acueducto
AGUA Y ALCANTARILLADO DE BOGOTÁ

MEMORANDO INTERNO

1050001-2023-0431

Bogotá, 22 de noviembre de 2023

PARA: Ing. Diego Fernando Naranjo – Gerente de Tecnología,
Ing. Adriana del Pilar Guerra – Dirección de Servicios de Informática

DE: Oficina de Control Interno y Gestión

ASUNTO: Remisión Informe Final 7. MPFT Gestión TIC.

Respetados Ingenieros:

En cumplimiento con el Programa Anual de Auditoría 2023 de la Oficina de Control Interno y Gestión aprobado por el Comité de Auditoría de la Junta Directiva, remitimos el Informe Final correspondiente a la auditoria referida en el asunto.

Recordamos que las áreas involucradas en las Observaciones del presente informe tendrán diez (10) días hábiles para hacer llegar los respectivos planes de mejoramiento a la OCIG de acuerdo con el procedimiento MPCS0202P - Mejoramiento Continuo, es decir a más tardar el próximo 07 de diciembre del 2023.

Así mismo, se les solicita informar a la Oficina de Control Interno, la gestión que se dé a las recomendaciones sugeridas en el presente informe ya sea mediante correo electrónico y/o memorando, a más tardar el próximo 07 de diciembre del 2023.

Finalmente, adjuntamos la encuesta de percepción para su diligenciamiento por parte de la Gerente y sus directores y el posterior envío al correo ldvalbuena@acueducto.com.co, a más tardar el próximo 28 de noviembre del 2023.

Cordialmente,

Firmado por MARIA NOHEMI PERDOMO RAMIREZ
el 22/11/2023 a las 09:12:41 COT

MARIA NOHEMÍ PERDOMO RAMIREZ
Jefe Oficina de Control Interno y Gestión

Aprobó y Revisó: Nohemí Perdomo
Proyectó: Paola M

INFORME FINAL DE AUDITORÍA		
ID - NOMBRE DE LA AUDITORÍA	**7. MPFT GESTIÓN TIC**	**1050001-2023-0431** **N° Consecutivo**
UNIDAD AUDITADA	Gestión Mesa de Ayuda Atención a Vulnerabilidades Plan Maestro de Tecnología Seguridad de la información	
ÁREA(S) RESPONSABLE(S)	Gerencia de Tecnología Dirección de Servicios Informáticos Seguridad de la Información	

Fecha Reunión de Inicio: 31 de julio de 2023

Fecha Reunión de Cierre: 20 de noviembre de 2023

1. OBJETIVO GENERAL DE LA AUDITORÍA.

Evaluar el proceso MPFT-Gestión TIC a través de la verificación del cumplimiento de la normatividad aplicable en el desarrollo de los procedimientos que soportan la prestación de los servicios de TI, así como la participación en la innovación de los sistemas de información de la EAAB-ESP.

2. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA.

- Verificar que las políticas de operación, actividades y puntos de control de la Gestión de la Mesa de Ayuda se ejecuten conforme a lo señalado en el subproceso de Gestión de servicios Informáticos.
- Comprobar que el desarrollo de las actividades del procedimiento MPFT0201-Gestión Atención de vulnerabilidades se cumplan, acorde a lo establecido en el procedimiento y normatividad aplicable.
- Evidenciar el cumplimiento de lo establecido en las políticas, actividades y demás normatividad asociada con Seguridad Digital.
- Evidenciar el cumplimiento en la implementación y ejecución de lo establecido en las políticas, actividades y demás normatividad asociada con el Plan Maestro de Tecnología (PMT).
- Validar la eficiencia y eficacia de la incorporación de módulos o actualizaciones en el aplicativo SAP

3. ALCANCE DE LA AUDITORÍA.

La auditoría validará la gestión de la vigencia 2022 hasta junio de 2023 del proceso Gestión TIC y las responsabilidades de los subprocesos encargados de la implementación de la Política de Seguridad Digital y ejecución de los procedimientos de la atención de vulnerabilidades informáticas, Gestión Mesa de Ayuda, Plan Maestro de Tecnología (PMT) e incorporación o actualización del aplicativo SAP, conforme a los lineamientos establecidos por MINTIC, MIPG (FURAG) y demás normatividad aplicable.

4. MARCO NORMATIVO DE LA AUDITORÍA.

- **Resolución 305 del 2008** Políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad,

democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

- **Resolución 740 del 2018** Política General de Seguridad y privacidad de la Información en la Empresa de Acueducto y Alcantarillado de Bogotá EAAB - EPS.
- **Ley 1266 del 2008** "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos".
- **Ley 1581 del 2008** “por la cual se dictan disposiciones generales para la protección de datos personales”, del Congreso de la Republica.
- **Resolución 1236 del 2018** Política de tratamiento de Datos Personales para la EAAB-ESP.
- **Resolución 520 del 2019** Por medio de la cual se definen los Objetivos de Control que se deben aplicar en el uso de la Información de la EAAB.
- **Decreto 338 del 2022** "Por el cual se adiciona el Titulo 21 a la parte 2 de Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
- **Resolución 500 del 2021** “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- Acuerdo 822 del 2021 Por medio del cual se dictan los lineamientos para la promoción del ciclo virtuoso de la seguridad, el uso y aprovechamiento de los datos en Bogotá.
- **Decreto 1263 del 2022** Por el cual se adiciona el título 22 a la parte 2 del libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, con el fin de definir lineamientos y estándares aplicables a la transformación digital pública.
- **Decreto del 767 del 2022** 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 libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.
- **Resolución 460 del 2022** Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- **Decreto 415 del 2016** "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones."
- **Decreto 1078 del 201**5 Decreto Único Reglamentario del Sector De Tecnologías de la Información y las Comunicaciones.
- **Decreto 221 del 2023** Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital, se deroga el Decreto Distrital 807 de 2019 y se dictan otras disposiciones.
- **Norma Técnica Colombiana NTS-ISO/IEC 200000-1** Tecnología de la información, Gestión del Servicio Capitulo 8.
- Guía para la Administración del Riesgo y el Diseño de Controles en las entidades públicas V5 del 2020.
- COMPES 3854 de 2016 Política Nacional de Seguridad Digital
- Guía No. 2 Elaboración de la política general de seguridad y privacidad de la información
- Plan Estratégico de Tecnologías de Información (PETI) de MinTIC 2023-2026
- Política de Gestión: Política de Seguridad y Privacidad de la información V3 del 2018
- ITIL V4 Fundamentos.
- ITIL V4 CDS, Crear, Entregar y Apoyar
- Procedimiento MPFT- 03- 02 Gestión Mesa de Ayuda
- Procedimiento MPFT- 02- 01 Atención de Vulnerabilidades Informáticas
- Procedimiento MPFT- 02- 03 Conexión de Equipos de Cómputo

5. DESARROLLO DE LA AUDITORÍA.

La Empresa a través de la Oficina de Control Interno y Gestión – OCIG por medio de la metodología de priorización enfocada en riesgos para la construcción del Plan Anual de Auditorías 2023 programó la Auditoría No. 7. MPFT – Gestión TIC, la cual se ejecutó conforme a los lineamientos establecidos en el marco de referencia MECI-COSO 2013.

Los auditores en la fase de planeación ejecutaron el alistamiento de la auditoría mediante la recopilación y análisis de información, apoyados en las diferentes herramientas dispuestas por la Empresa como: Página web, File Server, Aplicativo Archer, Mapa de Procesos, Acuerdos de Gestión PGE 2020-2024, Sistema de Información de Normalización Técnica, Lotus Notes entre otros, con el fin de establecer el objetivo general, los específicos y el alcance del ejercicio auditor, así como la identificación de los criterios de evaluación y la formulación del plan de trabajo.

En la fase de ejecución se identificaron, analizaron, evaluaron y documentaron las evidencias que soportan los resultados de la auditoría, para ello se solicitó información a los profesionales responsables designados por los directores que conforman el equipo de trabajo de la Gerencia de Tecnología y se programaron sesiones de trabajo presenciales y virtuales para aplicar los procedimientos de auditoría pertinentes de conformidad con el objetivo y alcance del ejercicio auditor.

Adicionalmente, se realizaron verificaciones con profesionales pertenecientes a otras gerencias de la Empresa encargados de gestionar políticas en el marco de MIPG y también con encargados de gestionar riesgos en la Empresa.

5.1 Análisis General

Lineamiento estratégico
Se identificó que en los años 2021 y 2022 el proceso de Gestión TIC con la planificación y ejecución del Plan Maestro de Tecnología contribuía y se encontraba alineado con el objetivo estratégico 3 Reputación y Liderazgo, para el 2023 la ejecución del plan se encuentra asociado al proceso MPEE – Direccionamiento Estratégico y Planeación / 03 – Modelo Integrado de Planeación y Gestión pese a que la ejecución y seguimiento está a cargo de la Gerencia de Tecnología.

Gestión de Riesgos y Oportunidades
Se analizó la matriz de riesgos asociados al proceso de Gestión TIC, evidenciando riesgos de Gestión, Corrupción y de seguridad de la información.

En el desarrollo de la auditoría, se identificaron los siguientes riesgos y causas inherentes al SGSI y al proceso de Gestión TIC:

Riesgo (Evento)	Tipo de Riesgo	Causa	Consecuencia
Pérdida de la confidencialidad, integridad o disponibilidad de la información en los sistemas que soportan las operaciones de la EAAB por la incorrecta	Seguridad información	➢ No mitigar oportunamente las vulnerabilidades detectadas en el escaneo ➢ Fallas en las herramientas de control (antivirus, Firewall, PAM etc) ➢ Ataques Cibernéticos	➢ Detrimento económico por sanciones, multas o demandas por entes de control o por ciudadanos ➢ Afectación en la imagen o reputación de la entidad **Consecuencia Positiva**

Riesgo (Evento)	Tipo de Riesgo	Causa	Consecuencia
aplicabilidad de controles se seguridad lógica y física.		➢ Fuga de información por, falta de conciencia de colaboradores ➢ No involucrar las diferentes áreas para fortalecer la seguridad física en las áreas e instalaciones de la entidad ➢ No todos los sistemas de información o herramientas tecnológicas son administradas por tecnología ➢ Uso de Software sin licencia y posibilidad de recibir actualizaciones o soporte del fabricante.	➢ Establecer procedimientos que aseguren la aplicabilidad de los controles de una manera sistemática
Retraso en la prestación de los servicios por falla en la funcionalidad de los sistemas de información.	Gestión	➢ No contar con planes de contingencias o DRP de los sistemas de información críticos. ➢ Desconocer el plan de continuidad de negocio y la participación de tecnología en su ejecución. ➢ No ejecutar con periodicidad planes de contingencia para garantizar el respaldo y continuidad de la información (backup, plantas eléctricas etc.) ➢ No contar con un procedimiento para la ejecución y control de los planes de contingencia.	➢ Detrimento económico por sanciones, multas o demandas por entes de control o por ciudadanos ➢ Afectación en la imagen o reputación de la entidad
Inadecuada identificación de las necesidades y oportunidades de innovación tecnológica para establecer el Plan Estratégico de Tecnología por no ejecutar las actividades conforme a los lineamientos establecidos por la Política de Gobierno Digital.	Gestión	➢ No contar con un Marco de Referencia de Arquitectura Empresarial ➢ No comprender y/o ejecutar los lineamientos de Gobierno Digital para la elaboración del PETI (PMT) ➢ Falta de participación y/o apoyo de la alta dirección	➢ Detrimento económico por sanciones, multas o demandas por entes de control ➢ Orientar recursos a proyectos o iniciativas que no apoyan a la estrategia y modelo operativo de la Entidad

Tabla 1. Riesgos de Gestión y Seguridad de la información identificados por la Auditoría

Nota: Las causas identificadas nacen sin tener en cuenta los controles existentes, tener presente que el SGSI establece lineamientos y controles a todos los activos de información.

Conforme con los lineamientos establecidos por MINTIC, MIPG (FURAG), durante la auditoría se realizó sesión para aclarar la participación del proceso Gestión TIC en la Dimensión 3. Gestión de Valores con Resultados, numeral 3.3 Relación Estado Ciudadano, asociado a la política 3.3.4 Gobierno Digital, entendiendo ésta como la directriz nacional que permite la transformación digital pública a través del aprovechamiento de las TIC para generar confianza entre la EAAB-ESP y el público de referencia; se pudo establecer que el proceso en mención incluye diversas actividades y acciones que permiten operar el proceso, ejemplo de ello es la Política de Seguridad y Privacidad de la Información, el procedimiento MPFT0204 - Detección y Atención Incidentes de Seguridad de la Información y la Atención de Vulnerabilidades Informáticas entre otros; así mismo las actividades operativas para dar cumplimiento a lo anterior, se vienen adelantando con actividades de Adecuación y transformación de los contenidos en el portal corporativo EAAB-ESP e Identificando los trámites que se implementarán con los servicios ciudadanos digitales del Plan de Gobierno; con respecto a el Líder Seguridad de la Información, evalúa el cumplimiento de los controles para garantizar la política en mención y producto de ello se producen alertas tempranas que son soportadas y tratadas por la Dirección de Servicios Informáticos.

Con relación a la norma técnica NTC 5854 accesibilidad web, también se encuentra incluida en el plan de gobierno, sin embargo, la norma debe complementarse a mejorar los contenidos de la página web a las personas que presentan discapacidad de diferentes tipos.

La Norma NTC 6047 Accesibilidad al medio físico espacios al servicio al ciudadano en la administración pública, hace referencia a condiciones técnicas locativas para el fácil ingreso de ciudadanos con discapacidad física a las instalaciones públicas, documento que no es de responsabilidad de Gestión TIC, no obstante, en el recorrido de las instalaciones de nivel central se pudo observar que la empresa tiene las condiciones técnicas adecuadas para la garantizar el cumplimiento de la presente norma.

A continuación, se desarrollan cada uno de los objetivos específicos planteados para esta auditoría.

5.2 Verificar que las políticas de operación, actividades y puntos de control de la Gestión de la Mesa de Ayuda se ejecuten conforme a lo señalado en el subproceso de Gestión de servicios Informáticos.

En el ejercicio de la auditoría, se analizó el procedimiento MPFT0302P- Gestión de Mesa de Ayuda v1, el Anexo 2 Condiciones Técnicas y de Servicio numeral 6.5.1 Mesa de servicios y Soporte sitio del contrato 1-05-26500-0848-2021 subscrito entre EAAB-ESP y Unión Temporal PS-UN 2021 contratista que ejecuta las actividades de la Gestión de la Mesa de ayuda. Identificando lo siguiente:

Las actividades que actualmente ejecuta la Mesa de ayuda son conforme al procedimiento registrado en el mapa de procesos, no obstante, este documento no refleja la totalidad de las actividades y políticas de operación con las que actualmente se está ejecutando el procedimiento, sin embargo, se evidenció el borrador del procedimiento en su v2.

Del procedimiento se validó el cumplimiento del objetivo, políticas de operación, actividades y la aplicabilidad de las buenas prácticas ITIL conforme a lo establecido en el Anexo 2 del contrato 1-05-26500-0848-2021, y como lo indica la Norma Técnica Colombiana NTS-ISO/IEC 200000-1 Tecnología de la información, Gestión del Servicio Capitulo 8.

Para validar la política No. 1 de operación que indica: *"Las recepciones de los servicios y solicitudes a la mesa de ayuda, se recibirán por vía telefónica, a través de la extensión 7777, SRM y correo electrónico."* Se procedió a identificar las fuentes de información de cada uno de los canales de comunicación habilitados (telefónico y correo electrónico) y se confrontan con los tickets generados en la herramienta de gestión (BMC Remedy), para lo anterior se tomó una muestra de la gestión realizada en el último trimestre del 2022 y primer semestre del 2023.

Para identificar cuantos tickets se crearon por cada canal activo se ejecutaron 2 métodos.

- De cada data (datos capturados por un sistema de información) se identificó las peticiones recibidas en los periodos que comprenden el último trimestre del 2022 y primer semestre del 2023, de lo anterior, se toma la siguiente muestra:

INFORMACIÓN DATAS POR CADA CANAL

Año	Periodo / Canal	Telefónico	Correo	Total Recibidos	**Tickets Registrados	Diferencia
2022	16 Oct al 15 Nov	2.886	611	3.497	4.668	1.171
	16 Nov al 15 Dic	3.292	673	3.965	5.539	1.574
2023	16 May al 15 Jun	2.987	566	3.553	4.851	1.298
	16 Jun al 15 Jul	2.538	503	3.041	4.285	1.244

Figura 1. Solicitudes recibidas por cada canal activo Vs Registro de los casos en la herramienta de gestión

***Tickets Registrados:** Corresponde a la data de la herramienta de gestión con la cantidad de tickets creados por los agentes de la Mesa de Ayuda, con la respectiva tipificación según el canal por el cual se recibió la petición del colaborador.*

Esta auditoría identificó que la Dirección de Servicios Tecnológicos adelanta el desarrollo y parametrización para poner en producción el canal web, por consiguiente, no existe una data correspondiente a este canal.

