MEMORANDO No CI2021-016715

Bogotá, 3 de diciembre de 2021

PARA: **Dr. Jaime León Gómez Salazar**
Jefe Oficina Asesora de Planeación

Giovanny Alejandro Lopez Insuasti
Jefe Oficina de Gestión de la información.

Sandra Milena Martinez
Gerente Talento Humano

DE: **María del Pilar Mayor Varela**

ASUNTO: **Informe Final De Auditoria Interna al Sistema de Gestión de Continuidad del Negocio**

Respetados Doctores:

Conforme al Plan Anual de Auditoría vigencia 2021 aprobado por Comité Institucional de Coordinación de Control Interno, la Oficina de Control Interno realizó auditoría de gestión al sistema de gestión de continuidad del negocio.

Adjunto se remite informe final que contiene los resultados de la auditoría, los cuales fueron comunicados previamente mediante correo electrónico del 25 de noviembre de 2021 y en reunión de cierre el 3 de diciembre de 2021.

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.

Cordialmente,

María del Pilar Mayor Varela
Jefe Oficina de Control Interno

Copias: Andrés Alberto Avila Avila-Presidente SAE
Anexo: Informe final en Word

APROBÓ: María del Pilar Mayor Varela
ELABORÓ: Equipo auditor.

INFORME DE AUDITORIA INTERNA

AI SISTEMA DE GESTION DE CONTINUIDAD DEL NEGOCIO

AUDITOR LIDER

JAVIER MAURICIO PERALTA CUBILLOS

AUDITORES ACOMPAÑANTES
GLADYS CAROLINA PALACIOS NIÑO

FECHA DE AUDITORIA
25 de octubre al 3 de diciembre de 2021

TABLA DE CONTENIDO

1. OBJETIVO (Norma desempeño 2210).....5
2. ALCANCE (Norma desempeño 2220) 5
3. METODOLOGÍA (Norma desempeño 2310).....5
4. CRITERIOS DE AUDITORIA (Norma desempeño 2040). 5
5. FORTALEZAS (Atributo desempeño 2300) 6
6. DEBILIDADES (Atributo desempeño 2300).....6
7. LIMITACIONES EN EL DESARROLLO DE LA AUDITORIA (Norma atributo 1130) 6
8. DECLARACION DEL AUDITOR (Norma atributo 1100-1120-1220).....6
10. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN (Norma desempeño 1220).....7
11. DESARROLLO DE LA AUDITORIA (Norma desempeño 2300) 7
12. SITUACIONES IDENTIFICADAS (Norma desempeño 2400).....10
12.1 DESCRIPCIÓN EVENTOS CON DESEMPEÑO ALTO 11
12.2 DESCRIPCIÓN OPORTUNIDADES DE MEJORA/OBSERVACIONES 11
Oportunidad de Mejora No 17 Plan De Mejoramiento Interno 2019 25
1. RESUMEN DE OPORTUNIDADES DE MEJORA Y OBSERVACIONES.....28
2. CONCLUSIONES 29
3. ANEXOS 30

INTRODUCCIÓN

La Oficina de Control Interno en desarrollo de su función constitucional, lo descrito en el Plan Anual de Auditoria de la vigencia 2021 y respondiendo a la solicitud realizada por la Presidencia de SAE, practicó auditoría interna de gestión orientada a verificar la eficacia del Sistema de Control Interno institucional en las actividades del sistema de gestión de continuidad del negocio.

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 DE AUDITORIA INTERNA
AI SISTEMA DE GESTION DEL PLAN DE CONTINUIDAD DEL NEGOCIO

1. OBJETIVO (Norma desempeño 2210)

- Evaluar la eficiencia, eficacia, efectividad y economía del macroproceso del Sistema de Gestión de continuidad del negocio en la SAE, teniendo en cuenta las políticas establecidas.
- Evaluar el diseño e implementación de los controles y riesgos asociados a los procesos a evaluar.
- Evaluación del Talento Humano de las áreas auditadas.
- Verificación de los avances del plan de mejoramiento interno.

2. ALCANCE (Norma desempeño 2220)

Efectuar procedimientos de solicitud de información y visita en campo, donde se verificará el estado de planeación y gestión de la continuidad del negocio durante la presente vigencia de enero 2020 a octubre de 2021.

La información que se tuvo en cuenta, para su análisis fue a corte del 30 de octubre de 2021.

3. METODOLOGÍA (Norma desempeño 2310)

- Solicitud de información (en todas las etapas de la auditoria).
- Verificación documental.
- Entrevistas con áreas. – A través de Teams.
- Consulta aplicativos
- Elaboración de informe.
- Presentación de resultados.

Teniendo en cuenta la coyuntura presentada por la emergencia sanitaria del Covid-19, el proceso auditor incluyó reuniones sincrónicas con los auditados y entre el equipo auditor.

4. CRITERIOS DE AUDITORIA (Norma desempeño 2040).

- Ley 1708 de 2014.
- Decreto 2136 de 2015
- ISO 22301:2019
- Mapa de Riesgos operativos, de seguridad de la información y de corrupción
- Manual de continuidad del negocio
- Metodología de impacto del negocio.
- Plan de manejo de crisis
- Plan de recuperación de desastres
- Plan de continuidad del negocio.
- ISO/IEC 27001:2013

- Guía para la preparación de las TIC para la continuidad del negocio
- Demás normas externas y políticas establecidas por la Organización frente a los temas evaluados.

5. FORTALEZAS (Atributo desempeño 2300)

- Disposición de la primera y segunda línea de defensa para atender el cronograma de las mesas de trabajo propuestas por la Oficina de Control Interno y remitir la información requerida.

- Se han venido realizando simulacros anuales de plan de recuperación de desastres por parte de la OGI, con miras a fortalecer debilidades o deficiencias encontradas en dichas pruebas.

6. DEBILIDADES (Atributo desempeño 2300)

- No existe articulado un plan de continuidad del negocio en la entidad actualizado a la fecha de la auditoría, el cual se emplee como una hoja de ruta en caso de presentarse algún desastre o alguna contingencia que afecte las actividades de la entidad.

- De igual forma no se evidencia capacitación, inducción y reinducción a la alta dirección que pueda articular el mismo y promocionarlo y gestionarlo en la entidad.

- Por otra parte, no se han venido realizando actualizaciones a los documentos presentados en vigencias anteriores y las deficiencias encontradas en auditorias anteriores no han sido resueltas a la fecha de la realización de la evaluación en la presente vigencia enmarcada en la realización de la auditoria.

- Incumplimiento parcial o total de la normatividad interna y externa.

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)

La auditoría se realizó con base en el análisis de diferentes muestras seleccionadas por el equipo auditor y se fundamentó en el siguiente soporte documental: Carpetas digitales, procesos y procedimientos del sistema de gestión, reportes de los sistemas de información, cruces y validaciones, página web y normas internas y externas.

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 CI2021-014519 del 19 de octubre de 2021, se les manifestó a los líderes de los procesos auditados 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.

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 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)

Mediante citación por correo electrónico del 25 de octubre de 2021 dirigido al jefe de Oficina Asesora de Planeación y Jefe Oficina Gestión de la Información, se solicita reunión de apertura de la auditoria a la gestión al plan de continuidad del negocio.

Conforme al procedimiento para ejecutar auditorías internas, se remitió el plan de auditoria a los auditados para revisión y aprobación de los tiempos y fechas mediante memorando No. CI2021- 014519 del 19 de octubre del 2021 y se llevó a cabo reunión de apertura el 25 de octubre de 2021 con los líderes de los procesos y sus equipos de trabajo mediante video llamada a través de Microsoft Teams.

