ALCALDÍA MAYOR
DE BOGOTÁ D.C.

UNIDAD ADMIN. CATASTRO DISTRITAL 09-09-2024 11:47:29
Al Contestar Cite Este Nr.:2024IE18561 O 1 Fol:1 Anex:0
ORIGEN: Sd:151 - OFICINA DE CONTROL INTERNO/RUIZ PERILLA DIAN
DESTINO: DIRECCION GENERAL/LOPEZ MORALES OLGA LUCIA/ DIREC
ASUNTO: AUDITORÍA AL PROCESO GESTIÓN Y DESARROLLO DE LAS
OBS: PROYECTO / LUIS ORLANDO BARRERA

MEMORANDO

Referencia: Plan Anual de Auditorías PAA-2024

Fecha: 6 de septiembre de 2024

PARA: Olga Lucia López Morales
Directora UAECD

DE: Diana Karina Ruiz Perilla
Jefe de Oficina de Control Interno

ASUNTO: Auditoría al proceso Gestión y Desarrollo de las TIC - Gestión del Sistema de Seguridad y Privacidad de la información.

Cordial saludo Doctora Olga Lucia:

La Oficina de Control Interno OCI, en el marco de sus actividades orientadas al fortalecimiento del Sistema de Control Interno -SCI de la Unidad Administrativa Especial de Catastro Distrital -UAECD, en ejecución del Plan Anual de Auditorias -PAA vigencia 2024, realizó auditoría al proceso Gestión y Desarrollo de las TIC - Gestión del Sistema de Seguridad y Privacidad de la información.

Como resultado de lo anterior, se ha elaborado el Informe Final de la mencionada Auditoría, que se le está remitiendo con el presente y sobre el cual a continuación, se presentan sus conclusiones y recomendaciones.

CONCLUSIONES:

- La Unidad Administrativa Especial de Catastro Distrital -UAECD a través de la Gerencia de Tecnología y el Oficial de Seguridad de la Información ha construido, desarrollado, socializado e implementado diferentes documentos necesarios para el desarrollo de la Seguridad y Privacidad de la Información, como es el caso de la Política de Seguridad y Privacidad de la Información, procedimiento, instructivos y documentos técnicos.

- 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.

MEMORANDO

- 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 Equipo de Seguridad desarrolló el Plan de Seguridad y Privacidad de la Información para la vigencia 2024, se evidenció su publicación en la Página web de la UAECD. El mismo contiene las actividades, responsables, producto/entregables, como las fechas de inicio y fin para cada actividad.

- 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.

- En la calificación efectuada en la vigencia 2024 en el Instrumento de Identificación de la Línea Base de Seguridad y la Evaluación de Efectividad de los Controles, se evidencia mejora en 5 puntos con la vigencia anterior, no obstante, es susceptible de continuar mejorando en la implementación y cumplimiento de los controles del Anexo A de la norma ISO 27001

RECOMENDACIONES:

- ✓ Revisar y actualizar el Documento Técnico GDT-DT-01 v3, para incluir el Mapa de Procesos debidamente actualizado conforme con la última cadena de valor aprobada para la Unidad.

- ✓ Revisar la posibilidad de ajuste los valores registrados para la medición del Indicador 4.1.D Plan de Seguridad y Privacidad de la Información Cumplido.

- ✓ Actualizar el indicador GEST-01 Plan de Seguridad y Privacidad de la Información, con el objeto de incluir los valores correspondientes al mes de junio, que permitan efectuar la medición cuantitativa y cualitativa para el mes de junio.

- ✓ Desarrollar las actividades correspondientes al mapa de riesgos institucional en lo referente al plan de manejo de riesgo -PMR de los procesos de Gestión Contractual y Gestión Jurídica, que no han sido iniciadas.

MEMORANDO

- ✓ Continuar con la implementación y fortalecimiento de los controles del anexo A de la norma ISO 27001, priorizando aquellos ítems que registran menor calificación.

Atentamente,

DIANA KARINA RUIZ PERILLA
Jefe Oficina de Control Interno

Elaboró: Luis Orlando Barrera C –Líder de Auditoría -Contratista O.C.I
Revisó: Diana Karina Ruiz Perilla – Jefe Oficina de Control Interno

Copia: Ing. Francisco Rodríguez Eraso – Gerente de Tecnología
Dr. Orlando José Maya M – Jefe OAPAP
Dra. Luz Elena Rodríguez Q – Subgerente Gestión Jurídica
Dra. Derly Jhoana León – Subgerente de Contratación
Comité Institucional de Coordinación de Control Interno

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 **2024,** a continuación, se presentan los resultados del Informe de Auditoría al proceso Gestión y Desarrollo de las TIC - 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: Proceso Gestión y Desarrollo de las TIC - Sistema de Gestión de Seguridad y Privacidad de la Información.

NOMBRE DEL INFORME: Auditoría al proceso Gestión y Desarrollo de las TIC - 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 2023 y 2024), 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 2023 y 2024.
- 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: Verificar las brechas identificadas por el Equipo de Seguridad de la Información de la Gerencia de Tecnología y las actividades implementadas por la Unidad en lo relacionado con el Anexo A de la norma ISO 27001, así como el Plan de Seguridad y Privacidad de la Unidad para las vigencias 2023 y 2024. Periodo a evaluar 01-07-2023 al 30-06-2024

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. *"Lineamientos para prevenir conductas irregulares relacionadas con el incumplimiento de los manuales de funciones y competencias laborales, 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.

- Resolución 732 del 1 de septiembre de 2020 de la UAECD. "*Por la cual se adopta la Política de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial de Catastro Distrital*"
- Decreto 767 de 2022 del MINTIC "*Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital …*"
- 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, de manera particular, el Anexo A de la norma ISO 27001.

Además, serán tenidos en cuenta los 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 realizó dentro del marco de las normas internacionales de auditoría, que incluye: Planeación, ejecución, generación y comunicación del informe con las conclusiones y recomendaciones, que tienen como objetivo el contribuir al mejoramiento del Sistema de Control Interno -SCI.

El desarrollo de la auditoría se realizó mediante solicitudes de información que fue suministrada en el OneDrive establecido para tal fin, así mismo en sesión de trabajo virtual efectuada con personal de la Gerencia de Tecnología, de manera específica con el Oficial de Seguridad de la Información y el enlace de calidad. se revisó el procedimiento GDT-PR-03 v2 PROCEDIMIENTO GESTION DE SEGURIDAD Y PRIVACIDAD DE LAINFORMACION, así como los instructivos y documentos técnicos, con el propósito de constatar la adecuada aplicación de los mismos, también se efectuó revisión documental de los documentos aportados en el OneDrive de acuerdo a la solicitud 1 de información, así mismo, se revisaron los riesgos de gestión, corrupción y seguridad, así como los indicadores asociados a Seguridad de la Información

La auditoría se ejecutó en el periodo comprendido entre el 2 de julio y el 30 de agosto de 2024, por el auditor ingeniero de sistemas de la OCI, Luis Orlando Barrera Cepeda. Como ya se mencionó, el periodo evaluado corresponde al comprendido entre el 1 de julio de 2023 al 30 de junio de 2024. La

información requerida para el desarrollo del presente ejercicio fue dispuesta en el One Drive https://catastrobogotacol-my.sharepoint.com/my?login_hint=lobarrera%40catastrobogota%2Egov%2Eco&id=%2Fpersonal%2Flobarrera%5Fcatastrobogota%5Fgov%5Fco%2FDocuments%2F2023%5FAud%5FGT%2DDes%5FSist%5FInfo

Así mismo, se suministró información a través del SharePoint en el enlace https://catastrobogotacol.sharepoint.com/sites/GerenciaTecnologa-GOBIERNODIGITAL/Shared%20Documents/Forms/AllItems.aspx?FolderCTID=0x012000ACB235DA450CEE49B9144ABDB139115A&id=%2Fsites%2FGerenciaTecnologa%2DGOBIERNODIGITAL%2FShared%20Documents%2FGOBIERNO%20DIGITAL%2FGobierno%20Digital%2F3%2E%20SegInf%2F3%2E3%20Doc%5FOper%2FRiesgosSD repositorio en lo relacionado con riesgos de seguridad digital, suministrado previamente por Seguridad de la Información.

