RESPONSABLE: JAIME HERNANDO ARIAS PATIÑO

NOMBRE DE LA AUDITORIA/SERVICIO DE ASEGURAMIENTO

Auditoría a la seguridad de la información en el marco de la norma 27001:2013 y los procedimientos TIC-PR09 Gestión de Vulnerabilidades y TIC-PR05 Gestión Incidentes de Seguridad de la Información

OBJETIVO:

Verificar el cumplimiento de lo establecido en los procedimientos TIC-PR05 Gestión incidentes de seguridad de la información versión:02, TIC-PR09 Versión:02 Gestión de vulnerabilidades, la aplicación de lo establecido en el Manual de Políticas de Seguridad y Privacidad de la información, la gestión de riesgos de Seguridad y Privacidad de la información con el fin de evaluar los controles que adopta la entidad para el manejo de la información basado en los dominios que plantea la norma técnica ISO 27001:2022

ALCANCE:

Se realizará la verificación de la apropiación de las buenas prácticas y los lineamientos de seguridad y privacidad de la información establecidos por la Entidad en el periodo comprendido entre enero de 2022 a febrero de 2023

CRITERIOS:

Constitución Política de Colombia: Artículo 15 (Derecho a la intimidad y buen nombre), artículo 20 (Derecho de información) y artículo 74 (Acceso a documentos públicos).
LEY 87 DE 1993 "Por la cual se establecen normas para el ejercicio de control interno en la entidades y organismos del estado y se dictan otras disposiciones"
Ley 44 de 1993 “por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.” (Derechos de autor)
Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones." Desarrollado por el Decreto 4487 de 2009 - Reglamentado parcialmente por el Decreto 1747 de 2000.
Ley Estatutaria 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales Parcialmente Reglamentada por el Decreto 1081 de 2015.
Ley 1273 de 2009. Ley por medio de la cual se crea y se protege el bien jurídico de la información y los datos personales. Así mismo, se tipifican conductas penales como daño informático, violación de datos personales, acceso abusivo a sistema informático, interceptación de datos informáticos, hurto por medios informáticos, entre otras.
Ley estatutaria 1581 de 2012 (Por la cual se dictan disposiciones generales para la protección de datos personales). Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015.
Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC
Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
Decreto Reglamentario 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
Decreto Único Reglamentario 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
Decreto 886 de 2014 “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.”
Decreto 103 de 2015: “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 (Ley de Transparencia y acceso

a la información pública) y se dictan otras disposiciones." Derogado Parcialmente por el Decreto 1081 de 2015.
Decreto 1081 de 2015, Título 1, Este Título tiene por objeto reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública.
Decreto 767 de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"
Directiva 008 DE 2021 Seguimiento al Cumplimiento de los Manuales de funciones y Competencias Laborales
Modelo Integrado de Planeación y Gestión MIPG.
Manual de seguridad de la información Plan de seguridad y privacidad de la información y Plan de gestión de riesgos de seguridad digital de la UAECOB, procedimientos TIC-PR05 Gestión incidentes de seguridad de la información versión:02, TIC-PR09 Versión:02 Gestión de vulnerabilidades
Norma técnica ISO 27001:2013
Demás normas que apliquen

PROCESO AUDITADO:

Gestión Tecnologías de la Información y las comunicaciones

SUBDIRECCIÓN/OFICINA/DEPENDENCIA/ÁREA:

Oficina Asesora de Planeación

LÍDER DE PROCESO/DEPENDENCIA:

Olga Soraida Silva Albarrán

EQUIPO AUDITOR:

Jaime Hernando Arias Patiño – Jefe de la Oficina de Control Interno
María del Carmen Bonilla- Profesional 219 grado 20 OCI

PERIODO DE EJECUCIÓN DE LA AUDITORÍA:

1 de marzo al 17 de mayo de 2023

METODOLOGÍA

De conformidad con la Guía de Auditoría para Entidades Públicas expedida por el DAFP, se emplearon los siguientes procedimientos de auditoría: Consulta, Observación, Inspección y Revisión de evidencia física. Adicionalmente, se empleó la metodología PHVA (Planear, Hacer, Verificar, Actuar)

a) Planear:

- Elaboración del Plan de auditoría y la lista de verificación
- Definición de los objetivos, el alcance y los tiempos de ejecución.
- Preparar la auditoría decampo, papeles de trabajo, investigación documental y procedimental sobre el proceso auditado.

b) Hacer:

- Auditoría de campo a través de entrevista
- Recolección y verificación de la información obtenida de las entrevistas y evidencias documentales.
- Entrega del Informe preliminar de auditoría a los líderes y/o responsables de los procesos auditados.

c) Verificar:

- Análisis de la información, evidencias, y verificación del cumplimiento de acuerdo a lo establecido en los procedimientos, requisitos legales, normas aplicables definidas para la auditoría.
- Mesas de validación de hallazgos donde se presentó el informe preliminar, se aclararon y/o justificaron los hallazgos de no conformidad por parte de los auditores y de los auditados, respectivamente.
- Análisis de las evidencias e información adicional entregada por los auditados en la mesa de validación de hallazgos, y determinar la subsanación de las no conformidades u observaciones.
- Entrega del Informe final de auditoría a los líderes y/o responsables de los procesos auditados.

d) Actuar:

- Solicitud del Plan de Mejoramiento de los hallazgos o desviaciones encontrados, en el FOR-GI-04-01 Solicitud de ACPM.

