ALCALDÍA MAYOR
DE BOGOTÁ D.C.

UNIDAD ADMIN. CATASTRO DISTRITAL 20-10-2025 05:08:13
Al Contestar Cite Este Nr.:2025IE27250 O 1 Fol:1 Anex:0
ORIGEN: Sd:181 - OFICINA DE CONTROL INTERNO/RUIZ PERILLA DIAN
DESTINO: DIRECCION GENERAL/LOPEZ MORALES OLGA LUCIA/ DIREC
ASUNTO: INFORME AUDITORÍA PROCESO GESTIÓN ESTRATÉGICA DE
OBS: PROYECTO/ LUIS ORLANDO BARRERA

MEMORANDO

Referencia: Plan Anual de Auditorías 2025

Fecha: 20 de octubre de 2025

PARA: Olga Lucia López Morales
Directora General

DE: Diana Karina Ruiz Perilla
Jefe Oficina Control Interno

ASUNTO: Informe Auditoría Proceso Gestión Estratégica de Tecnología - Sistema de Gestión de Seguridad y Privacidad de la Información.

Respetada Doctora Olga Lucía:

En cumplimiento del Plan Anual de Auditorías (PAA) 2025, actualmente en ejecución por la Oficina de Control Interno, y en el marco de las actividades orientadas al fortalecimiento del Sistema de Control Interno de la UAECD, se elaboró el Informe Final de Auditoría de Gestión al Proceso Gestión Estratégica de Tecnología - Sistema de Gestión de Seguridad y Privacidad de la Información.

El presente informe se remite para su conocimiento y los fines que correspondan.

Cordialmente,


Firmado digitalmente por DIANA KARINA RUIZ PERILLA
Fecha: 2025.10.20 16:55:35 -05'00'

DIANA KARINA RUIZ PERILLA
Jefe Oficina Control Interno

Copia: Integrantes Comité de Coordinación de Control Interno

Elaboró: Luis Orlando Barrera Cepeda – Ingeniero de Sistemas - Contratista OCI
Revisó: Diana Karina Ruiz Perilla, Jefe OCI

ALCALDÍA MAYOR DE BOGOTÁ D.C.	**INFORME DE EVALUACIÓN, SEGUIMIENTO O AUDITORÍA**

Evaluación: Seguimiento: Auditoría de Gestión: **X** Auditoría de Calidad:

En cumplimiento del Plan Anual de Auditorías de la vigencia **2025,** a continuación, se presentan los resultados del Informe de Auditoría de Gestión al proceso Gestión Estratégica de Tecnología – Sistema de Gestión de Seguridad y Privacidad de la Información dirigido a la señora directora de la UAECD con copia a las áreas o procesos involucrados

Proceso (s): Auditoría de Gestión al proceso Gestión Estratégica de Tecnología.

NOMBRE DEL INFORME: Informe de Auditoría de Gestión al proceso Gestión Estratégica de Tecnología – Sistema de Gestión de Seguridad y Privacidad de la Información.

1. OBJETIVO GENERAL: Revisar el Sistema de Gestión de Seguridad de la Información a través del seguimiento al Plan de Seguridad y Privacidad de la Información UAECD (en las vigencias 2024 y 2025), el Instrumento de Diagnóstico del MSPI, así como de las brechas determinadas y relacionadas con el Anexo A de la ISO 27001.

2. OBJETIVOS ESPECÍFICOS:

- Verificar la existencia del Plan de Seguridad y Privacidad de la Información vigencia 2024 y 2025.
- Verificar la existencia y aplicación de procedimientos, instructivos, documentos técnicos para la Seguridad y Privacidad de la Información.
- Constatar la formulación y aplicación de indicadores asociados a Seguridad de la Información.
- Revisar los Riesgos de Gestión y Corrupción relacionados con Seguridad de la Información.
- Verificar la existencia y tratamiento de los Riesgos de Seguridad de la información.
- Revisar el avance en el establecimiento de los controles conforme el Anexo A de la norma ISO 27001:2013

3. ALCANCE: Verificación de la Implementación y mantenimiento del modelo Seguridad de la Información en el periodo comprendido entre julio 2024-junio 2025.

4. MARCO NORMATIVO O CRITERIOS DE AUDITORÍA

- Decreto 221 de 2023 de la Alcaldía Mayor de Bogotá "*Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital, se deroga el Decreto Distrital 807 de 2019 y se dictan otras disposiciones.*"
- Directiva 008 de diciembre 30 de 2021 de la Alcaldía Mayor de Bogotá, D.C. "*Que establece los lineamientos para prevenir conductas irregulares con el incumplimiento de los manuales de funciones y competencias laborales y de los manuales de procedimientos institucionales, así como la pérdida, o deterioro, o alteración o uso indebido de bienes, elementos, documentos públicos e información contenida en bases de datos y sistemas de información*,"
- Decreto 767 de 2022 del MINTIC "*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 el MINTIC "*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*".
- Resolución 746 de 2022 del MINTIC "*Por la cual se fortalece el Modelo Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021*"
- Ley 594 de 2000. "*Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones*"
- Familia de Normas ISO 27000, Anexo A de la norma ISO 27001
- Documentos concomitantes que sean necesarios para cumplir con el objetivo de la auditoría, es decir, decretos, leyes, acuerdos, resoluciones, procedimientos, guías, manuales, instructivos, formatos y demás normas y actos administrativos relacionados o asociados al Sistema de Seguridad y Privacidad de la Información en la UAECD.

5. METODOLOGÍA

La auditoría se desarrolló dentro del marco de las normas internacionales de auditoría, que incluye: Planeación, ejecución, generación y comunicación del informe con las conclusiones y recomendaciones, que permitirán contribuir al mejoramiento del Sistema de Control Interno -SCI.

Para el desarrollo del seguimiento se solicitó información a través de memorando 2025IE20420 del 12 de agosto de 2025, información que fue suministrada de manera oportuna y completa, se desarrolló sesión de trabajo virtual efectuada con el Oficial de Seguridad de la información, quien funge como enlace de auditoría, establecido por la Gerencia. También se revisaron los procedimientos, instructivos, documentos técnicos suministrados que fueron contrastados con lo publicado en el aplicativo PANDORA, así mismo, se revisaron el estado de las No Conformidades y Oportunidades de Mejora así como los indicadores asociados al proceso Gestión Estratégica de Tecnología, especialmente los relacionados con el Sistema de Gestión de Seguridad y Privacidad de la Información y finalmente, los riesgos de gestión, fiscales, de corrupción y seguridad de la información.

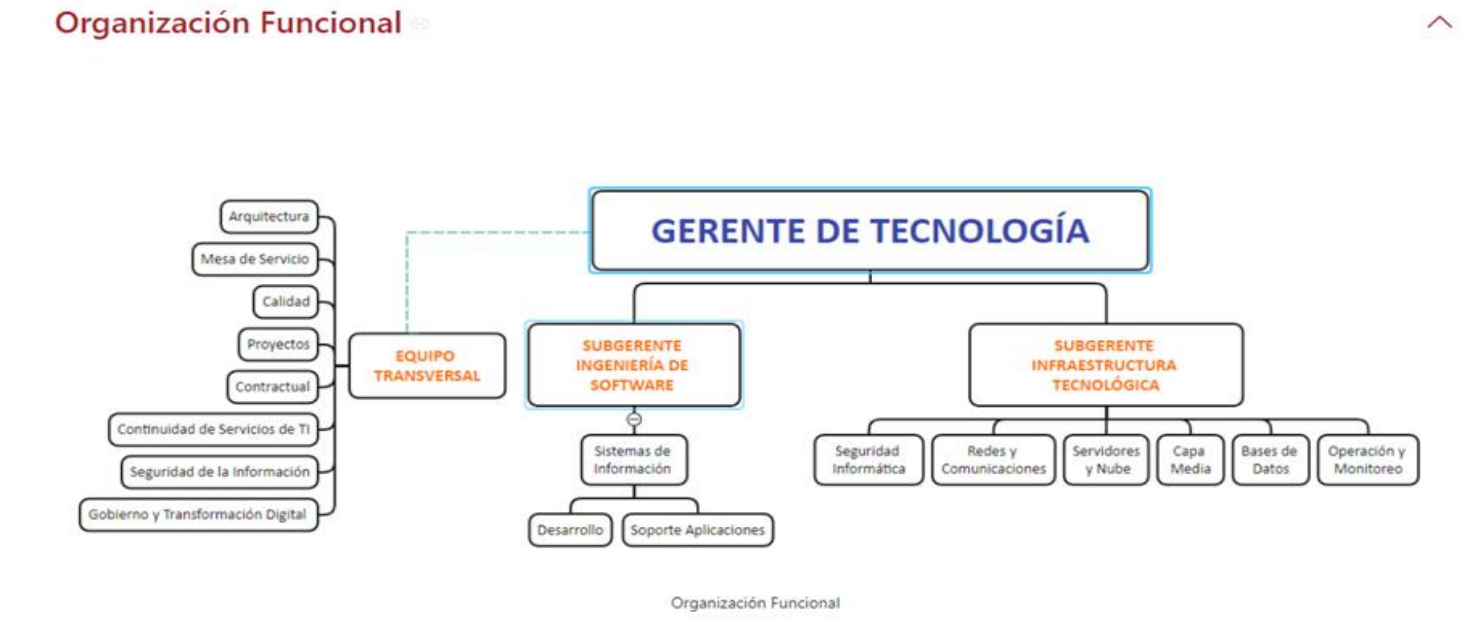
La auditoría se desarrolló en el periodo comprendido entre el 1 de agosto de 2025 al 30 de septiembre de 2025, por el Auditor Líder. Como ya se mencionó, el periodo evaluado corresponde al comprendido entre el 1 de julio de 2024 a 30 de septiembre de 2025. La información requerida para el desarrollo del presente ejercicio fue colocada en el One Drive determinado por la OCI para tal fin "2025_Audit_SGSPI"

6. PRESENTACIÓN DE RESULTADOS

6.1 Organización funcional y Organigrama

Se tiene como base en el Acuerdo No. 004 del 5 de noviembre de 2021, que la Gerencia de Tecnología está conformada por dos subgerencias, la Subgerencia de Ingeniería de Software y la Subgerencia de Infraestructura Tecnológica, adicionalmente, de acuerdo con la gráfica de la Organización Funcional de la Gerencia de Tecnología, suministrada como respuesta al punto 2 de la Solicitud 1, se identifican ocho (8) equipos transversales, siendo uno de ellos el de Seguridad de la Información, como se muestra a continuación:
https://catastrobogotacol.sharepoint.com/sites/TI/SitePages/GT.aspx?CT=1687292574204&OR=OWA-NT&CID=fc9e0fdd-656c-0bba-bf23-23505712f6f2&WSL=1#organizaci%C3%B3n-funcional

Gráfica 1. Organización Funcional Gerencia de Tecnología



Fuente: Información suministrada por la Gerencia de Tecnología

Organigrama:

Gráfica 2. Organigrama UAECD

Fuente: Información suministrada por la Gerencia de Tecnología

6.2 Presupuesto

Con base en la información suministrada por la Gerencia de Tecnología, se observa que el presupuesto asignado y comprometido para las vigencias 2024 y 2025 corresponde a $13.656.148.263 y $21.747.886.489 respectivamente, de estos valores para Seguridad correspondió a $1,703,568,500.00 para la vigencia 2024 y $2,163,529,863.00 para la vigencia 2025, como se detalla en las tablas a continuación:

Tabla 1. Presupuestos Tecnología vigencias 2024 y 2025

PRESUPUESTO 2024 INVERTIDO EN COMPONENTE SEGURIDAD

presupuesto	TOTAL COMPROMETIDO GERENCIA	%	Seguridad	%
Inversión	10,270,265,215	100%	$ 1,609,898,500.00	15%
Funcionamiento	3,385,883,048	100%	$ 93,670,000.00	3%
TOTAL	**13,656,148,263**		$1,703,568,500.00	

