INFORME DE AUDITORÍA INTERNA	acueducto AGUA Y ALCANTARILLADO DE BOGOTÁ
OFICINA DE CONTROL INTERNO Y GESTIÓN	

INFORME EJECUTIVO								
Nombre de la Auditoría Interna	**PROTECCIÓN DE DATOS PERSONALES LEY 1581 DE 2012**						**1050001-2020-0197**	
							N° Consecutivo	
Destinatario	**Dra. CRISTINA ARANGO OLAYA**							
	GERENTE GENERAL DE LA EAAB-ESP							
PROCESO:	GESTION COMERCIAL GESTION TIC			**SUBPROCESO**	MPMU05 - Atención al Cliente MPFT03 - Gestión de Servicios Informáticos MPFT02 - Gestión de Seguridad de la Información			
Dependencia / Área / Unidad Auditable	GERENCIA CORPORATIVA DE SERVICIO AL CLIENTE GERENCIA DE TECNOLOGÍA Y DIRECCION SERVICIOS DE INFORMATICA			**Responsable**	DR. NELSON VALENCIA VILLEGAS ING. NOEL VALENCIA LOPEZ ING. LINA MARIA CRUZ SILVA			
	SEGURIDAD DE LA INFORMACIÓN			**Responsable**	ING. ALVARO PINZÓN			
Reunión de Apertura	**19**	**05**	**2020**	**Reunión de Cierre**	**24**	**07**	**2020**	
	DIA	**MES**	**AÑO**		**DIA**	**MES**	**AÑO**	
Equipo Auditor								
Auditor Líder OCIG	**Gloria Piedad Roa Carrero**							
Auditor Líder de Grupo	**Luz Marina Gutiérrez Hernández**							
Auditor	**Carlos Alberto Guzmán Soriano**							
Dificultades del Proceso Auditor	Disponibilidad y oportunidad en el suministro de la información El tiempo de ejecución de la Auditoría Limitantes en la verificación de información física a consecuencia de las condiciones actuales del aislamiento preventivo obligatorio a consecuencia de la Pandemia COVID-19.							
Este "Informe Ejecutivo", solo relaciona información de interés para la Gerencia General de la EAAB-ESP, los resultados detallados de este proceso auditor (Resultados de la Auditoría), se ha puesto en conocimiento del(os) auditado(s) para que den inicio a la gestión correspondiente de acciones de mejora.								

1. OBJETIVO DE LA AUDITORÍA.

Evaluar el cumplimiento normativo de la EAAB-ESP frente a la Protección de Datos Personales - Ley 1581 de 2012.

2. ALCANCE DE LA AUDITORÍA.

Esta Auditoría evaluó la gestión y cumplimiento de los lineamientos de la Ley 1581 de 2012 Protección de Datos Personales en la EAAB-ESP para una muestra determinada en el período junio 2019 – mayo 2020. Para ello se consideró los siguientes aspectos:

- Políticas y procedimientos
- Análisis de Riesgos
- Cumplimiento de los responsables y encargados del tratamiento de datos
- Gestión y custodia de las autorizaciones de consentimiento del titular
- Tratamiento de datos sensibles
- Gestión de PQR relacionados
- Canales de comunicación
- Cumplimiento del Registro nacional de Bases de Datos
- Informes de gestión de acciones implementadas y gestión de incidentes Ley 1581.

Así mismo, se revisaron los planes de mejoras y actas de subcomité coordinación de Control Interno con el fin de identificar acciones relacionadas con el objeto de auditoría.

3. CONCLUSIONES DE LA AUDITORÍA

3.1 Aspectos Generales.

Resultado de la evaluación de cumplimiento normativo para la protección de datos personales Ley 1581 de 2012 y los Decretos 1377 de 2013 y 1074 de 2015, se identificaron observaciones y oportunidades de mejora para el fortalecimiento de la gestión realizada por la EAAB-ESP.

