acueducto
AGUA Y ALCANTARILLADO DE BOGOTÁ

MEMORANDO INTERNO

1050001-2019-0417

Bogotá, D.C., 18 de diciembre de 2019

GERENCIA GENERAL
EAB 2019 DEC19 11:05

PARA: Dra. Lady Johana Ospina Corso- Gerente General

DE: Oficina de Control Interno y Gestión

ASUNTO: Informe Ejecutivo Auditoría Seguridad Firewall, IPS, Antivirus, Hardening plataforma crítica y Gestión de Vulnerabilidades

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 Seguridad enfocada en Firewall, IPS, Antivirus, Hardening a plataforma crítica y gestión de vulnerabilidades a cargo de la Gerencia de Tecnología, bajo los lineamientos establecidos en el Marco de Referencia COBIT 5, ISO 27001 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 – Seguridad (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 SEGURIDAD FIREWALL, IPS, ANTIVIRUS, HARDENING Y VULNERABILIDADES**				1050001-2019-0417		
					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		
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 • Oportunidad en la entrega de la información solicitada para el ejercicio auditor • Disponibilidad de la información para la realización de las pruebas de auditoría						
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 los dispositivos y medidas de seguridad para la protección de los activos de información.

2. ALCANCE DE LA AUDITORÍA.

Evaluación de Seguridad está orientado a la gestión de los siguientes dispositivos de seguridad:

- Firewall
- IDS/IPS
- Antivirus
- Vulnerabilidades
- Hardening plataforma crítica

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.

Resultado de la evaluación a la gestión de los dispositivos y procesos de seguridad Firewall, IPS, Antivirus, Gestión de Vulnerabilidades y Hardening, se identifican observaciones en temas específicos de gestión de riesgos, definición y documentación de metodologías y procedimientos, mantenimiento de reglas de firewall, ejecución de actividades de gestión de vulnerabilidades e innovación tecnológica.
Se considera importante resaltar que en el Plan Maestro de Tecnología en el proyecto 30. "*Fortalecimiento de las capacidades de gestión de tecnología*", se encuentra la actividad "*Fortalecimiento del Modelo de Seguridad de la Información*" que se encuentra en desarrollo según cronograma, tema de interés para una próxima auditoría.

A continuación, se presentan las conclusiones de cada uno:

- ***Firewall:***

En la evaluación de la gestión y administración de Firewall se identifica que la EAAB cuenta con 5 Firewalls gestionados por la Gerencia de TI, esta gestión es apoyada con personal experto de SONDA. En el conocimiento no se identificaron políticas y procedimientos relacionados con la administración y gestión de estos dispositivos de seguridad. Se identifica que el proveedor SONDA cuenta con un manual de operación para el cumplimiento contractual el cual no fue suministrado a la auditoría. En el conocimiento de las características técnicas, se identifica 2 firewall cuya vida útil ya fue cumplida y para los cuales ya no se tiene soporte del fabricante lo que conlleva a que no puedan ser actualizados quedando limitada su funcionalidad, capacidad y el soporte para la solución de problemas.

- ***IPS***

En la evaluación de la gestión del IPS se identifica que es una herramienta de monitoreo de marca McAfee gestionada por la Gerencia de TI con el apoyo de personal experto de SONDA a través de un contrato de servicios de TI. En el conocimiento no se identificaron políticas y procedimientos relacionados con la administración y gestión de esta herramienta de seguridad, el proveedor SONDA cuenta con un manual de operación para el cumplimiento contractual el cual no fue suministrado a la auditoría. En el conocimiento de las características técnicas, se identifica que esta herramienta ya cumplió su vida útil y en este momento ya no se tiene soporte del fabricante lo que conlleva a que no pueda ser actualizada quedando limitada su funcionalidad en la identificación de nuevas modalidades de ataques y el soporte para la solución de problemas.