PRESUPUESTO 2025 INVERTIDO EN COMPONENTE SEGURIDAD

Presupuesto	TOTAL COMPROMETIDO GERENCIA	%	Seguridad	%
Inversión	16,805,618,253	100%	$ 2,064,859,363.00	15%
Funcionamiento	4,942,268,236	100%	$ 98,670,500.00	3%
TOTAL	**21,747,886,489**		$2,163,529,863.00	

Fuente: Gerencia de Tecnología

Tabla 2. Discriminado Seguridad vigencias 2024 y 2025

Discriminado Seguridad 2024

ITEM	Descripción / Objeto	Vr CRP	Número de Contrato	Nombre de Contratista
1	Equipos de seguridad informática, así como el servicio de monitoreo y seguridad SOC.	$ 1,506,873,500.00	476-2024	DATASEC S.A.S
2	Prestación de servicios profesionales	$ 28,847,000.00	566-2024	LUISA FERNANDA BARRAGAN NIETO
3	Prestación de servicios profesionales	$ 74,178,000.00	24 - 2024	LUISA FERNANDA BARRAGAN NIETO
4	Antivirus funcionamiento	$ 93,670,000.00	933-2023	GOLD SYS LTDA
		$ 1,703,568,500.00		

Discriminado Seguridad 2025

ITEM	Descripción / Objeto	Vr CRP	Número de Contrato	Nombre de Contratista
1	Equipos de seguridad informática, así como el servicio de monitoreo y seguridad SOC.	$ 1,424,900,663.00	357-2025	DATASEC S.A.S
2	Antivirus funcionamiento	$ 98,670,500.00	106-2025	M S L DISTRIBUCIONES & CIA S.A.S
3	Prestación de servicios profesionales	$ 104,588,000.00	211-2025	ALBEIRO GOMEZ SALAMANCA
4	Seguridad perimetral	$ 449,798,700.00	344-2025	DATASEC S.A.S
5	Prestación de servicios profesionales	$ 85,572,000.00	337-2025	IVAN GUILLERMO GARCIA BELTRAN
		$ 2,163,529,863.00		

Fuente: Gerencia de Tecnología

La asignación presupuestal registra un incremento en la vigencia 2025 por valor de $ 459,961,363.00 con respecto de la vigencia 2024, para soportar la renovación de equipos físicos de seguridad perimetral para el datacenter on-premise, incluidas las actividades de análisis de vulnerabilidades de seguridad de la UAECD.

Resalta el proceso que para la vigencia 2024 se contaba con dos personas de planta (José Ignacio Saavedra (Seguridad perimetral) y Luis Albeiro Cortés Castiblanco (Oficial de Seguridad de la información), mientras que para la vigencia 2025 se cuenta con una persona de planta Luis Albeiro Cortés Castiblanco (Oficial de Seguridad de la información).

6.3 Política

Una política de SGSI es el documento que establece el compromiso de una organización con la seguridad de la información, definiendo objetivos, alcance, roles y responsabilidades para proteger los activos de información contra riesgos, cumpliendo así con la norma ISO 27001 y fomentando una cultura de seguridad.

Solicitada la información a la política de seguridad de la información, fue remitida copia de la Resolución 732 del 1 de septiembre de 2020 "*Por la cual se adopta la Política de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial de Catastro Distrital*" y que en su artículo 2 establece "*Política de Seguridad y Privacidad de la Información: La UAECD entendiendo la importancia de la seguridad de la información como actividad estratégica en el cumplimiento de su misión, preservará la confidencialidad, integridad, disponibilidad y privacidad de sus activos de información,*

realizando sobre estos una gestión integral de los riesgos de seguridad digital con el fin de mitigar su impacto, en un proceso de mejora continua. Para lo cual implementará los controles necesarios, que son de estricto cumplimiento para todos los funcionarios, contratistas y terceros que en el cumplimiento de sus funciones u obligaciones accedan a los activos de información de la Unidad. De igual manera implementará los controles sobre los activos de información que son accedidos por la ciudadanía, la cual deberá darles cumplimiento a los lineamientos establecidos."

Criterio:
Establece la resolución en su artículo 5 *"Políticas y controles definidos por la Unidad en el marco del SGSI: La UAECD de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Norma ISO 27001:2013, realizará la especificación y actualización de las políticas y controles en el documento definido como "DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD DE LA INFORMACIÓN"*

Situación evidenciada:
Revisados los documentos aportados por el Equipo de Seguridad de la Información se constató el "*DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" GEST-DT-01 versión 3 de fecha 21-02-2025*" que tiene por objetivo "*Definir y disponer para conocimiento y cumplimiento de todos los funcionarios, contratistas y terceros que acceden a los activos de información de la Unidad, los lineamientos y directrices del Modelo de Seguridad y Privacidad de la Información, alineados con lo establecido en la Norma ISO 27001:2013 y demás normatividad vigente, con el fin de preservar la confidencialidad, disponibilidad e integridad de la información"*.

Revisada la página WEB de la Unidad, se observa que en el enlace de Transparencia en el numeral 1.8.1 se encuentra el documento "*Políticas Detalladas de Seguridad y Privacidad de la Información*", que detalla catorce (14) políticas relacionadas con Seguridad y Privacidad de la Información, documento que no es concordante con el *DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" GEST-DT-01*

Gráfica 3. Doc. Tec. Manual Políticas SPI

ALCALDÍA MAYOR DE BOGOTÁ D.C.

DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Proceso: Gestión Estratégica de Tecnología

Fuente: Documento aportado ppor la Gerencia de Tecnologia

Gráfica 4. Doc. Políticas Detalladas SPI

UAECD Catastro Bogotá

POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

POLITICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Este documento contiene la descripción general de las políticas específicas de seguridad y privacidad de la información definidas en la UAECD, las cuales permitirán:

1. Prestar de manera segura los servicios relacionados con el catálogo de servicios de TI.
2. Aplicar las mejores prácticas de seguridad y privacidad de la información en la información capturada, integrada y dispuesta por la Unidad.
3. Facilitar el cumplimiento de los requisitos legales a los cuales esté obligada la Unidad en torno a esta materia.
4. Guiar el comportamiento personal y profesional de funcionarios, contratistas y terceros que acceden a los activos de información.

Las políticas que a continuación se definen, se encuentran alineadas con la Política General de Seguridad y Privacidad de la Información adoptada por la Unidad mediante resolución 732 de 2020, en la cual se define:

"La Unidad Administrativa Especial de Catastro Distrital – UAECD entendiendo la importancia de la seguridad de la información como actividad estratégica en el cumplimiento de su misión, preservará la confidencialidad, Integridad, disponibilidad y privacidad de sus activos de información, realizando sobre estos una gestión integral de los riesgos de seguridad digital con el fin de mitigar su impacto, en un proceso de mejora continua. Para lo cual implementará los controles necesarios, que son de estricto cumplimiento para todos los funcionarios, contratistas y terceros que en el cumplimiento de sus funciones u obligaciones accedan a los activos de información de la Unidad. De igual manera implementará los controles sobre los activos de información que son accedidos por la ciudadania, la cual deberá darles cumplimiento a los lineamientos establecidos.", y son de estricto cumplimiento para todos los funcionarios, contratistas y terceros que acceden a los activos de información de la Unidad.

Los lineamientos y responsabilidades definidos para cada una de las políticas específicas se encuentran detallados en el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información.

1. POLITICA PARA DISPOSITIVOS MÓVILES

Descripción: La UAECD establece lineamientos para mitigar los riesgos asociados al acceso, pérdida y divulgación no autorizada de la información de la Unidad a través de dispositivos móviles, cumpliendo con controles de borrado seguro y mecanismos de aseguramiento de la información.

Fuente: Página web UAECD – numeral 1.8.1

6.3.1 Oportunidad de Mejora Diferencias Documentos Políticas SPI

Oportunidad de Mejora

(OM1) La Unidad cuenta con el *DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" GEST-DT-01 v3* del 21 de febrero de 2025 documento que difiere del publicado en la página web de la Unidad en el enlace Transparencia y acceso a la información pública en su numeral 1.8.1 Política de seguridad de la información del sitio web y protección de datos personales en su numeral 1. Políticas de Seguridad y Privacidad de la Información. Se recomienda unificar la presentación de la información con base en el *DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" GEST-DT-01 v3* del 21 de febrero de 2021

Respuesta GT./ No se acepta la oportunidad de mejora, toda vez que el Documento que está publicado en la página web de la Unidad en el enlace Transparencia y acceso a la información pública en su numeral 1.8.1 Política de seguridad de la información, contiene la descripción general de las políticas específicas de seguridad y privacidad de la información definidas en la UAECD, este documento contiene las 14 políticas de seguridad de la información con la respectiva descripción y no se publica el DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" GEST-DT-01 toda vez que este contiene lineamientos que solo es para uso interno, lo cuales pueden tomar ciberdelincuentes para realizar ingeniería social.
De igual manera se aclara que, la última actualización de la política corresponde al DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" GEST-DT-01 v3 del 21 de febrero de 2025 publicado en PANDORA.

RESPUESTA OCI
Revisada la respuesta entregada por la Gerencia de Tecnología a través de correo electrónico del pasado 3 de octubre de 2025, se acepta la observación planteada y el argmento interpuesto. Por lo anterior se levanta la Oportunidad de Mejora, la cual no será registrada en el aplicativo PANDORA.

Criterio:
Establece la Resolución en su artículo 6 Revisión de la Política: "*La UAECD revisará la Política de Seguridad y Privacidad de la Información y las políticas detalladas derivadas con una periodicidad mínima anual…*".

Situación evidenciada:
La última actualización de la política corresponden al *DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" GEST-DT-01 v3* del 21 de febrero de 2021, soportado con actas de Comité Institucional de Gestión y Desempeño, así: 1) Acta No. 11 del Comité Institucional de Gestión y Desempeño que en su reunión del 25 de noviembre de 2024 en el numeral 4 del orden contempló la Aprobación documento técnico Políticas de Seguridad y Privacidad de la Información - Gerencia de Tecnología y en Acta No. 2 de la reunión del 20 de febrero de 2025 en su punto 4 desarrolló la revisión del Ajuste Política de Seguridad de la Información.

