
¿Se comparan los resultados con los SLA definidos?	
¿Se detectan desviaciones o incumplimientos?	1
¿Se encuentra documentado el plan de monitoreo con roles, responsabilidades y herramientas?	
¿Se evalúa la capacidad actual vs. demanda proyectada?	
¿Se generan informes de desempeño por periodo (diario, mensual, trimestral)?	
¿Se ha determinado la frecuencia del monitoreo (en tiempo real, diario, semanal, etc.)?	
¿Se han definido los objetivos del monitoreo (disponibilidad, capacidad, desempeño, seguridad, etc.)?	
¿Se han establecido los indicadores clave de desempeño (KPI) y niveles de servicio (SLA/OLA)?	
¿Se han identificado los servicios TIC críticos a monitorear?	
¿Se mantiene un registro histórico de los datos de monitoreo?	1
¿Se mide el porcentaje de disponibilidad de cada servicio TIC?	1
¿Se miden los tiempos de respuesta de aplicaciones y servicios?	
¿Se monitorea Infraestructura clave (Aplicaciones y bases de datos)?	
¿Se monitorea Infraestructura clave (Seguridad)?	
¿Se monitorea Infraestructura clave (Servicios en la nube y virtualización)?	
¿Se monitorea Infraestructura clave (servidores, redes, almacenamiento)?	
¿Se registran y analizan los tiempos de inactividad (downtime)?	
¿Se revisa la experiencia del usuario final (tiempo de carga, latencia, errores)?	
¿Se revisan tendencias de uso de recursos (CPU, memoria, almacenamiento, ancho de banda)?	
¿Se verifican los mecanismos de respaldo y redundancia de los sistemas monitoreados?	
Total general	**4**

Tabla 4: Resultados de oportunidades de mejora

La tabla 3 y 4, permiten presentar el resultado de las oportunidades de mejora identificadas de cara a los criterios evaluados, sin embargo, es importante precisar que algunos de los criterios evaluados que desde la óptica del auditor “cumplen”, es necesario emprender una oportunidad de mejora para fortalecer dicho control.

A partir de la página 15, se listan y detallan los diferentes hallazgos representados en (No-conformidades y oportunidades de mejora) que fueron resultado de la evaluación realizada y para los cuales será necesario que los responsables tomen las acciones de mejora pertinentes que permitan subsanar y lograr que la entidad cumplan con los aspectos o criterios en el mediano o largo plazo.

A continuación, se listan y detallan los diferentes hallazgos representados en (No-conformidades y Oportunidades de mejora) que fueron resultado de la evaluación realizada.

Análisis con respecto a la Gestión de incidentes/requerimientos de los servicios TIC, y monitoreo/supervisión de redes y servicios TIC

Hallazgo	**1**
Fase	Contención y erradicación Identificación e investigación Análisis post-incidente y mejora continua
Criterio Evaluado	¿Se realiza investigación de la causa raíz de los incidentes registrados? ¿Como se lleva a cabo la contención del incidente para prevenir su propagación y limitar el daño? ¿Se actualiza la base de conocimientos (KB) si la solución es reutilizable? ¿Se realiza análisis de la respuesta dada al incidente y se documentan las lecciones aprendidas?
Dependencia Auditada:	Dirección TIC
Componente MECI relacionado	Actividades de Control Gestión de Riesgos Monitoreo y supervisión Información y Comunicación
Resultado de la evaluación	Si bien es cierto, en la actualidad existen: 1. lineamiento establecido para la “GESTION DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC”, codificado: SDS-TIC-LN-001-V51-1.pdf y su última versión del 20 de junio del año 2023 como se evidencia en la siguiente captura del aplicativo Isolucion.

HISTORIAL DE CAMBIOS	
Nombre del documento:	GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC.
Plantilla:	Lineamiento
Código:	SDS-TIC-LN-001
Revisó:	Gloria Yaneth, Sacristan Manotas Isabel, Mira Rivas Jeison Steven, Perdomo Polania
Aprobó:	Luis Carlos, Ocampo Ramos

Versión	Fecha	Razón del cambio
1	17/Abr/2013	Se crea en respuesta al procedimiento Gestión de incidentes y requerimientos de servicios TIC - 114-GTI-PR-014 y de acuerdo con la metodología ITIL v.3 que se está implementando en la entidad.
2	21/Jul/2014	se realiza asociación de los formatos 114-GTI-FT-035 Cambio definitivo 114 FT-036 Concepto técnico TIC -FT-038 Control de acceso al Centro de Cómputo , se modifica los textos de línea 55 por mesa de servicios Tic , ya que la línea 55 solo es un medio de los que se utilizan para el escalamiento de casos.
3	30/Mar/2016	Se actualiza el lineamiento, como parte del mejoramiento de procedimientos de TIC, con base en las mejores prácticas de ITIL.
4	11/Sep/2017	Modificación en los numerales: 6.1 pág. 9, 6.3 pág 10 - 13, 6.4 pág 14, 6.5 pág. 18, 6.6.1 pág 19 y 24, 6.6.3 pág 30, 6.7 pág 31, 6.8 pág 33, 6.8.2 pág 34.
5	20/Jun/2023	Actualización del documento, de acuerdo con las nuevas condiciones y alineación con la metodología ITIL, incluye ajuste de objetivos, nuevas definiciones, actualización a nuevo formato de lineamiento, actualización Matriz RACI y reorganización del documento. CODIGO SHA512: A4C0A21FDF80BD74ADF87B8B5881332E9FDAC04B2244C066B041F2FDCF8BA4EB178FD892683B2CEB5F254B09BD93E4FE95D8327FC1AA138E7AB5B302D26079C0

2. procedimiento establecido para la “GESTION DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC”, codificado: SDS-TIC-PR-002, en su versión 4 del 30 de septiembre del año 2025, como se evidencia en la siguiente captura del aplicativo Isolucion.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

HISTORIAL DE CAMBIOS	
Nombre del documento:	GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC
Plantilla:	Procedimiento SIG
Código:	SDS-TIC-PR-002
Revisó:	Sandra Patricia, Caycedo Hernandez Fernando Augusto, Salamanca Lopez Yuli Viviana, Osorio Vallejo
Aprobó:	Jaime Alberto, Pineda Ramirez

