INFORME EJECUTIVO DE AUDITORIA INTERNA

PROCESO DE INFRAESTRUCTURA TECNOLÓGICA – SEGURIDAD DE LA INFORMACIÒN: COMPONENTE COPIAS DE RESPALDO Y RESTAURACIÒN DE LA INFORMACIÓN

SOCIEDD DE ACTIVOS ESPECIALES SAE S.A.S.

OFICINA DE CONTROL INTERNO

VIGENCIA 2023

Bogotá, D.C. junio de 2024

INTRODUCCIÓN

La Oficina de Control Interno en desarrollo de su función constitucional con lo descrito en el Plan Anual de Auditoria basado en riesgos de la vigencia 2024, desarrolló auditoría interna al Proceso de infraestructura tecnológica – seguridad de la información: componente copias de respaldo y restauración de la información, orientada a evaluar la ejecución de las actividades y aplicación de controles de acuerdo con los procesos establecidos en la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de la Información OTI establecido en la arquitectura de la entidad hoy mapa de procesos, así como el cumplimiento de la normatividad legal vigente.

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

El proceso auditor de evaluación independiente se 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 EJECUTIVO AUDITORÍA INTERNA DE GESTIÓN
PROCESO DE INFRAESTRUCTURA TECNOLÓGICA – SEGURIDAD DE LA INFORMACIÒN:
COMPONENTE COPIAS DE RESPALDO Y RESTAURACIÒN DE LA INFORMACIÓN

1. OBJETIVO (Norma desempeño 2210).

Evaluar el Sistema de Control Interno los riesgos de gestión a la pertinencia y oportunidad de los Procesos de Infraestructura Tecnológica – Seguridad de la Información Componente Copias de Respaldo y Restauración de la Información establecidos en la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de la Información, como también el cumplimiento de la política y normatividad legal vigente aplicable, generando una cultura organizacional fundamentada en la información, el control y la evaluación.

1.1 Objetivos Específicos (Norma desempeño 2210)

- Evaluar y revisar el seguimiento a la gestión al proceso de copias de respaldo y restauración de la información
- Evaluar indicadores.
- Evaluar riesgos y controles.
- Evaluación de Talento Humano de las áreas auditadas
- Evaluar la conservación de la información y tablas de Retención Documental

2. ALCANCE (Norma desempeño 2220)

Evaluar la aplicabilidad de los procesos y procedimientos establecidos en los manuales y las circulares internas, políticas y normatividad legal vigente, en el periodo comprendido entre el 01 de enero de 2023 al 31 de diciembre de 2023, para la verificación de los controles existentes y el manejo de los riesgos en la Infraestructura Tecnológica – Seguridad de la Información: Componente Copias de Respaldo y Restauración de la Información.

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

3. FORTALEZAS (Atributo desempeño 2300)

La disposición de la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI como primera línea para gestionar y coordinar los debidos permisos de ingreso para ejecutar las visitas en sitio en las instalaciones del proveedor [redacted]

La diligencia para atender el cronograma de las mesas de trabajo citadas por la Oficina de control Interno y remitir la información requerida.

La Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI cuenta con la herramienta especializada de copias de respaldo [redacted] para realizar la parametrización de la programación de trabajos de backup completos, incrementales, y trabajos de restauraciones en los diferentes servidores y la programación de la periodicidad correspondiente.

Se evidencia en la visita a las instalaciones del proveedor Datacenter [redacted], que el Datacenter [redacted] está en una ubicación segura y dispone de los debidos controles de acceso físico entre otros [redacted]

Se evidencio los controles de acceso físico y la [redacted] en el Datacenter así como el [redacted]

En la visita en sitio a las instalaciones del proveedor [redacted] se encuentra en una ubicación segura y dispone de controles de acceso físico implementados como [redacted]

El recorrido en las instalaciones es guiado por personal operario de [redacted] y se evidencia que el acceso a la Bóveda donde se contienen los medios de almacenamiento de información de SAE es restringido por seguridad [redacted]

[redacted]

4. DEBILIDADES (Atributo desempeño 2300).

- Se evidencia incertidumbre en las labores del día a día de la operación de la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI como primera línea la gestión, en su quehacer la coordinación y ejecución de controles de verificación aleatoria de pruebas de recuperación a las copias de respaldo que en el ejercicio se pueda comprobar y verificar su integridad y la posibilidad de uso de la información en caso de ser necesario.