6.4 Procedimiento e Instructivos

El proceso de Gestión Estratégica de Tecnología antes Gestión y Desarrollo de las TIC diseño, construyó y tiene establecidos procedimientos, documentos técnicos, instructivos y formatos para gestionar proyectos estratégicos de Tecnologías de la Información y las Comunicaciones, fomentando la implementación de procesos, trámites y servicios que permitan la generación de valor en lo público, el acceso, uso y apropiación de los mismos, para el cumplimiento de los objetivos institucionales, **bajo lineamientos de seguridad y privacidad de la información** y la continuidad de los servicios tecnológico que en la actualidad se encuentran en PANDORA, como se muestra a continuación

Tabla 3. Comparativo Documentos Gestión Estratégica de Tecnología

TIPO DOCUMENTO	PANDORA 2024 Gest. Drrllo TIC	PANDORA 2025 Gest. Estrat. Tecnol.	PANDORA 2025 Gest. y Oper. TI.
Caracterización	1	1	1
Procedimientos	7	3	4
Documentos Técnicos	4	2	2
Instructivos	15	6	9

Fuente: Construcción del Auditor a partir del aplicativo PANDORA

Lo anterior evidencia que el proceso "Gestión y Desarrollo de las TIC que en la nueva cadena de valor dio paso a dos procesos: 1. Gestión Estratégica de Tecnología y 2. Gestión y Operación TI, en el primero de ellos registra cuatro (4) componentes: a) Gobierno y Transformación Digital, b) Gestión de proyectos de TI, c) Gestión de Continuidad y d) Gestión de Seguridad y Privacidad de la Información

Revisado el aplicativo PANDORA en lo que refiere al proceso Gestión Estratégica de Tecnología, se evidenciaron registrados los documentos relacionados en la tabla a continuación:

Tabla 4. Documentos del Proceso de Gestión Estratégica de Tecnología en PANDORA

Código	Nombre	Fecha	
GEST-CP v4	Caracterización del Proceso Gestión Estratégica de Tecnología	2025-02-05	
GEST-PR-01 v2	Procedimiento de Planeación Estratégica de TI	2024-09-19	
GEST-PR-02 v2	Procedimiento de Continuidad del Negocio	2025-02-14	
GEST-PR-03 v2	Procedimiento de Gestión de Seguridad y Privacidad de la Información	2024-12-12	
GEST-DT-01 v3	Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información	2025-02-21	
GEST-DT-02 v1	Documento Técnico de Arquitectura Tecnológica de Referencia	2024-08-29	
GEST-02-IN-01	Instructivo para la Definición del Plan de Continuidad del Negocio	2024-08-29	*
GEST-02-IN-02	Instructivo de Ejercicios y Pruebas	2024-08-29	*
GEST-03-IN-01 v1	Instructivo de Gestión de Activos de Información	2024-08-29	
GEST-03-IN-02 v1	Instructivo de Gestión de Incidentes de Seguridad de la Información	2024-08-29	
GEST-03-IN-03 v1	Instructivo de Cifrado de Información	2024-08-29	
GEST-03-IN-04 v1	Instructivo de Análisis Forense Digital	2024-08-29	

Fuente: Construcción del Auditor a partir del aplicativo PANDORA

Situación evidenciada:
El control documental en PANDORA evidencia que el proceso de Gestión Estratégica de Tecnología cuenta con 12 documentos distribuidos entre caracterización (1), tres (3) procedimientos, seis (6) instructivos, dos documentos (2), adicionalmente cuenta con tres (3) formatos y un (1) boletín, que en la anterior cadena de valor formaban parte del proceso de Gestión y Desarrollo de las TIC.

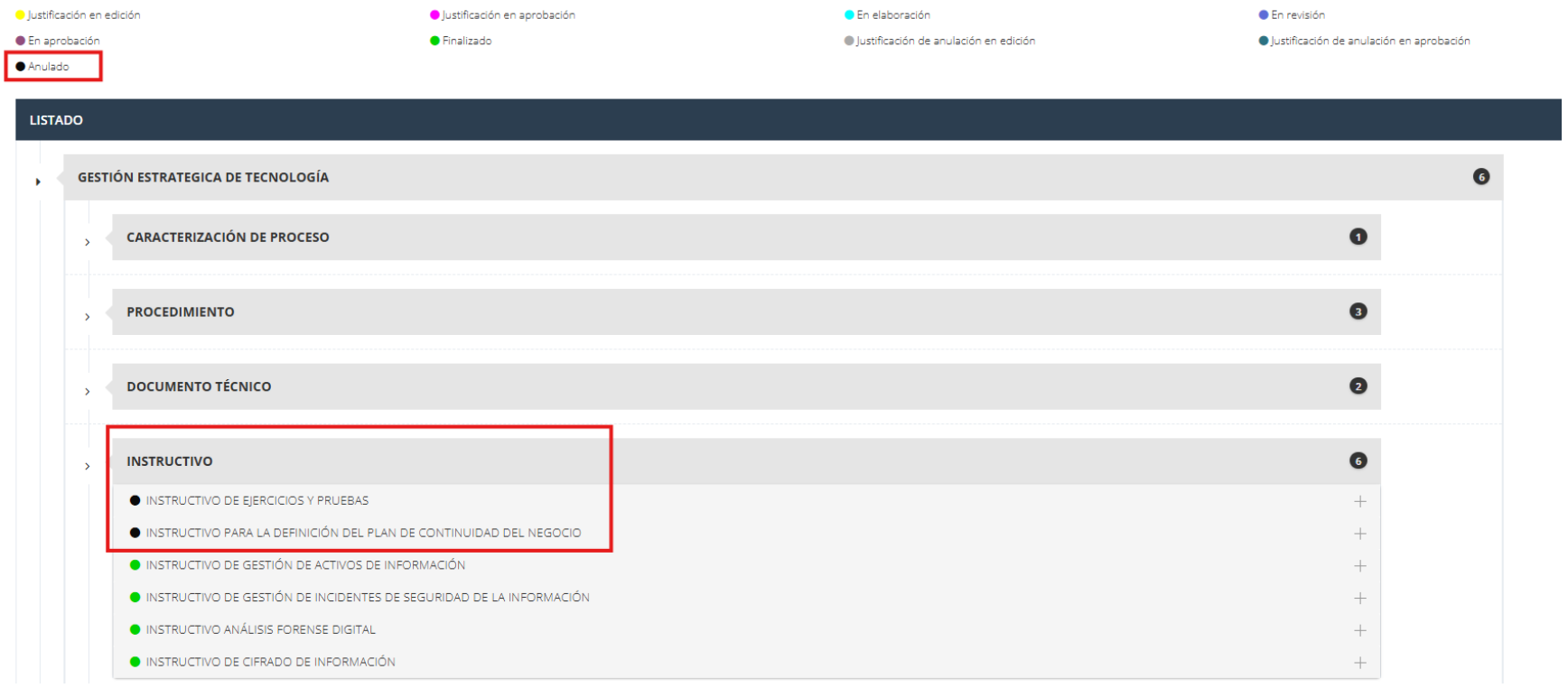
Se encontró que los instructivos GEST-02-IN-01 Instructivo para la Definición del Plan de Continuidad del Negocio y GEST-02-IN-02 Instructivo de Ejercicios y Pruebas, así como el boletín GEST-BI-01, no obstante estar registrados en el aplicativo, no están disponibles actualmente en PANDORA, en consecuencia, no se pueden descargar o consultar, como se detalla en el pantallazo a continuación:

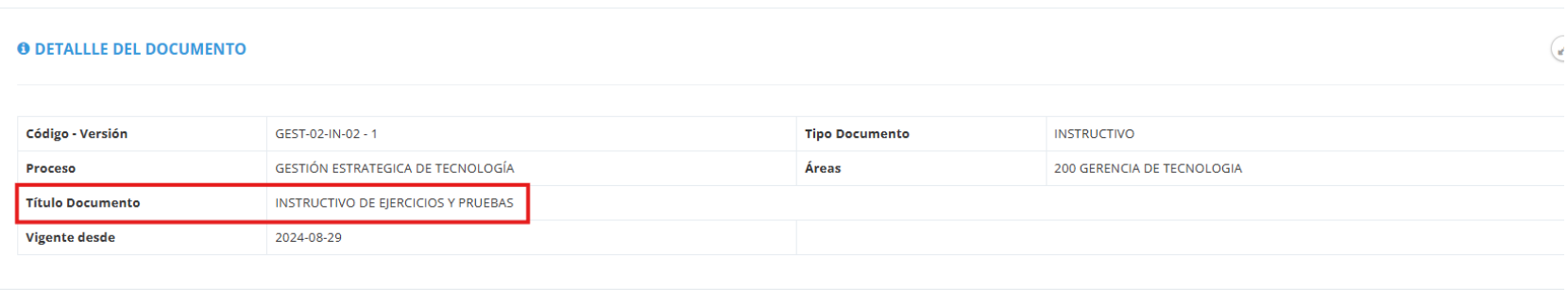
6.4.1 Oportunidad de Mejora Indisponibilidad de Documentos en PANDORA

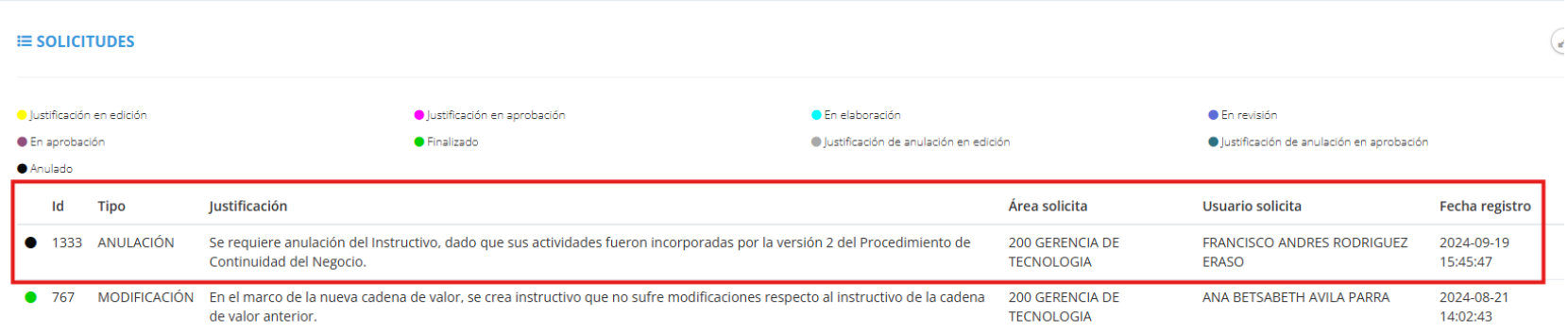
Recomendación:

Los instructivos GEST-02-IN-01 Instructivo para la Definición del Plan de Continuidad del Negocio y GEST-02-IN-02 Instructivo de Ejercicios y Pruebas registrados en PANDORA, no están disponibles para ser leídos o descargados para su consulta por cuanto se encuentran Anulados, por lo anterior se recomienda efectuar la marcación correspondiente en el aplicativo PANDORA o su retiro, para que no aparezcan o si lo hacen, se marquen como anulados a efecto de no crear expectativas frente a documentos inexistentes.

Respuesta GT./ No se acepta la oportunidad de mejora, dado que los instructivos GEST-02-IN-01 Instructivo para la Definición del Plan de Continuidad del Negocio y GEST-02-IN-02 Instructivo de Ejercicios y Pruebas en la actual cadena de valor son documentos anulados (ver imagen), por tanto, no son documentos que se deban tomar como referencia y no se encuentran en Pandora para consulta. En su momento se tomó la decisión de anularlos (19 de septiembre de 2024), dado que sus actividades se integraron al Procedimiento de Continuidad del Negocio GEST-PR-02.







ALCALDÍA MAYOR DE BOGOTÁ D.C.

