Sociedad de Activos Especiales S.A.S.

El emprendimiento es de todos

Minhacienda

INFORME EJECUTIVO DE AUDITORIA DE GESTIÓN
OFICINA DE GESTION DE LA INFORMACION - OGI

AUDITOR

CARLOS ANDRES RICO REINA

FECHA DE AUDITORIA

Del 09 de agosto al 17 de septiembre de 2019

TABLA DE CONTENIDO

1 OBJETIVO 3
1.1 Objetivos Específicos 3
2 ALCANCE 3
3 EVALUACION DE CONTROLES 4
4 ANALISIS DE RIESGOS POR COMPONENTES AUDITADOS 5
4.1 Componente: Planeación Y Gestión De La Continuidad Del Negocio 5
4.2 Componente: Nivel de Accesibilidad del Portal Web SAE según Políticas de Gobierno Digital. 5
4.3 Componente: Estado de Implementación del Sistema de Gestión de la Seguridad de la Información - SGSI. 6
4.4 Componente: Estado de Implementación y Funcionalidad del Sistema de Información Matrix versión 2.0 – Misional. 7
4.5 Componente: Estado de Implementación y Funcionalidad del Sistema de Información Matrix versión 2.0 – Técnico 7
4.6 Componente: Estado de Implementación y Funcionalidad del Sistema de Información Matrix versión 2.0 – Presupuesto. 8
4.7 Componente: Pruebas de Calidad, Carga y Estrés / Mitigación de Vulnerabilidades. 9
5 ESTADO DE PERCEPCIÓN DE USUARIOS FINALES EN ÁREAS 10
6 CONCLUSIONES 10

INFORME EJECUTIVO – AUDITORÍA INTERNA

1 OBJETIVO

Evaluar la efectividad del sistema de control interno de los procedimientos relacionados a los procesos de Seguridad de la Información, Mantenimiento y Soporte de Aplicaciones y Gestión de Infraestructura según la metodología de administración de riesgos de SAE, verificando y evaluando el estado de cumplimiento de cada uno de los lineamientos definidos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones contemplados dentro del Decreto 415 del 07 de marzo del 2016 aplicado a SAE, en el cual se indica que las entidades con el liderazgo del Director de Tecnologías y Sistemas de Información, se acojan a los lineamientos que en materia de TI define el Ministerio de Tecnologías de la Información y las Comunicaciones para el fortalecimiento institucional y ejecución de los planes, programas y proyectos de tecnologías y sistemas de información, planes de gestión de la continuidad del negocio, sistema de gestión de la seguridad de la información y políticas en el marco de la estrategia de Gobierno Digital.

1.1 Objetivos Específicos

- Evaluar la gestión realizada por la Oficina de Gestión de la Información – OGI con relación a la planificación, implementación, seguimiento a los planes de continuidad de negocio, sistema de gestión de la seguridad de la información – SGSI, nivel de accesibilidad del portal Web SAE según políticas de Gobierno Digital, implementación y funcionalidad del aplicativo Matrix, pruebas de carga y estrés y mitigación de las vulnerabilidades.

- Verificar la información solicitada a la Oficina de Gestión de la Información – OGI mediante correo electrónico anticipadamente y base de la auditoria, con el fin de evaluar la gestión real de la misma.

- Verificar la efectividad en el uso del presupuesto asignado a la Oficina de Gestión de la Información – OGI, específicamente en los proyectos que involucran procesos de migración, desarrollo, implementación, mantenimiento, actualización etc., del aplicativo Matrix versión 2.0.

- Verificar el cumplimiento y medición de los indicadores de gestión establecidos por la Oficina de Gestión de la Información – OGI, frente a los procesos de seguridad de la información, soporte de aplicaciones, gestión de infraestructura tecnológica.

- Evaluar la gestión de riesgos de los procesos a auditar según la Matriz de riesgos establecida por la Entidad.

- Verificar la gestión frente a los planes de acción y/o mejora planteados por la Contraloría General de la Nación – CGN e internos.

2 ALCANCE

Efectuar procedimientos de solicitud de información y visita en campo, donde se verificara el estado de planeación y gestión de la continuidad del negocio, nivel de accesibilidad del portal web de la SAE según las políticas de Gobierno Digital y norma técnica colombiana NTC 5854, aplicación del Sistema de Gestión de la Seguridad de la Información - SGSI en el marco de la norma ISO 27001 de 2013, evaluación del proceso actual de desarrollo, implementación y funcionalidad del sistema Matrix 2.0 (vigencias 2017, 2018 y 2019) a nivel Misional, Técnico y Presupuestal, estado de las pruebas de carga, estrés y mitigación de vulnerabilidades.

3 EVALUACION DE CONTROLES

De conformidad con los resultados obtenidos, en el siguiente cuadro se presenta la metodología de evaluación de controles con sus respectivos comentarios para la adecuada comprensión y correcta implementación del plan de mejoramiento, de acuerdo con la clasificación:

Definición de Criticidad – Evaluación del Control

	**DESEMPEÑO ALTO** En los procedimientos y pruebas de gestión y cumplimiento de auditoria, se evidencia que existe un alto grado de observancia de las políticas, directrices, normas, estrategia y otros factores; ademas los controles y actividades se están ejecutando con efectividad.
	**DESEMPEÑO MEDIO** En los procedimientos y pruebas de gestión y cumplimiento de auditoria, se evidencia que existe un grado de observancia de las políticas, directrices, normas, estrategia y otro factores; ademas los controles y actividades se están ejecutando, pero presentan oportunidades de mejora para elevar la ganancia de valor en la Entidad
	**DESEMPEÑO BAJO** En los procedimientos y pruebas de gestión y cumplimiento auditoria, se evidencia que existe un bajo grado de observancia de las políticas, directrices, normas, estrategia y otro factores; ademas solo algunos controles y activiadades se están ejecutando; pero son muy vulnerables y deben ser objeto de evaluación y rediseño para generar valor en la Entidad.
	**SIN CONTROL** Actividades sin controles en los procedimientos, manuales, guias etc., para el caso de procedimientos se deben establecer controles y registros con el fin de evidenciar gestion en la actividad auditada.

De la evaluación efectuada con base a los 5 componentes objeto de la auditoria de gestión y de acuerdo con los controles identificados de origen interno y externo y los que no tienen controles especificados en los procedimientos, se obtuvo la siguiente evaluación:

Resumen del Proceso Evaluado

COMPONENTES	DESEMPEÑO ALTO	DESEMPEÑO MEDIO	DESEMPEÑO BAJO	SIN CONTROL	TOTAL COMPONENTE
PLANEACION Y GESTION DE LA CONTINUIDAD DEL NEGOCIO	N/A	1	4	0	5
NIVEL DE ACCESIBILIDAD DEL PORTAL WEB SAE SEGÚN POLITICAS DE GOBIERNO DIGITAL	N/A	1	2	0	3
ESTADO DE IMPLEMENTACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI	N/A	4	7	0	11
ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - TECNICO	N/A	4	5	2	11
ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - MISIONAL	N/A	0	0	1	1

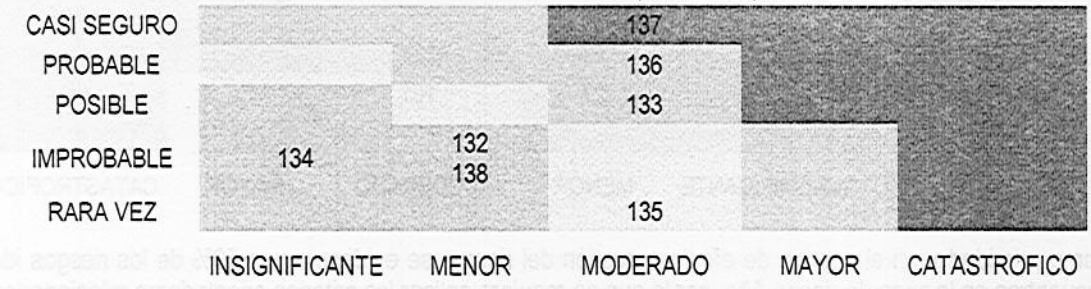
COMPONENTES	DESEMPEÑO ALTO	DESEMPEÑO MEDIO	DESEMPEÑO BAJO	SIN CONTROL	TOTAL COMPONENTE
ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - PRESUPUESTO	N/A	0	4	0	4
PRUEBAS DE CALIDAD, CARGA Y ESTRÉS / MITIGACION DE VULNERABILIDADES	N/A	0	1	0	1
TOTAL GENERAL	N/A	**10**	**23**	**3**	**36**
PROPORCIONES	N/A	**27.78%**	**63.89%**	**8.33%**	**100.00%**

La especificación de los 23 controles con desempeño bajo, oportunidades de mejora y recomendaciones, se relacionan en el anexo "OportunidadesMejora_AuditoriaOGI_OCI_2019".