La Sociedad de Activos Especiales SAE SAS ha venido operando desde el mes de junio del 2020 bajo la modalidad de alternancia, dentro de la nueva normalidad y autorizado por el Gobierno Nacional, la Oficina de Control Interno llevó a cabo el ejercicio de auditoria mediante la modalidad presencial y el mecanismo de trabajo en casa, realizando la etapa de entrevistas con los auditados a través de la herramienta tecnológica Teams.

11.1 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 los 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, pero presentan oportunidades de mejora para elevar la generación de valor en la Entidad
	**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.

11.2 Riesgos evaluados (Norma desempeño 2110)

Riesgos Identificados en el proceso de auditoría	Tipo de Riesgo	Calificación de riesgo inherente según matriz de riesgos SAE[1]
Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.	Operativo	Alto

Riesgos Identificados en el proceso de auditoría	Tipo de Riesgo	Calificación de riesgo inherente según matriz de riesgos SAE[1]
Se podría presentar fallas en la transferencia del conocimiento	Operativo	Extremo
Puede ocurrir que se genere un soporte inadecuado o inoportuno a los usuarios	Operativo	Moderado
Se podría presentar que la persona en el momento del retiro no haga la debida entrega del puesto de trabajo	Operativo	Alto
Podría presentarse que el personal capacitado no adquiera el conocimiento y/o las competencias de acuerdo con el objetivo establecido.	Operativo	Moderado
Podría ocurrir que se incumpla con la normatividad vigente	Operativo	Alto
Puede ocurrir que se presente la interrupción de la tecnología (Hardware y Software)	Operativo	Bajo
Posibilidad que se presente un evento de desorden publico	Operativo	Extremo
Podría ocurrir que se afecte el desempeño en las aplicaciones	Operativo	Moderado
Puede ocurrir que se presente falta de programas de gestión de cambio y seguimientos en el uso y apropiación de TIC's	Seguridad de la información	Alto
Podria presentarse inconsistencias o pérdida de la Información	Seguridad de la información	Este riesgo no está contemplado dentro del mapa riesgos de SAE
Puede ocurrir que no estén disponibles los Servicios de TI	Seguridad de la información	Extremo

Riesgos Identificados en el proceso de auditoría	Tipo de Riesgo	Calificación de riesgo inherente según matriz de riesgos SAE[1]
Puede ocurrir que se presente fuga o pérdida de información.	Seguridad de la información	Alto
Se podría presentar secuestro de datos “Ransomware”	Seguridad de la información	Este riesgo no está contemplado dentro del mapa riesgos de SAE
Se podría presentar que no se cuenten con las funciones debidamente establecidas en los formatos "Comunicación individual de funciones" y las ejecutadas por los colaboradores.	Operativo	Este riesgo no está contemplado dentro del mapa riesgos de SAE
Se podría presentar que los formatos "Comunicación individual de funciones "no se encuentre debidamente diligenciados y firmados	Operativo	Este riesgo no está contemplado dentro del mapa riesgos de SAE
Se podria presentar no dar respuesta adecuada y oportuna a las solicitudes de asesoría y acompañamiento a la gestión de la SAE	Operativo	Bajo
Se podría presentar Perdida de información por falta de comunicación en la entrega de cargos	Operativo	Este riesgo no está contemplado dentro del mapa riesgos de SAE

Para este punto, se realizó el ejercicio de verificación con el Jefe de Oficina Asesora de Planeación y Jefe Oficina Gestión de la Información de los riesgos identificados en la auditoria que posiblemente afecten el cumplimiento de las actividades enmarcadas en el seguimiento y documentación del plan de continuidad del negocio, al igual que actividades de control que permitan mitigar y minimizar la probabilidad de ocurrencia e impacto de los eventos identificados.

12. SITUACIONES IDENTIFICADAS (Norma desempeño 2400)

Las situaciones identificadas resultan de la comparación que se realiza entre un criterio y la situación actual encontrada durante la auditoria a un área o proceso. A continuación, se describirán los hechos y aspectos positivos, útiles o destacables del proceso auditado, bajo el símbolo o bandera verde , por otra parte, los hechos detectados en el examen de auditoría, referente a deficiencias, desviaciones, irregularidades o debilidades del proceso identificados como Oportunidades de Mejora con el símbolo o bandera roja o gris ya que son eventos que al ser evaluados

no cuenten con controles o los establecidos no se implementen de manera eficaz, eficiente y efectiva, por lo tanto, ameritan la implementación de un plan de mejoramiento.

Para el caso de las observaciones, se encuentran identificadas con el símbolo o bandera amarilla y son aquellos eventos que potencialmente podrían conducir una materialización de un riesgo y se documentan dentro de este informe para que el proceso o área auditada evalúe la pertinencia de implementar un plan de mejoramiento.

12.1 DESCRIPCIÓN EVENTOS CON DESEMPEÑO ALTO

No se encontraron aspectos en los cuales la ejecución de controles tenga un desempeño alto.

12.2 DESCRIPCIÓN OPORTUNIDADES DE MEJORA/OBSERVACIONES

Oportunidad de Mejora No 1: Procedimientos desactualizados

En revisión de los temas pertinentes a la gestión de continuidad del negocio se pudo observar los siguientes documentos que se encuentran desactualizados, adicionalmente es importante tener en cuenta que la entidad se encuentra certificada por en la ISO 9001 y de acuerdo a lo establecido en la norma la organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de calidad incluidos los procesos necesarios para revisar y actualizar la documentación pertinente.

A continuación, se presentan los procedimientos evaluados

- L-DE2-005_Plan_de_Continuidad_del_Negocio. Documento elaborado en el año 2018 y sin cambios realizados a la fecha.
- Informe BIA_v4. Documento elaborado en el año 2018.
- G-DE2-015 Metodología de Análisis de Impacto al Negocio BIA. Elaborado en el año 2018.
- L-DE2-007_Plan_Maestro_simulacro. Año 2019.

De acuerdo a lo anterior se evidencia incumplimiento a la norma citada, generando incertidumbre a las actividades a realizar por posibles riesgos que se presenten por el personal de la Entidad y no comprobar que siguen reflejando lo que ocurre en la organización.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Se podría presentar Secuestro de datos “Ransomware”
- Puede ocurrir que se presente fuga o pérdida de información.
- Puede ocurrir que no estén disponibles los Servicios de TI
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones

- Se sugiere realizar las actualizaciones a los procedimientos y la nueva documentación al respecto, esto debido a que no se ha realizado modificaciones, desde hace varios años
- Se recomienda realizar un análisis de la pertinencia de adquirir apoyo a través de una consultoría especializada en el tema.

Observaciones de la OGI: En todo el documento sugieren que se realice con una consultoría externa, sin embargo, se realizará fortaleciendo las competencias a través de capacitación y generar las mejoras con el personal de planta de la SAE, ¿esto podría quedar en las recomendaciones?

Observaciones de la OAP: No sé si de pronto se podría ampliar la recomendación incluyendo la opción de realizar planes de choque o priorización de la actualización de estos documentos dentro la labor que ya viene realizando el equipo del SGC de la OAP. Lo mismo para todas las recomendaciones que relacionan la consultoría externa**.**

Análisis Equipo Auditor: De acuerdo a las observaciones de las áreas auditadas, la Oficina de Control Interno realiza unas recomendaciones orientadas a la mejora continua de la entidad, con el fin que una consultoría especializada los oriente a fortalecimiento de un plan de continuidad del negocio, sin embargo, el líder del proceso es el responsable de establecer cuál es la actividad pertinente para que la oportunidad de mejora no se materialice.