INFORME DE EVALUACIÓN, SEGUIMIENTO O AUDITORÍA

DETALLLE DEL DOCUMENTO

Código - Versión	GEST-02-IN-01 - 1	**Tipo Documento**	INSTRUCTIVO
Proceso	GESTIÓN ESTRATEGICA DE TECNOLOGÍA	**Áreas**	200 GERENCIA DE TECNOLOGIA
Título Documento	INSTRUCTIVO PARA LA DEFINICIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO		
Vigente desde	2024-08-29		

SOLICITUDES

Justificación en edición · Justificación en aprobación · En elaboración · En revisión · En aprobación · Finalizado · Justificación de anulación en edición · Justificación de anulación en aprobación · Anulado

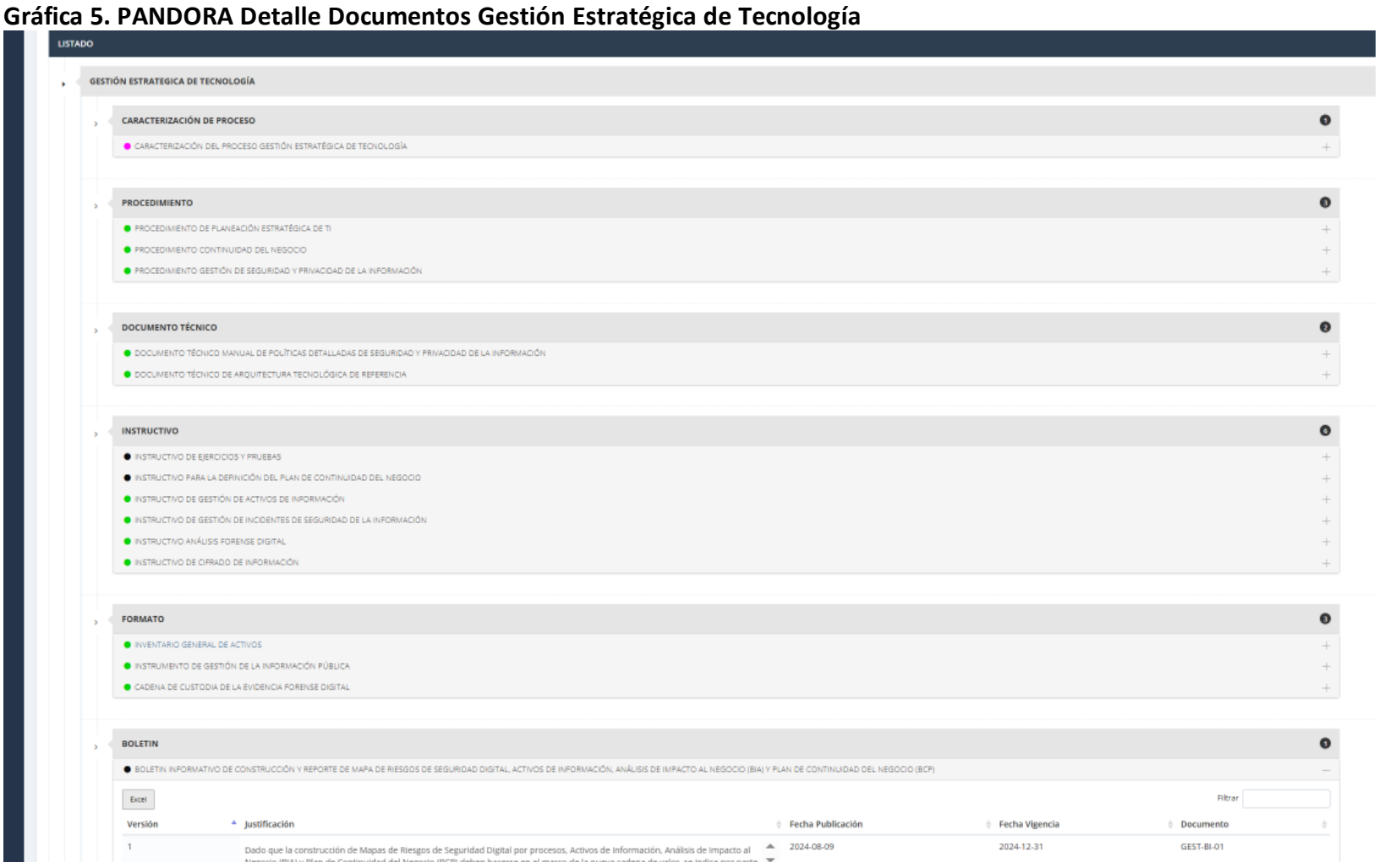
Id	Tipo	Justificación	Área solicita	Usuario solicita	Fecha registro
1334	ANULACIÓN	Se requiere anulación del Instructivo, dado que sus actividades fueron incorporadas por la versión 2 del Procedimiento de Continuidad del Negocio.	200 GERENCIA DE TECNOLOGIA	FRANCISCO ANDRES RODRIGUEZ ERASO	2024-09-19 15:46:19
768	MODIFICACIÓN	En el marco de la actualización de la cadena de valor, se crea instructivo que no sufre modificaciones respecto a la anterior cadena de valor.	200 GERENCIA DE TECNOLOGIA	ANA BETSABETH AVILA PARRA	2024-08-21 14:04:03

Respuesta OCI:

Revisados los soportes presentados por el proceso en respuesta emitida por la Gerencia de Tecnología en correo del pasado 3 de octubre de 2025, si bien es cierto que se solicitó y tramitó la anulación de los documentos aludidos en la oportunidad de mejora planteada, también lo es que para el usuario con privilegios de consulta de documentos en el aplicativo PANDORA no es identificable la condición de Anulado sobre el documento. En consecuencia, se acepta parcialmente la respuesta del proceso y por tanto se cambia la connotación de Oportunidad de Mejora a Recomendación, en cuanto a que los documentos que presenten la connotación de Anulado, se reflejen con esa anotación en el aplicativo PANDORA a efecto de la coherencia de la información presentada y de esta manera evitar el generar expectativas irreales hacia el usuario del aplicativo.

En desarrollo de la reunión la ingeniera Ana Betsabeth Ávila informa que efectivamente los documentos en el aplicativo PANDORA se encuentran marcados como Anulados y procede a realizar proyección de PANDORA evidenciando lo informado. Efectuada la revisión posterior por la OCI se constata lo presentado por la ingeniera Ávila. Como conclusión se retira la Oportunidad de Mejora y recomendación, la cual no será registrada en el aplicativo PANDORA.

Gráfica 5. PANDORA Detalle Documentos Gestión Estratégica de Tecnología



Fuente: PANDORA

El control documental en PANDORA también evidencia que el proceso de Gestión y Operación TI cuenta con 16 documentos distribuidos entre caracterización (1), tres (3) procedimientos, seis (6) instructivos, dos (2) documentos, tres (3) formatos y un (1) boletín, que en la anterior cadena de valor formaban parte del proceso de Gestión y Desarrollo de las TIC. Adicionalmente cuenta con dieciséis (16) formatos

Tabla 5. Documentos del Proceso de Gestión y Operación TI en PANDORA

Código	Nombre	Fecha
GOTI- CP v4	Caracterización del Proceso Gestión y Operación de TI	2025-03-28
GOTI-PR-01 v1	PROCEDIMIENTO GESTIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA	2024-08-29

GOTI-PR-02 v3	PROCEDIMIENTO GESTIÓN D E CAMBIOS Y LIBERACIONES	2025-07-11
GOTI-PR-03 v2	PROCEDIMIENTO SOPORTE Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	2025-03-28
GOTI-PR-04 v1	PROCEDIMIENTO GESTIÓ N DE MESA DE SERVICIOS	2024-08-29
GOTI-DT-01 v1	DOCUMENTO TÉCNICO CATÁLOGO DE SERVICIOS DE TI	2024-08-29
GOTI-DT-02 v1	DOCUMENTO TÉCNICO CONTROLES DE SEGURIDAD DE LA INFORMACIÓN PARA LA CONSTRUCCIÓN DE SOFTWARE SEGURO	2024-08-29
GOTI-01-IN-01 v1	INSTRUCTIVO DE COPIAS DE RESPALDO Y RECUPERACIÓN	2024-08-29
GOTI-01-IN-02 v1	INSTRUCTIVO GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD	2024-08-29
GOTI-03-IN-01 v1	INSTRUCTIVO DE VERSIONAMIENTO DE SOLUCIONES DE SOFTWARE	2024-08-29
GOTI-04-IN-01 v1	INSTRUCTIVO DE INSTALACIÓN Y DESINSTALACIÓN DE SOFTWARE	2024-08-29
GOTI-04-IN-02 v1	INSTRUCTIVO DE ALISTAMIENTO Y ENTREGA DE EQUIPOS	2024-08-29
GOTI-04-IN-03 v1	INSTRUCTIVO GESTIÓN DE CONFIGURACIÓN	2024-08-29
GOTI-04-IN-04 v1	INSTRUCTIVO GESTIÓN DE PROBLEMAS	2024-08-29
GOTI-04-IN-05 v1	INSTRUCTIVO PARA ATENDER SOLICITUDES DE INFORMACIÓN	2024-08-29
GOTI-04-IN-06 v1	INSTRUCTIVO GESTIÓN DE ACCESOS	2024-08-29

Fuente: Construcción del Auditor a partir de PANDORA

A partir de lo anterior y con base en la información aportada por el proceso auditado, para el alcance del presente ejercicio auditor solo hacen parte los siguientes documentos: 1) Procedimiento GEST-PR-03_V2 GESTION_SPI Procedimiento de Gestión de Seguridad y Privacidad de la Información, 2) Documento Técnicos GEST-DT-01_V3_MANUAL DE POLITICAS DETALLADAS_SPI, GOTI-DT-02_V1_ CONTROLES SEGURIDAD DE LA INFORMACION PARA LA CONSTRUCCION SOFTWARE SEGURO, DIES-DT-03_V2_DT_POLITICA Y METDOLOGIA DE RIESGOS y 3) Instructivos GEST-03-IN-01_V1_ GESTION DE ACTIVOS DE INFORMACION, GEST-03-IN-02_V1_GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, GEST-03-IN-03_V1_CIFRADO DE INFORMACION, GEST-03-IN-04_V1_ANALISIS FORENSE DIGITAL, GOTI-01-IN-01_V1_ COPIAS DE RESPALDO Y RECUPERACION, GOTI-01-IN-02_V1_GESTION DE LA CAPACIDAD Y DISPONIBILIDAD y GOTI-04-IN-06_V1_GESTION DE ACCESOS.

Se revisó el procedimiento GEST-PR-03_V2 GESTION_SPI Procedimiento de Gestión de Seguridad y Privacidad de la Información encontrando que establece dos puntos de control en las actividades 5 y 7 a cargo del Gerente de Tecnología y el Comité Institucional de Gestión y Desempeño respectivamente, consistente en la aprobación de GEST-PR-03_V2 GESTION_SPI Procedimiento de Gestión de Seguridad y Privacidad de la Información, se corroboró cumplimiento en el Acta 11 del 25 de noviembre de 2024 y acta 12 de diciembre de 2024, de igual manera en acta 2 del 20 de febrero de 2025 correspondientes a reuniones del Comité Institucional de Gestión y Desempeño con presentaciones realizadas por el Gerente de Tecnología.

El procedimiento GEST-03-IN-02_V1_GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN presenta dos puntos de control en las actividades 10 y 14, el primero corresponde a validar por parte del equipo de respuesta a incidente, cuando se requiera, que las actividades hayan sido planteadas adecuadamente, en caso de que no estén planeadas adecuadamente se debe volver a ajustar el plan de trabajo, el segundo permite determinar si el incidente fue resuelto con el plan de trabajo propuesto o si se requieren acciones adicionales que permitan su contención o mitigación.

Dentro del alcance del presente ejercicio auditor se revisó el Documento Técnicos GEST-DT-01_MANUAL DE POLITICAS DETALLADAS_SPI, observando la existencia y disponibilidad del mismo, documento fechado 21 de febrero de 2025 en su versión 3, presentado y aprobado por el Comité Institucional de Gestión y Desempeño en el punto 4 de la agenda del comité del 25 de noviembre de 2024 y actualizada en reunión del 20 de febrero de 2025 conforme con acta 2 de ese comité.

El Instructivo GEST-03-IN-01_V1_ GESTION DE ACTIVOS DE INFORMACION establece puntos de control en la actividad 3. Asesorar y revisar respecto al diligenciamiento del inventario de activos de información del proceso, dado que a través de ella se revisa que el inventario cumple con los lineamientos dados en el presente documento y 4. Revisar y aprobar el inventario de activos de información de su dependencia/proceso por cuanto a través de esta se revisa y aprueba el inventario por parte del propietario del activo de información. Este procedimiento fue desarrollado recientemente por la OCI durante la revisión y actualización de los activos de información.

Los instructivos GEST-03-IN-03_V1_CIFRADO DE INFORMACION, GEST-03-IN-04_V1_ANALISIS FORENSE DIGITAL describen paso a paso el uso de diferentes herramientas mas no contienen puntos de control.