4 ANALISIS DE RIESGOS POR COMPONENTES AUDITADOS

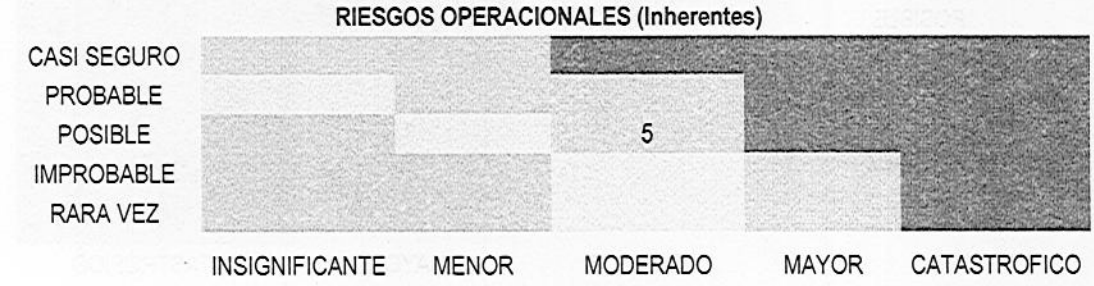
Con el fin de apoyar a la toma de decisiones, se presenta el siguiente análisis por cada componente auditado, es importante aclarar que los números mapeados corresponden al número de identificación del riesgo según el mapa de riesgos de la SAE (Operacionales, Seguridad de la Información y de Corrupción) para el año 2019:

4.1 Componente: Planeación Y Gestión De La Continuidad Del Negocio



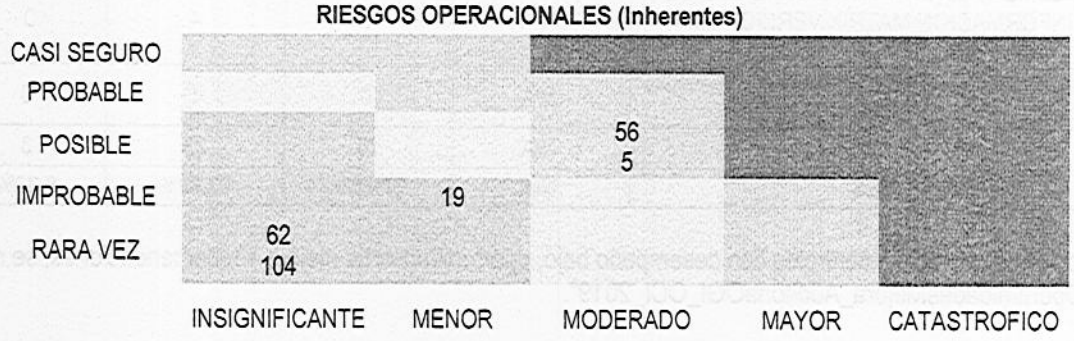
Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 42.85% de los riesgos identificados se encuentran en las zonas de riesgo Extremo y Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

4.2 Componente: Nivel de Accesibilidad del Portal Web SAE según Políticas de Gobierno Digital.

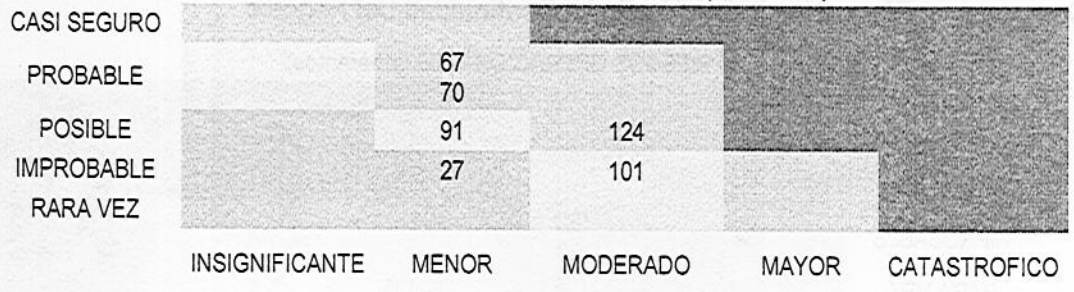


Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 100% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

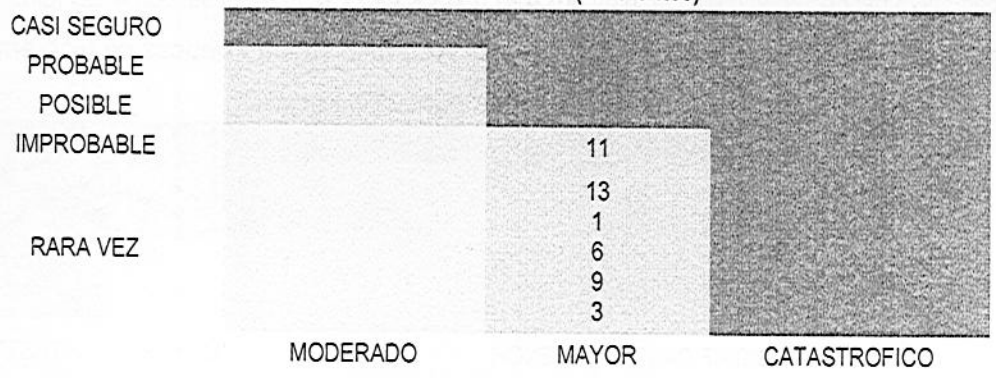
4.3 Componente: Estado de Implementación del Sistema de Gestión de la Seguridad de la Información - SGSI.



Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 40% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

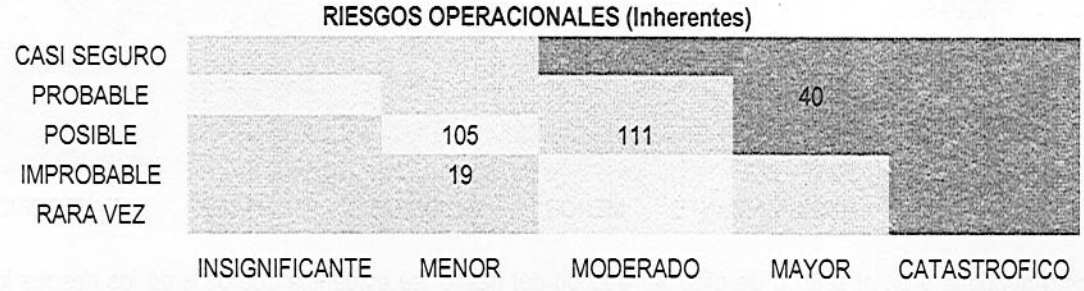


Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 50% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

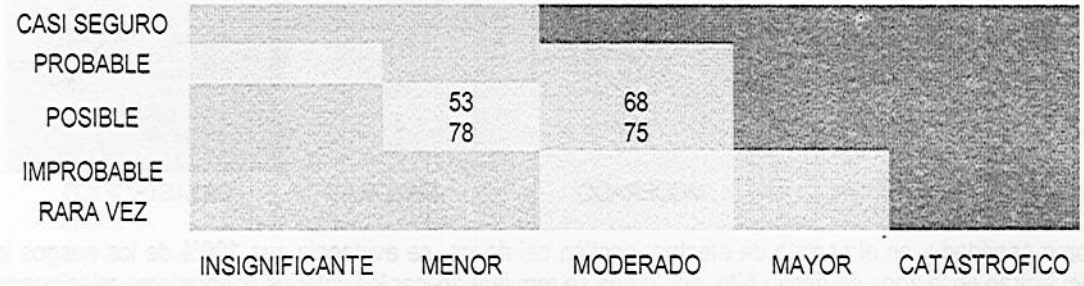


Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 100% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

4.4 Componente: Estado de Implementación y Funcionalidad del Sistema de Información Matrix versión 2.0 – Misional.

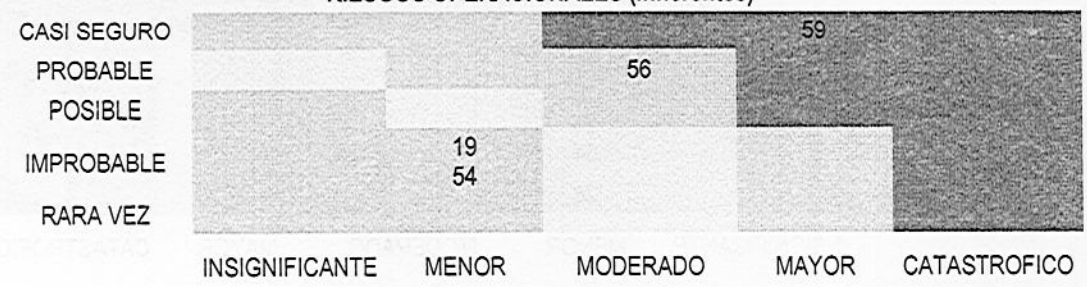


Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 50% de los riesgos identificados se encuentran en las zonas de riesgo Extremo y Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.



