MEMORANDO 20221400079263

Bogotá, 13 de diciembre de 2022

PARA: **José Daniel Rojas Medellín**
Presidente de SAE

DE: **María del Pilar Mayor Varela**
Jefe oficina de Control Interno

ASUNTO: **Informe Ejecutivo de auditoría interna de gestión – Proceso de Infraestructura Tecnológica Componente Seguridad de la Información y Ciberseguridad.**

Respetado José Daniel;

Conforme al Plan Anual de Auditoría vigencia 2022 aprobado por Comité Institucional de Coordinación de Control, la Oficina de Control Interno realizó auditoría interna de gestión de sociedades.

Adjunto se remite informe ejecutivo que contiene los resultados de la auditoría, los cuales fueron comunicados previamente en reunión de cierre el 01 de diciembre de 2022 y en el informe final a los lideres de los procesos evaluados el día 02/12/2022 mediante memorando No. 20221400073683

En cumplimiento de lo establecido en el procedimiento P-EC2-109- Para la elaboración y seguimiento de planes de mejoramiento, para las oportunidades de mejora, las áreas auditadas deben realizar un plan de mejoramiento en el formato F-EC1-177 y remitirlo a la Oficina de Control Interno dentro de los diez (10) hábiles siguientes a la recepción del presente documento, es decir, el 19 de diciembre de 2022.

Cordialmente,

María del Pilar Mayor Varela
Jefe Oficina de Control Interno

INFORME EJECUTIVO DE AUDITORIA INTERNA

PROCESO DE INFRAESTRUCTURA TECNOLÓGICA COMPONENTE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

AUDITOR LIDER

CAROLINA AGUILERA MARTÍNEZ

FECHA DE AUDITORIA

Desde el 30 de septiembre al 01 de diciembre de 2023

INTRODUCCIÓN

La Oficina de Control Interno en desarrollo de su función constitucional con lo descrito en el Plan Anual de Auditoria de la vigencia 2022, desarrolló auditoría interna al Proceso de Infraestructura Tecnológica Componente Seguridad de la Información y Ciberseguridad, orientada a evaluar la ejecución de las actividades y aplicación de controles de acuerdo con los procesos establecidos en la Oficina de Gestión de la información establecido en la arquitectura de la entidad, así como el cumplimiento de la normatividad legal vigente.

Este ejercicio se realizó con base en las Normas Internacionales en materia de Auditoría Interna del Instituto Internacional de Auditores, Guía de auditoría para entidades públicas de la Función Pública las cuales incluyen planeación de la auditoría, ejecución del trabajo y generación del informe.

El proceso auditor incluyó la solicitud, análisis y verificación de información, documentación, evaluación de controles y riesgos asociados a los procedimientos evaluados. Con los resultados obtenidos del ejercicio se pretende contribuir al mejoramiento continuo de SAE.

INFORME AUDITORÍA INTERNA DE GESTIÓN
PROCESO DE INFRAESTRUCTURA TECNOLÓGICA COMPONENTE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

1. OBJETIVO (Norma desempeño 2210).

Evaluar la eficiencia, eficacia y efectividad de los controles existentes, el manejo de los riesgos de gestión a la pertinencia y oportunidad de los Procesos de Infraestructura Tecnológica Componente Seguridad de la Información y Ciberseguridad establecidos en la Oficina de Gestión de la Información, como también el cumplimiento de la política y normatividad legal vigente aplicable, generando una cultura organizacional fundamentada en la información, el control y la evaluación.

1.1 Objetivos Específicos (Norma desempeño 2210)

- Evaluar y revisar el seguimiento a la gestión al proceso de Infraestructura Tecnológica Componente Seguridad de la Información y Ciberseguridad de la Oficina de Gestión de la Información de Activos Especiales SAE SAS.
- Evaluar los indicadores de medición de las actividades asociadas al procedimiento.
- Evaluar los riesgos y controles asociados al Proceso de Infraestructura Tecnológica Componente Seguridad de la Información y Ciberseguridad (Mapas de riesgos de la SAE - Riesgos operativos, de corrupción y de Seguridad de la Información)
- Evaluación de Talento Humano de las áreas auditadas
- Evaluar la conversación de la información y la gestión documental de las tablas de Retención Documental (TRD, transferencias documentales, organización documental), asociada al procedimiento.

2. ALCANCE (Norma desempeño 2220)

Evaluar la aplicabilidad de los procesos y procedimientos establecidos en los manuales y las circulares internas, políticas y normatividad legal vigente, en el periodo comprendido entre el 01 de enero de 2021 al 30 de junio de 2022, para la verificación de los controles existentes y el manejo de los riesgos en la Infraestructura Tecnológica Componente Seguridad de la Información y Ciberseguridad.