Lo importante es o bien capacitar el personal de la SAE, para lo cual se hace necesario la experticia de un consultor externo que ayude a integrar al BCP y a su vez capacite a los funcionarios en tal actividad.

Por lo anterior, la Oportunidad de Mejora se mantiene tal como se documentó inicialmente**.**

Oportunidad de Mejora No 2. Deficiencia en las políticas de gestión de la continuidad del negocio

En revisión realizada a la documentación publicada en la arquitectura de la entidad solo se observó la siguiente metodología en cuanto a gestión de continuidad del negocio, la cual debe ser impartida, conocida y divulgada desde la alta gerencia.

ELABORACIÓN Y APROBACIÓN DE LA METODOLOGÍA

Elaboró:	Técnica: Johan Leal Ramiro Merchán Revisión Técnica Dianalin Neme Prada	Consultor Consultor Profesional Especializado III	UT GLOBALTEK SECURITY – SAFEID Dianalin Neme Prada
	Metodológica: Alexander Cordero Gómez	Profesional I	Oficina Asesora de Planeación
Aprobó:	Antonio Orlando Olaya	Jefe Oficina Gestión de la Información	Oficina Gestión de la Información

De acuerdo con lo anterior se evidencia incumplimiento a la ISO 22301 del 2019 donde se debe establecer y documentar una política de continuidad de negocio alineada con la dirección estratégica de la organización. Los requisitos del SGCN deben integrarse en los procesos comerciales y contar con los recursos adecuados.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Se podría presentar fallas en la transferencia del conocimiento
- Podría presentarse que el personal capacitado no adquiera el conocimiento y/o las competencias de acuerdo con el objetivo establecido.
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones

- Se sugiere generar esquemas de trabajo con apoyo de una consultoría especializada que permita generar actualizaciones y nueva documentación al respecto
- Se recomienda establecer una Política de gestión de la continuidad del negocio teniendo en cuenta las especificaciones que establece la ISO 22301 del 2019, donde se encuentre debidamente aprobada y formalizada.
- Se recomienda socializar a los directivos y al interior de la entidad de su contenido y riesgos asociados.
- Se sugiere solicitar un presupuesto designado a la oficina encargada con el fin de gestionar el plan de continuidad del negocio en la entidad.

Observaciones OAP: En el documento de Política de Seguridad y Privacidad de la Información se encuentra relacionada una Política de Continuidad de negocio: Política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información (Pàg 80),

Con relación al tema del presupuesto, no sé si éste ya se vea reflejado en otros centros de costos y rubros para gestionar los planes de emergencia, la infraestructura física, en Tecnología todo el tema de mesa de ayuda, mantenimientos preventivos, evolutivos y corretivos…y en general todo el presupuesto para el normal funcionamiento y continuidad del negocio de SAE… ?

Análisis Equipo Auditor: Dentro de la arquitectura se observó un Manual de Seguridad de la Información, donde se incorporaron una "Políticas de Inclusión de Seguridad de la Informacion en la Gestión de la Continuidad del Negocio", al revisar su contenido se observa que no cumple en su totalidad con lo establecido en la ISO 22301 del 2019, al igual que en la Guía para la preparación de las TIC para la continuidad del negocio indica que *"Teniendo en cuenta lo establecido en el Plan Vive Digital, liderado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, en cuanto a la infraestructura, los servicios, las aplicaciones y los usuarios en el marco de un ecosistema digital; las recomendaciones brindadas en el Plan Nacional de Desarrollo 2015-2018 en cuanto a la necesidad de reconocer la seguridad y privacidad de la información, como un factor primordial para la apropiación de las TIC; la constante evolución de los mercados; y la dinámica de las entidades, plantea un marco de seguridad de la información para la prestación de servicios a los ciudadanos a través de las tecnologías de la información, el cual*

deberá ser respaldado por una gestión, unas políticas y unos procedimientos adecuados, que resalten el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que esté orientado a preservar los pilares fundamentales de la seguridad y privacidad de la información, de acuerdo a lo anterior se debe documentar una política de continuidad de negocio alineada con la dirección estratégica de la organización. Los requisitos del SGCN deben integrarse a través de toda la organización y contar con los recursos adecuados, para su debida gestión.

Adicionalmente, es pertinente precisar que de acuerdo con lo estipulado en el Manual del sistema integrado de gestión M-DE-005 Versión 8 - 16/07/2021, se tienen los siguientes conceptos:

- **Manual:** es un **"***Documento que contiene en forma explícita, ordenada y sistemática información sobre objetivos, políticas, atribuciones, así como la forma de utilización de sistemas informáticos y herramientas tecnológicas,* aprobado por comité Directivo
- **Política**: es un *"Documento de alto nivel, expresado por la alta dirección, para definir sus intenciones y dirección general en relación con el funcionamiento de la organización*", aprobado por la junta directiva.

Con respecto a lo del presupuesto, nos permitimos comunicar que, en mesas de trabajo, nos informaron que no se cuenta con un presupuesto designado para el tema y teniendo en cuenta la importancia el plan de continuidad del negocio, sugerimos establecer un presupuesto, con el fin que pueden generar mejora continua.

Por lo anterior, la Oportunidad de Mejora se mantiene tal como se documentó inicialmente**.**

Oportunidad de Mejora No 3. Ausencia de directrices claras que definan un marco o una ruta para gestionar el sistema de continuidad de negocio en la organización.

Al realizar las debidas reuniones con las áreas encargadas de gestionar el plan de continuidad de negocio se evidencia que a la fecha de la auditoria en los últimos dos años revisados no se han realizado gestiones al respecto desde la primera línea de defensa encargada del tema de continuidad del negocio, el cual permita a las áreas tener una ruta definida que les pueda aportar y articular todo el proceso de gestión de la continuidad del negocio.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Podría presentarse que el personal capacitado no adquiera el conocimiento y/o las competencias de acuerdo con el objetivo establecido.
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones

- Se recomienda definir un plan y cronograma de trabajo con apoyo de un consultor especializado en materia de gestión de continuidad del negocio, con el fin de crear una hoja de ruta la cual contemple toda la documentación y plan de acción necesario para la organización, la cual le permita estar preparada en caso de una contingencia.
- Se recomienda socializar el plan y el cronograma con la alta gerencia y directivos.

Observación de la OAP: Esta hoja de ruta no podría estar asociada con el procedimiento de activación del plan de manejo de crisis?

Análisis Equipo Auditor: Esta hoja de ruta no solamente va con el manejo de crisis, si no va orientada a todos los componentes del BCP tal como lo establecen en la Guía para la preparación de las TIC para la continuidad del negocio donde indica en la justificación que "*La gestión de la continuidad del negocio, es un proceso holístico a través del cual se identifican los impactos potenciales que amenazan la continuidad de las actividades de las Entidades, proveyendo un marco de referencia para la construcción de la resiliencia y la capacidad de una respuesta efectiva, que le permita proteger los intereses de las Entidades debido a disrupciones"*, teniendo en cuenta lo anterior, es un complemento del modelo de seguridad y privacidad de la información y se constituye en un referente de la continuidad del negocio para las entidades del Estado.

