29. SEGUIMIENTO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el marco del contrato suscrito el día 08 de noviembre de 2022 cuyo propósito fue la prestación del servicio de apoyo a la gestión para el acompañamiento en la identificación del estado actual de la Gobernación de Caldas con respecto del modelo de seguridad y privacidad de la información (MSPI), la firma IFD EVIDENCE, presentó informe de diagnóstico del modelo de seguridad y privacidad de la Gobernación de Caldas en el mes de febrero de la presente anualidad.

Este informe se realizó conforme a un test de vulnerabilidades y cuya socialización se realizó al equipo de la Unidad de Sistemas a fin de que la entidad implementara las diferentes recomendaciones presentadas en este informe.

La Oficina de Control Interno llevó a cabo seguimiento sobre el avance en la implementación de dichas recomendaciones, desde su rol de evaluación y seguimiento el cual permite evaluar y contribuir a la mejora en los procesos de gestión, control y administración de las entidades.

La presente evaluación se realiza teniendo como herramienta una visita previa el 24 de agosto del 2023 y la solicitud de documentos relacionados con la implementación del modelo de seguridad y privacidad de la información a la Unidad de Sistemas de la entidad.

FECHA DEL INFORME: 25 de octubre de 2023

1.1 PROCESO: Gestión y planificación prospectiva del desarrollo (Seguridad digital)

1.2 OBJETIVOS DEL PRESENTE SEGUIMIENTO

1.2.1 OBJETIVO GENERAL: Verificar la implementación / avance de los documentos sugeridos por la empresa IFD EVIDENCE de acuerdo con los resultados del diagnóstico realizado al proceso de seguridad digital.

OBJETIVOS ESPECÍFICOS:

Evaluar en sitio las condiciones físicas en cuanto a centros de cómputo, locaciones, equipos activos de red, equipos de seguridad perimetral, sistema eléctrico, sistemas de control de acceso a sitios privados y oficinas, conforme las observaciones que realizó la firma IFD EVIDENCE

1.3 ALCANCE:

El seguimiento se llevó a cabo de manera física, mediante recorrido a la Unidad de Sistemas de la Gobernación de Caldas, para verificar las condiciones físicas en cuanto a centros de cómputo, locaciones y equipos.

Así mismo la verificación de la implementación o avance de documentos sugeridos por la empresa IFD EVIDENCE

1.4 SALVAGUARDA:

La auditoría interna es una actividad independiente y objetiva de evaluación y asesoría, concebida para agregar valor y mejorar las operaciones de una entidad.

Dicha evaluación comprende la valoración y verificación objetiva de evidencias, recolectadas de acuerdo a muestras seleccionadas.

En consecuencia, el propósito de presentar las observaciones en este informe es soportar de una mejor manera las oportunidades de mejoramiento identificadas durante la evaluación. Es importante resaltar que la auditoría se realizó sobre bases selectivas y por tanto no expresan un concepto general o total sobre las situaciones del proceso.

De otro lado, las recomendaciones presentadas no necesariamente obedecen a inconsistencias o incumplimiento de la norma, algunas de ellas pueden solamente sugerir mejores prácticas para lograr una mayor efectividad del proceso.

2. ACTIVIDADES DESARROLLADAS

2.1 REVISIÓN Y ANÁLISIS DOCUMENTAL

Para este ejercicio de auditoría se revisó las siguientes normas:

- Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control

- ISO-IEC 2007:2013.

2.2 EJECUCIÓN:

El seguimiento realizado por la Oficina de Control Interno a la Secretaría de planeación del Departamento se le dio apertura el día 24 de agosto, a las 08:30 AM, en la Unidad de sistemas, en compañía de los funcionarios de la Secretaría: Felipe Augusto Marín Montoya - Jefe Unidad de Sistemas, y el grupo auditor de la oficina de Control Interno: Julieta Toro Gómez – Jefe de Control Interno, Diana Carolina Osorio Buitrago – Contratista del Equipo control interno, Carlos Alberto Osorio Ortiz – Practicante.

3. RESULTADOS:

3.1 CONCEPTO GENERAL DE LOS RESULTADOS DE LA AUDITORÍA:

Como resultado de la visita técnica, se pudo evidenciar que, aunque se han adelantado algunas gestiones para mejorar la parte física de los cuartos los cuartos eléctricos, falta un mayor control de los elementos que se encuentran dentro de los mismos, evidenciándose aún desorden y existencia de elementos que no deberían estar allí y que pueden poner en riesgo la seguridad de su funcionamiento.

