RESPONSABLE: Jaime Hernando Arias Patiño

NOMBRE DE LA AUDITORIA/SERVICIO DE ASEGURAMIENTO
Seguridad de la Información en el marco de la norma ISO 27001:2013

OBJETIVO:
Verificar el cumplimiento de lo establecido en el Modelo 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 marco del Modelo de Seguridad y Privacidad de la Información, Manual de Políticas de Seguridad y Privacidad de la Información, Plan Estratégico de Tecnologías de la Información (PETI), procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2 y documentos relacionados, en el periodo comprendido entre el 1 de junio 2024 y el 30 de junio de 2025

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
Decreto Reglamentario 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
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, capítulo 1 artículo 2.1.1.1.1. Este Título tiene por objeto reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública.
DIRECTIVA 008 DE 2021 Seguimiento al cumplimiento de los Manuales de funciones y Competencias Laborales
Modelo Integrado de Planeación y Gestión MIPG.
Modelo de seguridad y privacidad de la información y Plan de gestión de riesgos de seguridad digital de la UAECOB, procedimientos TI

Seguridad de la Información: ISO 27001:2022
Ciberseguridad: ISO 27032 Y Protección de la Privacidad:
ISO 27701 (Ley 1581)
Demás normas que apliquen

PROCESO AUDITADO:

Gestión Tecnologías de la Información y las Comunicaciones

SUBDIRECCIÓN/OFICINA/DEPENDENCIA/ÁREA:

Dirección- TIC

LÍDER DE PROCESO/DEPENDENCIA:

EQUIPO AUDITOR:

Jaime Hernando Arias Patiño- jefe de la OCI
María del Carmen Bonilla- Profesional Especializada OCI

PERIODO DE EJECUCIÓN DE LA AUDITORÍA:

1 de agosto al 30 de septiembre de 2025

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 lainformación 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.

Se inicia al proceso auditor con el oficio *Id: 235031* del 1 de agosto del 2025 mediante el cual se cita a la mesa de apertura de auditoría el día 11 de agosto del 2025, a las 9:00 a.m. la cual se oficiará de manera presencial, con la participación de los auditados y el equipo de trabajo que considere pertinente la líder del proceso auditado, la auditora asignada y el jefe de la Oficina de Control Interno.

Para esta auditoría se contempló el lineamiento establecido mediante el Modelo de Seguridad y Privacidad de la Información, Manual de Políticas de Seguridad y Privacidad de la Información, Plan Estratégico de Tecnologías de la Información (PETI), procedimiento Gestión Incidentes de Seguridad de la Información TIC-PR05 V2, que se encuentran publicados en la página Web de la Entidad.

Se realizó entrevista a los profesionales designados por la líder del proceso Gestión Tecnologías de la Información y las Comunicaciones del cual hace parte el procedimiento auditado, se verificó el mapa de riesgos de seguridad digital.

Se revisó la información reportada en la matriz institucional de reporte de la Gestión denominada FOGEDI para la vigencia 2024 y la información reportada en la herramienta dispuesta para el reporte de la gestión adelantada por las dependencias para la vigencia 2025 la cual se denomina Sinergia App.

Se seleccionaron cuatro dependencias de la Entidad (Oficina Jurídica, Subdirección de Gestión Humana, Oficina Asesora de Planeación y Subdirección de Gestión del Riesgo) con el fin de verificar la apropiación de los lineamientos establecidos desde el área de tecnología en materia de seguridad de la información, con el fin de que este ejercicio sirva de autoevaluación al proceso de Tecnologías de la Información y las comunicaciones, en el marco de lo establecido (instrumento de evaluación MSPI).

También se examinó el plan anual de adquisiciones vigencia 2024 y vigencia 2025 con el fin de constatar la disposición de recursos financieros para cumplir con el plan de acción propuesto para el proceso evaluado.

Durante la ejecución de la auditoria se observaron aspectos positivos que mencionamos a continuación:

Fortalezas

A- El Plan Estratégico de Tecnologías de la Información – PETI y Plan de Seguridad y Privacidad de la Información- PESI fueron presentados en el Comité Institucional de Gestión y Desempeño para su aprobación, según lo corroborado en el acta No. 1 del 29 de enero del 2024 y el acta No. Del 296 de enero del 2025, se encuentran publicados en la página Web de la Entidad, en cumplimiento a lo establecido en la Ley de Transparencia y acceso a la información pública.

B- Los profesionales que atendieron la auditoria mostraron buena disposición y diligencia durante el tiempo que duró el ejercicio auditor.

C- **Directiva 008 de 2021**– Alcaldía Mayor de Bogotá DC

En cuanto a la citada directiva que contempla “Lineamientos para prevenir conductas irregulares relacionadas con el incumplimiento de los manuales de funciones y competencias laborales y de los manuales de procedimientos institucionales, así como por la perdida, o deterioro, o alteración o uso indebido de bienes, elementos, documentos públicos e información contenida en bases de datos y sistemas de información”, se observó en las minutas de los contratos 322 y el 217 del 2025 que corresponden a profesionales que prestan sus servicios en la Dirección específicamente al proceso Gestión Tecnologías de la Información y las Comunicaciones que se incluyó una obligación general relacionada con :

13. Mantener la conservación, custodia, uso adecuado y especial cuidado de los elementos que le sean

suministrados por la Entidad y responder pecuniariamente por su deterioro o pérdida y hacer la devolución de los mismos cuando finalice el vínculo contractual con la Entidad.

Para las obligaciones específicas incluyeron las siguientes:

12. Guardar la confidencialidad de toda la información que conozca durante la ejecución del contrato.

14. Almacenar en los repositorios dispuestos por la entidad, toda la información, creaciones intelectuales u obras desarrolladas con ocasión a las obligaciones contractuales. Lo anterior, teniendo en cuenta que la Entidad es titular de los derechos patrimoniales sobre las creaciones intelectuales u obras, cuando sean producidos por un contratista o tercero como parte de sus obligaciones contractuales.

Lo anterior nos permite deducir que la Entidad ha venido dando cumplimiento con lo establecido en la mencionada Directiva.