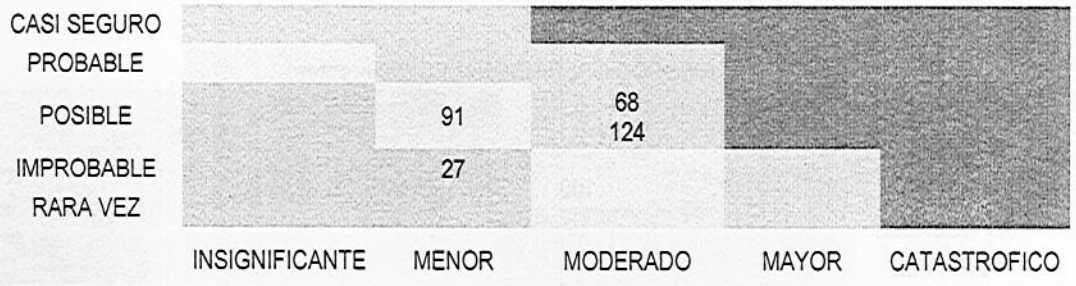
Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 50% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

4.5 Componente: Estado de Implementación y Funcionalidad del Sistema de Información Matrix versión 2.0 – Técnico.



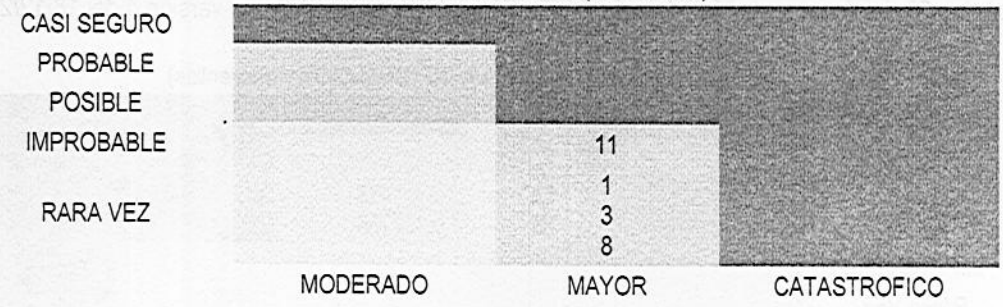
Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 50% de los riesgos identificados se encuentran en las zonas de riesgo Extremo y Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

RIESGOS SEGURIDAD DE LA INFORMACION (Inherentes)



Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 50% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

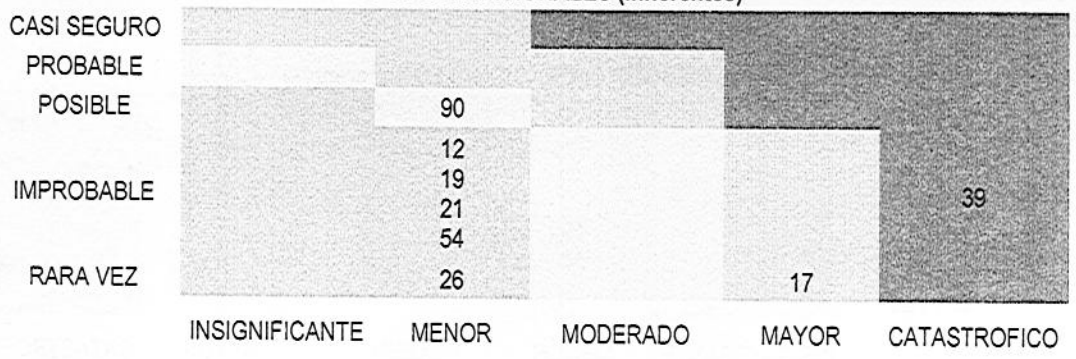
RIESGOS DE CORRUPCION (Inherentes)



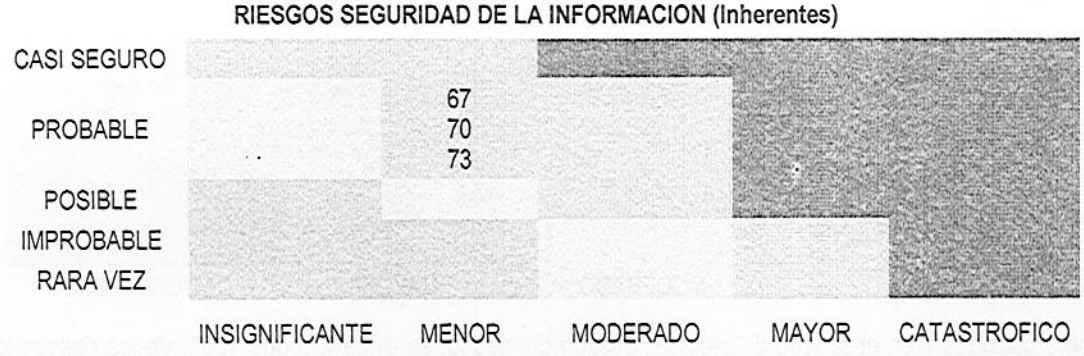
Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 100% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

4.6 Componente: Estado de Implementación y Funcionalidad del Sistema de Información Matrix versión 2.0 – Presupuesto.

RIESGOS OPERACIONALES (Inherentes)

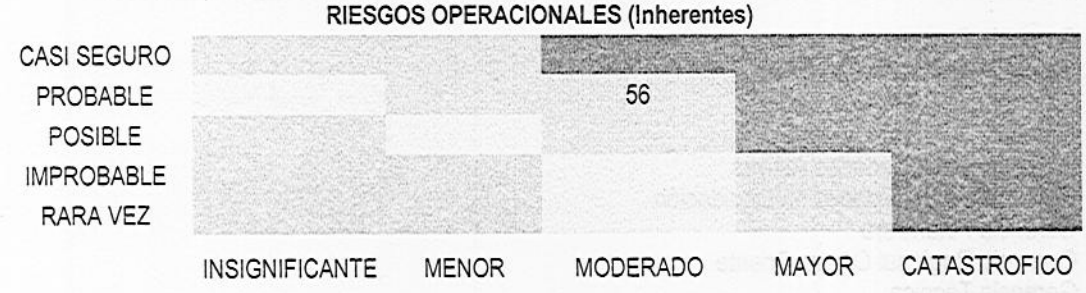


Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 25% de los riesgos identificados se encuentran en las zonas de riesgo Extremo y Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

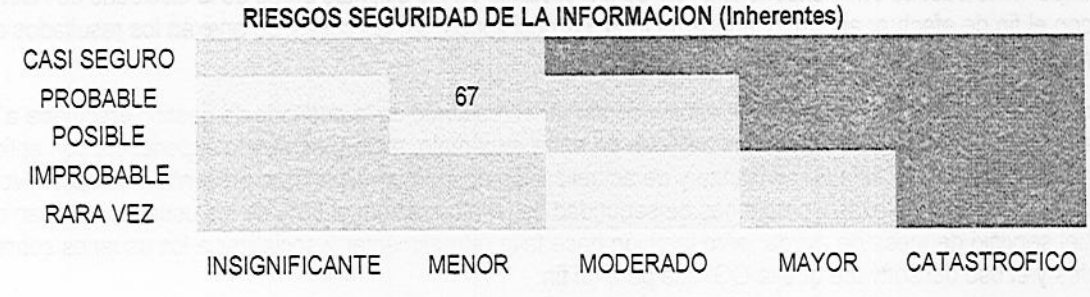


Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 100% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

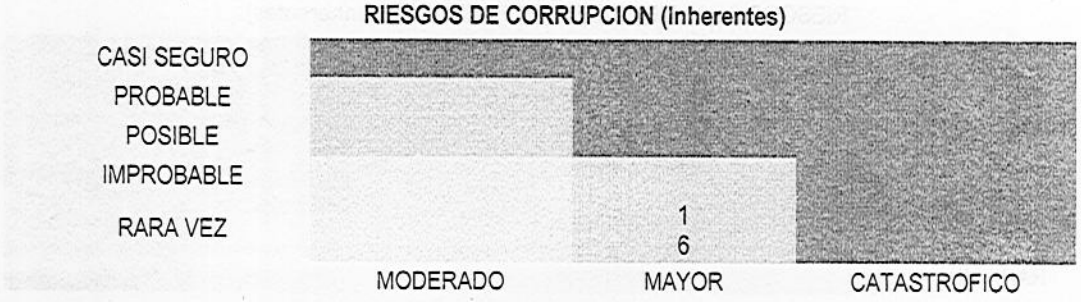
4.7 Componente: Pruebas de Calidad, Carga y Estrés / Mitigación de Vulnerabilidades.



Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 100% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.



Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 100% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.



Como prioridad y en el sentido de efectuar gestión del riesgo, se evidencia que 100% de los riesgos identificados se encuentran en la zona de riesgo Alto, por lo que se requiere aplicar los criterios orientadores relacionados en la página 25 del documento Metodología de Gestión del Riesgo G-DE2-001 versión 4 del 18/12/2018.

5 ESTADO DE PERCEPCIÓN DE USUARIOS FINALES EN ÁREAS

Como valor hacia la SAE la OCI planifico y aplico 28 encuestas a usuarios aleatorios de 9 áreas, donde como técnica de investigación del estado de opinión, se ejecutó este procedimiento en sitio para las siguientes áreas:

- Gerencia Comercial
- Gerencia de Asuntos Legales
- Gerencia de Bienes Inmuebles
- Gerencia de Bienes Muebles
- Gerencia de Sociedades Activas
- Gerencia de Sociedades en Liquidación
- Gerencia Financiera
- Gerencia Regional Centro Oriente
- Gerencia Técnica

Donde se recoge la opinión y recomendaciones de las áreas que interactúan con los distintos componentes y servicios tecnológicos como lo son la aplicación Matrix, la Mesa de Ayuda, la Seguridad de la Información y Página Web, lo anterior con el fin que la administración, la Oficina de Control Interno - OCI y la Oficina de Gestión de la Información - OGI tengan un insumo importante basado en la experiencia real de los usuarios en las distintas áreas de la Sociedad de Activos Especiales – SAE, con el fin de efectuar análisis y apoyar la toma de decisiones; así las cosas, se anexan los resultados de la encuesta anteriormente mencionada.