- De la data de la herramienta de gestión (BMC Remedy) se identifica el campo de "Fuente reportada", en este se registra el canal por el cual se recibió la petición del colaborador (teléfono, correo electrónico, web) del ejercicio se evidenció lo siguiente:

INFORMACIÓN TICKETS REGISTRADOS EN LA HERRAMIENTA POR CANAL DE RECEPCIÓN

Año	Periodo / Canal	Telefónico	Correo	AutoServicio	Otros	Tickets Registrados	Observación Auditoría
2022	16 Oct al 15 Nov	2.937	1.410	305	16	4.668	*4 Registros duplicados en la misma data *La WO0000001438472 duplicada con la data del 16 Abr al 15 May del 2023, misma solicitud, mismo correo que la originó, cambia la fecha de creación
	16 Nov al 15 Dic	3.455	1.715	354	15	5.539	*2 Registros duplicados en la misma data
2023	16 May al 15 Jun	3.050	1.428	367	6	4.851	*43 Registros duplicados en la misma data * 4 Registros duplicados en la data del 16 Abr al 15 May *2 Registros duplicados en la data 16 Jun al 15 Jul
	16 Jun al 15 Jul	2.552	1.297	431	5	4.285	* 1 Registro duplicado en la misma data *2 Registros duplicados en la data del 16 May al 15 Jun

Figura 2. Clasificación de los Tickets registrados en la herramienta de gestión por canal de comunicación

Nota 1: *El análisis de las datas se hizo sobre las enviadas después de la sesión del 14 septiembre donde la auditoría manifestó inconsistencias en la data enviada inicialmente.*

Nota 2*: Las mediciones internas (OLA- ITIL V3) deben estar contempladas para el ANS del servicio, por consiguiente, esta medición no debe modificarse.*

Al validar las diferencias en la cantidad de llamadas y correos recibidos frente a lo registrado en la herramienta de gestión, se identificó 115 casos duplicados entre el último trimestre del 2022 y primer semestre del 2023, el área auditada informa que podría ser por casos reabiertos, por lo anterior se solicita validar la traza de la Orden de trabajo (solicitud) WO0000001448548 en la herramienta de gestión, y el incidente INC000001106280, pero no se evidenció en ningún caso que presentara una reapertura.

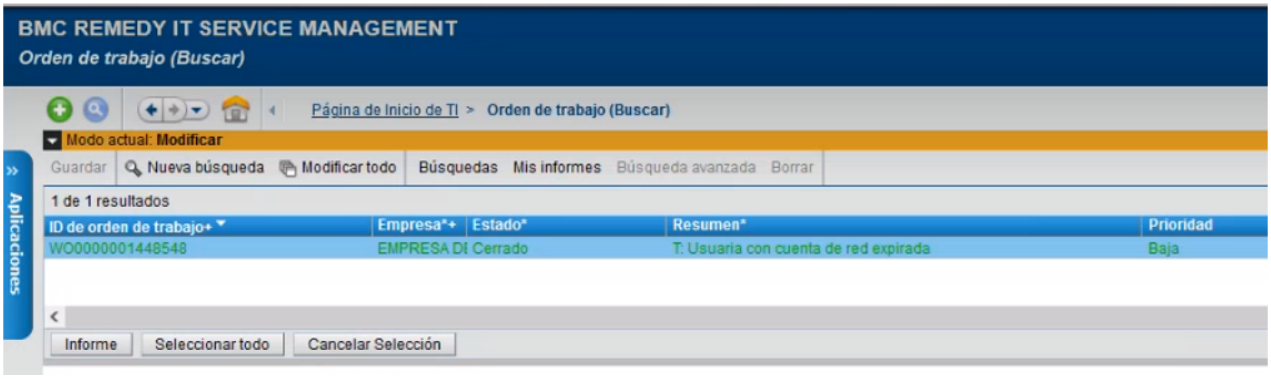


Figura 3. Revisión de la traza de una Orden de trabajo

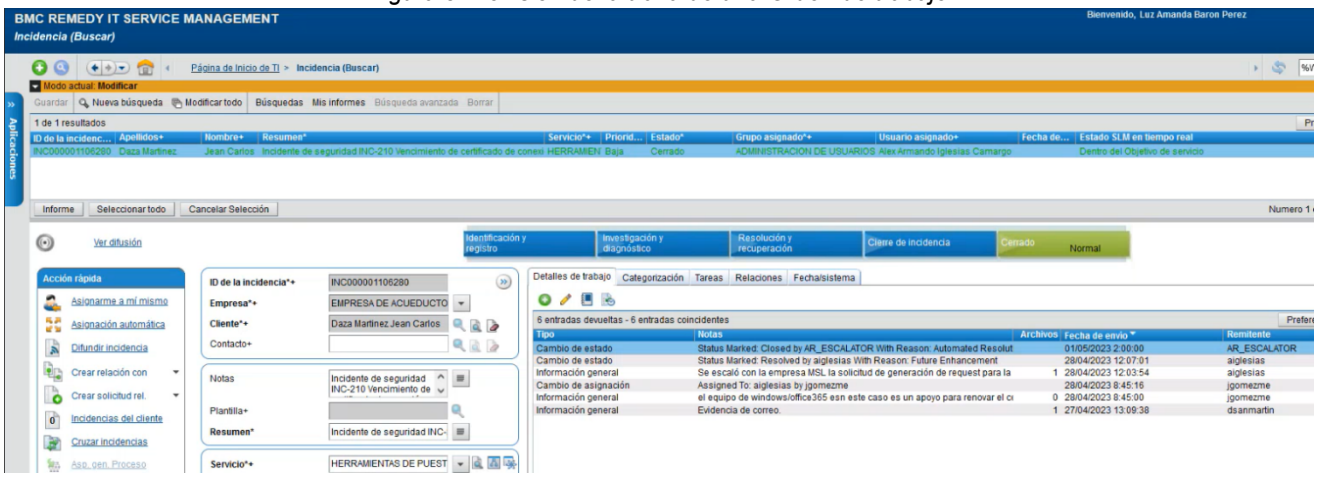


Figura 3.1 Revisión de la traza de un incidente

Adicional a lo anterior, para el periodo del 16 de octubre al 15 de noviembre del 2022 (data 14), en telefonía se crearon 51 tickets más (en la herramienta de gestión BMC Remedy) de los registrados en la data de telefonía (Isabel) y 799 más por correo electrónico, menciona el área auditada que por llamada se reciben más de una solicitud de diferentes colaboradores y el tema de correo electrónico es de validar la causa. Lo anterior permite identificar que no se ejecutan controles que permitan garantizar la calidad de lo registrado en la herramienta de gestión por los agentes de la mesa de ayuda e identificar de manera oportuna las desviaciones en la correcta ejecución de las actividades.

Para efectos de corroborar que los casos son recibidos únicamente por los canales autorizados según lo registra en las políticas de operación del procedimiento, se evidenció lo siguiente:

Cuenta de Fuente Reportada	Etiquetas		
Etiquetas de fila	Incidente	Orden de Trabajo	Total general
Autoservicio		300	300
Autosesrvicio	5		5
Correo Electronico	90	1320	1410
Entrada Directa	13	2	15
Otro		1	1
Teléfono		2199	2199
Telfono	738		738
Total general	**846**	**3822**	**4668**

Cuenta de Fuente Reportada	Etiquetas		
Etiquetas de fila	Incidente	Orden de Trabajo	Total general
Administración de Sistemas	1		1
Autoservicio		354	354
Correo Electronico	129	1586	1715
Entrada Directa	10	1	11
Ótro	3		3
Teléfono		2719	2719
Telfono	736		736
Total general	**879**	**4660**	**5539**

Figura 4. periodos 16 octubre al 15 noviembre y 16 de noviembre al 15 de diciembre de 2022.

Se identifica otros canales utilizados para el registro de las peticiones los cuales no se encuentran notificados en el procedimiento adicional a lo anterior, las opciones de fuente reportada o canal presentan errores ortográficos lo que genera doble registro para el mismo canal.

Cuenta de Fuente Reportada	Etiquetas de columna		
Etiquetas de fila	Incidente	Orden de Trabajo	Total general
Administración de Sistemas	1		1
Autoservicio		3970	3970
Autosesrvicio	3		3
Correo Electronico	709	9279	9988
Entrada Directa	44	4	48
Escalación Externa		1	1
Otro		13	13
Ótro	3		3
Teléfono		18600	18600
Telfono	3358		3358
Total general	**4118**	**31867**	**35985**

Figura 5. Tickets generados en el primer semestre del 2023 por canal reportado

Menciona el área auditada que el canal de “Autoservicio” corresponde a los casos GIA, al indagar la funcionalidad de éste se identifica que la herramienta recibe las solicitudes relacionadas con la administración de usuarios en los sistemas de información como SAP, Lotus, acceso a permisos específicos en los File Server, entre otros, el cual es administrado por el área de Seguridad de la información, el equipo de la Mesa de Ayuda no cuenta con usuarios de consulta, al indagar cómo garantizan que el flujo del servicio no sea afectado como los ANS y la percepción del colaborador, informa que es compartido dos veces en el día un archivo de Excel con los casos registrados en esta herramienta junto con las observaciones o gestión que se ha realizado a cada uno de los casos, por consiguiente estos son creados en la herramienta de gestión BMC Remedy.

Con el fin de poder identificar oportunidades de mejora al procedimiento, se identifican las áreas de la EAAB-ESP que radican mayor número de casos, se filtran por dirección y por colaborador, para el presente informe se relacionan las 10 primeras áreas.

ÚLTIMO TRIMESTRE DEL 2022			
No.	DEPARTAMENTO	CANTIDAD	% PARTICIPACIÓN
1	DIRECCION SERVICIOS DE INFORMATICA	4986	60,9%
2	DIRECCION APOYO COMERCIAL	452	5,5%
3	GERENCIA DE ZONA 1	415	5,1%
4	GERENCIA DE ZONA 3	378	4,6%
5	DIRECCION SISTEMAS DE INFORMACION EMPRESARIAL	365	4,5%
6	GERENCIA DE ZONA 4	364	4,4%
7	GERENCIA DE ZONA 2	323	3,9%
8	DIRECCION IMAGEN CORPORATIVA COMUNICACIONES	311	3,8%
9	DIRECCION SERVICIOS ADMINISTRATIVOS	309	3,8%
10	GERENCIA DE ZONA 5	289	3,5%
	Total	***8192***	***100,0%***

PRIMER SEMESTRE DEL 2023			
No.	DEPARTAMENTO	CANTIDAD	% PARTICIPACIÓN
1	DIRECCION SERVICIOS DE INFORMATICA	15309	63,8%
2	DIRECCION APOYO COMERCIAL	1291	5,4%
3	GERENCIA DE ZONA 1	1066	4,4%
4	DIRECCION SISTEMAS DE INFORMACION EMPRESARIAL	1003	4,2%
5	GERENCIA DE ZONA 3	912	3,8%
6	GERENCIA DE ZONA 2	902	3,8%
7	DIRECCION JURISDICCION COACTIVA	893	3,7%
8	DIRECCION SERVICIOS ADMINISTRATIVOS	890	3,7%
9	GERENCIA DE ZONA 4	884	3,7%
10	DIRECCION IMAGEN CORPORATIVA COMUNICACIONES	853	3,6%
	Total	***24003***	***100,0%***

Figura 6. Top 10 de las áreas o direcciones que más solicitudes registran en los periodos de la auditoría

***Nota**: Para el informe se toma solo los 10 primeros, sin embargo, al tomar la totalidad de la base la Dirección Servicios de Informática sigue encabezando el listado, información completa en el papel de trabajo del grupo auditor.*

Llama la atención que más del 50% de las solicitudes las radica la Dirección de Servicios de Informática, por lo anterior se valida qué usuarios generan más solicitudes.

USUARIOS DE LA DSI			
No.	USUARIO	CANTIDAD	% PARTICIPACIÓN
1	Mesa de ayuda Centro de servicios	9551	68,5%
2	WS IGA Remedy	2043	14,7%
3	Jenny Andrea Chaparro Perez	1463	10,5%
4	ChatBot 7777	239	1,7%
5	Oscar Humberto Chacon Vega	133	1,0%
6	Maria Del Pilar Zapata Castillo	126	0,9%
7	Vladimir Largo Perilla	108	0,8%
8	Angelica Maria Algarra Parra	104	0,7%
9	Yimmy Alberto Roncancio Ramirez	94	0,7%
10	Juan Carlos Montejo Escobar	80	0,6%
	Total	***13941***	***100,0%***

Figura 7. Top 10 usuarios de la Dirección Servicios de Informática

Los casos creados bajo el nombre de “Mesa de ayuda Centro de servicios” corresponden a solicitudes de información sea de los servicios de TI, seguimiento a ticktes, llamadas colgadas o que la consulta corresponde a otra área, los registrados a nombre de “WS IGA Remedy” corresponden a casos automáticos que son creados por GIA, de igual forma se crean de manera manual cuando se requiere brindar algún soporte en sitio y los asociados a Jenny Andrea Chaparro Pérez corresponden a casos reportados por el área de seguridad de la información lo anterior manifestado por el área auditada.

Se procedió a validar el informe de gestión del periodo del 16 de febrero al 15 de marzo de 2023 y la data No. 18 la cual corresponde al periodo en mención, se identifica que el reporte de la cantidad de casos coincide con los registrados en la data exportada de la herramienta de gestión, sin tener en cuenta los registros duplicados, inconsistentes, llamadas colgadas, adicional en el ítem de Top 5 de usuarios donde se reporta los usuarios que mayor número de casos reportaron en el periodo no coincide con la información que contiene la data No.18 a continuación se expone lo evidenciado:

Registros inconsistentes

Número de INC/WO	Tipo de	Titulo del Indicador	EstadoINC	Fecha de Creación	Di	Fecha de Inicio Medición	Fecha de Fin Medición	Fecha Vencimiento SVT	Estado de la
WO0000001453284	Proyecto	WORK ORDER DISEÑO DE SERVICIO	Cerrado	16/02/2023 9:30	16	18/01/2023 14:55	15/02/2023 21:09	30/03/2023 14:55	Cumplido
WO0000001453287	Proyecto	WORK ORDER DISEÑO DE SERVICIO	Cerrado	16/02/2023 9:30	16	18/01/2023 15:11	15/02/2023 22:32	30/03/2023 15:11	Cumplido
WO0000001453288	Proyecto	WORK ORDER DISEÑO DE SERVICIO	Cerrado	16/02/2023 9:30	16	18/01/2023 15:15	15/02/2023 22:39	30/03/2023 15:15	Cumplido
WO0000001453289	Proyecto	WORK ORDER DISEÑO DE SERVICIO	Cerrado	16/02/2023 9:30	16	18/01/2023 15:17	15/02/2023 22:47	30/03/2023 15:17	Cumplido
WO0000001453292	Proyecto	WORK ORDER DISEÑO DE SERVICIO	Cerrado	16/02/2023 9:30	16	18/01/2023 15:22	15/02/2023 23:00	30/03/2023 15:22	Cumplido
WO0000001453293	Proyecto	WORK ORDER DISEÑO DE SERVICIO	Cerrado	16/02/2023 9:30	16	18/01/2023 15:26	15/02/2023 23:30	30/03/2023 15:26	Cumplido
WO0000001453297	Proyecto	WORK ORDER DISEÑO DE SERVICIO	Cancelado	16/02/2023 9:30	16	18/01/2023 15:30	15/02/2023 23:47	30/03/2023 15:30	Cumplido

Figura 8. Ordenes de trabajo cuya medición inició antes de la fecha de creación del ticket.

Estos registros presentan una inconsistencia en cuanto a la fecha de creación y fecha de inicio de medición, pues registra que la medición del ANS es anterior a la fecha de creación.

Nota: Por gestión de proyectos existen actividades asociadas a un hito del proyecto, de igual forma en el cronograma no debería registrar actividades cuya medición inicie antes de la creación de la tarea, todo es secuencial.

Reporte de Incidentes y Solicitud de servicios

Etiquetas de fila	Cuenta de Filtro Módulo
Incidente	643
Orden de Trabajo	5927
Total general	6570

Orden de Trabajo	5927
PROCEDIMIENTOS	1440
VERIFICACION	974
CONFIGURACION	745
DESBLOQUEO DE CUENTA	582
ACTUALIZACION PRIVILEGIOS	535
(en blanco)	305
LLAMADA COLGADA	262
BAJA DE USUARIO	202
INSTALACION	138
CREACION USUARIO	118
USUARIO OLVIDA PASSWORD	98
SEGUIMIENTO A TICKET	67
INSTALACION Y CONFIGURACION	65
LLAMADA DE PRUEBA	41

Figura 9. Información registrada en el informe del mes 22 de ejecución y el tipo de Ordenes de trabajo registrados en la data No. 18

Las buenas prácticas no incluyen en su ejercicio de medición las llamadas colgadas o de prueba para evaluar la prestación del servicio por consiguiente no deben ser incluidas en los ANS, las asociadas a la entrega de una información sobre los servicios de tecnología son definidas como una solicitud de servicio, las cuales apoyarían a la mejora continua del procedimiento, de igual forma se identifica la opción de tipificación de “Llamada equivocada” la cual no debería estar asociada al igual que las colgadas y de prueba a un incidente o una solicitud de servicio (orden de trabajo).

Lo anterior puede alterar la medición del acuerdo de servicio pactado con el proveedor de servicios No. 5 Efectividad en gestión de solicitudes, registrado en el Anexo 2 en el numeral 7.6.2 el cual cita, Se definen Once (11) Acuerdos de Nivel de Servicio, cada uno con meta de efectividad y un peso sobre el valor de la Base Mensual de Pago:

No.	Acuerdo de Nivel de Servicio	Meta de efectividad	Peso por ANS
1	Efectividad en disponibilidad de las aplicaciones	100%	25%
2	Efectividad en gestión de actividades	98%	15%
3	Efectividad en gestión de incidentes	98%	8%
4	Efectividad en gestión cuentas de usuarios	98%	8%
5	Efectividad en gestión de solicitudes	98%	8%
6	Efectividad en gestión de cambios	95%	8%
7	Efectividad en gestión mesa de ayuda	80%	8%
8	Efectividad en administración de la CMDB	85%	8%
9	Efectividad en gestión de riesgos	90%	5%
10	Efectividad en gestión de problemas y causa raíz	98%	5%
11	Efectividad en gestión en diseño del servicio	100%	2%
			100%

Figura No. 10 Niveles de servicio pactados con el proveedor de servicios y su porcentaje de afectación en la factura

Toda vez, que al medir las llamadas colgadas y de prueba las cuales no representan una gestión podría obtener resultados del ANS superiores a la gestión real realizada.