- Ausencia de un lineamiento de configuración de la herramienta especializada de copias de respaldo [redacted] para realizar la parametrización de programación de tareas, la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI como primera línea realiza labor en el conocimiento y operación del equipo de infraestructura que tiene el conocimiento en la práctica más no se cuenta con el lineamiento de configuración documentado.

- Subutilización de la plataforma suite de gestión documental con la que cuenta el proveedor [redacted] para el ingreso y consulta del estado del medio de almacenamiento y su historial de préstamo, de acuerdo a la información suministrada por el proveedor [redacted] de la relación de usuarios creados para ingresar a la plataforma se evidencia que están creados usuarios que corresponden a personal que ya no se encuentran vinculados laboralmente a la entidad.

- Identificación del tiempo real acorde a la realidad de la operación y el procedimiento para establecer el tiempo aproximado de almacenamiento temporal de la cinta en los casilleros del Datacenter de [redacted] y su posterior entrega al proveedor de custodia [redacted].

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

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

6. COMPROMISO DEL AUDITADO (Norma desempeño 2420).

Dentro del aviso de la auditoría realizada a través de memorando interno No. 20241400039743 del 01 de abril de 2024, se informó a la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI que en el marco de la auditoría interna de gestión y en cumplimiento del artículo 2.2.21.4.8 del Decreto 648 de 2017 "*Instrumentos de la actividad de la Auditoría Interna -Carta de representación",* toda la información suministrada a la Oficina de Control Interno debe cumplir con los criterios de veracidad, calidad y oportunidad. Así mismo, en la reunión de apertura desarrollada el 05 de abril de 2024, se indicó a los auditados los compromisos y responsabilidades en la entrega de la información.

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

Dando cumplimiento al Plan Anual de Auditoría basado en riesgos vigencia 2024, y el rol de la Oficina de Control Interno en función de la actividad independiente y objetiva de evaluación y seguimiento que contribuye de manera efectiva al mejoramiento continuo de los procesos de Administración del Riesgo, Control y Gestión de la entidad, se programó la auditoría interna de gestión de infraestructura tecnológica – seguridad de la información: componente copias de respaldo y restauración de la información.

Conforme al procedimiento para ejecutar auditorías internas, en la etapa de planeación y ejecución se desarrolló lo siguiente:

