acueducto
AGUA Y ALCANTARILLADO DE BOGOTÁ

MEMORANDO INTERNO

GERENCIA GENERAL
EAB 2019 DEC19 11:05

1050001-2019-0415

Bogotá, D.C., 18 de diciembre de 2019

PARA: Dra. Lady Johana Ospina Corso- Gerente General

DE: Oficina de Control Interno y Gestión

ASUNTO: Informe Ejecutivo Auditoría Controles Generales de TI - SCADA

Respetada Dra. Lady

En cumplimiento del PAA-2019 aprobado por el Comité de Auditoría de la Junta Directiva de la EAAB-ESP, la Oficina de Control Interno y Gestión efectuó la evaluación de Controles Generales de TI al sistema de información SCADA a cargo de la Gerencia de Tecnología, bajo los lineamientos establecidos en el Marco de Referencia COBIT 5 y otros marcos de referencia específicos para el desarrollo de la auditoría.

Este informe fue dado a conocer a los Directivos responsables para que se tomen las medidas necesarias y se definan los planes de mejoramiento a que haya lugar de acuerdo con MPC50202P Mejora Continua.

Cordialmente,

Piedad Roa Carrero
Jefe de Oficina Control Interno y Gestión

Anexo: Informe Ejecutivo – Auditoría Gestión TI – Controles Generales de TI – SCADA (4 Folios)
Preparó: Equipo Auditor
Revisó/Aprobó: Piedad Roa Carrero.

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

PT-AC11

INFORME EJECUTIVO			
Nombre de la Auditoría Interna	**AUDITORIA CONTROLES GENERALES DE TI – SCADA**	1050001-2019-0415	**N° Consecutivo**
Destinatario	**Dra.** Lady Johana Ospina Corso **GERENTE GENERAL DE LA EAAB-ESP**		

PROCESO:	Gestión TIC	**SUBPROCESO**	Gestión de Seguridad de la Información Gestión de Servicios Informáticos Gestión del Sistema Integrado de Información Empresarial
Dependencia / Área / Unidad Auditable	Gerencia de Tecnología	**Responsable**	William Alberto Sastoque Jiménez
	Dirección Servicios de Informática	**Responsable**	Ricardo Abad Chacón Ibarra
	Líder de Seguridad de la Información	**Responsable**	Álvaro Pinzón Morales

Reunión de Apertura	**6**	**Sept**	**2019**	**Reunión de Cierre**	**17**	**Dic**	**2019**
	DIA	**MES**	**AÑO**		**DIA**	**MES**	**AÑO**

Equipo Auditor	
Auditor Líder OCIG	**Dra. Piedad Roa Carrero**
Auditor Líder de Grupo	**Ing. Luz Marina Gutiérrez Hernández**
Auditor	**Ing. Paola Mejía Cáceres**

Dificultades del Proceso Auditor	• Tiempo limitado para efectuar la auditoría • Calidad de la información fuente para el análisis (información incompleta, registros con errores) • Oportunidad en la entrega de la información solicitada para el ejercicio auditor

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 el monitoreo y control de SCADA - Red Matriz Centro – Modelia referente a la seguridad de la información y capacidad.

2. ALCANCE DE LA AUDITORÍA.

Evaluación de Controles Generales de TI SCADA está orientado a la gestión de los siguientes componentes:

- Seguridad del sistema de información SCADA: verificar que los criterios de seguridad sean aplicados de acuerdo a las políticas de seguridad de la información y las buenas prácticas de la industria y del negocio.

- Gestión de cambios: verificar que todos los cambios surtan el proceso definido por la EAAB, sean probados y aprobados para paso a producción
- Gestión de usuarios y accesos: verificar el mantenimiento de usuarios que aseguren el acceso solo a personal autorizado a la información de la EAAB
- Gestión roles y perfiles de acceso: verificar la definición de permisos y privilegios asignados a los usuarios para el desarrollo de sus funciones de acuerdo a la premisa del menor privilegio de acuerdo a la necesidad de saber y tener y que esta actividad sea monitoreada garantizando la segregación de funciones.
- Plan de Contingencia y Continuidad: Verificar los procedimientos y actividades definidas para SCADA que aseguren la protección de la información frente a eventos de indisponibilidad ocasionados por fallos en el servicio, infraestructura tecnológica, corrupción de datos, virus, entre otros.