6. PRESENTACIÓN DE RESULTADOS

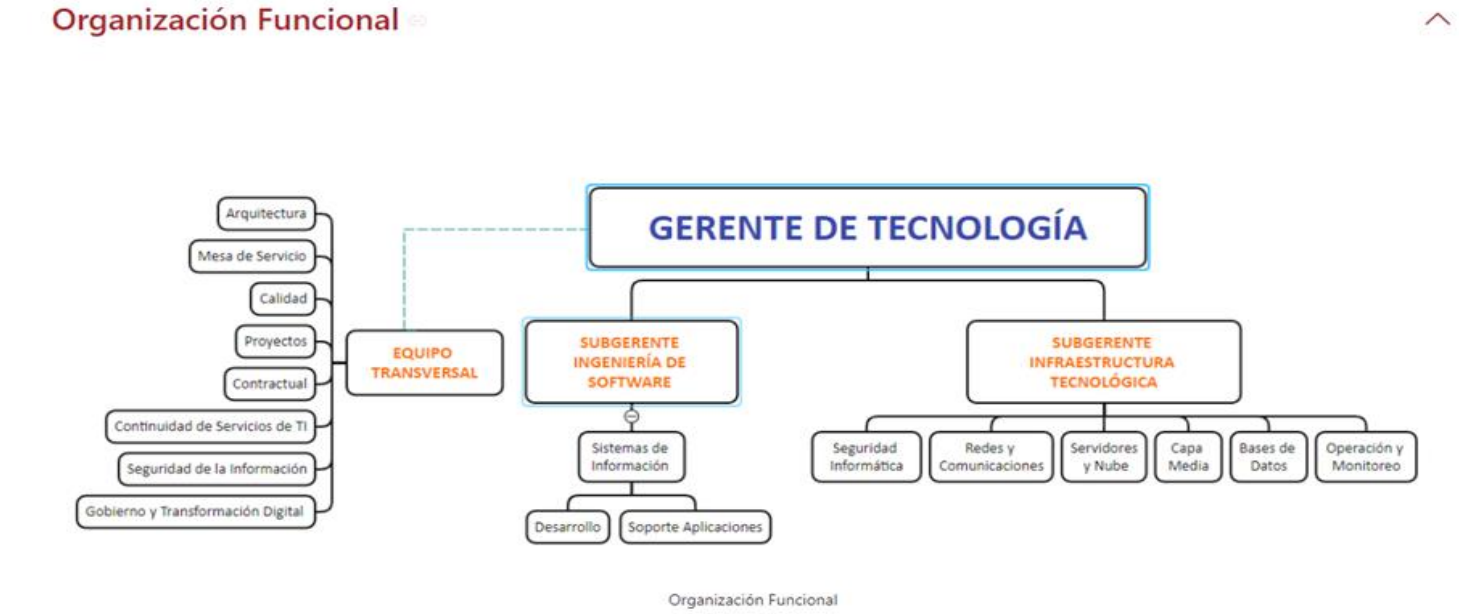
En desarrollo del ejercicio auditor, se solicitó a los enlaces designados para el suministro de la información, ingeniero Luis Albeiro Cortés e ingeniera Ana Betsabeth Avila, entregar o suministrar la información en el OneDrive dispuesto para tal fin, para lo cual se les compartió el enlace correspondiente, ya citado en el numeral anterior. Información que fue requerida en memorando 2024IE13844 del 17 de julio y correos electrónicos. Información suministrada con oportunidad.

6.1 Organización Funcional Gerencia de Tecnología

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

6.2 Presupuesto Gerencia de Tecnología

En lo que refiere al presupuesto para las vigencias 2023 y 2024 de la Gerencia de Tecnología, se encontró una variación final negativa del 42,11% para la presente vigencia, lo que equivale a una disminución de $5.308.860.860 para la vigencia 2024. Como se ilustra en el siguiente cuadro:

Tabla 1. Presupuesto Gerencia de Tecnología

Vigencia	Presupuesto Gerencia Tecnología
2023	$13.414.651.951
2024 A	$ 7.765.517.792
2024 N	$ 8.105.791.091

Fuente: Información suministrada por la Gerencia de Tecnología a Solicitud 1

Manifiesta la Gerencia que la variación está dada por priorización de los proyectos de la dependencia, proveniente de la planeación estratégica de la entidad.

Ahora, requerida la información correspondiente a los recursos que para las dos vigencias correspondían a Seguridad de la Información, fue informado que para el año 2023 los recursos fueron del orden de $1.103.319.333 de los cuales $956.000.000 corresponden a “Prestación de Servicios de garantía, soporte y mantenimiento para los equipos de seguridad informática con que cuenta la UAECD”. Para la vigencia 2024 los recursos ascienden a $1.392.191.000 en CDP y finalmente en CRP $1.292.191.000 establecidos para “Prestación de servicios de garantía, soporte, mantenimiento y

actualización para los equipos de seguridad informática, con que cuenta la UAECD, así como el servicio de monitoreo y seguridad SOC", lo anterior con respecto a la vigencia 2023 determina la no contratación de dos (2) profesionales entre ellos quien se encargaba de evaluar el avance de la implementación y realizar la planeación e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la UAECD, de acuerdo con la brecha establecida con la herramienta de MINTIC.

6.3 Política Seguridad y Privacidad de la Información

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" GDT-DT-01 versión 3 de fecha 20-03-2024*" 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.

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:
Se revisó el Acta No. 14 de la reunión del Comité de Gestión y Desempeño llevada a cabo el 27 de diciembre de 2023, evidenciando que en el numeral 6 del orden del día, se efectuó la Revisión de la política general y detalladas de seguridad y privacidad de la información y aprobación política de continuidad del negocio de la UAECD y política de continuidad de TI, incluyendo la política Seguridad para servicios en nube.

Así mismo, los cambios más relevantes en 2023 relacionados con el Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, corresponden a: 1.) Revisión y ajustes generales al documento DT SPI, 2.) Revisión y ajustes de los lineamientos y políticas de Gestión de Activos -Reglas para el uso de los repositorios de información y 3.) Inclusión de la política de seguridad para servicios en nube, que fueron presentados al Comité y aprobados por el mismo, como consta en acta 14

6.4 Procedimiento, Instructivos y Documentos Técnicos

Revisado el aplicativo PANDORA en lo que refiere al proceso Gestión y Desarrollo de las TIC – Seguridad de la Información, se observaron los siguientes documentos i). Procedimiento GDT-PR-03 "Procedimiento Seguridad y Privacidad de la Información", ii). Documentos Técnicos GDT-DT -01 "Documentro Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información" y GDT-DT-04 "Documento Técnico Controles de Seguridad de la Información para la Construcción de Software Seguro" y iii). Intructivos GDT-03-IN-01 "Instructivo de Gestión de Activos de Información", GDT-03-IN-02 "Instructivo Gestión de Incidentes de Seguridad de la Información", GDT-03-IN-03 "Instructivo Cifrado de Información" y GDT-03-IN-04 "Instructivo Análisis Forense Digital", copia de estos documentos fueron aportados por el Equipo de Seguiridad de la Información de la Gerencia de Tecnología en la respuesta al punto 6 de la solicitud 1.

Situaciones evidenciadas

- Procedimiento de Gestión de Seguridad y Privacidad de la Información GDT-PR-03.
  Este procedimiento presenta dos (2) versiones en el periodo de alcance de la auditoría, siendo el objetivo del procedimiento "Determinar las actividades para *planear, implementar y mantener el Sistema de Gestión de Seguridad de la Información, a través de la definición y ejecución de las actividades del Plan de Seguridad y Privacidad de la Información acordado para la vigencia, estableciendo controles necesarios para mitigar la materialización de los riesgos de seguridad relacionados con pérdida de confidencialidad, integridad y disponibilidad apoyados en un proceso de mejora continua*",

La primera corresponde a la versión 1 del 24 de mayo de 2022, contempla diez (10) actividades y dos (2) puntos de control en las actividades 4 y 6, para ser desarrollados por el Comité de Gestión y Desempeño.
La segunda versión presenta trece (13) actividades incluidos dos (2) puntos de control en las actividades 4 y 8, para ser desarrollados por el Comité de Gestión y Desempeño.

Criterio:
El primer control está asociado a la presentación del Plan de Seguridad y Privacidad de la información y la respectiva aprobación por el Comité de Gestión y Desempeño, el segundo control corresponde a la aprobación por parte del mencionado comité, del plan de tratamiento de riesgos de seguridad de la información.

Situación evidenciada:
Conforme con el Acta No. 14 del Comité virtual de Gestión y Desempeño, desarrollada el 27 de diciembre de 2023, en los numerales 5.12 Plan de Seguridad y Privacidad de la Información 2024, 5.13 Plan de Tratamiento de Riesgos de Seguridad Digital y 5.14 Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI, del orden del día, fueron presentados los planes referidos y sometidos a su aprobación, siendo aprobados por mayoría, dando de esta manera cumplimiento al procedimiento GDT-PR-03.

- Instructivo de Gestión de Activos de Información **GDT-03-IN-01** versión 1, de fecha 10 de junio de 2022, actualizado a través de la versión 2 de fecha 27 de marzo de 2024. El objetivo del mismo es "*Identificar, clasificar, etiquetar, mantener actualizados y publicados los inventarios de activos para monitorear la posible materialización de riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información con el fin de establecer los controles de seguridad correspondientes para evitar los riesgos de seguridad de la información a los que pueden estar expuestos estos activos de información*".
El instructivo en la última versión presenta dos puntos de control, el primero de ellos en desarrollo de la actividad 3 y el segundo en la actividad 4.

Criterio 1:
Asesorar y revisar respecto al diligenciamnento del inventario de activos de información del proceso, actividad desarrollada por el Equipo Revisor (Oficial de Seguridad de la Información, Gestión Documental y Gestión Jurídica). Esta actividad tiene como objetivo revisar que el inventario cumple con los lineamientos dados en este instructivo.

Criterio 2:
Revisar y aprobar el inventario de activos de información de su dependencia/proceso. Esta actividad tiene como objetivo revisar y aprobar el inventario por parte del propietario del activo de información y es desarrollada por el propietario del activo o responsable del proceso.

Situación evidenciada:
Para la revisión de los activos de información en la vigencia 2023 y haciendo uso del instructivo en su versión1, el Equipo de Seguridad de la Información llevó a cabo sensibilización con los enlaces de los procesos en el mes de mayo, presentado entre otros ítems el cronograma de actividades que comprende desde el 8 de mayo hasta el 31 de agosto de 2023. La responsabilidad del cumplimiento del instructivo se centra principalmente en el propietario del activo o responsable de cada proceso. El instructivo cuenta con un punto de control en la actividad No.3 a cargo del Equipo Revisor y de acuerdo al cronograma, se desarrolla desde el 1 de julio hasta el 15 de agosto.
Para la vigencia 2024 el instructivo se desarrolla sobre la versión 2 del mismo, para ello en correo del 2 de agosto de 2024 se socializó el Boletín Informativo GEST-BI-01: Construcción y Reporte Mapa de Riesgos Seguridad Digital, Activos de Información, BIA y BCP, sobre el cual a nivel de la Unidad se viene haciendo el desarrollo pertinente conforme al Plan de trabajo – Cronograma determinado.