- Remisión del plan de auditoría a los auditados para revisión y aprobación de los tiempos y fechas mediante memorando No. 202414000397743 del 01 de abril de 2024.
- Mediante correo electrónico del 02 de abril de 2024 dirigido a la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI , se realizó solicitud de información preliminar para la etapa de planeación.
- Respuesta de la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI, a la solicitud de información para la planeación de la Auditoria, 04 de abril de 2024
- Mediante correo electrónico del 02 de abril de 2024 dirigido a la Dirección de Talento Humano, se realizó solicitud de información preliminar para la etapa de planeación.
- Respuesta de la Dirección de Talento Humano, a la solicitud de información para la planeación de la Auditoria, 09 de abril de 2024.
- Mediante correo electrónico del 02 de abril de 2024 dirigido a la Dirección de Contratación, se realizó solicitud de información preliminar para la etapa de planeación.
- Respuesta de la Dirección de Contratación, a la solicitud de información para la planeación de la Auditoria, 05 de abril de 2024.
- Mediante correo electrónico del 03 de abril de 2024 dirigido a la Oficina de Integridad, Anticorrupción y Cumplimiento, se realizó solicitud de información preliminar para la etapa de planeación.
- Respuesta de la Oficina de Integridad, Anticorrupción y Cumplimiento, a la solicitud de información para la planeación de la Auditoria, 04 de abril de 2024.
- Reunión de apertura a través de la herramienta Teams el 05 de abril de 2024 para presentar a la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI el objetivo, alcance y cronograma de auditoría.
- El día 10 de abril de 2024, se realizó mesa de trabajo No. 1 Revisión de contextualización información recibida de la OTI, verificación archivos de Excel denominado "programación de tareas backup", y archivos de la herramienta [redacted]: "Export Register Tareas ejecutadas 2023", "Informe completo auditoria", visualización y toma de pantallazos de la parametrización de programación de tareas en la herramienta especializada de copias de respaldo [redacted] para los servidores, visualización espacio en DD BackUS, FileServer. FileServer NAS, revisión archivo de Excel "Tickets de Backups enero diciembre 2023" tickets de backups para vigencia 2023 generados en mesa de servicio, revisión archivo de Excel "Lista de Usuarios Desvinculación 2023 Backups". Compromiso de la Mesa la solicitud del trámite de permisos por parte de la OTI para ingresar a las instalaciones del proveedor Datacenter [redacted], se suministran los datos de la colabora del equipo OCI quien realizara la visita en sitio.
- El día 11 de abril de 2024, se realizó mesa de trabajo No. 2 Revisión de alcance de archivo enviado por la OTI de archivo de Excel denominado "Lista de Usuarios Retirados 2023 Backups" con información completa de la relación de tiquete generado en mesa de servicio, visualización configuración fileserver permisos usuarios, fileserver permisos grupos, visualización configuración SrvProdGest01 BKP User 2023.
- Respuesta por medio de Teams se recibe archivo de Excel "Listado de Usuarios Retirados 2023 Backups" listado desde la base con la información completa de número de tiquete generado en la mesa de ayuda y fecha, 11 de abril de 2024
- El día 18 de abril de 2024, se realizó mesa de trabajo No. 3 Se visualiza la información compartida por la OTI de los soportes de evidencia y archivos del seguimiento a los controles, tratamiento y materialización de riesgos que son responsabilidades de la OGI y que en su momento reportaron a la hoy Oficina de Integridad, Anticorrupción y Cumplimiento OIAC. Con Infraestructura se verifico el archivo de Excel "Inventario Infraestructura (Actual)" la hoja Mapa general de RED WAN se evidencia desactualizada a la infraestructura actual, se recibe en mesa de trabajo

el archivo de PDF “Ingeniería de detalle [redacted]A SAE” el cual si se encuentra actualizado el despliegue lógico de infraestructura de los servidores de la SAE, el diagrama general de [redacted] y la [redacted]. Queda el compromiso en la Mesa de Trabajo por parte de la OTI de realizar alcance de actualización al Formato FTE1-404 Relación de Cintas de Backups el cual no se evidencia diligenciado la fecha de registro.