6.5 Riesgos

La Oficina de Control Interno realizó el Seguimiento al Monitoreo y Materialización de Riesgos de la entidad en lo correspondiente al II y III trimestre 2024, remitiendo el informe con memorado 2024IE27473 dirigido a la señora Directora de la UAECD con copia a los miembros del Comité Institucional de Coordinación de Control Interno. Así mismo, se generó el informe del Seguimiento al Monitoreo y Materialización de Riesgos de la entidad los riesgos al corte de junio de 2025, emitido con radicado 2025IE22782 de fecha 5 de septiembre de 2025.

Con base en lo anterior, no se realiza y detalla un nuevo seguimiento a estos cortes dentro del presente informe, por el contrario, se extractan y/o copian a continuación los aspectos más relevantes de cada uno de ellos en lo relacionado con la presente auditoría:

- *"Al corte de diciembre de 2024 los procesos de Gestión Estratégica de Tecnología y Gestión de Operación de TI en el Mapa de Riesgos Institucional registraron 31 riesgos, clasificados de acuerdo con la zona residual en 21 en nivel bajo, 7 en moderado y 3 en alto. De los anteriores cuatro (4) corresponden a riesgos de gestión, uno (1) a riesgos de corrupción y veintiséis (26) a riesgos de seguridad de la información."*

  Teniendo en cuenta que la matriz de riesgos de la Unidad al corte de diciembre de 2024 registra 260 riesgos de los cuales 31 corresponden al proceso auditado, lo anterior conlleva a que el 12% de los riesgos contemplados en matriz de riesgos de la UAECD fueron contemplados por el proceso auditado

Tabla No.6: Mapa de Riesgos Institucional Vigencia 2024-V.4

MAPA DE RIESGOS INSTITUCIONAL 2024 V.4				
PROCESOS	BAJO	MODERADO	ALTO	TOTAL RIESGOS POR PROCESO (Gestión, Corrupción, Fiscales, Seguridad Digital)
DIRECCIONAMIENTO ESTRATÉGICO	5	2		7
GESTIÓN ESTRATÉGICA DE PERSONAS	16	8	3	27
GESTION DEL CONOC E INNOVACIÓN	5			5
RELACIONAMIENTO ESTRATÉGICO	22	11	4	37
GESTIÓN EST. DE TECNOLOGÍA	1	1		2
GESTION DE INF CATASTRAL Y VALUATORIA	10	14	9	33
GEST. DE INFORMACIÓN GEOGRÁFICA	19	5	2	26
GESTIÓN PRESPTAL Y FINANCIERA	17	3	2	22
GESTIÓN DOCUMENTAL	2	7	2	11
GESTIÓN DE SERV ADMTIVOS	9	1	3	13
GESTIÓN CONTRACTUAL	12	3		15
GESTIÓN JURÍDICA	5	7		12
GESTIÓN Y OPERACIÓN DE T. I	20	6	3	29
EVALUACIÓN INDEP DE LA GESTION	2	4		6

Fuente: Elaboración propia con base en el Mapa de Riesgos de la UAECD 2024 V 4 publicado página web de la UAECD

"Riesgos de Seguridad de la Información UAECD a corte de 2024

La matriz de riesgos de seguridad de la información presenta un total de 170 riesgos de los cuales 102 se encontraron en zona residual baja, lo que corresponde a un 60%, 55 en moderada 32% y 13 en zona residual alta- 8%, observando que se presentó modificación en la versión 4, con respecto a la versión 3, disminuyendo en un riesgo la zona residual baja y aumentando la zona moderada en un riesgo; esto en razón a la materialización presentada durante el tercer trimestre de la vigencia en el proceso Gestión y Desarrollo de las TIC.

La Gerencia de Tecnología emitió Boletín de Calidad GEST-BI-01 en el que determinaron y justifican mantener los riesgos según la estructura de la cadena de valor anterior, razón por la cual, estos no se ajustaron de acuerdo con los procesos de la nueva cadena."

Tabla No.7: Riesgos de Seguridad de la Información Vigencia 2024 V.4

RIESGOS SEGURIDAD DE LA INFORMACIÓN 2024 V.4					
PROCESOS	**BAJO**	**MODERADO**	**ALTO**	**EXTREMO**	**TOTAL**
DIRECCIONAMIENTO ESTRATÉGICO	4				4
COMUNICACIONES	8	1	1		10
GESTIÓN CATASTRAL	7	5			12
GESTIÓN CATASTRAL TERRITORIAL	1	6	7		14
GEST INFORMACIÓN GEOGRÁFICA	7	1			8
GEST. CONOCIMIENTO E INNOVACIÓN	2				2
GESTIÓN PRODUCTOS Y SERVICIOS	7	1			8
GESTIÓN Y DESARROLLO TIC	18	6	2		26
PART CIUDADANA Y EXP DEL SERVICIO	5	3			8
GESTIÓN FINANCIERA	9	3			12
GESTIÓN JURÍDICA	4	4			8
GESTIÓN TALENTO HUMANO	11	5			16
GESTIÓN CONTRACTUAL	7	3			10
GESTIÓN SERV ADMINISTRATIVOS	3	1			4
GESTIÓN DOCUMENTAL	1	5			6
GESTIÓN SEGUIMIENTO Y EVALUACIÓN	5	8	3		16
TRANSVERSALES (DIR-GGC)	3	3			6
TOTAL	**102**	**55**	**13**	**0**	**170**
% de Participación	**60%**	**32%**	**8%**	**0%**	**100%**

Fuente: Elaboración propia con base en el Mapa de Riesgos de la UAECD 2024 V4 publicado página web de la UAECD

"Se evidenció el seguimiento realizado por la Gerencia de Tecnología, como segunda línea de defensa a los riesgos de seguridad de la información para el II trimestre 2024, observando acorde con el informe presentado por el oficial de seguridad que en el segundo trimestre del 2024 NO se presentó materialización de riesgos de seguridad de la información; no así para el III trimestre 2024, en el cual si se presentó materialización de uno de los riesgos.

A continuación, se describe el riesgo materializado durante el III trimestre 2024, correspondiente al proceso Gestión y Desarrollo de las TIC:

Tabla No.8: Riesgo de Seguridad de la Información Materializado III Trimestre 2024

No.	*Proceso*	*No. Del Riesgo*	*Nombre del Riesgo*
1	*Gestión y Desarrollo de las TIC*	*RS-GDT-06*	*Pérdida de Disponibilidad de la mesa de servicios CA*

Fuente: Informe de Seguimiento Riesgos de Seguridad Digital III Trimestre 2024

Respecto de la materialización presentada, la OCI evidenció que la Gerencia de Tecnología gestionó diferentes acciones las cuales estuvieron encaminadas a la verificación y actualización de las vulnerabilidades, amenazas y revaloración del riesgo pasando de bajo a moderado, creando la respectiva actividad dentro del plan de tratamiento, encaminada a mitigar la materialización del riesgo y evitar futuras materializaciones, acorde con lo establecido en el documento técnico DIES-DT-03 V.2 "Política y Metodología de Riesgos de la Unidad"

Para el segundo y tercer trimestres se observó que la Gerencia de Tecnología, en cabeza del Oficial de Seguridad de la Información y el personal de apoyo, una vez revisadas las matrices de riesgos de seguridad de la información/digital y las actividades contempladas en el plan de tratamiento por cada uno de los procesos de la Unidad, se remitió correo electrónico a los enlaces de seguridad de cada proceso, con el fin que se realizarán los ajustes correspondientes a la información reportada; de igual manera se realizaron reuniones con los enlaces, con el fin de aclarar las dudas respecto a lo que se debería reportar en el seguimiento de los planes de tratamiento de riesgos de seguridad digital para el segundo trimestre y tercer trimestres 2024. Una vez, reportado por parte de los procesos de la Unidad que requirieron ajustes, la realización de los mismos en la matriz de riesgos de seguridad digital y en el seguimiento a los planes de tratamiento, se procedió a la consolidación de la información reportada por cada proceso."

"*Riesgos de Seguridad de la Información a corte de 2025*

- *Al corte de junio de 2025 los procesos de Gestión Estratégica de Tecnología y Gestión de Operación de TI en el Mapa de Riesgos Institucional registraron 31 riesgos, clasificados de acuerdo con la zona residual en 22 en nivel bajo, 7 en moderado y 2 en alto. De los anteriores cuatro (4) corresponden a riesgos de gestión, uno (1) a riesgos de corrupción y veintiséis (26) a riesgos de seguridad de la información."*

Tabla No.9: Mapa de Riesgos Institucional Vigencia 2025-V.3

MAPA DE RIESGOS INSTITUCIONAL 2025 V.3				
PROCESOS	BAJO	MODERADO	ALTO	TOTAL RIESGOS POR PROCESO (Gestión, Corrupción, Fiscales, Seguridad Digital)
DIRECCIONAMIENTO ESTRATÉGICO	4	3	0	7
GESTIÓN ESTRATÉGICA DE PERSONAS	15	9	2	26
GESTION DEL CONOC E INNOVACIÓN	3	0	0	3
RELACIONAMIENTO ESTRATÉGICO	12	11	4	27
GESTIÓN EST. DE TECNOLOGÍA	2	2	0	4
GESTIÓN DE INF CATASTRAL Y VALUATORIA	6	5	2	13
GEST. DE INFORMACIÓN GEOGRÁFICA	13	2	1	16
GESTIÓN PRESPTAL Y FINANCIERA	16	5	2	23
GESTIÓN DOCUMENTAL	2	5	2	9
GESTIÓN DE SERV ADMTIVOS	7	0	3	10
GESTIÓN CONTRACTUAL	13	6	0	19
GESTIÓN JURÍDICA	3	7	0	10
GESTIÓN Y OPERACIÓN DE T.I	20	5	2	27
EVALUACIÓN INDEP DE LA GESTIÓN	1	7	1	9
GESTIÓN DISCIPLINARIA	6	10	3	19
TRANSVERSALES (DIR-GGC)	3	3		6
TOTAL	126	80	22	228
% de Participación	55%	35%	10%	100%

Fuente: Elaboración propia con base en el Mapa de Riesgos de la UAECD 2025 V2 publicado página web de la UAECD

"Riesgos de Seguridad de la Información UAECD a corte de 2025

Se observó un total de 142 riesgos, disminuyendo en 28 riesgos respecto del mapa 2024, de ellos 126 en zona de riesgo Bajo, 80 en Moderado y 22 en Alto. La anterior disminución (de 170 a 142) según información del Oficial de Seguridad de la Información obedeció entre otros a los siguientes factores:

- *Criterios de formulación de riesgos*
- *Reducción de activos identificados*
- *Cambio en la cadena de valor*
- *Riesgos en los Territorios*
- *Reorganización de Procesos*
- *Procesos sin riesgos identificados*

De estos riesgos identificados 86 se encontraron en zona residual baja, lo que corresponde a un 60%, 51 en moderada, para un 36% y 5 en zona residual alta- 4%.

- *Para el primer trimestre del 2025 NO se presentó materialización sobre los riesgos de seguridad y privacidad*
- *Para el segundo trimestre del 2025 NO se presentó materialización sobre los riesgos de seguridad y privacidad*
- *Las actividades desarrolladas y las evidencias reportadas están conforme a las actividades programadas por los diferentes procesos.*

6.6 Seguimiento NC y OM

Se revisó el aplicativo PANDORA en el Módulo de Mejoramiento Continuo con el objeto de realizar seguimiento a las No Conformidades y Oportunidades de Mejora a cargo del proceso de Gestión Estratégica de Tecnología, evidenciando que para la vigencia 2023 se registraron cuatro (4) no conformidades y once (11) oportunidades de mejora, en lo que respecta a la vigencia 2024 se encontró una (1) no conformidades y nueve (9) oportunidades de mejora, todas las anteriores con estado "*Cerrado por el autor del hallazgo*", finalmente y en lo corrido de la presente vigencia se observó la apertura de una (1) oportunidad de mejora generada como consecuencia de la ineficacia al cierre de la OM-2024-015, que se encuentra pendiente de iniciar las actividades establecidas para su tratamiento.