- Instructivo Gestión de Incidentes de Seguridad de la Información **GDT-03-IN-02**, versión 1 de fecha 10 de junio de 2022, actualizado a través de la versión 2 de fecha 27 de marzo de 2024. El objetivo del instructivo corresponde a "*Gestionar adecuadamente los eventos e incidentes de seguridad y privacidad de la información ejecutando de manera oportuna las acciones que los contengan y mitiguen incluyendo las actividades de identificación, adquisición y preservación de información que pueda servir como evidencia, con el fin de fortalecer los controles que permitan mitigar la materialización de riesgos de seguridad de la información*".
El instructivo está conformado por 16 actividades con puntos de control en las actividades 10 y 14.

Criterio 1:
Actividad 10: Formalizar y verificar el plan de trabajo formal para la atención del incidente de seguridad o privacidad de la información, actividad desarrollada por el Equipo de Respuesta a Incidente de Seguridad de la Información. Se establece como autocontrol y tiene como objetivo 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. Actividad a cargo de Equipo de Respuesta a Incidentes de seguridad de la información.

Criterio 2:
Actividad 14: Revisar si se vulneró alguna política de seguridad, actividad desarrollada por el Equipo de Respuesta a Incidente de Seguridad de la Información para determinar si el incidente fue resuelto con el plan de trabajo propuesto o si se requieren acciones adicionales que permitan su contención o mitigación. Actividad a cargo del Equipo de Respuesta a Incidentes de seguridad de la información.

Situación evidenciada:
Para el segundo trimestre de 2023, se presentó materialización del riesgo afectando el File Server y la disponibilidad de la información en diferentes procesos, originado en el daño de la PCA. El

Equipo de Seguridad de la Información recepcionó correos informativos de materialización de riesgos de seguridad digital, solicitó la revisión y de ser pertinente, la reformulación del riesgo, sus controles y plan de manejo de riesgo, así mismo, se debe reportar si los riesgos residuales en nivel bajo continuaban igual, así como las matrices de los procesos.
Para los dos primeros trimestres de 2024, se informa la No materialización de riesgos.

- Instructivo de Cifrado de Información **GDT-03-IN-03** versión 1 de fecha 10 de junio de 2022, actualizado mediante versión 2 del 27 de marzo de 2024. El objetivo del instructivo corresponde a "*Definir los mecanismos de cifrado de información de la Unidad que deben ser tenidos en cuenta por las dependencias cuando se va a realizar un proceso de almacenamiento, intercambio / transferencia de información pública reservada o pública clasificada, con el objetivo de protegerla y prevenir su modificación y divulgación por parte de personas no autorizadas preservando la confidencialidad e integridad de esta*". Establece el paso a paso para el uso de diferentes herramientas como es el caso de 7-Zip para cifrado de información - Cifrado de información mediante Cryptomator - Cifrado de información mediante envío de correo seguro - Envío e intercambio de información cifrada mediante WormHole - Cifrado de información mediante GPG4USB - Cifrado de información mediante Veracryptor. Este instructivo no presenta puntos de control, donde las actividades están a cargo del Usuario o analista de primer nivel.

- Instructivo Análisis Forense Digital **GDT-03-IN-04** versión 1 de fecha 15 de diciembre de 2022, actualizado a través de la versión 2 del 27 de marzo de 2024. El objetivo del instructivo corresponde a "*Establecer el paso a paso de un análisis forense con el fin de asegurar, identificar, recolectar, preservar y presentar la evidencia forense referente a incidentes de seguridad de la información que se presenten en la infraestructura tecnológica de la UAECD (Equipos de cómputo, Servidores, equipos de red/seguridad perimetral y correo electrónico)*".
  Recomienda el instructivo que los lineamientos presentados se empleen específicamente en la fase de identificación, recolección, adquisición y preservación (ver GDT-03-IN-02 Instructivo Gestión de Incidentes de Seguridad de la información), ya que en este punto aún no se realiza manipulación de la información ni se afecta la integridad de esta, permitiendo obtener la evidencia necesaria adecuadamente.
  Registra 21 actividades y no establece controles, las cuales en su gran mayoría están a cargo del Oficial de Seguridad de la Información.

- Instructivo Gestión de Accesos **GDT-05-IN-01** versión 4 del 27 de marzo de 2024. El objetivo del instructivo corresponde a "*Gestionar la creación, activación, desactivación y/o modificación de las cuentas de usuario, sus privilegios o permisos para el acceso a la información y a los diferentes recursos tecnológicos que soportan los servicios de TI, relacionados en el catálogo de servicios de TI de la Unidad Administrativa Especial de Catastro Distrital – UAECD con la finalidad de salvaguardar la información de la Unidad y entregar oportunamente y con calidad, los servicios a los usuarios"*
  Registra 24 actividades, de las cuales seis (6) presentan punto de control. La primera de ellas es la actividad "*4. Revisar el formato*" por cuanto a través de ella se verifica que la solicitud está completa

y realizada por una persona autorizada, actividad a cargo del Operador gestión de cuentas de usuario; la segunda corresponde a la actividad "*9. Validar respuesta*" por cuanto permite verificar que la solicitud se haya gestionado completamente de acuerdo con la solicitud, actividad a cargo de Operador de cuentas de usuario; la tercera corresponde a "*10. Verificar los requisitos mínimos*" dado que a través de ella se mitiga el riesgo de afectación a la integridad, disponibilidad y confidencialidad de la información de la Entidad", actividad a cargo del Analista de primer nivel; la cuarta es "1*5. Revisar y solicitar depuraciones mensuales cuentas usuarios de red*" porque a través de ella se verifica que las cuentas de usuario activas de los sistemas de información sean las correctas, actividad a cargo de Jefes de Dependencias o a quien designe; la quinta es "*18. Revisar y solicitar depuraciones semestrales cuentas de usuario administradoras*" porque permite verificar que las cuentas de usuario administradoras y sus permisos o privilegios sean las correctas, actividad a cargo del Gestor de accesos y la sexta es "*22. Revisar reporte cuentas de usuario red activas*" dado que permite verificar que las cuentas de usuario y sus permisos o privilegios sean las correctas, actividad a cargo de Jefes de Dependencias o a quien ellos designen.

Este instructivo se utiliza por los diferentes procesos o dependencias de manera frecuente, adicionalmente en varios de los mapas de riesgos de seguridad de la información, algunas de las actividades de control forman parte de los controles establecidos o de las actividades establecidas en los planes de manejo de riesgo

- Instructivo Gestión de Accesos **GDT-05-IN-02** versión 2 del 27 de marzo de 2024. El objetivo corresponde a "*Realizar la definición, programación, ejecución y verificación de las copias de respaldo y la recuperación de los datos e información de la Unidad Administrativa Especial de Catastro Distrital – UAECD, soportados en la Infraestructura Tecnológica*", presenta 26 actividades, una de ellas como punto de control y corresponde a la actividad "*4. Verificar la ejecución de la Programación de las copias de respaldo*" porque permite verificar la correcta ejecución de la programación de las copias de respaldo en la solución de la Unidad, actividad desarrollada por el Operador del Data Center. La periodicidad de los respaldos puede ser diaria, semanal, mensual, anual por demanda, actividades que están cargo del Operador del Data Center.

- Instructivo Gestión de la Capacidad y Disponibilidad **GDT-05-IN-03** versión 1 del 10 de mayo de 2024. El objetivo corresponde a "*Mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro y de los requerimientos de capacidad de la Unidad Administrativa Especial de Catastro Distrital*", compuesto por 9 actividades y ninguna de ellas es punto de control, actividades que están cargo de diferentes roles de la Gerencia de Tecnología (Administradores de servicio de infraestructura, Subgerente de Infraestructura Tecnológica, Gerente de Tecnología).

Finalmente, la Unidad cuenta con los siguientes Documentos Ténicos

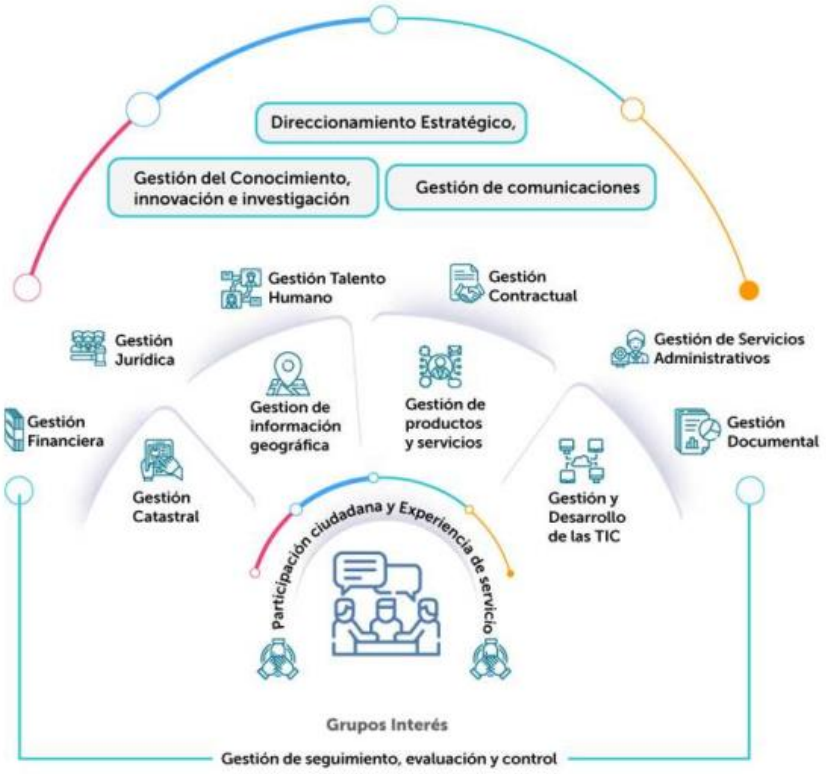
- GDT-DT-01 - V3, DOCUMENTO TECNICO MANUAL DE POLITICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, versión 3, del 20 de marzo de 2024, que presenta como objetivo "Definir y disponer para conocimiento y cumplimiento de todos los

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".