Por último, los resultados permitieron contrastar y confirmar el resultado de la auditoria de gestión efectuada a la OGI, donde a grandes rasgos, el 60 % de los usuarios califican de entre muy malo, malo y regular la experiencia con aplicativo Matrix y se indicaron problemas de falta de confianza y de actualización en la información que presenta este aplicativo; por otro lado se confirman algunas fortalezas y problemas de seguridad de la información; el 53% de los usuarios califican como buena la gestión del servicio de mesa de ayuda, pero también hace falta retroalimentar y socializar a los usuarios sobre la gestión de los tiquetes y el uso del software que la OGI usa para tal fin.

6 CONCLUSIONES

El equipo auditor considera que el Sistema de Control Interno continua en proceso de mejoramiento teniendo en cuenta los siguientes aspectos:

6.1 En lo que respecta a la Planeación y Gestión de la Continuidad del Negocio, la Oficina de Gestión de la Información – OGI inicio en el año 2018 un proceso vital para la Sociedad de Activos Especiales – SAE, el cual corresponde a la

definición del alcance tecnológico, planificación de actividades, actualización y construcción de documentación, todo esto dentro de un marco que estable la guía para que la OGI se encuentre preparada para responder adecuadamente ante una eventualidad (Crisis, Evento Catastrófico, Incidente, Desastre, Emergencia); al final del ejercicio auditor, se establece que la OGI aún no se encuentra preparada, dejo de documentar y de planificar actividades tan importantes como lo son los simulacro y la actualización de los BIA, para el año 2019 no se evidencio avance al respecto, por lo que se debe hacer seguimiento con mayor frecuencia a todas las actividades en las que la OGI se encuentra relacionado en el proceso de Continuidad del Negocio de la SAE; así mismo, es importante extender el seguimiento a las demás áreas responsables.

6.2 La política de Gobierno Digital enmarcada en el Decreto 1008 de 2018, estableció lineamientos de accesibilidad para las páginas web de entidades a las que les aplica la norma anteriormente mencionada, en lo que respecta a la SAE y como resultado del análisis del cumplimiento de la Norma Técnica Colombiana - NTC 5854 de accesibilidad web, ejecutado durante el periodo de auditoria, se estableció el incumplimiento técnico de la página web de la entidad, resultado de esto y como consecuencia, se evidencio la falta de controles durante y al momento de la entrega del producto por parte del contratista y otra serie de errores como la falta de documentación en la supervisión del contrato; por lo anterior es necesario ejercer más control sobre las actividades que ejecutan los contratistas y definir mecanismos de verificación normativa y técnica, así mismo, crear controles de calidad de los productos; para todo esto es necesario que las áreas técnicas y la Oficina Asesora de Planeación establezcan los aspectos anteriormente mencionados.

6.3 Por otro lado, es importante el avance de la SAE en el cumplimiento y desempeño de la mayoría de los componentes de la política de Gobierno Digital reportados a través del Formulario Único Reporte de Avances de la Gestión - FURAG en al año 2018, sin embargo es importante seguir trabajando para mejorar los indicadores en lo que respecta a los Tramites y Servicios en Línea y Parcialmente en Línea el cual se encuentra por debajo del promedio nacional, para esto es necesario que la OGI y las demás áreas se reúnan y se determine la posibilidad de ampliar el catálogo de servicios en línea.

6.4 El Sistema de Gestión y de Seguridad de la Información – SGSI es el elemento más importante de la Norma ISO/IEC 27001, canon que se encuentra definido como modelo de operación en el documento de Caracterización Macroproceso de Tecnología C-TE-002 Versión 3 del 06/02/2018; el SGSI se basa en 3 principios básicos (Confidencialidad, Integridad y Disponibilidad), durante el periodo de auditoria de gestión, se evidenciaron fallas que comprometen el cumplimiento de algunos de estos principios y en otros casos atenta contra todo el SGSI de la SAE, como lo son la falta de bloqueos automáticos de sesión, actualización y creación de procedimientos, guayas de seguridad en equipos con mayor riesgo de pérdida o robo, planificación de mantenimientos para la infraestructura tecnológica, protección adicional en correos electrónicos confidenciales y clasificados, notificación a la Oficina de Control Interno – OCI sobre incidentes de seguridad de la información, actualización en licenciamiento de software, tratamiento y protección de datos personales, supervisión y gestión de proveedores; así las cosas, es vital y critico establecer planes de acción y de mejoramiento de estricto cumplimiento para fortalecer el SGSI de la SAE con el fin de minimizar los riesgos relacionados con la seguridad de la información y teniendo en cuenta que la información misional presenta altos niveles de confidencialidad y que no hay confianza en lo que presentan los sistemas de información.

6.5 Durante varios años la SAE ha incorporado en los Planes Estratégicos, objetivos, iniciativas y acciones encaminadas a que la entidad consolide la implementación de un sistema de información con criterios de seguridad, integridad, calidad y cumplimiento ajustados a los procesos del negocio y donde una de las acciones es "Gestionar el Proyecto Matrix 2.0"; el cual como todo sistema de información se encuentra compuesto por elementos como lo son datos, actividades, recursos y personas con el fin de apoyar la operación misional y cumplir con los objetivos de la SAE; durante el periodo de auditoria se evidencio que hay problemas en algunos de sus componentes, como lo es el cumplimiento de las propiedades de la información (Oportunidad, Integridad, Veracidad, Calidad, Disponibilidad), a nivel documental hay procedimientos sin documentación, en etapa de construcción y desactualizados (Gestión de Bases de Datos, Pruebas, Requerimientos, Gestión de Capacidad), procedimientos que no se ejecutan de acuerdo a lo estipulado como lo es la Gestión de Usuarios y Accesos a sistemas de información, bases de datos y otros servicios; por otro lado y a nivel administrativo, se evidencian problemas de planificación, distribución y ejecución del presupuesto

asignado al proyecto de Matrix 2.0, no se evidencian mecanismos de priorización y efectividad entre los recursos invertidos y los resultados, razón por la cual no se ha cumplido con los objetivos de los Planes Estratégicos.

Cordialmente,

María del Pilar Mayor Varela.
Jefe Oficina de Control Interno

Elaboró: Carlos Andres Reina – Prof. II OCI.
Anexos: Anexo "OportunidadesMejora_AuditoriaOGI_OCI_2019" en (8) paginas

COMPONENTE : PLANEACION Y GESTION DE LA CONTINUIDAD DEL NEGOCIO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
1	Manual de Continuidad del Negocio M-DE2-040 Versión 1 - 27/09/2018 4. Declaración de la Política de Continuidad de Negocio 5 6. Ejercicios y Pruebas 6. Normatividad Plan De Manejo De Crisis L-DE2-004 Versión 1 - 22/10/2018 4. ¿Qué conceptos claves debo tener claros en el Plan? 5. ¿Qué políticas debo conocer? 8. ¿Cómo ejecuto el Plan?	No cuenta con controles establecidos		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	1. Oficializar y Socializar el Plan de Recuperacion de Desastres - DRP, es un documento clave dentro del Plan de Manejo de Crisis Riesgo Alto ante una eventualidad (Crisis, Evento Catastrófico, Incidente, Desastre, Emergencia) el Comité de Crisis y el Líder de Continuidad de Negocio no tendrían un procedimiento oficial, aprobado y publicado en el SIG para ser activado como lo es el DRP en lo que respecta a las actividades que debe ejecutar la OGI para la recuperación y restauración de los servicios tecnológicos de la SAE. Riesgo Relacionado: Riesgo Operacional No. 132 a 138 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019
	Norma ISO/IEC 27001:2013 A17.1.1. Planificacion de la Continuidad de la Seguridad de la Informacion	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.			
	Norma ISO/IEC 27001:2013 A17.1.2. Implementacion de la Continuidad de la Seguridad de la Informacion	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa			

COMPONENTE : PLANEACION Y GESTION DE LA CONTINUIDAD DEL NEGOCIO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
2	Plan Maestro De Simulacro L-DE2-007 Versión 1 – 11/02/2019 8.2.6. Sistemas y Servicios de TI Requeridos 8.2.7. Planes de continuidad a probar 8.2.8. Riesgos del Negocio Asociados a la Realización del Simulacro 8.2.11. Riesgos Del Simulacro	Plan Maestro De Simulacro 2. ¿Cual es la aplicación del Plan?		Para el año 2019 y proximos años, no se han planificado de forma oficial más simulacros a otras situaciones de crisis identificadas en el Plan de manejo de Crisis – PMC o en el Plan de Continuidad de Negocio – PCN.	1. Planificar y Ejecutar con las areas relacionadas todos lo simulacros requeridos segun las situaciones de crisis identificadas en el Plan de Manejo de Crisis, unicamente hay un 10% aproximado de ejecucion Riesgo Alto: No conocer los procedimientos tecnologicos y de reaccion ante una eventualidad (Crisis, Evento Catastrófico, Incidente, Desastre, Emergencia), impide la pronta recuperacion y la continuidad de las operaciones del negocio Riesgo Relacionado: Riesgo Operacional No. 132 a 138 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019
	Norma ISO/IEC 27001:2013 A17.1.1. Planificacion de la Continuidad de la Seguridad de la Informacion	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.			
	Norma ISO/IEC 27001:2013 A17.1.2. Implementacion de la Continuidad de la Seguridad de la Informacion	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa			