A continuación, se detallan cada una de ellas

Tabla No.10: Hallazgos (NC y OM) Proceso Gestión Estratégica de Tecnología

Código	Origen	Fec Regis	Fec Inicio	Fec Termina	Estado
NC-2023-010	O.C.I.	2023-07-07	2023-08-09	2023-12-29	CERRADO POR AUTOR DEL HALLAZGO
NC-2023-011	O.C.I.	2023-06-29	2023-08-09	2024-12-271	CERRADO POR AUTOR DEL HALLAZGO
NC-2023-012	O.C.I.	2023-07-07	2023-08-09	2024-02-28	CERRADO POR AUTOR DEL HALLAZGO
NC-2023-074	O.C.I.	2023-09-08	2023-09-22	2023-12-29	CERRADO POR AUTOR DEL HALLAZGO
NC-2024-062	OAPAP.	2024-10-07	2024-10-16	2025-09-01	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-005	O.C.I.	2023-07-07	2023-08-09	2024-02-28	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-006	O.C.I.	2023-07-07	2023-08-09	2024-02-28	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-007	O.C.I.	2023-07-07	2023-08-09	2024-02-28	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-008	O.C.I.	2023-07-07	2023-08-09	2024-02-28	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-034	O.C.I.	2023-08-10	2023-09-11	2023-12-29	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-035	O.C.I.	2023-08-10	2023-09-01	2024-07-31	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-045	GTIC	2023-08-30	2023-09-01	2024-07-26	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-068	OAPAP	2023-09-18	2023-09-22	2024-02-29	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-069	OAPAP	2023-09-18	2023-09-22	2024-02-29	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-105	O.C.I.	2023-12-18	2024-01-15	2024-02-29	CERRADO POR AUTOR DEL HALLAZGO
OM-2023-106	O.C.I.	2023-12-18	2024-03-29	2024-01-15	CERRADO POR AUTOR DEL HALLAZGO
OM-2024-001	GTIC	2024-01-16	2024-01-16	2024-02-29	CERRADO POR AUTOR DEL HALLAZGO
OM-2024-019	O.C.I.	10/09/2024	2024-08-30	2025-01-31	CERRADO POR AUTOR DEL HALLAZGO
OM-2024-020	O.C.I.	2024-09-10	2024-09-12	2024-10-31	CERRADO POR AUTOR DEL HALLAZGO
OM-2024-021	O.C.I.	2024-09-10	2025-01-02	2025-08-29	CERRADO POR AUTOR DEL HALLAZGO
OM-2024-043	OAPAP	2024-10-07	2024-10-16	2025-03-31	CERRADO POR AUTOR DEL HALLAZGO
OM-2024-051	O.C.I.	2024-11-14	2024-12-02	2025-01-31	CERRADO POR AUTOR DEL HALLAZGO
OM-2025-019	OAPAP	2025-09-15	2025-10-01	2025-12-31	EN PROCESO
OM-2025-020	OAPAP	15/09/2025	1/10/2025	31/12/2025	EN PROCESO
OM-2025-021	OAPAP	2025-09-15	2025-10-01	2025-12-31	EN PROCESO

Fuente: Construcción del Auditor a partir del aplicativo PANDORA

Revisados los datos en la anterior tabla, se resalta la disminución vigencia tras vigencia, en la cantidad de no conformidades y oportunidades de mejora generadas al proceso de Gestión Estratégica de Tecnología, es así como para la vigencia 2023 se registraron quince (15), para 2024 se registraron siete (7) y en lo corrido de 2025 se han registrado tres (3), evidenciando la mejora continua del proceso.

El Instructivo Acciones y Oportunidades de Mejora DIE-04-IN-01, establece

Criterio:
En el numeral 2 Instrucciones – sub numeral 2.5 "El responsable de proceso tiene tres (3) días hábiles, para aprobar la no conformidad u oportunidad de mejora en la herramienta de registro y seguimiento de planes acción y designar el líder implementador"

Situación evidenciada:
Se encontró que tanto las no conformidades como para las oportunidades de mejora, fueron formuladas las actividades de mejora miento de manera oportuna, así mismo, se verificó el cierre de cada una de las No Conformidades y Oportunidades de Mejora por el cumplimiento de la eficacia y efectividad para las primeras (NCs) y la eficacia en el caso de las segundas (OMs), con excepción de las oportunidades de mejora OM2025-019, 20 y 21 generadas por la Oficina Asesora de Planeación el pasado 15 de septiembre en desarrollo de la auditoría interna de calidad, encontrándose estas dentro del término para su desarrollo (31 de diciembre de 2025)

6.7 Seguimiento Indicadores del proceso

6.7.1 Indicadores 2024

Situación evidenciada
Consultado el aplicativo PANDORA en sus módulos de Planeación e Indicadores, en lo relacionado con el proceso de Gestión Estratégica de Tecnología, se observaron los siguientes indicadores al cierre de la vigencia 2024: 1) 4.4.1 Plan Estratégico de Tecnologías de la Información -PETI, 2) GEST-01 Plan de Seguridad y Privacidad de la Información Cumplido, 3) GEST-02 Plan de Continuidad Implementado y 4) GEST-03 Incidentes de Seguridad de la Información que impiden la prestación de Servicios de TI, con los resultados al corte de diciembre 2024 registrados en la tabla a continuación:

Tabla No.11. Indicadores 2024 del Proceso Gestión Estratégica de Tecnología

Indicador	Nombre	Corte	Frecuencia	Tipo	Programado %	Logrado %
4.4.1	Plan Estratégico de Tecnologías de la Información PETI	2024-12	Mensual	Creciente	100	100
GEST-01	Plan de Seguridad y Privacidad de la Información Cumplido	2024-12	Mensual	Creciente	97	100
GEST-02	Plan de Continuidad Implementado	2024-12	Mensual	Creciente	95	100
GEST-03	Incidentes de Seguridad de la Información que impiden la prestación de servicios de TI	2024-12	Trimestral	Constante	75	100

Fuente: Construcción del Auditor a partir del aplicativo PANDORA

6.7.2 Indicadores 2025

Situación evidenciada
Consultado el aplicativo PANDORA en sus módulos de Planeación e Indicadores, en lo relacionado con el proceso de Gestión Estratégica de Tecnología, se observaron los siguientes indicadores al cierre de la vigencia 2025: 1) 4.4.1 Plan Estratégico de Tecnologías de la Información -PETI, 2) GEST-01 Plan de Seguridad y Privacidad de la Información Cumplido, 3) GEST-02 Plan de Continuidad Implementado y 4) GEST-03 Incidentes de Seguridad de la Información que impiden la prestación de Servicios de TI, con los resultados al corte de diciembre 2024 registrados en la tabla a continuación:

Tabla No.12: Indicadores 2025 del Proceso Gestión Documental (corte junio)

Indicador	Nombre	Corte	Frecuencia	Tipo	Programado %	Logrado %
4.4.1	Plan Estratégico de Tecnologías de la Información PETI	2024-12	Mensual	Creciente	47,41	47,41
GEST-01	Plan de Seguridad y Privacidad de la Información Cumplido	2024-12	Mensual	Creciente	44,60	44,60
GEST-02	Plan de Continuidad Implementado	2024-12	Mensual	Creciente	45,45	45,45
GEST-03	Incidentes de Seguridad de la Información que impiden la prestación de servicios de TI	2024-12	Trimestral	Constante	85	100

Fuente: Construcción del Auditor a partir del aplicativo PANDORA

Situación evidenciada:
Si bien es cierto que resta un semestre para el cumplimiento de las metas indicadas en cada uno de los indicadores y que al corte de junio todos cumplen con la ejecución conforme a la programación, se resalta que para los meses de julio y agosto el indicador GEST-01 registra leves diferencias por debajo de lo ejecutado frente a lo programado, es así como para los meses de julio y agosto la programación corresponde al 54,47% y 62,27% frente a ejecuciones del 54,34% y 62,14% respectivamente.

Recomendación:
Por lo anterior, se recomienda determinar la causa que ha llevado a la ligera desviación presentada para los meses de julio y agosto, con el objeto de prevenir que la desviación presentada se incremente o mejor aún corregir la desviación registrada.

6.8 PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Solicitado el Plan de Seguridad y Privacidad de la Información la Gerencia aportó el documento Word denominado "ESTRATEGIA SPI_2024_2027", documento que registra la siguiente información de acuerdo con su tabla de contenido

Gráfica No.6: Plan de Seguridad y Privacidad de la Información

Contenido

Fuente: Gerencia de Tecnología

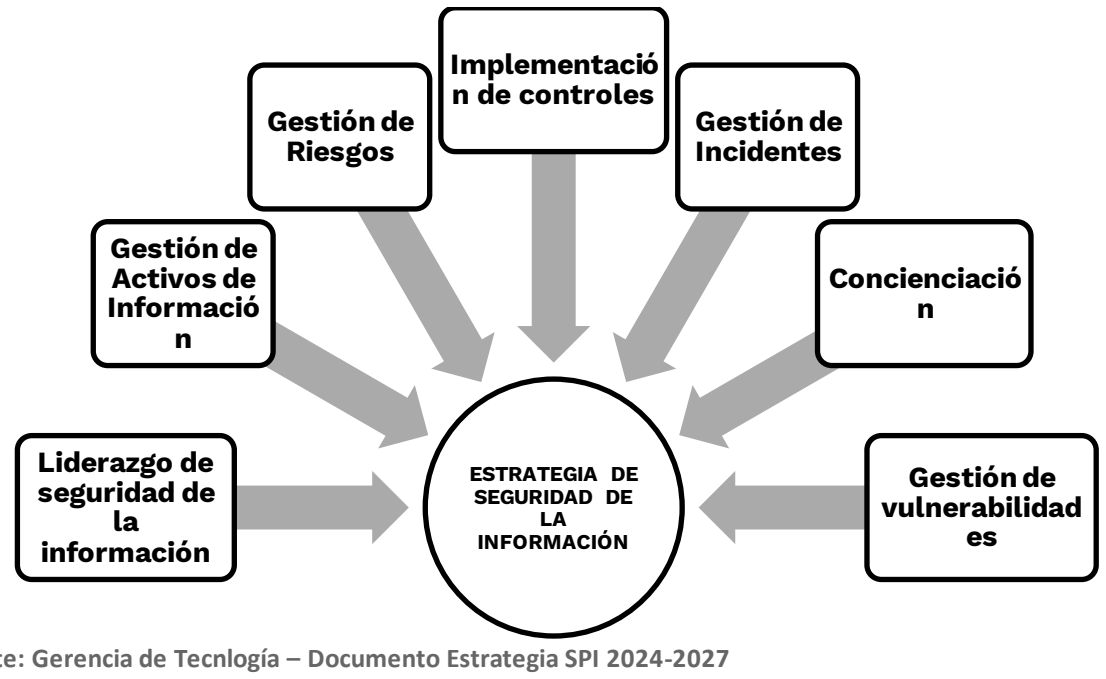
Se plantea como objetivo en este documento

"Alcanzar el estado de madurez deseado en el periodo 2024-2027 en materia de seguridad de la información implementando nuevos controles y fortaleciendo los existentes con el fin de proteger los activos de información de la Unidad y evitar la materialización de riesgos relacionados con la pérdida de confidencialidad, integridad y disponibilidad de los activos de información de la Unidad"
y como objetivos específicos:

- ✓ Establecer el estado de madurez al que se desea llegar en seguridad de la información.
- ✓ Definir las actividades del plan de seguridad y privacidad de la información vigencia 2024-2027