SITUACIONES GENERALES

El objetivo del proceso Tecnologías de la Información y las comunicaciones de la Entidad establece: "Generar e implementar soluciones estratégicas y proyectos de optimización, para el cumplimiento de los fines misionales de la UAECOB, apoyados en los lineamientos, estándares y mejores prácticas de Tecnologías de la Información y las comunicaciones de acuerdo con el modelo de arquitectura definido por MINTIC y demás organismos, comunicando la información pertinente y relevante para la entidad"

1- Para dar cumplimiento al objetivo del proceso, la Entidad adopta entre otros los siguientes lineamientos:

a- Manual de Políticas de Seguridad y Privacidad de la Información versión 2

Objetivo
Establecer las políticas específicas de seguridad y privacidad de la información que permitan reducir amenazas y vulnerabilidades de los activos de información de la Unidad Administrativa Especial Cuerpo Oficial Bomberos de Bogotá (UAECOB), enfocadas en afianzar los principios de confidencialidad, disponibilidad e integridad de la información, con el fin de asegurar la continuidad del negocio y gestionar los riesgos asociados interpretado conforme los términos de la norma ISO 22301 sobre las buenas prácticas.

b- Plan Estratégico de Tecnologías de la Información – PETI para las vigencias 2024 aprobado en el Comité Institucional de Gestión y Desempeño en la sesión No. 1 del 29 de enero del 2024 y para la vigencia 2025 aprobado en la sesión No.1 del 29 de enero del 2025

Objetivo -2024
Construir la ruta para implementar la gestión estratégica de tecnología de la información y que se convierta en elemento facilitador para el cumplimiento de los logros y metas de la Entidad a través de los lineamientos de la política de gobierno digital relacionados con el uso y operación de los servicios ciudadanos digitales.
El cual fue construido siguiendo la metodología propuesta por Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC en la Guía G.ES.06

Objetivo -2025
Plantear una estrategia para el proceso de las TIC a cargo de la Dirección en la vigencia 2025 al 2027, soportada en las buenas prácticas de Seguridad Digital y Arquitectura Empresarial para establecer un modelo de Gestión de TI que responda a las necesidades de información, de infraestructura tecnológica,

modelo operativo, procesos y procedimientos propios de la Unidad Administrativas Especial Cuerpo Oficial de Bomberos de Bogotá (UAECOB), para el cumplimiento de sus objetivos estratégicos, así como aquellas que surjan para el direccionamiento institucional y las alineadas a la Política de Seguridad Digital y Gobierno Digital como eje de desarrollo institucional en la Entidad."

"Esto, alineado con las políticas de Gobierno Digital y Seguridad Digital, logrando el estado de madurez tecnológica para avanzar hacia la total digitalización de trámites y servicios que presta de la UAECOB."

c- Plan de Seguridad y Privacidad de la Información- PESI vigencia 2024 aprobado en el Comité Institucional de Gestión y Desempeño en la sesión No. 1 del 29 de enero del 2024 y para la vigencia 2025 aprobado en la sesión No. 1 del 29 de enero del 2025

Objetivo 2024

Definir las actividades necesarias para implementar y apropiar el Modelo de Seguridad y privacidad de la información para brindar confianza a los grupos de valor en cuanto al tratamiento de la información basado en la gestión de riesgos de seguridad y privacidad con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información.

Objetivo 2025

Definir la estrategia de seguridad de la información y ciberseguridad en adelante PESI liderada por la alta dirección apoyado y alineado su cumplimiento con el plan estratégico de LA UAECOB, respondiendo a la necesidad de preservar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los activos de información.

Disminuir el nivel de riesgos que responda a las necesidades de preservar la confidencialidad, la integridad, la disponibilidad, autenticidad y no repudio sobre los activos de información, priorizando su nivel de criticidad.

d- Plan de tratamiento de riesgos

Objetivo

Implementar una herramienta para la gestión de riesgos de Seguridad y Privacidad de la información con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y desarrollar de manera adecuada los procesos misionales, estratégicos y administrativos.

De acuerdo con lo establecido en el Decreto 612 de 2018, la creación del Plan de Tratamiento de Riesgos de Seguridad Digital debe estar alineado con la Planeación Estratégica Institucional

e- Procedimiento Gestión Incidentes de Seguridad de La Información- *TIC-PR05 versión 2*

Objetivo:

Definir las actividades para gestionar los incidentes de seguridad y privacidad de la información, teniendo en cuenta los lineamientos y estándares definidos, a través de una oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la Unidad Administrativa Especial Cuerpo Oficial de Bomberos.

Con el fin de verificar el cumplimiento de las actividades propuestas en el Plan Estratégico de Tecnologías de Información (PETI) y el Plan de Seguridad y Privacidad de la Información (PESI) se solicitó al área de tecnología de la Entidad allegar las evidencias que dieran cuenta de la ejecución de las gestiones realizadas entre el 1 de junio 2024 y el 30 de junio de 2025 observando lo siguiente:

PETI segundo semestre del 2024:

Para el segundo semestre propusieron las siguientes actividades:

Cuadro 1

Plan Versión final	Fecha fin Estimada	Producto o entregable	% de cumplimiento
1-Uso y Apropiación del Plan de Respuesta a Incidentes Informáticos	I/II/III/IV Trimestre 2024	GAP análisis actualizado en herramienta MSPI del SGSI y GAP de Ciberseguridad.	65%
2-Herramientas con Inteligencia Artificial Fortalecer el uso de la herramienta Office 365- Power BI	III Trimestre 2024	Certificados de asistencia a capacitaciones en seguridad de la información y ciberseguridad.	70%
3-Actualizar activos de información de todos los procesos de la Entidad	III Trimestre 2024	Informes de auditorías a terceros.	35%
4-Continuar con la actualización tecnológica de la estación de Marichuela Participar y generar los requerimientos técnicos y tecnológicos en la construcción de la nueva estación Ferias	III Trimestre 2024	Informes de resultados de pruebas realizadas.	50%
5-Adquisición de equipos de audio y video para la producción audio visual	IV trimestre del 2024	Contrato ejecutado	55%
6-Alcanzar un nivel de madurez optimizado en el Modelo de Seguridad y Privacidad de la Información	IV trimestre del 2024	La UAECOB se encuentra directamente realizando actividades de soporte de la herramienta, en ambos módulos (Portal de Servicios y emergencias). El propósito para el 2025, es validar con las tecnologías emergentes optimizar las herramientas misionales con la finalidad que la data mejore la toma de decisiones a los directivos.	100%
		Cumplimiento segundo semestre del 2024	63%

Las actividades propuestas en este Plan se confrontaron contra la matriz de Fortalecimiento de la Gestión Institucional FOGEDI, herramienta que dispuso la entidad para reportar los avances de las gestiones adelantadas de los planes, proyectos y políticas establecidas y, se evidenció lo siguiente:

Actividades PETI reportadas en la FOGEDI 2024

Cuadro 2

1-Fortalecimiento del soporte, mejora continua, funcionales y administración del Sistema FUOCO. Coordinar con las demás áreas que participan en la implementación de FUOCO, las campañas de uso y apropiación del sistema	100%
2-Continuar con la actualización tecnológica de la estación de Marichuela	100%

3-Herramientas con Inteligencia Artificial Fortalecer el uso de la herramienta Office 365- Power BI	100%
4-Adquisición de equipos de audio y video para la producción audio visual	100%
5-Soportar, mantener y dar continuidad a los servicios de infraestructura tecnológica y de comunicaciones	100%
6-Actualizar el catálogo de servicios de TI	100%
Cumplimiento 2024	**100%**

Fuente: TIC- UAECOB

Se observa en el reporte un cumplimiento del 100% de las actividades propuestas.