Para el desarrollo de esta auditoria se procedió a verificar y evaluar los soportes documentales de la información enviada por el área auditada; destacándose entre otra, la siguiente información:

- Documentos soporte del proceso (Políticas, Procedimientos, Resoluciones Internas, Instructivos, planes, etc.)
- Informes del sistema de Gestión de seguridad de la información y ciberseguridad (SGSI) de la Entidad vigencia 2022
- Estrategia de la Seguridad de la Información en la Entidad y cronograma del plan de acción
- Inventario de activos de Información.
- Mapa de riesgos digitales de la entidad.
- Indicadores del proceso con seguimiento y resultados de las vigencias 2022.
- Avances en el cumplimiento del Plan de Mejoramiento

Adicionalmente realizamos visita al Datacenter y al espacio en donde opera el sistema de seguridad CCTV (Circuito Cerrado de Televisión) con el fin de verificar la seguridad física del entorno y los espacios. Se realizaron entrevistas a los profesionales designados por la Jefe de la Oficina Asesora de Planeación para atender la auditoria y reuniones virtuales con el fin de aplicar las listas de verificación preparadas para esta auditoría.

SITUACIONES GENERALES

Teniendo en cuenta que la Seguridad de la Información es uno de los habilitadores transversales de la Política de Gobierno Digital que debe ser implementada por parte de los sujetos obligados según el Decreto Único Reglamentario 1078 de 2015 del Sector de Tecnologías de la Información y las Comunicaciones que en su artículo 2.2.17.5.6 establece: "*Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio. en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital. que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas. políticas. procedimientos. recursos técnicos,*

administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones."

En este sentido y con el objetivo de facilitar y apoyar la implementación de mecanismos de identificación, evaluación y control de riesgos de seguridad de la información y de preservar la confidencialidad, integridad y disponibilidad de la información, a través de los lineamientos y controles que se adoptan en cumplimiento a los requisitos exigidos por la norma técnica Internacional ISO/IEC 27001:2013,para la seguridad y privacidad de sus activos de información, con el propósito de minimizar posibles impactos no deseados que puedan comprometer los principios esenciales del Sistema de Gestión de Seguridad de la Información al interior de la Entidad el área de tecnología genera entre otros documentos el Manual de Políticas de Seguridad y Privacidad de la información TIC-MN01 V2.

Dentro de las políticas definidas por la entidad establece roles y responsabilidades transversales de obligatorio cumplimiento por parte de todos los actores involucrados en el desarrollo e implementación de la Política de Seguridad Digital, dadas las responsabilidades compartidas, se evidencia un sistema de gestión de naturaleza transversal a toda la entidad, en el cual todos sus actores deben estar comprometidos en el mantenimiento y mejora continua.

Dadas las precedentes premisas la Oficina de Control Interno ha identificado las siguientes fortalezas:

1. Compromiso de la Alta Dirección:

   Se observa que la Alta Dirección se encuentra comprometida con la seguridad de la Información, en razón a que ha definido una política de Seguridad y privacidad de la Información y ha dispuesto los distintos recursos financieros, administrativos, humanos y técnicos para su implementación y mejora. Por otra parte, se evidenció que la Alta Dirección realiza seguimiento al cumplimiento de las actividades propuestas para la Seguridad de la información dentro de las sesiones del Comité Institucional de Gestión y Desempeño y a través de la revisión de la metodología de riesgos de la seguridad de la información presentada en el Comité de Coordinación de Control Interno realizado en el mes de noviembre de 2022.