Para identificar las actividades que contribuyen a mejorar el procedimiento de la Gestión de la Mesa de ayuda, se validan las actividades ejecutadas respecto a los resultados de las encuestas de satisfacción enviadas aleatoriamente por el sistema a los colaboradores que han radicado peticiones en la mesa de ayuda, del análisis de la data de las encuestas de satisfacción se identificó lo siguiente.

La encuesta de satisfacción consta de 5 preguntas, es decir cada Orden de trabajo o Incidente atendido cuenta con estas preguntas para evaluar la precepción:

1. ¿La solución que se le dio a su requerimiento fue satisfactoria?
2. ¿El personal de mesa de ayuda y soporte en sitio, demuestran conocimiento e información suficiente para responder a las preguntas que se les hace?
3. ¿Cómo califica la disposición y aptitud del técnico que lo atendió?
4. ¿La atención y capacidad técnica del personal de mesa de ayuda y soporte en sitio le transmite confianza y seguridad?
5. ¿Qué sugerencias tiene en pro del mejoramiento del proceso de mesa de ayuda y soporte en sitio?

Del alcance de la auditoría último trimestre del 2022 y primer semestre del 2023 se evidenció:

Tipo de solicitud	Cantidad de solicitudes		Cantidad de preguntas realizadas de las 5 establecidas
	2022	2023	
Orden de Trabajo	6	10	4
	8	9	3
	3	13	2
	0	3	1
	0	3	10
Total	**17**	**38**	

Figura 11. Ordenes de trabajo que presentaron inconsistencias en las encuestas de satisfacción

En el primer semestre del 2023 se presentó inconsistencia a 55 órdenes de trabajo que generaron encuesta, 52 solicitudes no presentaron una encuesta completa y 3 presentan duplicidad, es decir, la encuesta de satisfacción se envió más de una vez al colaborador para que fuese calificada.

Orden de trabajo	Fecha Primera encuesta	Fecha segunda encuesta
WO0000001450912	5/01/2023 8:14:30	18/01/2023 14:35:12
WO0000001452121	13/01/2023 14:07:15	18/01/2023 7:46:44
WO0000001457948	6/03/2023 11:01:14	22/03/2023 8:20:01

Figura 12. Ordenes de trabajo que le fue enviada dos veces la encuesta de satisfacción

Adicional a lo anterior, se identificó que la encuesta de satisfacción no está llegando de manera adecuada al colaborador, no se logra ver el contenido de la pregunta de manera completa.

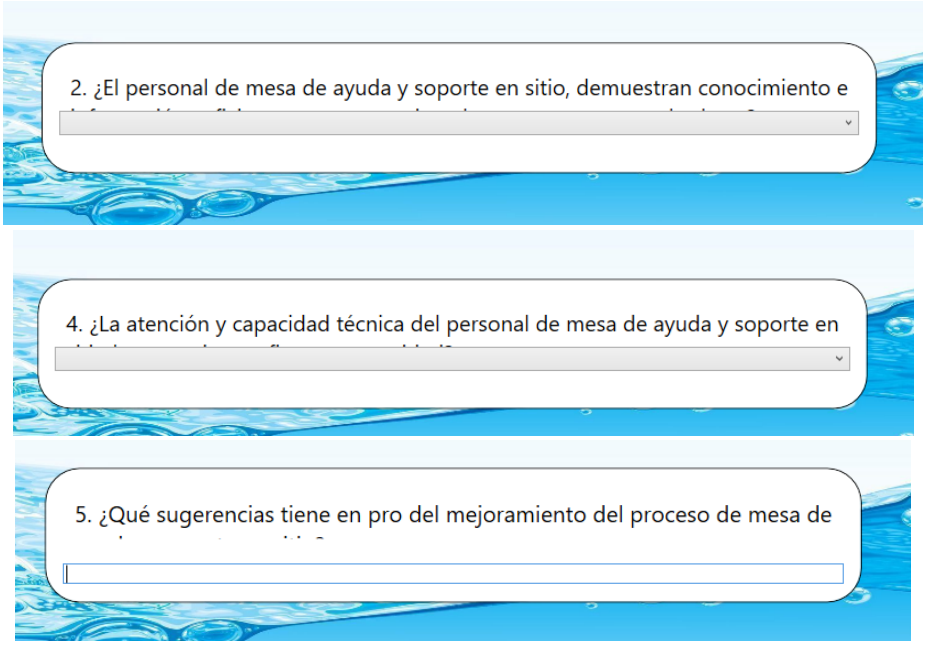


Figura 12. Evidencia de encuestas renviadas de manera incompleta.

Las encuestas de satisfacción se envían con varios días de diferencia de la fecha real del soporte, lo que dificulta al colaborar recordar a cuál solicitud se refiere toda vez, que la calidad de documentación no es clara.

Encuesta de Servicio DSI (Caso Número WO0000001494044) (septiembre 2023)

Información del Servicio Solicitado

Fecha del Requerimiento: 28/08/2023 10:56:46 a. m.
Detalle: Descripción de la solicitud: se comunica el usuario solicitando realizar verificación de mensaje que le sale en el normograma
Solución: Pruebas realizadas: Se toma por remoto
Técnico: John Edward Guerra Rocha (MESA DE AYUDA)

(Por favor califique de 1 a 5, en donde 1 es la calificación más baja y 5 la más alta).

Figura 13. Calidad de documentación

Se indaga con el área auditada las actividades que se ejecutan frente a las respuestas de las encuestas de satisfacción, manifiesta que estas son entregadas por el proveedor para validar las excepciones al contrato las

cuales son registradas en el archivo “Posibles Excepciones periodo (se registra el periodo a excepcionar)” en este archivo se evidencia que son seleccionadas las preguntas que han dado una calificación 1. Muy Mala, 2. Mala y 3. Regular, que el gestor de calidad analiza, identifica y gestiona los casos críticos dejando las observaciones en este documento para que el Líder del servicio por parte de la EAAB-ESP verifique y excepcione o no la gestión, es de mencionar que se cuenta con un ANS asociado a la factura del proveedor que, si no cumple con la meta establecida, afectará la factura. (información en el anexo 2 del contrato con el proveedor)

De la data de encuestas, se toma una muestra del 15 de octubre al 15 de noviembre del 2022 y el periodo del 15 de mayo al 16 de junio del 2023 para un total de 2.500 encuestas contestadas, se identifica la cantidad de encuestas negativas (encuestas que tuvieron una o más preguntas con valoración muy mala, mala y regular) obteniendo el siguiente comportamiento.

Periodo: 16 de oct al 15 nov 2022	1 Muy mala	2 Mala	3 Regular	Total	Encuestas Contestadas	Encuestas Negativas	% Encuestas Negativas sobre el total de encuestas	% Cumplimiento
1. ¿La solución que se le dio a su requerimiento fue satisfactoria?	8	8	29	45	1180	79	6.69%	93.31%
2. ¿El personal de mesa de ayuda y soporte en sitio, demuestran conocimiento e información suficiente para responder a las preguntas que se les hace?	6	4	44	54				
3. ¿Cómo califica la disposición y aptitud del técnico que lo atendió?	4	4	24	32				
4. ¿La atención y capacidad técnica del personal de mesa de ayuda y soporte en sitio le transmite confianza y seguridad?	5	2	43	50				
Periodo: 16 de may al 15 jun 2023	**1 Muy mala**	**2 Mala**	**3 Regular**	**Total**	**Encuestas Contestadas**	**Encuestas Negativas**	**% Encuestas Negativas sobre el total de encuestas**	**% Cumplimiento**
1. ¿La solución que se le dio a su requerimiento fue satisfactoria?	9	9	57	75	1330	114	9.66%	90.34%
2. ¿El personal de mesa de ayuda y soporte en sitio, demuestran conocimiento e información suficiente para responder a las preguntas que se les hace?	9	5	59	73				
3. ¿Cómo califica la disposición y aptitud del técnico que lo atendió?	6	4	41	51				
4. ¿La atención y capacidad técnica del personal de mesa de ayuda y soporte en sitio le transmite confianza y seguridad?	6	5	56	67				

Tabla 2. Análisis de resultado de encuestas por pregunta

Nota: El resultado de las encuestas negativas no tienen la validación que define si aplica valoración dada por el colaborador la cual se basa en la verificación de tiempos de respuesta (ANS), alcance, cumplimiento de procedimientos y actitudes de los agentes de mesa de ayuda y soporte en sitio.

Y del periodo auditado 15 de octubre al 31 de diciembre del 2022 y del 01 enero al julio 31 de 2023 se tomaron 213 encuestas de aquellas que únicamente en sus observaciones que sugieren una mejora continua, se estandarizan y se obtiene el siguiente resultado:

Comentario estandarizado	2022	2023	Total general
Demora en la atención y/o Solución	31	51	82
Cerrado sin gestión o solución no efectiva	17	21	38
Capacidad Tecnica (conocimiento en la funcionalidad de los sistemas de información de la EAAB-ESP)	8	10	18
Encuesta a destiempo	5	13	18
Optimizar los procesos	2	15	17
Cerrado sin Contactar al Colaborador	4	7	11
Capacitar al colabordor nuevo (en los sistemas de información y en cómo reportar casos a la mesa)	8	2	10
Encuesta Repetida	3	1	4
Mejorar encuesta	1	3	4
Mala practica de Call center	1	2	3
Ampliar presencia de Técnico en Sitio	2		2
Mejorar Actitud de servicio	1	1	2
Empatía en la comunicación escrita		1	1
Mejorar solución de primer nivel	1		1
Mejorar comunicación entre Mesa y Soporte en Sitio	1		1
Falta de documentación del caso	1		1
Total general	**86**	**127**	**213**

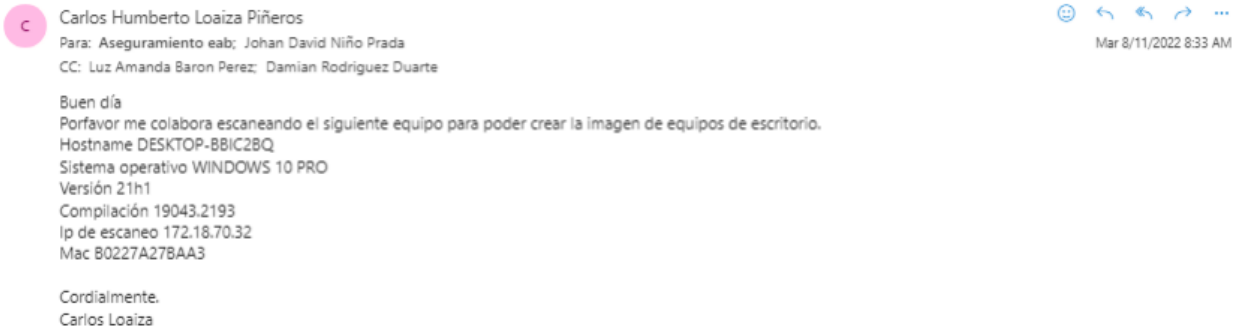
Tabla 3. Estandarización de los Comentarios del periodo auditado

Del ejercicio de auditoría se concluye que la percepción común del colaborador en el 2022 y 2023 de la muestra auditada es la demora en la atención o solución de sus solicitudes, en cuanto a ítem 3 Capacidad Técnica los colaboradores tienen la precepción que los agentes de mesa de ayuda como soporte en sitio desconocen de la funcionalidad y soporte en los sistemas de información de la entidad.

5.3 Comprobar que el desarrollo de las actividades del procedimiento MPFT0201-Atención de vulnerabilidades se cumplan, acorde a lo establecido en el procedimiento y normatividad aplicable.

Del análisis del procedimiento, se identificaron 10 políticas de operación y 6 actividades que el proveedor de servicios debe ejecutar para la correcta identificación y tratamiento de las vulnerabilidades, de éste se identifican las respectivas evidencias. Con el propósito de comprobar el desarrollo de las actividades y que éstas se ejecutan conforme a las políticas de operación, se estableció reunión con el Líder de procedimiento por parte de la EAAB-ESP y el responsable de la ejecución de las actividades por parte del operador de servicios, en las sesiones se Corroboró lo siguiente:

1. **Actividad 1 IDENTIFICACIÓN DE EQUIPOS**, evidencia: listado de equipos aprobados, para la ejecución de esta actividad se debe tener en cuenta la política No. 2 la cual cita: *"Todo equipo que se conecte a la red de datos de la Empresa debe contar con la autorización del GCV, quien mantiene el registro de la totalidad de los equipos incluidos en el proceso de Gestión de Vulnerabilidades. Únicamente los equipos incluidos en este registro cuentan con autorización expresa (Número de autorización) de conexión a la red de datos, de acuerdo con lo contemplado en los procedimientos "MPFT0204P - Conexión de equipos a la red de datos". Las infracciones detectadas a esta política constituyen incidente de seguridad. Aplica la Excepción de número de autorización individual para los equipos ingresados masivamente al comienzo del contrato de Servicios Informáticos (periodo de transición)."* De lo anterior se corrobora la solicitud de escaneo de los equipos para poder vincularlos al dominio (red) de la EAAB-ESP, se solicitó evidencia del periodo del 16 de octubre al 15 de nov del 2022 y 16 de febrero al 15 de marzo del 2023.


Carlos Humberto Loaiza Piñeros
Para: Aseguramiento eab; Johan David Niño Prada
CC: Luz Amanda Baron Perez; Damian Rodriguez Duarte
Mar 8/11/2022 8:33 AM

Buen día
Porfavor me colabora escaneando el siguiente equipo para poder crear la imagen de equipos de escritorio.
Hostname DESKTOP-BBIC2BQ
Sistema operativo WINDOWS 10 PRO
Versión 21h1
Compilación 19043.2193
Ip de escaneo 172.18.70.32
Mac B0227A27BAA3

Cordialmente.
Carlos Loaiza

Figura 14. Solicitud de escaneo de imagen de un equipo periodo del 16 de octubre al 15 de nov del 2022

Al indagar sobre los criterios que tiene el equipo de GCV (Grupo de Control de Vulnerabilidades), manifiesta el área auditada que éstos es que dentro del escaneo de vulnerabilidades realizado al equipo específico no presente vulnerabilidades, se evidencia la respuesta realizada por el GCV.

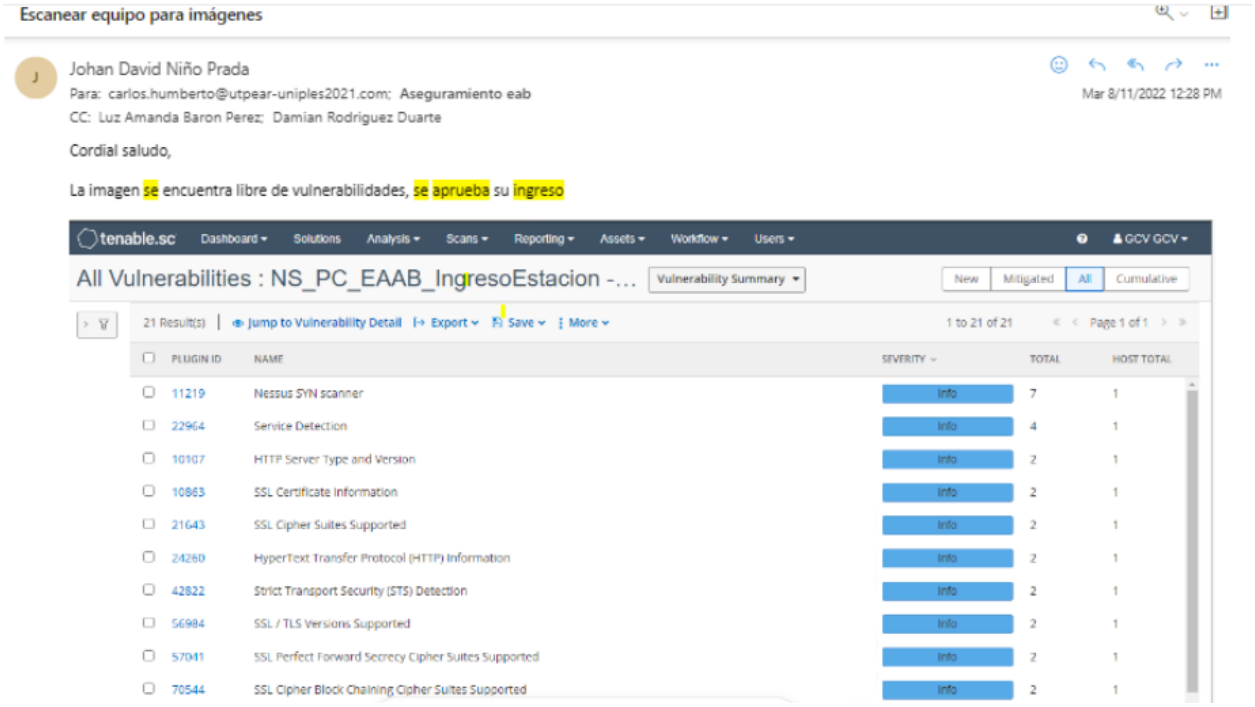


Figura 15. Resultado del escaneo de la imagen del equipo específico

El listado que se visualiza en la imagen entregada por el GCV corresponde a los criterios que se tienen en cuenta para que un equipo sea aceptado para ser vinculado a la red de la entidad.