- ***Antivirus***

En la evaluación de la gestión del Antivirus se identifica que esta es una Suite Antivirus McAfee ePolicy Orchestrator (EPO) gestionada por la Gerencia de TI con el apoyo de personal experto de SONDA a través de un contrato de servicios de TI que incluye soporte, mantenimiento, actualización, instalación, capacitación y migración hasta el 15 de diciembre de 2019. En el

conocimiento no se identificaron políticas y procedimientos relacionados con la administración y gestión de esta herramienta de seguridad, el proveedor SONDA cuenta con un manual de operación para el cumplimiento contractual el cual no fue suministrado a la auditoría.

- ***Gestión de Vulnerabilidades***

En la evaluación de la gestión de vulnerabilidades se identifica que se utiliza la herramienta Nexpose de Rapid7 gestionada por la Gerencia de TI con el apoyo de personal experto de SONDA a través del contrato de servicios de TI que incluye mantenimiento, soporte, actualización, instalación, capacitación y migración.

Para la evaluación de este proceso, se solicitó la siguiente información:

- El inventario detallado de los recursos tecnológicos que son monitoreados con la herramienta
- Los reportes de escaneos generados por la herramienta Nexpose
- Soporte del análisis realizado a las vulnerabilidades identificadas con base en los reportes generados

Es importante manifestar que la información no fue suministrada al auditor, argumentando que la información era de carácter confidencial; En reunión se mostraba apartes de la información sin que eso implique que el auditor pueda tener realmente un concepto o criterio sobre la gestión realizada; por lo que se desconoce el estado actual de la gestión de vulnerabilidades o si se está realizando gestión de forma adecuada sobre las vulnerabilidades identificadas. Igualmente se desconoce si los resultados de la gestión han sido comunicados a la Alta Gerencia.

- ***Hardening Plataforma Crítica***

En la evaluación de la gestión de Hardening plataforma crítica se identifica que esta es una actividad realizada por el grupo de seguridad y el apoyo de personal experto de SONDA a través del contrato de servicios de TI, donde se diseñaron y aplicaron plantillas de seguridad para el aseguramiento del Sistema Operativo y Bases de Datos de la plataforma crítica definida por la EAAB a nivel contractual y sobre otros recursos tecnológicos. Del resultado de la gestión realizada para asegurar la plataforma se generaron los informes con los resultados de la actividad, está pendiente es el análisis de las excepciones que se presentaron en la ejecución de las líneas base de seguridad para las cuales se deberan establecer controles compensatorios y dejarlos debidamente documentados.

3.2 Fortalezas.

✓ La Gerencia de TI es consciente de su rol y responsabilidades en la EAAB y el apoyo transversal que brinda al soportar los procesos manteniendo la disponibilidad de la infraestructura tecnológica.

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

Identificación, Medición, Control de Riesgos de Gestión de Seguridad

Para la realización de la auditoría, inicialmente se realiza análisis de la matriz de riesgos suministrada por la Gerencia de TI, con el fin de identificar riesgos asociados al proceso auditor. Una situación identificada es el número limitado de riesgos identificados relacionados con seguridad informática y la cantidad y diversidad de dispositivos o herramientas gestionadas.

Se seleccionan los riesgos relacionados con el objeto de auditoría y como resultado de este análisis se identifican las siguientes situaciones:

a. Activo de información: En la matriz de riesgos no se hace referencia al activo sobre el cual se hace la identificación de riesgos.
b. Controles: no se identifican las actividades de control específicas para mitigar el riesgo. Se registran procedimientos que pueden tener varias actividades. Es importante indicar la actividad específica de manera que facilite su seguimiento, verificación, asignación, responsable, periodicidad, etc.
c. Riesgo residual: la calificación del riesgo residual está dada por la evaluación de los controles por su diseño, ejecución, solidez individual, solidez del conjunto de controles. La ponderación de todos estos elementos debe llevar a disminuir la probabilidad o el impacto. No obstante, la valoración está siendo dada aun cuando el control no es adecuado ni está claramente definido. De otra parte, el desplazamiento del riesgo residual en el Mapa de riesgos es gradual de acuerdo a la efectividad de los controles y el comportamiento histórico (madurez) que este demuestre. Es decir, aun cuando un control sea fuerte no puede desplazar un riesgo de importante a bajo de primera vez.