Por lo anterior, la Oportunidad de Mejora se mantiene tal como se documentó inicialmente, el cual establece el PCN en conjunto como hoja de ruta o directriz para que la entidad responda ante un eventual desastre.

Oportunidad de Mejora No 4. Ausencia de actas de reuniones de entrega y que evidencie la debida estructura de la organización en el sistema de continuidad del negocio.

Se solicitó al área encargada mediante correo electrónico soportes de las reuniones realizadas con miras a gestionar el plan de continuidad del negocio las cuales no fueron suministradas a la auditoría, adicionalmente, se realizó consulta sobre el acta de entrega al respecto por el anterior jefe encargado y tampoco se adjuntó evidencia.

De acuerdo con lo anterior no se pudo evidenciar seguimiento de las actividades en materia de gestión de continuidad del negocio, que conlleva a un inadecuado gobierno por parte de las áreas encargadas y responsables de implementar este sistema en la SAE.

Riesgos asociados

- Se podrían presentar que no se cuenten con las funciones debidamente establecidas en los formatos "Comunicación individual de funciones" y las ejecutadas por los colaboradores.
- Se podría presentar que la persona en el momento del retiro no haga la debida entrega del puesto de trabajo
- Podría presentarse que el personal capacitado no adquiera el conocimiento y/o las competencias de acuerdo con el objetivo establecido.
- Se podría presentar fallas en la transferencia del conocimiento.

Recomendaciones

- Se sugiere generar esquemas de trabajo que permitan gestionar el plan de continuidad del negocio a través de las diferentes áreas involucradas.
- Se recomienda implementar mesas de trabajo donde se presente al avance de la gestión de continuidad del negocio
- Se recomienda documentar las mesas de trabajo, donde se establezcan compromisos y responsabilidades.

Oportunidad de Mejora No 5. Matriz de riesgos con respecto al plan de continuidad del negocio.

A pesar de que se encuentra en la matriz de riesgos de la entidad unos riesgos específicos en aspectos de continuidad del negocio, no se evidencia una articulación específica en la entidad y en la cual se puedan identificar todos los riesgos asociados a la gestión de continuidad del negocio y que a su vez puedan ayudar a la administración y la entidad a mitigar el impacto en la interrupción de las operaciones del negocio.

Teniendo en cuenta lo descrito en el párrafo anterior se evidencia incumplimiento a la ISO 22301 en cuanto que la entidad presenta deficiencias en la evaluación de riesgos completa para el plan de continuidad del negocio que permitirá a la organización determinar la probabilidad de ocurrencia de incidente, donde le ayude a identificar las acciones necesarias para reducir la probabilidad y el impacto en las actividades priorizadas de la organización en caso de un incidente disruptivo.

Las evaluaciones de riesgos deben realizarse a intervalos planificados o cuando se produzcan cambios significativos en la organización o en el contexto en el que opera

Riesgos asociados

- Puede ocurrir que se presente la interrupción de la tecnología (Hardware y Software)
- Posibilidad que se presente un evento de desorden publico
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones

- Se sugiere generar esquemas de trabajo con apoyo de una consultoría especializada o bien con personal capacitado en materia de continuidad del negocio, que permita elaborar una matriz de riesgos especifica en materia de gestión de continuidad del negocio.
- Se recomienda incluir dentro de la Política de riesgos de SAE la matriz de Continuidad del Negocio o bien incluirla en la cual se haga necesario dar la importancia de la continuidad del negocio dentro de la organización y poder garantizar la operación de la misma en medio de una interrupción o un desastre en la entidad.
- Se recomienda realizar un análisis e implementación de una Matriz de riesgos de Continuidad del Negocio.

Observación OAP: Evaluación de riesgos en temas de continuidad del negocio, ya que sería desconocer los riesgos ya descritos en la matriz de riesgos… ¿No sé si esto sería un incumplimiento como tal a la norma o una oportunidad de mejora a fin de identificar más riesgos asociados a la continuidad del negocio?

¿O aclarar en este aspecto que es una matriz de riesgos específica asociada al plan de continuidad de negocio como lo da entender el título de esta oportunidad de mejora…?

Análisis Equipo Auditor: El tema es que en materia de plan de continuidad del negocio no se presenta un esquema completo o presenta deficiencias en materia del plan de continuidad del negocio esto dicho en otra forma se traduce en que a pesar de haber comenzado en el 2018 desde esa fecha no se han retomado los análisis y recomendaciones respectiva en materia de continuidad del negocio y a su vez el plan de continuidad de negocio está en una fase inicial

según nivel de madurez evaluado lo cual hace necesario terminar la implementación del mismo en la entidad prueba de ello es que no se han realizado las pruebas a todos los escenarios planteados en el mismo tal como lo establece en la Guía para la preparación de las TIC para la continuidad del negocio en su numeral 13.4 Gestión del Riesgo "*La metodología del plan de continuidad del negocio determina los diversos escenarios de amenazas de una Entidad, el cual permite desarrollar las estrategias de continuidad y los planes para reanudar los servicios que estaban en operación. La gestión del riesgo debe contemplar el "cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia. A pesar de la existencia de diversidad de métodos es recomendable iniciar con los más sencillos, que forman parte de lo que denominamos análisis previos. Una primera aproximación es la de establecer un conjunto de causas que pueden generar dificultades" de acuerdo a lo anterior,* es necesario que la entidad fortalezca la gestión del riesgo y a su vez su clasificación y análisis específico en materia de continuidad del negocio.

Observación OAP: Me parecería prudente dejarlo abierto también a que se pueda realizar con la capacidad operativa interna de la SAE.

Análisis Equipo Auditor: Se sugiere que se realice a través de una consultoría ayude o apalanque el negocio debido a la complejidad del tema, o si el dueño de proceso lo determina mediante fortalecimiento de las competencias a través de capacitación y generar las mejoras con el personal de planta de la SAE, con el fin que pueda mitigar la OM

Observación OAP: Está estaría incorporada dentro de la matriz general de riesgos operacionales, donde una de las categorías sería el tema de continuidad del negocio.

Análisis Equipo Auditor: Es necesario establecer todo un capítulo al respecto porque es un tema indispensable hoy en día, para todas las organizaciones.

Por lo anterior, la Oportunidad de Mejora se mantiene tal como se documentó inicialmente**.**

Oportunidad de Mejora No 6. Ausencia de un debido marco de gestión como lo solicita la norma enmarcada del ciclo de gestión P-H-V-A, ISO 22301 aplicado al sistema de gestión de continuidad del negocio.

Al realizar la revisión y solicitud de información no se evidencia la aplicación del ciclo PHVA dentro del marco de sistema de gestión de continuidad del negocio, una muestra de ellos es la ausencia de gestión por parte de la administración dentro del alcance de la auditoria y a su vez una muestra de control de cambios en el versionamiento y actualización de la documentación al respecto.

Al igual no se encontro una herramienta para administrar los cambios al preguntar por està, en la cual se pueda observar y administrar los cambios con su debido análisis de impacto y probabilidad del riesgo.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Podría presentarse inconsistencias o pérdida de la Información
- Puede ocurrir que se presente falta de programas de gestión de cambio y seguimientos en el uso y apropiación de TIC's
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones

Se sugiere generar esquemas de trabajo con apoyo de una consultoría especializada que permita generar actualizaciones y nueva documentación al respecto.