Así mismo, se revisarán 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

El procedimiento de monitoreo y control SCADA de Red Matriz en Centro Modelia, soporta al cumplimiento de la estrategia "Prestación del Servicio", lo que genera que una indisponibilidad tenga un impacto importante sobre el negocio.

Como resultado del entendimiento del proceso de monitoreo y control que la EAAB - ESP tiene para los servicios de agua y alcantarillado por medio de SCADA y entrevistas realizadas a personal clave de la Gerencia de TI, se concluye que, a pesar de que la Gerencia de TI cuenta con procedimientos transversales las direcciones a su cargo desconocen la aplicabilidad de éstos generando posibles brechas de seguridad en cuanto al control de accesos y permisos, control de cambios y/o gestión de aplicaciones, así mismo los lineamientos o políticas que se deben cumplir para garantizar la disponibilidad, integridad y confidencialidad de la información.

3.2 Fortalezas.

- ✓ El conocimiento de la parametrización, monitoreo y control que tienen el administrador y los operadores.

- ✓ La baja rotación del personal hace que los operarios tengan mayor conocimiento y reacción ante los eventos que pueden llegar a afectar la correcta operatividad del monitoreo.

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

Control y seguimiento gestión de usuarios en el Directorio Activo de SCADA y en la aplicación de SCADA

DIRECTORIO ACTIVO

Como resultado de las pruebas realizadas a los usuarios del Directorio Activo de SCADA respecto al mantenimiento de las cuentas de usuarios no usadas por más de 30 días, se evidenció lo siguiente:

El 64% de los usuarios no han ingresado a la red entre el 2009 - 2018, el 25% se creó el usuario, pero nunca se autenticó en el DA y 10% presentó un inicio de sesión en el 2019; no obstante, los usuarios que interactúan en el DA en el 2019 son usuarios administradores o genéricos donde no se evidencia el responsable de su uso.

Periodo del último logueo	Cantidad de Usuarios
Entre 2009 - 2018	44
Nunca Ingresaron	17
Ingresaron en 2019	7
Total	*68*

De otra parte, de los 68 usuarios activos en el DA, se toma una muestra aleatoria de 35 usuarios, con el fin de validar la aplicabilidad de los lineamientos establecidos para la administración de usuarios en cuanto al tratamiento de los usuarios del personal retirado y cambio de contraseñas con periodicidad, como resultado se identificó que el 29% (10) se encuentran activos pese a que ya están retirados de la EAAB -ESP y el 40% (14) tiene activa la opción de que la contraseña nunca expira.

SCADA

De los 26 usuarios activos se identificó el incumplimiento a los siguientes lineamientos:

Política administración de usuarios	Cantidad Identificada	Observación de Auditoría
El nombre de la cuenta de usuario es único en todos los sistemas y recursos a los que se le autorice acceder	3	Se validó con el DA de la EAAB
Toda cuenta de acceso es de uso estrictamente personal e intransferible, quedando terminantemente prohibido (i) el acceso a las mismas por parte de cualquier persona distinto al titular y (ii) su transmisión y/o cesión.	10	Se identificó 9 usuarios genéricos sin un titular o responsable de su uso registrado.
Para la creación, modificación, cambio de contraseña y eliminación de cuentas se aceptarán únicamente las solicitudes aprobadas por medio del formulario SIMI	5	No se evidenció la solicitud por SIMI de la creación de 5 usuarios genéricos,

Lo anterior incumple con la Política de Seguridad de Información registrada en el procedimiento para la administración de cuentas de acceso y autorizaciones.

Efecto / Impacto

Perdida de trazabilidad de la gestión realizada al utilizar usuarios genéricos sin un responsable asignado para su uso.
Fuga de información por no realizar depuración periódica de los usuarios.

