UAECD
Catastro Bogotá

UNIDAD ADMIN. CATASTRO DISTRITAL 08/08/2023 14:08:22
Al contestar cite este número: 2023IE18368O1 Folios: 1 Anexos: 1
ORIGEN: Sd:90 - OFICINA DE CONTROL INTERNO/CORREA RODRIGU
DESTINO: DIRECCION GENERAL/RODRIGUEZ SOSA HENRY
ASUNTO: Informe final Auditoría al proceso Gestión y Desarrollo de las TIC
OBS: Plan Anual de Auditorías PAA 2023

Memorando

Fecha elaboración: 08 de agosto de 2023

Para: Henry Rodriguez Sosa
Director_General
Hector Henry Pedraza Piñeros
Gerente_Gt

De: Elbi Asaneth Correa Rodriguez
Jefe_Oficina_Oci

Referencia: Plan Anual de Auditorías PAA 2023

Asunto: Informe final Auditoría al proceso Gestión y Desarrollo de las TIC Sistema de Gestión de Seguridad y Privacidad de la Información

Respetado Ingeniero Pedraza:

En cumplimiento del Plan Anual de Auditorias PAA que actualmente ejecuta la Oficina de Control Interno OCI, en el marco de sus actividades orientadas al fortalecimiento del Sistema de Control Interno de la Unidad, se realizó la Auditoria al proceso Gestión y Desarrollo de las TIC Sistema de Gestión de Seguridad y Privacidad de la Información.

Consecuente con lo anterior, adjunto con el presente le remito para su consideración y demás fines, el Informe Final.

Cordialmente,

ELBI ASANETH CORREA RODRÍGUEZ
Jefe Oficina de Control Interno

Anexo: Informe final Auditoria al proceso Gestión y Desarrollo de las TIC Sistema de Gestión de Seguridad y Privacidad de la Información.

Memorando

Aprobado digitalmente por:

Elbi Asaneth Correa Rodriguez
Jefe_Oficina_Oci
Fecha y hora: 08/08/2023 14:08:22

Elaboró: Ricardo Andres Paloma Puentes
Revisó: Ricardo Andres Paloma Puentes Funcionario_Oci

Código de verificación: 2497928577

ALCALDÍA MAYOR DE BOGOTÁ D.C. UAECD Catastro Bogotá	**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 **2023,** 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 al director de la UAECD con copia a las áreas o procesos involucrados.

Proceso: Auditoría al 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

Verificar el desarrollo, implementación y uso de los lineamientos definidos para el Sistema de Gestión de Seguridad y Privacidad de la Información en la UAECD.

2. OBJETIVOS ESPECÍFICOS

- Verificar la existencia del Plan de Seguridad y Privacidad de la Información vigencias 2022 y 2023.
- 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 A.10 a A.13, conforme el Anexo A de la norma ISO 27001:2013
- Efectuar seguimiento a la implementación de los controles A.5 – A.9 del Anexo A de la norma ISO 27001:2013

3. ALCANCE

Revisar los controles A.10 a A.13 del Anexo Técnico de la norma ISO 27001:2013 y efectuar seguimiento a los controles A.5 - A.9, en el periodo comprendido entre el 1 de julio de 2022 a 30 de junio de 2023.

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 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 …*".
- 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 permitirán contribuir al mejoramiento del Sistema de Control Interno -SCI.

Para el desarrollo de la auditoría mediante sesiones de trabajo virtuales, efectuadas con personal de la Gerencia de Tecnología y, de manera específica con el Oficial de Seguridad de la Información y la enlace de calidad, se revisó tanto el procedimiento como los instructivos con el propósito, con el ánimo de constatar la adecuada aplicación de los mismos y realizar revisión documental que permita evidenciar su correcta aplicación, 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 13 de junio y el 31 de julio de 2023, 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 2022 al 30 de junio de 2023. La información requerida para el desarrollo del presente ejercicio fue dispuesta en el One Drive https://catastrobogotacol-my.sharepoint.com/personal/lobarrera_catastrobogota_gov_co/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Flobarrera%5Fcatastrobogota%5Fgov%5Fco%2FDocuments%2FAudit%5FGT%5FSGSPI%5F2023&view=0.

Así mismo, se suministró información a través del SharePoint en el enlace https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcatastrobogotacol.sharepoint.com%2F%3Af%3A%2Fr%2Fsites%2FGerenciaTecnologa-GOBIERNODIGITAL%2FShared%2520Documents%2FGOBIERNO%2520DIGITAL%2FGobierno%2520Digital%2F3.%2520SegInf%2F3.2%2520Doc_Tact%2FAuditorias%2F2023%2FSGSI%2Fsol_info11072023%3Fcsf%3D1%26web%3D1%26e%3DjTTfDf&data=05%7C01%7Clobarrera%40catastrobogota.gov.co%7C25a6e6f736254db973ca08db8866cc26%7C25a519376bbd469d9e25d53cbb4bf3a2%7C0%7C0%7C638253747338805754%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=yC%2FAjQeikwjHRXdSBVso1gc1iW%2BRQ9ePLO6uGv5Ni5g%3D&reserved=0, aportado en correo del 19 de julio de 2023 por la ingeniera Lourdes María Acuña del Equipo de seguridad de la Información.

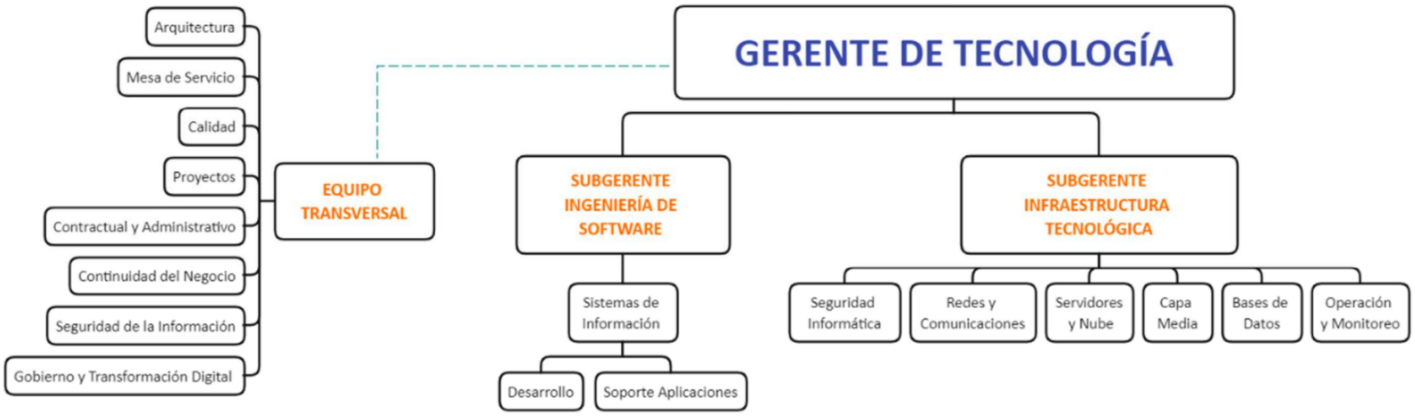
6. PRESENTACIÓN DE RESULTADOS

En desarrollo del ejercicio auditor, se pidió al enlace designado para el suministro de la información, ingeniero Luis Albeiro Cortés e ingeniera Lourdes María Acuña, entregar o disponer la información en el One Drive dispuesto para tal fin, compartiéndole el enlace correspondiente, citado anteriormente. Información que fue requerida en correos del 20 de junio de 2023, correo del 11 de julio. 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:

Gráfica 1. Organización Funcional Gerencia de Tecnología



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 2022 y 2023 de la Gerencia de Tecnología, se encontró una variación negativa del 27,27% para la presente vigencia, lo que equivale a una disminución de $3.989.258.143 para la vigencia 2023. Como se ilustra en el siguiente cuadro:

Gráfica 2. Presupuesto Gerencia de Tecnología

Vigencia	Presupuesto aprobado Gerencia de Tecnología
2022	$ 14.627.747.238
2023	$ 10.638.489.595

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

Con anterioridad la Gerencia de Tecnología informó de manera general, las afectaciones que se generaron para la Gerencia y en consecuencia para la Unidad, como se relaciona a continuación:

- Nubes Azure y Oracle que afectan directamente el tema de Seguriddad y Privacidad de la Información conexo a Continuidad del Negocio de TI, en el sentido que actualmente el principal riesgo que existe, es el de no poder dar continuidad a los procesos de negocio de Catastro debido a la obsolescencia en la infraestructura actual y a la falta de una infraestructura tecnológica alterna que en caso de una contingencia permita recuperarse de una manera mas expedita y óptima.

- Licenciamiento Office.
- Licenciamiento SAS.
- Disminución del personal por contrato de prestación de servicios al disminuir de 55 en la vigencia 2022 a 20 personas en 2023.

Ahora, requerida la información correspondiente a los recursos que para las dos vigencias correspondían a Seguridad de la Información, se recibieron dos archivos Excel "RECURSOS 2022 SEGURIDAD" y "RECURSOS 2023 SEGURIDAD", en los que se relacionan recursos por $1.321.367.227 y $1.203.319.333 respectivamente.

En lo que corresponde a la vigencia 2023, los recursos se encuentran destinados a contratación directa (contratos prestación de servicios por valor de $147.319.333, con un valor pendiente de giro de $111.485.200. Los recursos por $1.056.000.000 corresponden a dos procesos de selección abreviada por subasta inversa, el primero de ellos por $956 millones para la "Prestación de Servicios de garantía, soporte y mantenimiento para los equipos de seguridad informática con que cuenta la UAECD", el segundo por $100 millones para "Compraventa de licenciamiento de antivirus".

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.*"

Asimismo, 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"*

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 1 de fecha 09-12-2022*" 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 link de Transparencia en el numeral 1.11.3.1 se encuentra el documento "*Políticas Detalladas de Seguridad y Privacidad de la Información*", que detalla trece (13) políticas relacionadas con Seguridad y Privacidad de la Información.

Establece la Resolución en su artículo 6 Revisión de la Política: "*La UAECD revisará la Política de Seguridad y Privecidad de la Información y las políticas detalladas derivadas con una periodicidad mínima anual…*". Se revisó el Acta No. 11 del Comité de Gestión y Desempeño llevado a cabo el 29 de diciembre de 2022, evidenciando que en el numeral 5 del orden del día, se efectuó la revisión de la Política General y detalladas de seguridad y privacidad de la información, concluyendo que se mantienen las mismas 13 políticas detalladas.

6.4 Procedimiento e Instructivos

Revisado el ISODOC 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 se Seguiridad de la Información de la Gerencia de Tecnología en la respuesta al punto 6 de la solicitud 1.

Situaciones evidenciadas

- Procedimiento GDT-PR-03 versión 1, de fecha 24 de mayo de 2022,.
  Revisado el documento cuyo objetivo corresponde a "*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*", el procedimiento 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.
  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.

Al Comité de Gestión y Desempeño en su sesión 11 del 29 de diciembre de 2022, de acuerdo al Acta en los numerales 7.2 y 7.3, fueron presentados los planes referidos y sometidos a su aprobación, siendo aprobados por unanimidad, dando de esta manera se brindó pleno cumplimiento al procedimiento GDT-PR-03.

- Instructivo GDT-03-IN-01 versión 1 "Instructivo de Gestión de Activos de Información", de fecha 10 de junio de 2022.
  El objetivo del instructivo 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".
  Para la revisión de los activos de información, 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.
  Actualmente el instructivo se desarrolla normalmente.

- Instructivo GDT-03-IN-02 versión 1, de fecha 10 de junio de 2022, Instructivo Gestión de Incidentes de Seguridad de la Información
  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 "Formalizar y verificar el plan de trabajo formal para la atención del incidente de seguridad o privacidad de la información" siendo el control: Se establece como autocontrol, ya que se valida 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, y actividad 14 "Revisar si se vulnero alguna política de seguridad" siendo el control: "Esta actividad se establece como control del procedimiento dado que 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."
  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 y si los riesgos residuales en nivel bajo continuaban igual, así como las matrices de los procesos.

- Instructivo GDT-03-IN-03 versión 1 de fecha 10 de junio de 2022, Instructivo de Cifrado de Información
  El objetivo del instructivo corresponde a "Definir los mecanismos de cifrado1 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.

- Instructivo GDT-03-IN-04 versión 1 de fecha 15 de diciembre de 2022, Instructivo Análisis Forense Digital
  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

- Documento Técnico GDT-DT-01 v1. del 9 de diciembre de 2022, "Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información"

- Documento Técnico GDT-DT-04 v1. del 15 de diciembre de 2022, "Documento Técnico Controles de Seguridad de la Información para la construcci[on de software seguro"
  El objetivo del Documento es "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"

6.5 Indicadores

- 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 “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

Gráfica 1. 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 tecnologia
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 PERIÓDICO 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 PERIÓDICO 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

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 en un 100%. Al corte del 30 de junio se reporta cumplido 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 corte del 30 de junio reporta ejecución del 49,98%.

6.6 Riesgos de Gestión y Corrupción

Revisada la matriz Institucional de Riesgos Gestión, 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 reisgo 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 del segundo trimestre informa la ejecución de la totalidad de las actividades programadas en la estrategia de comunicaciones.