Versión	Fecha	Razón del cambio
1	15/Abr/2013	Se crea este procedimiento en respuesta a la etapa del ciclo de vida de Operación del Servicio, de acuerdo a la metodología ITIL v3 aplicada dentro de la prestación de servicios TIC de la entidad.
2	28/Ago/2015	El presente documento fue creado antes de la reorganización de la Secretaría distrital de salud y se identificaba con la codificación 114-GTI-PR -002 , por cambios estructurales y con fundamento en el Decreto 507 de 2013 fue necesario actualizar el nombre de las dependencias, procesos y el código
3	29/Jun/2017	Se revisó el procedimiento, se ajustó el objetivo, alcance y las actividades, se incluyen tiempos y glosario de términos.
4	30/Sep/2025	Se actualiza el procedimiento con la inclusión de la desagregación de roles entre la Mesa de Servicios y los especialistas del Grupo de Infraestructura - DataCenter. Asimismo, se fortalecen los aspectos normativos y conceptuales para mejorar la claridad y alineación con las buenas prácticas de gestión de servicios de TI.

3. Guía establecida para la “GESTION DE INCIDENTES DE SEGURIDAD INFORMATICA”, codificado: SDS-TIC-001 en su versión 1 del 30 de julio del año 2025, como se evidencia en la siguiente captura del aplicativo Isolucion.

HISTORIAL DE CAMBIOS	
Nombre del documento:	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA
Plantilla:	Guia
Código:	SDS-TIC-001
Revisó:	Yuli Viviana, Osorio Vallejo Camilo, Tiriat Ballesteros Sandra Patricia, Caycedo Hernandez
Aprobó:	Jaime Alberto, Pineda Ramirez

Versión	Fecha	Razón del cambio
1	25/Jul/2025	Brindar una orientación de las activades a realizar en los casos que se presente un incidente de seguridad informática

De acuerdo con lo establecido por dichos instrumentos y tomando como insumo la base de registros de incidentes reportados del periodo solicitado, identificamos que no existe evidencia que demuestre el ejercicio de análisis causa raíz de los diferentes incidentes presentados. Así mismo, se informa por parte de los profesionales o especialistas designados que, los incidentes que no pudieron son resueltos en “primer nivel de atención”, deben ser escalados al grupo de especialistas o en su defecto al proveedor, y lo concerniente al análisis causa raíz, no se está realizando. Es importante precisar que las consecuencias de no realizarlo, se perpetúa en un ciclo continuo de soluciones temporales o “WorkArounds”, en lugar de abordar las causas fundamentales o definitivas, lo que conlleva a problemas recurrentes, ineficiencias, costos continuos y riesgos incrementados. La falta de análisis de causa raíz, significa no aprender de los errores, lo que impide tomar decisiones estratégicas para prevenir futuras interrupciones, mejorar la estabilidad del sistema y fortalecer la seguridad. Es por eso que los incidentes que presentan comportamientos o patrones similares o reincidentes, van a seguir presentándose, lo que conlleva a altos tiempos de respuesta e ineficacia.

Así mismo, y el propósito de la guía es detener la propagación de incidentes, permitiendo limitar el daño y prevenir un mayor acceso no autorizado a los sistemas que fueron objeto o producto de un ciberataque, se debe identificar las diferentes situaciones que surgen del monitoreo que realizan los especialistas e implementar las acciones de mejora que permitan evitar su propagación y así mismo informar a los grupo de especialistas (infraestructura, seguridad, entre otros).

	Casos de incidentes donde se aplicaron medidas de contención, no se tiene identificados en la base de datos de incidentes de Aranda Software. Por último, al consultar la base de datos de conocimiento en el módulo del software ARANDA, constatamos que dicha actividad no se está haciendo, ya que se informa que la persona que reúne el perfil y que debería gestionar la base de datos de conocimiento no se tiene en el momento. Es importante precisar, que la SDS cuenta con el módulo de KBD mediante el software de ARANDA, pero no se le está dando uso. Así mismo, encontramos que el módulo de autogestión y registro de incidentes vía TEAMS siendo este otro canal de recepción el cual no se utiliza y es desconocido por parte de los colaboradores de la Entidad. En síntesis, no utilizar la base de conocimiento de incidentes puede tener consecuencias graves, ya que retrasa la resolución de problemas, impide la identificación de patrones, aumenta los costos operativos, así como daños a la reputación y pérdida de datos. Ignorar la base de conocimiento, significa no aprovechar una herramienta fundamental para la gestión de incidentes, lo que perpetúa los mismos problemas y debilita la postura de seguridad y de gestión general. De acuerdo con todo lo anterior, se incumplen el requisito del sistema de gestión de calidad y del sistema de seguridad de la información (específicamente en lo referente a la gestión de no conformidades y la implementación de acciones correctivas), ya que esto conduce a que la causa raíz del incidente no se elimine, lo que a su vez impide que se tomen medidas efectivas para prevenir la recurrencia del incidente y puede llevar a que el misma causa se repita indefinidamente. Por último, el LINEAMIENTO GESTION DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC - SDS-TIC-LN-001 versión 5, en sus numerales 5.3.2. Políticas Para Gestión de Incidentes Mayores y 5.1.7. Gestor de Conocimientos, define y establece varios ítems, que a la fecha se están incumpliendo e identificamos que el LINEAMIENTO PARA GESTIÓN DEL CONOCIMIENTO EN LA MESA DE SERVICIOS - SDS-TIC-LN-011 establecido ya no existe, en consecuencia, todo lo anterior, constituye una no-conformidad a tratar.
Estado	No Cumple