En el conocimiento de la gestión se identificó que, la Política de tratamiento de datos personales define que la Gerencia Corporativa de Servicio al Cliente es el líder de su cumplimiento, no obstante, en la comunicación enviada a la OCIG el 4 de junio de 2020, indican que dicha Gerencia no está de acuerdo con la asignación ya que esta decisión no fue comunicada ni concertada.

De otra parte, la Gerencia de Tecnología a través del Líder de seguridad de la información, (mail 16/07/2020), aportó dos documentos donde se evidencia la participación y aprobación de la Gerencia Corporativa de Servicio al Cliente y Dirección de Apoyo Comercial (Ayuda de memoria de la reunión del Grupo Técnico de Seguridad con fecha 24 de febrero de 2020 para la revisión y aprobación de la política de tratamiento de datos personales en la que se observa la participación del Director de Dirección de Apoyo Comercial y el acta de Comité Directivo de fecha 25 de febrero 2020 para la aprobación de la política de tratamiento de datos personales).

Lo anterior, permite identificar una controversia sobre el liderazgo de la gestión de la protección de los datos personales y considerando que el tratamiento de datos personales es un tema transversal y que implica a todas las Gerencias de la EAAB-ESP, es pertinente que, desde la Alta Gerencia y la Gerencia General, se evalúe la designación del Oficial de Protección de Datos Personales encargado de liderar coordinar, apoyar y verificar la implementación de la gestión de la Protección de Datos Personales en la EAAB-ESP. Esta observación se presenta en el numeral 6.3.

En la revisión de las actas de Subcomité Coordinación de Control Interno relacionados a los objetivos de la Auditoría Protección de Datos Personales no se encontraron acciones relacionadas.

- **Políticas y procedimientos aplicación Ley 1581**

Se cuenta con una política definida para la protección de datos personales, que fue actualizada y aprobada en febrero 2020. Sobre esta política y su implementación, se dialogó en las reuniones virtuales y por las diferencias entre la Gerencia Corporativa de Servicio al Cliente y la Gerencia de Tecnología se estaría revisando con instancias superiores como la Gerencia General y la Gerencia Corporativa de Planeamiento. Sin embargo, no se desconoce que la EAAB-ESP cuenta con controles implementados tanto a nivel de infraestructura tecnológica y en la operación en cada una de las áreas. Por el momento está pendiente definir qué área tendrá el liderazgo y establecerá el Gobierno de la Protección de Datos Personales.

- **Cumplimiento de los responsables y encargados del tratamiento de datos**

Como parte de la operación diaria en cada una de las áreas que gestionan datos personales se tiene establecido el diligenciamiento de formatos para obtener los datos personales y firmas de autorización de los titulares para los trámites que así lo requieran.

Los sistemas de información de la EAAB-ESP, tienen definidos controles de identificación y autenticación, roles y perfiles asignados de acuerdo a la función de los usuarios, lo anterior como cumplimiento de las políticas de seguridad de la información establecidas en la Entidad.

En la RNBD - SIC se registran los siguientes datos

RESPONSABLE DEL TRATAMIENTO	
Nombre o Razón Social	EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE BOGOTA ESP
Tipo de Documento	NUMERO DE IDENTIFICACION TRIBUTARIA
Número de Documento	899999094
Naturaleza	Pública
Actividad Económica	Captación, tratamiento y distribución de agua
Sitio Web	www.acueducto.com.co
Cantidad de Bases de Datos Inscritas	15

En la política de “tratamiento de datos personales” se referencia los puntos de contacto por los cuales serán atendidas las solicitudes de tratamiento de datos personales:

Teléfono (PBX): 3447000
Dirección: Av. Calle 24 No. 37-15, Bogotá D.C.
Portal web: www.acueducto.com.co
Correo electrónico: protecciónddedatos@acueducto.com.co

En la política de tratamiento de datos personales se encuentra como líder a la Gerencia Corporativa de Servicio al Cliente y es la responsable por dar respuesta al usuario, es importante indicar que los dueños de los procesos en la EAAB-ESP son los responsables en atender los requerimientos de información que sean solicitados por este concepto.