- El día 24 de abril de 2024, se realiza visita en sitio a las instalaciones del proveedor Datacenter [redacted]. Visualización e identificación de equipos en la distribución del Rack [redacted]. Resultado de la Visita quedan los compromisos por parte de la OTI Genero Caso a Claro: SD3005327 Solicitud Manos Remotas de la identificación RACK, Gabinete, Casilleros de SAE para la toma de registro fotográfico. Y OTI - Solicitara permisos de acceso a instalaciones a Proveedor [redacted] (custodia de cintas de backup) para la próxima semana lo más pronto posible.
- Mediante correo electrónico del 25 de abril de 2024 dirigido a la Dirección de Talento Humano, se realizó solicitud de aportes parafiscales de colaboradora del equipo OCI con el fin de realizar visita a las instalaciones del Proveedor [redacted] (proveedor de custodia de medios de almacenamiento).
- Respuesta de la Dirección de Talento Humano, aportes parafiscales colaboradora OCI para el ingreso a las instalaciones del Proveedor [redacted] (proveedor de custodia de medios de almacenamiento), 26 de abril de 2024.
- Mediante correo electrónico del 26 de abril de 2024 dirigido a la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI, se enviaron aportes para fiscales con el fin de cumplir con los procedimientos de dicho proveedor para realizar la visita en sitio.
- Respuesta de la OTI por medio de Teams se recibe archivo PDF del registro fotográfico suministrado por Manos Remotas del Datacenter de [redacted], 26 de abril de 2024.
- Respuesta de la OTI copiando correo electrónico del Proveedor de Custodia [redacted] confirmando visita en sitio a las instalaciones ubicada en [redacted] para el día 02-may-2024, 29 de abril de 2024.
- El día 29 de abril de 2024, se realizó mesa de trabajo No. 4 Solicitando a la OTI el alcance del compromiso de la mesa de trabajo No.3 del 18-abr-2024 la actualización al Formato FTE1-404 Relación de Cintas de Backups, se recibe archivo de Excel del Formato FTE1-404 Relación de Cintas de Backups actualizado la fecha de registro, y se recibe el archivo PDF “Cintoteca Piso [redacted] SAE” correspondiente al registro fotográfico realizado por manos remotas del Data Center de [redacted] de los casilleros de SAE del almacenamiento de las cintas LTO. Queda el compromiso en la Mesa de Trabajo por parte de la OTI el suministro de la Tabla de Roles y Responsabilidades del personal de infraestructura, del archivo de Excel “Inventario Infraestructura (Actual)” verificación de la hoja “Librería de Backups” la cual no se evidencia en el contenido del archivo y es citada en el Instructivo para Recuperación de la Librerías de Backups N-TE1-069 al igual que la Matriz de escalamiento de proveedores y el chack list del dispositivo de la librería de backups funcionando correctamente. En la mesa de trabajo se recibe el archivo de Excel “Matriz Escalamiento”.
- El día 02 de mayo de 2024, se realiza visita en sitio a las instalaciones del proveedor de custodia de medios de [redacted] Resultado de la Visita quedan los compromisos por parte de la OTI de solicitar: Información de los usuarios de SAE de ingreso a la plataforma Suite Documental de ATS, que usuario de a SAE esta como interventor? Y que roles tiene dentro del aplicativo. Registro fotográfico del recorrido realizado al acceso a la [redacted] y demás donde está contenida la información de cintas LTO, CD, etc. Registro fotográfico del marcado de los medios de SAE donde se evidencie el (código SAE, código uniarchi y el código de asignación física). Los registros de los formatos de consulta [redacted] de la vigencia 2023.
- El día 03 de mayo de 2024, se realizó mesa de trabajo No. 5 Solicitando el compromiso en la Mesa de Trabajo No.4 del 29-abr-2024 por parte de la OTI el suministro de la Tabla de Roles y Responsabilidades del personal de infraestructura, del archivo de Excel “Inventario Infraestructura (Actual)” verificación de la hoja “Librería de

Backups" la cual no se evidencia en el contenido del archivo y es citada en el Instructivo para Recuperación de la Librerías de Backups N-TE1-069 al igual que la Matriz de escalamiento de proveedores y el chack list del dispositivo de la librería de backups funcionando correctamente. En la mesa de trabajo se recibe el archivo de Excel "Funciones – Técnico Virtualización y Backups".