Observación OAP: No sé si estos cambios se refieran a los cambios enmarcados dentro del plan de continuidad del negocio o cambios organizacionales generales que puedan afectar la continuidad del negocio. Frente a esto contamos con un procedimiento de gestión de cambios, en los cuales se han documentado los cambios significativos en la sae junto con los posibles efectos a causar en la organización

Análisis Equipo Auditor: Hay un procedimiento de control de cambios, pero hace falta uno que ayude a establecer el impacto de cada cambio y así poder manejar toda la trazabilidad del mismo, en el cual se ajuste a las necesidades del negocio y ayude administrar precisamente estos cambios, muestra de eso es la gestión en materia de observaciones ya realizadas en BCP y actualización documental necesaria al respecto, así mismo se hace necesario la mejora continua del SGCN, según lo establecido en la Guía para la preparación de las TIC para la continuidad del negocio en el *componente12 Mejora continua para la preparación de las tic para la continuidad del negocio*, donde indica que "*Este componente le permitirá a la Entidad realizar acciones correctivas apropiadas a los potenciales impactos determinados por el análisis de impacto del negocio BIA de la Entidad*".

A continuación, se presenta el ciclo de funcionamiento del modelo de operación de continuidad de negocio, con el fin que se observe la mejora continua del mismo



Por lo anterior, la Oportunidad de Mejora se mantiene tal como se documentó inicialmente**.**

Oportunidad de Mejora No 7. Establecer un paso a paso detallado por funcionario, actividad y tiempo específico al ejecutar las actividades a desarrollar en el DRP.

Omisión de un debido detalle en la matriz de DRP en la cual se desglose actividades realizadas para restablecer un servicio por funcionario y tiempos de RTO debidamente calculados y soportados, al igual que tiempos utilizados en reestablecer el servicio.

Al adjuntar la matriz de DRP se evidencian actividades realizadas en las pruebas, sin embargo, como una oportunidad de mejora se puede llegar al detalle de las actividades específicas por servicio y los diferentes pasos para ejecutar cada una de las actividades a realizarse al subir o bajar servicios.

Riesgos asociados

- Podría ocurrir que se afecte el desempeño en las aplicaciones
- Puede ocurrir que se genere un soporte inadecuado o inoportuno a los usuarios

Recomendaciones

Se recomienda generar esquemas de trabajo que permitan generar el paso a paso por actividad, al igual que un cálculo de los RTO por cada uno de ellos los cuales sean insumo para articular todo el PCN.

Observación OGI: No es claro a que se refiere la oportunidad de mejora, agradezco ampliar la explicación para el desarrollo del plan de mejoramiento.

Así está desarrollado en el minutograma del simulacro enviado como evidencia del 2020

Análisis Equipo Auditor; Este tipo de procedimiento ayuda para que en próximas pruebas realizadas al DRP, se den omisiones o a su vez se puedan generar confusiones al respecto.

La Oportunidad de mejora va orientada a que se especifique cada procedimiento a realizar de su paso a paso detallado por funcionario, actividad y tiempo específico para ejecutar las actividades a desarrollar en el DRP los cuales sean insumo para articular todo el sistema en caso de ausencia de algún funcionario, el cual puede conllevar a una disrupción de las operaciones.

Todos los planes de recuperación deben definir los roles y responsabilidades de miembros del equipo de recuperación de desastre, y marcar el criterio para poner en marcha el plan. El plan entonces especifica en detalle, la respuesta del incidente y actividades de recuperación. Los protocolos para un DRP deben incluir quien y como contactar apropiadamente a los miembros del equipo del DRP y en qué orden recuperar los sistemas y correrlos tan pronto como sea posible.

De acuerdo a lo anterior se hace necesario no solo documentar el DRP sino específicamente los calculo establecidos en el BIA documento desarrollado por un externo, contratado por la SAE en el año 2018 y el paso a paso detallando actividad por actividad con el fin de eliminar brechas en el momento de activación o retorno de las operaciones especificadas y desarrolladas durante las pruebas de DRP a desarrollarse por cada uno de los ingenieros los cuales pueden estar o no presentes en un futuro.

Por lo anterior, la Oportunidad de Mejora se mantiene tal como se documentó inicialmente**.**

Oportunidad de Mejora No 8. Se observa que a la fecha no se han realizado las pruebas a todos los escenarios enmarcados en el plan de continuidad del negocio.

Cuando se estructura el sistema de gestión de continuidad del negocio se debe incluir no solo al área de TI en los planes de continuidad enmarcados, sino que se debe involucrar a toda la organización.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones

Se sugiere generar esquemas de trabajo con apoyo de una consultoría especializada que permita involucrar a las diferentes áreas y no solo a la OGI en el marco de trabajo del sistema de gestión de continuidad del negocio.

Oportunidad de Mejora No 9. Actualmente la organización no ha establecido intervalos de tiempo apropiados con el fin de revisar el plan de continuidad del negocio en donde asegure la disponibilidad continua, la adecuación y la efectividad. Estas revisiones deben quedar documentadas.

Se observa que la organización no ha gestionado desde hace varios años un marco y una hoja de ruta adecuado que permita involucrar a las diferentes áreas, al igual que un programa de gestión de cambios que permita actualizar los diferentes componentes del plan de continuidad del negocio como un plan de recuperación de desastres actualizado a la fecha de la revisión.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones

Se recomienda generar esquemas de trabajo con apoyo de una consultoría especializada que permita generar actualizaciones y nueva documentación al respecto, tal como lo establece la norma ISO 22301 en materia del sistema de gestión de continuidad del negocio.

Oportunidad de Mejora No 10. La organización debe establecer un programa continuo de capacitación y entrenamiento para su plan de continuidad del negocio no solo a los funcionarios, sino en materia específica a los funcionarios encargados de articularlo.

Se evidencia ausencia de capacitaciones a los funcionarios encargados articular y gestionar el plan de continuidad del negocio, lo cual permita gestionar el mismo, a través de toda la organización.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Se podría presentar que no se cuenten con las funciones debidamente establecidas en los formatos Comunicación individual de funciones" y las ejecutadas por los colaboradores.

Recomendaciones

Se sugiere generar esquemas de trabajo con apoyo de una consultoría especializada que permita capacitar a los funcionarios de la entidad en materia de gestión de continuidad del negocio.

Oportunidad de Mejora No 11 Los procedimientos de control de cambios deben operar efectivamente y deben ser un reflejo de su efectividad constante.

Al preguntarse por la aplicación de los procedimientos de control de cambios en el sistema de gestión de cambios no se ven reflejados en toda el área involucrada en el marco del sistema, esto conlleva a ineficacia del sistema de gestión de continuidad del negocio

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones

Deben reflejarse los procedimientos de control de cambios en la gestión de continuidad del negocio a través de toda la organización con el fin de minimizar el impacto en caso de presentarse interrupciones en la operación del negocio.

Oportunidad de Mejora No 12 Incluir a toda la organización en las pruebas al plan de continuidad
Se observan pruebas de DRP en el área involucrada de tecnología de información en cabeza de la OGI, sin embargo, no se evidencian pruebas de continuidad específicas para los diferentes escenarios contemplados que sean un reflejo de lo enmarcado.

Riesgos asociados

- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.
- Se podría presentar que no se cuenten con las funciones debidamente establecidas en los formatos "Comunicación individual de funciones" y las ejecutadas por los colaboradores.

Recomendaciones

Se Recomienda generar esquemas de trabajo con apoyo de una consultoría especializada que permita generar actualizaciones y nueva documentación al respecto.

Oportunidad de Mejora No 13 Comunicar a las autoridades, clientes y proveedores externos al realizar las pruebas al DRP.