- **Gestión y custodia de las autorizaciones de consentimiento del titular**

En las reuniones virtuales con los funcionarios de las áreas que manejan datos personales, se indicó que el archivo y custodia de las autorizaciones de consentimiento del titular en físico cumplen el procedimiento de archivo documental y se mantiene en archivo el tiempo estipulado en las tablas de retención documental. Después de cumplir el tiempo establecido en el archivo del área pasan al archivo general de la EAAB-ESP.

El mantenimiento de los sistemas de información, Bases de datos y almacenamiento de la información están a cargo de la Gerencia de Tecnología – Dirección Servicios de Informática los cuales están alineados a las políticas de seguridad de la información, y las áreas que gestionan datos personales son las responsables de definir los niveles de protección de los datos gestionados en la plataforma tecnológica y de solicitar los ajustes a que haya lugar a la Gerencia de Tecnología.

- **Tratamiento de datos sensibles**

De acuerdo a las reuniones con el líder de seguridad de la información indicó que desde hace tiempo se viene trabajando con cada Gerencia en la identificación de activos de información y su clasificación, en el desarrollo de esta actividad los dueños de los procesos definieron los datos sensibles que se gestionaban en su proceso. Con esta información se definieron los controles a nivel de roles y perfiles para el acceso a los sistemas de información.

Las Gerencias que se entrevistaron indicaron que en sus áreas es controlado a través de los perfiles asignados a los usuarios para la gestión de la información en los sistemas de información y cuando la información sensible es gestionada en físico está restringida a unos pocos funcionarios.

- **Gestión de PQR relacionados con Protección de Datos Personales**

La EAAB-ESP tiene a disposición el canal PQR`s (Peticiones, Quejas, Reclamos y Recursos de Reposición) en la página web, al igual está a disposición el chat, Call Center y las Oficinas, los cuales son gestionados a través de la Gerencia de Servicio al Cliente.

Al indagar si se presentan PQR`s relacionados con datos personales las Gerencias entrevistadas indicaron que no se presentan este tipo de solicitudes. En el caso de presentarse se daría el mismo tratamiento de canalizar al área responsable y generar su respuesta en los tiempos establecidos en la ley.

- **Canales de comunicación**

La empresa tiene disponible varios canales de comunicación para la recepción de solicitudes de los usuarios. Entre estos canales de comunicación se tienen los presenciales como los puntos propios de la EAAB-ESP, los cades y supercades, atención telefónica Acua-Linea 116 con su Call Center y virtuales disponibles en la página Web el correo electrónico, chat, video llamada y llamada.

- **Cumplimiento del Registro nacional de Bases de Datos**

La empresa ha cumplido con el Registro Nacional de Bases de Datos ante la Superintendencia de Industria y Comercio- SIC, dejando inscrito desde enero de 2019 las 14 Bases de datos que contienen datos personales, con lo cual dio cumplimiento a la Ley 1581 de 2012.

- **Informes de gestión de acciones implementadas y gestión de incidentes Ley 1581.**

Con relación a los informes de gestión no se obtuvo evidencia. Las directrices para la implementación de la nueva Política están pendientes.

- **Actas de Subcomité Coordinación de control Interno**

En la revisión de las actas de Subcomité Coordinación de Control Interno de la Gerencia de Tecnología se buscó acciones asociadas a los objetivos de la Auditoría Protección de Datos Personales, sin encontrar acciones relacionadas.

3.2 Fortalezas.

- ✓ La EAAB-ESP cuenta una nueva Política de Protección de datos publicada en febrero de 2020.
- ✓ La EAAB-ESP cuenta un inventario de activos de información que identifican si se incluyen datos personales.

3.3 Observaciones

"Las OBSERVACIONES, deben ser objeto de Plan de Mejoramiento en el marco del procedimiento de -Mejoramiento Continuo- de la EAAB-ESP, con el fin de eliminar las causas que les dieron origen. La OCIG analizará y verificará la efectividad de las acciones formuladas y gestionadas en el marco de los seguimientos a los Planes de mejoramiento o en próximas auditorías del proceso o tema en cuestión".