- Mediante correo electrónico del 06 de mayo de 2024 dirigido a la Dirección de Talento Humano, se realizó solicitud del comunicado individual de funciones F-GT1-104 de los ingenieros de infraestructura de la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI.
- Respuesta de la Dirección de Talento Humano, comunicado individual de funciones de los ingenieros de infraestructura de la Oficina de Gestión de la Información OGI hoy Oficina de Tecnologías y Sistemas de Información OTI, 08 de mayo de 2024.
- El día 08 de mayo de 2024, por teams se solicita el archivo maestro de Excel del Modelo de Seguridad y Privacidad de la Información MSPI versión al 31-dic-2023.
- El día 06 de mayo de 2024, por teams se solicita nuevamente avance la información que debe suministrar el proveedor [redacted] de acuerdo con la visita realizada en sitio el 02-may-2024.
- El día 08 de mayo de 2024, por teams se solicita nuevamente avance la información que debe suministrar el proveedor [redacted] de acuerdo con la visita realizada en sitio el 02-may-2024.
- Respuesta de la OTI, reenvía correo electrónico del proveedor [redacted] con el adjunto del registro fotográfico correspondiente al recorrido e ingreso a la [redacted] evidenciando el cumplimiento de ciertas características y controles ambientales de temperatura, humedad, detección de fuego, etc, el 09-may-2024.
- Respuesta de la OTI, envía correo electrónico con los archivos adjuntos de Excel de los inventarios mes por mes que enviaba [redacted] durante el año 2023, el 09-may-2024.
- El día 14 de mayo de 2024, por teams se solicita nuevamente el avance la información faltante por suministrar el proveedor [redacted] de la información de los usuarios creados para SAE en la Suite de Gestión Documental.
- Respuesta de la OTI, reenvía correo electrónico del proveedor [redacted] con el pantallazo del resultado búsqueda de historial de auditoría de inicios de sesión en la plataforma Suite de Gestión Documental y archivo de Excel "USUARIOS ACTIVOS SAE -08052024", el 14-may-2024.
- El día 14 de mayo de 2024, por teams se solicita la consulta del usuario ammoremo@saesas.gov.co en el reporte BI "Report Usuarios Perfiles por Sistema"
- Respuesta de la OTI, envía por teams la imagen de la consulta del usuario ammoreno@saesas.gov.co en estado Inactivo, el 14-may-2024
- Respuesta de la OTI, envía correo electrónico con los archivos adjuntos de Excel de los inventarios mes por mes que enviaba [redacted] durante el año 2023, el 14-may-2024
- El día 15 de mayo de 2024, por teams se solicita imagen de consulta del Tiquete No.93288 registrado en la Mesa de Servicio.
- Respuesta de la OTI, envía por teams la imagen y el PDF generado de la consulta del Tiquete No.93288 registrado en la Mesa de Ayuda, el 15-may-2024
- El día 16 de mayo de 2024, por teams se solicita nuevamente el archivo maestro de Excel del Modelo de Seguridad y Privacidad de la Información MSPI versión al 31-dic-2023.
- Respuesta de la OTI, deja en la carpeta publica los archivos de Excel "Diagnostico sistema ISO 27000 – 2022 _OGI y el archivo de Excel denominado "Instrumento de Evaluación MSPI 2023", y también lo envían por correo electrónico el archivo de instrumento de evaluación para el avance de implementación del Modelo de Seguridad y Privacidad de la Información, y el diagnostico que se envió para la actualización de la Norma ISO 27001:2022, 17 de mayo de 2024
- El día 17 de mayo de 2024, por teams se solicitan los archivos de Excel generados de la herramienta [redacted] de la carpeta pública (fileservernas) para la vigencia 2023
- Respuesta de la OTI, deja en la carpeta publica los archivos de Excel generados de la herramienta [redacted] de la carpeta pública (fileservernas) para la vigencia 2023, 17 de mayo de 2024

- El día 17 de mayo de 2024, por teams se solicita de muestra aleatoria de 21 desvinculaciones de personal, los archivos PDF de los tiquetes registrados en la Mesa de Ayuda
- Respuesta de la OTI, deja en la carpeta publica los 21 archivos de la muestra aleatoria (archivos de PDF generados de los tiquetes registrados en la mesa de ayuda por desvinculación de personal), 17 de mayo de 2024

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

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

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

9. 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]
Posibilidad de Afectación Operacional por indisponibilidad de los servicios tecnológicos debido a falta de capacidad técnica y operativa	Operacional	Alto
Posibilidad de Afectación Económica por fallas en la infraestructura tecnológica que soporte los servidores ofertados por TI debido a falta de capacidad técnica, operativa y de negocio	Operacional	Moderado
Posibilidad de Afectación Económica y Reputacional por procesos documentados de manera indebida o desactualizados debido a desconocimiento técnico y/o falencias en los controles en la documentación del SIG	Operacional	Moderado

