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

INFORME EJECUTIVO							
Nombre de la Auditoría Interna	**CONTROLES GENERALES DE TI - SIGUE**						**1050001-2020-0245** **N° Consecutivo**
Destinatario	**Dra. CRISTINA ARANGO OLAYA** **GERENTE GENERAL DE LA EAAB-ESP**						
PROCESO:	GESTION TIC			**SUBPROCESO**	MPFT03 Gestión de Servicios Informáticos MPFT04 Gestión de Sistema de Información Geográfica Unificado Empresarial		
Dependencia / Área / Unidad Auditable	DIRECCION INFORMACIÓN TECNICA Y GEOGRAFICA			**Responsable**	JHON JAIRO CASTRO AFANADOR		
	DIRECCION SERVICIOS DE INFORMATICA			**Responsable**	LINA MARIA CRUZ SILVA		
Reunión de Apertura	**8**	**07**	**2020**	**Reunión de Cierre**	**3**	**09**	**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							
Auditor							
Dificultades del Proceso Auditor	La oportunidad y disponibilidad de la información La calidad de la información suministrada para el análisis y pruebas 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.

Proveer aseguramiento sobre los controles clave implementados en SIGUE (Sistema de Información Geográfico Unificado Empresarial) referente a la funcionalidad y seguridad.

2. ALCANCE DE LA AUDITORÍA.

Esta auditoría evaluó los controles generales de TI del Sistema de Información SIGUE para el período comprendido entre enero y julio 2020, considerando los siguientes componentes:

- Seguridad del sistema de información SIGUE: verificar que los criterios de seguridad son aplicados de acuerdo a las políticas de seguridad de la información y las buenas prácticas de la industria y del negocio.
- Gestión de Riesgos: verificar el diseño y efectividad de los controles que determinan el riesgo residual
- Gestión de cambios: verificar que todos los cambios surtan el proceso definido por la EAAB-ESP, sean probados y aprobados para paso a producción
- Gestión de licenciamiento de software: Verificar que el software que soporta la operación cumple con las disposiciones legales y se gestiona y controla adecuadamente.
- Gestión de usuarios y accesos: verificar el mantenimiento de usuarios que aseguren el acceso solo a personal autorizado a la información de la EAAB-ESP
- Gestión roles y perfiles de acceso: verificar la definición de permisos y privilegios asignados a los usuarios para el desarrollo de sus funciones.
- Contingencia y Continuidad: Verificar los procedimientos y actividades definidas para el sistema SIGUE que aseguren la protección de la información y disponibilidad del sistema y del servicio.

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.

Como resultado del conocimiento y entendimiento del Sistema de Información Geográfico Unificado Empresarial – SIGUE, con el cual se gestiona la georreferenciación de la información geográfica y topográfica para la gestión integral del agua en la EAAB-ESP y apoyando a otras entidades del Distrito mediante el convenio IDECA, las entrevistas realizadas al personal clave que gestiona los diferentes componentes evaluados de la Dirección Información Técnica y Geográfica – DITG y las pruebas de realizadas a cada uno de los procesos auditados. A continuación, se presentan las conclusiones de la evaluación:

- *Gestión de Riesgos*

Resultado del análisis de los riesgos considerados en la auditoría se concluye que en la definición de los controles asociados para la mitigación de los riesgos se identificó que éstos son generales asociados a procedimientos o manuales, lo que no permite llegar a una evaluación del diseño y efectividad sobre actividades de control específicas y su posterior calificación del riesgo inherente. Al respecto se presenta recomendación para su revisión dado que la Gerencia de Tecnología tiene definido un plan de mejoramiento para la revisión de la matriz de riesgos Gestión TIC.

- *Gestión Licenciamiento de Software*

Resultado de la evaluación del proceso de gestión de licenciamiento de software se concluye que hay inconsistencia en la información entre las diferentes fuentes evaluadas. Por lo anterior y como resultado

de las pruebas realizadas al licenciamiento de software, se identificaron situaciones que son objeto de revisión por parte de la Dirección Información Técnica y Geográfica y que son detalladas en la sección de observaciones numeral 3.3.