En la revisión documental se puede ver reflejado que muchas de las acciones no se han iniciado y algunas de las que tienen avances, muestran inconsistencias.

3.2 OBSERVACIONES

3.2.1 RIESGOS EN CUARTOS ELÉCTRICOS

Criterio: Políticas, procesos y procedimientos

Observación: A continuación, se mostrarán las observaciones encontradas en la visita a los cuartos eléctricos de la unidad de sistemas:

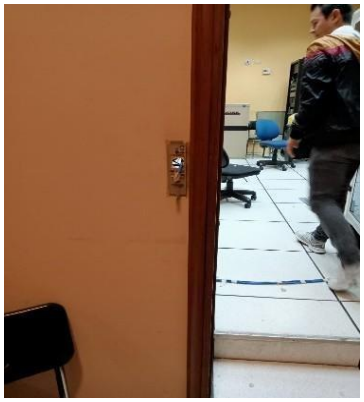
- **Visita técnica.**

  El día 24 de agosto se desarrolló la visita técnica prevista, con el objeto de hacer seguimiento a las condiciones físicas de los cuartos eléctricos de la

Gobernación de Caldas de conformidad con las sugerencias de la firma IFD EVIDENCE.

En la siguiente tabla se podrá visualizar el antes y después de los factores que fueron motivo de observación por la empresa IFD EVIDENCE.

Factor 1: Controles de acceso a cuartos eléctricos.

ANTES	DESPUÉS	OBSERVACIÓN
		Los sensores de los cuartos y centro de cómputo se encuentran en su correcto funcionamiento, haciendo los mantenimientos pertinentes.

Factor 2: Estructuración de cableado

ANTES	DESPUÉS	OBSERVACIÓN
		Se puede evidenciar una correcta distribución de cableados marquillados y etiquetados en todos los cuartos eléctricos y centro de cómputo.

Factor 3: Riesgos a cuartos eléctricos

ANTES	**DESPUÉS**
	
Observaciones: Los riesgos asociados con elementos inflamables (cartón, escobas, sillas, cables entre otros). **No han sido controlados de forma adecuada, ya que en todos los cuartos eléctricos es común encontrar alguno de estos objetos ya mencionados**, generando riesgo de incendio dentro de las instalaciones. **Recomendaciones:** Garantizar que en los cuartos eléctricos no se almacenen este tipo de elementos, por medio de planes, políticas y asignación de responsables.	

Factor 4: Estado estructural

ANTES	**DESPUÉS**
	

Observaciones: A pesar de que visualmente se observa deterioro en la imagen 1, se realizó un mantenimiento desde la terraza para controlar la humedad del cuarto eléctrico del piso 4.

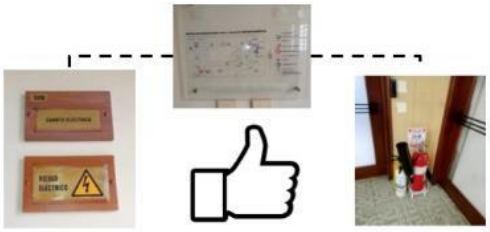
Con respecto al cuarto eléctrico que se encuentra ubicado en el piso subterráneo del edificio de la licorera y el cielo raso del centro de cómputo, **no existe algún tipo de mejoramiento, mantenimiento, modificación o plan de acción**.

Así mismo, se puede visualizar en la imagen 3, que **no se ha realizado mantenimiento al cielo raso al centro de cómputo.** Para terminar, los sistemas de contra incendio, sensores de humo y control de temperatura en los cuartos eléctricos del edificio de la Gobernación se encuentran en proceso de avance. **Caso contrario pasa con los cuartos eléctricos del edificio licorera, ya que no cuentan con algún tipo de avance plan o recomendación propuesta**.

Recomendaciones: Realizar plan de acción o propuesta para el cuarto eléctrico que se encuentra en el piso sótano del edificio licorera, debido a que se encuentra en un espacio abierto (imagen 2) y para el cielo raso del centro de cómputo

.

Para finalizar todo lo referente al estado y clase de extintores, señalización y mapas de evacuación, se pudo evidenciar que si se encuentran cerca de los cuartos eléctricos de la Gobernación de Caldas.



RESPUESTA UNIDAD DE SISTEMAS

Factor 3.

Actualmente, la Unidad de Sistemas, con el acompañamiento de la Secretaría General, está realizando la evacuación de material ajeno al cuarto, como son papelería y cajas de cartón (Fecha de finalización: Diciembre de 2023).