Hallazgo	**2**
Fase	Revisión y métricas
Criterio Evaluado	¿Se revisan los tickets cerrados para control de calidad? ¿Se miden los tiempos de resolución? Resolución de casos en Nivel1 - Mensual Resolución de casos en Nive2 – Mensual ¿Se cuenta con resultados de operación mediante la matriz de seguimiento de casos de mesa de servicios de TIC - SDS-TIC-FT-029? ¿Se han establecido los indicadores clave de desempeño (KPI) ¿Se analizan tendencias (incidentes recurrentes, áreas críticas)? Porcentaje de incidentes mayores – Mensual ¿Se cuenta con soportes de operación (resultados) de: Bitácora Incidentes Mayores - SDS-TIC-FT-056?
Dependencia Auditada:	Dirección TIC
Componente MECI relacionado	Actividades de Control Monitoreo y supervisión Información y Comunicación

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Resultado de la evaluación	Al particular, se informa por parte de los referentes que: 1. el control de calidad no se realiza a la fecha, no existe evidencia al respecto, es por eso que, determinar si los incidentes o requerimientos se han "categorizado" de manera acertada, saber si, los incidentes y requerimientos de están cerrando de manera consistente y además determinar y tratar "casos sin solución", se constata que no se realiza. 2. Al consultar el reporte de medición de ARANDA y la base de datos de registros del periodo solicitado, identificamos múltiples incidentes y requerimientos registrados en la herramienta, no obstante, a la fecha de la presente evaluación, no existe evidencia que respalde la medición de tiempos de respuesta y resolución discriminados para los diferentes niveles de atención (nivel 1 y nivel 2). De igual forma, resultados de operación diligenciados mediante la matriz de seguimiento de casos de mesa de servicios de TIC (SDS-TIC-FT-029) no se lleva a cabo. El LINEAMIENTO GESTION DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC - SDS-TIC-LN-001 versión 5, en su numeral 5.6. Elementos de Control del Lineamiento, define los Indicadores Clave de Rendimiento KPI para el proceso como son: 1. Cumplimiento ANS de solución, 2. Resolución de casos en Primer Nivel, 3. Resolución de casos en Nivel 2, sin embargo, a la fecha de la presente evaluación, no se están midiendo, adicionalmente, se consultan los informes de resultados mensuales remitidos y se constata que dichos indicadores KPI no se están midiendo. No medir los KPIs de un proceso tiene consecuencias como la falta de visibilidad sobre el rendimiento, la imposibilidad de tomar decisiones, la pérdida de oportunidades de mejora, y la desorganización general. Sin medición, consideramos que la entidad opera a ciegas, sin saber si está cumpliendo los objetivos específicos del proceso y los objetivos estratégicos de la entidad 3. Por último, resultados de incidentes mayores atendidos de forma mensual, lo cual es un KPI establecido a partir del lineamiento, procedimos a consultar el repositorio de SharePoint compartido, el cual a la fecha solo cuenta con 2 reportes en formato Excel del mes de enero y febrero del año 2025 respectivamente, al parecer dejo de realizarse. De otra parte, el lineamiento hace el llamado al instructivo SDS-TIC-INS-008 del año 2023, el cual define y determina el flujo de los incidentes mayores, sin embargo, dicho instructivo ya no existe en la base documental de isolucion. El auditor por su parte, procede a consultar la base de datos de registros de incidentes de ARANDA del periodo comprendido, y no es posible determinar el "criterio y/o campos" específicos que permitan identificar o reconocer los incidentes mayores. De acuerdo con lo indicado por los auditados, los casos de incidentes mayores se reconocen porque tienen asociados incidentes hijos, no obstante, a la fecha de la presente evaluación no ha sido medido dicho KPI o indicador. En consecuencia de todo lo anterior, constituye una no-conformidad a tratar.
Estado:	No Cumple

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Hallazgo	**3**
Fase	Revisión y métricas Desempeño del servicio
Criterio Evaluado	¿Se miden los tiempos de respuesta? ¿Oportunidad? ¿Se mide el cumplimiento de SLA? Cumplimiento ANS de solución – Mensual ¿Se comparan los resultados con los SLA definidos?
Dependencia Auditada:	Dirección TIC
Componente MECI relacionado	Monitoreo y supervisión
Resultado de la evaluación	En relación a la medición de indicadores generales, la dirección TIC cuenta con un profesional encargado de generar el informe mensual de gestión de la mesa de servicios y genera y emite los resultados del mes vencido. Para efectos de validación, se consulta el informe emitido del mes de septiembre 2025 y los resultados fueron los siguientes:

Resultados obtenidos: Requerimientos atendidos:1267 Incidentes:150
En incidentes: • Tiempo promedio de atención real: 115,88 horas • Tiempo promedio de solución real: 2010,51 horas
En requerimientos: • Tiempo promedio de atención real: 30,32 horas

Al consultar el informe resultado de la gestión mensual de la mesa de servicios mediante presentación elaborada, encontramos una diapositiva que presenta los resultados de cumplimiento SLA. Así mismo, presenta un gráfico donde se desglosan los incidentes y requerimientos atendidos en el periodo y en donde también permite evidenciar los resultados de cumplimiento de SLA así:
Para incidentes, el cumplimiento de atención del SLA fue del 87% y requerimientos, fue del 29% de un total de 1420 casos reportados. Se informa además que, la carencia de personal en la mesa de servicios ha conllevado al incumplimiento del SLA, lo cual constituye un primer aspecto a resaltar.

En cuanto a los casos CERRADOS, la diapositiva informa que:

- Casos Cerrados en el mes de septiembre: 1210 casos
- Total de casos atendidos: 1420,
- % de casos de Cerrados: 85%,
- promedio de tiempo de atención de requerimientos: 30 horas.

No obstante, al consultar la base de datos del periodo evaluado, identificamos las siguientes aspectos:

1. El administrador del software Aranda, debe verificar la regla automática implementada en la herramienta ARANDA que permite realizar el cambio de las transacciones en estado “SOLUCIONADO” a estado “CERRADO” el cual se aplica en base a ciertas características, pero al parecer no está funcionando, ya que el auditor identifica un volumen de transacciones de meses y años que a la fecha siguen en estado SOLUCIONADO. Lo cual conlleva a depurar todas las transacciones que presentan este comportamiento, lo anterior, conlleva a una acción de mejora.