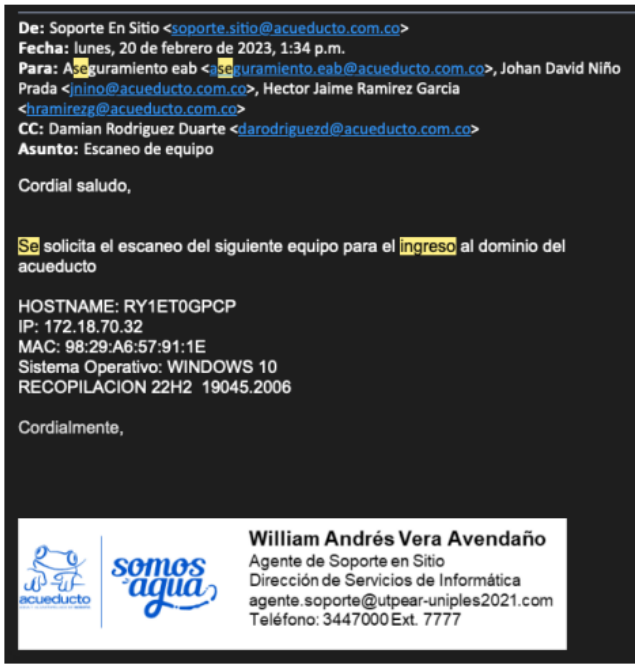


Figura 16. Solicitud de escaneo para ingreso de equipo al dominio del periodo 16 de febrero al 15 de marzo del 2023.

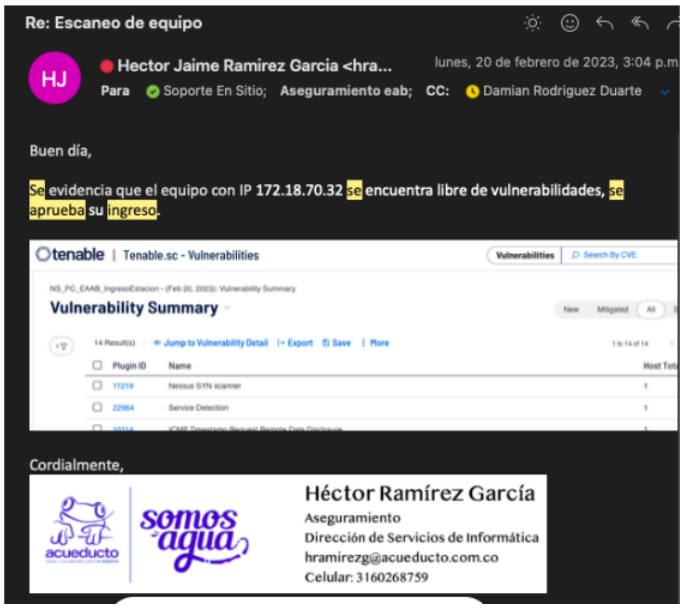
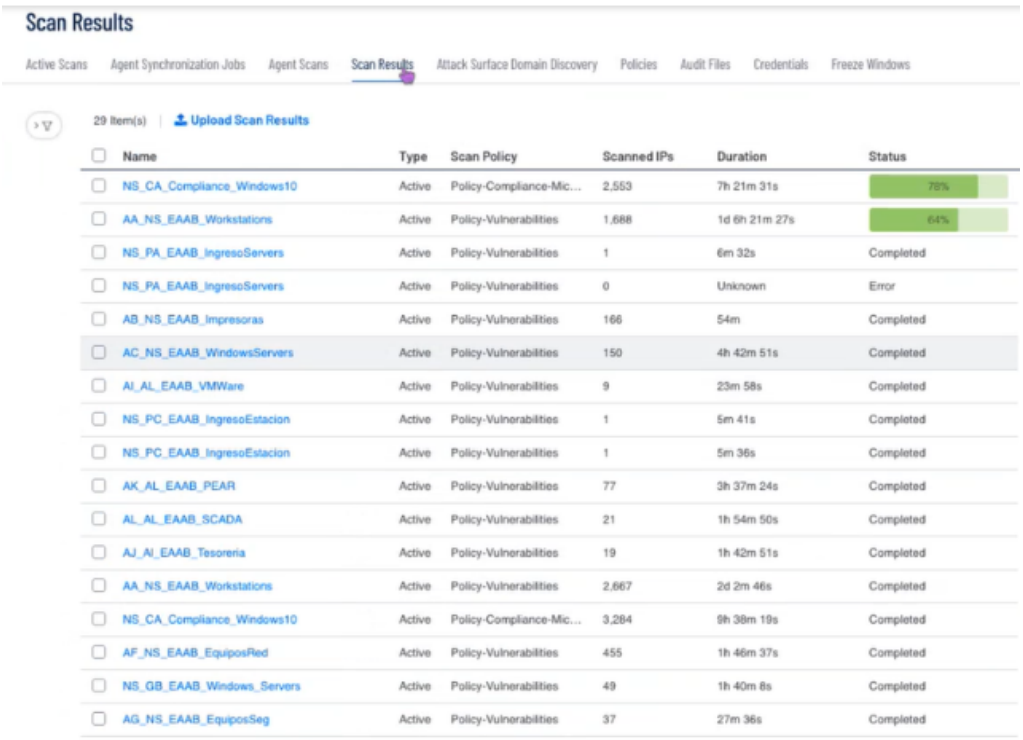


Figura 17. Resultado del escaneo al equipo específico

Según el procedimiento como evidencia de la ejecución se cuenta con el listado de equipos aprobados, el área auditada menciona que al momento de realizar el escaneo y éste no presenta vulnerabilidades, queda vinculado en el listado el cual se mantiene dentro del Software de vulnerabilidades.



Name	Type	Scan Policy	Scanned IPs	Duration	Status
NS_CA_Compliance_Windows10	Active	Policy-Compliance-Mic...	2,553	7h 21m 31s	78%
AA_NS_EAAB_Workstations	Active	Policy-Vulnerabilities	1,688	1d 6h 21m 27s	64%
NS_PA_EAAB_IngresoServers	Active	Policy-Vulnerabilities	1	6m 32s	Completed
NS_PA_EAAB_IngresoServers	Active	Policy-Vulnerabilities	0	Unknown	Error
AB_NS_EAAB_Impresoras	Active	Policy-Vulnerabilities	166	54m	Completed
AC_NS_EAAB_WindowsServers	Active	Policy-Vulnerabilities	150	4h 42m 51s	Completed
AI_AL_EAAB_VMWare	Active	Policy-Vulnerabilities	9	23m 58s	Completed
NS_PC_EAAB_IngresoEstacion	Active	Policy-Vulnerabilities	1	5m 41s	Completed
NS_PC_EAAB_IngresoEstacion	Active	Policy-Vulnerabilities	1	5m 36s	Completed
AK_AL_EAAB_PEAR	Active	Policy-Vulnerabilities	77	3h 37m 24s	Completed
AL_AL_EAAB_SCADA	Active	Policy-Vulnerabilities	21	1h 54m 50s	Completed
AJ_AI_EAAB_Tesoreria	Active	Policy-Vulnerabilities	19	1h 42m 51s	Completed
AA_NS_EAAB_Workstations	Active	Policy-Vulnerabilities	2,667	2d 2m 46s	Completed
NS_CA_Compliance_Windows10	Active	Policy-Compliance-Mic...	3,284	9h 38m 19s	Completed
AF_NS_EAAB_EquiposRed	Active	Policy-Vulnerabilities	455	1h 46m 37s	Completed
NS_GB_EAAB_Windows_Servers	Active	Policy-Vulnerabilities	49	1h 40m 8s	Completed
AG_NS_EAAB_EquiposSeg	Active	Policy-Vulnerabilities	37	27m 36s	Completed

Figura 18. Lista de equipos vinculados y autorizados en la red, agrupados según el tipo de equipo.

En caso de que el resultado del escaneo detecte vulnerabilidades, no se aprueba la vinculación del equipo a la red y se deniega la solicitud hasta que sean subsanadas.

Una vez aprobados los equipos, el GCV envía correo al grupo de NOC (Centro de operaciones de Red, monitorean, supervisan y mantienen la red) para que estos equipos autorizados no sean alertados ni bloqueados por los procesos que manera dicha área.

Como resultado se tiene el siguiente recuadro, donde se evidencia un total de 2.913 equipos o estaciones de trabajo de usuario vinculados al dominio y sujetos a que sean escaneados y demás equipos que mantienen los servicios del acueducto (servidores, equipos de monitoreo Scada, entre otros).

PLATAFORMA	CMDB	TENABLE	FALCON	NAC	No monitoreado	COMPARADOR	PORCENTAJE VIGILANCIA POR GRUPO
Estaciones Usuarios	2698	2913	2897	2998		2913	70.26%
Servidores Windows	230	216			10	240	5.21%
Servidores Unix	113	114				114	2.75%
Clusters VMWare	9	9				9	0.22%
Equipos Criticos	107	107				107	2.58%
Equipos redes	484	499				499	12.04%
Equipos Seguridad	42	37				42	0.89%
Centro de datos	12	12				12	0.29%
Imacenamiento y respaldo	18	18				18	0.43%
UPS	23	22				23	0.53%
Platas Telefonicas	3	3				3	0.07%
Impresoras	166	166				166	4.00%
TOTAL DE EQUIPOS EN LA RED						4146	
ORCENTAJE VIGILADO DE PLATAFORMA	99.28%						
		Equipos de Colegio				151	
		En Inventario, En Préstamo, En Reparación, Fuera de Servicio, Fin de vida Util, Devolver al Proveedor				76	

Figura 19. Cantidad de equipos sujetos a la revisión periódica de vulnerabilidades

Lo anterior da cumplimiento a la política de operación No. 1 la cual cita: *"La totalidad de los elementos y equipos físicos o virtuales que conforman la plataforma informática y que tengan asignada una dirección IP que permita su comunicación sobre la red de datos de la EAAB-ESP, deben estar sujetos a una revisión periódica de vulnerabilidades".*

Es de mencionar que uno de los puntos de control que tiene el procedimiento para evitar la vinculación de equipos no autorizados es el NAC (Controla accesos a la red) el cual, descubre nuevos equipos y procede a bloquearlos en caso de no estar en el listado del software de escaneo (TENABLE).

Lo anterior da cumplimiento a la política de operación No. 3 la cual cita: "*La identificación, análisis y medición permanente de las vulnerabilidades de los equipos conectados a la red de datos de la EAAB-ESP la realiza el Grupo de Control de Vulnerabilidades -GCV- con las herramientas de detección de vulnerabilidades con que cuenta la EAAB-ESP, de la cual el GCV es responsable por su administración. Adicionalmente, el Operador de Servicios de Informática tiene la obligación de reportar otras vulnerabilidades complementarias que detecte, al GCV".*

2. **CONFIGURACIÓN EQUIPOS**: Este punto está relacionado a las actividades que ejecuta el administrador del equipo para que el Software de escaneo de vulnerabilidades pueda detectarlo acorde a la agenda establecida entre el GCV y los administradores, lo anterior está relacionado con la política No. 4 la cual cita: *"Es responsabilidad de los Administradores de los equipos ajustar la configuración para permitir el análisis automatizado de vulnerabilidades mediante herramientas."* Como evidencia el procedimiento registra la Agenda de Scan.

   Se evidencia que la agenda está parametrizada en el Software de escaneo previa validación con los administradores, la ejecución del escaneo se hace por grupos los cuales están segmentados, por ejemplo, las estaciones de trabajo (equipos de los colaboradores), están en un grupo y la periodicidad es mínima, equipos

de operaciones críticas (por ejemplo, tesorería) tiene un horario específico que no afecte las operaciones, servidores, entre otros,

Name	Policy	Start Time	Schedule
AA_NS_EAAB_Workstations	Policy-Vulnerabilities	Oct 06, 2023 08:00	Every week on Mon, Wed, Fri at 08:00 -05:00
AB_NS_EAAB_Impresoras	Policy-Vulnerabilities	Oct 12, 2023 08:00	Every week on Thu at 08:00 -05:00
AC_NS_EAAB_WindowsServers	Policy-Vulnerabilities	Oct 11, 2023 21:00	Every week on Wed at 21:00 -05:00
AD_NS_EAAB_Unix_Servers	Policy-Vulnerabilities	Oct 06, 2023 21:00	Every week on Fri at 21:00 -05:00
AE_NS_EAAB_Storage_Backup	Policy-Vulnerabilities	Oct 09, 2023 22:00	Every week on Mon at 22:00 -05:00
AF_NS_EAAB_EquiposRed	Policy-Vulnerabilities	Oct 09, 2023 22:00	Every week on Mon at 22:00 -05:00
AG_NS_EAAB_EquiposSeg	Policy-Vulnerabilities	Oct 05, 2023 22:00	Every week on Mon, Thu at 22:00 -05:00
AH_AL_EAAB_CentroComputo	Policy-Vulnerabilities	Oct 09, 2023 08:00	Every week on Mon at 08:00 -05:00
AI_AL_EAAB_VMWare	Policy-Vulnerabilities	Oct 09, 2023 21:00	Every week on Mon, Wed at 21:00 -05:00
AJ_AI_EAAB_Tesoreria	Policy-Vulnerabilities	Oct 06, 2023 08:00	Every week on Mon, Wed, Fri at 08:00 -05:00

Figura 20. Agenta establecida para ejecutar los escaneos,

Para la ejecución del escaneo de equipos críticos, como por ejemplo SCADA, se acuerda previamente con el administrador a fin de minimizar posibles riesgos de afectar los equipos a escanear.

3. **REALIZAR ESCANEOS**: Esta actividad corresponde a la ejecución del escaneo conforme a la agenda establecida. Por medio de la herramienta Nessus se ejecuta el escaneo de las estaciones el primer día hábil del periodo y el ultimo se toma evidencias de las vulnerabilidades detectadas para verificar que las actividades de remediación son efectivas.

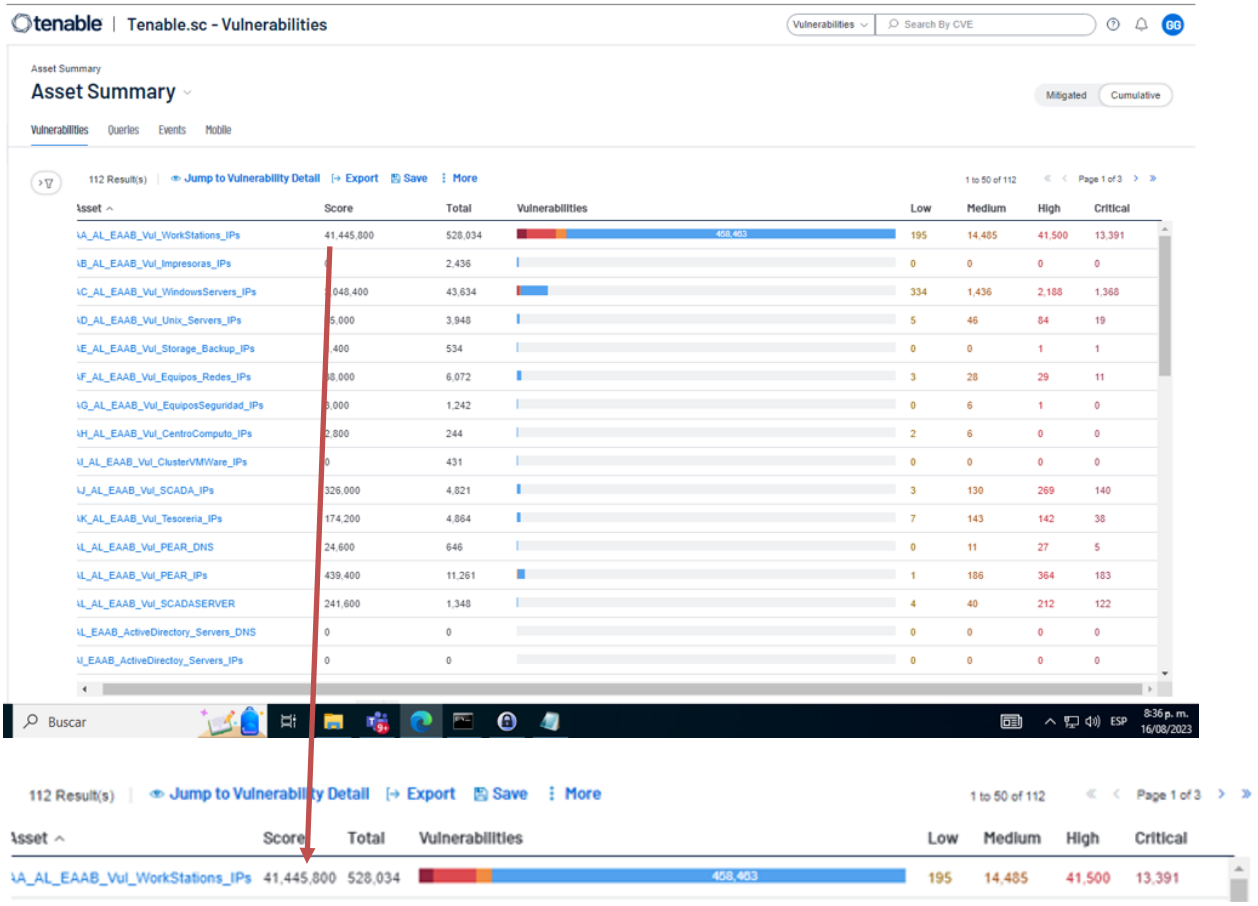


Figura 21. Resultado del escaneo

El agendamiento para realizar los escaneos fue concertado con los administradores desde el 2021 y siempre se ejecutan en el mismo horario los cuales están parametrizados en el software de vulnerabilidades Nessus Tenable y su periodicidad es diferente para los grupos que se tienen identificados:

1.Estaciones críticas (servidores, equipos que ejecutan transacciones críticas o estratégicas)
2.Resto de estaciones (PC, portátiles, impresoras, Scanner todo equipo que tenga una IP asignada)
3.Plataforma central (Equipos de monitoreo Scada, servidores, switch etc)

Conforme a lo indicado por el líder de la Gestión de Vulnerabilidades se procede a validar el anexo 2 del contrato 1-05-26500-0848-2021 subscrito entre EAAB-ESP y Unión Temporal PS-UN 2021 contratista que ejecuta las actividades de Atención de Vulnerabilidades, se corrobora en el numeral 6.2.3.2 Servicios de Gestión de vulnerabilidades las funciones a ejecutar lo que incluye el entendimiento y aceptación del procedimiento y lineamientos establecidos, no obstante, no se evidencia lo relacionado al conocimiento o participación en la elaboración y aceptación del agendamiento.