Criterio:
"El alcance de la Gestión de Seguridad de la Información de la UAECD comprende todos los procesos de la cadena de valor de la Unidad Administrativa Especial de Catastro Distrital según declaración de aplicabilidad vigente.

Situación evidenciada:
El Documento Técnico GDT-DT-01 - V3 presenta en el numeral 2.5 Alcance del SGSI el Mapa de Procesos de la anterior cadena de valor de la UAECD (mostrado en la gráfica a continuación), lo anterior debido a que este documento técnico fue emitido el 20 de marzo de 2024 y la nueva cadena de valor fue aprobada en mayo de 2024. Así las cosas, el DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, requiere de actualización en el ítem ALCANCE a efecto de hacerlo coherente con la realidad de la Unidad

Gráfica 2: Mapa de Procesos de la UAECD



Fuente: Documento Técnico Manual de Políticas de Seguridd y Privacidad de la Información

(OM1): Se evidenció que el Mapa de Procesos presentado en el numeral 2.5 ALCANCE DEL SGSI del Documento Técnico GDT-DT-01 - V3, no corresponde a la actual cadena de valor de la UAECD, por lo anterior, se debe actualizar el DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Observación del proceso:
"*Se acepta esta Oportunidad de Mejora, indicando que en la publicación de documentación de los procesos para la nueva cadena de valor, se actualizó el diagrama, y que esta publicación se realizará el 1 de septiembre/24. Adicionalmente y de acuerdo al Plan de Seguridad y Privacidad de la Información, la actividad relacionada ala actualización de este documento técnico está programada para ejecutarse en octubre - noviembre de 2024.*"

Respuesta OCI:
A partir de la respuesta de la Gerencia de Tecnología en la que se acepta la oportunidad de mejora, se mantiene la observación.

- GDT-DT-04 - V2, DOCUMENTO TECNICO CONTROLES DE SEGURIDAD DE LA INFORMACION PARA LA CONSTRUCCION DE SOFTWARE SEGURO, del 20 de marzo de 2024, siendo su objetivo el "Establecer los controles de seguridad y privacidad de la información para el desarrollo de sistemas de información nuevos o mejoras a los ya existentes, con el fin de proteger los activos de información que se encuentran involucrados en el ciclo de desarrollo del software".

  Presenta acápite de los Controles para los ambientes de software y otro para Controles para la seguridad del sistema de información en el ciclo de vida de desarrollo de software

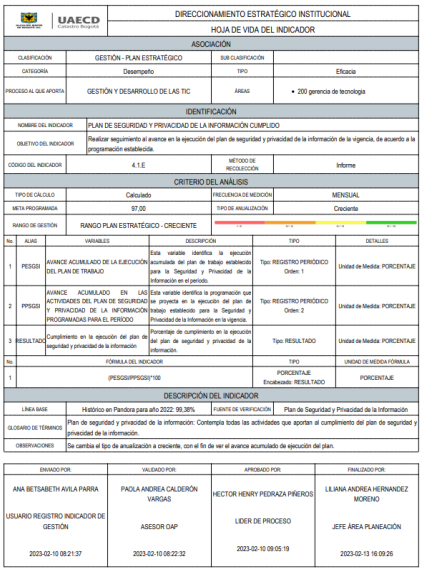
6.5 Indicadores

Criterio:

- De los indicadores establecidos por la Gerencia de Tecnología, solo uno (1), el indicador 4.1.E PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION CUMPLIDO está orientado a Seguridad y Privacidad de la Información y específicamente a "Realizar seguimiento al avance en la ejecución del plan de seguridad y privacidad de la información de la vigencia, de acuerdo a la programación establecida.", registra el indicador como meta programada el 97%, con frecuencia de medición mensual y tipo de anualización creciente

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

Gráfica 3. Hoja Indicador 4.1.E



UAECD Catastro Bogotá — DIRECCIONAMIENTO ESTRATÉGICO INSTITUCIONAL

HOJA DE VIDA DEL INDICADOR

ASOCIACIÓN

CLASIFICACIÓN	GESTIÓN - PLAN ESTRATÉGICO	SUB CLASIFICACIÓN	
CATEGORÍA	Desempeño	TIPO	Eficacia
PROCESO AL QUE APORTA	GESTIÓN Y DESARROLLO DE LAS TIC	ÁREAS	• 200 gerencia de tecnología

IDENTIFICACIÓN

NOMBRE DEL INDICADOR	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CUMPLIDO		
OBJETIVO DEL INDICADOR	Realizar seguimiento al avance en la ejecución del plan de seguridad y privacidad de la información de la vigencia, de acuerdo a la programación establecida.		
CÓDIGO DEL INDICADOR	4.1.E	MÉTODO DE RECOLECCIÓN	Informe

CRITERIO DEL ANÁLISIS

TIPO DE CÁLCULO	Calculado	FRECUENCIA DE MEDICIÓN	MENSUAL
META PROGRAMADA	97,00	TIPO DE ANUALIZACIÓN	Creciente
RANGO DE GESTIÓN	RANGO PLAN ESTRATÉGICO - CRECIENTE		

No.	ALIAS	VARIABLES	DESCRIPCIÓN	TIPO	DETALLES
1	PESGSI	AVANCE ACUMULADO DE LA EJECUCIÓN DEL PLAN DE TRABAJO	Esta variable identifica la ejecución acumulada del plan de trabajo establecido para la Seguridad y Privacidad de la Información en el periodo.	Tipo: REGISTRO PERÓDICO Orden: 1	Unidad de Medida: PORCENTAJE
2	PPSGSI	AVANCE ACUMULADO EN LAS ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PROGRAMADAS PARA EL PERÍODO	Esta variable identifica la programación que se proyecta en la ejecución del plan de trabajo establecido para la Seguridad y Privacidad de la Información en la vigencia.	Tipo: REGISTRO PERÓDICO Orden: 2	Unidad de Medida: PORCENTAJE
3	RESULTADO	Cumplimiento en la ejecución del plan de seguridad y privacidad de la información	Porcentaje de cumplimiento en la ejecución del plan de seguridad y privacidad de la información.	Tipo: RESULTADO	Unidad de Medida: PORCENTAJE

No.	FÓRMULA DEL INDICADOR	TIPO	UNIDAD DE MEDIDA FÓRMULA
1	(PESGSI/PPSGSI)*100	PORCENTAJE Encabezado: RESULTADO	PORCENTAJE

DESCRIPCIÓN DEL INDICADOR

LÍNEA BASE	Histórico en Pandora para año 2022: 99,38%	FUENTE DE VERIFICACIÓN	Plan de Seguridad y Privacidad de la Información
GLOSARIO DE TÉRMINOS	Plan de seguridad y privacidad de la información: Contempla todas las actividades que aportan al cumplimiento del plan de seguridad y privacidad de la información.		
OBSERVACIONES	Se cambia el tipo de anualización a creciente, con el fin de ver el avance acumulado de ejecución del plan.		

ENVIADO POR:	VALIDADO POR:	APROBADO POR:	FINALIZADO POR:
ANA BETSABETH AVILA PARRA	PAOLA ANDREA CALDERÓN VARGAS	HECTOR HENRY PEDRAZA PIÑEROS	LILIANA ANDREA HERNANDEZ MORENO
USUARIO REGISTRO INDICADOR DE GESTIÓN	ASESOR OAP	LIDER DE PROCESO	JEFE ÁREA PLANEACIÓN
2023-02-10 08:21:37	2023-02-10 08:22:32	2023-02-10 09:05:19	2023-02-13 16:09:26

Fuente: Aplicativo PANDORA

Situación evidenciada:

El indicador presenta dos actividades clave para su desarrollo, la primera corresponde a “Elaborar diagnóstico, identificación de brechas y diseño del plan de seguridad y privacidad” programada para ser desarrollada en el mes de enero, con una ejecución del 100%.

La segunda actividad corresponde a “Seguimiento a la ejecución del plan de seguridad y privacidad”, con una programación para su desarrollo del 8,33% para cada mes a partir del mes de enero, al cierre de la vigencia (31 de diciembre 2023) reporta ejecución del 100%.

La medición del indicador que como ya se mencionó es de anualización creciente al corte de diciembre de 2023 registra un acumulado del 99,83% que frente a la meta establecida del 97% genera un ejecutado del 102,92%

Para la vigencia 2024 el indicador se codifica como 4.1.D PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CUMPLIDO. La primera actividad clave “Elaborar diagnóstico, identificación de brechas y diseño del plan de seguridad y privacidad” programada para ser desarrollada en el mes de enero, fue ejecutada en el mes programado y registra un cumplimiento del 100%

La segunda actividad corresponde a “Seguimiento a la ejecución del plan de seguridad y privacidad”, con una programación para su desarrollo del 8,33% para cada mes a partir del mes de enero, al cierre de mayo reporta un avance en la ejecución del 41,65%.

El indicador 4.1.D PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CUMPLIDO en PANDORA, al cierre del mes de mayo, no registra un resultado coherente en el aplicativo PANDORA, como se muestra en la gráfica en la siguiente hoja, en donde se visualiza que para las variables "AVANCE ACUMULADO DE LA EJECUCIÓN DEL PLAN DE TRABAJO" y "AVANCE ACUMULADO EN LAS ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PROGRAMADAS PARA EL PERÍODO", los valores registrados son crecientes hasta el mes de marzo, para los meses de abril y mayo, los valores registrados son puntuales y ya no son acumulativos creciente, por lo cual, el valor reflejado de 33,40% para la columna denominada "Cumplimiento en la ejecución del plan de seguridad y privacidad de la información (RESULTADO)" no es coherente con los datos registrados, aunque el valor es cierto

(OM2): Se encontró que la información registrada y presentada en el aplicativo PANDORA en los meses de abril y mayo, para el indicador 4.1.D PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CUMPLIDO, no es coherente con el registro efectuado para los meses enero a marzo, ni con el valor presentado como medición del indicador, por lo cual se debería corregir los valores capturados para las variables del indicador.