- *Gestión de usuarios*

Resultado de la evaluación del proceso de gestión de usuarios se concluye que este proceso por su particularidad no aplica el procedimiento establecido en la EAAB-ESP, a través del cual se surte la solicitud mediante el diligenciamiento del formulario de solicitud disponible en la herramienta SIMI. Las solicitudes se realizan por correo electrónico. Así mismo, no se está surtiendo el proceso de notificación de novedades de usuarios para gestionar el mantenimiento de usuarios en los sistemas que conforman SIGUE. Por lo anterior y como resultado de las pruebas realizadas a los usuarios, se identificaron situaciones que son objeto de revisión por parte de la Dirección Información Técnica y Geográfica y que son detalladas en la sección de observaciones numeral 3.3.

- *Gestión Roles y Perfiles*

Resultado de la evaluación del proceso de gestión de roles y perfiles se concluye que los roles y privilegios en AGOL están definidos de acuerdo a las características, funcionalidades del sistema y necesidades del negocio. Se tiene claramente definido los roles que son asignados a los usuarios de acuerdo a las necesidades y responsabilidades. Sin embargo, como resultado de las pruebas realizadas a los usuarios, se identificó un grupo de usuarios sin rol asignado, situación que es detallada en la sección de observaciones numeral 3.3.

- *Gestión Desarrollo de Programas*

Resultado de la evaluación del proceso de gestión de desarrollo de programas se concluye que la mejoras o nuevas funcionalidades en el Sistema SIGUE, son apoyadas por el proveedor Esri con las horas de servicios profesionales adquiridas en el acuerdo ELA. Los desarrollos internos están orientados a las mejoras o nuevas funcionalidades del sistema de información SGO y con la interfaz con SAP. Como resultado de las pruebas realizadas se identificó las iniciativas desarrolladas tanto por el proveedor Esri como las iniciativas desarrolladas internamente durante el período de alcance de la auditoría, las cuales se encontraban en fase de pruebas.

- *Gestión de Cambios*

Resultado de la evaluación del proceso de gestión de cambios se concluye que los procedimientos realizados son los establecidos por la DSI, en este caso la DITG entrega al líder de cambios de la DSI toda la información soporte para surtir el proceso de cambios y esto es documentado en la herramienta BMC-Remedy y los controles definidos permiten asegurar que los cambios efectuados al sistema de información y la infraestructura tecnológica que soporta los procesos de SIGUE y SGO son probados, aprobados y autorizados para paso a producción, mitigando los riesgos de estabilidad o integridad en el ambiente de producción. Al respecto, no se pudo evaluar la gestión de cambios para las iniciativas desarrolladas en el período de auditoría por cuanto se encontraban en fase de pruebas.

- *Contingencia y Continuidad*

Resultado de la evaluación del proceso de contingencia y continuidad se concluye que actualmente el Sistema SIGUE cuenta con infraestructura en alta disponibilidad y redundancia ubicada en el centro de cómputo principal Centro Nariño y centro de cómputo alterno Modelia con un enlace de fibra oscura que

brinda una conectividad de LAN extendida entre las sedes, esquema de backups, herramienta de almacenamiento en alta redundancia y compresión.

- *Actas de Subcomité Coordinación de control Interno*

Resultado de la revisión en las actas de Subcomité Coordinación de Control Interno de la Gerencia de Tecnología, se encontró en el acta Nº 6 de subcomité de control interno del mes de junio la actividad de "La Adquisición, implementación y puesta en funcionamiento de ArcGis monitor for ArcGis server up to four cores junto con ArcGis monitor jump start" que está en ejecución.

3.2 Fortalezas.

- ✓ La Dirección Información Técnica y Geográfica - DITG es consciente de su rol y responsabilidad en la EAAB-ESP y el apoyo transversal que brinda a otras áreas con la información que suministra para el cumplimiento de los objetivos estratégicos.