4. **PRESENTAR PLANES DE REMEDIACIÓN**: Esta actividad se enfoca en la presentación de los planes de remediación conforme a los resultados del escaneo periódico donde se registran las vulnerabilidades,

Cuando se ejecuta el escaneo por cada grupo establecido, el sistema arroja las vulnerabilidades y registra el plan de remediación consolidado en un archivo de Excel, el grupo de GCV remite al administrador de manera individual el archivo con el listado de vulnerabilidades y su plan de remediación.
Como evidencia se solicita planes de remediación de los periodos 16 de octubre al 15 de noviembre del 2022 y 16 de febrero al 15 de marzo del 2023.

- 16 de octubre de 2022 – 15 de noviembre 2022:

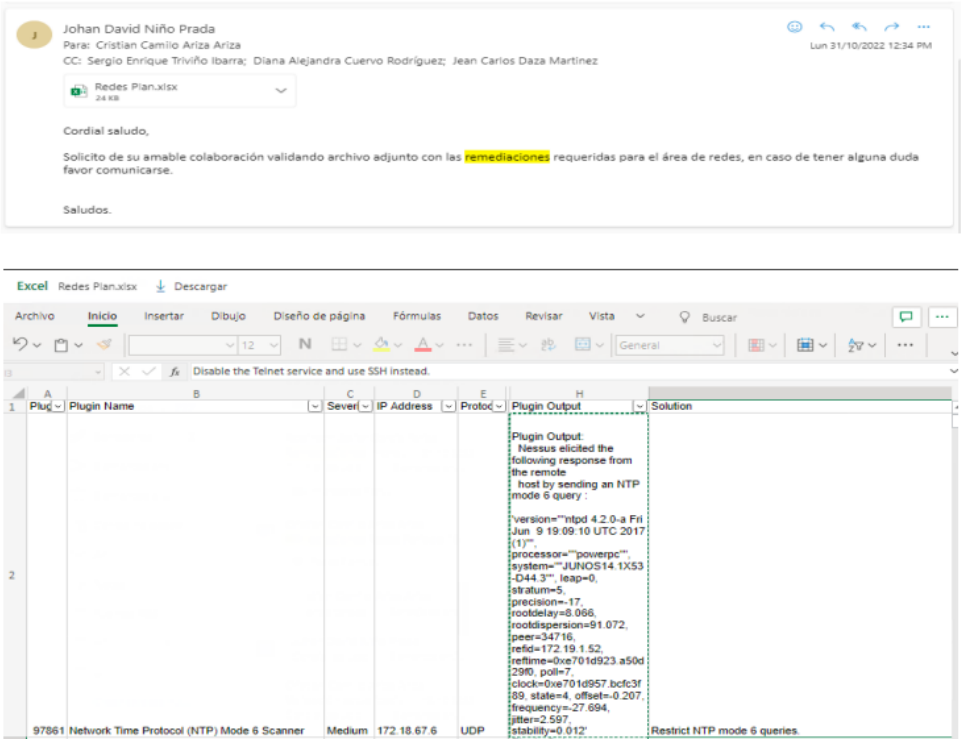


Figura 22. Reporte o presentación del plan de remediación al administrador del periodo 16 de octubre al 15 de noviembre del 2022

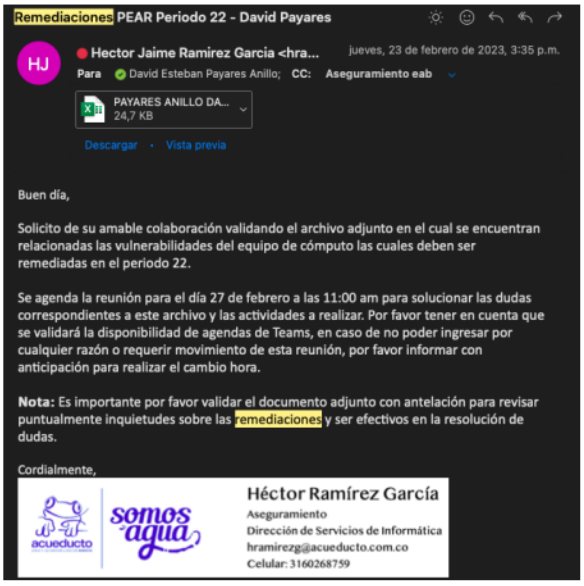
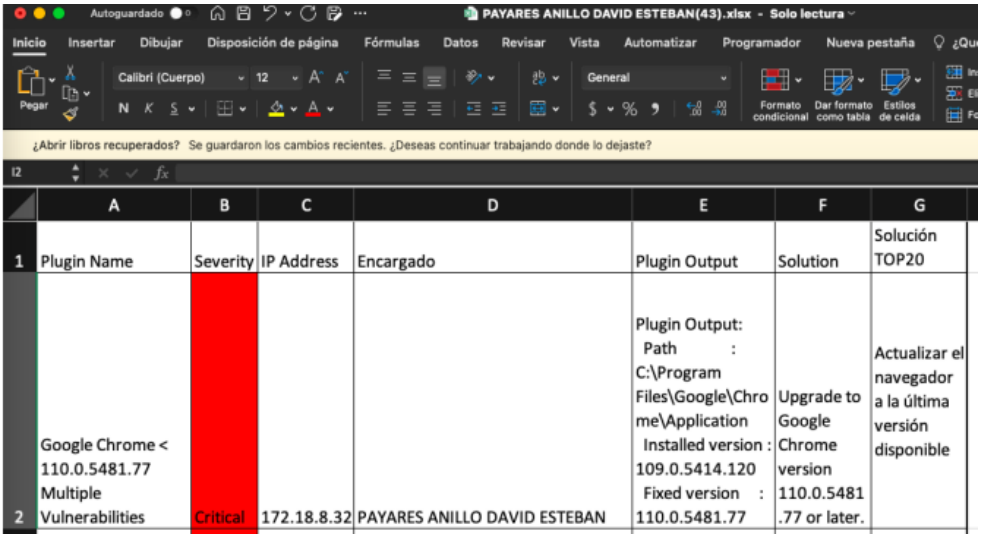


Figura 23. Correo enviado por GCV al administrador adjuntando el plan de remediación del periodo 16 de febrero al 15 de marzo del 2023



	A	B	C	D	E	F	G
1	Plugin Name	Severity	IP Address	Encargado	Plugin Output	Solution	Solución TOP20
2	Google Chrome < 110.0.5481.77 Multiple Vulnerabilities	Critical	172.18.8.32	PAYARES ANILLO DAVID ESTEBAN	Plugin Output: Path : C:\Program Files\Google\Chrome\Application Installed version : 109.0.5414.120 Fixed version : 110.0.5481.77	Upgrade to Google Chrome version 110.0.5481.77 or later.	Actualizar el navegador a la última versión disponible

Figura 24. Plan de remediación enviado periodo 16 de febrero al 15 de marzo del 2023

Lo anterior da cumplimiento a la política de operación No. 9 la cual cita*: "El GCV tiene como función priorizar las vulnerabilidades que deben ser atendidas en primer lugar y revisar el cumplimiento de las prioridades de acuerdo con el nivel de riesgo asociado".*

5. **REMEDIAR VULNERABILIDADES**: El administrador del equipo una vez recibido el plan de remediación ejecuta las actividades conforme a las funciones establecidas en el anexo 2 del contrato, el Líder del procedimiento de vulnerabilidades por parte de la EAAB-ESP corrobora la aplicabilidad del plan de remediación realizando seguimiento al indicador donde evidencia la disminución de las vulnerabilidades encontradas al inicio del periodo.

6. **INDICADORES:** El indicador está establecido a nivel contractual con el proveedor de servicios cuya meta es del 20% de disminución riesgo de vulnerabilidades en el periodo (mensual)

%Disminución del riesgo por vulnerabilidad mensual

El líder de servicio valida el indicador según los 3 grupos establecidos los cuales son actualizados conforme a la ejecución de la agenda.

Figura 25. Seguimiento a los indicadores de vulnerabilidades establecidos con el proveedor

Como conclusión se evidencia el control del procedimiento por parte del líder del procedimiento de la EAAB-ESP y ejecución de las actividades con sus evidencias por parte del proveedor de servicios.

5.4 Evidenciar el cumplimiento de lo establecido en las políticas, actividades y demás normatividad asociada con Seguridad Digital.

La estructura de la Política de Gobierno Digital, consta de la Gobernanza y la Innovación pública digital, la Seguridad Digital la cual es un elemento que compone el grupo de habilitadores los cuales generan los lineamientos y buenas prácticas en los procesos de planeación y gestión de la seguridad de la información es parte fundamental para la gestión de riesgos y actividades de control conforme al decreto 1083 de 2015, modificado por el decreto 1499 de

2017, el cual consolida los elementos requeridos respecto a las 16 políticas de Gestión y Desempeño y dentro de las cuales se establece la política de Seguridad Digital.

Se identifica que mediante resolución 740 de 2018 "*por medio de la cual se adopta la política general de seguridad y privacidad de la información en la Empresa de Acueducto y Alcantarillado de Bogotá, EAAB-ESP"* consolida las políticas, actividades y normatividad asociada con Seguridad de la información.

Partiendo de lo anterior se procede a validar el cumplimiento de la resolución en mención.

ARTICULO UNO: Adoptar la política de seguridad y privacidad de la información enfocado en la protección de la información de la organización, colaboradores y usuarios.

Se identifica el documento MPEE01 V3 – Política de seguridad y privacidad de la información en la cual se describe y justifica la adopción de los lineamientos establecidos en resolución 740 del 2018, por lo anterior se evidencia cumplimiento a este artículo, no obstante, la publicación de la política corresponde al 2018, no se evidenció una versión reciente.

POLÍTICA	
Tipología: Política de gestión	**Página:** 1 de 6
Nombre: Política de seguridad y privacidad de la información	**Versión:** 03

Control de cambios (se lleva el control de las versiones y la justificación de las mismas)

VERSIÓN	FECHA DE APROBACIÓN	RESPONSABLE DEL CAMBIO	CONTROL DE CAMBIOS	FIRMA
01	23-12-2009	Jorge Enrique Pizano Callejas Gerente General	Versión inicial según resolución 1127 de 2009	
02	22-06-2017	Pedro Buitrago Aguilar Gerente de Tecnología	Adición tratamiento de datos personales	
03	20-12-2018	Lady Johanna Ospina Corso Gerente General	Modificaciones: Descripción, objetivos, líneas de defensa e indicadores	

Descripción

La EAAB-ESP está comprometida a proveer un ambiente seguro en el tratamiento de la información, preservando sus características esenciales de confidencialidad, integridad, disponibilidad y privacidad de activos de información y de la información vital de la organización para la sostenibilidad de la Empresa, aplicando las mejores prácticas de seguridad y privacidad de información.

Justificación

La EAAB-ESP define y establece la política de seguridad y privacidad de la información con el fin de declarar las responsabilidades y conductas que debe ser observada por cada una de las áreas responsables de la protección y uso de la información, sus funcionarios, colaboradores, usuarios de información, de recursos y servicios informáticos; proteger la información de los procesos organizacionales para la prestación de sus servicios; adoptar y desarrollar el Subsistema de Gestión de Seguridad de la Información (SGSI); precisar las medidas y controles que debe observar la

Figura 26. Descripción y justificación de la política de seguridad y privacidad de la información en la EAAB-ESP.

ARTICULO TRES: Protección de la información independiente del medio en que se encuentre al interior de la empresa, en este artículo se define las responsabilidades de custodia, activos de información, clasificación de la información.

ARTICULO SEXTO: Responsabilidad frente a la protección de la información.

Dentro de la política de seguridad y privacidad de la información establecida en la EAAB-ESP, se define los roles y responsabilidades respecto a la protección de la información, estas responsabilidades son segmentadas en las líneas de defensa como se muestra a continuación:

Roles y responsabilidades

ROLES	RESPONSABILIDADES
Directivos – Responsables o determinadores de los activos de información	**Primera línea de defensa** Definir los criterios de protección y buen uso de los activos de información, para lo cual deberá: 1. Identificar y clasificar los activos de información que se originan en sus procesos en las herramienta de gestión de riesgos – GRC de la Empresa. 2. Definir, aprobar y divulgar las pautas de protección y uso determinadas de acuerdo a los riesgos asociados para sus activos de información. 3. Autorizar expresamente el acceso a la información, ya sea mediante formulario SIMI o el registro definido para la información física.
	4. Elaborar planes de continuidad a los procesos críticos del área. 5. Vigilar y reportar desviaciones e incidentes de seguridad y tomar acciones y controles establecidos para sus activos de información. 6. Autogestionar la seguridad, protección y gestión de riesgos de la información. 7. Realizar el autocontrol y reportar el estado de los indicadores de la gestión de seguridad y privacidad de la información.
Funcionarios, terceros o colaboradores de EAAB-ESP	**Primera línea de defensa** 1. Acatar la política de seguridad y privacidad de la información y procedimientos corporativos que de ella se deriven o de los acuerdos de uso y/o confidencialidad a los que esté comprometido. 2. Proteger y dar buen uso de los activos de información de acuerdo a la clasificación aprobada por el área dueña del mismo. 3. Informar a la instancia encargada los eventos de incumplimiento de la política de seguridad y privacidad de la información o de los procedimientos corporativos que de ella se deriven y ésta al Comité de Gestión y Desempeño Institucional.
Comité de Gestión y Desempeño Institucional	**Segunda línea de defensa** 1. Formalizar, divulgar, analizar y hacer cumplir el gobierno del Subsistema de Gestión de Seguridad de la Información, junto con cada uno de sus componentes. 2. Asegurar, aprobar y verificar la implementación de las directrices en materia de seguridad digital y de la información junto con cada uno de sus componentes para el uso y protección adecuada de la información.
Líder Subsistema de Seguridad de la Información (SGSI) – Gerente de Tecnología	**Segunda línea de defensa** 1. Diseñar, desarrollar, implementar, monitorear, mejorar, evaluar, reportar a la organización y verificar el buen funcionamiento del Subsistema de Seguridad y Privacidad de la Información. 2. Las demás que establezca la normatividad vigente.

Equipo de trabajo del Subsistema de Seguridad de la Información (SGSI)	**Segunda línea de defensa** 1. Acompañar y asesorar a las áreas para que los responsables de la protección y uso de la información puedan cumplir con las actividades del Subsistema de Gestión de Seguridad de la Información. 2. Apoyar al líder del Subsistema de Gestión de Seguridad de la Información con los planes, actividades y/o seguimientos a los mismos.
Oficina de Control Interno y Gestión	**Tercera línea de defensa** 1. Verificar el cumplimiento de las responsabilidades frente al SGSI y frente a la política de seguridad y privacidad de la información.

Figura 26. Roles y responsabilidades por línea de negocio establecidos en la política de seguridad de la información

Para las actividades adicionales que cita el artículo, el subsistema de Gestión de Seguridad de la información establece procedimientos y lineamientos en los mismos para dar su cumplimiento, de igual forma se apoya en las subdirecciones del proceso de Gestión TIC para ejecutar controles de seguridad, como evidencia en el ejercicio de la auditoría, se corrobora la Gestión de Activos y configuraciones en cuanto la ejecución de controles de seguridad de la información.

En el procedimiento PFT0308P - Gestión de Activos y Configuración en la actividad 2 Identificar un CI (elemento de configuración – equipo, impresora, etc) ejecuta las herramientas establecidas en el procedimiento de Atención de Vulnerabilidad la cual no sólo identifica los elementos o activos sino que ejecuta procesos de identificación de vulnerabilidades, reporta (plan de remediación) y bloquea el acceso a la red de la entidad hasta que sean remediadas las observaciones registradas en el plan de remediación.

Nota: Las evidencias de esta gestión están registradas en el numeral 5.3 del presente informe.

ARTICULO SEPTIMO: Gestión de riesgos de la información, en este artículo se establece la articulación de la gestión de riesgos de seguridad con el Sistema Integrado de Gestión SIG, para identificar, evaluar, tratar, monitorear y reportar riesgos asociados con los procesos, personas, sistemas de información entre otro, relacionados con la integridad, confidencialidad, disponibilidad y privacidad de la información.

Es de mencionar, que en la política de Seguridad digital se basa en la política de Seguridad Nacional, uno de sus principios fundamentales cita: *Adoptar un enfoque basado en riesgos, que permita a los individuos el libre, confiable y seguro desarrollo de sus actividades en el entorno digital*.

Se corrobora la gestión que ha ejecutado el Subsistema de Seguridad de la información SGSI respecto a la gestión de riesgos que la primera línea de defensa debe conocer, identificar, medir y tratar.

Dentro del desarrollo para la implementación de MIPG, las partes involucradas como cumplimiento a lo establecido, deben realizar un autocontrol frente a las políticas establecidas. La responsabilidad de Gestión TIC se relacionan con la política de seguridad y privacidad de la información.

2023 : Divulgar la metodología de Seguridad y Privacidad de la Información

Primera publicación: 4/04/2023 12:58 p.m. Última actualización: 11/10/2023 3:54 p.m.