Observación del proceso:

"*No se acepta, teniendo en consulta realizada a la asesora de Oficina de Planeación Andrea Vela, se indica que estas mediciones están dadas para la cadena de valor anterior por lo que no se podrían modificar los valores capturados de abril y mayo, sin embargo en la nueva cadena se recoge el valor total acumulado que se llevaba para 2024.*"

Respuesta OCI:

La UAECD establece en el documento "Documento Técnico Manual del Sistema de Gestión Integral DIE-DT-01 v4 del 20 de octubre de 2023" en su numeral 11. GESTION DE INDICADORES:

- Los indicadores son mecanismos que permiten controlar el comportamiento de factores críticos en la ejecución de los planes, programas, proyectos y de los procesos en al entidad.
- …se diseñan los indicadores, cuya medición periódica permite establecer el grado de avance o logro de los objetivos trazados y de los resultados esperados del proceso…
- Los responsables de dependencia y de Proceso y sus equipos de trabajodeberán hacer seguimiento a los mismos según periodicidad definida.
- El seguimiento de los indicadores debe realizarse hasta el día 10 calendario siguiente al corte de la periodicidad estipulada

Con los anteriores precedentes, es claro que el proceso ha debido realizar seguimiento mensual y lo ha debido realizar durante los 10 días siguientes al corte reportado (abril y mayo), detectando y corrigiendo los errores en la captura de información en el indicador 4.1.D PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CUMPLIDO.

De otra parte, el planteamiento de no poder efectuar modificación a los valores registrados erróneamente en el aplicativo PANDORA, correspondería a una corrección pero se recomienda formular una acción correctiva que determine la causa raíz de la deficiencia presentada y prevenga nuevas ocurrencias en el cargue de información, ya sea en este o en otros indicadores del proceso.

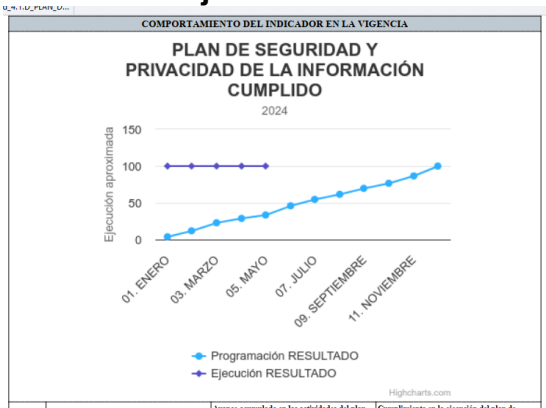
Finalmente y ante el planteamiento de la Asesora de la Oficina Asesora de Planeación y Aseguramiento de Procesos -OAPAP en cuanto a "…que estas mediciones están dadas para la cadena de valor anterior por lo que no se podrían modificar los valores capturados de abril y mayo…" se recomienda revisar el aplicativo y efectuar las modificaciones necesarias que permitan superar eventualidades como la detectada, y considerar estas correcciones cuando se esté formulando el plan de mejoramiento.

En consecuencia de lo anterior, se mantiene la observación

Situación evidenciada:
Por efecto del cambio en la cadena de valor de la UAECD, a partir de mayo, el indicador 4.1.D es sustituido por el indicador "GEST-01-PLAN-DE-SEGURIDAD-Y-PRIVACIDAD-DE-LA-INFORMACIÓN-CUMPLIDO" debido a que el campo "Proceso al que aporta" está relacionado con el nuevo proceso GESTION ESTRATEGICA DE TECNOLOGIA, e inicia su medición desde el mes de julio de 2024, arrancando con una medición de 54,50 para la variable "Avance acumulado de la ejecución del Plan de Seguridad y Privacidad de la Información"

Dado lo anterior, en ninguno de los dos indicadores (GEST-01 y 4.1.D) quedó cuantificado y cualificado el mes de junio de 2024, y en consecuencia se observa un bache entra la medición final del indicador 4.1.D que registra un valor de 33,40% y el valor inicialde del indicador GEST-01 que inicia con un valor de 54,50%

Gráfica 4. Hoja Indicador 4.1.D



Mes	Avance acumulado de la ejecución del plan de trabajo	Avance acumulado en las actividades del plan de seguridad y privacidad de la información programadas para el periodo	Cumplimiento en la ejecución del plan de seguridad y privacidad de la información (RESULTADO)	
	Valor	Valor	% Programado	% Ejecutado
01. ENERO	3,80	3,80	3,80	100,00
02. FEBRERO	11,95	11,95	11,95	100,00
03. MARZO	22,80	22,80	22,80	100,00
04. ABRIL	6,00	6,00	28,80	100,00
05. MAYO	4,60	4,60	33,40	100,00
06. JUNIO			45,85	
07. JULIO			54,70	
08. AGOSTO			61,65	
09. SEPTIEMBRE			69,60	
10. OCTUBRE			76,65	
11. NOVIEMBRE			86,50	
12. DICIEMBRE			100,00	

Fuente: Aplicativo PANDORA

(OM3): Se evidenció que el indicador 4.1.D PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CUMPLIDO así como el indicador que lo sustituye GEST-01-PLAN-DE-SEGURIDAD-Y-PRIVACIDAD-DE-LA-INFORMACIÓN-CUMPLIDO, no registran la medición cuantitativa y cualitativa para el mes de junio de 2024. El indicador GEST-01 inicia registro de medición para el mes de julio.

Observación del proceso:
"*No se acepta, dado que este indicador es de tipo estratégico, y de acuerdo con lineamientos del proceso de Direccionamiento Estratégico, la planeación estratégica de la UAECD finalizó el 31 de mayo/24, y se reactivó el 1 de julio/24, por lo para el mes de junio no se realizó medición. En el Plan de Seguridad y Privacidad de la Información se ejecutaron actividades en junio que contribuyeron al acumulado que se reporta en julio.*"

Respuesta OCI:
Efectuada la consulta con la Oficina Asesora de Planeación y Aseguramiento de Procesos – OAPAP, se confirmó el lineamiento impartido en lo relacionado con los indicadores PEI (Plan Estratégico Institucional) en cuanto a su medición hasta el 31 de mayo/2024 y conforme con la nueva cadena de valor el inicio de medición a partir del mes de julio/2024

En consecuencia de lo anterior, se retira la observación del presente informe y así mismo, no será incluida en el aplicativo PANDORA.

.

6.6 Riesgos de Gestión Proceso Gestión y Desarrollo de las TIC -Seguridad de la Información.

- Vigencia 2023: Revisada la matriz Institucional de Riesgos Gestión para la vigencia 2023, se observa que el proceso de Gestión y Desarrollo de las TIC tiene establecidos seis (6) riesgos, que fueron revisados y de los cuales, uno, el riesgo 5, presenta como producto asociado o activo de información el Sistema de Gestión de Seguridad de la Información implementado, con una calificación de riesgo inherente de alto. Tiene establecido cinco controles y como responsables de ellos, el Oficial de Seguridad de la Información y el Comité de Gestión y Desempeño. Ahora, teniendo en cuenta que después de los controles el riesgo residual registra una valoración de alto, de acuerdo a la metodología se debe reducir, para lo cual se formuló como plan de tratamiento "Fortalecer la Estrategia de comunicaciones para dar a conocer tips y las políticas de seguridad y privacidad de la información", el reporte al cierre de la vigencia 2023 informa la ejecución de la totalidad de las actividades programadas en la estrategia de comunicaciones, de igual manera informa la No materialización del riesgo.

- Vigencia 2024: El mapa de riesgos de Gestión para el proceso Gestión y Desarrollo de las TIC para la presente vigencia muestra 4 riesgos para los productos asociados o activos de información 1.) Plan Estratégico de Tecnologías de la Información– PETI, 2.) Administración de la infraestructura

tecnológica de la Entidad, 3.) Plan de seguridad y privacidad de la información y 4.) Solicitud gestionada, resuelta y documentada en la herramienta tecnológica de mesa de servicios de TI.
Para el caso específico del riesgo 3, que es el que atañe al ejercico auditor en desarrollo, se establecen los siguientes cuatro controles:

- ✓ Oficial y/o equipo de Seguridad de la Información, anualmente define y presenta el plan de seguridad y privacidad de la información y la aprobación se encuentra a cargo del Comité Institucional de Gestión y Desempeño
- ✓ Comité Institucional de Gestión y Desempeño elabora el Plan de Tratamiento de riesgos de seguridad de la información, basado en un análisis de riesgos para identificar las amenazas, vulnerabilidades y riesgos asociados a cada activo critico de acuerdo con el apetito de riesgo de la Unidad, y definiendo controles para minimizar los niveles de riesgo.
- ✓ Jefe de Dependencia y/o el designado mediante memorando, solicitan la inactivación de las cuentas de usuario expiradas
- ✓ Sensibilización a los funcionarios en temas de Seguridad y Privacidad de la Información

Los cuatro controles al trimestre II de 2024 se califican con un avance del 50%, adicionalmente se informa la No materialización del riesgo durante los 2 trimestres

6.7 Riesgos de Corrupción Proceso Gestión y Desarrollo de las TIC -Seguridad de la Información.

En lo que refiere a los Riesgos de Corrupción revisada la matriz, se identificó un único riesgo asociado al procesos de Gestión y Desarrollo de las TIC, que corresponde a "*Posibilidad de acceso a información, por parte de personal no autorizado, en beneficio propio y particular*" que presenta un riesgo residual con valoración de Alto y, en consecuencia, de acuerdo a la metodología de administración de riesgo, se debe Reducir a través del establecimiento de un plan de manejo de riesgo - PMR, para lo cual se establecieron dos actividades, 1) Revisión mensual de TI (gestor de acceso o quien se designe) verficar que los Jefes de Dependencia realicen la solicitud de inactivación conforme el reporte remitido respecto de las cuentas de usuario de red que expiraron hasta el corte mensual y por inactividad mayor a 60 días. y 2.) Socializar trimestralmente los lineamientos establecidos para la entrega de información en el marco de las políticas de seguridad y privacidad de la información.