2. Vinculación de la Seguridad de la Información al Sistema de Gestión Institucional

   Se identificó que en la vigencia 2022 en el Comité #1 de Gestión y desempeño se aprobaron los siguientes documentos: El Plan estratégico de tecnologías de la información y las comunicaciones PETI, Plan de Seguridad y privacidad de la Información y, el Plan de tratamientos de riesgos de seguridad y privacidad de la Información, lo que demuestra los esfuerzos que ha realizado la entidad en la optimización de su sistema de gestión fortalecido en temas de seguridad de la información, en pro de prestar un mejor servicio a las partes interesadas

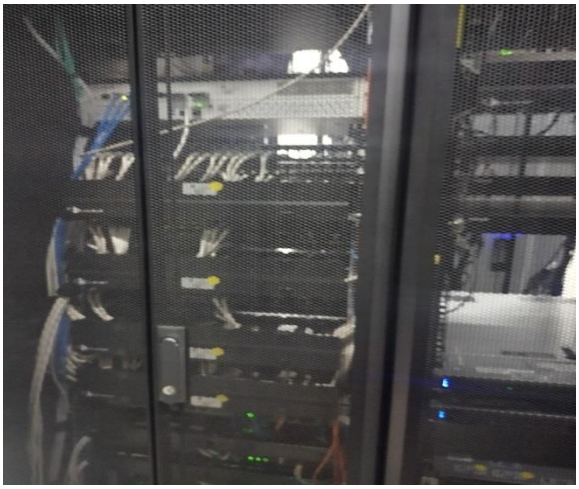
3. Equipo Humano comprometido

   Se resalta el compromiso, responsabilidad, idoneidad y dedicación del equipo de profesionales que conforman el área de recursos tecnológicos para atender los diferentes frentes de servicios que demanda la Unidad.

4. Áreas seguras

   Se observó que la UAECOB cuenta con una recepción donde se controla el ingreso y salida de funcionarios, terceros, y el ingreso y salida de elementos.

Por inspección directa se evidenció que el datacenter o centros de cableado cuenta con mecanismos que cumplen con los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados para los servidores y equipos de comunicaciones que alberga, igualmente cuenta con un sistema para el control de incendios y un mecanismo digital que impide el acceso a personal no autorizado.



Imágenes capturadas al interior del Data Center- Oficina de Control Interno UAECOB- abril de 2023

Se evidenció el contrato de comodato número: CTO – 687-2020 suscrito entre la Secretaría de Seguridad Convivencia y justicia -SSCJ y la UAE Cuerpo Oficial de Bomberos cuyo objeto establece: *Entregar a título de COMODATO, por parte de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá D.C, a la Secretaría de Seguridad, Convivencia y Justicia –SDSCJ un espacio del datacenter, de acuerdo con la capacidad de ocupación, para su USO gratuito y con cargo a restituir los bienes que se mencionan en los Anexos 1 y 2 que hacen parte integral del contrato.*

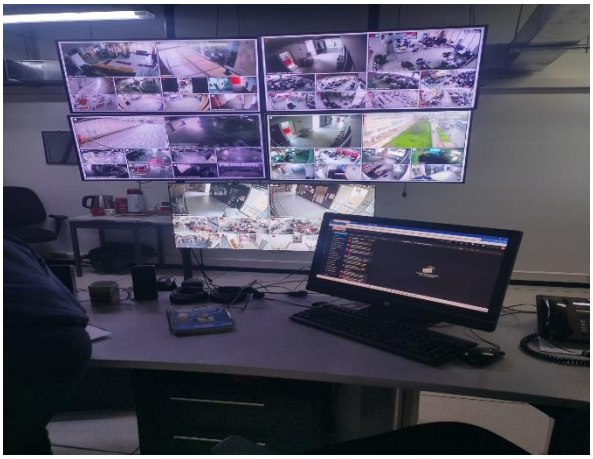
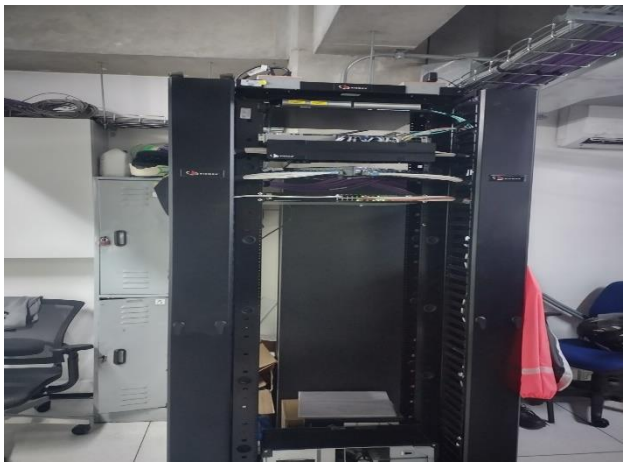
Y en el alcance del objeto establecen: *La UAE Cuerpo Oficial de Bomberos. mantendrá la administración y gestión del espacio restante, 41,94%, el cual se distribuye en un 19,35 % de uso exclusivo de la misma*

entidad y el espacio restante queda disponible para crecimiento a futuro. El espacio utilizado, por parte de la Secretaría de Seguridad, Convivencia y Justicia, será inicialmente del 58,06%, sin embargo, este porcentaje podría variar de conformidad con las necesidades planteadas por las Entidades contratantes.