COMPONENTE : PLANEACION Y GESTION DE LA CONTINUIDAD DEL NEGOCIO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
3	Manual de Continuidad del Negocio M-DE2-043 Versión 1 - 27/06/2018 Plan De Manejo De Crisis L-DE2-004 Versión 1 - 22/10/2018 Norma ISO/IEC 27001:2013 A17.1.1 Planificacion de la Continuidad de la Seguridad de la Informacion	No cuenta con controles establecidos La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre		No hay a la fecha una decisión oficial por parte de la administración donde se establezca el Plan presentado por la OGI como ruta oficial de implementación de la Continuidad de Negocio, así como de la inclusión de la Continuidad de Negocio dentro de los presupuestos de la SAE	1. Aprobar el Plan de Implementacion de Continuidad de Negocio 2. Incluir la Continuidad del Negocio dentro de las Lineas Presupuestales anuales de la SAE Riesgo Alto: No contar con un Plan de Continuidad de Negocio Implementado y con recursos exclusivos dentro del presupesto de la SAE, pone al alto riesgo las operaciones de la entidad, ante una eventualidad (Crisis, Evento Catastrófico, Incidente, Desastre, Emergencia) Riesgo Relacionado: Riesgo Operacional No. 132 a 138 Maça de Riesgos Operacionales 2019 F-DE2-274 Version 2 16/05/2019
	Norma ISO/IEC 27001:2013 A17.1.2 Implementacion de la Continuidad de la Seguridad de la Informacion	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa			

COMPONENTE : PLANEACION Y GESTION DE LA CONTINUIDAD DEL NEGOCIO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
4	Manual de Continuidad del Negocio M-DE2-043 Versión 1 - 27/06/2018 Plan De Manejo De Crisis L-DE2-004 Versión 1 - 22/10/2018 Norma ISO/IEC 27001:2013 A17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No cuenta con controles establecidos La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas		A la fecha no hay decisión oficial para la implementación del plan desarrollado entre el consultor UT GLOBALTEK SECURITY - SAFE ID, la OGI y la Oficina Asesora de Planeación, por lo tanto no podrían efectuarse procedimientos de verificación, revisión y evaluación de este plan,	1. Diseñar los controles de continuidad de seguridad de la información 2 Probar y Evaluar la efectividad de los controles Riesgo Alto: No contar con un Plan oficial de Implementacion de Continuidad de Negocio a corto, mediano y largo plazo, pone en un riesgo muy alto las operaciones de la SAE ante ante una eventualidad (Crisis, Evento Catastófico, Incidente, Desastre, Emergencia), debido a que no hay fortalecimiento en el nivel de preparacion para afrontar estas situaciones, asi mismo, no es posible efectuar, verificaciones, revisiones para determinar la efectividad del mismo plan. Riesgo Relacionado: Riesgo Operacional No. 132 a 138 Maça de Riesgos Operacionales 2019 F-DE2-274 Version 2 16/05/2019

COMPONENTE : NIVEL DE ACCESIBILIDAD DEL PORTAL WEB SAE SEGUN POLITICAS DE GOBIERNO DIGITAL					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
5	Norma Tecnica Colombiana - NTC 5854 de 2011 Lineamiento LI SIS 24 en el marco de la política de Gobierno Digital - Decreto 1078 de 2015	Establecer los requisitos de accesibilidad que son aplicables a la página Web de la Sociedad de Activos Especiales - SAE, que se presentan agrupados en tres niveles de conformidad A, AA, y AAA, lo anterior en el marco de la política de Gobierno Digital		En total para la página Web https://www.saesas.gov.co/ se presentan 17 problemas, 435 advertencias y 56 eventos que se deben verificar de forma manual, lo anterior evidencia posible incumplimiento técnico de los requisitos de accesibilidad según Norma Tecnica Colombiana – NTC 5854	1. Efectuar prueba de accesibilidad a través de la pagina https://www.tawdis.net/ 2. Hacer entrega de los resultados de la prueba al contratista Micrositios para efectue los ajustes de acuerdo al objeto del contrato No. 002 de 2018. Riesgo Alto: No cumplir con lo incluido por la NTC 5854 de 2011, implica falta de cumplimiento normativo aplicable a la SAE, de acuerdo a la Naturaleza Jurídica. Riesgo Relacionado: Riesgo Operacional No. 5 Maça de Riesgos Operacionales 2019 F-DE2-274 Version 2 16/05/2019

COMPONENTE : NIVEL DE ACCESIBILIDAD DEL PORTAL WEB SAE SEGÚN POLITICAS DE GOBIERNO DIGITAL					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
6	P-ES3-027 Procedimiento de Supervisión o Interventoria y Liquidacion de Contratos 9. Controlar el avance del contrato 12. Elaborar Informes de Ejecucion 20. Recibir todos los servicios, obras, bienes y/o elementos entregados por el contratista Ley 1712 de 2014	Controlar el avance del contrato con base al cronograma de ejecucion aprobado y recomendar ajustes necesarios cada vez que sea requerido Archivar documento en carpeta de supervision y publicar informe de ejecucion en la pagina web da SAE Verificar que la cantidad y calidad de los mismos este de acorde con lo exigido en los estudios y documentos previos al contrato, terminos de referencia y contrato		Durante la auditoria se entrega un solo Informe de Ejecución de Contratos con fecha 29 de mayo de 2018 donde se relaciona un avance del 50% de ejecución y avances, donde en las obligaciones cumplidas por el contratista No se presentó evidencia (Listados de Asistencia Reuniones e Informes de Ejecución de Contratos) de un procedimiento de verificación detallada (soporte para la supervisión del contrato) para cada uno de los requisitos técnicos para determinar el alcance de la OGI y del contratista No se evidencia en ningún momento un mecanismo manual o automático de control hacia el proveedor Morositos S.A.S., donde se verifique el cumplimiento en la implementación en la página Web de SAE de los requisitos de accesibilidad según Norma Técnica Colombiana – NTC 5854 durante la ejecución del contrato y a la entrega de la página web	1. Se recomienda que cada area defina mecanismos de control y verificacion detallados durante la ejecucion y a la entrega de productos 2. Se recomienda publicar la documentacion soporte de los contratos con el fin de cumplir con la Normatividad relacionada Riesgo Alto. No contar con mecanismos de verificacion dentro de las areas con el fin de controlar los contratos durante la ejecucion y al final al momento que el contratista hace entrega de los productos objeto del contrato, todo genera un riesgo alto de incumplimiento contractual, asi mismo, no llevar el control de los documentos soportes de cada contrato ni publicarlos en los portales web definidos para tal fin. Riesgo Alto Incumplimiento Normativo Ley de Transparencia y del Derecho de Acceso a la Información Publica Nacional Riesgo Relacionado. No hay ninguno que estipule incumplimiento normativo en los Mapas de Riesgo Operacional, Corrupcion y Operativo Riesgo Relacionado. Riesgo Operacional No. 19 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
7	Norma ISO/IEC 27001:2013 A.11.2.1 Ubicación y Proteccion de los Equipos	Los equipos deben estar ubicados y protegidos para reducir el riesgos de amenaza y peligros del entorno, y las posibilidades de acceso no autorizado		En áreas como lo son atencion al usuario, recepciones y oficinas donde se atienda a personal visitante, es donde se presentan riesgos mayores de seguridad de equipos, a pesar de existir procedimientos de seguridad para visitantes, es necesario que existan controles adicionales como lo son el aseguramiento de equipos con guayas de seguridad y reforzar con campañas de seguridad de equipos personales como lo son telefonos celulares, por otro lado, ante una eventualidad como lo es el robo de un equipo y la aplicación de los procedimientos de reclamación ante aseguradores (afectación de la póliza), es posible que el asegurador en su proceso de verificación de los hechos, determine que los protocolos de la Sociedad de Activos Especiales - SAE no son suficientes y no surta efecto la reclamación, por ende sea la SAE quien asuma esa perdida, tipificándose un posible detrimento patrimonial.	1. Se recomienda instalar guayas de seguridad para equipos portatiles y en equipos de computo de areas con acceso publico como lo son atencion al usuario, recepciones etc Riesgo Alto. Se podria presentar riesgo de perdida de informacion y de equipos en areas de acceso publico, por no tener medidas adicionales de seguridad, asi mismo, podria presentarse perdidas economicas por el valor de los equipos Riesgo Relacionado. Riesgo de Corrupcion No. 13 Mapa de Riesgos de Corrupcion F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado. Riesgo de Seguridad de la Informacion No. 27, 91, 124 Mapa de Riesgos de Seguridad de la Informacion 2019 F-DE2-318 Version 1 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
8	Norma ISO/IEC 27001:2013 A.11.2.8 Equipos de Usuario Desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada		Se efectuó prueba en la Gerencia Técnica el dia 04/09/2019 a las 4:40 pm, donde en medio de una actividad grupal todos los funcionarios de esta área se desplazaron hacia otra parte del piso 3 y se dejaron sesiones abiertas aproximadamente en 10 equipos de cómputo, después de 5 minutos no se ejecutó el control de bloqueo automático	1. Se recomienda verificar el cumplimiento de las políticas de bloqueo automatico, teniendo en cuenta la informacion importante que se maneja en la SAE. 2. Se recomienda efectuar campañas continuas de concientización del riesgo de dejar informacion física y magnética a la vista y/o alcance de otras personas (internas o externas), las campañas no se deben limitar al envio de mensajes por el correo electrónico, se debe efectuar visitas y auditorías a las áreas Riesgo Alto. No tener activos protocolos de seguridad y de bloqueo de sesiones de usuario, es un riesgo alto tener visible informacion confidencial e importante que maneja la SAE. Riesgo Relacionado. Riesgo de Seguridad de la Informacion No. 27, 91, 124 Mapa de Riesgos de Seguridad de la Informacion 2019 F-DE2-318 Version 1 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
9	Norma ISO/IEC 27001:2013 A.15.2.1 Seguimiento y Revision de los Servicios de los Proveedores P-BS3-027 Procedimiento de Supervisión o Interventoria y Liquidación de Contratos 12. Elaborar Informes de Ejecucion Ley 1712 de 2014	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de los servicios de los proveedores Archivar documento en carpeta de supervision y publicar informe de ejecucion en la pagina web de SAE		Al verificar la obligacion de publicar los informes de gestion contractual en la pagina web de la SAE, unicamente se encontraron informes de los contratos (Gestion de Seguridad Electronica - Contrato 041, Computel System - Contrato 057 y Digital Ware - Contrato 036) todos del año 2018, en lo que respecta al año 2019 no hay informes publicados	1. Se recomienda publicar toda la informacion correspondiente a la supervision de los contratos a cargo de la OGI. Riesgo Alto: Incumplimiento Normativo Ley de Transparencia y del Derecho de Acceso a la Información Publica Nacional. Riesgo Relacionado: Riesgo de Corrupcion No. 9 Mapa de Riesgos de Corrupcion 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo Operacional No. 5 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
10	Manual Política de Seguridad y Privacidad de la Información M-TE4-038 Version 2 05/09/2018 Política para el Reporte y Tratamiento de Incidentes de Seguridad Norma ISO/IEC 27001:2013 A.16.1.2 Reporte de Eventos de Seguridad de la Informacion Norma ISO/IEC 27001:2013 A16.1.3 Reporte de Debilidades de Seguridad de la Informacion	Los propietarios de los activos de información deben informar a la Oficina de Control Interno - OCI, los incidentes de seguridad que les haya sido reportados Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios		A la fecha de la auditoria no existen reportes hacia la OCI de ningún tipo de eventos, incidentes o debilidades de seguridad de la informacion.	1. Se debe informar a todos los usuarios (internos u externos) que deben copiar a OCI todos los eventos, incidentes o debilidades de seguridad de la informacion notificados a la OGI a través de cualquier medio. Riesgo Alto: No informar a la Oficina de Control Interno los todos los eventos, incidentes o debilidades de seguridad de la informacion, como parte del rol de control y de seguimiento a las areas de la SAE. Riesgo Relacionado: No hay ninguno que estipule la omision de reporte a la OCI en los Mapas de Riesgo Operacional, Corrupcion y Operativo