El monitoreo efectuado al cierre del trimestre IV de 2023, reporta un cumplimiento del 100% en cada una de las dos actividades formuladas, de la misma manera, informa la No materialización del riesgo

El monitoreo efectuado al cierre del trimestre II de 2024, reporta un cumplimiento del 50% en cada una de las dos actividades formuladas, así mismo, informa la No materialización del riesgo

6.8 Riesgos de Seguridad de la Información

6.8.1 Riesgos Proceso Gestión y Desarrollo de las TIC -Seguridad de la Información

- Vigencia 2023 (Trimestres 3 y 4)

La Matriz de Riesgos Institucional para el proceso Gestión y Desarrollo de las TIC para la vigencia 2023, contempla 30 riesgos, los relacionados con Pérdida de Disponibilidad son los identificados con los códigos RS-GDT-02, 04, 06, 08, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28 y 30, los restantes corresponden a riesgos por pérdida de confiabilidad e integridad.

Requieren tratamiento o plan de manejo de riesgos -PMR los riesgos RS-GDT-02, 03, 10, 11, 12, 13, 14, 15, 16, 19, 20, 23, 26 y 28, para estos riesgos la Gerencia tiene estandarizadas cinco (5) actividades a desarrollar para el tratamiento o la reducción del riesgo y que corresponden a:

- ✓ Realizar la actualización del inventario de activos asociados a cargo de la Subgerencia de Infraestructura.
- ✓ Ejecutar de forma permanente las actividades de mantenimiento y actualización de los recursos tecnológicos bajo responsabilidad de la Subgerencia de Infraestructura.
- ✓ Realizar seguimiento y monitoreo al uso de los recursos haciendo proyecciones periodicas de la capacidad futura requerida.
- ✓ Ejecutar copias de respaldo de la información y la configuración de los sistemas de acuerdo con las políticas de copias de respaldo definidas.
- ✓ Mantener documentados y actualizados los procedimientos de operación de las plataformas tecnólogicas a cargo de la Subgerencia de Infraestructura tecnológica.

Para el tercer y cuarto trimestre de 2023 los mapas de riesgos reportan que NO se presentó materialización de riesgos, así mismo, el cumplimiento de las actividades establecidas en los PMR para cada uno de los riesgos que así lo ameritaron con el desarrollo de las metas al 100%

- Vigencia 2024 (Trimestres 1 y 2)

  La Matriz de Riesgos Institucional para el proceso Gestión y Desarrollo de las TIC para la vigencia 2024, contempla 26 riesgos. Los relacionados con Pérdida de Disponibilidad son los identificados con los códigos RS-GDT-02, 04, 06, 08, 10, 12, 14, 16, 18, 20, 22, 24 y 26, los restantes corresponden a riesgos por pérdida de confiabilidad e integridad.

  Requieren tratamiento o plan de manejo de riesgos -PMR los riesgos RS-GDT-01, 02, 03, 13, 14, 21 y 26, para estos riesgos la Gerencia tiene estandarizadas cinco (5) actividades a desarrollar para el tratamiento o la reducción del riesgo y que corresponden a:

  En la vigencia 2024 en los mapas de riesgos correspondientes a los trimestres 1 y 2, no se reportó la materialización de riesgos, las actividades formuladas en los PMR registran avances en su ejecución entre el 50%y el 100%, con excepción de la correspondiente al riesgo 21, donde se estableció “Sensibilizar a los administradores de las plataformas en las responsabilidades relacionadas con seguridad para mitigar los riesgos relacionados con pérdida de disponibilidad, confidencialidad e integridad”, que si bien es cierto contempla un plazo de ejecución hasta el 31 de diciembre de 2024, es la única actividad que no registra avance

6.8.2 Riesgos Unidad Adminsitrativa Especial de Catastro Distrital -UAECD

Dando cumplimiento a lo establecido en el Documento Técnico Metodología de Riesgos y alineado al Modelo de Gestión de Riesgos de Seguridad Digital (Mintic), así como a la Guía para la Administración del Riesgo y el Diseño de controles en entidades públicas – DAFP V6.0, el Oficial de Seguridad de la Información, recibe las matrices de riesgo de los diferente procesos, las consolida y elabora el Informe de Seguimiento Riesgos de Seguridad Digital.

- Cuarto Trimestre 2023

El Oficial de Seguridad elaboró y presentó el informe correspondienten al cuarto trimestre de 2023, en el que se evidencia que se mantienen los 178 riesgos residuales de seguridad digital, de los cuales 15 se clasifican en nivel Alto, 68 corresponden al nivel Moderado y 98 en nivel Bajo, tal como se registran en la tabla a continuación.

Con base en la anterior clasificación se evidencia que 83 riesgos (nivel moderado y alto) requieren y cuentan con plan de manejo de riesgo -PMR.

Tabla 2. Riesgos Residuales de Seguridad Digital por Proceso vigencia 2023 – IV TRIMESTRE

`	Riesgo Final				Total	%
	Extremo	Alto	Moderado	Bajo		
Direccionamiento Estratégico				4	4	2%
Gestión de Comunicaciones		1	2	7	10	6%
Gestión de Conocimiento e Innovación				2	2	1%
Gestión Catastral (GIC_SIE_SIFJ)			5	7	12	7%
Gestión Catastral (Territorios)		8	7	1	16	9%
Gestión de Información Geográfica			3	5	8	4%
Gestión de Talento Humano			5	11	16	9%
Gestión de Productos y Servicios			2	6	8	4%
Gestión y Desarrollo de las TIC		3	12	15	30	17%
Gestión Jurídica			4	4	8	4%
Gestión de Servicios Administrativos		0	0	0	0	0%
Gestión Financiera			3	9	12	7%
Gestión Contractual			5	11	16	9%
Participación Ciudadana y Experiencia de Servicio			2	4	6	3%
Gestión de Seguimiento, Evaluación y Control		3	7	8	18	10%

Gestión Documental			5	1	6	3%
Transversal (Dirección - GGC)			3	3	6	3%
Total	**0**	**15**	**65**	**98**	**178**	100%
%	**0%**	**8%**	**37%**	**55%**	**100%**	

Fuente: INFORME_SEG_RSD_IVTRI2023 – SharePoint Gerencia de Tecnología

Informa el Oficial que en el cuarto trimestre de 2023 se presentó materalización de riesgos en el proceso de Gestión de Comunicaciones, concretamente en el riesgo RS-COM-04 – Perdida de Disponibilidad - Redes Sociales de Catastro - Credenciales de acceso a las Redes Sociales, por lo que, se actualiza valoración del riesgo y se crea actividad de plan de tratamiento.

- Primer y segundo Trimestre 2024
  En la vigencia 2024 a corte del primer trimestre la Unidad tiene identioficados 170 riesgos de seguridad digital, que con base en nivel de apetito del riesgo establecido por la UAECD 103 riesgos correspondientes al 61% se clasificacn en el nivel Bajo y, los restantes 67 riesgos, equivalentes al 39%, requieren plan de manejo de riesgos – PMR

Tabla 3. Riesgos Residuales de Seguridad Digital por Proceso vigencia 204 – IV TRIMESTRE

Proceso / Dependencia	Riesgo Final				Total	%
	Catastrófico	Alto	Moderado	Bajo		
0. TRANSVERSAL - DIRECCIÓN - GGC	0	0	3	3	6	4%
1. DIRECCIONAMIENTO ESTRATÉGICO - OAPAP	0	0	0	4	4	2%
2. GESTIÓN DE COMUNICACIONES	0	1	1	8	10	6%
3. GESTIÓN DEL CONOCIMIENTO, INNOVACIÓN E INVESTIGACIÓN.	0	0	0	2	2	1%
4. GESTIÓN CATASTRAL - (GIC_SIE_SIFJ)	0	0	5	7	12	7%
4. GESTIÓN CATASTRAL - TERRITORIOS	0	7	6	1	14	8%
5. GESTIÓN DE INFORMACIÓN GEOGRÁFICA	0	0	1	7	8	5%
6. GESTIÓN DEL TALENTO HUMANO	0	0	5	11	16	9%
7. GESTIÓN DE PRODUCTOS Y SERVICIOS	0	0	1	7	8	5%
8. GESTIÓN Y DESARROLLO DE LAS TIC	0	2	5	19	26	15%
9. GESTIÓN JURÍDICA	0	0	4	4	8	5%
10. GESTIÓN DE SERVICIOS ADMINISTRATIVOS	0	0	1	3	4	2%
11. GESTIÓN FINANCIERA	0	0	3	9	12	7%
12. GESTIÓN CONTRACTUAL	0	0	3	7	10	6%
13. PARTICIPACIÓN CIUDADANA Y	0	0	3	5	8	5%

EXPERIENCIA DEL SERVICIO						
14. GESTIÓN DE SEGUIMIENTO, EVALUACIÓN Y CONTROL - OCI - OCDI	0	3	8	5	16	9%
15. GESTIÓN DOCUMENTAL	0	0	5	1	6	4%
Total	**0**	**13**	**54**	**103**	**170**	
%	**0%**	**8%**	**32%**	**61%**	**100%**	

Fuente: INFORME_SEG_RSD_IITRI2024 – SharePoint Gerencia de Tecnología

Informa el Oficial que en el cuarto trimestre de 2023 se presentó materalización de riesgos en el proceso de Gestión de Comunicaciones, concretamente en el riesgo RS-COM-04 – Perdida de Disponibilidad - Redes Sociales de Catastro - Credenciales de acceso a las Redes Sociales, por lo que, se actualiza valoración del riesgo y se crea actividad de plan de tratamiento.