Lo anterior beneficia a la entidad teniendo en cuenta que solo se ocupa 41,94% de la capacidad instalada y en adelante mientras duré en contrato compartirá el espacio restante con SSCJ quien realizará los pagos proporcionales de las facturas del servicio público de energía eléctrica del Edificio Comando, correspondientes a cubrir los gastos en que se incurra por concepto consumo de energía eléctrica y del mantenimiento preventivo, correctivo y evolutivo de los bienes muebles aportados por la UAECOB*.*

También se observó que la Entidad cuenta con un sistema de seguridad CCTV (Circuito Cerrado de Televisión) para otorgar la mayor seguridad posible tanto a los terceros como a los funcionarios que ingresan a sus instalaciones.



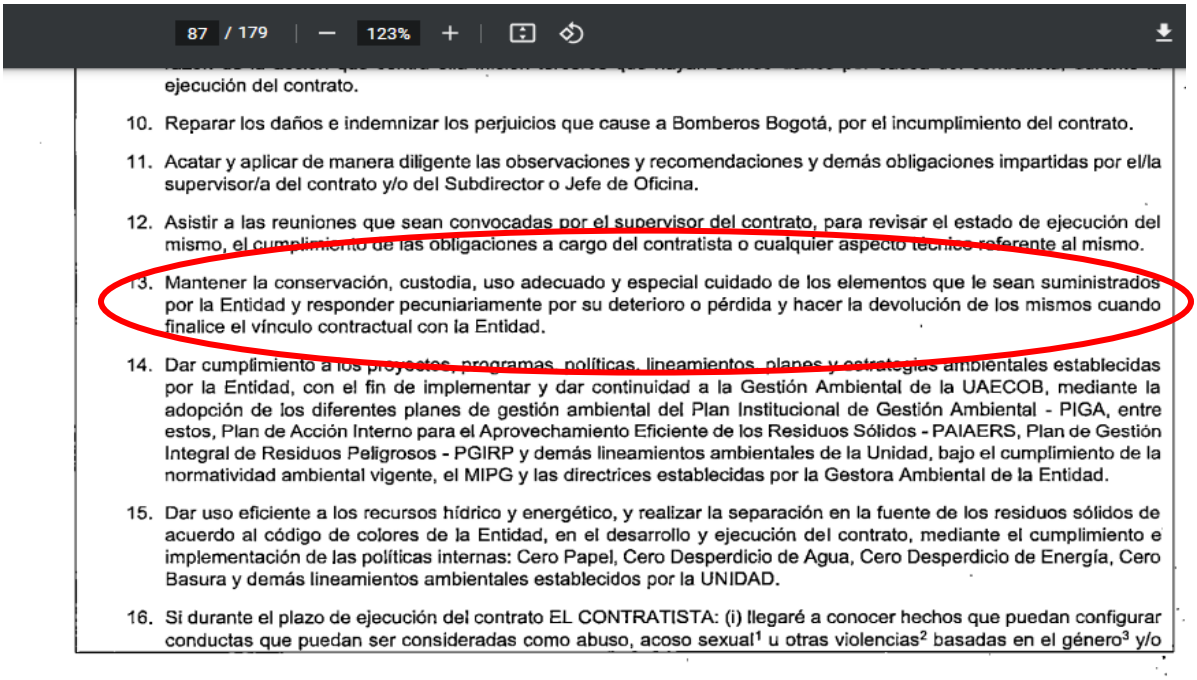
Imágenes capturadas en el Edificio Comando punto de operación del CCTV- Oficina de Control Interno UAECOB- abril de 2023

El profesional que atendió la auditoría por parte del área de tecnología informa que desde esa dependencia se garantiza el funcionamiento del sistema CCTV las 24 horas del día de los 365 días del año, y que con el apoyo de la Subdirección de Gestión Corporativa de la Entidad se garantiza la operación y monitoreo permanente de este sistema, se observa que el acceso al centro de monitoreo es de carácter restringido.

Por observación directa se estableció que el operador de medios tecnológicos del CCTV registra en un libro (bitácora) diariamente cualquier evento ocurrido durante su turno.