Asimismo, se reporta la materialización del riesgo para el 24 de abril de 2023 y como acciones implementadas informa "A raiz de las situaciones originadas por la indisponibilidad de la infraestructura tecnológica, la Unidad ha venido implementando un plan de contingencia para dar solución inmediata a la situación para restablecer la disponibilidad, y poder restablecer los sistemas de información. Conforme a la magnitud de los eventos sucedidos, se procederá a crear una oportunidad de mejora en el sistema Pandora, que permita documentar y registrar las acciones del plan de contingencia que se están ejecutando. Se revisará la matriz de riesgos para fortalecer las acciones de tratamiento y/o mejorar o fortalecer controles"

El proceso reportó a la Oficina Asesora de Planeación en el seguimiento del segundo trimestre, las actividades desarrolladas y un avance del 50% dentro de la programación anual. Así mismo, colocó los soportes o evidencias correspondientes en el SharePoint, dando cumplimiento a la metodología establecida.

En cuanto a los riesgos de corrupción, el proceso Gestión y desarrollo de las TIC, solo registra un riesgo, el RC-GDT-01 que corresponde a la "Posibilidad de acceso a información por parte de personal no autorizado, en beneficio propio y particular, se evidenció el reporte a la OAP y el desarrollo durante el segundo trimestre de las actividades 1 y 2 establecidas para reducir el riesgo. Para la primera se reporta un avance del 42% y para la segunda el avance es del 50%

La funcionaria a cargo del seguimiento y monitoreo a estos riesgos y de su reporte a la OAP, informa que para el periodo de alcance de esta auditoría, no se presentó materialización del riesgo.

6.7 Riesgos de Seguridad de la Información

La Matriz de Riesgos Institucional para el proceso Gestión y Desarrollo de las TIC, contempla 28 riesgos, de los que se revisaron y verificaron los pares, que corresponden en su mayoría a Pérdida de Disponibilidad, y que SON

los identificados con los códigos RS-GDT-02, 04, 06, 08, 10, 12, 14, 16, 18, 20, 22, 24, 26 y 28, de ellos requieren tratamiento los riesgos RS-GDT-02, 10, 12, 16, 20, 26 y 28, para estos riesgos la Gerencia tiene estandarizadas cinco (5) actividades a desarrollar para 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 segundo trimestre de 2023 el proceso reporta la materialización de seis (6) riesgos, indicados en la siguiente tabla, todos asociados a Pérdida de Disponibilidad

Tabla 1. Riesgos Materializados II trimestre 2023

Riesgo	Activo de información	Eventos	Acciones de tratamiento
RS-GDT-02	Base de datos del Sistema Infodoc Integrada con software de CA Base de datos SIIC, LPC, FOCA Base de datos ERP (SICAPITAL) Repositorios de información misional histórica Repositorios de información índice del archivo digital Base de datos de Desarrollo - SIIC Base de datos de PreProducción - SIIC Base de datos de Pruebas SIIC	El riesgo de disponibilidad de las bases de datos se identifica por estar incluidas dentro del activo PCA que fue el activo afectado. - Este riesgo no aplica para la base de datos de GoCatastral toda vez que el servicio se encuentra dispuesto en nube. El evento principal que materializó el riesgo de disponibilidad de las bases de datos está relacionado con el daño físico que se presentó en la PCA, activo donde se encontraban los activos afectados. - La PCA tuvo soporte hasta febrero del 2022 y se toma la decisión de no renovar el contrato de soporte por el grado de obsolescencia del activo y por los costos que conllevaba la renovación del contrato de un activo que ya se encontraba obsoleto. - Causa raíz relacionada con la falta de presupuesto en la entidad.	Estrategia Migración de servicios a la nube de Azure y a la Nube de OCI Los servicios de Oracle - se migran a la Nube de OCI Los servicios de Microsoft - se migran a la Nube de Azure La información del Fileserver - Inicialmente se dispone un servidor en tierra provisional para la restauración de la información de las dependencias - Se restaura la información más importante requerida por las dependencias, sin embargo la estrategia será subir la información necesaria por las deoendencias , sin embargo la estrategia será subir la información necesaria por las dependencias al Repositorio de nube actual de la entidad (sharepoint) A la fecha se han realizado las siguientes actividades por parte del equipo de Infraestrcutura - Migración gradual de servicios a la nube de servicios principales de la entidad - Identificación de servicios que deben permanecer en tierra : Se dejan algunos servicios en tierra , infraestrcutura que por su grado de obsolescencia debe contar con los respectivos contratos de soporte. (Directorio Activo - Servidor de dominio - Bases de datos historica que por el tamaño no se migra la nube - Sistemas de información que por su obsolescencia no se migrar a la nube) - Posiblemente un esquema de backup de la nube

RS-GDT-06	MESA DE SERVICIOS - CA	El riesgo de disponibilidad de la herramienta de CA se identifica por estar incluida dentro de un servidor ubicado en el activo PCA, activo afectado. El evento principal que materializó el riesgo de disponibilidad de la HERRAMIENTA DE CA está relacionado con el daño físico que se presentó en la PCA, activo donde se encontraban los activos afectados. - La PCA tuvo soporte hasta febrero del 2022 y se toma la decisión de no renovar el contrato de soporte por el grado de obsolescencia del activo y por los costos que conllevaba la renovación del contrato de un activo que ya se encontraba obsoleto. - Causa raíz relacionada con la falta de presupuesto en la entidad.	Estrategia Migración de servicios a la nube de Azure y a la Nube de OCI Los servicios de Oracle - se migran a la Nube de OCI Los servicios de Microsoft - se migran a la Nube de Azure La información del Fileserver - Inicialmente se dispone un servidor en tierra provisional para la restauración de la información de las dependencias - Se restaura la información más importante requerida por las dependencias, sin embargo la estrategia será subir la información necesaria por las deoendencias , sin embargo la estrategia será subir la información necesaria por las dependencias al Repositorio de nube actual de la entidad (sharepoint) A la fecha se han realizado las siguientes actividades por parte del equipo de Infraestrcutura - Migración gradual de servicios a la nube de servicios principales de la entidad - Identificación de servicios que deben permanecer en tierra : Se dejan algunos servicios en tierra , infraestrcutura que por su grado de obsolescencia debe contar con los respectivos contratos de soporte. (Directorio Activo - Servidor de dominio - Bases de datos historica que por el tamaño no se migra la nube - Sistemas de información que por su obsolescencia no se migrar a la nube) - Posiblemente un esquema de backup de la nube
RS-GDT-14	FILESERVER (Hardware)	El riesgo de disponibilidad de la herramienta de CA se identifica por estar incluida dentro de un servidor ubicado en el activo PCA, activo afectado. El evento principal que materializó el riesgo de disponibilidad de la HERRAMIENTA DE CA está relacionado con el daño físico que se presentó en la PCA, activo donde se encontraban los activos afectados. - La PCA tuvo soporte hasta febrero del 2022 y se toma la decisión de no renovar el contrato de soporte por el grado de obsolescencia del activo y por los costos que conllevaba la renovación del contrato de un activo que ya se encontraba obsoleto. - Causa raíz relacionada con la falta de presupuesto en la entidad.	Estrategia Migración de servicios a la nube de Azure y a la Nube de OCI Los servicios de Oracle - se migran a la Nube de OCI Los servicios de Microsoft - se migran a la Nube de Azure La información del Fileserver - Inicialmente se dispone un servidor en tierra provisional para la restauración de la información de las dependencias - Se restaura la información más importante requerida por las dependencias, sin embargo la estrategia será subir la información necesaria por las deoendencias , sin embargo la estrategia será subir la información necesaria por las dependencias al Repositorio de nube actual de la entidad (sharepoint) A la fecha se han realizado las siguientes actividades por parte del equipo de Infraestrcutura - Migración gradual de servicios a la nube de servicios principales de la entidad - Identificación de servicios que deben permanecer en tierra : Se dejan algunos servicios en tierra , infraestrcutura que por su grado de obsolescencia debe contar con los respectivos contratos de soporte. (Directorio Activo - Servidor de dominio - Bases de datos historica que por el tamaño no se migra la nube - Sistemas de información que por su obsolescencia no se migrar a la nube) - Posiblemente un esquema de backup de la nube