Las actividades que se resaltaron en el cuadro 1 y 2 coinciden, las actividades 1, 3 y 6 (cuadro1) propuestas y aprobadas en Comité de Gestión y Desempeño PETI, no se monitorearon en la FOGEDI, es decir no se presentaron resultados periódicos de los avances de la gestión con el fin de dar cumplimiento a las actividades propuestas.

No se observa consistencia en la información reportada en las diferentes herramientas de Gestión que dispone la Entidad para dar cuenta de las actividades adelantada por las dependencias, lo que dificulta establecer el grado de cumplimiento de los compromisos pactados para el PETI 2024.

No obstante, esta oficina verificó las evidencias allegadas y, concluyó un avance para la vigencia 2024 del **81,5%**

Recomendamos para las actividades que no alcanzaron la meta (100%), continuarlas en la vigencia 2025.

En cuanto al **Plan de Seguridad y Privacidad de la Información- PESI** 2do. Semestre 2024 se evidenció lo siguiente:

Cuadro 3

PESI	% de cumplimiento
Uso y Apropiación del Plan de Respuesta a Incidentes Informáticos	65%
Herramientas con Inteligencia Artificial Fortalecer el uso de la herramienta Office 365- Power BI	70%
Actualizar activos de información de todos los procesos de la Entidad	35%
Continuar con la actualización tecnológica de la estación de Marichuela Participar y generar los requerimientos técnicos y tecnológicos en la construcción de la nueva estación Ferias	50%
Adquisición de equipos de audio y video para la producción audio visual	55%
Alcanzar un nivel de madurez optimizado en el Modelo de Seguridad y Privacidad de la Información	100%
Cumplimiento 2do. Semestre del 2024	**63%**

Fuente: TIC- UAECOB

Las actividades propuestas en este Plan se confrontaron contra la matriz de Fortalecimiento de la Gestión Institucional FOGEDI, herramienta que dispuso la entidad para reportar los avances de las gestiones adelantadas de los planes, proyectos y políticas establecidas y, se evidenció lo siguiente:

Actividades establecidas en la FOGEDI 2024- PESI

Cuadro 4

Actividad de gestión	Resultado de la vigencia
Destinar recursos económicos y humanos para la seguridad y privacidad de la información	100%
Uso y Apropiación del Plan de Respuesta a Incidentes Informáticos	100%
Actualizar activos de información de todos los procesos de la Entidad	100%
Alcanzar un nivel de madurez optimizado en el Modelo de Seguridad y Privacidad de la Información	100%
Estrategia de Uso y apropiación de las políticas y procedimientos de seguridad y privacidad de la información	100%

Fuente: TIC- UAECOB

Se observa en el reporte un cumplimiento del 100% de las actividades propuestas.

Las actividades que se resaltaron en el cuadro 3 y 4 coinciden, las demás propuestas y aprobadas en Comité de Gestión y Desempeño no se monitorearon en la FOGEDI, es decir no se presentaron resultados periódicos de los avances de la gestión con el fin de dar cumplimiento a las actividades propuestas.

No se observa consistencia en la información reportada en las diferentes herramientas de Gestión que dispone la Entidad para dar cuenta de las actividades adelantada por las dependencias, lo que dificulta establecer el grado de cumplimiento de los compromisos pactados para el PESI 2024.

No obstante, esta oficina verificó las evidencias allegadas y, concluyó un avance para la vigencia 2024 del **81,5%**

Recomendamos para las actividades que no alcanzaron la meta (100%), continuarlas en la vigencia 2025.

PETI primer semestre del 2025

Para la vigencia 2025 proponen en el plan aprobado por el Comité Institucional de Gestión y Desempeño ejecutar catorce actividades como se observa a continuación y reportan el avance (% de cumplimiento):

Cuadro 5

No.	Actividad	% de cumplimiento
1	Formular e implementar el PETI y transformación digital	100%
2	Adquirir de servicio de monitoreo, control y seguimiento satelital a los vehículos de la UAECOB	100%
3	Adquirir servicios de nube pública	100%
7	Contratar la renovación del licenciamiento y soporte de las plataformas de seguridad perimetral Fortinet, firewalls y WAF	100%
8	Contratar adquisición, actualización tecnológica, soporte y mantenimiento preventivo y correctivo con repuestos para los sistemas de video vigilancia	20%
9	Adquisición de software para análisis de vulnerabilidades	30%
10	Contratar el servicio de mantenimiento preventivo y correctivo de los radios portátiles y móviles marca Motorola	100%
11	Control de acceso a las instalaciones y áreas restringidas de la UAECOB	100%

12	Adquisición de sistemas de monitoreo para la prevención y alertas tempranas en lo que corresponde a forestales	15%
13	Adquisición de antenas servicios de Internet Satelital	100%
14	Contratar la adquisición de tarjetas de comunicación satelital de voz	40%
Avance corte 30 de junio del 2025		**73%**

Fuente: TIC- UAECOB

La Oficina de Control interno verificó las evidencias allegadas por el área de TIC que dan cuenta de las actividades adelantadas para cumplir con los compromisos pactados y encontró conformidad.

PESI primer semestre del 2025

Cuadro 6

No.	Actividad	% de cumplimiento
1	Fortalecimiento del MSPI	73%
2	Fortalecimiento del sistema de seguridad adaptativo	90%
3	Implementar un DRP	50%
4	Implementar herramienta uso de las redes	100%
5	Implementar herramienta y procedimiento para desarrollo seguro	50%
6	Licenciamiento de Microsoft 365, gestión avanzada de identidades y accesos MFA	100%
	Porcentaje de avance al corte del 30 de junio del 2025	77%

Fuente: TIC- UAECOB

Esta oficina verificó las evidencias allegadas por el área de TIC que dan cuenta de la ejecución de las actividades pactadas y encontró conformidad.