- ✓ El conocimiento de la funcionalidad del sistema SIGUE por parte de los funcionarios de la DITG que tienen la responsabilidad de la administración, monitoreo y operación.

- ✓ La baja rotación del personal (contratista) hace que tengan conocimiento a profundidad de la funcionalidad y operatividad del sistema y atención oportuna ante eventos que pueden llegar a afectar la disponibilidad del servicio.

- ✓ La Gerencia de Tecnología tiene en operación el esquema de contingencia y continuidad de la infraestructura tecnológica que soporta el sistema SIGUE que permite asegurar la alta disponibilidad del servicio.

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	**Inconsistencias en la información de licenciamiento de software** Se evidenció diferencias en la información de licenciamiento de software con base en los inventarios de AGOL, MyEsri, inventario del servidor de licencias y software de los servidores. Lo anterior puede acarrear sanciones o multas por incumplimiento legal
Efecto / Impacto	Sanciones o multas por incumplimiento de regulaciones externas por ausencia de políticas y procedimientos relacionadas con derechos de autor y propiedad intelectual Fallas en la integridad de la información de licencias de software Debilita el Sistema de Control Interno, componente Información y Comunicación.

Responsable	Gerencia de Tecnología Dirección Servicios de Informática Dirección Información Técnica y Geográfica
Recomendaciones de la OCIG a la Observación.	Se recomienda a la Dirección Información Técnica y Geográfica, actualizar y sincronizar los inventarios de licencias de software con el propósito que la información sea íntegra y consistente con la situación actual a la EAAB-ESP. Así mismo, se recomienda que se realice entrega formal a la Dirección Servicios de Informática para que allí se continúe la gestión del licenciamiento del software relacionado con el Sistema de información SIGUE y demás software asociado. Esta es una actividad a ser considerada en los procedimientos establecidos.
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	**Organizar la entrega formal de los certificados de uso del software adquirido a la Dirección Servicios de Informática - DSI** En el ejercicio de auditoría se evidenció que no se cuenta con los certificados de uso del software que se gestiona en la DITG, lo anterior, por cuanto la información suministrada fueron los inventarios de software, contratos, orden de compra y oferta comercial, documentación que no permitió establecer el software adquirido, la cantidad, tipo de licencia y vigencia. No obstante, durante el conocimiento del informe preliminar la DITG consiguió los certificados de uso los cuales fueron revisados por Auditoría y los resultados presentados en la reunión de cierre de la auditoría, por tal razón se cambia la observación hacia la organización y entrega formal a la DSI.
Efecto / Impacto	Sanciones o multas por incumplimiento de regulaciones externas por ausencia de políticas y procedimientos relacionadas con derechos de autor y propiedad intelectual Desactualización del Inventario de licencias de software y certificados que lo soportan Debilita el Sistema de Control Interno, componente Información y Comunicación, Componente monitoreo y autoevaluación.
Responsable	Gerencia de Tecnología Dirección Servicios de Informática Dirección Información Técnica y Geográfica
Recomendaciones de la OCIG a la Observación.	Se recomienda a la Dirección Información Técnica y Geográfica organizar la documentación soporte del licenciamiento de software con el propósito de realizar entrega formal a la Dirección Servicios de Informática, para que ellos gestionen el licenciamiento de software.
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 mantenimiento (Licencias, vacaciones, contratos de personal Contratistas y retiros) de usuarios en el Sistema SIGUE (AGOL, ArcGis_Pro)** En el ejercicio de conocimiento se identificó que la Gerencia Corporativa de Gestión Humana y aprobadores de área, no están realizando las notificaciones de novedades de personal (Licencias, vacaciones, contratos de personal Contratistas y retiros) a la Dirección Información Técnica y Geográfica, que le permita efectuar mantenimiento de los usuarios. Evidenciando que las actividades (puntos de control 2.3. y 2.4 Procedimiento *Administración Cuentas Acceso y Autorizaciones*) se encuentran presentes, pero no son efectivos.
Efecto / Impacto	Pérdida de integridad por accesos o privilegios no autorizados Dificultad en el seguimiento de usuarios privilegiados Debilita el Sistema de Control Interno.
Responsable	Dirección Información Técnica y Geográfica
Recomendaciones de la OCIG a la Observación.	Se recomienda evaluar los lineamientos definidos en el "*Manual de Administración cuentas de acceso y autorizaciones"* y el procedimiento "*Administración Cuentas Acceso y Autorizaciones"* con relación a las actividades (punto de control 2.3 y 2.4) con el fin de garantizar la actividad de reporte de novedades de personal por parte de la Dirección de Mejoramiento Calidad de Vida de la Gerencia de Gestión Humana y los aprobadores de novedades de cada área, con el fin gestionar oportunamente el mantenimiento de los usuarios en los sistemas de información. Así mismo, se recomienda realizar mantenimiento a la base de usuarios del sistema de información (AGOL, ArcGis_Pro) con el fin de: • Inhabilitar los usuarios retirados con base en los reportes de novedades de personal directo y contratista. • Revisar los usuarios que tienen registrada una cuenta de correo de otro funcionario y establecer la viabilidad para asignarles una cuenta de correo propia. • Complementar la información de los usuarios incluyendo la información de su cuenta de correo • Revisar los usuarios que no tienen grupos asociados e identificar si estos usuarios requieren el acceso o se les debe asignar un grupo especial por la actividad que desempeñan. • Asignar responsables a los usuarios propios del sistema y documentarlo • Establecer la necesidad de mantener usuarios genéricos o inhabilitarlos. En caso de requerirse deben estar asignados a un responsable y documentarlos. Establecer con el apoyo de seguridad de la información los lineamientos para el manejo de usuarios genéricos y del sistema para los cuales se debe definir responsables y estar debidamente documentados y ser monitoreados (Log de Auditoría). • Revisar los usuarios presentados que tienen una cuenta diferente a la cuenta de usuario del Directorio Activo y establecer su necesidad y proceder a realizar la modificación de ser el caso o de lo contrario inhabilitarlo.