RS-GDT-16	Servidores Virtualizados en producción (Hardware)	El riesgo de disponibilidad de la herramienta de CA se identifica por estar incluida dentro de un servidor ubicado en el activo PCA, activo afectado. El evento principal que materializó el riesgo de disponibilidad de la HERRAMIENTA DE CA está relacionado con el daño físico que se presentó en la PCA, activo donde se encontraban los activos afectados. - La PCA tuvo soporte hasta febrero del 2022 y se toma la decisión de no renovar el contrato de soporte por el grado de obsolescencia del activo y por los costos que conllevaba la renovación del contrato de un activo que ya se encontraba obsoleto. - Causa raíz relacionada con la falta de presupuesto en la entidad.	Estrategia Migración de servicios a la nube de Azure y a la Nube de OCI Los servicios de Oracle - se migran a la Nube de OCI Los servicios de Microsoft - se migran a la Nube de Azure La información del Fileserver - Inicialmente se dispone un servidor en tierra provisional para la restauración de la información de las dependencias - Se restaura la información más importante requerida por las dependencias, sin embargo la estrategia será subir la información necesaria por las deoendencias , sin embargo la estrategia será subir la información necesaria por las dependencias al Repositorio de nube actual de la entidad (sharepoint) A la fecha se han realizado las siguientes actividades por parte del equipo de Infraestrcutura - Migración gradual de servicios a la nube de servicios principales de la entidad - Identificación de servicios que deben permanecer en tierra : Se dejan algunos servicios en tierra , infraestrcutura que por su grado de obsolescencia debe contar con los respectivos contratos de soporte. (Directorio Activo - Servidor de dominio - Bases de datos historica que por el tamaño no se migra la nube - Sistemas de información que por su obsolescencia no se migrar a la nube) - Posiblemente un esquema de backup de la nube
RS-GDT-20	ORACLE FLASH STORAGE SYSTEM FS1 ORACLE STORAGETEK SL150 (Hardware)	El riesgo de disponibilidad de la herramienta de CA se identifica por estar incluida dentro de un servidor ubicado en el activo PCA, activo afectado. El evento principal que materializó el riesgo de disponibilidad de la HERRAMIENTA DE CA está relacionado con el daño físico que se presentó en la PCA, activo donde se encontraban los activos afectados. - La PCA tuvo soporte hasta febrero del 2022 y se toma la decisión de no renovar el contrato de soporte por el grado de obsolescencia del activo y por los costos que conllevaba la renovación del contrato de un activo que ya se encontraba obsoleto. - Causa raíz relacionada con la falta de presupuesto en la entidad.	Estrategia Migración de servicios a la nube de Azure y a la Nube de OCI Los servicios de Oracle - se migran a la Nube de OCI Los servicios de Microsoft - se migran a la Nube de Azure La información del Fileserver - Inicialmente se dispone un servidor en tierra provisional para la restauración de la información de las dependencias - Se restaura la información más importante requerida por las dependencias, sin embargo la estrategia será subir la información necesaria por las deoendencias , sin embargo la estrategia será subir la información necesaria por las dependencias al Repositorio de nube actual de la entidad (sharepoint) A la fecha se han realizado las siguientes actividades por parte del equipo de Infraestrcutura - Migración gradual de servicios a la nube de servicios principales de la entidad - Identificación de servicios que deben permanecer en tierra : Se dejan algunos servicios en tierra , infraestrcutura que por su grado de obsolescencia debe contar con los respectivos contratos de soporte. (Directorio Activo - Servidor de dominio - Bases de datos historica que por el tamaño no se migra la nube - Sistemas de información que por su obsolescencia no se migrar a la nube) - Posiblemente un esquema de backup de la nube

RS-GDT-26	PLATAFORMA: ORACLE PCA (PRIVATE CLOUD APPLIANCE)- ORACLE VM (Hardware)	El riesgo de disponibilidad de la herramienta de CA se identifica por estar incluida dentro de un servidor ubicado en el activo PCA, activo afectado. El evento principal que materializó el riesgo de disponibilidad de la HERRAMIENTA DE CA está relacionado con el daño físico que se presentó en la PCA, activo donde se encontraban los activos afectados. - La PCA tuvo soporte hasta febrero del 2022 y se toma la decisión de no renovar el contrato de soporte por el grado de obsolescencia del activo y por los costos que conllevaba la renovación del contrato de un activo que ya se encontraba obsoleto. - Causa raíz relacionada con la falta de presupuesto en la entidad.	Estrategia Migración de servicios a la nube de Azure y a la Nube de OCI Los servicios de Oracle - se migran a la Nube de OCI Los servicios de Microsoft - se migran a la Nube de Azure La información del Fileserver - Inicialmente se dispone un servidor en tierra provisional para la restauración de la información de las dependencias - Se restaura la información más importante requerida por las dependencias, sin embargo la estrategia será subir la información necesaria por las deoendencias , sin embargo la estrategia será subir la información necesaria por las dependencias al Repositorio de nube actual de la entidad (sharepoint) A la fecha se han realizado las siguientes actividades por parte del equipo de Infraestrcutura - Migración gradual de servicios a la nube de servicios principales de la entidad - Identificación de servicios que deben permanecer en tierra : Se dejan algunos servicios en tierra , infraestrcutura que por su grado de obsolescencia debe contar con los respectivos contratos de soporte. (Directorio Activo - Servidor de dominio - Bases de datos historica que por el tamaño no se migra la nube - Sistemas de información que por su obsolescencia no se migrar a la nube) - Posiblemente un esquema de backup de la nube

Fuente: Propio del Auditor con base en el archivo Matriz_riesgosSD_GDT_2023_II

Riesgos materializados que terminaron de una manera u otra impactando la gestión de la UAECD, siendo los Eventos y Acciones de tratamiento implementadas, las mismas para ellos

(OM1) Evidenciada la materialización del riesgo se debería revisar los controles establecidos y la efectividad de los mismos, a efecto de buscar el prevenir la presentaci[on de nuevas materializaciones que afecten la funcionalidad de la entidad.