Responsable	Dirección de Servicios de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda realizar mantenimiento a la base de usuarios del sistema de información y del Directorio Activo de SCADA con el fin de: • Renombrar usuarios que no cumplen con la nomenclatura establecida por la EAAB -ESP. · • Asignar responsables a los usuarios propios del sistema • Establecer la necesidad de mantener usuarios genéricos o bloquearlos. En caso de requerirse deben están asignados a un responsable y estar documentados. • Establecer, con el apoyo de Seguridad de la Información los lineamientos para el manejo de usuarios genéricos y usuarios del sistema para los cuales se defina responsables y estar debidamente documentados e incluirlos en el monitoreo (log de auditoría). • Revisar los usuarios que presentan diferencias en el campo nombre con Directorio Activo y unificarlos.

NOTA: Los análisis de causas y recomendaciones 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

Identificación, Medición, Control de Riesgos de Gestión

Validado la metodología de Gestión de Riesgos adoptado por la EAAB – ESP y verificado su cumplimiento en la matriz de riesgos de Gestión TIC se observan las siguientes situaciones:

1. **Activo de información**: En la matriz de riesgos no se hace referencia al activo sobre el cual se hace la identificación de riesgos.
2. **Redacción de riegos:** En la matriz de riesgos se describen los riesgos a una plataforma o conjunto de activos de información lo que puede generar que el control no sea efectivo para cada activo que conforma la plataforma. Ej: Plataforma tecnológica, son varios los activos de información que la conforman como hardware, software, redes, comunicación, entre otros.
3. **Identificación de riesgos de los subprocesos asociados al Macro Procesos Gestión TIC:** En la matriz de riesgos no se observan riesgos asociados a los subprocesos que conforman la Gestión TIC, lo que puede generar que los objetivos del proceso como los estratégicos no se cumplan o se desvíen.
4. **Controles:** Se identifican controles que no son de conocimiento de los involucrados de su ejecución, al dejar un control como un procedimiento, política o manual, la descripción del control debe cumplir con los criterios para su documentación y dejar explicito el rol responsable de su ejecución. Por ejemplo, el siguiente control:

Proceso	Código Ctrl. ID	Nombre Control	Descripción	Afectación del Control	Tipología	Responsable Ejecución (Si cargo, "No")
Gestión de TIC	CTFT14	Aplicación de procedimiento de administración de cuentas de acceso y autorizaciones	Objetivo: Controlar el acceso a los sistemas o aplicativos informáticos Descripción: Se establecen los criterios para que de manera centralizada se gestionen los acceso, privilegios, entrega de cuentas y contraseñas al usuario final, así mismo se establecen los criterios o los lineamientos y tareas que deben cumplir los administradores de las plataformas tecnológicas, a partir de lo definido en el procedimiento MPFT020GP Administración de cuentas de acceso y/o autorizaciones, manual para la administración de cuentas de acceso y autorizaciones	Causa	Detectivo	Líder de Seguridad de la información

	El Líder de Seguridad de la Información, es el responsable de definir las políticas de seguridad de información aplicables según las normas establecidas para cada proceso o subproceso, los responsables de la ejecución de los procedimientos, políticas o manuales son aquellos roles responsables de realizar las actividades, en este caso el responsable de ejecutar los controles de acceso serían los administradores de los sistemas de información o el responsable de creación, modificación o eliminación de cuentas de usuario. **Riesgo identificado por Auditoría** Debilidad en la identificación, medición, monitoreo y seguimiento de los riesgos asociados a los procesos de TI. **Objetivo afectado** Validar la gestión y ejecución de medidas apropiadas para mitigar los riesgos que pueden llegar a afectar los objetivos de negocio
Efecto / Impacto	Identificación, Medición, Control y Seguimiento errada de riesgos
Responsable	Gerencia TI Dirección de Servicios de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda considerar en la metodología de riesgos y oportunidades de la EAAB -ESP, incluir como punto de partida los activos involucrados en cada uno de los procesos para la identificación del riesgo o los riesgos, como se indica en la Guía Administración de riesgos de gestión, Corrupción, Seguridad Digital y Diseño de Controles. La identificación de los activos involucrados en el proceso es el punto de partida para identificar los riesgos a los cuales está expuesto el proceso dando mayor cobertura a todos los posibles escenarios de riesgo, las causas generadoras de riesgo, valoración de la probabilidad e impacto y la identificación de los controles preventivos, detectivos y correctivos y la calificación del diseño y la solidez del mismo para la mitigación del riesgo.