COMPONENTE : ESTADO DE IMPLEMENTACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
11	Norma ISO/IEC 27001:2013 A.15.2.1 Seguimiento y Revision de los Servicios de los Proveedores P-BS3-027 Procedimiento de Supervision o Interventoria y Liquidación de Contratos 9. Controlar el avance del contrato	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de los servicios de los proveedores Controlar el avance del contrato con base al cronograma de ejecucion aprobado y recomendar ajustes necesarios cada vez que sea requerido		Se evidencian oportunidades en la atención muy altas, se presentan incumplimientos en los Acuerdos de Niveles de Servicios - ANS según lo estipulado en el Contrato No. 029-2014, hay porcentajes muy altos de incidentes categorizados como "Falta de Aplicación" (97% incidentes relacionados con Matriz), con relacion a la validación y valoración por parte del usuario, insumo importante para la mejora constante del servicio de mesa de ayuda, se evidencia que el software de gestión que apoya el servicio no tiene parametrizado para que las solicitudes o incidentes estén sujetos a validación por parte de usuario, asi mismo, no se encuentra habilitada la opción de valoración del mismo, por lo tanto, no hay conocimiento desde la perspectiva del usuario sobre la calidad y efectividad del servicio prestado por el proveedor de Mesa de Ayuda.	1. SE recomienda validar la informacion de los informes de gestion de la mesa de ayuda contra los ANS y ajustar procedimientos donde se evidencian fallas. Riesgo Alto: Oportunidades muy altas en la atencion de tiquetes por parte de la Mesa de Ayuda por el posible incumplimiento de los ANS del contrato 029-2014. Riesgo Relacionado: Riesgo Operacional No. 19 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 3 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
12	Norma ISO/IEC 27001:2013 A.18.1.2 Derechos de Propiedad Intelectual Decision Andina 351 de 1993 Ley 599 de 2000 Ley 603 de 2000	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados		Durante el periodo de auditoria se evidenciaron varios equipos de computo con licenciamiento sin activación como lo son Sistemas Operativos Windows, es el caso de varios equipos de cómputo ubicados en la Gerencia Técnica (Ver Informe)	1. Se recomienda verificar el estado del licenciamiento del software, activar y/o renovar las licencias vencidas. Riesgo Alto: Incumplimiento Normativo y Posibilidad de Sanciones por parte de entes de control. Riesgo Alto: Los equipos con licencias sin activacion son reconocidas como no originales y no cuentan con el soporte del proveedor, por lo que existe riesgo de perdida de informacion y de seguridad. Riesgo Relacionado: Riesgo Operacional No. 104 Mapa de Riesgo Operacionales 2019 F-DE2-274 Version 3 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION SGSI					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
13	Norma ISO/IEC 27001:2013 A.18.1.4 Privacidad y Protección de Información de Datos Personales Ley 1581 de 2012	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.		El actual formulario del Sistema para el Registro de Peticiones, Quejas o Reclamos no informa al usuario el Marco Normativo relativo al Régimen General de Protección de Datos, ni solicita la autorización para el Manejo de datos Personales	1. Se recomienda implementar avisos y solicitar la autorizacion para el tratamiento de datos, asi como, explicar el uso dado a los mismos. Riesgo Alto: Incumplimiento Normativo y Posibilidad de Sanciones por parte de entes de control. Riesgo Alto: El no tratamiento de los datos personales de todos los usuarios. Riesgo Relacionado: Riesgo de Corrupcion No. 1, 3, 9, 11 Mapa de Riesgos de Corrupcion 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo Operacional No. 5, 19 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo de Seguridad de la Informacion No. 27, 101, 124 Mapa de Riesgos de Seguridad de la Informacion 2019 F-DE2-318 Version 1 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - TECNICO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
14	Política de Gobierno Digital - Decreto 1078 de 2015 Guía Técnica "G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI" del Ministerio de las Tecnologías de la Información y Comunicaciones - MnTIC Gestion de Software	El Plan Estratégico de las Tecnologías de la Información y Comunicaciones – PETI es el artefacto que se utiliza para expresar la Estrategia de TI, hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI. Cada vez que la SAE hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI		La aplicación Matrix se encuentra desarrollada bajo el lenguaje de programación Microsoft Visual Studio Professional 2017 C# .Net Framework 4.6 , información que no se encuentra disponible en el Plan Estratégico de Tecnologías de la Información – PETI (PETI v1 v-001.pdf), documento que se encuentra en construcción, de acuerdo a lo informado por la Oficina de Gestión de la Información - OGI a la Oficina de Control Interno – OCI mediante correo electrónico el día 10 de julio de 2019 La SAE actualmente no tiene de forma oficial un documento que defina la estrategia bajo la cual se espera que las Tecnologías de la Información se integren con la Misión, Visión y los Objetivos Estratégicos, incumpliendo con la normatividad relacionada a la Política de Gobierno Digital aplicable a la SAE.	1. Se recomienda terminar, oficializar y comunicar el Plan Estrategico de Tecnologías de la Informacion - PETI. 2. Se recomienda que el PETI se ajuste de acuerdo a la Guia Tecnica del MnTIC Riesgo Alto: No contar con un documento que defina la estrategia bajo la cual se espera que las Tecnologías de la Información se integren con la Misión, Visión y los Objetivos Estratégicos de la SAE. Riesgo Alto: Incumplimiento Normativo Riesgo Relacionado: Riesgo Operacional No. 21, 26, 39, 56, 57, 62, 72,133 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo de Seguridad de la Informacion No. 20, 67, 70, 73 Mapa de Riesgos de Seguridad de la Informacion 2019 F-DE2-318 Version 1 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - TECNICO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
15	Norma ISO/IEC 27001:2013 A.12.1.1 Procedimientos de Operación Documentados Documentacion	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan		Actualmente en la OGI no existe documentación como lo son los procedimientos de pruebas de software, casos de uso, liberaciones, etc	1. Se recomienda construir y comunicar el procedimiento, para que sea fuente de información y soporte del proceso Riesgo Alto. No tener un procedimiento oficial que sea fuente de consulta para los usuarios, al momento de ejecutar los distintos tipos de pruebas que se hacen a nivel de software, redes etc Riesgo Relacionado: Riesgo de Corrupcion No. 1 Mapa de Riesgos de Corrupcion 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo Operacional No. 19, 56 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - TECNICO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
16	Norma ISO/IEC 27001:2013 A.12.1.1 Procedimientos de Operación Documentados Documentacion	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan		No existen procedimientos para el levantamiento y especificación de requerimientos funcionales y no funcionales	1. Se recomienda construir y comunicar el procedimiento, para que sea fuente de información y soporte del proceso Riesgo Alto. No tener un procedimiento oficial que sea fuente de consulta para los usuarios, al momento que los profesionales efectuen el levantamiento o especificacion de requerimientos Riesgo Relacionado: Riesgo de Corrupcion No. 1 Mapa de Riesgos de Corrupcion 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo Operacional No. 19, 56 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - TECNICO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
17	Norma ISO/IEC 27001:2013 A.9.2 Gestion de Acceso de Usuarios Gestion de Accesos	Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a sistemas y servicios		Se registran grandes cantidades usuarios con roles roles como lo son "db_owner", "db_datawriter" y "db_ddladmin" tienen permisos para efectuar rutinas de configuración, mantenimiento, agregar, eliminar o cambiar datos, agregar o eliminar accesos, así como de definicion de estructuras, procedimientos o funciones de las bases de datos	1. Se recomienda verificar el estado actual de los usuarios con estos roles, es importante aplicar el ciclo de vida para el caso de usuarios activos de funcionarios desvinculados Riesgo Alto. No asegurar el acceso a los sistemas y servicios tecnologicos Riesgo Alto. Posible fuga de informacion Riesgo Relacionado: Riesgo de Corrupcion No. 1, 3, 8, 11 Mapa de Riesgos de Corrupcion 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo Relacional No. 19, 56 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo de Seguridad de la Informacion No. 27, 68, 91, 124 Mapa de Riesgos de Seguridad de la Informacion 2019 F-DE2-318 Version 1 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - TECNICO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
18	Procedimiento Administracion y Control de Acceso a Usuarios en la Plataforma Tecnologica P-TE4-094 Version 5 del 21/05/2018 Gestion de Accesos	El usuario se creará con la siguiente estructura: primera inicial del nombre y el primer apellido, en caso de repetirse el usuario se tomará la primera y segunda letra del nombre y el primer apellido. En su defecto, en caso de repetirse con alguna de las dos opciones anteriores, se tomará la primera letra del primer y segundo nombre y el primer apellido		La base entregada por la OGI "Usuarios Matrix 15 Activos.xlsx" presenta 5 registros de usuarios activos en matrix 15 con inconsistencias en los nombres y 3 usuarios con nombre de administrador y robot.	1. Se recomienda verificar los usuarios que no cumplen con las reglas para la creacion de usuarios para el acceso a sistemas y servicios Riesgo Alto: No aplicar los procedimientos en la creacion de usuarios es un riesgo alto de seguridad de la informacion. Riesgo Relacionado: Riesgo de Corrupcion No. 1, 3, 8, 11 Mapa de Riesgos de Corrupcion 2019 F-DE2-274 Version 2 16/05/2019 Riesgo Relacionado: Riesgo Relacional No. 19, 56 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 16/05/2019 Riesgo Relacionado: Riesgo de Seguridad de la Informacion No. 27, 68, 91, 124 Mapa de Riesgos de Seguridad de la Informacion 2019 F-DE2-318 Version 1 16/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - PRESUPUESTO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
19	Procedimiento Elaboracion y Actualizacion del Presupuesto P-GF1-015 Version 1 del 02/03/2015 Formato Anteproyecto Presupuestal F-GF1-031 Version 2 del 03/06/2015 Decreto 115 de 1996 IV De la Ejecucion del Presupuestos Articulo 28 Ejecucion Presupuestal	El Consejo Superior de Política Fiscal, Confis, o quien éste delegue podrá suspender, reducir o modificar el presupuesto cuando la Dirección General del Presupuesto Nacional estime que los recaudos del año pueden ser inferiores al total de los gastos presupuestados, o cuando no se perfeccionen los recursos del crédito, o cuando la coherencia macroeconómica así lo exija, o cuando el Departamento Nacional de Planeación lo determine, de acuerdo con los niveles de ejecución de la inversión.		Las vigencias de los años 2017 (66.7%) y 2018 (44.7%) muestran una baja ejecución presupuestal, lo que se ve reflejado en la efectividad de la inversión de recursos contra los resultados y el avance en los proyectos relacionados a la aplicación Matrix	1. Se recomienda ejecutar los presupuestos de acuerdo a lo planificado Riesgo Alto: No ejecutar los recursos del presupuesto de acuerdo a las lineas definidas para tal fin, pone en riesgo el cumplimiento de los proyectos Riesgo Alto: La disposicion tardia de los recursos del presupuesto hacia las areas, genera que algunas lineas no puedan ser ejecutadas y que los proyectos y/o servicios no puedan desarrollarse durante la vigencia Riesgo Alto: recorte presupuestal Riesgo Relacionado: Riesgo Operacional No. 12, 17, 19, 21, 26, 39 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 16/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - PRESUPUESTO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
20	Procedimiento Elaboracion y Actualizacion del Presupuesto P-GF1-015 Version 1 del 02/03/2015 Formato Anteproyecto Presupuestal F-GF1-031 Version 2 del 03/06/2015 Distribucion Presupuestal (Honorarios Asesorias Administrativas)	La definicion del valor de cada una de las lineas en el anteproyecto, debe corresponder y ajustarse a la real necesidad de gasto de la operación para la siguiente vigencia.		Se presentan porcentajes de inversión para las lineas presupuestales de "Honorarios Asesorias Administrativas" del 6.1%, 13.7% y 11.3% respectivamente frente al total del presupuesto, la proporción de ejecución dentro de la linea presupuestal es del 29.41%, 95.49% y 60.25% respectivamente	1. Se recomienda aumentar el valor del presupesto asignado a la linea de Honorarios Asesorias Administrativas, asi mismo ejecutarlo en la mayor parte posible, para asi cumplir con los proyectos criticos como lo es el desarrollo de la aplicacion Matrix. Riesgo Alto: No planificar y distribuir el presupuesto teniendo en cuenta la criticidad de los proyectos Riesgo Relacionado: Riesgo Operacional No. 12, 17, 19, 21, 26, 39 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 16/05/2019