2. En lo que refiere a los tiempos promedio de atención real y de solución real obtenidos para los incidentes, identificamos que están desfasados o por encima del umbral permitido del SLA establecido, toda vez que un incidente por definición es una acción inmediata apague incendio para mitigar la afectación presentada por tal medida se debe cumplir los ANS de negocio establecidos, y esto no está ocurriendo. Por ejemplo de los 150 incidentes atendidos en el mes de septiembre, el tiempo promedio de atención real fue de: 115,88 horas y el tiempo promedio de solución real fue de: 2010,51 horas, lo cual está incumpliendo el ANS pactado. Este aspecto no está siendo tratado al interior del proceso y se afirma que esta situación se debe a que no cuentan por persona suficiente para atender la demanda, así mismo, la mesa de servicios TI, tiene horario de atención de 6 am a 6pm de lunes a viernes, fuera de esta franja de horario los incidentes que se presenten serán atendidos hasta el día siguiente o el día hábil. Lo cual afectada los tiempos de atención, solución y los ANS pactados, Dicha situación es conocida por el equipo de TIC, sin embargo, no se han tomado los correctivos o medidas del caso.

A continuación, se presenta un análisis general realizado por el auditor, haciendo uso de la base la información suministrada denominada: 01-10-24 - 14-10-25.xls

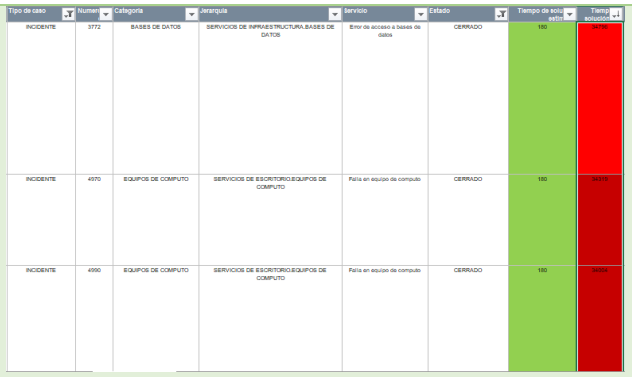
Estado	INCIDENTE	REQUERIMIENTO	Total general
Cerrado	2287	14513	16800
EN CURSO	56	102	158
REGISTRADO	1	3	4
SOLUCIONADO	10	5	15
SUSPENDIDO	2	13	15
Total general	2356	14636	16992

De acuerdo con los resultados de la tabla dinámica elaborada, identificamos que se hizo el cierre o se pasó a estado “CERRADO” 2287 registros, no obstante, siguen existiendo a la fecha casos en estado “SOLUCIONADO” que de acuerdo con la regla configurada no han cambiado de manera automática al estado “CERRADO”.

De otra parte, de los 2287 incidente CERRADOS, hacemos el análisis correspondiente a partir del “**Cumplimiento de Solución de SLA**” como se refleja en la siguiente tabla.

	INCIDENTE			Total INCIDENTE
Estado	Cumplio	No Cumplio	(en blanco)	
Cerrado	680	1545	62	2287
SOLUCIONADO		10		10
Total general	680	1555	62	2297

Los resultados, permiten identificar que existen 1545 incidentes en estado “CERRADO”, lo cual corresponde a un porcentaje del 68% del universo, no obstante, encontramos 1545 incidentes que “incumplieron el SLA”, ya que tiene un promedio de solución de 2645 horas en función del SLA establecido de 180 minutos.
Anexo captura de la tabla que contiene 3 registros o incidentes donde el SLA está desbordado.



Tipo de caso	Numero	Categoria	Jerarquia	Servicio	Estado	Tiempo de solucion en horas	Tiempo solucion en h
INCIDENTE	3772	BASES DE DATOS	SERVICIOS DE INFRAESTRUCTURA.BASES DE DATOS	Error de acceso a bases de datos	CERRADO	180	34356
INCIDENTE	4970	EQUIPOS DE COMPUTO	SERVICIOS DE ESCRITORIO.EQUIPOS DE COMPUTO	Falla en equipo de computo	CERRADO	180	34315
INCIDENTE	4990	EQUIPOS DE COMPUTO	SERVICIOS DE ESCRITORIO.EQUIPOS DE COMPUTO	Falla en equipo de computo	CERRADO	180	34304

A la fecha de la presente evaluación, el KPI o indicador de “cumplimiento de SLA” se está midiendo, sin embargo, los resultados demuestran incumplimiento del indicador, de acuerdo con todo lo anterior, constituye una no-conformidad a tratar.

Estado	No cumple

Hallazgo	**4**
Fase	Identificación e investigación Herramientas y mecanismos de monitoreo
Criterio Evaluado	¿Se realiza registro de incidentes tan pronto como sea reportado o detectado el incidente o requerimiento, incluyendo fecha, hora y descripción inicial? ¿Se realiza monitoreo de sistemas y servicios para detectar incidentes proactivamente? ¿Las herramientas generan alertas automáticas en caso de falla o degradación? ¿Se mantiene un registro histórico de los datos de monitoreo?
Dependencia Auditada:	Dirección TIC
Componente MECI relacionado	Gestión de Riesgos Monitoreo y supervisión
Resultado de la evaluación	Al particular se informa que: 1. Se cuenta con diferentes herramientas de monitoreo propias del fabricante y otras de uso libre establecidas por los especialistas para la infraestructura y los servicios TIC, se cuenta con profesionales o especialistas en cada frente tecnológico (redes, servidores, motores de bases de datos, nube, infraestructura, seguridad, servicios) y que de acuerdo con su experticia, responden a las necesidades y eventualidades del servicio y en caso de detectarse una falla masiva como resultado del monitoreo de la red y servicios, los agentes de mesa de servicios (calldispachers) deben realizar la creación el caso (incidente) y realizan la categorización en el aplicativo ARANDA. Para efectos de comprobación, el auditor solicito identificar los casos que fueron registrados en ARANDA software producto del monitoreo de la red y servicios, sin embargo, identificamos que dicha categoría no existe, por lo que se desconoce el volumen de incidentes que han sido registrados bajo este criterio. 2. De otro lado, se informa que el canal de recepción de incidentes y requerimientos establecido es mediante: correo electrónico, llamada telefónica a la (linea55),chatbot de TEAM, se cuenta actualmente con un equipo humano de 3 personas, por consiguiente, cuando la demanda o volumen de casos es alto, la atención puede tomar más de 2 horas. Se informa además que, desde el momento que se reportan los casos hasta la creación en ARANDA, transcurren 2 horas. Es importante mencionar que el

canal de CHATBOT es desconocido para los colaboradores de la entidad es por eso que al identificar los casos (incidentes y requerimientos) resultado de la categorización en la base de datos suministrada, no existen casos.