Realizado seguimiento al Informe de Seguimiento Riesgos de Seguridad Digital que prepara trimestralmente el Equipo de Seguridad y Privacidad de la Información -Oficial de Seguridad de la Información, se observa:

- Segundo trimestre de 2022, no se presentó materialización de riesgos de seguridad digital en ninguno de los procesos y áreas de la Unidad
- En el tercer trimestre de 2022 se presentó materialización de riesgos en el proceso de Gestión y Desarrollo de las TIC, que desencadenó la materialización de riesgos en diferentes procesos y/o áreas

Tabla 2. Riesgos Materializados III trimestre 2022

Proceso	Cod	Nombre Riesgo	Observaciones

	Riesgo		
Gestión y Desarrollo de las TIC	S-GDT-14	Pérdida de Disponibilidad del Fileserver (Hardware)	Se genera indisponibilidad en los servicios de Dirección, GGC, GCA – Riesgo actualmente controlado en monitoreo constante
Gestión y Desarrollo de las TIC	S-GDT-18	Pérdida de Disponibilidad del Firewalls, Switch Core, Switch WAN (Hardware)	Riesgo presentado a nivel de los firewalls – actualmente controlado en monitoreo constante
Gestión y Desarrollo de las TIC	S-GDT-26	Pérdida de Disponibilidad Plataforma Oracle PCA (Hardware)	Riesgo permanente por obsolescencia y falta de soporte – En monitoreo constante. Se incluye nuevo
Gestión y Desarrollo de las TIC	S-GDT-28	Pérdida de Disponibilidad infraestructura de Nube Azure-OCI (Servicio)	Riesgo a nivel de la infraestructura de Azure – Se incluye nuevo Control y en monitoreo constante
Dirección / Gestión Corporativa	RS-TRV-4	Pérdida de Disponibilidad Fileserver Dirección / GGC (Servicio)	Riesgo se desencadena por materialización de RS-GDT-14 Riesgo controlado
Gestión Catastral (SIE-SIFJ-GIC	RS-GCA-6	Pérdida de Disponibilidad Fileserver SIE-SIFJ-Gestión_GIC (Servicio)	Riesgo se desencadena por materialización de RS-GDT-14 Riesgo controlado
Gestión Catastral (Territorios)	RS-GCA-16	Pérdida de Disponibilidad Información Digital / Electrónica	Riesgo materializado por malware. Riesgo controlado
Gestión de información Geográfica	RS-GIG-7	Pérdida de Disponibilidad Servicios Web Geográficos, Mapas base, Mapa de Referencia, etc. (Servicios)	Riesgo se desencadena por materialización de RS-GDT-28 Riesgo controlado

Fuente: Informe Seguimiento Riesgos III Trimestre 2022

- En el cuarto trimestre de 2022 se presentó materialización de riesgos en el proceso de Gestión de Información Geográfica.

Tabla 3. Riesgos Materializados IV trimestre 2022

Proceso	Cod Riesgo	Nombre Riesgo	Observaciones
Gestión de Información Geográfica	RS-GIG-2	Pérdida de disponibilidad en las aplicaciones móviles y web de IDECA (servicios web geográficos - software)	Inicialmente el evento que materializo el riesgo de perdida de disponbilidad del activo infraestructura de nube de Azure, esta relacionado con el daño de un cluster virtual. Este daño se presentó (información referida por proveedor Esri), porque no se llevó a cabo una secuencia en el apagado de los servidores. Se aclara que los servidores de la nube de Azure fueron apagados toda vez que había escases de recursos en la nube de Azure. Este apagado y posterior daño del cluster generó una indisponibilidad en los servicios web geográficos que se encuentran alojados en la nube de Azure. Se presentaron fallas en el componente denominado Portal for ArcGIS de la infraestructura ArcGIS Enterprise, lo que motivo indisponibilidad temporal de los servicios web geográficos. Si bien se restauraron el dia 28 de octubre de 2022 algunos de estos servicios web (los que deben

			estar configurados como servicios seguros) no tomaron la configuración correspondiente, razón por la cual, se solicitó detenerlos para evitar inconvenientes de seguridad al exponer una información pública clasificada, situación que se mantiene a la fecha de presentación del seguimiento del cuarto trimestre 2022. Adicionalmente seguimos sin disponibilidad de la nube de Azure.
Gestión de Información Geográfica	RS-GIG-4	Pérdida de disponibilidad en las bases de datos geográficas	Dificultades en la lectura y/o recuperación de los datos, principalmente en aquellos con un alto número de registros que impide una visualización nula o parcial de los datos

Fuente: Informe Seguimiento Riesgos IV Trimestre 2022

- En el primer trimestre de 2023 se presentó materialización de riesgos en el proceso de Gestión de Información Geográfica

Tabla 3. Riesgos Materializados I trimestre 2023

Proceso	Cod Riesgo	Nombre Riesgo	Observaciones
Gestión de Información Geográfica	RS-GIG-2	Pérdida de Disponibilidad de Aplicaciones móviles y web IDECA Servicios Web Geográficos, Mapas base, Mapa de Referencia	Evento: Se mantiene la materialización del resgo de pérdida de disponibilidad del activo servicios web geográficos de la Infraestructura de Datos Espaciales de Bogotá, toda vez que ocurrió un daño en el servidor de imágenes en la infraestructura OnPremise que conllevo a la caída de los servicios de Mapa Base. Una vez restablecido el servicio desde Ideca se han efectuado verificaciones de los mismos evidenciado una disminución en el rendimiento de los servicios. Fecha Ocurrencia: Reporte inicial del 17 de marzo con cierre del evento el 22 de marzo de 2023. Acción de tratamiento implementadas: Una vez identificada la indisponibilidad de los servicios se crea por parte de Ideca mesa de servicios SOL0288720-23 con reporte de la situación. Gerencia de Tecnología proceden a revisar el caso, a la revisión de los servidores y restablecimiento de los mismos.
Gestión de Información Geográfica	RS-GIG-4	Pérdida de disponibilidad en las 1. Bases de datos geográfica 2. Bases de datos geográfica de servicios público	Evento: Se mantiene la materialización del riesgo de pérdida de disponibilidad del activo servicios web geográficos de la Infraestructura de Datos Espaciales de Bogotá, toda vez que ocurrió un daño en el servidor de imágenes en la infraestructura OnPremise que conllevo a la caída de los servicios de Mapa Base. Una vez restablecido el servicio desde Ideca se han efectuado verificaciones de los mismos evidenciado una disminución en el rendimiento de los servicios. Fecha Ocurrencia: Reporte inicial del 17 de marzo con cierre del evento el 22 de marzo de 2023 Acción de tratamiento implementadas: Una vez identificada la indisponibilidad de los servicios se crea por parte de Ideca mesa de servicios SOL0288720-23 con reporte de la situación.