DIRECTIVA 008 DE 2021

Se evidenció que la Entidad adoptó incorporar en los contratos de prestación de servicios cláusulas relacionadas con la conservación y uso adecuado de los bienes, servicios y documentos de la Unidad, así como la obligación de responder por su deterioro o pérdida, a manera de ejemplo:



Fuente: Unidad documental CPS 041-2022 suministrada por la Oficina Jurídica UAECOB

También se comprobó que los profesionales del área de tecnología son conscientes de la responsabilidad del manejo y buen uso de la información y la tecnología que se pone a su disposición para el cumplimiento de sus obligaciones contractuales y para ello firman el documento denominado “Acuerdo de confidencialidad y no divulgación de la Información”, lo anterior se corroboró en los contratos 075,416, 375,048,413,047,264,076,386 de 2022

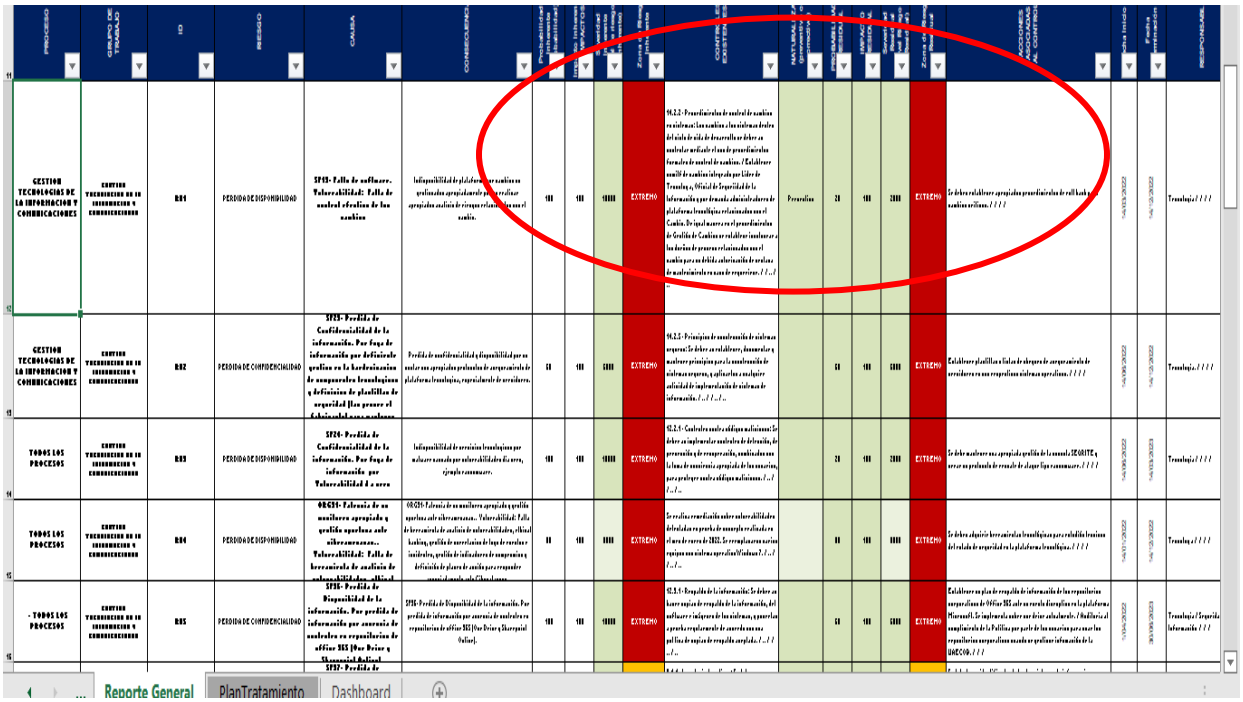
OBSERVACIONES

Aspectos por mejorar

Tomando como referencia la documentación aportada y lo observado dentro del desarrollo de las diferentes sesiones de auditoría, se identifican a continuación los aspectos susceptibles de mejora:

1- Matriz de Riesgos Digitales.

a- Se observó que el área de tecnología tiene identificados trece (13) riesgos digitales, en la matriz establecida describen las amenazas, vulnerabilidades, controles, plan de tratamiento de riesgos, entre otros que se articula con la guía de Gestión de riesgos sugeridas por el Departamento Administrativo de la Función Pública - DAFP dentro del marco de la implementación del Modelo Integrado de Planeación y Gestión – MIPG; de acuerdo a las evidencias aportadas se observa que han venido aplicando los controles establecidos con el fin de mitigar los riesgos, no obstante se observa que el riesgo residual se mantiene en la misma zona en el mapa de calor después de controles, por lo que se recomienda revisar la metodología aplicada toda vez que el objetivo del tratamiento de los riegos es lograr disminuir el impacto, la probabilidad de ocurrencia o las dos en el mejor de los casos.



Fuente: Matriz suministrada por el área de tecnología de la Entidad

Una vez se revise la metodología y se compruebe que los controles son adecuados y, que el riesgo residual permanece en la misma zona en el mapa de calor, es importante que se comunique a la Alta Dirección con el fin de que estos sean tenidos en cuenta en los lineamientos que considere la Entidad para el apetito del riesgo.