OBSERVACION 1	
Condición	**Definir y designar el Rol de Oficial de Protección de Datos Personales** Se evidencia que, la EAAB-ESP no cuenta con un rol de "Oficial de protección de datos personales" de acuerdo a los lineamientos establecidos en la "Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability)" del 28 de mayo de 2015, en concordancia con el artículo 26 y 27 del Decreto 1377 de 2013. La adecuada implementación del marco legal en datos personales indicado en la "Guía para la implementación del Principio de Responsabilidad Demostrada", está relacionado con la designación de competencias que realice la alta gerencia en las diferentes áreas de su organización y de la designación del Oficial de Protección de Datos Personales. Lo anterior, incumple la Ley 1581 de 2012 y sus decretos reglamentarios.
Efecto / Impacto	1. Sanciones por Incumplimiento de regulaciones internas y externas relacionadas con protección de datos personales. 2. Deterioro de la imagen ante usuarios u otros grupos de interés. (por fallas en el tratamiento de datos). 3. Debilita el Sistema de Control interno en el componente Ambiente de Control.
Responsable	Gerencia General Gerencia Corporativa de Servicio al Cliente Gerencia de Tecnología

Recomendaciones de la OCIG a la Observación.	1. Se recomienda al Comité institucional de gestión y desempeño revisar la competencia que le ha sido dada a Gerencia Corporativa de Servicio al Cliente frente a la asignación y responsabilidad del tratamiento de datos personales, con el fin de dirimir o concertar el área y/o estructura que adopte el liderazgo y sus responsabilidades frente al cumplimiento normativo. 2. Una vez se revise y determine quien asumirá la responsabilidad, se recomienda definir y designar el rol de oficial de protección de datos personales, donde considere como mínimo las siguientes funciones: • Establecer el Gobierno de los datos en la EAAB-ESP • Definir y establecer las políticas y procedimientos para la protección de datos personales en la EAAB-ESP • Definir el procedimiento para la gestión de incidentes y establecer acciones para mitigar los riesgos y su impacto • Definir los lineamientos para la respuesta de PQRs relacionados con la protección de datos personales en la EAAB-ESP • Controlar y mantener actualizado el inventario de información personal para identificar y evaluar usos y divulgaciones. • Evaluar los riesgos y definir controles para la protección de los datos • Definir y ejecutar planes de capacitación que sensibilicen y concienticen la protección de datos gestionados en los diferentes procesos. • Revisar, actualizar, modificar contratos suscritos con los encargados del tratamiento de los datos. • Revisar, actualizar, modificar los formatos de autorización y los textos que deben llevar dando cumplimiento a la Ley y el uso de la información. • Reportar semestralmente a la Alta Gerencia la evolución del riesgo, los controles implementados, el monitoreo y estado general del programa de protección de datos personales. Para el cumplimiento de su función, el Oficial de protección de datos es el garante de la implementación de buenas prácticas de gestión de los datos personales en la EAAB-ESP, es por ello que debe considerar como mínimo las siguientes directrices: • Estructurar, diseñar y administrar el Programa Integral de Gestión de Datos Personales para cumplir las normas sobre protección de datos personales. • Servir de enlace y coordinador con las demás áreas de la organización para asegurar la implementación transversal del Programa Integral de Gestión de Datos Personales. • Promover la cultura de protección de datos en la EAAB-ESP. • Mantener un inventario de las bases de datos personales de la EAAB-ESP y clasificarlas según su tipo. • Registrar las bases de datos de la EAAB-ESP en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo las instrucciones emitidos por la SIC. • Obtener las declaraciones de conformidad de la SIC.