Riesgos Identificados en el proceso de auditoría	Tipo de Riesgo	Calificación de riesgo inherente según matriz de riesgos SAE[1]
Posibilidad de Afectación Reputacional por incumplimiento de la normativa vigente debido a desconocimiento técnico y/o debilidades en la aplicación de controles operacionales.	Operacional	Moderado
Posibilidad de Afectación Económica y Reputacional por falta de identificación de los activos productivos dentro del sistema de información debido a información, conocimiento y capacidad operativa insuficiente.	Operacional	Moderado
Posibilidad de Afectación Reputacional por incumplimiento del proceso de evaluación de rendimiento laboral debido a faltade apropiación y ejecución oportuna del proceso de evaluación.	Operacional	Bajo
Posibilidad de recibir o solicitar cualquier dávida o beneficio a nombre propio o de terceros, con el fin de dar un tratamiento especial o preferencial utilizando indebidamente influencias personales o poder derivadas del ejercicio del cargo, de las funciones asignadas o conocimiento de asuntos propios de la entidad	Corrupción	Extremo
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros, con el fin de dar uso indebido o ilícito de información confidencial, privilegiada o reservada relativa a los procesos que adelanta la SAE así como de sus sistemas de información	Corrupción	Extremo
Inconsistencias o Pérdida de la Información	Seguridad de la información	Moderado
Posibilidad de Pérdida de confidencialidad con Afectación Económica y Reputacional por fuga de información privilegiada o sensible debido a fallas en la administración y custodia de la información	Seguridad de la información	Moderado

Fuente: Papeles de trabajo auditoria

Nota: Los riesgos identificados en la tabla anterior corresponden a los aprobados por la entidad y se toman con el texto y valoración de riesgo inherente que han sido realizadas y evaluados por los dueños del proceso.

10. 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.

En el proceso de auditoria no se evidenciaron eventos con desempeño alto.

10.1 DESCRIPCIÓN OPORTUNIDADES DE MEJORA/OBSERVACIONES

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

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

No	OM/OB[1]	Oportunidad de mejora y Observaciones	Repetido
1	OM	Realización de pruebas aleatorias de recuperación a las copias de respaldo que permitan comprobar la posibilidad de uso en caso de ser requeridas	No
2	OM	Lineamiento escrito que documente la configuración de programación de tareas backup en la herramienta [redacted] vs archivo excel "programación de tareas backup" tal y como se está realizando actualmente	No
3	OM	Actualización de procedimientos en cuanto a la relación de los documentos que se utilizan en la ejecución de los Instructivos	Si
4	OM	definición de matriz y/o tabla de roles y responsabilidades para los usuarios de infraestructura, así como establecer cuenta de usuario personalizada para cada uno de los administradores de los recursos tecnológicos y los sistemas de información	No

No	OM/OB[1]	Oportunidad de mejora y Observaciones	Repetido
5	OM	Verificación de las novedades de desvinculación de personal de la entidad y validar la completa eliminación o bloqueo de cuentas de acceso creadas en recursos tecnológicos o plataformas que proveen terceros a SAE	No
6	OM	identificación, clasificación, revisión y estado de la información contenida en el inventario de medios magnéticos (CD, DVD) custodiados en Bodega Proveedor [redacted]	Si
1	OB	Actualización y publicación en la página web de la entidad de los cuatrimestres 2023 del Seguimiento Mapa de Riesgos Seguridad Información, Seguimiento Mapa de Riesgos de Corrupción y Seguimiento Mapa de Riesgos Operaciones.	Si
2	OB	Actualización de Inventario de Hardware a cargo de la OTI vs Placas de Inventario evidenciado en [redacted] vs archivo de Excel "Inventario Infraestructura (Actual)" y sus diferentes hojas.	Si
3	OB	Actualización comunicación individual de funciones acorde al formato F-GT1-004 V6 06-07-2023 y diligenciamiento "Fecha de Comunicación" con todas las firmas requeridas en formato.	Si

Fuente: Papeles de trabajo auditoria

CONCLUSIONES (Atributo desempeño 2400).

- La oficina de control interno y de acuerdo con lo evidenciado y reportado en el presente informe en el ejercicio de evaluación y seguimiento concluye que el sistema de control interno del Proceso de infraestructura tecnológica – seguridad de la información: componente copias de respaldo y restauración de la información se encuentra en mejora continua y requiere análisis para la implementación de controles efectivos enfocados a la definición de lineamientos de configuración de la herramienta de backup para un seguimiento continuo a fin de procurar la correcta ejecución de las actividades según la relación de los documentos, formatos, lineamientos relacionados en sus actividades bajo los principios que lo regulan a la realidad de la operación del día a día.