3. Por ultimo más crítico, se informa que en la actualidad los canales de atención solo operan de lunes a viernes en horario de 6 am a 6pm, fuera de esta franja los incidentes que se presenten serán atendidos hasta el día siguiente o el siguiente día hábil, lo cual afectada los tiempos de atención, solución y los ANS pactados, Dicha situación es conocida por el equipo de TIC, por consiguiente, los incidentes que presentan el fin de semana no son registrados de manera inmediata y conlleva el registro el primer día de la semana hábil. Dicha situación o debilidad, se ve reflejada en los reportes o informes mensuales, toda vez que los tiempos de atención se están incumpliendo en comparación con los ANS establecidos, dicha repercute en la insatisfacción del usuario y la indisponibilidad de los servicios afectado a continuidad del servicio. Dicha situación se viene presentando hace más de 2 años y a la fecha no se han tomado los correctivos o medidas del caso. El incidente por definición es una acción inmediata apague incendio para mitigar la afectación presentada, por tal medida se debe cumplir los ANS de negocio establecidos, y esto no está ocurriendo. Por ejemplo: En el mes de septiembre 2025, se ha atendido 150 incidentes, el tiempo promedio de atención real fue de: 115,88 horas y el tiempo promedio de solución real fue de: 2010,51 horas, lo cual está incumpliendo el ANS pactado.

4. En cuanto a las herramientas de monitoreo que generan alertas automáticas en caso detectar una falla o degradación del servicio, se informa que, en el caso del servicio de la nube de Azure, cuenta con la funcionalidad de reportar, se cuenta con IQCLOUD, que corresponde a la herramienta para la gestión de los elementos de la red LAN (switches de piso), sin embargo, se informa que no todas las redes y servicios a partir de las herramientas de monitoreo propias y libres generan alertas o notificaciones. Lo cual constituye una debilidad del servicio.

En síntesis, no registrar los incidentes o requerimientos TIC tan pronto como se detectan, confirma una incorrecta gestión y respuesta, constituye un incumplimiento ya que no se cuenta con documentación adecuada, lo que a su vez imposibilita un análisis de causa raíz y la implementación de acciones correctivas, potencialmente, puede violar normativas de protección de datos o ciberseguridad al retrasar la notificación de brechas de seguridad. No realizar el registro de incidentes de servicio TIC, incumple los requisitos de normas de gestión y procedimientos establecidos para la administración de la infraestructura tecnológica y servicios, ya que se omiten pasos clave para la trazabilidad, diagnóstico, solución y mejora continua del servicio. Específicamente, se incumplen requisitos de documentación, seguimiento y control.
A su vez no realizar el monitoreo proactivo de sistemas y servicios, expone a la entidad a riesgos de seguridad (como brechas de datos y ataques cibernéticos), pérdidas financieras (por inactividad del servicio, multas o pérdida de usuarios) y daños a la reputación, esto se debe a que las vulnerabilidades o debilidades no se detectan a tiempo, lo que permite a los atacantes explotarlas, genera una respuesta tardía ante incidentes y puede causar incumplimiento normativo. De acuerdo con todo lo anterior, se constituye una no-conformidad a tratar.

Estado:	No Cumple

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Hallazgo	**5**
Fase	Preparación y prevención Análisis post-incidente y mejora continua
Criterio Evaluado	¿Se ha realizado capacitación al personal en los procedimientos de respuesta a incidentes y en el uso de herramientas? ¿Se incorporan las mejoras identificadas en los procedimientos y entrenamientos futuros?
Dependencia Auditada:	Dirección TIC
Componente MECI relacionado	Ambiente de control información y Comunicación
Resultado de la evaluación	Al particular, se informa que la mesa de servicios en la actualidad está conformada por 3 profesionales “calldispachers” (nivel 1) y 4 profesionales de “soporte en sitio” (nivel 2), que son las personas que se desplazan hasta el puesto de trabajo para tender y solucionar, sin embargo, a la fecha de la presente evaluación, se informa que no se tiene curva de aprendizaje y no se realiza inducción, toda vez que las personas que conforman el equipo hicieron parte del contrato con ETB, por consiguiente, dichas personas conocen el modo de operación de la mesa de ayuda de la SDS. En cuanto al procedimiento SDS-TIC-PR-002, este se actualizo el día 30 de septiembre del 2025. No obstante, los roles y demás actividades, no han sido divulgadas o dadas a conocer a todos los responsables del proceso. Se informa que capacitación a la fecha no se ha realizado y no se cuenta con evidencia al respecto. En cuanto a las mejoras identificadas en los procedimientos establecidos, se informa que un profesional de la dirección TIC, realiza seguimientos de los usuarios insatisfechos, dicha actividad se realiza mensualmente y su propósito consisten en verificar los resultados obtenidos de las encuesta de percepción frente al servicio TIC, insumo para determinar las razones por la cuales hubo insatisfacción por parte de los usuarios. Se explica que la fuente de información para determinar los usuarios insatisfechos es a partir de la encuesta de percepción y estos resultados se consolidan en el formato SDS-TIC-FT-057 version2. Para efectos de comprobación, el auditor solicito los reportes de usuarios insatisfechos obtenidos durante el periodo de agosto, septiembre y julio del presente año, esto con el fin de validar las estrategias o acciones de mejora definidas, al consultar el reporte del mes de se detectaron 11 reportes de insatisfacción, sin embargo, la estrategia definida no tiene control de los avances, no se sabe el estado de avance de las estrategias definidas que entre otras cosas conducen a fortalecer y capacitar a los usuarios y grupos de profesionales. En síntesis, el riesgo principal de no capacitar al personal en procedimientos de respuesta a incidentes TIC, es un aumento en la probabilidad y el impacto de las brechas de seguridad, lo que puede causar pérdidas financieras, daños a la reputación y la interrupción de las operaciones. La falta de capacitación genera errores humanos, respuestas ineficaces ante incidentes y desventajas competitivas. Dicho lo anterior, se demuestra el incumpliendo del requisito 6.3. concientización, educación y capacitación en seguridad de la información de la norma ISO/IEC 27002:2022, decreto 338 de 2022 frente al lineamientos generales en la gestión de incidentes de seguridad y la guía para la gestión de incidentes de seguridad informática - SDS-TIC-001 y se constituye una no-conformidad a tratar.
Estado:	No cumple