	• Analizar las responsabilidades de cada cargo de la EAAB-ESP, para diseñar un programa de entrenamiento en protección de datos específicos acorde con los procesos a su cargo. • Realizar el entrenamiento general en protección de datos a todos los empleados, funcionarios, contratistas de la EAAB-ESP. • Realizar el entrenamiento a los nuevos empleados, funcionarios, contratistas que por sus funciones gestionan datos personales. • Integrar las políticas de protección de datos personales dentro de las actividades de las áreas de la EAAB-ESP (talento humano, seguridad, call centers, gestión de terceros, etc.).

NOTA: Los análisis de causas y recomendaciones de la OCIG a las observaciones del presente informe son indicativas y no eximen del análisis de causa y formulación de planes de mejora que le corresponden al responsable en el marco del procedimiento de Mejoramiento Continuo de la EAAB-ESP.

OBSERVACION 2	
Condición	**Definir los procedimientos específicos para cada proceso donde se realiza tratamiento de datos personales, para dar cumplimiento a la Ley 1581/2012 y sus decretos reglamentarios.** Se observó que la EAAB-ESP, no tiene definido procedimientos específicos que den cumplimiento a la política de tratamiento de datos personales de acuerdo a la Ley 1581 y Decreto 1377 de 2013 Artículo 11, Decreto 1071 de 2015 Artículo 2.2.2.25.2.1 y Decreto 1074 de 2015 sección 2 artículo 2.2.2.25.2.2. y 2.2.2.25.3.1, lo cual podría acarrear sanciones de Ley a la EAAB-ESP.
Efecto / Impacto	1. Sanciones por Incumplimiento de regulaciones internas y externas relacionadas con protección de datos personales. 2. Afectación negativa de personas por el Incumplimiento a la protección de los datos personales debido a los daños o perdidas de la información (grabación, vídeos, papel, magnético, entre otras). 3. Deterioro de la imagen ante usuarios u otros grupos de interés. 4. Debilita el Sistema de Control Interno – SCI- componente Ambiente de Control.
Responsable	Gerencia Corporativa de Servicio al Cliente
<u>Recomendaciones de la OCIG a la Observación.</u>	Se recomienda que la EAAB-ESP establezca procedimientos estandarizados y/o se actualicen los existentes con el fin de definir las actividades de control que se deben aplicar para protección y tratamiento de los datos personales y el cumplimiento de las políticas de seguridad y privacidad vigentes. Para que el aseguramiento de las actividades de control se cumpla, se debe establecer un programa de mejoramiento continuo en el cual se considere la validación y verificación del cumplimiento de los requisitos exigibles en la Ley 1581 de 2012 y sus decretos reglamentarios. Lo anterior debe venir acompañado de una sensibilización y concienciación que asegure una cultura organizacional e individual dirigido a la protección de datos personales.

NOTA: Los análisis de causas y recomendaciones de la OCIG a las observaciones del presente informe son indicativas y no eximen del análisis de causa y formulación de planes de mejora que le corresponden al responsable en el marco del procedimiento de Mejoramiento Continuo de la EAAB-ESP.

OBSERVACION 3	
Condición	**Falta Identificación, Medición, Control de Riesgos de Gestión y Corrupción** Se observó que, no hay riesgos relacionados con el cumplimiento normativo Ley 1581 de 2012 y sus decretos reglamentarios, según lo verificado en la Matriz de Riesgos Institucional a 31/12/2019 en los procesos Gestión TIC y Gestión Comercial, incumpliendo la metodología de riesgos en lo relacionado al contexto externo, lo cual puede acarrear sanciones de Ley.
Efecto / Impacto	1. Debilidad en la identificación, medición, control y seguimiento de riesgos exponiendo a la EAAB-ESP. 2. Debilita el Sistema de Control Interno – SCI- en el componente Gestión del Riesgo.
Responsable	Gerencia Corporativa de Servicio al Cliente Gerencia de Tecnología
Recomendaciones de la OCIG a la Observación.	Se recomienda analizar la regulación legal vigente acerca de la Protección de Datos Personales, con el fin de identificar los posibles riesgos y evaluar su registro en la matriz de riesgos del proceso correspondiente que permita su gestión, valoración de probabilidad e impacto, calificación riesgo inherente, identificación de controles y establecimiento del riesgo residual al igual que su gestión y seguimiento. En el ejercicio de auditoría el equipo auditor, identificó riesgos del proceso de protección de datos personales, que pueden ser considerados para su análisis e inclusión.
NOTA: Los análisis de causas y recomendaciones de la OCIG a las observaciones del presente informe son indicativas y no eximen del análisis de causa y formulación de planes de mejora que le corresponden al responsable en el marco del procedimiento de Mejoramiento Continuo de la EAAB-ESP.	