Esta auditoría se ejecutó dando cumplimiento a las normas y técnicas de auditoría generalmente aceptadas, con fundamento en normas internacionales de auditoría basadas en riesgos, la guía de auditoría interna basada en riesgos para entidades públicas versión 4, Estatuto de Auditoría Interna de la SAE V.2, Código de ética de los auditories internos de la SAE V2, séptima dimensión y tercera línea de defensa del Modelo Integrado de Planeación y Gestión – MIPG.

3. METODOLOGÍA (Norma desempeño 2310)

- Solicitud de información (en todas las etapas de la auditoria).
- Selección de muestra.
- Verificación documental de la información remitida por las áreas (expedientes digitales).
- Prueba de recorrido mediante entrevista a través de Teams con el área auditada.
- Prueba de recorrido mediante visita en sitio y verificación de Inventario de Hardware en Datacenter Triara Autopista Medellín Km 7.5 Celta TRADE Park bodega 32, Cota, Funza Cundinamarca.

- Prueba de recorrido mediante visita en sitio y verificación de Inventario aleatorio de Hardware en Sótano 1, Piso 1, Piso 2, Piso 3, Piso 4, Piso 5 Calle 93 B # 13 – 47.
- Prueba de recorrido mediante visita en sitio y verificación de Inventario aleatorio de Hardware en OGI (Oficina de Gestión de la Información) Calle 93b # 12-48
- Elaboración de informe.
- Presentación de resultados.

El proceso auditor incluyó visitas en sitio y reuniones sincrónicas a través de TEAMS con los auditados y entre el equipo auditor.

4. CRITERIOS DE AUDITORIA (Norma desempeño 2040).

- Resolución Mintic 1519 de 2020
- M-TE4-038 Manual Política de seguridad y Privacidad de la Información Versión 3 – 22/07/2021
- Plan de Ethical Hacking
- Normas Internaciones de Auditoría
- Mapas de riesgos de la SAE - Riesgos operativos, de corrupción y de Seguridad de la Información publicados a junio de 2022.
- Política de riesgos de SAE- Metodología de identificación de riesgos, Procedimiento Gestión de riesgos.
- ISO/IEC 27001:2013
- RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021
- Políticas, guías, procedimientos, circulares, instructivos, aplicables los Procesos de Infraestructura Tecnológica Componente Seguridad de la Información y Ciberseguridad
- Arquitectura de la entidad procedimientos, demás normas internas y externas concordantes y complementarias que apliquen al proceso objeto de auditoría.

5. FORTALEZAS (Atributo desempeño 2300)

La disposición de la Oficina de Gestión de la Información como primera línea de defensa para atender el cronograma de las mesas de trabajo citadas por la Oficina de control Interno y remitir la información requerida.

La Oficina de Gestión de la Información OGI cuenta con monitoreo 7/24 por 365 días por parte de ITELCA recibiendo la información del comportamiento de los equipos monitoreados a través del SIEM de Fortinet – FORTISEM de esta manera la OGI genera un valor agregado en la ejecución del procedimiento, aportando a la mejora continua del servicio de seguridad informática y disponibilidad de la información detectando así posibles incidentes de seguridad y mitigando el impacto de estos a la entidad.

6. DEBILIDADES (Atributo desempeño 2300).

- No se tiene definida en específico una política de ciberseguridad en la entidad con el fin de garantizar la máxima protección en caso de incidentes de ciberseguridad y ataques de ransomware, y sí ocurre un ataque cibernético las diversas áreas sepan exactamente que pasos seguir para limitar el daño. De la misma manera para evaluar continuamente la preparación de la entidad para las amenazas e implementar las prácticas correctas para la respuesta a incidentes cibernéticos, que incluya un plan de respuesta efectivo y que se pruebe el plan regularmente con ejercicios de simulación de ciberseguridad.

- Al no existir un plan de continuidad del negocio en la entidad actualizado a la fecha de la auditoria, no se cuenta con una hoja de ruta para alinear un programa de ciberseguridad con el plan de continuidad y recuperación de

qué hacer si un ciberdelincuente intenta infiltrarse en la infraestructura tecnología de la entidad, para mantener una supervisión y un mantenimiento constante y que la entidad este un paso más delante de los ataques cibernéticos.

7. LIMITACIONES EN EL DESARROLLO DE LA AUDITORIA (Norma atributo 1130).

No se presentaron limitaciones que impidieran el desarrollo de la auditoria.