Lo anterior con el fin de proteger a la Entidad de cualquier tipo de pérdida o sanción por la materialización de alguno de estos riesgos.

b- Revisados los procedimientos TIC-PR09 Gestión de Vulnerabilidades, TIC-PR05 Gestión de Incidentes Seguridad de la Información TIC-PR04 Copias de Seguridad no se observan que tengas establecidas actividades de control preventivas que mitiguen los riesgos identificados en la matriz de riesgos digitales; importante revisar y en lo posible establecer dentro de los procedimientos los controles que se definieron con el fin de mitigar los riesgos identificados, lo anterior con el fin de no saturar el sistema de seguridad de la información con exceso de documentos y controles y, lograr que con el cumplimiento de los procedimientos se apliquen los controles de manera permanente en el que hacer de la Entidad.

c- Se observó el documento denominado *Plan de Tratamiento de Riesgos de Seguridad Y Privacidad de la Información TIC-PL02* el cual contempla las amenazas (37), vulnerabilidades (66) y riesgos (157) clasificados por tipo (software, hardware, personas, red, información, instalaciones, entre otros) pero no se tiene establecido la declaración de aplicabilidad de los controles lo que dificulta la comprensión y aplicación del mencionado plan. Se recomienda revisar este documento y acotarlo a la realidad de la Entidad con el fin de que sirva de insumo para contribuir con la mejora de la Seguridad de la Información en la UAECOB.

d- Revisado el Manual de Políticas de Seguridad y Privacidad de la Información no se observa una directriz relacionada con la salvaguarda de información que manejan los usuarios de la UAECOB en los equipos de cómputo dispuestos por la Entidad para el cumplimiento de sus labores o actividades, teniendo en cuenta que uno de los riesgos identificados por el área de tecnología *R9 PE09- Indisponibilidad de la información. Causada por alta rotación de personal*, se hace importante que se establezca un lineamiento apropiado para la entrega de información cuando se finalizan los contratos de prestación de servicios o se desvincula un funcionario de la Entidad.

e- Teniendo en cuenta que en la sesión #4 del Comité de Coordinación de Control Interno celebrada el pasado 8 de noviembre de 2022 la jefe de la Oficina Asesora de Planeación informo que tienen identificados trece (13) riegos relacionados con la seguridad de la información, que de estos se tienen cinco (5) riesgos por tratar, principalmente por tema presupuestal y presentan el siguiente cuadro:

Tabla de riesgos no controlados

Id Riesgo	Riesgo	Descripción del riesgo	Activo asociado al riesgo	Riesgo Residual	Acción Asociada al Control
R3	PERDIDA DE DISPONIBILIDAD	SF24- Perdida de Confidencialidad de la información. Por fuga de información por Vulnerabilidad día cero	Sistema Operativo Server	Extremo	Se debe mantener una apropiada gestión de la consola SEQRITE y crear un protocolo de rescate de ataque tipo ransomware.
R6	PERDIDA DE CONFIDENCIALIDAD	SF37- Perdida de Confidencialidad de la información. Por fuga de información en la UAECOB por accesos no autorizados, por la existencia de puertas traseras en plataformas Shadow IT (plataforma obsoleta no controlada y puertos desatendidos).	Plataforma Tecnológica	Alto	Se debe tener identificados todos los sistemas de información y aplicaciones utilizados en todos los procesos. Implementación de la CMDB de Aranda para gestionar todos los activos de información y componentes relacionados. Controlar fechas de vencimiento de garantías, contratos de soporte, certificados digitales, entre otros con alertamiento oportuno. Entre otras bondades de la CMDB.
R7	PERDIDA DE DISPONIBILIDAD	ORG27- Indisponibilidad de la información. Por vencimiento de contrato de suscripción con los proveedores, vigencias de certificados digitales, servicios SaaS, contratos de soporte y mantenimiento, garantías, entre otros.	Software	Alto	Se debe implementar la CMDB donde se pueden controlar los contratos, garantías, suscripciones de seguridad, entre otros. Esto con el fin de gestionar oportunamente los vencimientos de vigencias.

R8	PERDIDA DE DISPONIBILIDAD	ORG28- Indisponibilidad de Servicios por no contar con centro alterno de datos.	Plataforma Tecnológica	Extremo	Se debe establecer centro alterno de datos para replicar la plataforma más critica que soporta los servicios tecnológicos que soportan los procesos críticos de la entidad.
R9	PERDIDA DE CONFIDENCIALIDAD	PE09- Indisponibilidad de la información. Causada por alta rotación de personal.	Personal	Extremo	Establecer Ciclo de Vida de Usuarios. Establecer apropiado procedimiento de entrega de información cuando se entrega puesto de trabajo por vencimiento de contrato. Establecer estrategia para documentar el know how de los funcionarios de Bomberos en todos los procesos. Estrategia de Gestión del Conocimiento.