La información observada en los cuadros 5 y 6 se cotejó contra la reportada en herramienta gestión de dispuesta por la Entidad para la vigencia 2025 denominada Sinergia App y se observó lo siguiente:

Cuadro 7

Código	Actividad	Avance II trimestre	Avance I trimestre	Promedio
252188	Proponer un plan de trabajo y el desarrollo de sus actividades al sistema de seguridad de la información, bajo la norma ISO27001-2022	25,00%	10,00%	35%
252192	Proponer un plan de trabajo para la actualización de los activos de la información de la entidad.	25,00%	10,00%	35%
252193	Optimizar y renovar las soluciones tecnológicas en los procesos que se requieran para el fortalecimiento institucional de la UAECOB.	25,00%	10,00%	35%
252189	Implementar el Plan Estratégico de Tecnologías de Información y las Comunicaciones-PETI ajustados a los requisitos del MIPG	20,00%	10,00%	30%
252190	Implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información ajustados a los requisitos del MIPG	25,00%	10,00%	35%

252191	Implementar el Plan de Seguridad y Privacidad de la información PESI ajustados a los requisitos del MIPG	25,00%	10,00%	35%
252187	Construir un plan de contingencia en caso de que la entidad reciba (sufra) un ataque cibernético y/o fallas permanentes de conexión.	25,00%	10,00%	35%
	Promedio de avance al corte del 30 de junio			**34%**

Fuente: Oficina Asesora de Planeación

Tal como se observa en el cuadro 7, el avance de los compromisos pactados por el proceso TIC para el primer semestre del 2025 es del **34%**, lo que a criterio de esta oficina es satisfactorio teniendo en cuenta que el proceso propuso como meta para el primer semestre del año 2025 el 35% para cada actividad.

Se recomienda revisar la declaración de las actividades establecidas en el PETI y PESI vigencia 2025 aprobados por el Comité de Gestión y Desempeño, contra las que se dispusieron en la herramienta gestión denominada Sinergia App, con el fin de que coincidan o que sean de fácil identificación para facilitar la interpretación del cumplimiento de los mencionados planes.

2- Plan anual de adquisiciones vigencia 2025

Se evidencia en el reporte realizado por la Oficina Asesora de Planeación denominado “Mesa de Seguimiento y Control Presupuestal” con fecha de corte 30 de junio del 2025 que el proceso de Gestión de Tecnologías de la Información y las comunicaciones tiene compromisos con dos metas en el proyecto 8126 denominado Fortalecimiento Institucional de la UAECOB para un gobierno con fiable Bogotá D.C así:

Cuadro 8

ACTIVIDAD PROYECTO UAECOB	PROGRAMADO	COMPROMISO / CONTRATADO	% RECURSO	META PROGRA.	AVANCE META
05 - Desarrollar 100% de las acciones asociadas al fortalecimiento de la infraestructura tecnológica y de comunicaciones de la UAECOB	2.480,69	1.724,95	69,50%	100	59,58
06 - Formular e Implementar 1 Plan(es) estratégico de tecnologías de la información y transformación digital de la UAECOB	530,21	255,71	48,20%	0,3	0,19
06 - Implementar 1 Sistema(s) de monitoreo y seguimiento a incidentes y emergencias para Bogotá, incluyendo cerros orientales	495	340,6	68,80%	0,3	0,12
07 - Actualizar e implementar 100 %del plan anual de seguridad y privacidad de la información	522,67	333,64	63,80%	100	65,5

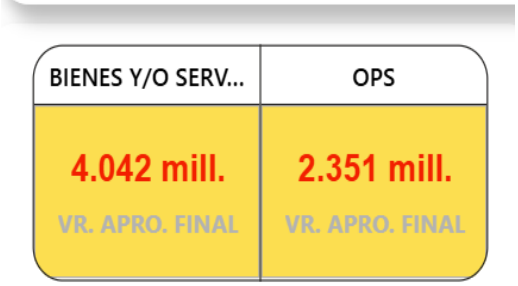
Fuente: Oficina Asesora de Planeación- Sinergia App- corte 30 de junio del 2025

Cuadro 9

DEPENDENCIA	VR. APRO. INICIAL	REDUCCIÓN	VR. APRO. FINAL	VR. NETO CRP	% CRP	GIROS
Dirección Tic	6.265 mill.	0 mill.	6.265 mill.	5.086 mill.	81,20%	2.545 mill.

Fuente: Oficina Asesora de Planeación- Sinergia App- corte 30 de junio del 2025

Imagen 1



Fuente: Oficina Asesora de Planeación- Sinergia App

Lo observado en los cuadros 8 y 9, muestra que el área de TIC ha venido ejecutando los recursos asignados con el fin de cumplir con los objetivos del proceso Tecnologías de la Información y las comunicaciones; lo que confirma el liderazgo y compromiso de la Alta Dirección con respecto al Sistema de Gestión de la Seguridad de la Información.

3- Matriz de Riesgos Digitales.