8. DECLARACION DEL AUDITOR (Norma atributo 1100-1120-1220).

En aplicación al Decreto 648 de 2017 Artículo 2.2.21.4.8, la Oficina de Control Interno incorpora los siguientes instrumentos para la Actividad de la Auditoría Interna:

i. Código de Ética del Auditor Interno que tiene como bases fundamentales, la integridad, objetividad, confidencialidad, conflictos de interés y competencia de esté.

ii. Estatuto de auditoría, en el cual se establecen y comunican las directrices fundamentales que definen el marco dentro del cual se desarrollan las actividades de la Oficina de Control Interno, según los lineamientos de las normas internacionales de auditoría.

9. COMPROMISO DEL AUDITADO (Norma desempeño 2420).

Dentro del aviso de la auditoría realizada a través de memorando interno No. 20221400050683 del 30 de septiembre de 2022, se informó a la Oficina de Gestión de la Información que en el marco de la auditoría interna de gestión y en cumplimiento del artículo 2.2.21.4.8 del Decreto 648 de 2017 "*Instrumentos de la actividad de la Auditoría Interna - Carta de representación",* toda la información suministrada a la Oficina de Control Interno debe cumplir con los criterios de veracidad, calidad y oportunidad. Así mismo, en la reunión de apertura desarrollada el 07 de octubre de 2022, se indicó a los auditados los compromisos y responsabilidades en la entrega de la información.

10. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN (Norma desempeño 1220).

Este documento contiene información de interés exclusivo del auditor y el auditado para surtir los trámites establecidos en la Guía de Auditoria de la función pública acogida por la oficina de control interna de la SAE en el macroproceso de evaluación y control.

En ese sentido, hasta tanto no se constituya como informe final y sea publicado en la página Web de la Sociedad de Activos Especiales SAE SAS, no podrá ser distribuido ni utilizado por terceros, ni se podrá hacer referencia a él en ningún otro asunto, sin el consentimiento previo y por escrito del jefe de Control Interno.

11. DESARROLLO DE LA AUDITORIA (Norma desempeño 2300).

Dando cumplimiento al Plan Anual de Auditoría vigencia 2022, y el rol de la Oficina de Control Interno en función de la actividad independiente y objetiva de evaluación y seguimiento que contribuye de manera efectiva al mejoramiento continuo de los procesos de Administración del Riesgo, Control y Gestión de la entidad, se programó la Auditoría interna de gestión – Proceso de Infraestructura Tecnológica Componente Seguridad de la Información Ciberseguridad.

12. INTERPRETACIÓN DE LOS RESULTADOS DE LA AUDITORÍA (Norma desempeño 2320).

Los aspectos evaluados en el proceso de auditoría tienen la siguiente interpretación según sus resultados, indicando el grado de cumplimiento de los controles establecidos en los riesgos y/o procedimientos evaluados o el impacto que supone la carencia o debilidad de éstos.

	**DESEMPEÑO ALTO** En los procedimientos y pruebas de gestión y cumplimiento de auditoría, se evidencia que existe un alto grado de observancia de las políticas, directrices, normas, estrategia y otros factores; además los controles y actividades se están ejecutando con efectividad.
	**DESEMPEÑO ADECUADO** En los procedimientos y pruebas de gestión y cumplimiento de auditoría, se evidencia que existe un grado de observancia de las políticas, directrices, normas, estrategia y otros factores; además los controles y actividades se están ejecutando, sin embargo, en caso de que, se presente alguna desviación podrían presentarse posibles oportunidades de mejora.
	**DESEMPEÑO BAJO** En los procedimientos y pruebas de gestión y cumplimiento de auditoría, se evidencia que existe un bajo grado de observancia de las políticas, directrices, normas, estrategia y otros factores; además, solo algunos controles y actividades se están ejecutando; pero son muy vulnerables y deben ser objeto de evaluación y rediseño para generar valor en la Entidad.
	**SIN DESEMPEÑO** En los procedimientos y pruebas de gestión y cumplimiento de auditoría, se evidencia que no se documentan y no se llevan a cabo actividades de control que garantizan el cumplimiento de los lineamientos de la alta dirección para mitigar los riesgos con impacto potencial en los objetivos institucionales.

RESUMEN DE OPORTUNIDADES DE MEJORA Y OBSERVACIONES (Atributo desempeño 2400)

Producto de la evaluación realizada por parte de la Oficina de Control Interno, fueron identificadas las siguientes oportunidades de mejora las cuales requieren de la formulación de acciones correctivas y de mejora que permitan subsanar las causas que dieron origen a las situaciones evidenciadas:

No	OM/OB[1]	Oportunidad de mejora y Observaciones	Repetido
1	OM	Procedimientos desactualizados	Si
2	OM	Matriz de riesgos establecidos y asociados a factores de riesgos en ciberseguridad.	No
3	OM	Gestión de Plan de remediación de Vulnerabilidades de Ethical Hacking.	No
1	OB	Actualización de Inventario de Hardware a cargo de la Oficina de Gestión de la Información	No
2	OB	Talento Humano	Si

Fuente: Papeles de trabajo auditoria

[1] OM: Oportunidad de Mejora. OB: Observación

CONCLUSIONES (Atributo desempeño 2400).