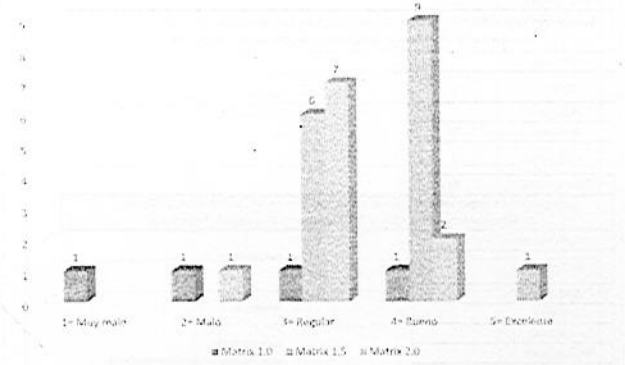
COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - PRESUPUESTO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
21	Plan Estrategico 2014-2018	Se requiere desarrollar un proyecto que permita completar el aplicativo de manera adecuada, conforme a las metodologías y procesos adoptados por la Sociedad de Activos Especiales - SAE, con los esquemas de seguridad requeridos para la información que se maneja y con el personal requerido para completar un aplicativo de las dimensiones estipuladas en un proyecto que requiere más de 15.000 horas hombre dedicadas a la construcción de los elementos faltantes en el aplicativo y cerca de 22.000 horas hombre en el proyecto en general		La OCI no cumplió con los planes de mejoramiento descritos en el Plan Estrategico 2014-2018, presentando a la fecha de la auditoria un retraso de 9 meses El indicador del proyecto Matrix 2.0 presenta inconsistencias, la información reportada y presentada en el Plan de Accion de la vigencia 2018 no es consistente	Riesgo Alto: Incumplimiento en los proyectos Riesgo Relacionado: Riesgo Operacional No. 12, 54, 90 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo de Seguridad de la Información No. 67, 70, 73 Mapa de Riesgos de Seguridad de la Información 2019 F-DE2-318 Version 1 15/05/2019

COMPONENTE : ESTADO DE IMPLEMENTACION Y FUNCIONALIDAD DEL SISTEMA DE INFORMACION MATRIX VERSION 2.0 - PRESUPUESTO					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
22	Plan Estrategico 2019-2022	Consolidar la implementacion de un sistema de información con criterios de seguridad, calidad y cumplimiento ajustados a los procesos del negocio		El Plan Estrategico 2019-2022 para el proyecto Matrix 2.0 define un peso más la formula del indicador (% de ejecucion del proyecto / % proyectado del plan de trabajo) , unicamente pretende medir eficacia (cumplimiento)	1. Se recomienda usar metricas de desempeño para proyectos de desarrollo ágil como lo es el "Valor del Negocio Entregado al Cliente", donde se tiene en cuenta la priorización en la atención a las funcionalidades que se van desarrollando en el proyecto Matrix 2.0 y que mas valor agregan al negocio, lo anterior teniendo en cuenta que la operación en la OCI se basa en metodologías agiles en lo que respecta al desarrollo de aplicaciones, según lo indicado en el documento Caracterización de Macroproceso de Tecnología C-TE-002 Versión 3 del 06/02/2018 Riesgo Alto: No tener indicadores de eficiencia y evidenciables Riesgo Relacionado: Riesgo Operacional No. 12, 54, 90 Mapa de Riesgos Operacionales 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo de Seguridad de la Información No. 67, 70, 73 Mapa de Riesgos de Seguridad de la Información 2019 F-DE2-318 Version 1 15/05/2019