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

Hallazgo	**6**
Fase	Preparación y prevención Planificación del monitoreo
Criterio Evaluado	¿Se han definido, asignado roles y responsabilidades claras para el equipo de respuesta a incidentes y requerimientos? ¿Se encuentra documentado el plan de monitoreo con roles, responsabilidades y herramientas?
Dependencia Auditada:	Dirección TIC
Componente MECI relacionado	Ambiente de control información y Comunicación
Resultado de la evaluación	Si bien es cierto, en el lineamiento SDS-TIC-LN-001 para GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC en el numeral 5.1, definen los diferentes roles y responsabilidades frente al servicio, como son: usuarios del servicio TIC, mesa de servicios TIC, Soporte nivel 1, Soporte nivel 2, soporte nivel 3, gestor de incidentes y requerimientos, Gestor de conocimiento y el Analista de mesa de servicios TIC, y al realizar la comparación de las actividades que interviene o participa cada uno de estos roles a partir del procedimiento codificado: SDS-TIC-PR-002 - GESTIÓN DE INCIDENTES Y REQUERIMIENTOS, identificamos que los roles de nivel 2, nivel 3, gestor de incidentes, gestor de conocimiento y analista de mesa de servicios TIC, no cumplen ninguna función, ya que no están vinculados al procedimiento, lo cual deriva en una oportunidad de mejora De otra parte, no existe un estándar definido en la SDS, que defina y establezca las herramientas de monitoreo más convenientes, se explica que varias de las herramientas que utilizan los especialistas son de uso libre y otras son las otorgadas por el fabricante o proveedor de las diferente herramientas de gestión. En el caso de los switches de piso, se utiliza la plataforma Streamnetworks y para servicios de la nube de Azure, se utiliza otra. Sin embargo, roles, responsabilidades y herramientas estándar para el monitores de la red y servicios no está definidas. De acuerdo con lo anterior, se deriva una oportunidad de mejora frente al lineamiento y manual existentes que conlleva capacitar a todos los responsables.
Estado:	Oportunidad de mejora

El presente informe contiene la síntesis de todo el ejercicio realizado y es importante resaltar que la auditoría, implicó la revisión y evaluación de cada uno de los aspectos trazados de conformidad con el cronograma establecido, las evidencias y soportes solicitados corresponden al alcance establecido.

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

7. ASPECTOS POSITIVOS (NIA 2410 A2).

- Es importante resaltar la cordialidad y la atención prestada por los profesionales que participaron de la auditoria, mostrando un alto grado de compromiso frente a la cultura del control.
- Existe el compromiso de la dirección TIC de atender y responder a los incidentes y requerimientos del servicio TIC, ya que es una práctica de gestión esencial para minimizar el impacto negativo de las interrupciones y restaurar el servicio, en cumplimiento de lo concerniente a la política de seguridad digital y gobierno digital.
- El recurso humano que participó de la auditoria, reúne el conocimiento y la experiencia necesarias para dar respuesta a las dudas e inquietudes que se formularon.
- El recurso humano conoce las entradas y las salidas de cada uno de los procedimientos, guías e instructivos implementados y determina de forma preventiva los recursos físicos, financieros y tecnológicos que son necesarios para la operación de la mesa de servicios TIC en la entidad.

8. NO CONFORMIDADES. (NIA 2431).

8.1. Si bien es cierto, el proceso de “GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC”, define y establece en el lineamiento SDS-TIC-LN-001 V5 numeral 5.6 iindicadores Clave de Rendimiento KPI claves como son: 1. Cumplimiento ANS de solución, 2. Resolución de casos en 1er Nivel, 3. Resolución de casos en 2do Nivel, y dichos indicadores deben ser medidos y reportados mensualmente a la dirección TIC, al cotejar la información suministrada, encontramos que: 1. no existe evidencia, que respalde la medición de tiempos de respuesta y resolución discriminados para los diferentes niveles de atención (nivel 1 y nivel 2), de igual forma, resultados de operación diligenciados mediante la matriz de seguimiento de casos de mesa de servicios de TIC mediante el formato (SDS-TIC-FT-029) no se lleva acabo, 2. No se realiza “control de calidad” sobre la información registrada de incidentes y requerimientos en ARANDA software y 3. Resultados de medición del porcentaje de incidentes mayores atendidos de conformidad con el numeral 5.3.2 del lineamiento dejo de generarse, adicionalmente, el INSTRUCTIVO SDS-TIC-INS-005 PARA GESTIÓN DE INCIDENTES MAYORES DEFINIDO ya no existe, y el formato SDS-TIC-FT-056 BITÁCORA INCIDENTES MAYORES, dejó de aplicarse. En virtud de todo lo anterior, existe un incumplimiento de varios aspectos del lineamiento SDS-TIC-LN-001 y Caracterización SDS-TIC-CAR-001 por lo que hace necesario e indispensable tomar las acciones correctivas del caso.
Responsables: Dirección TIC

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)