Al preguntar por el esquema de comunicaciones al realizar las pruebas al DRP se evidenció que no solo deben tomar en cuenta los clientes internos, sino externos, así como las diferentes autoridades.

Riesgos asociados

- Se podría presentar que los formatos "Comunicación individual de funciones "no se encuentre debidamente diligenciados y firmados
- Puede ocurrir que los procesos no estén debidamente documentados, o que los documentos se encuentren desactualizados.

Recomendaciones

Se recomienda establecer un esquema de árbol de llamadas en la cual involucre a los diferentes clientes tanto internos como externos de la entidad.

Oportunidad de Mejora No 14 Documentar y Realizar pruebas a los backups realizados en la entidad

Establecer un procedimiento y un formato de diligenciamiento con las pruebas realizadas a los backups realizados en la organización que permitan fortalecer el esquema de los mismos y mitigar la materialización de los riesgos ya identificados y materializados en la entidad y soportados por el área encargada.

De esta misma forma está actividad permite fortalecer a la entidad en caso de presentarse un secuestro de datos e información (actividad que se está evidenciando actualmente en varias entidades a la fecha.

Riesgos asociados

- Podría presentarse inconsistencias o pérdida de la Información.
- Puede ocurrir que no estén disponibles los Servicios de TI.
- Puede ocurrir que se presente fuga o pérdida de información.
- Se podría presentar secuestro de datos “Ransomware”

Recomendaciones

Se sugiere documentar, establecer y diligenciar periódicamente un formato de realización de las pruebas a los backups generados en la entidad y a su vez contemplar los riesgos de ciberseguridad.

Observación OGI: No estoy de acuerdo con esta oportunidad de mejora, el esquema de Backup se encuentra documentado y contamos con la bitácora de Backup y las herramientas de backups tiene las tareas configuradas.

Por favor indicar, que información hace falta.

¿A que pruebas hacen referencia?

Análisis Equipo Auditor:

En reunión programada el día 27 de octubre de 2021, con la OGI, se realizó la consulta, si existía un procedimiento y un formato para las pruebas a los backups realizados en la entidad, por lo cual el grupo de la oficina de gestión de la informacion manifestaron no estar realizan pruebas a los backups, solo se realizan restauraciones a demanda, esto genera posibles pérdidas de informacion sensible de la Entidad, como se ha presentado en ocasiones que han sido reportadas por diferentes áreas a la OGI (Vicepresidencia Jurídica y Oficina de Control Interno, esto conlleva a una posible materialización del riesgo "*Puede ocurrir que se presente fuga o pérdida de información*"

Adicionalmente, se revisó el procedimiento el PT-1- 169 V1 del 23/04/2018 "*Procedimiento copias de respaldo y restauración"*, sin embargo, es necesario actualizar el documento, debido a que su última actualización fue en el año 2018 y se hace necesario establecer pautas para realizar pruebas a los backups lo cual pueda mitigar el impacto en caso de presentarse un ataque de ransomware como se ha venido realizando actualmente en diferentes entidades. Actualmente en la SAE.

Por lo anterior, la Oportunidad de Mejora se mantiene tal como se documentó inicialmente.

Oportunidad de Mejora No 15. Talento Humano

Se solicitó información el día 21 de octubre de 2021 a la Gerencia de Talento Humano de la copia del formato de las funciones establecidas y suscritas por los colaboradores de planta y temporal de las Oficinas de planeación y de Gestión de la información.

De la respuesta recibida mediante correo electrónico el día 28 de octubre de 2021, por la Gerencia de Talento Humano, se realizó la validación de veinte y dos (22) formatos *"Comunicación individual de funciones"* remitidas por la Gerencia de Talento Humano se evidenció lo siguiente:

- 6 formatos no cuentan con fecha de comunicación, corresponden a un 27% del 100% de los formatos remitidos.
- 10 formatos *"Comunicación individual de funciones* fueron comunicados y firmados el día 25 de octubre de 2021, fecha de la ejecución de la auditoria a personal que está vinculado desde el 2017, corresponde a un 45 % del 100% de los formatos remitidos.
- 22 formatos no tienen el visto bueno de la Gerencia de Talento Humano, corresponde a un 100% del 100% de los formatos remitidos.
- 1 formatos tienen diligenciada la fecha de ingreso errada, corresponden a un 5% del 100% de los formatos remitidos.
- Se evidencio que de 2 formatos de *"Comunicación individual de funciones revisados* no cuentan con una función que actualmente realizan los colaboradores, corresponden a un 9% del 100% de los formatos remitidos.
- 6 formatos tienen la fecha de comunicaciones anterior al ingreso del jefe Asignado al área, corresponden a un 27% del 100% de los formatos remitidos.

De acuerdo con lo anterior se evidencia que los formatos de *"Comunicación individual de funciones*" fueron comunicados y firmados por algunos colaboradores (vinculados desde el año 2017) en el trascurso de la auditoria (25 de octubre de 2021), adicionalmente los formatos no se encuentran debidamente diligenciados y las funciones que están establecidas en el documento, que fue suministrado a esta Oficina, no son las que actualmente están ejecutando

Adicionalmente, en desarrollo de la auditoria se solicitó, mediante correo electrónico los dias 5 y 12 de noviembre de 2021, copia del acta de entrega del puesto del jefe de la Oficina asesora de planeación, a la fecha de la entrega del informe de auditoría no fue posible recibir la información, sin embargo como se dejó la nota aclaratoria en los correos de solicitud "…*Si la información no es remitida a la OCI en la fecha establecida se da por entendido que la Oficina asesora de planeación no cuenta con lo solicitado*"**,**

Teniendo de acuerdo lo informado se logró evidenciar debilidad en la entrega y recibo del cargo incumpliendo las actividades 2, 3 y 4[1] del instructivo *"Desvinculación laboral o traslado y entrega de puesto de trabajo"* Código N-GT1-002 Versión 2 del 29/09/2016 y del Procedimiento de *"Traslado o Desvinculación de Talento Humano"* P-GT1-014 Versión 3 del 3/06/2020.

Riegos Asociados

- Se podrían presentar que no se cuenten con las funciones debidamente establecidas en los formatos *"Comunicación individual de funciones"* y las ejecutadas por los colaboradores.
- Se podría presentar que los formatos *"Comunicación individual de funciones "*no se encuentre debidamente diligenciados y firmados
- Se podría presentar que la persona en el momento del retiro no haga la debida entrega del puesto de trabajo
- Se podría presentar perdida de información por falta de comunicación en la entrega de cargos

Recomendaciones:

- Se recomienda mantener en la carpeta del historial Laboral la certificación laboral, firmada y actualizada desde la vinculación y sus respectivas modificaciones.
- Se sugiere revisar y actualizar las funciones vigentes de los Colaboradores de las Gerencias Regionales.
- Se recomienda dar cumplimiento al instructivo "Desvinculación laboral o traslado y entrega de puesto de trabajo" Código N-GT1-002 y garantizar que la entrega del puesto se realice directamente al jefe o coordinador de área.
- Se sugiere diligenciar y comunicar en debida forma y de manera oportuna el formato "Comunicación individual de funciones" del colaborador Emir Stevens Solano Rodríguez en cuanto a la denominación del empleo.