COMPONENTE : PRUEBAS DE CALIDAD, CARGA Y ESTRES / MITIGACION DE VULNERABILIDADES					
No.	Subproceso y/o Actividad	Actividades de Control	Evaluacion de Control	Oportunidad de Mejora	Riesgos y Recomendaciones
23	Norma ISO/IEC 27001:2013 A.14.2.9 Prueba de Aceptacion de Sistemas Gestion de Pruebas Planificación, Ejecución y Seguimiento	Para los Sistemas de Información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptacion relacionados		Se presentó una falla de actualización de estado de la prueba "CU1 Autentica Usuario", donde al verificar la trazabilidad en sitio del caso, a pesar de que se habian corregido 2 errores detectados durante las pruebas, no fue actualizado el estado del caso "2953 CU1 – Fallo al parametrizar el acceso a Visitas Inmuebles", el estado se encontraba en estado "Resuelto" y debió dejarse en "Cerrado", esto corresponde a actividades de marzo de 2019 El profesional de pruebas es el responsable de mantener actualizado el estado de las pruebas durante todo el ciclo de las mismas, así como de monitorearlas y gestionarlas según el estado en el que se encuentren, periódicamente se genera un informe que es entregado al Project Manager – PM de la OCI, donde no se recibe ninguna retroalimentación al profesional de pruebas por parte del PM o de instancias superiores.	1. Se recomienda efectuar seguimiento, valoracion y retroalimentar a todo el equipo de pruebas 2. Se Recomienda documentar el procedimiento, establecer controles y registros para el seguimiento al mismo Riesgo Alto: No efectuar seguimiento y valorar la gestion de pruebas, no permite conocer el estado real del procedimiento y plantear estrategias basadas en hechos Riesgo Relacionado: Riesgo de Corrupcion No. 1, 6 Mapa de Riesgo de Corrupcion 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo Operativo No. 56 Mapa de Riesgos Operativos 2019 F-DE2-274 Version 2 15/05/2019 Riesgo Relacionado: Riesgo de Seguridad de la Información No. 67 Mapa de Riesgos de Seguridad de la Información 2019 F-DE2-318 Version 1 15/05/2019
	Norma ISO/IEC 27001:2013 A.12.1.1 Procedimientos de Operación Documentados Gestion de Pruebas Planificación, Ejecución y Seguimiento	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan		No existe documentación oficial de apoyo al procedimiento de pruebas	

ANEXO - RESULTADOS Y ANALISIS DE ENCUESTAS

COMPONENTE MATRIX					
Funcionalidad Califique de 1 a 5, donde 1 = muy malo, 2 = malo, 3 = regular, 4 = bueno, 5 = excelente					
Version Instalada	1= Muy malo	2= Malo	3= Regular	4= Bueno	5= Excelente
Matrix 1.0	1	1	1	1	
Matrix 1.5			6	9	1
Matrix 2.0		1	7	2	
Total General	**1**	**2**	**14**	**12**	**1**



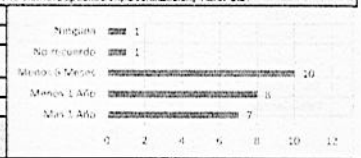
Integracion e Interfaz	
Necesita ver informacion y/o gestion de otras areas? (Si - No)	
SI	21
NO	6
Total General	**27**
En caso de Si, solicitó la integracion u interfaz? (Si - No)	
SI	8
NO	11
Total General	**19**
Hace cuantos dias/meses solicito la Integracion?	
mas 1 año	2
menos 1 año	2
No responde	4
Total General	**8**
Problemas	
Ha tenido problemas con Matrix?, (Si - No)	
SI	19
NO	9
Total General	**28**
Cual?	
1= Rendimiento	5
2= Falta de Actualizacion de Informacion o Parametrizacion	17
3= Falta de Campos	8
4= Falta de Controles	7
5= Fallas Recurrentes	8
6= Falta de Mensajes Confirmaciones	2
7= Falta de Confianza	10
8= Mucha Digitacion	3
9= Desbloqueo de usuarios	1
10= Otro	6
11= Ninguno	4
12= Otro cual	4
Total General	**75**
Solicitudes a Mesa de Ayuda	
El area ha efectuado solicitides a la Mesa de Ayuda relacionadas con Matrix? (Si - No)	
SI	21
NO	6
Total General	**27**
De que tipo?	
1= Correcciones	12
2= Mejoras	10
3= Nuevos Desarrollos	10
4= Incidentes	13
Total General	**45**
Tiene solicitudes sin atencion? (Si - No)	
SI	8
NO	14
Total General	**22**
Documentacion	
Conoce la documentacion de la aplicación y su ubicación? (Si - No)	
SI	5
NO	23
Total General	**28**

COMPONENTE PAGINA WEB	
Funcionalidad Califique de 1 a 5, donde 1 = Muy Malo, 2 = Malo, 3 = Regular, 4 = Bueno, 5 = Excelente	
1= Muy malo	0
2= Malo	1
3= Regular	3
4= Bueno	20
5= Excelente	3
Total General	**27**

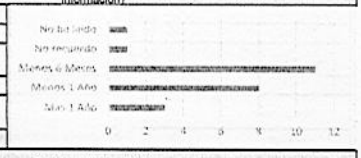
Integracion	
Cree que le falta integrar mas objetos a la pagina (aplicaciones, menus, documentos - Publicaciones etc.)? (Si - No)	
SI	11
NO	16
Total General	**27**
Cuales?	
Aplicaciones	2
Menus	1
Documentos - Publicaciones	5
Otros	4
Total General	**12**
Problemas	
Ha tenido problemas con la Pagina Web?, (Si - No)	
SI	8
NO	19
Total General	**27**
Cuales?	
1-Actualizacion de Informacion	5
2= Disponibilidad	3
3= Rendimiento	2
4= Diseño	3
5= Otro	0
6= Ninguno	3
Total General	**16**
Solicitudes a Mesa de Ayuda	
El area ha efectuado solicitides relacionadas con la pagina Web? (Si - No)	
SI	3
NO	22
Total General	**25**
De que tipo?	
1= Correcciones	0
2= Mejoras	2
3= Nuevos Desarrollos	1
4= Incidentes	1
Total General	**4**

ANEXO - RESULTADOS Y ANALISIS DE ENCUESTAS

COMPONENTE SEGURIDAD DE LA INFORMACION	
Capacitacion, Socializacion	
Cuando recibio la ultima Capacitacion, Socializacion, Taller etc?	
Mas 1 Año	7
Menos 1 Año	8
Menos 6 Meses	10
No recuerdo	1
Ninguna	1
Total General	**27**

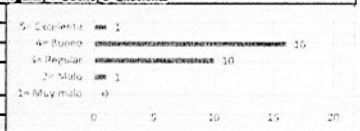


Conocimiento	
Hace cuanto fue la ultima vez que leyo el Manual Politica de Seguridad y Privacidad de la Informacion?	
Mas 1 Año	3
Menos 1 Año	8
Menos 6 Meses	11
No recuerdo	1
No he leido	1
Total General	**24**

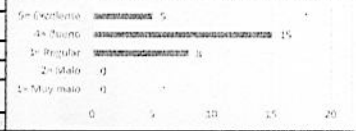


Pruebas de Seguridad	
Tiene acceso de escritura a Medios Extraibles (Memoria USB, CD-DVD)? (Si - No)	
SI	1
NO	27
Total General	**28**
Restricciones en Carpeta Compartida? (Si - No)	
SI	28
NO	0
Total General	**28**
Acceso a Youtube, Redes Sociales? (Si - No)	
SI	1
NO	27
Total General	**28**
Equipo Desatendido (Bloqueo Automatico del Equipo de Computo) (Si - No)	
SI	15
NO	13
Total General	**28**

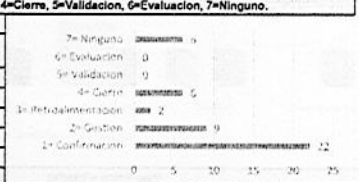
COMPONENTE MESA DE AYUDA	
Funcionalidad Califique el software de Gestion de Tiquetes, de 1 a 5 donde, 1=Muy Malo, 2=Malo, 3=Regular, 4=Bueno, 5=Excelente	
1= Muy malo	0
2= Malo	1
3= Regular	10
4= Bueno	16
5= Excelente	1
Total General	**28**



Servicio califique el servicio, presencial o telefonico del personal de la mesa de ayuda, de 1 a 5 donde, 1= Muy Malo, 2=Malo, 3=Regular, 4=Bueno, 5=Excelente	
1= Muy malo	0
2= Malo	0
3= Regular	8
4= Bueno	15
5= Excelente	5
Total General	**28**



Integracion Le llegan los mensajes al correo electronico, 1=Confirmacion, 2=Gestion, 3=Retroalimentacion, 4=Cierre, 5=Validacion, 6=Evaluacion, 7=Ninguno.	
1= Confirmacion	22
2= Gestion	9
3= Retroalimentacion	2
4= Cierre	6
5= Validacion	0
6= Evaluacion	0
7= Ninguno	6
Total General	**45**



Conoce el procedimiento de validacion del servicio? (Si - No)	
SI	7
NO	21
Total General	**28**
Conoce el procedimiento de valoracion del servicio? (Si - No)	
SI	0
NO	28
Total General	**28**
Conoce el procedimiento de rechazo del servicio? (Si - No)	
SI	2
NO	26
Total General	**28**
Los mensajes enviados al correo electronico son claros? (Si - No)	
SI	15
NO	9
Total General	**24**
Problemas	
ha tenido problemas con el servicio de Mesa de Ayuda?, (Si - No)	
SI	9
NO	14
Total General	**23**
Cual?	
Comunicacion	4
Software	1
Demora en el Servicio	6
Otros	1
Ninguno	3
Total General	**15**