Fuente: Informe Seguimiento Riesgos I Trimestre 2023

Lo anterior con base en el seguimiento periódico que el Oficial de Seguridad de la Información efectúa a los mapas de riesgo de cada uno de los procesos de la UAECD, elaborando los informes pertinentes que incluyen un punto relacionado con la materialización o no de los riesgos y cuando se materializan, las observaciones necesarias.

Observación del proceso -Equipo de Seguridad

"Solicitamos que se considere el ajuste de la siguiente manera:
Para el segundo trimestre de 2023, aunque se presentó materialización de riesgos en diferentes procesos y asociados al daño de la PCA, no ha sido emitido el informe por parte del Equipo de Seguridad de la Información, toda vez que el proceso de reporte y revisión ha sido complicado para las dependencias, el cual ha sido subsanado por el equipo de seguridad realizando mesas de trabajo para aclaración respecto a lo que se debe reportar sobre la materialización de los riesgos."

Respuesta OCI.
Se acepta la solicitud presentada por el Equipo de Seguridad de la Información, por consiguiente, el texto queda como se indica a continuación:

Para el segundo trimestre de 2023, aunque se presentó materialización de riesgos en diferentes procesos y asociados al daño de la PCA, no ha sido emitido el informe por parte del Equipo de Seguridad de la Información, toda vez que el proceso de reporte y revisión ha sido complicado para las dependencias, el cual ha sido subsanado por el Equipo de Seguridad realizanod mesas de trabajo para aclaración respecto a lo que se debe reportar sobre la materialización de los riesgos.

6.8 EVALUACION MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El archivo Excel "Inst_Eval_MSPI_2022" en su hoja "PORTADA" bajo el título "INTRUMENTO DE IDENTIFICACION DE LA LINEA BASE DE SEGURIDAD" diligenciado por la UAECD al corte del 30 de abril de 2023, 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 UAEC en la implementación de estos

Gráfica 2. Brechas frente al Anexo A ISO 27001:2013

Fuente: Tomado de "Inst_Eval_MSPI_2023"

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

La gráfica muestra que, dentro del alcance de la presente auditoría, las debilidades se encuentran en la implementación y ejecución de los controles establecidos en los dominios A.10 CRIPTOGRAFIA con una calificación de 80 puntos, seguido por los dominios A.9 CONTROL DE ACCESO con una calificación de 81 puntos, A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION y A.11 SEGURIDAD FISICA Y DEL ENTORNO, con calificaciones de 82 puntos respectivamente, lo que con respecto a la efectividad del control indica que el primero se ubica como GESTIONADO (rango de la calificación entre 61 y 80) y los restantes como OPTIMIZADO (rango de la calificación entre 81 y 100).

Observación del proceso -Equipo de Seguridad

Ajustar Tabla 4. Evaluación de Efectividad de Controles Anexo A -27001:2013, página 19:

Respuesta OCI.

Se acepta la solicitud presentada por el Equipo de Seguridad de la Información, por consiguiente, el texto queda como se indica a continuación:

Tabla 4. Evaluación de Efectividad de Controles Anexo A -27001:2013

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**	**Calificación Anterior**
A.5	INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA HOJA LEVANTAMIENTO DE INFORMACIÓN	100	**OPTIMIZADO**	100
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION	82	**OPTIMIZADO**	75
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	88	**OPTIMIZADO**	88
A.8	GESTION DE ACTIVOS	89	**OPTIMIZADO**	89
A.9	CONTROL DE ACCESO	81	**OPTIMIZADO**	64
A.10	CRIPTOGRAFÍA	80	**GESTIONADO**	70
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	82	**OPTIMIZADO**	82
A.12	SEGURIDAD DE LAS OPERACIONES	85	**OPTIMIZADO**	84
A.13	SEGURIDAD DE LAS COMUNICACIONES	85	**OPTIMIZADO**	85
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	79	**GESTIONADO**	56
A.15	RELACIONES CON LOS PROVEEDORES	80	**GESTIONADO**	70
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	97	**OPTIMIZADO**	97
A.17	Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio	64	**GESTIONADO**	76,5
A.18	Cumplimiento	83	**OPTIMIZADO**	82,5
PROMEDIO EVALUACIÓN DE CONTROLES		**84**	**OPTIMIZADO**	**80**

Fuente: Tomado de "Inst_Eval_MSPI_2023"

Para el caso de los dominios A.5 al A.13, el promedio de los controles arroja un valor de 85,78 que, de acuerdo a la valoración del instrumento, posiciona la Evaluación de Efectividad de estos controles en "OPTIMIZADO". Se resalta la gestión efectuada en el dominio A.5 POLITICAS DE SEGURIDAD DE LA INFORMACION, que registra una calificación de 100 puntos.

Para los dominios objeto de la presente evaluación, se mantiene o mejora la calificación con respecto de la registrada en la Auditoría vigencia 2022. Se destaca los avances en los dominios A.6 Organización de la Seguridad de la Información, A.9 Control de Acceso y A.10 Criptografía.

Aunque esta por fuera del alcance del presente ejercicio auditor, llama la atención la variación negativa en la calificación del dominio A.17 que de una calificación de 76,5 disminuyo a 64 puntos.

- **Dominio A.5- Políticas de Seguridad de la Información**

Con base en la información en cuadro Excel denominado "Inst_Eval_MSPI_2023" se evidencia para el dominio A.5 una calificación de 100 puntos, para el cual la recomendación corresponde a continuar con las revisiones de las políticas de seguridad y privacidad de la información por parte de Comité de Gestión y Desempeño, por lo menos una vez al año y, fortalecer la comunicación de las políticas a los directivos.

- **Dominio A.6 – ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

La calificación registrada para este dominio A.6 corresponde a 82 puntos, promedio de los componentes A.6.1 y A.6.2, mostrados a continuación

LITERAL	ITEM	CALIFICACION
A.6.1	**ORGANIZACIÓN INTERNA**	**84**
A.6.1.1	Roles y responsabilidades para la seguridad de la información	80
A.6.1.2	Separación de deberes / tareas	80
A.6.1.3	Contacto con las autoridades.	80
A.6.1.4	Contacto con grupos de interés especiales	100
A.6.1.5	Seguridad de la información en la gestión de proyectos	80
A.6.2	**DISPOSITIVOS MOVILES DE TELETRABAJO**	**80**
A.6.2.1	Política para dispositivos móviles	80
A.6.2.2	Teletrabajo	80

Todos los literales de este dominio registran calificación de 80 puntos con excepción del literal A.6.1.4 que registra una calificación de 100 puntos, en tal sentido para los demás literales se deben atender y desarrollar las recomendaciones plasmadas en el archivo "Inst_Eval_MSPI_2023"

- **Dominio A.7 – SEGURIDAD DE LOS RECURSOS HUMANOS**

La calificación registrada para este dominio A.7 corresponde a 88 puntos, promedio de los componentes A.7.1 y A.7.2, mostrados a continuación