El documento presenta en su numeral 4.2 ESTADO ACTUAL AL 2024 POR DOMINIOS, el estado de los diferentes dominios para la vigencia 2024 y en su numeral 5 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN plantea "Planear, implementar y mantener el Sistema de Gestión de Seguridad de la Información, estableciendo controles de seguridad para evitar la materialización de riesgos relacionados con la pérdida de confidencialidad, integridad y disponibilidad de los activos de información de la Unidad", es así como a partir de este y del establecimiento de los objetivos específicos, establece la Estrategia de Seguridad de la información como "*LA UAECD establecerá una estrategia de seguridad de la información en la que se integren los principios, políticas, procedimientos, instructivos, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, alineado a la gestión de riesgos de seguridad la información, dominio de arquitectura de seguridad y el proceso de gestión de incidentes de seguridad de la información definidos*"

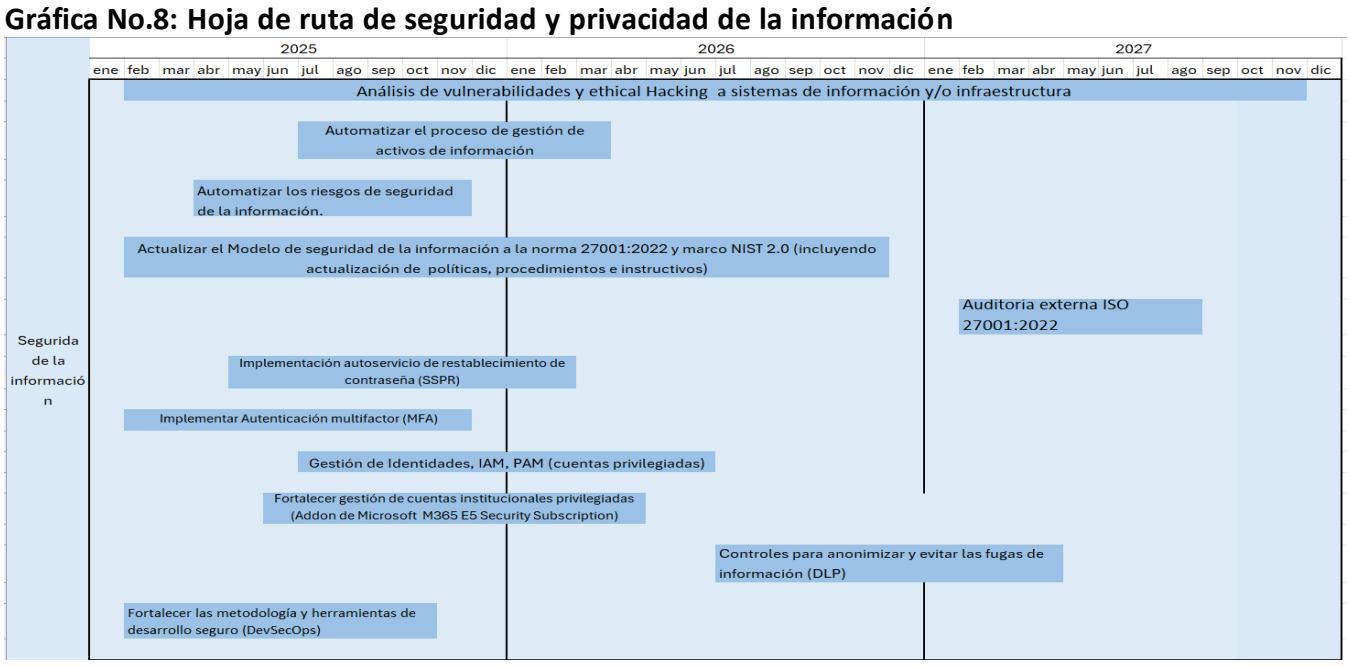
Gráfica No.7: Estrategia Seguridad de la Información



Fuente: Gerencia de Tecnlogía – Documento Estrategia SPI 2024-2027

A partir de lo anterior establece y define las estrategias: 1) Liderazgo de seguridad de la información, 2) Gestión de Activos de Información, 3) Gestión de riesgos, 4) Concientización, 5) Implementación de controles, 6) Gestión de incidentes y 7) Gestión de vulnerabilidades. Con base en lo anterior se establecen las once (11) brechas relevantes de TI que contiene el nombre de la brecha, acción de la brecha y descripción de la misma, lo anterior con el objeto de establecer el Cronograma de Actividades (Plan_SGSI_2 024 Detallado V2.xlsx)

Gráfica No.8: Hoja de ruta de seguridad y privacidad de la información



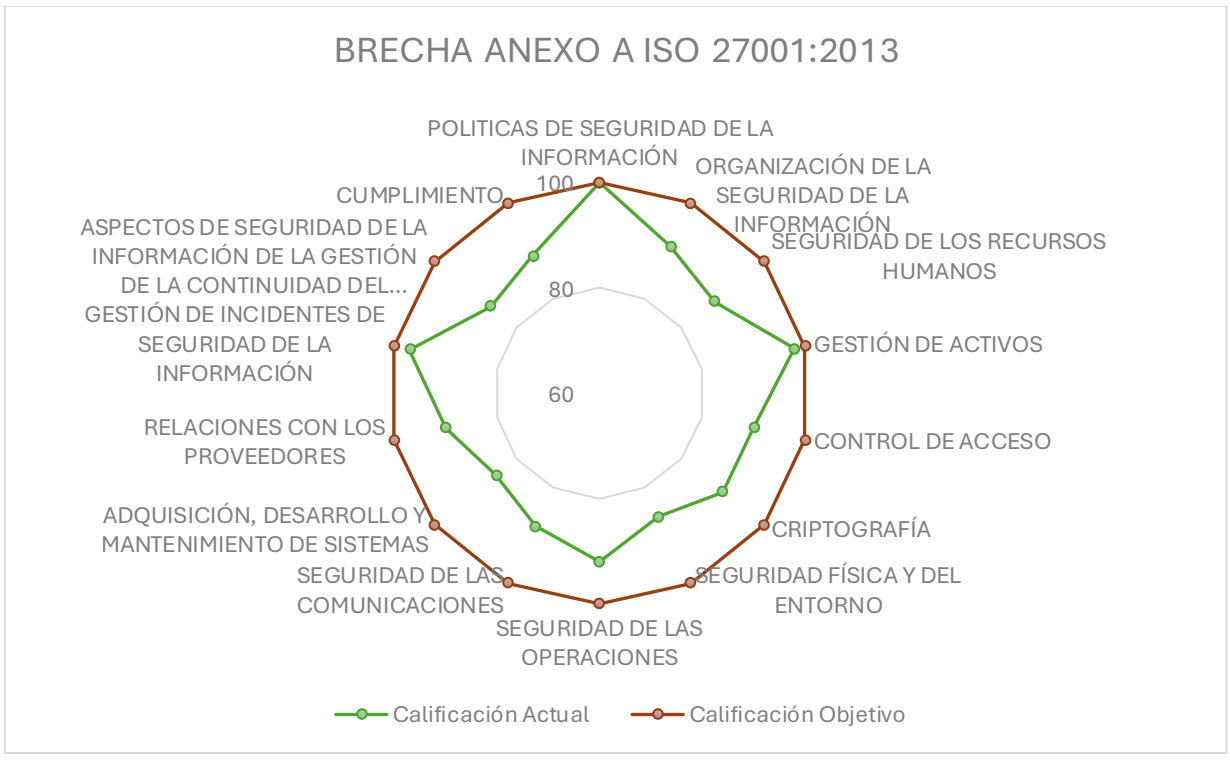
Fuente: Gerencia de Tecnlogía – Documento Estrategia SPI 2024-2027

En conclusión, la Unidad cuenta con el Plan Estratégico de Seguridad y Privacidad de la Información que de manera detallada y a partir de la determinación de sus objetivos específicos y del establecimiento o identificación del Estado Actual para la Unidad pasa a establecer las brechas (hallazgos) y la hoja de ruta y cronograma para el tratamiento de las brechas, estableciendo rangos de tiempo para su implementación.

6.9 EVALUACION MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El archivo Excel "Diagnostico_ Inst_Eval_MSPI_2025" en su hoja "PORTADA" bajo el título "INTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD" diligenciado por la UAECD para el periodo 1 de enero de 2025 a 30 de junio de 2025, registra el nivel de avance de la Unidad en la implementación de los diferentes dominios del Anexo A de la norma ISO 27001:2013 y en la gráfica a continuación registra la Brecha de la UAECD en la implementación de estos

Gráfica No.9: Brechas frente al Anexo A ISO 27001:2013



Fuente: Gerencia de Tecnología Doc Diagnostico_ Inst_Eval_MSPI_2025

La gráfica muestra que los puntajes máximos d la UAECD se encuentran en torno de las Políticas de Seguridad de la Información, Gestión de Activos y Gestión de Incidentes de Seguridad de la Información, a su vez los puntajes más débiles corresponden a Adquisición, Desarrollo y Mantenimiento de Sistemas, Seguridad Física y del Entorno, Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio, Seguridad de los Recursos Humanos y Seguridad de las Comunicaciones.

La anterior gráfica se construye con base en los datos consolidados en el cuadro "Evaluación de Efectividad de controles" mostrado a continuación

Tabla No.13: Evaluación de Efectividad de Controles Anexo A -27001:2013

No.	Evaluación de Efectividad de controles				
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL	Calificación Anterior
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**	100
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	91	100	**OPTIMIZADO**	91
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	88	100	**OPTIMIZADO**	88
A.8	GESTIÓN DE ACTIVOS	98	100	**OPTIMIZADO**	98

A.9	CONTROL DE ACCESO	90	100	**OPTIMIZADO**	90
A.10	CRIPTOGRAFÍA	90	100	**OPTIMIZADO**	90
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	86	100	**OPTIMIZADO**	84
A.12	SEGURIDAD DE LAS OPERACIONES	92	100	**OPTIMIZADO**	90
A.13	SEGURIDAD DE LAS COMUNICACIONES	88	100	**OPTIMIZADO**	88
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	85	100	**OPTIMIZADO**	83
A.15	RELACIONES CON LOS PROVEEDORES	90	100	**OPTIMIZADO**	80
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	97	100	**OPTIMIZADO**	97
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	87	100	**OPTIMIZADO**	80
A.18	CUMPLIMIENTO	89	100	**OPTIMIZADO**	89
PROMEDIO EVALUACIÓN DE CONTROLES		**91**	**100**	**OPTIMIZADO**	89

Fuente: Gerencia de Tecnología - Diagnostico_Inst_Eval_MSPI_2025

La tabla muestra que, dentro del alcance de la presente auditoría, los menores avances se encuentran en la implementación y ejecución de los controles establecidos en los dominios A.14 ADQUISICION, DESARROLLO Y MANTENIMENTO DE SISTEMAS con 85 puntos y A.11 SEGURIDAD FISICA Y DEL ENTORNO con una calificación de 86 puntos, seguido por los dominios A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO con una calificación de 87 puntos, A.7 SEGURIDAD DE LOS RECURSOS HUMANOS y A.13 SEGURIDAD DE LAS COMUNICACIONES con una calificación de 88 puntos y A.18 CUMPLIMIENTO CON 89 puntos, los demás dominios presentan una calificación de 90 puntos por encima. Sin perjuicio de lo anterior. todos los dominios registran una Evaluación de Efectividad de Control en "OPTIMIZADO". Se destaca la gestión efectuada en los dominios A.5 POLITICAS DE SEGURIDAD DE LA INFORMACION y A8 GESTION DE ACTIVOS, que registran calificaciones de 100 y 98 puntos respectivamente, siendo las mayores logradas por la UAECD.

El promedio de calificación de los diferentes dominios arroja un valor de 91 puntos, lo que ubica a la Unidad en el nivel de OPTIMIZADO y registra un avance de 2 puntos con relación a la calificación del periodo anterior. Así mismo, se observa que los dominios se obtuvo una mejor calificación que en la evaluación anterior.