OBSERVACION 4	
Condición	**Ajustar el "Aviso de privacidad" en los formatos dispuestos en los canales virtuales y formatos físicos referente a la Ley 1581 de 2012.** Se observó que, en los formatos dispuestos en los canales virtuales, tales como: página web, video llamada, llamada, chat y los formatos físicos de Derecho de Petición y Recurso de Reposición y en subsidio de apelación, no se referencia la ley 1581, de igual forma se identifica que en los avisos se sugiere consultar la Política de Tratamiento de Datos, la cual debería estar al alcance del usuario y tener la opción de aceptar o no esta autorización. Lo anterior incumple la Ley 1581 de 2012 y el Decreto 1074 de 2015 en sus artículos 2.2.2.25.1.3, 2.2.2.25.3.4. y 2.2.2.25.3.5, lo cual podría acarrear sanciones de Ley a la EAAB-ESP.
Efecto / Impacto	1. Sanciones por Incumplimiento de regulaciones internas y externas relacionadas con protección de datos personales. 2. Afectación negativa de personas por el Incumplimiento a la protección de los datos personales debido a los daños o perdidas de la información (grabación, vídeos, papel, magnético, entre otras). 3. Debilita el Sistema de Control Interno en el componente Información externa.

Responsable	Gerencia Corporativa de Servicio al Cliente Gerencia de Tecnología
Recomendaciones de la OCIG a la Observación.	Se recomienda considerar los siguientes aspectos para fortalecer los avisos de privacidad para el cumplimiento normativo de la EAAB-ESP así: Canales virtuales • incluir la opción de consulta de la política de tratamiento de datos personales mediante la habilitación de un link que presente la política de tratamiento de datos personales de la EAAB-ESP, al igual que un botón para que el usuario tenga la opción de aceptar o no el tratamiento de sus datos personales. • El aviso de privacidad en los formularios debe describir el uso y tratamiento de los datos e indicar la Ley 1581 de 2012, con el fin de dar claridad del cumplimiento normativo y se solicite la autorización expresa para su tratamiento. • En el guion de la acualinea 116, se debe incluir que los datos que el usuario dará para la atención cumplen con la política de tratamiento de datos, ley 1581 y cuál es la finalidad del tratamiento de datos, así mismo, se habilite una opción para éste indique su aceptación o no. Canales presenciales • En todos los formularios o comunicaciones donde se consigne información de datos personales de usuarios, se incluya el aviso de privacidad correspondiente a la política de tratamiento de datos personales, se referencie la Ley 1581 y se solicite la autorización expresa al usuario para el tratamiento de sus datos y su finalidad. • Almacenar los soportes de consentimiento físicos o digitales y estar disponibles cuando se requiera soportar que el cliente ha dado su autorización para el tratamiento de sus datos personales y establecer a nivel procedimental la periodicidad de actualización de este consentimiento.
NOTA: Los análisis de causas y recomendaciones de la OCIG a las observaciones del presente informe son indicativas y no eximen del análisis de causa y formulación de planes de mejora que le corresponden al responsable en el marco del procedimiento de Mejoramiento Continuo de la EAAB-ESP.	