LITERAL	ITEM	CALIFICACION
A.7.1	**ANTES DE ASUMIR EL EMPLEO**	**90**
A.7.1.1	Selección e investigación de antecedentes	100
A.7.1.2	Términos y condiciones del empleo	80
A.7.2	**DURANTE LA EJECUCION DEL EMPLEO**	**93**
A.7.2.1	Responsabilidades de la dirección	80
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	100
A.7.2.3	Proceso disciplinario	100
A.7.3	**TERMINACION Y CAMBIO DE EMPLEO**	**80**
A.7.3.1	Terminación o cambio de responsabilidades de empleo	80

En este dominio se debe enfatizar en el desarrollo de las recomendaciones establecidas en el archivo "Inst_Eval_MSPI_2023" para los literales A.7.1.2, A.7.2.1 y A.7.3.1

- **Dominio A.8 – GESTIÓN DE ACTIVOS**

La calificación registrada para este dominio A.8 corresponde a 95 puntos, promedio de los componentes A.8.1. A.8.2 y A.8.3, mostrados a continuación

LITERAL	ITEM	CALIFICACION
A.8.1	**RESPONSABILIDAD DE LOS ACTIVOS**	**95**
A.8.1.1	Inventario de activos	100
A.8.1.2	Propiedad de los activos	100
A.8.1.3	Uso aceptable de los activos	100
A.8.1.4	Devolución de activos	80
A.8.2	**CLASIFICACION DE INFORMACION**	**93**
A.8.2.1	Clasificación de la información	100
A.8.2.2	Etiquetado de la información	80
A.8.2.3	Manejo de activos	100
A.8.3	**MANEJO DE MEDIOS**	**80**
A.8.3.1	Gestión de medios removibles	80
A.8.3.2	Disposición de los medios	80
A.8.3.3	Transferencia de medios físicos	80

En este dominio se debe enfatizar en el desarrollo de las recomendaciones establecidas en el archivo “Inst_Eval_MSPI_2023” para los literales del componente A.8.3 Manejo de Medios

- **Dominio A.9 – CONTROL DE ACCESO**

La calificación registrada para este dominio A.9 corresponde a 91 puntos, promedio de los componentes A.9.1. A.9.2, A.9.3 y A.9.4, mostrados a continuación

LITERAL	ITEM	CALIFICACION
A.9.1	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**80**
A.9.1.1	Política de control de acceso	80
A.9.1.2	Acceso a redes y a servicios en red	80
A.9.2	**GESTIÓN DE ACCESO DE USUARIOS**	**80**
A.9.2.1	Registro y cancelación del registro de usuarios	80
A.9.2.2	Suministro de acceso de usuarios	**80**
A.9.2.3	Gestión de derechos de acceso privilegiado	80
A.9.2.4	Gestión de información de autenticación secreta de usuarios	80
A.9.2.5	Revisión de los derechos de acceso de usuarios	80
A.9.2.6	Retiro o ajuste de los derechos de acceso	80
A.9.3	**RESPONSABILIDADES DE LOS USUARIOS**	**80**
A.9.3.1	Uso de información de autenticación secreta	80
A.9.4	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	**84**
A.9.4.1.	Restricción de acceso a la información	80
A.9.4.2	Procedimiento de ingreso seguro	80

A.9.4.3	Sistema de gestión de contraseñas	80
A.9.4.4	Uso de programas utilitarios privilegiados	100
A.9.4.5	Control de acceso a códigos fuente de programas	80

En el dominio A.9 es necesario atender las recomendaciones establecidas en el archivo "Inst_Eval_MSPI_2023" para cada uno de los literales que conforman los cuatro (4) componentes del dominio, con excepción del literal A.9.4.4

- **Dominio A.10 – CRIPTOGRAFÍA**

La calificación registrada para este dominio A.10 corresponde a 80 puntos

LITERAL	ITEM	CALIFICACION
A.10.1	**CONTROLES CRIPTOGRÁFICOS**	**80**
A.10.1.1	Política sobre el uso de controles criptográficos	80
A.10.1.2	Gestión de llaves	80

Para el dominio A.10 CRIPTOGRAFIA se debe aceptar y desarrollar las recomendaciones establecidas para los dos literales en el archivo "Inst_Eval_MSPI_2023".

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

La calificación registrada para este dominio A.11 corresponde a 82 puntos, promedio de los componentes A.11.1 y A.11.2, mostrados a continuación

LITERAL	ITEM	CALIFICACION

A.11.1	**ÁREAS SEGURAS**	**83**
A.11.1.1	Perímetro de seguridad física	100
A.11.1.2	Controles físicos de entrada	80
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

En el dominio A.11 es pertinente para cada uno de los literales de los dos componentes, desarrollar las recomendaciones establecidas en el archivo “Inst_Eval_MSPI_2023”.

- **Dominio A.12 – SEGURIDAD DE LAS OPERACIONES**

La calificación registrada para este dominio A.12 corresponde a 84 puntos, promedio de los componentes A.12.1, A.12.2, A.12.3, A.12.3, A.12.4, A.12.5, A.12.6 Y A.12.7 mostrados a continuación

LITERAL	ITEM	CALIFICACION
A.12.1	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**70**
A.12.1.1	Procedimientos de operación documentados	80
A.12.1.2	Gestión de cambios	100
A.12.1.3	Gestión de capacidad	40
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	60
A.12.2	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**80**
A.12.2.1	Controles contra códigos maliciosos	80
A.12.3	**COPIAS DE RESPALDO**	**80**
A.12.3.1	Respaldo de la información	80
A.12.4	**REGISTRO Y SEGUIMIENTO**	75
A.12.4.1	Registro de eventos	80
A.12.4.2	Protección de la información de registro	60
A.12.4.3	Registros del administrador y del operador	60

A.12.4.4	Sincronización de relojes	100
A.12.5	**CONTROL DE SOFTWARE OPERACIONAL**	100
A.12.5.1	Instalación de software en sistemas operativos	100
A.12.6	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	90
A.12.6.1	Gestión de las vulnerabilidades técnicas	80
A.12.6.2	Restricciones sobre la instalación de software	100
A.12.7.	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**	100
A.12.7.1	Controles sobre auditorías de sistemas de información	100

En el dominio 12 SEGURIDAD DE LAS OPERACIONES se debe priorizar el desarrollo de las recomendaciones para los literales A.12.1.3, A.12.1.4, A.12.4.2, A.12.4.3, que son los que registran las calificaciones más bajas

- **Dominio A.13 – SEGURIDAD DE LAS COMUNICACIONES**

La calificación registrada para este dominio A.13 corresponde a 85 puntos, promedio de los componentes A.13.1, y A.13.2 mostrados a continuación

LITERAL	ITEM	CALIFICACION
A.13.1	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**80**
A.13.1.1	Controles de redes	80
A.13.1.2	Seguridad de los servicios de red	80
A.13.1.3	Separación en las redes	80