8.2. Pese a que los tiempos de respuesta y cumplimiento de SLAs del proceso de "GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC" se miden mensualmente y se cuenta con reporte de resultados el cual fue suministrado, evidenciamos que, los resultados de: 1. tiempo promedio de atención real y de solución real obtenidos se están incumpliendo frente al ANS pactado, ya que los resultados obtenidos se encuentran por encima del umbral permitido de 180 horas para el caso de incidentes, dicho aspecto ha sido reincidente en el tiempo y no está siendo tratado al interior del proceso, se afirma por parte de los especialistas que, dicha situación obedece a que no cuenta por persona suficiente para atender la demanda, y sumado a esto el horario de atención establecido de la mesa de servicios TI, es de 6 am a 6pm de lunes a viernes, fuera de esta franja de horario los incidentes que se presenten serán atendidos hasta el siguiente día hábil, situación que afecta de manera directa los tiempos de atención, solución y los ANS pactados. En virtud de todo lo anterior, existe un incumplimiento de los numerales 5.3 y 5.6 del lineamiento SDS-TIC-LN-001, por lo que hace necesario e indispensable tomar las medidas correctivas del caso.
Responsables: Dirección TIC

8.3. Pese a que, la dirección TIC cuenta con diferentes herramientas de monitoreo para las redes y servicios propias de los fabricantes y también se hace uso de herramientas libres establecidas por los especialistas en cada frente tecnológico (redes, servidores, bases de datos, nube, infraestructura, seguridad, servicios) con las cuales se busca "detectar" eventos e incidentes proactivamente para darles solución, evidenciamos que, 1. No todos los incidentes son registrados por los especialistas o agentes de la mesa de ayuda, 2. No todos las redes y servicios TIC están siendo monitoreadas, 3. Las herramientas de monitoreo en la entidad, no están configuradas para registrar de manera automática incidentes y 4. los colaboradores o especialistas en cada frente TIC, no están capacitados para la identificación y registro, el mismo lineamiento y procedimiento no lo establece, en consecuencia, el no realizar el monitoreo proactivo de redes y servicios, expone a la entidad a riesgos de seguridad (como brechas de datos y ataques cibernéticos), pérdidas financieras (por inactividad del servicio, multas o pérdida de usuarios) y daños a la reputación, y se genera una respuesta tardía ante incidentes y puede causar incumplimiento normativo. En virtud de todo lo anterior, se constituye una no conformidad, por lo que hace necesario e indispensable tomar las medidas correctivas del caso.
Responsables: Dirección TIC

8.4. Si bien es cierto, la mesa de servicios TIC en la actualidad está conformada por 3 profesionales "calldispachers" (nivel 1) y 4 profesionales de "soporte en sitio" (nivel 2), y varios especialistas de (nivel 3), evidenciamos que, a la fecha de la presente evaluación: 1. no se existe un plan o curva de aprendizaje, 2. no se han realizado ninguna jornada de inducción o capacitación al personal sobre los procedimientos de respuesta a incidentes y el uso de herramientas, no existe evidencia al respecto y se afirma que esto obedece a que el personal de mesa de ayuda fue personal del antiguo contrato con ETB y por consiguiente conocen, 3.No existe un estándar definido para el uso de

herramientas de monitoreo de red y servicios, 4. El procedimiento SDS-TIC-PR-002, fue actualizado el día 30 de septiembre del 2025. Y contemplo cambios en roles y demás actividades, dichos cambios no han sido divulgadas o dados a conocer a todos los responsables del proceso lo que conlleva a errores humanos, respuestas ineficaces ante incidentes y desventajas competitivas. En virtud de lo anterior, existe un incumpliendo del requisito 6.3. Concientización, educación y capacitación en seguridad de la información de la norma ISO/IEC 27002:2022, Decreto 338 de 2022 frente al lineamientos generales en la gestión de incidentes de seguridad y la guía para la gestión de incidentes de seguridad informática - SDS-TIC-001 por lo que hace necesario e indispensable tomar las acciones correctivas del caso.
Responsables: Dirección TIC

9. ACCIONES PARA ABORDAR RIESGOS. (NIA 2410-A1).

9.1. Aun cuando, en el lineamiento SDS-TIC-LN-001 en su numeral 5.3 establece, que se debe tomar una muestra representativa diaria de al menos el 15% de los registros solucionados para el control de calidad, y que los incidentes y requerimientos en estado “SOLUCIONADO” una vez superado el tiempo de retención u obteniendo el aval del usuario final, debe haber un “cierre automático” en la herramienta ARANDA SOFTWARE, sin embargo, evidenciamos que control de calidad no se hace y regla implementada en el aplicativo no está funcionado en su totalidad, ya que siguen existiendo registros de incidentes y requerimientos en estado SOLUCIONADO, situación que afecta el desempeño y la eficiencia del proceso, en consecuencia, se deben tomar las medidas necesarias que permitan fortalecer este aspecto, permitiendo ajustar la herramienta y depurar los registros.
Responsables: Dirección TIC

9.2. Pese a que, existe un lineamiento codificado: SDS-TIC-LN-001 para la GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC y en su numeral 5.1, definen los diferentes roles y responsabilidades frente al servicio, como son: usuarios del servicio TIC, mesa de servicios TIC, Soporte nivel 1, Soporte nivel 2, soporte nivel 3, gestor de incidentes y requerimientos, Gestor de conocimiento y el Analista de mesa de servicios TIC, evidenciamos que, dichos roles no tiene relación y no cumplen o no están vinculados con las actividades del procedimiento codificado: SDS-TIC-PR-002 - GESTIÓN DE INCIDENTES Y REQUERIMIENTOS, en consecuencia, existe una debilidad y por consiguiente se deben tomar las medidas necesarias que permitan fortalecer dicho aspecto.
Responsables: Dirección TIC

9.3. Pese a que se cuenta con un proceso definido para la “GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC”, que contempla (lineamiento, procedimiento, guía, formatos) aprobados/publicados en isolucion, y en respuesta a la operativización del mismo, se cuenta la base general de registros de incidentes reportados en ARANDA

Software, identificamos que: 1. no existe evidencia suficiente que demuestre los ejercicios de "análisis causa raíz" en búsqueda de comportamientos o patrones similares o reincidentes, 2. la base de conocimiento o módulo de la KDB de ARANDA software para el manejo de incidentes conocidos y el módulo de autogestión para registro de incidentes mediante "Chatbot" del aplicativo TEAMS no están siendo usados, en virtud de lo anterior, existe una debilidad del proceso de gestión de incidentes definido, por lo que hace necesario e indispensable tomar las acciones de mejora del caso.
Responsables: Dirección TIC

10. CONCLUSIONES. (NIA 2410-A1).

- La Dirección TIC, ejerce el liderazgo y define a partir del lineamiento, procedimientos, guías y formatos, la gestión eficiente de los incidentes y requerimientos del servicio de conformidad con la normatividad y las buenas prácticas de gestión de servicio existentes.