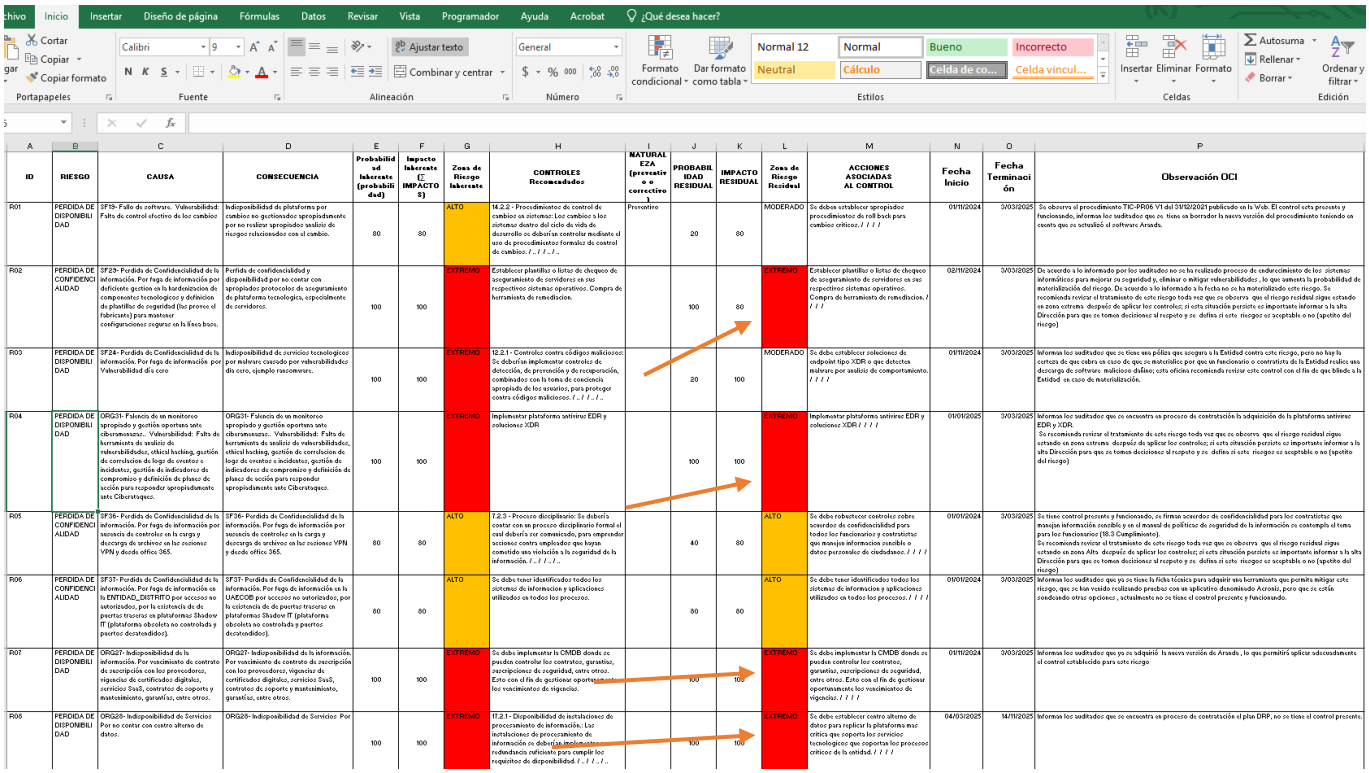
En el documento denominado Plan de Tratamiento de Riesgos versión 1 del 29 de enero del 2025, publicado en la página Web de la Entidad mencionan:

*El nivel de madurez de implementación del Modelo de Seguridad y Privacidad de la Información- MPSI, en la Unidad corresponde al **nivel 1 Inicial**, lo que implica que: a) Se han identificado las debilidades en la seguridad de la información. b) Los incidentes de seguridad de la información se tratan de forma reactiva. c) Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.*

Así las cosas, esta Oficina verificó la matriz de riesgos digitales establecida para la Entidad y observó lo siguiente:

a- 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 responde a l*a* metodología adoptada para la gestión de riesgos de seguridad de la información está definida en la norma técnica ISO 27005 y 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 revisadas se deduce que han venido aplicando los controles establecidos con el fin de mitigar los riesgos, no obstante se observa que para los riesgos R2, R4, R7 y R8 el riesgo residual se mantiene en la misma zona en el mapa de calor después de controles (extremo), 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.