INFORMACIÓN GENERAL

Nombre de la actividad:	Divulgar la metodología de Seguridad y Privacidad de la Información	**ID de la Actividad:**	353318

Nombre del Plan(1)

Nombre de Plan	Líder del Plan
Plan de Seguridad y Privacidad de la Información	Cruz Silva, Lina Maria

Eje temático

Nombre del eje temático
Política De Seguridad De La Información

Vigencia:	2023	**Versión:**	1
Fecha de elaboración:	24/01/2023	**Fecha de aprobación:**	27/01/2023
Alineación:	MIPG		

MIPG: ESTADO DE LOS AUTOCONTROLES

Informe General Monitoreo MIPG Ener

								procesos.
Plan de Seguridad y Privacidad de la Información	Divulgar la metodología de Seguridad y Privacidad de la Información	Cinco talleres	Reporte GRC-Archer	1/09/2023	30/09/2023	Al dia	Cumplida	Actividad cumplida: De acuerdo con lo registrado en el autocontrol, se evidencia que durante la vigencia se han realizado talleres con diferentes área de la empresa en los que se han llevado temas como: 1. Divulgación de metodología y acompañamiento 2. Seguimiento de la gestión de tratamiento de Datos Personales 3. Seguimiento a la clasificación de los activos de información 4. Seguimiento de la gestión de incidentes de seguridad de la información 6. Seguimiento al tratamiento de riesgos de seguridad y privacidad de información 7. Capacitación protección de datos personales
Realizar capacitación y seguimiento de la gestión de tratamiento de Datos Personales	Cinco talleres	Reporte GRC-Archer	1/09/2023	30/09/2023	Al dia	Cumplida	Actividad cumplida: De acuerdo con lo registrado en el autocontrol, se evidencia que durante la vigencia se han realizado talleres con diferentes área de la empresa en los que se han llevado temas como: 1. Divulgación de metodología y acompañamiento 2. Seguimiento de la gestión de tratamiento de Datos Personales 3. Seguimiento a la clasificación de los activos de información 4. Seguimiento de la gestión de incidentes de seguridad de la información 6. Seguimiento al tratamiento de riesgos de seguridad y privacidad de información 7. Capacitación protección de datos personales						

Figura 27. Autocontrol MIPG – Política de Seguridad y Privacidad de la información

Dentro de las evidencias registradas en Archer, se identifica que de enero a septiembre del 2023 se ha divulgado la metodología de seguridad y privacidad de la información, en los aspectos de: Tratamiento de datos personales, seguimiento a la clasificación de activos e incidentes de seguridad de la información, seguimiento al tratamiento de riesgos de seguridad y privacidad de la información y capacitación de datos personales, de las 36 direcciones que registran han recibido la sensibilización o seguimiento de la política, solo 6 registran la inclusión de seguimiento de tratamiento de riesgos de seguridad y privacidad de la información.

Con el fin de validar la aceptación y adopción de la sensibilización dada por el SGSI, se procede a validar las siguientes matrices:

- Gestión Contractual
- Servicios Administrativos
- Gestión Documental
- Gestión Comercial

- Financiera

Del análisis se evidenció la inclusión de riesgos de seguridad en la matriz de la Gestión Contractual y Servicios Administrativos.

La resolución 740 del 2018 en sus demás artículos, establece lineamientos a tener en cuenta y demás lineamientos en cuanto a Continuidad de negocio, autoevaluación, control de acceso físico y de red, fomentar cultura de seguridad, para lo cual se evidencia dentro de los procedimientos de la Gestión TIC la atención a estos artículos.

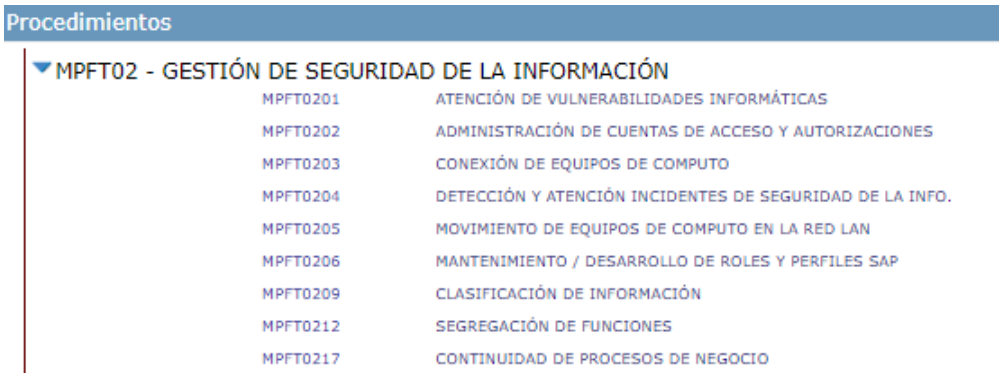


Figura 28. Procedimientos que soportan la atención de la resolución 740 del 2018

No obstante, a lo anterior, se evidencia que los procedimientos no han sido actualizados, estos fueron publicados entre el 2013 al 2020.

5.5 Evidenciar el cumplimiento en la implementación y ejecución de lo establecido en las políticas, actividades y demás normatividad asociada con el Plan Maestro de Tecnología (PMT).

Conforme a lo establecido en la guía MGGTI.GE.ES.01 - Guía para la Construcción del PETI (Plan Estratégico de Tecnología) la cual hace parte de los instrumentos y herramientas del Marco de Referencia de Arquitectura definido por MinTIC y reúne la descripción de la metodología, estructura, técnicas y herramientas que deben contener los Planes Estratégicos de TI, garantizando su alineación con la Política de Gobierno Digital. Se valida su cumplimiento en cuanto a: Entendimiento estratégico, Gestión de la arquitectura TI y Planeación de TI.

Del análisis de la información registrada en el indicador estratégico asociado al Plan Maestro de Tecnología y entrevista con la Gerencia de Tecnología se identifica lo siguiente:

Que por medio del contrato 1215 del 2018 se ejecutaron actividades para lograr el entendimiento estratégico de la entidad, así como la ejecución de los componentes que abarcan la arquitectura de TI y la planeación de TI (elaboración del PMT). Como resultado de la ejecución del contrato en mención se obtuvo el siguiente resultado.

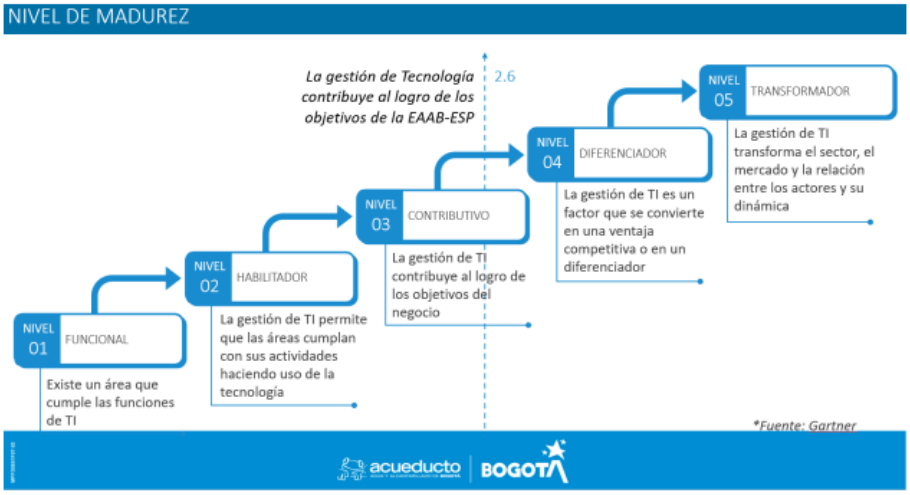


Figura 29. Contribución de la gestión de tecnología al logro de los objetivos de la EAAB-ESP

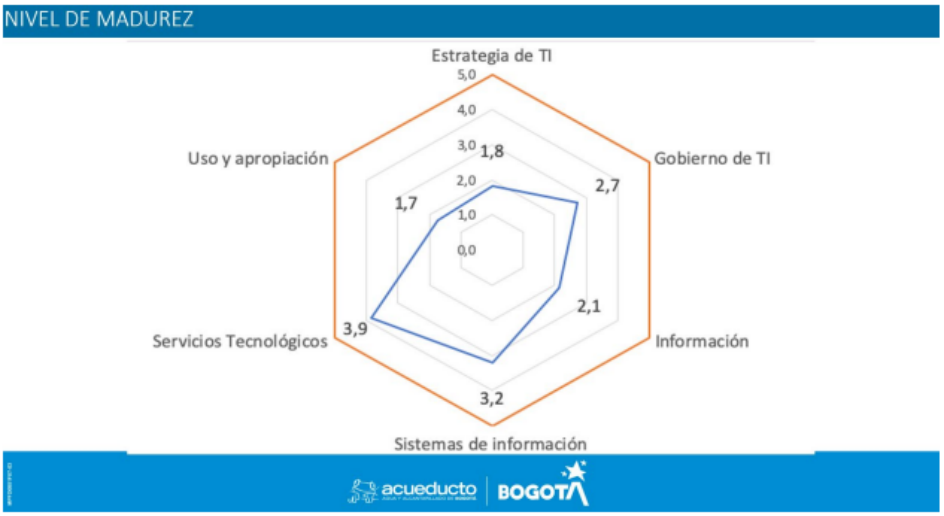


Figura 30. Nivel de madurez componentes de la arquitectura de TI

Conforme a lo establecido en la política de Gobierno Digital, se establecen los ejes estratégicos de tecnología, ejes a tener en cuenta para la planificación del Plan Maestro de Tecnología.

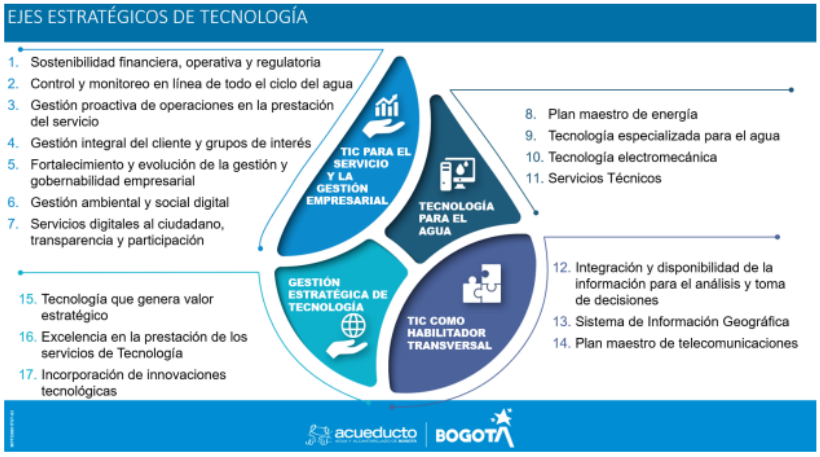


Figura 31. Ejes estratégicos de tecnología.

Lo anterior cumple con lo establecido en la guía MGGTI.G.ES - ESTRATEGIA DE TI punto 4.1 Entendimiento estratégico del capítulo 4 Etapas de la guía y el punto 4.2 Gestión de Arquitectura TI.

Para dar cumplimiento a la totalidad del punto 4.1 respecto al entendimiento de los servicios y gestión de la entidad, lo que corresponde a la Arquitectura Empresarial la Gerencia de Tecnología con el apoyo de la DSI, continúa con el proyecto para la identificación y definición de la Arquitectura Empresarial.

Con respecto al punto 4.4 Planeación de TI, la Gerencia de Tecnología estructura su Plan Maestro de Tecnología con la información y análisis ejecutada en el contrato en mención y establece los proyectos a ejecutar lo anterior contribuye al cumplimiento del punto 4.4.2 Portafolio de Planes, Programas y Proyectos de TI, como evidencia se identifica las fases que se tuvieron en cuenta para la elaboración del Plan Maestro de Tecnología y los proyectos establecidos inicialmente.

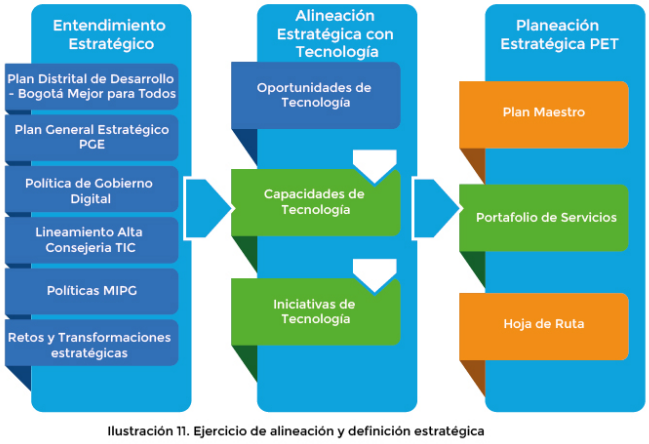


Ilustración 11. Ejercicio de alineación y definición estratégica

Figura 32. Participación del PMT en la Estrategia de la EAAB-ESP

Código proyecto	Nombre proyecto
PRY_01	Proyecto de Fortalecimiento de la sostenibilidad financiera y operativa
PRY_02	Implementación del Sistema de Información de Gestión Jurídica
PRY_03	Fortalecer el Control en Línea del Sistema Maestro
PRY_04	Tecnología apoyando el ciclo del agua
PRY_05	Fortalecer la gestión del monitoreo al consumo
PRY_06	Implementar el Sistema de Gestión de Operaciones
PRY_07	Implementar el sistema de información de mantenimiento centralizado
PRY_08	Proyecto de Gestión Integral del Cliente y los Grupos de Interés
PRY_09	Facturación confiable y oportuna
PRY_10	Sistema de Información de Gestión Integral del Documento Electrónico y Archivo - SGIDEA
PRY_11	Evolución SIE 4.0
PRY_12	Gestión Contractual Integral
PRY_13	Apoyo al Sistema integrado de gestión
PRY_14	Sistema de Información de Gestión Predial
PRY_15	Fortalecimiento de los Sistemas de Información de Apoyo
PRY_16	Sistematización de procesos y sus flujos de trabajo
PRY_17	Definición e implementación del sistema de información del Sistema Hídrico
PRY_18	Implementar la Ventanilla Única de Servicios
PRY_19	Definir el Plan Maestro de Energía
PRY_20	Fortalecer la Gestión de procesos de la Dirección de Ingeniería Especializada
PRY_21	Páramos frente al cambio climático
PRY_22	Definir el Plan Maestro de Calidad del Agua
PRY_23	Proyecto de fortalecimiento de tecnología electromecánica
PRY_24	Proyecto de fortalecimiento de servicios técnicos
PRY_25	Información para consulta, análisis y toma de decisiones
PRY_26	Proyecto de Integración de información y sistemas de información
PRY_27	Fortalecimiento del Sistema de Información Geográfica Unificado Empresarial
PRY_28	Densificación de la Red Geodésica
PRY_29	Definir e Implementar el Plan maestro de telecomunicaciones
PRY_30	Fortalecimiento de las capacidades de gestión de tecnología
PRY_31	Definición del marco de gobierno para la gestión de tecnología
PRY_32	Prestación de servicios de tecnología con excelencia
PRY_33	Innovaciones tecnológicas y gestión del conocimiento para una mejor empresa

Figura 33. Proyectos establecidos planificados para el 2022

Para el 2023 ya se cuentan con 119 proyectos los cuales están distribuidos en las diferentes áreas o direcciones de la EAAB-ESP, los cuales, tienen un seguimiento, este seguimiento se evidenció en la reunión presencial realizada el 26 de septiembre del 2023 en el cual el equipo auditor evidenció la estructura de seguimiento a los contractos con su estado que soportan la ejecución de los proyectos.
Lo anterior da cumplimiento al punto 4.6 Seguimiento y Evaluación de la Estrategia de TI.

Nota: Los aspectos de la guía validados por el equipo auditor son enfocados conforme al objetivo y alcance de la auditoría, los demás lineamientos relacionados en la guía se estarán validando en el espacio de otra auditoría con un objetivo y alcance diferente.

5.6 Validar la eficiencia y eficacia de la incorporación de módulos o actualizaciones en el aplicativo SAP

Partiendo del impacto que tiene SAP en los procesos de la EAAB-ESP se identifica la participación de los módulos y el estado actual el cual, está conformado de la siguiente manera:

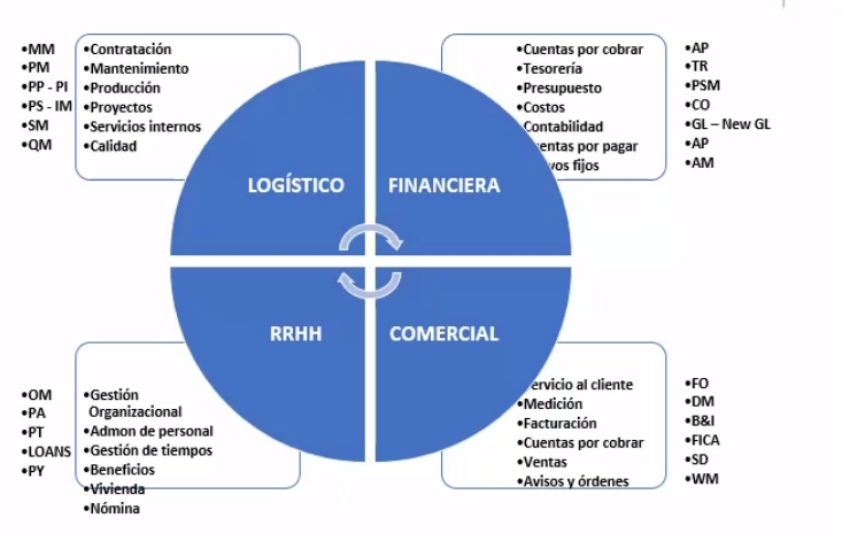


Figura 34. Participación de SAP en los procesos de la EAAB-ESP

Actualmente la versión de SAP (ECC 6.18) estará soportada por el proveedor hasta el 2027, con el fin de migrar a la nueva versión (S/4HANA Cloud), Gestión TIC adelanta actividades de análisis y consultoría a fin de madurar el proyecto.

El ejercicio de la auditoría verificó las actividades que se adelantan para la maduración del proyecto a proponer para el 2024, por lo anterior, queda pendiente incluir este punto para posteriores ejercicios de auditoría.