Fuente: Acta CCCI #4 noviembre 8 de 2022

Teniendo en cuenta lo anterior esta Oficina procedió a revisar el Plan anual de adquisiciones versión 8 vigencia 2023, y no se observa que se tengan destinados recursos para invertir en la adquisición de los servicios que propone el área de tecnología para mitigar los riesgos identificados en el cuadro anterior.

Por lo que se hace importante, que se presente ante el Comité de Coordinación de Control Interno una estrategia que contemple el costo de implementar los controles identificados por el área de tecnología, además que se presente una estrategia alterna para el caso de que no sea posible la consecución de recursos para invertir en el plan de mitigación para los mencionados riesgos.

En cualquier caso, se recomienda que sea este órgano colegiado quien tome la decisión de cuál será la estrategia que adoptará para administrar dichos riesgos y lograr de esta manera proteger a la Entidad en caso de que se llegase a materializar alguno de estos eventos.

2- Indicadores de gestión de seguridad de la Información

Revisada la batería de indicadores para el proceso Gestión Tecnologías de la Información y las comunicaciones, se observa que tiene identificados seis (6) indicadores (2 de impacto, 3 de gestión y 1 sin clasificar), en el tablero de control analizado se observa que definen el resultado satisfactorio de los indicadores cuando es igual o mayor al 86%.

Se observa para el cuarto período de la vigencia 2022 que para el indicador denominado: Gestión de vulnerabilidades de TI este presentó un resultado de avance de 0% y en la casilla de observaciones se lee: No se realizaron nuevo análisis de vulnerabilidades ni se avanzó en remediaciones para el 4to período.

Para los indicadores denominados: Sensibilización en Modelo de Seguridad y Privacidad de la Información y Tratamiento de Riesgos de Seguridad de la Información y Ciberseguridad, el resultado en el 4to período fue del 70%, en la casilla denominada observaciones anotan el análisis del comportamiento de estos, no obstante, no se observa ni el plan de mejoramiento ni en el plan de acción (FOGEDI) que se hayan formulado acciones que ayuden a mejorar el resultado de los citados indicadores.

La relevancia de los indicadores es facilitarle al líder del proceso controlar el comportamiento de los factores críticos en la ejecución de su plan de acción y analizar las tendencias de cambio, con el fin de cumplir con los objetivos y metas previstos y coadyuvar en la toma decisiones a la Alta Dirección.

Otros Aspectos

En el repositorio de información compartido con esta Oficina como soporte de la presente auditoria, se observa la Política de Continuidad del Negocio TIC- PR00 V1 del 14/07/2022 (este documento no se encuentra publicado en la Web de la Entidad) y un documento en borrador denominado "Análisis de impacto al negocio", los dos documentos enfocados a: *Establecer planes que permitan a la UAE Cuerpo Oficial de Bomberos estar preparada para responder a escenarios de interrupción, recuperarse de estos y mitigar los impactos ocasionados, permitiendo la continuidad de los servicios tecnológicos críticos para la operación.*

Teniendo en cuenta que la Entidad en el marco de la Ley 1523 de 2012, actúa en la Gestión del Riesgo con sus componentes más importantes: conocimiento, reducción de riesgos y manejo de eventos adversos, liderado por la Subdirección de Gestión del Riesgo, diseñó la Estrategia Institucional de Respuesta EIR cuyo objetivo es el siguiente: *Organizar, articular y generar mecanismo de funcionalidad del esquema organizacional y procedimental para la atención y administración de emergencias, por parte de las subdirecciones, áreas y grupos Operativos durante y después de las distintas posibles emergencias y así garantizar la prestación de los servicios de la UAE Cuerpo Oficial de Bomberos.*

Como se puede observar las dos estrategias mencionadas apuntan hacia un mismo objetivo, por lo que se hace importante recomendar la articulación de estas con el fin de no generar reprocesos y disminuir todo tipo de costos en los que se podría incurrir al implementarlos desarticuladamente.

RECOMENDACIONES

- Revisar la metodología aplicada a la matriz de riesgos con el fin de lograr que una vez aplicados los controles el riesgo residual disminuya su impacto o su probabilidad de ocurrencia.

- Una vez se revise la metodología y se compruebe que los controles son adecuados y, que el riesgo residual permanece en la misma zona en el mapa de calor, es importante que se comunique a la Alta Dirección con el fin de que estos sean tenidos en cuenta en los lineamientos que considere la Entidad para el apetito del riesgo.

- En lo posible establecer dentro los procedimientos que se tienen para el procesos de Gestión Tecnologías de la Información y las comunicaciones, los controles que se identificaron en el mapa de riesgos de seguridad de la información con el fin de mitigar los riesgos referidos, con lo anterior se evita saturar el sistema de seguridad de la información con exceso de documentos y controles y, lograr que con el cumplimiento de los procedimientos se apliquen los controles de manera permanente en el que hacer de la Entidad.