Situación evidenciada:
En lo correspondiente a los trimestres I y II de la vigencia 2024, no fue reportada materialización de riesgos. El avance en la implementación de las actividades formuladas en los PMR es del 49,92% y advierte el Oficial de Cumplimiento bajo avance o cumplimiento en los procesos de Gestión Jurídica y Gestión Contractual.

En el caso de Gestión Contractual los riesgos RS-GCO-02 y RS-GCO-05 registran avance 0% en el desarrollo de la actividad “Sensibilizar al equipo de la subgerencia de contrataciòn respecto a los controles y manejo de la informaciòn digital para evitar la perdida de confidencialidad, integridad y disponibilidad de la información”, actividad que cuenta con plazo hasta el 31 de diciembre de 2024 pero transcurrido la mitad del tiempo no registra avance alguno.

En cuanto al Proceso de Gestión Jurídica los riesgos RS-GJU-01, RS-GJU-03, RS-GJU-04 y RS-GJU-05 registran avance en el desarrollo de la actividad “Continuar con las sensibilizaciones en temas de seguridad de la información (acceso a areas seguras) para los servidores y contratistas del proceso Gestión Jurídica (GJ y SGJ)”, actividad que cuenta con plazo hasta el 31 de diciembre de 2024 pero transcurrido la mitad del tiempo del presente año, no registra avance alguno.

(OM4): Revisadas las matrices Mapa de Riesgos SD para los trimestres I y II de 2024, se observó que las actividades en los planes de manejo de riesgo -PMR para los riesgos RS-GCO-02 y RS-GCO-05 del proceso de Gestión Contractual y RS-GJU-01, RS-GJU-03, RS-GJU-04 y RS-GJU-05 del proceso de Gestión Jurídica, no registran avance en el desarrollo de las actividades formuladas, por lo anterior se recomienda iniciar de manera prudencial, la ejecución de las actividades establecidas.

Observación de la Gerencia de Tecnología:
“*Se acepta, y desde Seguridad de la Información se realizará el seguimiento de las actividades establecidas en el plan de tratamiento para los procesos de Gestión Contractual y Gestión Jurídica.*”

Observación de la Gerencia Jurídica:
Plantea la Gerencia en el chat "*…¿Por qué se deja la oportunidad si la actividad en el plan de riesgos tiene fecha de ejecución en la matriz de riesgos a 31 de diciembre de 2024? y ni siquiera todavía se ha realizado el reporte del 3 trimestre*".

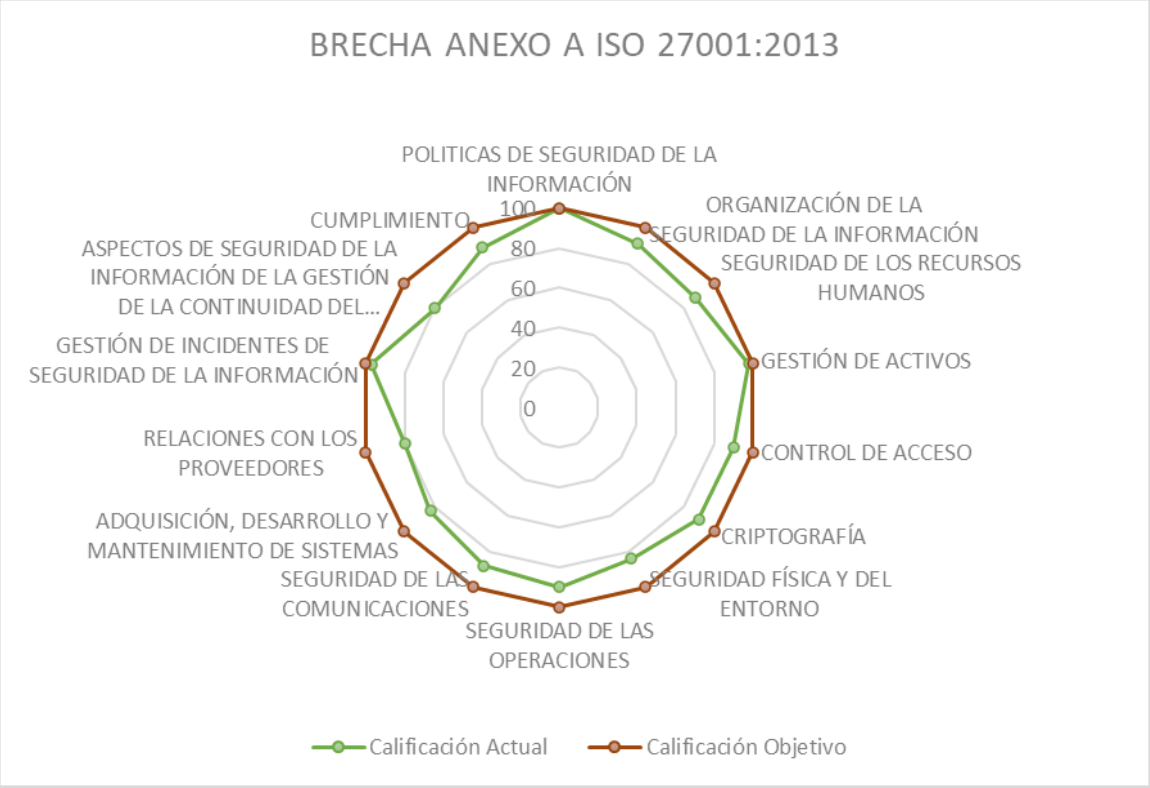
Respuesta OCI:
No obstante el no haber recibido respuesta formal de la Gerencia Jurídica y de otra parte, que el planteamiento efectuado en el chat es extemporáneo frente a los tres (3) días hábiles establecidos en el memorando 2024IE17487, para dar respuesta al informe preliminar de auditoría; la OCI luego de revisar lineamiento de la OAPAP frente al reporte de actividades de tratamiento de riesgos, retira la oportunidad de mejora (OM4) del presente informe y así mismo, no se incluirá en el aplicativo PANDORA, pero es fundamental avanzar con las actividades de manera progresiva para garantizar el cumplimiento de lo planificado en el marco de la Gestión de Riesgos de Seguridad de la Información. Por lo tanto, se le otorga la categoría de Recomendación.

Recomendación:
Se recomienda a la Gerencia Jurídica y a la Subgerencia de Contratación dar inicio a la menor brevedad al desarrollo de las actividades establecidas en el plan de manejo de riesgos -PMR para los riesgos RS-GCO-02 y RS-GCO-05 del proceso de Gestión Contractual y RS-GJU-01, RS-GJU-03, RS-GJU-04 y RS-GJU-05 del proceso de Gestión Jurídica, lo anterior teniendo en cuenta las multiples funciones y tareas que debe desarrollar durante el segundo semestre el Oficial de Seguridad de la Información, lo que podría conllevar a que no se puedan desarrollar las actividades en el PMR de las dos dependencias mencionadas.

6.9 EVALUACION MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El archivo Excel "Diagnostico_Inst_Eval_MSPI_2024" 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 2024 a 30 de junio de 2024, 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 5. Brechas frente al Anexo A ISO 27001:2013



Fuente: Tomado del archivo "Diagnostico_Inst_Eval_MSPI_2024"

Gráfica construida con base en los datos consolidados en el cuadro "Evaluación de Efectividad de controles" mostrado a continuación

Tabla 4. 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**	82
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	88	100	**OPTIMIZADO**	88
A.8	GESTIÓN DE ACTIVOS	98	100	**OPTIMIZADO**	89
A.9	CONTROL DE ACCESO	90	100	**OPTIMIZADO**	81
A.10	CRIPTOGRAFÍA	90	100	**OPTIMIZADO**	80

A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	84	100	**OPTIMIZADO**	82
A.12	SEGURIDAD DE LAS OPERACIONES	90	100	**OPTIMIZADO**	85
A.13	SEGURIDAD DE LAS COMUNICACIONES	88	100	**OPTIMIZADO**	85
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	83	100	**OPTIMIZADO**	79
A.15	RELACIONES CON LOS PROVEEDORES	80	100	**GESTIONADO**	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	80	100	**GESTIONADO**	64
A.18	CUMPLIMIENTO	89	100	**OPTIMIZADO**	83
PROMEDIO EVALUACIÓN DE CONTROLES		**89**	**100**	**OPTIMIZADO**	**84**

Fuente: Tomado del archivo "Diagnostico_Inst_Eval_MSPI_2024"

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.15 RELACIONES CON LON PROVEEDORES y A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO con una calificación de 80 puntos en cada uno de ellos, seguido por los dominios A.14 CONTROL DE ACCESO con una calificación de 83 puntos y A.11 SEGURIDAD FISICA Y DEL ENTORNO con una calificación de 84 puntos, lo que con respecto de la "Evaluación de la Efectividad de los Controles" indica que los dos primeros se ubican como GESTIONADO (rango de la calificación entre 61 y 80) y los restantes como OPTIMIZADO (rango de la calificación entre 81 y 100).
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 89 puntos, lo que ubica a la Unidad en el nivel de OPTIMIZADO y registra un avance de 5 puntos con relación a la calificación del periodo anterior. Así mismo, se observa que en general en todos los dominios se obtuvo una mejor calificación que en la evaluación anterior, con excepción de los dominios A.7 SEGURIDAD DE LOS RECURSOS HUMANOS, A.15 RELACIONES CON LOS PROVEEDORES y A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, que mantuvieron la misma calificación que en la evaluación inmediatamente anterior.

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

- **Dominio A.15- RELACIONES CON LOS PROVEEDORES**

Este dominio en las dos últimas vigencias ha registrado calificación de 80 puntos de 100 posibles, lo anterior evidencia que no ha presentado mejora o evolución de periodo a periodo.