Imagen 2



ID	RIESGO	CAUSA	CONSECUENCIA	Probabilidad Inherente (probabilidad)	Impacto Inherente (IMPACTO S)	Zona de Riesgo Inherente	CONTROLES Recomendados	NATURALEZA (preventivo o correctivo)	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	Zona de Riesgo Residual	ACCIONES ASOCIADAS AL CONTROL	Fecha Inicio	Fecha Terminación	Observación OCI
R01	PERDIDA DE DISPONIBILIDAD	SF59- Falla de software. Vulnerabilidad: Falta de control efectivo de los cambios	Indisponibilidad de plataforma por cambios no gestionados apropiadamente por no realizar apropiados análisis de riesgos relacionados con el cambio.	80	80	ALTO	14.2.2 - Procedimientos de control de cambios en sistemas: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios. / ../ ../..	Preventivo	20	80	MODERADO	Se debes establecer apropiados procedimientos de roll back para cambios críticos. / / / /	01/11/2024	5/03/2025	Se observa el procedimiento TIC-PR06 V1 del 31/12/2021 publicado en la Web. El control sets presente y funcionando, informan los auditados que ya tiene en borrador la nueva versión del procedimiento teniendo en cuenta que ya actualizó el software Aranda.
R02	PERDIDA DE CONFIDENCIALIDAD	SF29- Perdida de Confidencialidad de la información. Por fuga de información por deficiente gestion en la hardenización de componentes tecnológicos y definición de plantillas de seguridad (las provee el fabricante) para mantener configuraciones seguras en la líneas base.	Perfida de confidencialidad y disponibilidad por no contar con apropiados protocolos de aseguramiento de plataforma tecnológica, específicamente de servidores.	100	100	EXTREMO	Establecer plantillas o listas de chequeo de aseguramiento de servidores en sus respectivos sistemas operativos. Compra de herramienta de remediacion.		100	80	EXTREMO	Establecer plantillas o listas de chequeo de aseguramiento de servidores en sus respectivos sistemas operativos. Compra de herramienta de remediacion. / / / /	02/11/2024	5/03/2025	De acuerdo a lo informado por los auditados no se ha realizado proceso de endurecimiento de los sistemas informáticos para mejorar su seguridad y, eliminar o mitigar vulnerabilidades , lo que aumenta la probabilidad de materialización del riesgo. De acuerdo a lo informado a la fecha no se ha materializado este riesgo. Se recomienda revisar el tratamiento de este riesgo toda vez que se observa que el riesgo residual sigue situado en zona extrema después de aplicar los controles; si esta situación persiste es importante informar a la alta Dirección para que se tomen decisiones al respecto y se defina si este riesgo es aceptable o no (apetito del riesgo)
R03	PERDIDA DE DISPONIBILIDAD	SF24- Perdida de Confidencialidad de la información. Por fuga de información por Vulnerabilidad día cero	Indisponibilidad de servicios tecnologicos por malware causado por vulnerabilidades día cero, ejemplo ransomware.	100	100	EXTREMO	12.2.1 - Controles contra códigos maliciosos: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. / ../ ../..		20	100	MODERADO	Se debe establecer soluciones de endpoint tipo XDR o que detectes malware por análisis de comportamiento. / / / /	01/11/2024	5/03/2025	Informan los auditados que ya tiene una póliza que asegura a la Entidad contra este riesgo, pero no hay la certeza de que cubra en caso de que se materialice por que un funcionario o contratista de la Entidad realice una descarga de software malicioso dañino; esta oficina recomienda revisar este control con el fin de que blinde a la Entidad en caso de materialización.
R04	PERDIDA DE DISPONIBILIDAD	ORG31- Falencia de un monitoreo apropiado y gestión oportuna ante ciberamenazas.. Vulnerabilidad: Falta de herramients de analisis de vulnerabilidades, ethical hacking, gestión de correlacion de logs de creantes o incidentes, gestión de indicadores de compromiso y definición de planes de acción para responder apropiadamente ante Ciberataques.	ORG31- Falencia de un monitoreo apropiado y gestión oportuna ante ciberamenazas.. Vulnerabilidad: Falta de herramients de analisis de vulnerabilidades, ethical hacking, gestión de correlacion de logs de creantes o incidentes, gestión de indicadores de compromiso y definición de planes de acción para responder apropiadamente ante Ciberataques.	100	100	EXTREMO	Implementar plataforma antivirus EDR y soluciones XDR		100	100	EXTREMO	Implementar plataforma antivirus EDR y soluciones XDR / / / /	01/01/2025	5/03/2025	Informan los auditados que se encuentra en proceso de contratación la adquisición de la plataforma antivirus EDR y XDR. Se recomienda revisar el tratamiento de este riesgo toda vez que se observa que el riesgo residual sigue situado en zona extrema después de aplicar los controles; si esta situación persiste es importante informar a la alta Dirección para que se tomen decisiones al respecto y se defina si este riesgo es aceptable o no (apetito del riesgo)
R05	PERDIDA DE CONFIDENCIALIDAD	SF36- Perdida de Confidencialidad de la información. Por fuga de información por ausencia de controles en la carga y descarga de archivos en las instancias VPN y drives office 365.	SF36- Perdida de Confidencialidad de la información. Por fuga de información por ausencia de controles en la carga y descarga de archivos en las instancias VPN y drives office 365.	80	80	ALTO	7.2.3 - Proceso disciplinario: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. / ../ ../..		40	80	ALTO	Se debe robustecer controles sobre acuerdos de confidencialidad para todos los funcionarios y contratistas que manejen información sensible o datos personales de ciudadanos. / / / /	01/01/2024	5/03/2025	Se tiene control presente y funcionando, se firman acuerdos de confidencialidad para los contratistas que manejan información sensible y en el manual de políticas de seguridad de la información se contempla el tema para los funcionarios (R8.3 Cumplimiento). Se recomienda revisar el tratamiento de este riesgo toda vez que se observa que el riesgo residual sigue situado en zona Alta después de aplicar los controles; si esta situación persiste es importante informar a la alta Dirección para que se tomen decisiones al respecto y se defina si este riesgo es aceptable o no (apetito del riesgo)
R06	PERDIDA DE CONFIDENCIALIDAD	SF37- Perdida de Confidencialidad de la información. Por fuga de información en la ENTIDAD_DISTRITO por accesos no autorizados, por la existencia de de puertas traseras en plataformas Shadow IT (plataforma obsoleta no controlada y puertos desatendidos).	SF37- Perdida de Confidencialidad de la información. Por fuga de información en la UAECOB por accesos no autorizados, por la existencia de de puertas traseras en plataformas Shadow IT (plataforma obsoleta no controlada y puertos desatendidos).	80	80	ALTO	Se debe tener identificados todos los sistemas de información y aplicaciones utilizados en todos los procesos.		80	80	ALTO	Se debe tener identificados todos los sistemas de información y aplicaciones utilizados en todos los procesos. / / / /	01/01/2024	5/03/2025	Informan los auditados que ya se tiene la ficha técnica para adquirir una herramienta que permita mitigar este riesgo, que se han venido realizando pruebas con un aplicativo denominado Acronis, pero que se están sondeando otras opciones , actualmente no se tiene el control presente y funcionando.
R07	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.	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.	100	100	EXTREMO	Se debe implementar la CMDB donde se puedan controlar los contratos, garantías, suscripciones de seguridad, entre otros. Esto con el fin de gestionar oportunamente los vencimientos de vigencias.		100	100	EXTREMO	Se debe implementar la CMDB donde se puedan controlar los contratos, garantías, suscripciones de seguridad, entre otros. Esto con el fin de gestionar oportunamente los vencimientos de vigencias. / / / /	01/11/2024	5/03/2025	Informan los auditados que ya se adquirió la nueva versión de Aranda , lo que permitirá aplicar adecuadamente el control establecido para este riesgo
R08	PERDIDA DE DISPONIBILIDAD	ORG28- Indisponibilidad de Servicios Por no contar con centro alterno de datos.	ORG28- Indisponibilidad de Servicios Por no contar con centro alterno de datos.	100	100	EXTREMO	17.2.1 - Disponibilidad de instalaciones de procesamiento de información.: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. / ../ ../..		100	100	EXTREMO	Se debe establecer centro alterno de datos para replicar la plataforma mas critica que soporta los servicios tecnológicos que soportan los procesos criticos de la entidad. / / / /	04/03/2025	14/11/2025	Informan los auditados que se encuentra en proceso de contratación el plan DRP, no se tiene el control presente.

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 tengan 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 quehacer de la Entidad. Esta observación se realizó en la auditoría realizada por la OCI a la Seguridad de la Información en la vigencia 2023, no se observa que se haya realizado la mejora correspondiente.

c- En 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), muestran la matriz con los trece (13) riesgos identificados para la Entidad y las acciones asociadas al control 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 en lo posible

describir los controles con el fin que sirva de directriz a los profesionales que trabajan en el área de tecnología con el tema de seguridad de la información y asegurar de esta manera que se apliquen, estén presentes, funcionando y perduren con el tiempo.

4- Indicadores de gestión de seguridad de la Información

Revisada la batería de indicadores que reporta la Entidad al Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC y a la Alta Consejería del Distrito con fechas de corte 31 de diciembre del 2024 y 30 de junio del 2025, se observa que se identificaron catorce (14) indicadores que miden el desempeño de los lineamientos establecidos para el cumplimiento de lo establecido en la ISO 27001:2013, y cinco indicadores de ciberseguridad en el marco de la ISO 27032:2012 que hacen parte del MSPI, para el segundo semestre de la vigencia la medición se realizará en el marco de la ISO 27001:2022, fecha en la cual entre en vigencia en nuevo modelo de seguridad y privacidad de la información con la resolución 02277 del 3 de junio del 2025 del MINTIC. Se realizó presentación del resultado de los indicadores a corte del 30 junio del 2025 en el CIGD.

Se observa que todos los indicadores presentaron resultados positivos es decir mejora la medición de junio con respecto a diciembre del 2024.