- Establecer la declaración de aplicabilidad de los controles para el Plan de Tratamiento de Riesgos de Seguridad Y Privacidad de la Información TIC-PL02 y en lo posible revisar el documento con el fin de acotar los riesgos a la realidad de la Entidad.

- Revisar los documentos que hacen parte del proceso de Gestión Tecnologías de la Información y las comunicaciones con el fin de evitar la redundancia normativa y asegurar que los documentos existentes se encuentran actualizados y facilitan la consulta a las partes interesadas.

- Revisar la batería de indicadores existente con el fin de que definan acciones de mejora para aquellos cuyo resultado no fue satisfactorio al finalizar la vigencia 2022, lo anterior con el fin de asegurar el cumplimiento de las metas y objetivos previstos para el proceso en comento.

- Importante costear la implementación de los controles para los cinco (5) riesgos que fueron presentados en el Comité de Coordinación de Control Interno en el mes de noviembre de 2022 y que de acuerdo con lo expuesto se encontraban sin tratamiento, especialmente por temas de recursos financieros, lo anterior con el fin de que sea está instancia la que defina que tratamiento seguir para este caso.

- Importante tener en cuenta las recomendaciones realizadas por el oficial de seguridad de la Entidad, quien en el Informe Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI) de fecha noviembre de 2022 sugiere lo siguiente para la vigencia 2023:

  - *Realizar gestión de vulnerabilidades a través de planes de remediación oportunos.*
  - *Realizar actualizaciones en clasificación de activos de información.*
  - *Realizar actualizaciones en riegos digitales e implementación de planes de tratamiento.*
  - *Mantener el cumplimiento de la política de seguridad de la información y sus directrices.*
  - *Continuar con Estudios de Análisis de Impacto al Negocio a procesos misionales de Riesgos y Logística.*
  - *Capacitar y concientizar permanentemente a los empleados y terceros de la entidad en todo lo relacionados con ISO27001.*
  - *Preservar las evidencias de los requisitos y controles de la ISO27001:2013.*
  - *Continuar con sensibilización en seguridad de la información hasta brindar cobertura al 100% de los funcionarios y contratistas de la Entidad*

CONCLUSION

Con base en la evaluación adelantada por la Oficina de Control Interno y una vez valorados los documentos presentados por los auditados, se puede concluir que la Alta Dirección se encuentra comprometida con la seguridad de la Información, en razón a que ha definido una política de Seguridad y privacidad de la Información y ha dispuesto los distintos recursos financieros, administrativos y técnicos para su implementación y mejora, así como un equipo humano profesional, calificado y comprometido en el área de tecnología, sin embargo se observan aspectos susceptibles de mejora que se presentaron en el capítulo precedente de recomendaciones

Hay que mencionar que desde el área de tecnología de la Entidad y con el apoyo de los líderes de los procesos se lograron implementar requisitos y controles en 71% en el marco de la norma ISO 27001:2013 como se observa en el siguiente cuadro:

No.	Evaluación de Efectividad de controles					
	DOMINIO	Calificación a Jun 30 de 2021	Calificacion a Feb 28 de 2022	Calificacion a Jun 30de 2022	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	90	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	70	65	78	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	82	86	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	19	46	70	100	GESTIONADO
A.9	CONTROL DE ACCESO	41	65	77	100	GESTIONADO
A.10	CRIPTOGRAFÍA	20	60	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	52	67	85	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	36	55	68	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	20	27	58	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	37	61	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	10	20	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	29	57	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	43,5	63,5	100	GESTIONADO
A.18	CUMPLIMIENTO	56	48,5	59	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES SGSI		39	53	71	100	GESTIONADO

Fuente: Informe Sistema de Gestión de seguridad de la información y ciberseguridad (SGSI)-noviembre de 2022-OAP

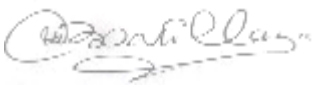
Teniendo en cuenta el resultado anterior se insta a la líder del proceso Gestión Tecnologías de la Información y las comunicaciones en coordinación con la Alta Dirección, para que se continúe con la implementación de los requisitos y controles que aún faltan (29%), hasta lograr al 100% de la implementación del Modelo de Seguridad y Privacidad de la información – MSPI en la Entidad, tal como lo establece la Resolución 500 de 2021 de MINTIC.

EQUIPO AUDITOR

Nombre(s): JAIME HERNANDO ARIAS PATIÑO

Firma (s):
JEFE OFICINA DE CONTROL INTERNO

Nombre: MARÍA DEL CARMEN BONILLA



Firma:
Profesional 219 grado 20-OCI Auditora