OBSERVACION 5	
Condición	**Ajustar el "Aviso de privacidad" sobre el tratamiento de los datos y referencia a la Ley 1581 de 2012 en los formularios de PQRS** Se observó que, en los formularios de PQRs disponibles en la página web para que el usuario ingrese su petición, queja, reclamo o recurso de reposición, se solicita la autorización para el tratamiento de los datos; sin embargo, no se referencia la Ley 1581 dentro del texto y la política de tratamiento de datos no está disponible para que el usuario conozca el contenido de la política. Lo anterior incumple la Ley 1581 de 2012 y el Decreto 1074 de 2015 en sus artículos 2.2.2.25.1.3, 2.2.2.25.3.4. y 2.2.2.25.3.5, lo cual podría acarrear sanciones de Ley a la EAAB-ESP.

Efecto / Impacto	1. Sanciones por Incumplimiento de regulaciones internas y externas relacionadas con protección de datos personales. 2. Afectación negativa de personas por el Incumplimiento a la protección de los datos personales debido a los daños o perdidas de la información (grabación, vídeos, papel, magnético, entre otras). 3. Sanción por Incumplimiento de la atención PQRs sobre protección de datos personales. 4. Debilita el Sistema de Control interno- Información y Comunicación.
Responsable	Gerencia Corporativa de Servicio al Cliente Gerencia de Tecnología/Dirección Servicio de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda incluir en los formularios de los PQR´S, la opción de consulta de la política de tratamiento de datos personales mediante la habilitación de un link que permita conocer al usuario la política de tratamiento de datos personales de la EAAB-ESP. Así mismo, el aviso de privacidad describa el uso y tratamiento de los datos e indique la Ley 1581 de 2012, con el fin de dar claridad del cumplimiento normativo.
NOTA: Los análisis de causas y recomendaciones de la OCIG a las observaciones del presente informe son indicativas y no eximen del análisis de causa y formulación de planes de mejora que le corresponden al responsable en el marco del procedimiento de Mejoramiento Continuo de la EAAB-ESP.	

OBSERVACION 6	
Condición	**Promover la divulgación y sensibilización sobre las políticas de gestión en la Entidad.** Se evidenció durante el ejercicio de la auditoría, que la EAAB-ESP no cuenta con un programa que promueva la divulgación y sensibilización sobre la política de tratamiento de datos personales de la EAAB-ESP y la aplicación de la Ley 1581 de 2012 y sus decretos reglamentarios. Lo anterior da incumplimiento al Decreto Reglamentario 1074 de 2015, artículo 2.2.2.25.6.2 y artículo 2.2.2.25.6.2 generando posibles sanciones legales.
Efecto / Impacto	1. Deterioro de la imagen ante usuarios u otros grupos de interés. 2. Sanciones por Incumplimiento de regulaciones internas y externas relacionadas con protección de datos personales. 3. Debilita el Sistema de Control Interno en el componente Ambiente de Control.
Responsable	Gerencia Corporativa de Servicio al Cliente
Recomendaciones de la OCIG a la Observación.	Se recomienda que la entidad dentro de la estrategia de Gobierno y Gestión para el cumplimiento de la Ley 1581 establezca un programa de capacitación, dirigido a todos los funcionarios involucrados en el tratamiento de datos personales de la Entidad, además de una capacitación de mayor profundidad para los responsables y encargados del tratamiento de datos personales de la EAAB-ESP.
NOTA: Los análisis de causas y recomendaciones de la OCIG a las observaciones del presente informe son indicativas y no eximen del análisis de causa y formulación de planes de mejora que le corresponden al responsable en el marco del procedimiento de Mejoramiento Continuo de la EAAB-ESP.	

<table>
<tr><th colspan="2">OBSERVACION 7</th></tr>
<tr><td>Condición</td><td>Evaluar la reasignación o pertinencia del indicador “Autoevaluación del cumplimiento de las actividades de protección de datos personales”

Se evidenció que el indicador “Autoevaluación del cumplimiento de las actividades de protección de datos personales” no está siendo gestionado y medido por la Gerencia de Tecnología/Dirección Servicios de Informática, por cuanto esta Gerencia indica que no gestiona datos personales.