No se observa que se tenga el comité técnico de seguridad y privacidad de la información lo que ha retrasado la gestión para agilizar la aprobación de los lineamientos establecidos es el caso del Plan de Gestión de Crisis el cual no ha sido aprobado por el CIGD, no obstante, se observa un indicador de gestión denominado A17 Aspectos de la Seguridad de la Información de la Continuidad del Negocio.

Teniendo en cuenta que es un proceso transversal se recomienda que se conforme el comité técnico de seguridad y privacidad de la información con un integrante como mínimo por dependencia en lo posible que sea de planta, con el fin de asegurar la permanencia en el tiempo y se logre a cabalidad el cumplimiento de los lineamientos establecidos.

Para los indicadores denominados: A13 Seguridad de las Comunicaciones (75%), A14 Adquisición, Desarrollo y Mantenimiento de Sistemas (67%), A15 Relación con los proveedores (70%), A16 Gestión de incidentes de Seguridad de la Información (74%), A17 Aspectos de la Seguridad de la Información de la Continuidad del Negocio (73,5) y A18 Cumplimiento (79%) se observa en la imagen 3 que el resultado de la medición se encuentra por debajo del 80% y la calificación objetivo que propone el área de TIC es del 100%; por lo anterior se hace importante que se formule un plan de mejoramiento o un plan de acción que ayude 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.

Imagen 3

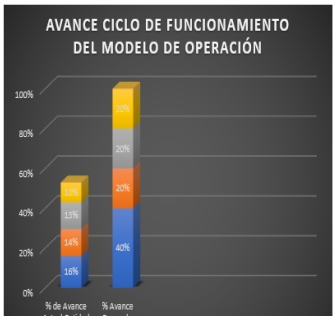
ELABORADO POR	Jose Hernan Morales Muñoz

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles						
	DOMINIO	Calificación a Mayo de 2024	Calificacion a Nov 15 de 2024	Calificacion a Dic 31 de 2024	Calificación a Junio/2025	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	70	90	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	78	45	78	82	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	89	66	86	89	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	75	58	77	89	100	GESTIONADO
A.9	CONTROL DE ACCESO	77	76	68	82	100	GESTIONADO
A.10	CRIPTOGRAFÍA	80	80	80	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	84	67	75	86	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	68	81	82	85	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	58	78	70	75	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	61	56	64	67	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	50	20	70	70	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	57	29	54	74	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	63,5	43,5	50	73,5	100	EFECTIVO
A.18	CUMPLIMIENTO	59	48,5	65	79	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES SGSI		71	58	72	81	100	GESTIONADO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
20XX	Planificación	16%	40%
	Implementación	14%	20%
	Evaluación de desempeño	13%	20%
	Mejora continua	10%	20%
TOTAL		53%	100%



Fuente: Proceso Tecnologías de la Información y las comunicaciones- Oficial de Seguridad UAECOB

MESA DE VALIDACIÓN DE HALLAZGOS

En el desarrollo del ejercicio auditor se adelantaron reuniones con los equipos auditados, circunstancia que permitió no solo una retroalimentación de lo observado, sino que se gestionaran de manera oportuna las acciones que se consideraban pertinentes para subsanar las debilidades encontradas, así como tener en cuenta las observaciones y/o recomendaciones; por lo anterior y al considerar que no se presentaron hallazgos o materialización de riesgos no fue necesario realizar esta actividad.

CUADRO RESUMEN DE HALLAZGOS

No se observaron desviaciones o materialización de riesgos, se evidenciaron situaciones susceptibles de mejora las cuales quedaron descritas en el acápite de recomendaciones de este informe

OBSERVACIONES

Por solicitud del oficial de seguridad de la información de la Entidad, la Oficina de Control Interno acompaño el ejercicio de autoevaluación programado con el fin de verificar que en las dependencias de la Entidad estuvieran aplicando los lineamientos impartidos en las capacitaciones realizada relacionadas con el Modelo de Seguridad y Privacidad de la Información.

Se programó visita a cuatro (4) dependencias de la Entidad: Oficina Jurídica, Subdirección de Gestión Humana,

Subdirección de Gestión del Riesgo y Oficina Asesora de Planeación, se aplicó una lista de verificación conformada por dieciséis (16) preguntas relacionadas con la seguridad de la información; el resultado se muestra a continuación:

No	Preguntas	No	Preguntas
1	¿Como se gestiona los riesgos de seguridad de la información en los proyectos tecnológicos de su proceso?	9	¿Se controla el acceso a herramientas tecnológicas (Excel o Word con datos sensibles, PCT, Portal de servicios, Control doc., ¿etc.)?
2	¿Cómo se involucra los riesgos de seguridad de la información en la gestión de proyectos?	10	¿Quiénes participan en la realización de la matriz de clasificación de activos de información?
3	¿Se han identificado los activos de información críticos del proceso o dependencia?	11	¿Existen políticas para compartir información con otras áreas o terceros?
4	¿Se han considerado las partes interesadas en seguridad de la información (internas y externas) que interactúan con su proceso?	12	¿Se aplican controles para el almacenamiento seguro de documentos (físicos y digitales)?
5	¿Existen un enlace en su proceso con el Grupo TIC para temas relacionados con seguridad de la información?	13	¿El personal de su proceso ha participado en charlas de seguridad de la información?
6	¿Se ha realizado un análisis de riesgos específico para los activos de información críticos de su proceso?	14	¿La dependencia o proceso conoce los canales de la entidad para reportar incidentes de seguridad?
7	¿Se han documentado los controles para mitigar los riesgos identificados?	15	¿Se ha realizado Análisis de Impacto de Negocio a su proceso?
8	¿Se aplican controles de acceso físico y lógico a la información sensible de su proceso?	16	¿Tienen actualmente planes de contingencia o continuidad en su proceso documentados?