Tabla 5. Literales Dominio 15

LITERAL	ITEM	CALIFICACION
A.15.1	Seguridad de la información en las relaciones con los proveedores: Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	80
A.15.2	Gestión de la prestación de servicios de proveedores: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	80

Fuente. Construcción del auditor

El literal de este dominio registra calificación de 80 puntos, en tal sentido se deben atender y desarrollar las recomendaciones plasmadas en el archivo “Diagnostico_Inst_Eval_MSPI_2024”

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

Al igual que el anterior dominio, este en las dos últimas vigencias ha registrado calificación de 80 puntos de 100 posibles, lo anterior evidencia que no ha presentado mejora

Tabla 6. Literales Dominio 17

LITERAL	ITEM	CALIFICACION
A.17.1	Continuidad de la seguridad de la información	80
A.17.1.1	Planificación de la continuidad de la seguridad de la información	80
A.17.1.2	Implementación de la continuidad de la seguridad de la información	80
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	80
A.17.2	Redundancias	80
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	80

Fuente. Construcción del auditor

Todos los literales de este dominio registran calificación de 80 puntos, en tal sentido se deben atender y desarrollar las recomendaciones plasmadas en el archivo "Diagnostico_Inst_Eval_MSPI_2024"

- **Dominio A.14 – ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**

En la evaluación registrada en el instrumento Diagnostico_Inst_Eval_MSPI_2024, la calificación para este dominio es la tercera de menor valor entre todos los dominios, con un valor de 83 puntos.

Tabla 7. Literales Dominio 14

LITERAL	ITEM	CALIFICACION
A.14.1	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	80
A.14.1.1	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	80
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	80
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	80
A.14.2	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	89
A.14.2.1	Política de desarrollo seguro	100
A.14.2.2	Procedimientos de control de cambios en sistemas	100
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	80
A.14.2.4	Restricciones en los cambios a los paquetes de software	100
A.14.2.5	Principios de construcción de sistemas seguros	80
A.14.2.6	Ambiente de desarrollo seguro	80
A.14.2.7	Desarrollo contratado externamente	100

A.14.2.8	Pruebas de seguridad de sistemas	80
A,14,2,9	Prueba de aceptación de sistemas	80
A.14.3	DATOS DE PRUEBA	80
A.14.3.1	Protección de datos de prueba	80

Fuente. Construcción del auditor

En este dominio se debe enfatizar en el desarrollo de las recomendaciones establecidas en el archivo "Diagnostico_Inst_Eval_MSPI_2024" para los literales con calificaciones de 80 puntos.

Observación del proceso:
"*En revisión del informe se encuentra que en la tabla de literales del dominio 14, en la página 25, hay un error de digitación en la calificación del literal A.14.3.1 Protección de Datos de Prueba, que quedó en 800 y debería ser 80*"

Respuesta OCI
La Oficina de Control Interno agradece la precisión y procede a efectuar la corrección correspondiente.

- **Dominio A.11 – SEGURIDAD FÍSICA Y DEL ENTORNO**

En la evaluación registrada en el instrumento Diagnostico_Inst_Eval_MSPI_2024, la calificación para este dominio es la tercera de menor valor entre todos los dominios, con un valor de 84 puntos

Tabla 8. Literales Dominio 11

LITERAL	ITEM	CALIFICACION
A.11.1	**ÁREAS SEGURAS**	**87**
A.11.1.1	Perímetro de seguridad física	100
A.11.1.2	Controles físicos de entrada	100
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	80
A.11.1.4	Protección contra amenazas externas y ambientales	80

A.11.1.5	Trabajo en áreas seguras	**80**
A.11.1.6	Áreas de despacho y carga	80
A.11.2	**EQUIPOS**	**80**
A.11.2.1	Ubicación y protección de los equipos	80
A.11.2.2	Servicios de suministro	80
A.11.2.3	Seguridad del cableado	80
A.11.2.4	Mantenimiento de equipos	80
A.11.2.5	Retiro de activos	80
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	80
A.11.2.7	Disposición segura o reutilización de equipos	80
A.11.2.8	Equipos de usuario desatendidos	80
A.11.2.9	Política de escritorio limpio y pantalla limpia	80

Fuente. Construcción del auditor

(OM5) Revisado el archivo Excel “Diagnostico_ Inst_Eval_MSPI_2024” en lo relacionado con la Evaluación de Efectividad de controles, se evidenció que los dominios que registran menor calificación corresponden a: A.11 SEGURIDAD FÍSICA Y DEL ENTORNO, A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, A.15 RELACION CON PROVEEDORES y A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, 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.

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-15, A-17, A-14 y A-11

Observación del proceso:
"*Se acepta. Con cada uno de los líderes se realizarán actividades tendientes a la mejora continúa de los dominios de control: A.11 SEGURIDAD FÍSICA Y DEL ENTORNO, A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, A.15 RELACION CON PROVEEDORES y A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.*"

Respuesta OCI:
A partir de la respuesta de la Gerencia de Tecnología en la que se acepta la oportunidad de mejora, se mantiene la observación.

Hallazgos

No.	Descripción del hallazgo	No Conformidad	Oportunidad	Norma, criterio, Requisito o Documento asociado	Área /Cargo Responsable	Anexo Evidencia
1	**(OM1)** Se evidenció que el Mapa de Procesos presentado en el numeral 2.5 ALCANCE DEL SGSI del Documento Técnico GDT-DT-01 - V3, no corresponde a la actual cadena de valor de la UAECD, por lo anterior, se debe actualizar el DOCUMENTO TÉCNICO MANUAL DE POLÍTICAS DETALLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.		X		Gestión y Desarrollo de las TIC (Gestión Estratégica de Tecnología)	Documento Técnico GDT-DT-01 - V3

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

No.	Descripción del hallazgo	No Conformidad	Oportunidad	Norma, criterio, Requisito o Documento asociado	Área /Cargo Responsable	Anexo Evidencia
2	**(OM2)** Se encontró que la información registrada y presentada en el aplicativo PANDORA en los meses de abril y mayo, para el indicador 4.1.D PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CUMPLIDO, no es coherente con el registro efectuado para los meses enero a marzo, ni con el valor presentado como medición del indicador, por lo cual se debería corregir los valores capturados para las variables del indicador.		**X**		Gestión y Desarrollo de las TIC (Gestión Estratégica de Tecnología)	PANDORA – indicador 4.1.D Plan de Seguridad y Privacidad de la información cumplido
3	**(OM5)** Revisado el archivo Excel "Diagnostico_ Inst_Eval_MSPI_2024" en lo relacionado con la Evaluación de Efectividad de controles, se evidenció que los dominios que registran menor calificación corresponden a: A.11 SEGURIDAD FÍSICA Y DEL ENTORNO, A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, A.15 RELACION CON PROVEEDORES y A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, 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.		X		Gestión Estratégica de Tecnología	"Diagnostico_ Inst_Eval_MSPI_2024

7. FORTALEZAS (aplica para auditorías)

- El Oficial de Seguridad de la Información aporta conocimiento y experiencia que se transfiere a los enlaces de seguridad en los procesos y contribuyen al mejoramiento del SGSPI y que son base o pilar para el tratamiento 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 5 puntos para la vigencia 2024, indicativo el mejoramiento en algunas de las brechas determinadas

8. DEBILIDADES*:*

- Para la vigencia 2024 el Equipo Transversal de Seguridad de la Información se ve afectado negativamente por la no contratación de prestación de servicios de la profesional que prestaba apoyo al Oficial de Seguridad de la Información

9. CONCLUSIONES

- La Unidad Administrativa Especial de Catastro Distrital -UAECD a través de la Gerencia de Tecnología y el Oficial de Seguridad de la Información ha construido, desarrollado, socializado e implementado diferentes documentos necesarios para el desarrollo de la Seguridad y Privacidad de la Información, como es el caso de la Política de Seguridad y Privacidad de la Información, procedimiento, instructivos y documentos técnicos.
- 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.
- 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 Equipo de Seguridad desarrolló el Plan de Seguridad y Privacidad de la Información para la vigencia 2024, se evidenció su publicación en la Página web de la UAECD. El mismo contiene las actividades, responsables, producto/entregables, como las fechas de inicio y fin para cada actividad.
- 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.
- En la calificación efectuada en la vigencia 2024 en el Instrumento de Identificación de la Línea Base de Seguridad y la Evaluación de Efectividad de los Controles, se evidencia mejora en 5 puntos con la vigencia anterior, no obstante, es susceptible de continuar mejorando en la implementación y cumplimiento de los controles del Anexo A de la norma ISO 27001

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.

10. RECOMENDACIONES

- ✓ Revisar y actualizar el Documento Técnico GDT-DT-01 v3, para incluir el Mapa de Procesos debidamente actualizado conforme con la última cadena de valor aprobada para la Unidad.
- ✓ Revisar la posibilidad de ajuste los valores registrados para la medición del Indicador 4.1.D Plan de Seguridad y Privacidad de la Información Cumplido.
- ✓ Actualizar el indicador GEST-01 Plan de Seguridad y Privacidad de la Información, con el objeto de incluir los valores correspondientes al mes de junio, que permitan efectuar la medición cuantitativa y cualitativa para el mes de junio.
- ✓ Desarrollar las actividades correspondientes al mapa de riesgos institucional en lo referente al plan de manejo de riesgo -PMR de los procesos de Gestión Contractual y Gestión Jurídica, que no han sido iniciadas.
- ✓ Continuar con la implementación y fortalecimiento de los controles del anexo A de la norma ISO 27001, priorizando aquellos ítems que registran menor calificación.

DIANA KARINA RUIZ PERILLA
Jefe Oficina de Control Interno

Elaboró: Luis Orlando Barrera Cepeda, Contratista O.C.I
Revisó: Diana Karina Ruiz Perilla. Jefe Oficina de Control Interno

Copia: Comité Institucional de Coordinación de Control Interno