A.13.2	**TRANSFERENCIA DE INFORMACIÓN**	**90**
A.13.2.1	Políticas y procedimientos de transferencia de información	80
A.13.2.2	Acuerdos sobre transferencia de información	100
A.13.2.3	Mensajería electrónica	80
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	100

En el dominio A.13 SEGURIDAD DE LAS COMUNICACIONES es pertinente desarrollar las recomendaciones a los literales del componente A.13.1 Gestión de la seguridad de las redes

(OM) 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 literales A.12.1.3, A.12.1.4, A.12.4.2 Y A.12.4.3

Hallazgos

No.	Descripción del hallazgo	No Conformidad	Oportunidad	Norma, criterio, Requisito o Documento asociado	Área /Cargo Responsable	Anexo Evidencia
1	**(OM)** Evidenciada la materialización del riesgo se debería revisar los controles preventivos establecidos y la efectividad de los mismos, a efecto de buscar el prevenir la presentación de nuevas materializaciones que afecten la funcionalidad de la entidad.		**X**	Guía para la Administración del Riesgo v.6 DAFP	Equipo Seguridad de la Información	Archivo "Matriz_riesgosSD_GDT_2023_II"

No.	Descripción del hallazgo	No Conformidad	Oportunidad	Norma, criterio, Requisito o Documento asociado	Área /Cargo Responsable	Anexo Evidencia
2	**(OM)** 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 literales A.12.1.3, A.12.1.4, A.12.4.2 Y A.12.4.3		**X**	Anexo A de la ISO27001 de 2013	Equipo Seguridad de la Información	Archivo "Inst_Eval_MSPI_2023"

7. FORTALEZAS

El conocimiento y experiencia del Equipo de Seguridad de la información que son base o pilar para el tratamiento de los riesgos de seguridad de la información en la UAECD y que trasciende a los enlaces de los procesos para las diferentes actividades que se deben desarrollar en esta materia

La UAECD en los dominios A.5 a A.13, registra y evidencia los setenta y seis (76) controles que están contemplados en el anexo A de la norma ISO 27001:2013, para los cuales ha efectuado levantamiento de información que en general ha permitido evidenciar cómo se cumple (evidencia), establecer la brecha existente y la recomendación(es) pertinentes.

La calificación registrada para los dominios objeto de esta auditoría en el archivo "Inst_Eval_MSPI_2022" que en promedio arroja un valor de 85.8, evidencia el trabajo adelantado por la Unidad a través del Equipo de Seguridad de la Información, para la documentación, establecimiento y mejoramiento de los controles de la norma, con el objetivo de blindar a la entidad en materia de seguridad y privacidad de la información.

La documentación aportada para el desarrollo del ejercicio auditor evidencia el esfuerzo y trabajo efectuado por el Oficial de Seguridad y por el Equipo de Seguridad de la Información, para la actualización del Documento Técnico Manual de Políticas Detalladas de Seguridad y Privacidad de la Información, demás documentos técnicos, procedimientos y otros relacionados con el SGSPI.

La gestión que ha adelantado y adelantan las diferentes Líneas de Defensa de la UAECD para la administración y gestión del riesgo y de manera específica en materia de gestión del riesgo de seguridad de la información en la Unidad, a través de la revisión, análisis y determinación de los activos de información y sus riesgos, para el establecimiento de la matriz de riesgos de seguridad de la información, matriz que es aprobada a través del Comité de Gestión y Desempeño de la UAECD.

8. DEBILIDADES:

Para la vigencia 2023 la UAECD fue sujeto de un recorte presupuestal, situación que trasciende a la Gerencia de Tecnología, impactada con una disminución de aproximadamente $3.990 millones equivalentes al 27,27% con respecto de la vigencia 2022, afectando temas como las nubes Azure y Oracle que podrían impactar en materia de Seguridad y Privacidad de la Información. Así mismo, la afectación en la continuidad de la prestación de servicio de la contratista que forma parte del Equipo de Seguridad de la Información, que de manera directa repercuten en las actividades que debe adelantar el Equipo de Trabajo de Seguridad y Privacidad de la Información.

9. CONCLUSIONES

Se evidenció la existencia y aplicación de procedimientos, instructivos y documentos técnicos que en materia de Seguridad y Privacidad de la información orientan y rigen el actuar de la entidad, estableciendo controles y determinando responsabilidades

Se verificó la formulación, aprobación y desarrollo del Plan de Seguridad y Privacidad de la Información para la vigencia 2023, así como la parametrización en PANDORA del indicador 4.1.E PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION CUMPLIDO, para el monitoreo, seguimiento y cumplimiento del Plan de Seguridad de la Información de la Información

Se constató la gestión en materia de la determinación de los riesgos de gestión y corrupción, así como el desarrollo de los controles establecidos a ellos y su reporte periódico a la Oficina Asesora de Planeación -OAP

Se verificó la formulación y seguimiento en lo relacionado con los riesgos de seguridad de la información, as[i como el desarrollo de actividades de asesoría, acompañamiento y seguimiento a los procesos de la entidad en materia de gestión y administración de los riesgos de seguridad de la información.

Se revisó y efectuó seguimiento al establecimiento, implementación de los controles y evolución en la calificación de los controles determinados en el Anexo A de la norma ISO27001, para los dominios A.5 al A.13, observando avance en cada uno de ellos respecto de la medición registrada para el periodo de la auditoría anterior

9. RECOMENDACIONES

Desarrollar las dos (2) oportunidades de mejora planteadas en este ejercicio auditor, con el objeto de fortalecer y optimizar el sistema de control interno de la entidad

Aunque esta por fuera del alcance del presente ejercicio auditor, monitorear la variación negativa en la calificación del dominio A.17 que de una calificación de 76,5 disminuyo a 64 puntos.

Observación del proceso -Equipo de Seguridad

Se informa que la seguridad de la información es un proceso dinámico, en el cual cada vigencia se realiza el proceso de revisión del modelo MSPI con el fin de verificar la realidad de la Unidad respecto a los controles de seguridad implementados al interior de la entidad.

Respuesta OCI.

Se reconoce que efectivamente la seguridad de la información es un proceso dinámico …, precisamente por ser un proceso dinámico en el cual se presentó una variación negativa, se realiza la recomendación para el monitoreo de este literal en específico

Finalmente, las evidencias obtenidas de acuerdo con los criterios establecidos y los resultados de este informe se refieren a los soportes y evidencias aportadas en desarrollo de la auditoría y que fueron suministrados por el proceso Gestión y Desarrollo de las TIC - Sistema de Gestión de Seguridad y Privacidad de la Información como responsable del Sistema de Gestión y Seguridad de la Información, por tanto, no se hacen extensibles a otros soportes.

Asaneth Correa Rodriguez

ELBI ASANETH CORRREA RODRIGUEZ
Jefe Oficina de Control Interno

Elaboró: Luis Orlando Barrera Cepeda, Contratista Ing. Sistemas OCI.

Copia: Ing. Héctor Henry Pedraza P - Gerente de Tecnología