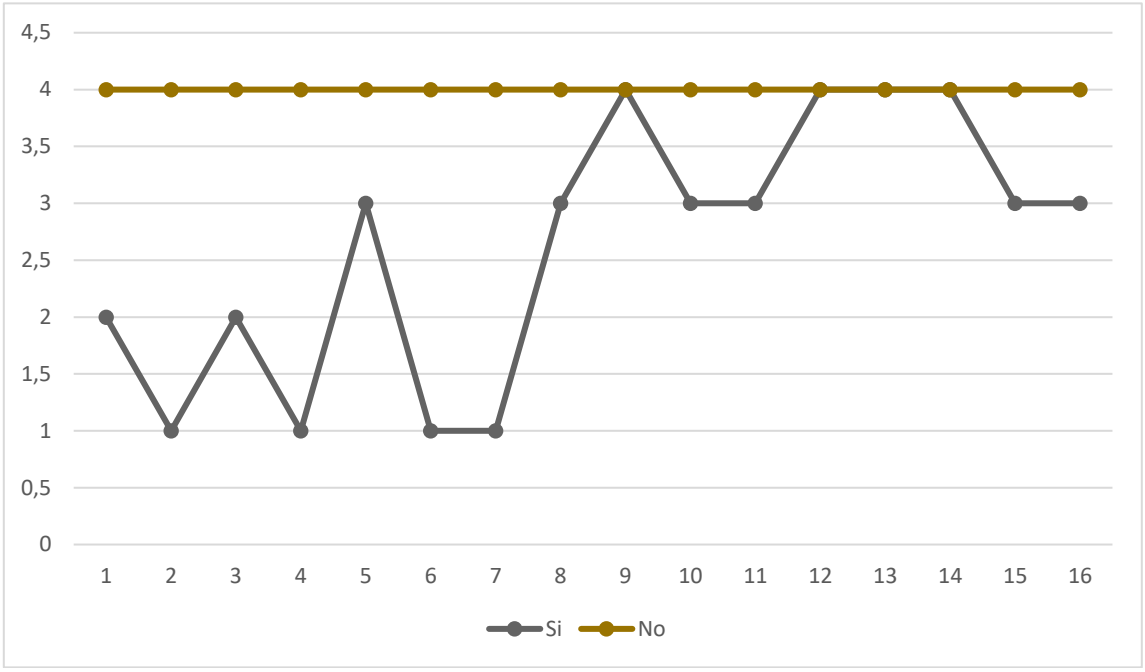
Fuente: Encuesta elaborada por TIC-UAECOB

Tabulación de las respuestas:

	Total, respuestas				
Pregunta	**Si**	**No**	**Pregunta**	**Si**	**No**
1	2	2	9	4	0
2	1	3	10	3	1
3	2	2	11	3	1
4	1	3	12	4	0
5	3	1	13	4	0
6	1	3	14	4	0
7	1	3	15	3	1
8	3	1	16	3	1
			Total	42	22

Fuente: Oficina de Control Interno

Grafica 1



Elaboración: OCI- UAECOB

Analizada la información que arroja la tabulación de las repuestas obtenidas en las dependencias de la Entidad visitadas, se observa que el 66% conoce y ha venido aplicando los lineamientos establecidos por el proceso de Tecnologías de la Información y las comunicaciones relacionadas con la seguridad de la Información.

Se observaron debilidades como las siguientes:

- No hay claridad de cuales son los Proyectos Tecnológicos que se manejan dentro de los procesos a los cuales pertenecen las personas encuestadas.
- No identifican con claridad como se involucra los riesgos de seguridad de la información en la gestión de proyectos que se generan en las dependencias de la Entidad.
- No es claro el cómo identificar los riesgos específicos para los activos de información críticos de los procesos.
- En tres de las cuatro dependencias visitadas no se cuentan con estrategia preventiva que detalle las acciones, recursos y procedimientos necesarios para responder a un evento o situación imprevista y potencialmente dañina, como desastres naturales, fallas tecnológicas o emergencias ambientales, con el objetivo de minimizar interrupciones y proteger activos, personas e instalaciones (planes de contingencia)

Se hace importante revisar la estrategia de comunicación y capacitación que se ha venido aplicando para socializar los lineamientos relacionados con la seguridad de la información, con el fin de garantizar que se identifiquen los riesgos pertinentes y, se formulan y documenten los controles.

Con lo anterior se asegura que los requisitos del sistema gestión de la seguridad de la información están integrados a los procesos de la Entidad y se minimiza la materialización de los riesgos identificados por la Entidad.

RECOMENDACIONES

- Teniendo en cuenta que la información es uno de los activos importantes de la Entidad, la seguridad de ésta debe ser un asunto institucional, no es solo del proceso del Gestión de Tecnologías de la Información y las comunicaciones, por lo tanto, es importante que desde cada dependencia que lidera procesos se designe un referente que interactúe y coadyuve en la implementación de los lineamientos impartidos en esta materia, es decir conformar el Equipo Técnico de Seguridad de la Información.

  En materia de riesgos se recomienda:

  - Para los residuales que siguen estando en nivel extremo y alto es importante revisar la metodología aplicada, si esta situación persiste es importante informar a la alta Dirección para que se tomen decisiones al respeto y se defina si estos riesgos son aceptables o no (apetito del riesgo).

  - Importante para el riesgo identificado con R10, se documente el control que han venido aplicando, actualmente no se observan.

  - Se recomienda asegurar que desde el inicio de la vigencia los controles establecidos se encuentren presentes y funcionando con el fin de blindar a la Entidad de posibles pérdidas de información y sanciones derivadas; lo anterior teniendo en cuenta que, a la fecha de este seguimiento, no se cuenta con las contrataciones pertinentes y no se tiene plan de choque establecido para los riesgos R2, R3, R4, R6, R8.

  - Se recomienda para el R3 verificar el cubrimiento de la póliza para los casos en los que se materialice el riesgo por descargar de software dañino por parte de los usuarios internos; si no hay cubrimiento establecer que procede en este caso y en ese sentido formular el control pertinente.

- Para los indicadores de gestión de Seguridad y Privacidad de la información que presentaron resultados por debajo de la meta propuesta por TIC, formular los planes de mejoramiento pertinentes con el fin de aportar a la mejora de los resultados del Modelo de Seguridad y Privacidad de la Información Institucional.

- Importante revisar la estrategia de comunicación y capacitación que se ha venido aplicando para socializar los lineamientos relacionados con la seguridad de la información, con el fin de garantizar que se identifiquen los riesgos pertinentes y, se formulan y documenten los controles.

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.

Es importante que adopten las acciones de mejora pertinentes para lograr cumplir a cabalidad con el objetivo del

Modelo de seguridad y privacidad de la Información MSPI, asegurar que perdure en el tiempo, blinde a la Entidad de posibles sanciones, ayude al cumplimiento de sus metas estratégicas y que redunde en beneficio de la ciudadanía, quien es la razón de ser de la UAECOB.

EQUIPO AUDITOR

Jaime Hernando Arias Patiño

Firma:
Jefe Oficina de Control Interno

María del Carmen Bonilla

Firma:
Profesional Especializada 222 grado 20
Auditora Oficina de Control Interno