6. CONCLUSIONES DE LA AUDITORÍA.

6.1 Fortalezas.

- El procedimiento de MPFT0201- Atención de vulnerabilidades ejecuta las actividades conforme al procedimiento y estas corroboran la aplicabilidad de las políticas de operación establecidas en el mismo, se identificó compromiso del líder del procedimiento en el seguimiento y control de las actividades.
- La Gerencia de Tecnología en pro al cumplimiento de lo establecido en la política de Gobierno Digital respecto a la planificación y ejecución del Plan Maestro de tecnología ha adelantado actividades que permiten mantener los lineamientos establecidos.
- El proceso de Gestión TIC se adelanta (3 años) con el análisis y planificación de la migración del ERM (SAP) a su nueva versión antes de finalizar el soporte del fabricante en su versión actual.
- Se resalta la disposición y atención de las áreas auditadas por la atención de la auditoría.

6.2 Comunicaciones de Alertas tempranas.

No Aplica

6.3 Observaciones

OBSERVACIÓN NO. 1

Uso inapropiado de Software no licenciado

Condición: Para la prueba de auditoría, se solicitó apoyo a la Mesa de ayuda por su canal telefónico el 27 de julio y 28 de agosto de 2023, en el primer soporte solicitaron descargar la aplicación AnyDesk versión gratuita e indicar el ID que este software genera para poder tomar el equipo en remoto, en el segundo soporte, nuevamente solicitan el ID para la toma del equipo en remoto, una vez finalizado el soporte el agente no cerró la conexión remota lo que permite que el agente pueda visualizar todo lo que se ejecutan en el equipo aun cuando ya no se está brindando el soporte.

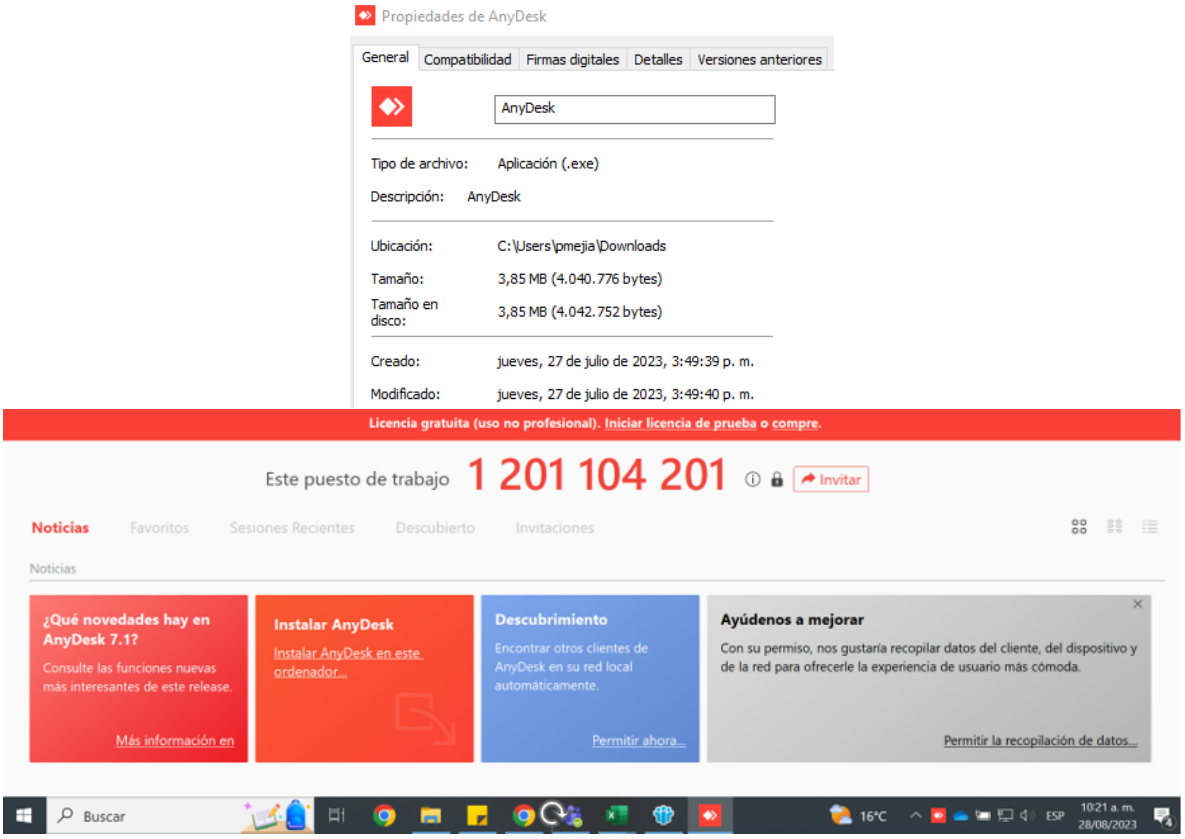


Figura 35. Fecha de descargue de Anydesk gratuito y evidencia de la conexión con el aplicativo gratuito

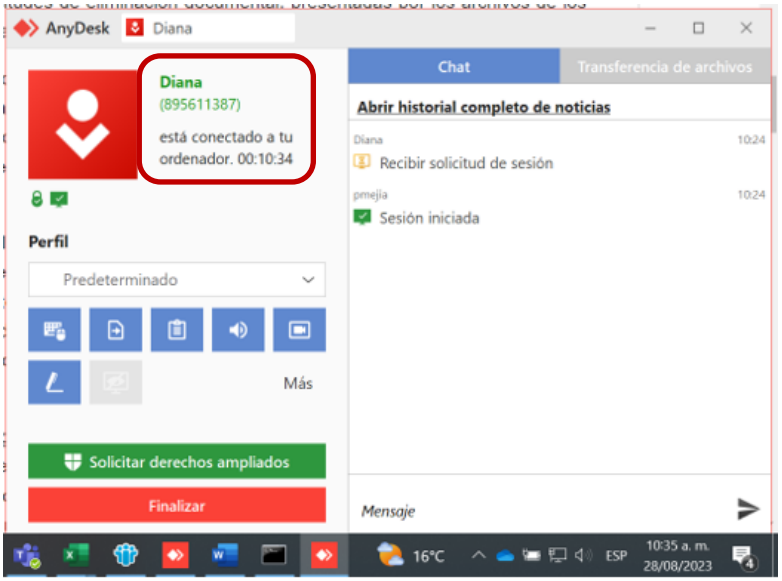


Figura 36. Duración de la conexión total en remoto

El cierre de la conexión se hizo desde el equipo tomado en remoto y no desde la conexión establecida por la Mesa de ayuda.

Esta auditoría identificó que en el año 2021 la EAAB-ESP adquirió 2.800 licencias del software de BMC Client Management para tomar los equipos en remoto de la entidad.

Criterio: Acuerdo 11 de 2013, artículo 68. Responsabilidades de la Dirección de Servicios Informáticas, ítem 6. *Desarrollar las acciones necesarias para garantizar que la entidad cumpla con las normas relacionadas con la defensa de los derechos de autor por el uso de programas de software en la Empresa*.

Causa: Debilidad o ausencia de una actividad que garantice la funcionalidad de BMC Client Management en todos los equipos de la EAAB-ESP para identificar y corregir aquellos que no se logran tomar en remoto y sensibilizar a los agentes de la Mesa de ayuda frente a la seguridad de la información para garantizar la confidencialidad de la información almacenadas en los equipos de los colaboradores una vez se finalice el soporte técnico.

Consecuencias: Lo anterior pone a la EAAB-ESP a demandas y posibles sanciones por el uso inadecuado de software de terceros conforme a la Ley 603 del 2000 articulo 2 el cual dicta *"Las autoridades tributarias colombianas podrán verificar el estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación, también se evadan tributos*".

OBSERVACIÓN NO.2

Falla en la ejecución de las actividades de Gestión de Solicitudes (requerimientos) conforme a las buenas prácticas de ITIL

Condición: Del alcance de la auditoría (último trimestre del 2022 y primer semestre del 2023), se identificó 10.207 tickets generados para el 2022 y 36.107 para el 2023, el 18,35% (1.873) en 2022 y el 20.34% (7.347) en 2023 corresponden a solicitudes de información las cuales quedaron registradas a nombre de la mesa de ayuda centro de servicios y no a nombre de colaborador, por lo cual no se genera una encuesta de satisfacción que aporte a le mejora continua del procedimiento.

USUARIOS DE LA DSI

No.	USUARIO	CANTIDAD	% PARTICIPACIÓN
1	Mesa de ayuda Centro de servicios	9551	**68,5%**
2	WS IGA Remedy	2043	14,7%
3	Jenny Andrea Chaparro Perez	1463	10,5%
4	ChatBot 7777	239	1,7%
5	Oscar Humberto Chacon Vega	133	1,0%
6	Maria Del Pilar Zapata Castillo	126	0,9%
7	Vladimir Largo Perilla	108	0,8%
8	Angelica Maria Algarra Parra	104	0,7%
9	Yimmy Alberto Roncancio Ramirez	94	0,7%
10	Juan Carlos Montejo Escobar	80	0,6%
	Total	***13941***	***100,0%***

Figura 37. Top 10 de los usuarios que más generan solicitudes a la Mesa de ayuda último trimestre de 2022 y primer trimestre del 2023

La anterior situación además de ser una mala práctica genera una posible incertidumbre sobre la ocurrencia en la prestación del servicio, ya que se puede asociar con la diferencia que se encuentra entre los datos registrados en las datas de telefonía y correo frente al reporte dado por los contratistas de servicio, situación explicada en la observación 3. Figura 38.

Criterio: Contrato 1-05-26500-0848-2021 Anexo 2 Condiciones técnicas y de servicio del numeral 6.5.1.2 Características del servicio – mesa de servicio ítem 3. *"Implementar un servicio basado en procesos de atención a servicios de TI (basados en ITIL e ISO 20000) para permitir una gestión y relación adecuada con los usuarios…"*

Norma NTC/IEC 20000, 8.3.2 Gestión de Relaciones de Negocio, 4 párrafo cita**: "***La organización debe, a intervalos planificados medir la satisfacción con los servicios tomando como base una muestra representativa de clientes. Los resultados se deben analizar, revisar para identificar oportunidades de mejora e informar"*

Causas: Falta de profundizar la aplicabilidad de las buenas prácticas orientando la gestión en la mejora continua de la prestación del servicio.

Consecuencia: Desvió en la implementación y gestión de las buenas prácticas adoptadas por el proceso Gestión TIC de la EAAB-ESP dificultando identificar el área, dirección o colaborador que genera consultas recurrentes sobre los servicios que pueden ser atendidos en la Mesa de ayuda e identificar oportunidades de mejora para fortalecer las capacitaciones sobre los sistemas de información, servicios o herramientas tecnológicas, lo que contribuye a la implementación de estrategias en pro a la mejora del procedimiento.

OBSERVACIÓN NO. 3

Incumplimiento en la recepción y registro de las peticiones y objetivo establecido en el procedimiento MPFT0302P- Gestión de Mesa de Ayuda V1.

Condición: De los 10.207 tickets generados para el 2022 y 36.107 para el 2023, se evalúa el cumplimiento de las políticas de operación y objetivo del procedimiento en la gestión realizada en los periodos del 16 oct al 15 de nov, 16 nov al 15 dic del 2022, 16 mayo al 15 de jun y del 16 de jun al 15 jul de 2023, identificando diferencias de la cantidad de tickets creados frente a los casos recibidos por los canales activos (telefonía y correo electrónico) como se muestra a continuación:

INFORMACIÓN DATAS POR CADA CANAL

Año	Periodo / Canal	Telefónico	Correo	Total Recibidos	**Tickets Registrados	Diferencia
2022	16 Oct al 15 Nov	2.886	611	3.497	4.668	1.171
	16 Nov al 15 Dic	3.292	673	3.965	5.539	1.574
2023	16 May al 15 Jun	2.987	566	3.553	4.851	1.298
	16 Jun al 15 Jul	2.538	503	3.041	4.285	1.244

INFORMACIÓN TICKETS REGISTRADOS EN LA HERRAMIENTA POR CANAL DE RECEPCIÓN

Año	Periodo / Canal	Telefónico	Correo	AutoServicio	Otros	Tickets Registrados
2022	16 Oct al 15 Nov	2.937	1.410	305	16	4.668
	16 Nov al 15 Dic	3.455	1.715	354	15	5.539
2023	16 May al 15 Jun	3.050	1.428	367	6	4.851
	16 Jun al 15 Jul	2.552	1.297	431	5	4.285

Figura 38. Análisis de datas de telefonía y correo Vs tickets registrados en la herramienta de gestión.

*****Tickets Registrados**: Corresponde a la data de los tickets creados por los agentes de la Mesa de Ayuda, con la respectiva tipificación según el canal por el cual se recibió la petición del colaborador.*

Se crearon 214 tickets más en el 2022 y 77 en el 2023 de las llamadas recibidas, de igual forma se evidencia una diferencia de casi el 100% más en el canal de correo.

Se identificó de la herramienta de gestión, el registro de los incidentes o solicitudes por otros medios no establecidos en el procedimiento como lo son: Administración de Sistemas, Autoservicio, Entrega Directa, Escalación Externa y

Otro, de la siguiente manera el 6.87% (321) de los tickets del periodo del 16 oct al 15 nov, 6.66% (369) del 16 nov al 15 dic 2022, y 11.18% (4.023) del primer semestre del 2023 como se muestra a continuación:

Cuenta de Fuente Reportada	Etiquetas		
Etiquetas de fila	Incidente	Orden de Trabajo	Total general
Autoservicio		300	300
Autosesrvicio	5		5
Correo Electronico	90	1320	1410
Entrada Directa	13	2	15
Otro		1	1
Teléfono		2199	2199
Telfono	738		738
Total general	846	3822	4668

16 de octubre al 15 de noviembre

Cuenta de Fuente Reportada	Etiquetas		
Etiquetas de fila	Incidente	Orden de Trabajo	Total general
Administración de Sistemas	1		1
Autoservicio		354	354
Correo Electronico	129	1586	1715
Entrada Directa	10	1	11
Ótro	3		3
Teléfono		2719	2719
Telfono	736		736
Total general	879	4660	5539

16 de noviembre al 15 de diciembre

Cuenta de Fuente Reportada	Etiquetas de columna		
Etiquetas de fila	Incidente	Orden de Trabajo	Total general
Administración de Sistemas	1		1
Autoservicio		3970	3970
Autosesrvicio	3		3
Correo Electronico	709	9279	9988
Entrada Directa	44	4	48
Escalación Externa		1	1
Otro		13	13
Ótro	3		3
Teléfono		18600	18600
Telfono	3358		3358
Total general	4118	31867	35985

Casos registrados en el primer semestre del 2023

Figura 39. Diferentes canales de comunicaciones registrados en la herramienta de gestión

Criterio: Procedimiento MPFT0302P- Gestión de Mesa de Ayuda V1 objetivo el cual idica: "*Ser el único punto de contacto entre el proveedor de servicios y los usuarios del Acueducto, donde se registren todas las llamadas…"*

Gestionar todos los servicios y solicitudes registrados, vía telefónica, web, correo electrónico, SRM, por medio de la herramienta de mesa de ayuda. Centralizando todos los casos de los usuarios, para llevar un registro de los incidentes y requerimientos que se presentan; el tiempo de respuesta y solución; repetibilidad de los problemas. Que los servicios y solicitudes correspondan a lo contratado entre el proveedor del servicio de Mesa de Ayuda y la EAAB".

Dentro de la auditoría se evidenció que la herramienta Digital WorkPlace se encuentra en parametrización para que los colaboradores puedan radicar y hacer seguimiento a sus casos vía web.
Política de operación No. 1 la cual indica: *"Las recepciones de los servicios y solicitudes a la mesa de ayuda, se recibirán por vía telefónica, a través de la extensión 7777, SRM y correo electrónico.",*

Causa: Ausencia o debilidad de un rol o procedimiento que asegure la calidad de la información en las datas, parametrizaciones y garantice el cumplimiento del procedimiento y las buenas prácticas.

Consecuencia: Incumplimiento del procedimiento MPFT0302P- Gestión de Mesa de Ayuda" por lo cual dificulta la adopción y adaptación de los procesos de ITIL conforme a lo establecido en el "anexo 2-Condiciones Técnicas Contrato Maestro Informática-Modificación punto 6.5.1.2 Características del servicio – mesa de servicio, numeral de igual forma incumple conforme a la práctica de Mesa de servicio establecida por ITIL que indica *"*El propósito de la práctica de la mesa de servicios es capturar la demanda de resolución de incidentes y solicitudes de servicio. También debe ser el punto de entrada y el único punto de contacto del proveedor de servicios con todos sus usuarios. la Mesa de ayuda o Service Desk es el único punto de contacto*".

**AXELOS® ITIL® Foundation, "Practica Mesa de servicios Service Desk*"

OBSERVACIÓN NO. 4

Debilidad en la identificación y/o ejecución de las actividades para el tratamiento de encuestas de satisfacción sobre la prestación del servicio de la Mesa de ayuda y soporte en sitio.

Condición: Del alcance de la auditoría (último trimestre de 2022 y primer semestre del 2023) se tomó las encuestas contestadas del 16 oct al 15 nov de 2022 y del 16 may al 15 de jun de 2023 identificando lo siguiente:

Periodo evaluado	Encuestas contestadas	**Encuestas Negativas	% de participación Encuestas Negativas
16 de oct al 15 Nov 2022	1.180	79	6,69%
16 de may al 15 jun 2023	1.330	114	9,66%
Total	**2.510**	**193**	**7.7%**

Tabla 4. Encuestas generadas e identificación de las que presentaron mal calificación.