La oficina de control interno y de acuerdo con lo evidenciado y reportado en el presente informe en el ejercicio de evaluación y seguimiento concluye que el sistema de control interno del proceso de infraestructura tecnológica componente de seguridad de la información y ciberseguridad se encuentra en mejora continua y requiere análisis para la implementación de controles efectivos enfocados a la ciberseguridad y de un seguimiento continuo a fin de procurar la correcta ejecución de sus actividades bajo los principios que lo regulan.

Se observa la necesidad de establecer una política de ciberseguridad en la entidad con el fin de garantizar la máxima protección en caso de incidentes de ciberseguridad y ataques de ransomware.

Se logra evidenciar que la entidad no tiene específicamente identificados los riesgos clasificados como ciberseguridad, y de la misma manera pueda identificar causas, consecuencias y evaluar continuamente los controles y acciones para los riesgos identificados como de ciberseguridad en un seguimiento de mapa de riesgos para ciberseguridad.

El área como dueña del proceso, es responsable de realizar seguimiento en conjunto con las áreas involucradas y mantener una adecuada documentación actualizada de los procesos en la arquitectura de la SAE en lo concerniente a su Macro Proceso de tecnología.

Se evidencia la importancia de establecer un programa de ciberseguridad que este inmerso en todos los procesos de la entidad al igual que se encuentre alineado con la evaluación de la gestión del plan de continuidad y recuperación de la entidad.

La importancia de ejecutar planes de remediación de los escaner de vulnerabilidades sobre los activos y establecer cronogramas de remediación de vulnerabilidades por la identificación de la criticidad de los activos y desarrollarlas en los tiempos establecidos para mitigar riesgos de seguridad de la infraestructura tecnológica.

La Oficina de Control Interno informa que no se desconoce el trabajo realizado por la Oficina de Gestión de la Información en las campañas de comunicaciones informadas de manera general a través de los correos comunicaciones@saesas.gov.co del martes 22/11/2022 11:47 a.m, y correo del martes 22/11/2022 11:49 a.m. de: "*Objetivos de Seguridad y privacidad de la información*" y el correo de 24/11/2022 06:18 p.m. de: "*identificar, etiqueta y clasificar documentos en Office 365"* y esto genera un valor agregado para que los colaboradores de la entidad puedan identificar, etiquetar y clasificar los documentos de Office y de esta manera controlar: prevenir acceso no autorizado, evitar la fuga de información de acuerdo con su clasificación, reforzar los principios de "confidencialidad, integridad y disponibilidad" campañas que se realizaron dentro de las vigencias del proceso de auditoría.

La Oficina de Control Interno en su rol de enfoque hacia la prevención, asesoría y acompañamiento y dada las situación actual y condiciones de aumento de casos por enfermedades respiratorias y posible aislamiento para trabajo remoto, sugiere que la Oficina de Gestión de la Información a cargo del Macroproceso de Tecnología – Proceso de Gestión de infraestructura tecnológica componente Seguridad de la Información y Ciberseguridad, como generadora de valor y en pro de evitar perdida, fuga y secuestro de información de la entidad, valide la propuesta de plantear a la dirección de la entidad el suministro de equipos corporativos para el trabajo remoto seguro sobre los dispositivos personales, de esta manera poder controlar mejor el tráfico de información para las políticas de seguridad de la entidad.

15 SOCIALIZACIÓN Y SOPORTE DE LOS RESULTADOS DE LA AUDITORÍA

De acuerdo con lo establecido en el procedimiento para ejecutar auditorías internas P-EC2-156 Versión 4 - 21/08/2019, actividad 15. Se remitió mediante correo electrónico del 25 de noviembre de 2022 informe preliminar con el objeto de que el área auditada pudiera desvirtuar las situaciones identificadas con las respectivas evidencias dentro de los tres (3) días hábiles siguientes al recibo del documento.

Se recibió respuesta en términos por parte de las áreas de sociedades activas y en liquidación el día 28 de noviembre del 2022 mediante correo electrónico, información que fue sujeta análisis de la oficina de control interno, cuyos resultados se incluyeron en el cierre de la auditoria que se realizó el 01/12/2022 y en el contenido del informe final que se presentó el día 02/12/2022 a las áreas que intervinieron.

Cordialmente,

Diana del Pilar Mayor Varela.
Jefe Oficina de Control Interno

Proyecto: Equipo Auditor
Aprobó: Jefe Oficina de Control Interno