	• Revisar los usuarios y cuentas de correo inexistentes, identificar si son retirados y proceder a inhabilitarlos o realizar las modificaciones correspondientes. • Revisar la pertinencia de mantener usuarios activos del proveedor. De otra parte, para el mantenimiento de usuarios en los sistemas de información es importante establecer acuerdos de niveles de servicios – ANS entre las áreas para generar el compromiso de reportar la información con oportunidad.
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	Debilidad en la gestión de las novedades de cuentas de usuarios por la herramienta SIMI En el ejercicio de evaluación se evidenció que las novedades de cuentas de usuarios no se realizan a través de SIMI como está establecido en el procedimiento MPFT0202P Administración Cuentas Acceso y Autorizaciones y Acuerdo de uso de la información y los servicios informáticos, que dan las políticas generales y de operación desde el registro de identidad hasta la entrega de cuentas y contraseñas al usuario final o la eliminación de los permisos. Las novedades de creación de usuarios en SIGUE se reciben por correo electrónico sin que surta el proceso por SIMI.
Efecto / Impacto	Pérdida de integridad por accesos o privilegios no autorizados Debilita el Sistema de Control Interno.
Responsable	Dirección Información Técnica y Geográfica
Recomendaciones de la OCIG a la Observación.	Se recomienda analizar e implementar el proceso SIMI para la gestión de las novedades de cuentas de usuarios (creación, modificación, inhabilitación, eliminación) a los sistemas de información SIGUE. Lo anterior, permite mantener inventario total de todas cuentas de acceso y recibir los reportes de novedades de personal directo y contratista. De otra parte, permitirá obtener el reporte de novedades de personal (vacaciones, licencias, incapacidades, retiros, terminaciones de contrato y traslados de área) de la Dirección de Mejoramiento Calidad de Vida de la Gerencia de Gestión Humana de los empleados a término indefinido, fijo y a labor. Así como, el reporte de novedades de personal de contratistas y personas con contrato OPS por parte del aprobador de las novedades de cada área.
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.	

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