A continuación, se presentan los dominios con sus respectivos sub numerales que registran las menores calificaciones

- **Dominio A.14- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
  Este dominio en las dos últimas vigencias ha registrado calificación de 83 y 85 puntos de 100 posibles, lo anterior evidencia una leve mejora o evolución de periodo 2024 a periodo 2025.

Tabla No.14. Literales Dominio 14

LITERAL	ITEM	CALIFICACION
A.14.1	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.	80
A.14.2	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	96
A.14.3	DATOS DE PRUEBA Asegurar la protección de los datos usados para pruebas.	80

Fuente. Construcción del auditor - Archivo Diagnostico_Inst_Eval_MSPI_2025

- **Dominio A.11- SEGURIDAD FÍSICA Y DEL ENTORNO**
  Este dominio en las dos últimas vigencias ha registrado calificación de 84 y 86 puntos de 100 posibles, lo anterior evidencia una leve mejora o evolución de periodo 2024 a periodo 2025.

Tabla No.15: Literales Dominio 11

LITERAL	ITEM	CALIFICACION
A.11.1	ÁREAS SEGURAS Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	87
A.11.2	EQUIPOS Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	84

Fuente. Construcción del auditor - Archivo Diagnostico_Inst_Eval_MSPI_2025

- **Dominio A.17- ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

Este dominio en las dos últimas vigencias ha registrado calificación de 80 y 87 puntos de 100 posibles, lo anterior evidencia mejora o evolución de periodo 2024 a periodo 2025.

Tabla No.16. Literales Dominio 17

LITERAL	ITEM	CALIFICACION
A.17.1	Continuidad de la seguridad de la información La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.	93
A.17.2	Redundancias Asegurar la disponibilidad de las instalaciones de procesamiento de la información.	80

Fuente. Construcción del auditor - Archivo Diagnostico_Inst_Eval_MSPI_2025

Oportunidad de mejora preliminar

(OM3) Revisado el archivo Excel "Diagnostico_ Inst_Eval_MSPI_2025" en lo relacionado con la Evaluación de Efectividad de controles, se evidenció que los dominios que registran menor calificación corresponden a: A.14 ADQUISICION, DESARROLLO Y MANTENIMENTO DE SISTEMAS, A.11 SEGURIDAD FISICA Y DEL ENTORNO, A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, A.7 SEGURIDAD DE LOS RECURSOS HUMANOS, A.13 SEGURIDAD DE LAS COMUNICACIONES y A.18 CUMPLIMIENTO, lo que podría conllevar la materialización de riesgos de seguridad digital. Se recomienda el análisis basado en enfoque de riesgos para minimizar materializaciones y propender por la mejora continua de la valoración.

Respuesta GT./ No se acepta la oportunidad de mejora, considerando que la UAECD se encuentra actualmente en proceso de migración de la norma ISO/IEC 27001:2013 a su versión 2022. Este proceso permitirá a la Entidad adaptarse a los nuevos estándares internacionales de seguridad de la información, optimizando procesos y alineando los requerimientos del modelo de seguridad y privacidad definido por MinTIC. Cabe resaltar que los controles actuales, conforme a la versión 2013, se encuentran en niveles óptimos de cumplimiento. No obstante, elevar su efectividad por encima del 90% implicaría la asignación de recursos adicionales y la automatización de procesos, lo cual será evaluado en el marco de la consultoría vigente. Como resultado de dicha consultoría, se establecerán actividades de mejoramiento orientadas a los dominios de la norma ISO/IEC 27001:2022, garantizando una transición ordenada y efectiva hacia el nuevo marco normativo.

RESPUESTA OCI:
Revisada la respuesta emitida por la Gerencia de Tecnología en su correo del pasado 3 de octubre, si bien es cierto que conforme lo reportado se encuentran en proceso de migración a la versión 2022 de la norma ISO/IEC 27001, aun esta no se ha producido y por tanto continua aún vigente la versión 2013, sobre la cual se está generando la oportunidad de mejora. En tal sentido, no se acepta la respuesta del proceso y en consecuencia se mantiene la oportunidad de mejora, de la cual muy posiblemente como actividad propuesta, hará parte la migración correspondiente a la versión 2022 con la correspondiente implementación de los controles necesarios.

Si bien es cierto que la Evaluación de Efectividad de Controles ISO27001:2013 en su Anexo A, califica y clasifica a la UAECD en un estado de OPTIMIZADO, es pertinente canalizar y catalizar el desarrollo o ejecución de las recomendaciones establecidas a cada uno de los literales que conforman los diferentes dominios para el mejoramiento continuo de la UAECD y cierre de las brechas establecidas, de manera especial los dominios A.14, A.11, A.17, A.7, A.13 y A.18

Discutido los argumentos de la Gerencia y la OCI, se mantiene la oportunidad de mejora, pero se ajusta la redacción para hacerla más general y orientarla a la actividad actual de diagnóstico y la migración correspondiente a la versión 2022. Esta queda en los siguientes términos:

Oportunidad de mejora definitiva

(OM3) Revisado el archivo Excel "Diagnostico_ Inst_Eval_MSPI_2025" en lo relacionado con la Evaluación de Efectividad de controles, se evidenció que los catorce dominios presentan calificaciones de 85 puntos hacia arriba (de manera particular el dominio A5 registra calificación de 100 sobre 100 puntos), lo que los coloca en estado OPTMIZADO, no obstante, trece de los catorce dominios aún registran brechas para el mejoramiento continuo de la Unidad, por lo que se recomienda analizar estos frente al proceso de migración a la versión 2022 y conforme a lo anterior, establecer las acciones de mejora pertinentes.

ALCALDÍA MAYOR DE BOGOTÁ D.C.	INFORME DE EVALUACIÓN, SEGUIMIENTO O AUDITORÍA

7. Hallazgos

No.	Descripción del hallazgo	No Conformidad	Oportunidad	Norma, criterio, Requisito o Documento asociado	Área /Cargo Responsable	Anexo Evidencia
3	**(OM3)** Revisado el archivo Excel "Diagnostico_ Inst_Eval_MSPI_2025" en lo relacionado con la Evaluación de Efectividad de controles, se evidenció que los catorce dominios presentan calificaciones de 85 puntos hacia arriba (de manera particular el dominio A5 registra calificación de 100 sobre 100 puntos), lo que los coloca en estado OPTMIZADO, no obstante, trece de los catorce dominios aún registran brechas para el mejoramiento continuo de la Unidad, por lo que se recomienda analizar estos frente al proceso de migración a la versión 2022 y conforme a lo anterior, establecer las acciones de mejora pertinentes.		X		Gerencia de Tecnología – Equipo de Seguridad de la Información	Archivo Excel "Diagnostico_ Inst_Eval_MSPI_2025"

8. FORTALEZAS (aplica para auditorías)

- Compromiso desde la Alta Dirección que se refleja en la asignación e incremento de los recursos para temas relacionados con Seguridad de la Información
- Conocimiento y experiencia del funcionario que funge como Oficial de Seguridad de la Información, que se transfiere a los enlaces de seguridad en los procesos, contribuyendo al mejoramiento del SGSPI y que son base o pilar para la gestión de los riesgos de seguridad de la información en la UAECD.
- Actividades desarrolladas en torno a los controles de los diferentes dominios del anexo A de la norma ISO 27001, para el desarrollo y fortalecimiento de los controles que se reflejan en un incremento de 2 puntos para la vigencia 2025, indicativo del mejoramiento en algunas de las brechas determinadas

9. DEBILIDADES:

- Para la vigencia 2025 el Equipo Transversal de Seguridad de la Información se ve impactado por la disminución del número de personas (Funcionarios y contratistas) para el desarrollo de actividades y atención en lo relacionado con seguridad y privacidad de la información .

10. CONCLUSIONES

- En la calificación efectuada en la vigencia 2025 en el Instrumento de Identificación de la Línea Base de Seguridad y la Evaluación de Efectividad de los Controles, se evidencia mejora en 2 puntos respecto de la vigencia anterior, sin perjuicio de lo anterior, es susceptible continuar mejorando en la implementación y cumplimiento de los controles del Anexo A de la norma ISO 27001

- La Unidad Administrativa Especial de Catastro Distrital -UAECD a través de la Gerencia de Tecnología los Oficiales de Seguridad y Privacidad de la Información como la Oficial de Continuidad siguen construyendo, desarrollando, socializando e implementando diferentes instrumentos y documentos necesarios para el desarrollo de la Seguridad y Privacidad de la Información y la Continuidad del Negocio, como es el caso de la Política de Seguridad y Privacidad de la Información, procedimientos, instructivos y documentos técnicos, las charlas de sensibilizaciones.

- Se evidenció en el aplicativo de PANDORA la formulación de indicadores asociados al proceso de Gestión y Desarrollo de las TIC hoy Gestión Estratégica de Tecnología, entre ellos el asociado al Plan de Seguridad y Privacidad de la Información, que son objeto de seguimiento periódico y reporte a la OAPAP a través del aplicativos PANDORA.

- La Unidad tiene publicado en su página web la matriz de riesgos institucional, que recoge los riesgos de gestión, corrupción, fiscales y de seguridad de la información de los diferentes procesos de la Unidad, así mismo se verificó el tratamiento y seguimiento periódico (trimestral) de los riesgos.

- La Unidad a través del Oficial de Seguridad de la Información desarrolló el Instrumento de Identificación de la Línea Base de Seguridad y la Evaluación de Efectividad de los Controles, instrumento que es actualizado en cada vigencia y permite visualizar el estado de implementación de los controles conforme al anexo A de la norma ISO 27001, con el objeto de actualizar el estado de las brechas de seguridad e incluir lo pertinente en el Plan Estratégico de Seguridad de la Información

- Conforme lo informado por el Oficial de Seguridad de la Información, en la presente vigencia se está trabajando para la migración a la versión 2022 en la norma ISO 27001

9. RECOMENDACIONES

- En relación con los indicadores establecidos en el aplicativo PANDORA, de manera específica en el indicador GEST-01 se recomienda determinar la causa que ha llevado a la ligera desviación presentada para los meses de julio y agosto, con el objeto de prevenir que la desviación presentada se incremente o mejor aún, corregir la desviación registrada.

ALCALDÍA MAYOR DE BOGOTÁ D.C.	INFORME DE EVALUACIÓN, SEGUIMIENTO O AUDITORÍA

- Los dominios de la ISO 2701 - 2013 registra calificaciones de 85 puntos hacia arriba lo que los coloca en estado OPTMIZADO, no obstante, trece de ellos aún registran brechas para el mejoramiento continuo de la Unidad, por lo que se recomienda analizar estos frente al proceso de migración a la versión 2022 y conforme a lo anterior, establecer las acciones de mejora pertinentes.

- Los dominios que registran menor calificación corresponden a: A.14 ADQUISICION, DESARROLLO Y MANTENIMENTO DE SISTEMAS, A.11 SEGURIDAD FISICA Y DEL ENTORNO, A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, A.7 SEGURIDAD DE LOS RECURSOS HUMANOS, A.13 SEGURIDAD DE LAS COMUNICACIONES y A.18 CUMPLIMIENTO, lo que podría conllevar la materialización de riesgos de seguridad digital. Se recomienda el análisis basado en enfoque de riesgos para minimizar materializaciones y propender por la mejora continua de la valoración.

El hallazgo de este Informe, determinado como Oportunidades de Mejora, se registrará en el aplicativo Pandora, para que el responsable del proceso determine y ejecute el plan de acción de la situación evidenciada, para posterior seguimiento y verificación a la eficacia y efectividad de las acciones por parte del auditor.

Finalmente, los resultados de este informe y las evidencias obtenidas de acuerdo con los criterios definidos se refieren a los documentos aportados y verificados, no se hacen extensibles a otros soportes.

DIANA KARINA RUIZ PERILLA
Jefe Oficina de Control Interno

Elaboró: Luis Orlando Barrera Cepeda – Contratista OCI