***Encuesta negativa se determinó conforme a lo manifestado por el área auditada, cuando se presenta una calificación 1. Muy Mala, 2. Mala, 3. Regular en cualquiera de las 4 primeras preguntas.*

En la prueba de recorrido y análisis de la información suministrada no se evidenció un procedimiento que incluya el análisis e identificación de errores en la data y tratamiento de las encuestas de satisfacción (método de identificación de las encuestas negativas, protocolo de comunicación y atención con los colaboradores insatisfechos, análisis de resultados, etc), que involucre de manera activa y oportuna a los colaboradores que han manifestado en su calificación alguna oportunidad de mejora.

También se hizo un análisis al 8.5% (213) observaciones de las 2.510 encuestas registradas en la pregunta número 5 que sugieren una mejora en la prestación del servicio, se procedió a estandarizar las observaciones obteniendo el siguiente resultado:

No.	Comentario estandarizado	2022	2023	Total, general
1	Demora en la atención y/o Solución	31	51	82
2	Cerrado sin gestión o solución no efectiva	17	21	38
3	Capacidad Técnica (conocimiento del personal de la mesa de ayuda o soporte en sitio en la funcionalidad de los sistemas de información de la EAAB-ESP)	8	10	18
4	Encuesta a destiempo	5	13	18
5	Optimizar los procesos	2	15	17
6	Cerrado sin Contactar al Colaborador	4	7	11
7	Capacitar al colaborador nuevo (en los sistemas de información y en cómo reportar casos a la mesa)	8	2	10
8	Encuesta Repetida	3	1	4
9	Mejorar encuesta	1	3	4
10	Mala práctica de Call center	1	2	3
11	Ampliar presencia de Técnico en Sitio	2		2
12	Mejorar Actitud de servicio	1	1	2
13	Empatía en la comunicación escrita		1	1
14	Mejorar solución de primer nivel	1		1
15	Mejorar comunicación entre Mesa y Soporte en Sitio	1		1

No.	Comentario estandarizado	2022	2023	Total, general
16	Falta de documentación del caso	1		1
	Total general	**86**	**127**	**213**

Tabla 5. Comentarios unificados de 213 encuestas de satisfacción

Adicional a lo anterior, se identifica encuestas incompletas, o duplicadas como se muestra a continuación:

Tipo de solicitud	Cantidad de solicitudes		Cantidad de preguntas realizadas de las 5 establecidas
	2022	2023	
Orden de Trabajo	6	10	4
	8	9	3
	3	13	2
	0	3	1
	0	3	10
Total	**17**	**38**	

Tabla 6. Encuestas incompletas identificadas en el periodo auditado

Criterio: Objetivos estratégicos y características del servicio de la Mesa de ayuda establecidas en el numeral 6.5.1.2 punto 3 *"Implementar un servicio basado en procesos de atención a servicios TI (basados en ITIL e ISO 20000) para permitir una gestión y relación adecuada con los usuarios…"* y *20 "Realizar encuestas de satisfacción inmediatamente después de haber utilizado el servicio de la Mesa de servicio por los usuarios e informar del resultado."* del anexo 2 del contrato 1-05-26500-0848-2021 establecido con el proveedor de Servicios.

Causa: Ausencia de un procedimiento y responsable que identifique, analice, atienda de manera oportuna todas las observaciones registradas en las encuestas de satisfacción y ejecute actividades de corrección en pro a la mejora continua.

Debilidad en las actividades se seguimiento y control a la ejecución de las actividades del proveedor.

Consecuencias: Quejas y/o reclamos por parte de los colaboradores, incumplimiento de la norma NTC-ISO/IEC 20000, disminuir su percepción positiva respecto a la prestación de los servicios de la Mesa de ayuda y soporte en sitio e incumplimiento a la norma no actuar de manera preventiva para la mejora en la prestación del servicio.

OBSERVACIÓN NO. 5

Debilidad en las actividades de Control y seguimiento al cumplimiento contractual con el proveedor de Servicios.

Condición: Se evalúa el volumen de los incidentes y requerimiento registrado en los 9 informes (gestión del último trimestre del 2022 y primer semestre del 2023), se evidencia que en los 9 informes suman las llamadas colgadas, de prueba y equivocadas (501 para el 2022 y 1.640 para el 2023) como gestión efectiva a la Gestión de Solicitudes u Ordenes de trabajo, como se muestra a continuación:

16 Oct a 15 Nov 2022

Servicios	Total Servicios
Incidente	846
Orden de Trabajo	3.822
Total general	4.668

229 Llamadas colgadas y de pruebas incluidas

16 Mar a 15 Abr 2023

Servicios	Total, Servicios
Incidente	505
Orden de Trabajo	4.609
Total, general	5.114

216 Llamadas colgadas y de pruebas incluidas

16 Nov a 15 Dic 2022

Servicios	Total, Servicios
Incidente	879
Orden de Trabajo	4.660
Total general	5.539

272 Llamadas colgadas y de pruebas incluidas

16 Abr a 15 May 2023

Servicios	Total, Servicios
Incidente	558
Orden de Trabajo	4.281
Total, general	4.839

217 Llamadas colgadas y de pruebas incluidas

16 Dic al 15 Ene 2022/2023

Servicios	Total, Servicios
Incidente	548
Orden de Trabajo	3.731
Total general	4.279

210 Llamadas colgadas y de pruebas incluidas

16 May a 15 Jun 2023

Servicios	Total, Servicios
Incidente	627
Orden de Trabajo	4.224
Total, general	4.851

265 Llamadas colgadas y de pruebas incluidas

16 Ene al 15 Feb 2023

Servicios	Total, Servicios
Incidente	738
Orden de Trabajo	5.431
Total general	6.169

261 Llamadas colgadas y de pruebas incluidas

16 Jun a 15 Jul 2023

Servicios	Total, Servicios
Incidente	527
Orden de Trabajo	3.758
Total, general	4.851

167 Llamadas colgadas y de pruebas incluidas

16 Feb a 15 Mar 2023

Servicios	Total, Servicios
Incidente	643
Orden de Trabajo	5.927
Total, general	6.570

304 Llamadas colgadas y de pruebas incluidas

Figura 40. Cantidad de incidentes y solicitudes reportadas por el proveedor Vs llamadas colgadas y de pruebas incluidas en la gestión

Este tipo de llamadas en la data tienen asociado un ANS y todas registran como cumplida, es de mencionar que en las buenas prácticas ITIL no se contempla este tipo de llamadas ni como incidentes ni como solicitudes ni tampoco son casos sujetos para tener asociado una medición, se profundiza la validación con el informe del 16 may a 15 junio 2023 encontrando:

Servicios	Total, Servicios
Incidente	627
Orden de Trabajo	4.224
Total, general	4.851

Figura 41. Datos reportados en el informe 25 de ejecución

De las Ordenes de trabajo se detectaron 265 llamadas entre colgadas y de pruebas con un ANS asociado como cumplido adicional a lo anterior 49 registros duplicados entre incidentes y ordenes de trabajo.

Filtro Módulo	Tipo de Incidente/Orden de	Número de INC/WO	EstadoINC_WO	Grupo de Soporte	Servicio	Categoria Operacional Nivel 3	Categoria Producto Nivel 2	Fecha de Inicio Medición	Fecha de Fin Medición	Fecha Vencimiento SVT	Estado de la Medición	Periodo	Mes Según informe
Orden de Trabajo	General	WO0000001475747	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	16/05/2023 10:02	16/05/2023 10:02	18/05/2023 8:02	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001475754	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	16/05/2023 11:05	16/05/2023 13:32	18/05/2023 9:05	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001475786	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	16/05/2023 14:39	16/05/2023 17:34	18/05/2023 11:39	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001475667	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	16/05/2023 8:04	16/05/2023 8:04	17/05/2023 15:04	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001475673	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	16/05/2023 8:16	16/05/2023 8:16	17/05/2023 15:16	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001476080	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	18/05/2023 9:47	18/05/2023 9:47	19/05/2023 16:47	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001476081	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	18/05/2023 9:49	18/05/2023 9:49	19/05/2023 16:49	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001475677	Cerrado	MESA DE AYUDA	TELEFONIA	LLAMADA DE PRUEBA	TELEFONIA	16/05/2023 8:28	16/05/2023 8:28	17/05/2023 15:28	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001475680	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	16/05/2023 8:35	16/05/2023 8:36	17/05/2023 15:35	Cumplido	16 May al 15 Jun	25
Orden de Trabajo	General	WO0000001475964	Cerrado	MESA DE AYUDA	INFORMATIVOS DEL 7777	LLAMADA COLGADA	TELEFONIA	16/05/2023 16:00	16/05/2023 16:00	18/05/2023 14:00	Cumplido	16 May al 15 Jun	25

Figura 42. Llamadas colgadas y de pruebas con ANS asociado

Dentro de la medición o cumplimiento de los ANS de las Ordenes de servicio, indica en el informe el cumplimiento del 99,84%, se verifica la obtención de esta información y se evidencia que incluye, los registros duplicados, llamadas colgadas y equivocadas y adicional se incluyen aquellos tickets cuyo estado de la medición están en un estado diferente al cumplido o terminado (atendidos y solucionados).

El 97,87% se genera excluyendo aquellos tickets que aún no se han gestionado, ahora sin tener en cuenta las llamadas colgadas, ni de prueba, el indicador quedaría en el 91,60% como se muestra a continuación:

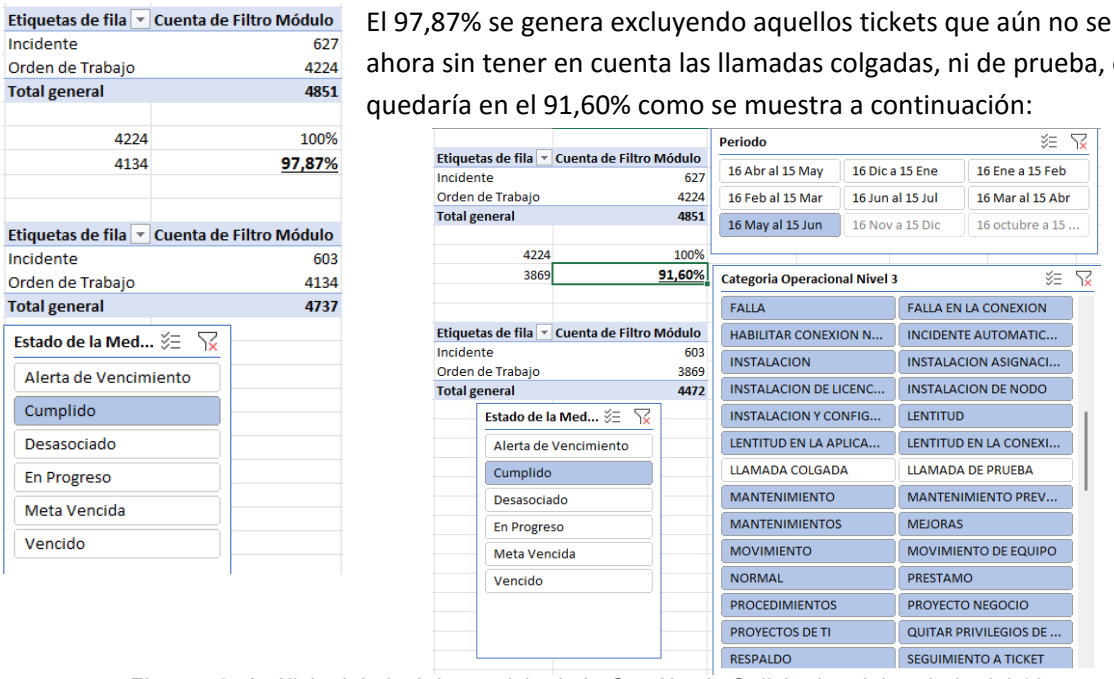


Figura 43. Análisis del nivel de servicio de la Gestión de Solicitudes del periodo del 16 may al 15 jun.

Es de mencionar que los estados, "alerta de vencimiento", "Desasociado" y "En progreso" son tickets que siguen abiertos sin gestión o solución, y que los "Meta Vencida y Vencido" son los tickets que no cumplieron con el nivel de servicio por lo cual no entran en la medición.

Criterio: ***Objetivo del procedimiento*** *el cual cita: "…Gestionar todas los servicios y solicitudes registrados, vía telefónica, web, correo electrónico, SRM, por medio de la herramienta de mesa de ayuda. Centralizando todos los casos de los usuarios, para llevar un registro de los incidentes y requerimientos que se presentan; el tiempo de respuesta y solución; repetibilidad de los problemas. Que los servicios y solicitudes correspondan a lo contratado entre el proveedor del servicio de Mesa de Ayuda y la EAAB***.**

Alcance del procedimiento el cual cita: *Inicia con el registro de la incidencia, petición o problema en la aplicación de Mesa de Servicio para el soporte técnico; culminando con la solución y cierre de la solicitud.*

Nota: *Las llamadas colgadas, de prueba no son una incidencia, petición o problema, tampoco generan un soporte técnico, ni una solución, por consiguiente, no están dentro del alcance del procedimiento y no forman parte de las mediciones para validar la efectividad de éste.*

Anexo No. 2 Condiciones técnicas y de servicio numeral 6.5.1.4 Informes ítem 1 *"Presentar el reporte sobre la gestión de ANS, incidentes y requerimiento que incluya -Volumen de incidentes y requerimientos que cumplen los niveles de servicio*.

La resolución 1148 del 07 de diciembre de 2018, por la cual "Se adopta el manual de supervisión e interventoría de la Empresa de Acueducto y Alcantarillado de Bogotá - ESP", **artículo quinto – Objeto de la supervisión e interventor**ía establece la finalidad de la supervisión e interventoría, las cuales son:

1. *Velar por el cumplimiento del objeto contractual*
2. *Proteger la moralidad administrativa*
3. *Prevenir la ocurrencia de actos de corrupción y*

4. *Tutelar la transparencia de la actividad contractual, en el marco de sus responsabilidades puntuales*

Lo anterior se deben observar según a 4 principios, el *principio de **Control** indica: "Se orienta fundamentalmente a constatar el cumplimiento del objeto del contrato de acuerdo con las especificaciones técnicas, las actividades administrativas, legales y financieras, dentro del plazo de ejecución establecido. Para tal fin se deben desarrollar labores de inspección, comprobación y evaluación, con el fin de establecer si la ejecución se ajusta a lo pactado, dentro del marco de responsabilidades que le son propias a la interventoría y a la supervisión propiamente dichas.*

Causa: Debilidad en la inspección y comprobación sobre la veracidad y confiabilidad de las bases de datos e informes suministrados por el proveedor para las mediciones del servicio y cumplimiento del procedimiento.

Consecuencias: Sanciones o reportes por incumplimiento a las responsabilidades de supervisión citadas en la resolución 1148 del 2018; Pérdida de oportunidad para establecer estrategias de manera oportuna y con información veraz.

Áreas sugeridas para el equipo de mejoramiento: Gerencia de TI, Seguridad de la información.

***Nota aclaratoria:** Las causas y consecuencias indicadas en las observaciones, son presuntas ya que se fundamentan en lo observado durante el ejercicio de auditoría, más no son objeto de análisis derivado de técnicas de identificación de causa raíz.*

7. RECOMENDACIONES PARA LA MEJORA.

RECOMENDACIÓN No. 1

Gestión del riesgo operativos y de seguridad de la información del proceso.

- Fortalecer la matriz de riesgos actual, en cuanto a la identificación de los riesgos teniendo como enfoque los eventos que afectan la consecución de los objetivos del proceso y de la entidad y el análisis de los factores generadores de riesgo para determinar las causas inherentes que aportan a la materialización de éste, incluir los relacionados con Seguridad Digital, a fin de documentar y/o implementar controles que permitan mitigar la materialización del riesgo.

RECOMENDACIÓN No. 2

Segregación de Funciones para la elaboración, revisión y aprobación de documentos, lineamientos, estrategias, metodologías etc.

- Dentro de la validación documental de los informes de gestión de la Mesa de Ayuda, se identificó que el responsable de la elaboración de los informes de gestión también firma la revisión del documento, por metodología y buenas prácticas la revisión la debe hacer un rol diferente para asegurar que la calidad de la información registrada en el informe no contenga errores estadísticos, de redacción, ausencia de análisis y confronte los resultados con las fuentes que lo originaron, con el objetivo de asegurar que los informes de gestión aporten de manera acertada la toma de decisiones estratégicas.

RECOMENDACIÓN No. 3

Fortalecer los procesos de soporte de la Gestión TIC que involucran a otras áreas.

- Se recomienda fortalecer la interacción (tiempos de atención y solución) con el proceso de creación y administración de los casos que son radicados y gestionados desde GIA, a fin de que la Mesa de ayuda pueda contar con información en línea de los casos y minimizar los tiempos de respuesta.

RECOMENDACIÓN No.4

Evidencia sobre el agendamiento concertado con los administradores para la ejecución del escaneo de vulnerabilidades

Mantener una evidencia sobre el conocimiento y entendimiento de los administradores de las plataformas tecnológicas sobre agendamiento parametrizado en el Software de vulnerabilidades a fin de garantizar que éstos tengan conocimiento y su apoyo en la ejecución del escaneo para suplir cualquier incidencia que se pueda presentar en el proceso.

DIFICULTADES DEL PROCESO AUDITOR:
Ninguna

EQUIPO AUDITOR

Auditor Líder: Leonardo Duque García

Auditor: Paola Andrea Mejía C.

Para constancia se firma en Bogotá D.C., a los 22 días del mes de 11 del año 2023

Firmado por MARIA NOHEMI PERDOMO RAMIREZ
el 22/11/2023 a las 09:12:41 COT

_____

Firma
Nombre: María Nohemí Perdomo Ramírez
Jefe Oficina de Control Interno y Gestión

Elaboró: Equipo Auditor
Copia: Ing. Adriana del Pilar Guerra – Directora de Servicios de Informática