El indicador de gestión diseñado y propuesto en algún momento por la Gerencia de Tecnología y que se encuentra a su cargo, hoy no es procedente ya que se manifiesta que esta responsabilidad debe ser asumida por las áreas que tengan bajo su responsabilidad el tratamiento de datos personales.</td></tr>
<tr><td>Efecto / Impacto</td><td>1. Ausencia de monitoreo y seguimiento al cumplimiento de la protección de datos personales y el mejoramiento continuo.
2. Debilita el SCI en el componente Elementos de Control.</td></tr>
<tr><td>Responsable</td><td>Gerencia Corporativa de Planeamiento y Control/Dirección Planeación y Control de Resultados
Gerencia Corporativa de Servicio al Cliente
Gerencia de Tecnología</td></tr>
<tr><td><u>Recomendaciones de la OCIG a la Observación.</u></td><td>Evaluar la pertinencia del indicador que en este momento se encuentra asignado a la Gerencia de Tecnología.

Se recomienda a la Dirección Planeación y Control de Resultados, considerar los indicadores que fueron definidos en la Política de Tratamiento de Datos Personales para medir su cumplimiento. Estos indicadores son:
<table>
<tr><th colspan="5">INDICADORES TÁCTICOS O DE PROCESO
No aplica debido a que no existen procedimientos de tratamiento de datos personales.</th></tr>
<tr><th colspan="5">INDICADORES OPERATIVOS</th></tr>
<tr><th>CÓDIGO</th><th>NOMBRE</th><th>PROCESO</th><th>CATEGORÍA</th><th>FUENTE</th></tr>
<tr><td>ND</td><td>% de áreas con socialización realizada.</td><td>Gestión TI</td><td>Eficacia</td><td>Listados de asistencia y ayuda de memoria.</td></tr>
<tr><td>ND</td><td>% incidentes resueltos de seguridad de los datos personales</td><td>Todos los procesos que manejan datos personales</td><td>Eficacia</td><td>Resultado de la gestión de consultas, peticiones y reclamos.</td></tr>
<tr><td>ND</td><td>% de casos de tratamiento atendidos por la Dirección de cobro coactivo.</td><td>Gestión Financiera</td><td>Eficacia</td><td>Resultado de la gestión de cobro coactivo.</td></tr>
<tr><td>ND</td><td>% de casos de tratamiento atendidos por la Dirección Mejoramiento Calidad de Vida</td><td>Gestión Mejoramiento y Calidad de Vida</td><td>Eficacia</td><td>Resultado de la gestión de la Dirección Mejoramiento Calidad de Vida.</td></tr>
<tr><td>ND</td><td>% de casos de tratamiento atendidos por la Dirección Salud</td><td>Gestión Salud</td><td>Eficacia</td><td>Resultado de la Dirección Salud</td></tr>
<tr><td>ND</td><td>% de casos de tratamiento atendidos por la Dirección Seguridad.</td><td>Gestión de Servicios Administrativos</td><td>Eficacia</td><td>Resultado de la gestión de la seguridad física.</td></tr>
<tr><td>ND</td><td>% de casos de tratamiento atendidos por la Dirección Bienes Raíces.</td><td>Gestión Bienes Raíces</td><td>Eficacia</td><td>Resultado de la gestión de la Dirección Bienes Raíces</td></tr>
</table></td></tr>
<tr><td colspan="2">NOTA: Los análisis de causas y recomendaciones de la OCIG a las observaciones del presente informe son indicativas y no eximen del análisis de causa y formulación de planes de mejora que le corresponden al responsable en el marco del procedimiento de Mejoramiento Continuo de la EAAB-ESP.</td></tr>
</table>

Nombres / Equipo Auditor		Fecha Inicio Auditoría	Fecha Fin Auditoría
Auditor Líder OCIG	Piedad Roa Carrero	**19 mayo 2020**	**24 junio 2020**
Auditor Líder de Grupo	Luz Marina Gutiérrez H.		
Auditor	Carlos Alberto Guzmán S.		

Gloria Piedad Roa Carrero
Jefe Oficina de Control Interno y Gestión.
Con Copia: Dirección Gestión de Calidad y procesos