Riesgos del Proceso	Riesgo inherente	Controles	Riesgo Residual	Observaciones Auditoría
Indisponibilidad de la plataforma tecnológica	Importante	CTFT14: Aplicación de procedimiento de administración de cuentas de acceso y autorizaciones CTFT10: Segregar privilegios de acceso a la plataforma tecnológica y aplicaciones	Bajo	Los controles definidos no mitigan el riesgo de indisponibilidad
Insuficiencia de la plataforma tecnológica	Importante	CTFT05: Actualizaciones en la plataforma tecnológica (hardware y software) CTFT09: Plan Estratégico de Tecnologías de la Información – PETI	Moderado	Las actividades planteadas como controles no están relacionados al riesgo de insuficiencia
Pérdida de la integridad de la información	Importante	CTFT10: Segregar privilegios de acceso a la plataforma tecnológica y aplicaciones CTFT14: Aplicación de procedimiento de	Moderado	Las actividades planteadas mitigan el riesgo de

			administración de cuentas de acceso y autorizaciones		integridad. No obstante, se debe ser especifico a las actividades a realizar puntualmente.
			CTFT15: Monitoreo de las cuentas de acceso		
	Divulgación no autorizada de información confidencial de la EAAB	Inaceptable	CTFT10: Segregar privilegios de acceso a la plataforma tecnológica y aplicaciones	Moderado	Las actividades planteadas mitigan el riesgo de integridad. No obstante, se debe ser especifico a las actividades a realizar puntualmente.
			CTFT11: Clasificación y protección de la información		
			CTFT14: Aplicación de procedimiento de administración de cuentas de acceso y autorizaciones		
			CTFT15: Monitoreo de las cuentas de acceso		

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 de TI Dirección Servicios de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda realizar inicialmente la identificación de los activos de información involucrados en el proceso de seguridad de manera que se identifiquen los riesgos asociados y se desarrolle la medición y control según la metodología de riesgos y oportunidades establecida en la EAAB

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	**Definir políticas y procedimientos para la gestión de Firewall, IPS, Antivirus y Hardening** En el conocimiento de la gestión de los dispositivos de seguridad Firewall, IPS, Antivirus y Hardening se identificó que la EAAB no cuenta con políticas y procedimientos que den los lineamientos de gestión y control, describan las actividades desarrolladas por la Dirección Servicios de Informática para la gestión y administración de estas herramientas y los procesos de seguridad.

	La gestión y administración de la seguridad informática hace parte de los servicios contratados con la empresa SONDA y su personal experto es el encargado de llevar a cabo las actividades que están definidas contractualmente.
Efecto / Impacto	Actividades y controles definidos sin ser un proceso sistemático
Responsable	Gerencia de TI Dirección Servicios de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda definir las políticas y procedimientos para la administración y gestión de cada una de las herramientas y procesos de seguridad utilizados para la protección de los activos de información y la zona perimetral de la EAAB. Las políticas dan las directrices de gestión y los procedimientos y documentos relacionados (instructivos, formatos) establecen el paso a paso de las actividades que deben ser realizadas para el cumplimiento de la política, los responsables de su ejecución, soportes documentales y así mismo, aseguran la implementación y ejecución consistentes con las necesidades del negocio. Todos los documentos que soportan la gestión de la entidad deben estar o hacer parte del sistema de gestión documental de la EAAB-ESP