Observación OGI: Este informe debe ser remitido a la Gerencia de Talento Humano, dado que esta actividad es de su responsabilidad

Análisis Equipo Auditor: El informe se le copiara a la Gerencia de Talento humano, sin embargo, esta OM se deja plasmada dentro de este informe debido a que uno de los objetivos de la auditoria es *"Evaluación del Talento Humano de las áreas auditadas*", cabe resaltar que el plan de mejoramiento de esta OM la debe realizar la Gerencia de Talento Humano, como primera línea de defensa y debe ir incluida en el plan de mejoramiento que remite el dueño del proceso a la OCI.

[1] 2. Realizar Informe de entrega puesto de trabajo
3. Hacer entrega del Informe al jefe inmediato
4. Realizar seguimientos

Por lo anterior, la Oportunidad de Mejora se mantiene tal como se documentó inicialmente**.**

Oportunidad de Mejora No 16 Capacitación y directrices en materia de gestión de Continuidad del Negocio

En el trascurso de mesas de trabajo de la auditoria no se puedo evidenciar las capacitaciones, directrices y roles dadas a los directivos en gestión de continuidad del negocio.

Conforme a lo anterior se solicitó por correo electrónico el 28 de octubre a la Gerencia de Talento Humano, de la evidencia de la socialización a los directivos antiguos y nuevos del plan de continuidad del negocio y rol desempeñado por cada uno de ellos (copia del material y relación de la asistencia y evaluación si aplica 2020 y Cronograma según PEC 2021), la respuesta emitida por la gerencia fue el día 04 de noviembre de 2021, donde informo que "*No hay ningún registro en el PEC de esta socialización ni en el año 2020 ni 2021, se debe solicitar esta información al líder del plan de continuidad del negocio el cual es el Jefe de la Oficina Asesora de Planeación*"

Teniendo en cuenta que no se obtuvo respuesta a las solicitudes, se observa que a la fecha los directivos no cuentan con la información necesaria, el rol que ejercen en ello (1 o 2 línea de defensa), la importancia y el riesgo de un plan de continuidad del Negocio del Entidad.

Riegos Asociados:

- Se podría presentar fallas en la transferencia del conocimiento
- Podría ocurrir que se incumpla con la normatividad vigente

Recomendaciones:

Se recomienda realizar capacitaciones y socializaciones continuas en materia de gestión de continuidad del Negocio a los directivos, donde se les informe las responsabilidades, la importancia y el riesgo que tiene la Entidad.

Oportunidad de Mejora No 17 Plan De Mejoramiento Interno 2019

En el desarrollo de la auditoría se evidencio que a la fecha de desarrollo de la auditoría se encontraron aún sin cerrar y sin un avance significativo las oportunidades de mejora establecidas por la Oficina de Gestión de la Información con cierre al 31 de diciembre de 2021:

A continuación, se presentan las OM revisadas:

OM1	La Oficina de Gestión de la Información – OGI se encuentra en proceso de construcción el Plan de Recuperación de Desastres - DRP, el cual establece de forma detallada los procedimientos para recuperar los servicios de TI más críticos de la SAE, documento que se encuentra referenciado dentro de las políticas, como soporte en la toma de decisiones por parte del Líder de Continuidad del Negocio y del Comité de Crisis (Oportunidad de Mejora No. 1)

OM3

En el mes de abril de 2018, se practicaron las entrevistas y el levantamiento de información correspondientes a los Análisis de Impacto de Negocio – BIA con el fin de identificar para cada macroproceso los servicios críticos, clientes - proveedores internos y externos, sistemas de información y servicios tecnológicos clientes, recursos mínimos que se requieren para la apoyar la operación bajo circunstancias normales y en contingencias y tiempos de tolerancia, con relación a ejercicios para el año 2019 y próximos años, no hay una planificación oficial para actualizar la información anteriormente mencionada, lo anterior teniendo en cuenta la dinámica del negocio y de factores externos (Oportunidad de Mejora No. 3).

OM4

Por otro lado, para la Sociedad de Activos Especiales – SAE y específicamente para la Oficina de Gestión de la Información – OGI y ante una eventualidad (Crisis, Evento Catastrófico, Incidente, Desastre, Emergencia), el Plan de Recuperación de Desastres – DRP es un documento vital que permite detallar los procedimientos para recuperar y lograr el retorno de las operaciones a nivel tecnológico, donde para este caso el documento se encuentra en proceso de construcción; por lo anterior, no existe un DRP oficial y aprobado por la administración ante una eventualidad; por otro lado y en relación a lo anteriormente mencionado, la Oficina de Gestión de la Información – OGI desarrollo en el año 2018 el Plan de Implementación de Continuidad de Negocio, el cual en términos de corto, mediano y largo plazo prepararía y fortalecería a la Sociedad de Activos Especiales – SAE ante eventualidades (Crisis, Evento Catastrófico, Incidente, Desastre, Emergencia), este documento fue remitido el día 12 de septiembre de 2018 a la jefatura de la Oficina de Planeación mediante comunicado interno No. CI2018-022142, con el fin de poner en conocimiento de acuerdo al rol de Líder de Continuidad de Negocio que tiene el Jefe de la Oficina de Planeación; De acuerdo con lo anterior, se establece que a pesar que el Plan de Implementación de Continuidad de Negocio se encuentre aprobado por la OGI y la Oficina de Planeación, no hay a la fecha una decisión oficial por parte de la administración donde se establezca este plan como ruta oficial de implementación de la Continuidad de Negocio (Oportunidad de Mejora No. 4).

OM5

De acuerdo con lo descrito y evidenciado para dar cumplimiento al control del punto 10.2 Implementación, se establece que a la fecha no hay decisión oficial para la implementación del plan desarrollado entre el consultor UT GLOBALTEKSECURITY - SAFEID, la OGI y la Oficina Asesora de Planeación, por lo tanto, no podrían efectuarse procedimientos de verificación, revisión y evaluación de este plan (Oportunidad de Mejora No. 5), por lo que se debe controlar el cumplimiento desde los componentes de la norma ISO27001 – 2013, los que se auditan en el marco de esta auditoria por intermedio de la verificación periódica del estado de actualización de la documentación (Procedimientos, Metodologías, Guías, Planes, Instructivos etc.) relacionada con la Continuidad del Negocio y publicada en el Sistema Integrado de Gestión – SGI; así como, del seguimiento a la planificación, ejecución, socialización y evaluación de los resultados de simulacros a las situaciones de crisis identificadas en el Plan de manejo de Crisis – PMC o en el Plan de Continuidad de Negocio – PCN con el fin de determinar la validez y efectividad, así como de la inclusión de la Continuidad de Negocio dentro de los presupuestos de la SAE