NOTA: Los análisis de causas y recomendaciones 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	**Definición de planes de contingencia y continuidad.** Validando la documentación del sistema de monitoreo y control SCADA de Red Matriz, no se evidenció los planes de continuidad del proceso, ni planes de contingencia, lo que permite que al momento de presentarse algún evento que genere indisponibilidad en el proceso éste no pueda dar continuidad de las actividades de monitoreo y control.
Efecto / Impacto	Pérdida de reacción ante un evento de desastre por desconocimiento de las actividades a ejecutar y capacidad de los responsables involucrados Afectación de la misionalidad de la EAAB-ESP
Responsable	Gerencia TI Dirección de Servicios de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda considerar el proceso de monitoreo y control SCADA Red Matriz dentro de los procesos críticos de negocio para que sea incluido en el DRP que la Gerencia de TI vaya a implementar.

NOTA: Los análisis de causas y recomendaciones 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	Documentación del procedimiento de Monitoreo y Control de SCADA e incluirlo dentro del SIG. En la visita realizada al Centro de Control y Monitoreo Modelia, se evidenció que los operarios ejecutan actividades clave para adelantar sus actividades y mantener el control del proceso, se valida con el administrador del sistema, quien manifiesta que este proceso no se encuentra documentado.
Efecto / Impacto	Debilita el Sistema de control Interno
Responsable	Gerencia TI Dirección de Servicios de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda establecer el procedimiento y manual respecto a las actividades que se ejecutan en el proceso de monitoreo y control, y vincularlo en el SIG.

NOTA: Los análisis de causas y recomendaciones 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.

4. OPORTUNIDADES DE MEJORA

Las "Oportunidades de mejora" si bien no requieren plan de mejoramiento, si deberán ser analizadas y en caso de ser procedentes, deberán ser atendidas por los responsables en el marco de la gestión propia del área o dirección a cargo, ya que serán objeto de monitoreo en próximas auditorías, y su desatención en más de dos oportunidades será comunicada al superior inmediato o escalado a la alta dirección según consideración de la Jefatura OCIG.

	OPORTUNIDADES DE MEJORA	RESPONSABLE
1	Tener en cuenta la resolución 740 de 2018 Política General de Seguridad y Privacidad de la Información en su artículo 8 gestión tecnológica. Dentro de los proyectos establecidos en el Plan Maestro de Tecnología se incluye el proyecto PRY_03 *Fortalecer el Control en Línea del Sistema Maestro*, el cual busca actualizar y fortalecer el sistema e infraestructura que soporta SCADA e integrar SCADA SIGUE, por lo anterior, se recomienda que para el desarrollo de este proyecto se consideren los lineamientos de seguridad de la información establecidos en la Política.	**Dirección de Servicios de Informática**
2	Unificar criterios para la gestión de cuentas de usuario definidos en el procedimiento y el manual En el proceso de revisión documental se evidenció que el procedimiento *MPFT0202P Administración Cuentas Acceso y Autorizaciones V5- Público VF* y el *Manual MPFT0202M03-01 Adm cuentas acceso autorización Nvo* tiene conceptos contradictorios que pueden generar inconsistencias al momento de aplicar los controles. **PROCEDIMIENTO**: Respecto a cancelación de cuentas — Las cuentas de usuarios no usadas **por más de 30 días, pasarán a estado de** **MANUAL**: Respecto a los usuarios — Las cuentas de usuarios no usadas **por más de 60 días deben pasar a**	**Dirección de Servicios de Informática** **Dirección Gestión de Calidad y Procesos.**

	cuarentena y serán bloqueadas y notificadas al Supervisor y al Jefe inmediato quién se deberá pronunciar mediante formulario SIMI respecto a la necesidad para que no sean eliminadas.	**estado de cuarentena y serán bloqueadas**. El rol de Administrador de Usuarios debe reportar vía correo corporativo al supervisor, Jefe inmediato y a la mesa de servicio, la acción a tomar con dichas cuentas. Las cuentas en cuarentena que no sean confirmadas por el supervisor o jefe inmediato serán eliminadas.	

Piedad Roa Carrero
Jefe Oficina de Control Interno y Gestión.