- Se observa la necesidad de garantizar el principio fundamental basado en la norma la ISO 27001 de la integridad y disponibilidad de la información contenida en las copias de respaldo y que estas al momento de requerir su recuperación se pueda acceder a la información con el adecuado dispositivo de lectura, el

hardware, sistema operativo y sistema de información donde se pueda comprobar la efectividad del uso de copias de respaldo. De tal manera la importancia de realizar controles periódicos y aleatoriamente realizar pruebas de restauración de copias de respaldo sin limitarse solo a realizar las restauraciones por solicitud de demanda.

- El área como dueña del proceso, es responsable de realizar seguimiento y mantener una adecuada documentación actualizada de los procesos en la arquitectura de la SAE de acuerdo a los diferentes procedimientos y teniendo en cuenta que la entidad debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de calidad incluidos los procesos necesarios para revisar y actualizar la documentación pertinente, de acuerdo con los documentos mencionados para el Macroproceso de Tecnología: Proceso de Gestión de Infraestructura Tecnológica, mencionados anteriormente con la fecha de versión y suministrados por la OTI estos deben estar publicados con la información actualizada y acorde a la ejecución de las tareas en el actual desarrollo de las actividades y que no difieran en relación de contenido de documentos, identificando que se usa realmente.

- Es importante para la trazabilidad y control la definición de una matriz de roles y/o permisos del equipo de infraestructura por usuario para el debido control y monitoreo del registro de ingreso de todas las acciones que tienen a lugar en los servidores.

- Realizar inventario del contenido de la información de los medios magnéticos CD, DVD que están en custodia del proveedor [redacted] y verificar que se cuente con los dispositivos adecuados para la lectura de los medios magnéticos CD, y de esta manera obtener el levantamiento de la información, el estado o calidad de información allí contenida y poder verificar que también se puede recuperar la información.

- Es importante validar y/o actualizar en la política de gestión de acceso de usuarios que la OTI establezca un control y seguimiento asociado que evite el acceso no autorizado a sistemas y servicios de plataformas tecnológicas prevista por proveedores para SAE, para garantizar que el tiquete registrado en la mesa de ayuda para desvinculación de los colaboradores se valide el reportar al proveedor de las plataformas tecnológicas a las cuales accede SAE sean inhabilitados o eliminados. Se sugiere definir estrategias, normas, procedimientos, que fortalezcan los sistemas de control enfocados a asumir determinado nivel de riesgo y así fortalecer la toma de decisiones correspondientes.

Cabe resaltar que, debido a las limitaciones de cualquier estructura de control interno, pueden ocurrir errores o irregularidades que no hayan sido detectadas bajo la ejecución de nuestros procedimientos de auditoría, evaluación o seguimiento, previamente planeados.

Así mismo, es responsabilidad del área la información suministrada, por cualquier medio, para la realización de esta actividad de manera oportuna, completa, integra y actualizada y la de informar en su momento las posibles situaciones relevantes y/o errores que pudieran haber afectado el resultado final de la actividad.

Por lo anteriormente expuesto y en cumplimiento del *procedimiento "Elaboración y seguimiento planes mejoramiento"* se solicita suscribir un Plan de Mejoramiento para las oportunidades de mejora y observaciones identificadas en términos de oportunidad, calidad y efectividad, de acuerdo con las posibles materializaciones de riesgos identificados y/o evaluados y el impacto que trae consigo para la Entidad.

Dicho plan, además de servir de base para la detección de mejoras, debe permitir el control y seguimiento de las diferentes actividades a desarrollar, así como la incorporación de acciones correctivas ante posibles contingencias no previstas en la efectividad, en la mitigación de riesgos, reducción en la probabilidad y en el impacto hacia la SAE.

Cordialmente,

Firmado digitalmente por MARIA DEL PILAR MAYOR VARELA
Fecha: 2024.06.07 13:12:34 -05'00'

María del Pilar Mayor Varela.
Jefe Oficina de Control Interno

Proyecto: Equipo Auditor
Aprobó: Jefe Oficina de Control Interno