- La dirección TIC, deberá mejorar la eficacia y eficiencia del proceso de gestión de incidentes y requerimientos de servicios TIC en operación, por medio de la adopción de los hallazgos presentados en el presente informe y que deberán corresponder a la implementación de las acciones correctivas, preventivas y de mejora, así mismo se detallan las principales fortalezas y debilidades detectadas.

- La estructura de roles y responsabilidades definida frente a la gestión de incidentes, requerimientos y el monitor de la red y los servicios TIC de la entidad, deberán ser dadas a conocer a todas las partes interesadas y se deben poner en práctica.

- La primera recomendación sugiere implementar un plan que permita priorizar los incidentes de acuerdo con el nivel de criticidad y que se automatice la comunicación para agilizar la respuesta, así como analizar de manera continua las causas raíz que buscan la mejora proactiva, todo esto apoyado por herramientas tecnológicas con las que cuenta la entidad.

- Seguir el lineamiento, procedimiento, formatos y guías establecidos para la gestión de incidentes de cara a la detección, investigación, resolución y documentación de incidentes, asegura la respuesta consistente y eficiente hacia el usuario final y generando satisfacción del cliente frente al servicio brindado.

- De cara a la mejora continua, se debe seguir realizando el análisis de los incidentes resueltos o cerrados, lo cual proporciona información valiosa para la identificación de ciertos patrones o comportamientos y prevenir problemas recurrentes a futuro.

- Se recomienda definir, establecer claramente los niveles de severidad de los incidentes para priorizar las respuestas y asignar recursos de manera adecuada, si bien es cierto, dichos niveles se encuentran implementados en la aplicación ARANDA software, los agentes (Calldispachers) de primer nivel y los especialistas de segundo nivel no han sido capacitados, y desconocen los procedimientos, guías y con ello los niveles de severidad y priorización definidos, por lo cual los diferentes casos han sido clasificados de manera incorrecta.

- Es necesario implementar y adoptar un marco de trabajo como es el caso de ITIL, para crear procesos de gestión de incidentes estandarizados.

- Es necesario automatizar la comunicación y utilizar herramientas existentes de gestión y monitoreo para las diferentes alertas y notificaciones, asegurando que las personas idóneas de la operación sean informada de manera oportuna o inmediata, facilitando la colaboración y coordinación de cara a la atención rápida frente a los incidentes presentados.

- Es necesario que mesa de ayuda o helpdesk (línea 55), amplié su horario de atención de incidentes y requerimientos, toda vez que el horario actual de atención es de lunes a viernes de 6 am a 6 pm, lo cual no lo hace eficiente y ágil, ya que incidentes que se presentan fuera de los horarios establecidos, se les atiende de forma tardía.

- Se recomienda mantener registros detallados de todos los incidentes y requerimientos, así como realizar análisis post-incidente para identificar causas raíz y áreas de mejora, ya que no todos los incidentes presentados son documentados y el análisis de causa raíz no se lleva a cabo.

- Se recomienda capacitar al personal o equipo de respuesta de incidentes y requerimientos, asegurando que el que tengan la capacitación adecuada, incluyendo la fase de recopilación de información durante las investigaciones de los incidentes materializados

- De acuerdo con el presente informe, se comunican los resultados y comparten los hallazgos con los profesionales designados para fomentar una cultura de prevención y mejora.

- A partir del lineamiento SDS-TIC-LN-001 - GESTIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIOS TIC, se definen los diferentes KPI o indicadores de desempeño del proceso de gestión de incidentes y requerimientos, no obstante, varios de ellos se no cumplen el umbral o meta y otros no se miden o

cual conlleva a una no conformidad, ya que existe ausencia de seguimiento y control, para lo cual es indispensable implementar las acciones correctivas que haya lugar.

- Es necesario enfatizar y recalcar que se deben redoblar los esfuerzos definiendo estrategias de comunicación, permitiendo asegurar el conocimiento y apropiación de todos los especialistas encargados de la gestión de incidentes y requerimientos.

11. PLAN DE MEJORAMIENTO (NIA 2500).

Como resultado de la auditoría, el proceso deberá cumplir con el lineamiento establecido por la dirección de planeación institucional y calidad para la elaboración del plan de mejoramiento que haya lugar, con el fin de realizar el tratamiento adecuado a los riesgos, incluyendo las actividades del ciclo PHVA y de ser necesario realizar mesas de trabajo cuando los acciones para abordar los riesgos involucren otros procesos o dependencias. Nota: Sera responsabilidad de los referentes elaborar el plan de mejoramiento adecuado que responda a las no-conformidades y oportunidades de mejora identificadas.

12. ANEXOS.

Corresponde a los papeles de trabajo utilizados en cada mesa de trabajo realizadas y que serán remitidos a las partes interesadas para el análisis de cada uno de los casos.

- LISTADEVERIFICACION AUDITORIADEGESTIONTIC.xlsx

NOMBRE (S) Y APELLIDO (S) Y FIRMA (S) DE AUDITOR (ES).

Firmado digitalmente por Francisco Javier Pinto

FRANCISCO JAVIER PINTO GONZÁLEZ

APRUEBA JEFE OFICINA DE CONTROL INTERNO.

Firmado digitalmente por OLGA LUCIA VARGAS COBOS

OLGA LUCIA VARGAS COBOS

*La nomenclatura de cada numeral del informe corresponde a las Normas Internacionales de Auditoría (NIA)