OM9	La OGI tiene el inventario actualizado de infraestructura tecnológica y de equipos de cómputo, el cual permite identificar las características técnicas, configuraciones, ubicación y propiedad; así mismo y con relación a los activos de información, se registra en el documento Matriz de Activos de Información – F-TE4-246 la caracterización del activo, donde se identifican datos como el proceso, nombre, descripción, serie, subserie, idioma, tipo de activo, ubicación, nivel de clasificación, propiedad, acceso y gestión; El etiquetado individual de cada activo de información, aun no se encuentra totalmente realizado, este etiquetado se encuentra definido de acuerdo al esquema de clasificación adoptado por la SAE (Oportunidad de Mejora No. 9).
OM12	Los documentos publicados actualmente y que pertenecen a la OGI en el Sistema Integrado de Gestión – SIG son en total 48, el documento de Caracterización de Macroproceso de Tecnología publicado en la intranet y que tiene fecha de actualización el 06/02/2018, presenta 7 (Procedimiento para dispositivos móviles, Procedimiento sobre el uso de controles Criptográficos, Procedimiento Gestión de la Continuidad del Negocio, Procedimiento de Desarrollo Seguro, Procedimiento para copias de respaldo y restauración, Procedimiento de Mantenimiento de la Infraestructura tecnológica, Procedimiento de Soporte de la Infraestructura tecnológica, Procedimiento de Monitoreo de la Infraestructura tecnológica, Procedimiento para la inteligencia de negocios, Procedimiento para la proyección, Procedimiento para la prospección) documentos que se mencionan en estado de construcción; al momento de la auditoria, se efectúa un contraste para determinar el avance en el desarrollo de los documentos en construcción y se evidencia que solo 1 (Procedimiento para copias de respaldo y restauración) ha sido desarrollado y publicado (Oportunidad de Mejora No. 12).
OM30	Gestión de Infraestructura: Inventario de Ambientes, Capacidad de Almacenamiento Bases de Datos; existen implementados ambientes separados de pruebas, preproducción, producción y desarrollo, estos se encuentran debidamente controlados para el acceso, destinados y hay identificación de roles y responsabilidades; la OGI presenta el inventario de las bases de datos por cada de uno de los ambientes en los que se encuentra ubicado, se determinan las características de cada una (Ubicación, Nombre de Servidor, Motor, Instancia, Base de Datos, Descripción, Ubicación de Archivos, Aplicaciones Soportadas, Tamaño), así mismo, este inventario debe encontrarse alineado al instructivo de Gestión de la Capacidad y al Plan descrito en el mismo, el cual determina la capacidad actual y prevista de almacenamiento, el instructivo de Gestión de Capacidad presenta como última fecha de actualización 26/05/2015, es un documento que para el periodo de la auditoria presenta más de 5 años (Oportunidad de Mejora No. 30), el cual debe mantenerse actualizado, debido a que la gestión de la capacidad es un proceso muy complejo en que todas las personas y la tecnología tienen que interactuar de forma estrecha con la planificación, supervisión y recursos de ajuste, por lo cual este documento debe reflejar la situación actual y la capacidad de almacenamiento hacia un futuro planificado, es el equilibrio entre el precio y el rendimiento con el fin de satisfacer las necesidades de los clientes

Conforme a lo anterior, se observa que a la fecha no se han mitigado las OM presentadas en el año 2019, con cierre a 31 de diciembre de 2021, lo que evidencia que no se cuenta con un avance significativo para la entidad o que las actividades propuesta en el plan no son acorde para su cumplimiento, conllevando a una posible materialización del riesgo "*No dar respuesta adecuada y oportuna a las solicitudes de asesoría y acompañamiento a la gestión de la SAE*" en cuanto a la actividad de *no documentar los planes de mejoramiento acorde a la necesidad*

Riegos Asociados:

Se podría presentar no dar respuesta adecuada y oportuna a las solicitudes de asesoría y acompañamiento a la gestión de la SAE

Recomendaciones:

Se recomienda establecer un plan de acción que pueda mitigar las OM establecidas por la OCI en el año 2019.

1. RESUMEN DE OPORTUNIDADES DE MEJORA Y OBSERVACIONES

Producto de la evaluación realizada por parte de la Oficina de Control Interno, fueron evidenciadas las siguientes oportunidades de mejora y observaciones las cuales requieren de la formulación de acciones de mejora que permitan subsanar la causa que las generó:

No	OM/OB	Oportunidad de mejora y Observaciones	Repetido
1	OM1	Procedimientos desactualizados	SI
2	OM2	Ausencia de una política de gestión de la continuidad del negocio.	NO
3	OM3	Ausencia de directrices claras que definan un marco o una ruta para gestionar el sistema de continuidad de negocio en la organización	NO
4	OM4	Ausencia de actas de reuniones de entrega y que evidencie la debida estructura de la organización en el sistema de continuidad del negocio.	NO
5	OM5	Matriz de riesgos con respecto al plan de continuidad del negocio.	NO
6	OM6	Ausencia de un debido marco de gestión como lo solicita la norma enmarcada del ciclo de gestión P-H-V-A, ISO 22301 aplicado al sistema de gestión de continuidad del negocio.	NO
7	OM7	Establecer un paso a paso detallado por funcionario, actividad y tiempo específico al ejecutar las actividades a desarrollar en el DRP	NO
8	OM8	La norma enmarca la prueba total de los escenarios, por tal razón se observa que a la fecha no se han realizado las pruebas a todos los escenarios enmarcados en el plan de continuidad del negocio	NO

9	OM9	Actualmente la organización no ha establecido intervalos de tiempo apropiados con el fin de revisar el plan de continuidad del negocio en donde asegure la disponibilidad continua, la adecuación y la efectividad. Estas revisiones deben quedar documentadas.	NO
10	OM10	La organización debe establecer un programa continuo de capacitación y entrenamiento para su plan de continuidad del negocio no solo a los funcionarios, sino en materia específica a los funcionarios encargados de articularlo.	NO
11	OM11	Los procedimientos de control de cambios deben operar efectivamente y deben ser un reflejo de su efectividad constante.	NO
12	OM12	Incluir a toda la organización en las pruebas al plan de continuidad	NO
13	OM13	Comunicar a las autoridades, clientes y proveedores externos al realizar las pruebas al DRP	NO
14	OM14	Documentar y Realizar pruebas a los backups realizados en la entidad	NO
15	OM15	Talento Humano	SI
16	OM16	Capacitación y directrices en materia de gestión de Continuidad del Negocio	NO
17	OM17	Plan De Mejoramiento Interno 2019	NO

2. CONCLUSIONES

Al evaluar la eficiencia, eficacia, efectividad y economía de la gestión del plan de continuidad del negocio de la SAE a corte 31 de octubre de 2021, se puede concluir que

- En la entidad, se puede concluir que a pesar de que la entidad trabajo con apoyo de una consultoría en la construcción del plan de continuidad del negocio en el año 2018 y que anualmente se está realizando un ejercicio simulado del DRP, a la fecha la entidad no tiene una hoja de ruta Articuladas según el Modelo integrado de planeación y gestión según la Guía de MINTIC propia y actualizada en conjunto con todas las áreas que permita articular un sistema completo de gestión de continuidad del negocio a la fecha de la auditoria.
- Con el fin de generar más valor a la entidad, referente a plan de continuidad del negocio, es importante realizar inducciones, reinducciones, capacitaciones y socializar a la alta gerencia como al interior de la Entidad.
- Realizar un análisis de las actividades que se encuentran establecidas en el plan de mejoramiento interno en cuanto al tema de continuidad del negocio del año 2019 como de su fecha de cierre, con el fin de generar un resultado eficiente y eficaz en el momento de su nueva revisión.

- Revisar en conjunto con las áreas involucradas la normatividad vigente, con el fin de ser actualizada la documentación que se encuentra publicada en la arquitectura como la faltante.
- Se debe asignar un presupuesto con el fin de poder realizar una consultoría que ayude a preparar a la entidad en materia de continuidad del negocio.
- Al evaluar la gestión de continuidad del negocio es importante anotar que se deben tener en cuenta los riesgos cibernéticos, los cuales pueden desembocar y poner en riesgo la continuidad del negocio en la entidad y los cuales se han visto abocadas muchas entidades en la presente fecha.

Cordialmente

María del Pilar Mayor Varela.
Jefe Oficina de Control Interno

Proyecto: Equipo Auditor
Aprobó: Jefe Oficina de Control Interno