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	**Evaluar la obsolescencia tecnológica de la infraestructura que soporta los procesos de seguridad de la EAAB** En el conocimiento de las características técnicas, soporte, mantenimiento y actualización, vida útil de los dispositivos que apoyan la gestión de seguridad como el Firewall e IPS se identifica que: De los 5 firewall: 2 firewall ya cumplieron su vida útil y para los cuales ya no se tiene soporte del fabricante lo que conlleva a que no puedan ser actualizados quedando limitada su funcionalidad, capacidad y el soporte para la solución de problemas. Otros 2 no presentan actualización del Firmware desde el 2016 y el último firewall tiene soporte hasta el 20 de abril de 2020 contratado con SONDA. De igual manera sucede con el IPS que ya cumplió su vida útil y en este momento ya no se tiene soporte del fabricante, lo que conlleva a que no pueda ser actualizada quedando limitada su funcionalidad en la identificación de nuevas modalidades de ataques y el soporte para la solución de problemas.
Efecto / Impacto	Exposición a nuevas formas de ataques informáticos y cibernéticos
Responsable	Gerencia de TI Dirección Servicios de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda estudiar la viabilidad de adquisición de herramientas de seguridad que brinden una adecuada seguridad informática y de la información conociendo que todos los días la entidad se encuentra expuesta a nuevos ataques informáticos y cibernéticos.

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	**Definir actividades de revisión y mantenimiento de las reglas de firewall** En el conocimiento se identificó que no se tiene definido un procedimiento que dé los lineamientos para la gestión eficiente del Firewall y como consecuencia de ello no se tiene establecida una periodicidad para la revisión y mantenimiento de las reglas de firewall. De acuerdo a la documentación suministrada se identifica que la última revisión de reglas de firewall se realizó en octubre de 2017.
Efecto / Impacto	Si las reglas del firewall no se revisan de forma periódica y se actualizan conforme a los cambios del entorno, entonces el nivel de protección perimetral puede verse afectado
Responsable	Gerencia de TI Dirección Servicios de Informática
Recomendaciones de la OCIG a la Observación.	Se recomienda definir periodicidad para la revisión y mantenimiento de las reglas de firewall con el propósito de eliminar reglas innecesarias, desactualizadas o incorrectas al menos cada 6 meses o con mayor frecuencia si se implementan numerosos cambios en las reglas de firewall y asegurar que los conjuntos de reglas otorguen permiso solo a los servicios y puertos autorizados de acuerdo a las necesidades del negocio, estos deben quedar debidamente justificado y documentado. Estas actividades mejoran el rendimiento del Firewall y el nivel de seguridad. Estas actividades deben ser incluidas dentro de la política y procedimiento de la gestión de Firewall.

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	**Definir los criterios de priorización de vulnerabilidades considerando el valor del activo** En la auditoría fue suministrado el procedimiento "MPFT0201P 03 Atención de Vulnerabilidades Informáticas V2 SVSAP", el cual se encuentra en borrador.	Dirección Servicios de Informática, Seguridad de la Información

	En la política 9 indica: "*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.*" Para garantizar una adecuada priorización de las vulnerabilidades, el procedimiento debe definir claramente cuáles deben ser los criterios de priorización de vulnerabilidades y donde uno de estos criterios sea el valor del activo que se ve afectado con el fin de dar orientación al administrador. Lo anterior, por cuanto no solo se debe considerar la severidad del riesgo indicado por la herramienta de vulnerabilidades sino la evaluación que se realice sobre el valor y criticidad del activo y el entorno del mismo.	

Dificultades del proceso Auditor	El tiempo de ejecución de la Auditoría Disponibilidad de la información para el ejercicio de la auditoría • Respuesta al requerimiento de información de Firewall, IPS, Antivirus • Inventario de equipos escaneados en la gestión de vulnerabilidades • Informes de la gestión de vulnerabilidades • Los reportes de escaneos generados por la herramienta Nexpose • Soporte del análisis realizado a las vulnerabilidades identificadas con base en los reportes generados

Nombres / Equipo Auditor		**Fecha Inicio Auditoría**	**Fecha Fin Auditoría**
Auditor Líder OCIG	Piedad Roa Carrero	**30 de septiembre de 2019**	**5 de diciembre de 2019**
Auditor Líder de Grupo	Luz Marina Gutiérrez H.		
Auditor	Paola Mejía Cáceres		

Piedad Roa Carrero
Jefe Oficina de Control Interno y Gestión