Factor 4.

Actualmente, la Unidad de Sistemas, en el desarrollo del contrato con la firma Data&Service, se está realizando las adecuaciones pertinentes, para garantizar la organización y seguridad del cuarto ubicado en el subterráneo del edificio de La Licorera (Fecha de finalización: Diciembre de 2023).

RESPUESTA CONTROL INTERNO

Es válida la aclaración dada en los puntos anteriores, sin embargo la Oficina de Control Interno considera que estas acciones ya adelantas sean incluidas dentro del plan de mejoramiento, anexando de igual manera el mantenimiento del cielo raso del centro de cómputo (imagen 3).

3.2.2PLANES, POLÍTICAS, Y PROCEDIMIENTOS SIN ESTADO DE AVANCE O ACTUALIZACIÓN.

Criterio: Políticas, planes, procesos y procedimientos.

Observación: Dentro de la revisión de planes, políticas y procedimientos que se debían implementar o actualizar de acuerdo con las recomendaciones de IFD EVIDENCE, se evidenció que algunos no se habían iniciado o actualizado.

- **Revisión documental**

  A continuación, se podrá observar las actividades propuestas por IFD EVIDENCE a la unidad de sistemas en cumplimiento del diagnóstico SGSI realizado por la misma en el mes de febrero. Así mismo se consigna el estado actual evidenciado por parte de la oficina de control interno y las observaciones en tal sentido.

Ítem	Actividad	Act implementada (si/no)	% de avance	Observaciones (unidad de sistemas)	Observaciones (Control interno)	ESTADO
1	Diagnóstico Comité de ciberseguridad de la información.	No	0%	Se tiene un comité de seguridad, pero no tiene el alcance de un comité de diagnóstico de ciberseguridad. No se cuenta con recursos económicos ni personal especializado para realizar la actividad	Definir la prioridad de crear el Comité de ciberseguridad, dejar planteado el analisis de la necesidad de dicho comité para la siguiente administración	PENDIENTE
2	Actualización de los activos de información	No	0%		La última actualización realizada según el documento soporte, fue para marzo 2022. El documento se encuentra en proceso de actualización.	PENDIENTE
3	Actualización del manual de políticas de seguridad basada en el MSPI	No	0%	La Política General de seguridad de la información. Reposa unidad drive unidad sistemas. Manual políticas de seguridad y privacidad de la información. https://site.caldas.gov.co/10-modelo-integrado-de-planeación-y-gestión/254-2019/909-politica-seguridad-de-la-informacion-gobernacion-v3-	Última actualización realizada, 14-11-2018 versión 3. Evidenciando que no se ha realizado la actualización según las recomendaciones de IFD EVIDENCE	PENDIENTE
4	Socialización y divulgación del manual de MSPI.	No	0%	La Política General de seguridad de la información. Reposa unidad drive unidad sistemas. Manual políticas de seguridad y privacidad de la información. https://site.caldas.gov.co/10-modelo-integrado-de-planeación-y-gestión/254-2019/909-politica-seguridad-de-la-informacion-gobernacion-v3-2	No se encuentran soportes o evidencias de socialización o divulgación del manual de MSPI	PENDIENTE
5	Diseño del plan de inteligencia de amenazas	No	0%	Este plan se debe diseñar, se debe considerar el personal especializado para realizar la actividad	No se entregaron soportes de avance	PENDIENTE

6	Diseño del plan de recuperación de desastres	SI	30%	El plan esta en proceso de revisión ajuste.	Se Pueden evidenciar elementos del plan de recuperación dentro del plan de continuidad del negocio de TI (documento soporte facilitado por la unidad de sistemas). DE acuerdo al plan de continuidad los elementos inmerso se encuentran en los apartados 5.1.2. ; 5.1.3.1. ; 5.1.3.2.;5.1.3.3. ; 5.1.3.4 .;	CUMPLIDO
7	Plan anual de concientización de Ciberseguridad	SI	35%	En articulación con el enlace de prensa designado para la secretaria de planeación se está realizando una campaña de concientización con los funcionarios que se inició con el lanzamiento de los videos: - Instructivo Apertura de casos en almera. - importancia del OneDrive para el Backup de la información. Cargados en el canal de @comunicacionesPrensa	se evidencias las acciones señaladas(https://www.youtube.com/watch?v=7AejpG7kvMY - https://www.youtube.com/watch?v=Zeno0Ju9dCM), pero es necesario plantear el plan donde se estipule: acciones, fechas, metas, responsables, periodicidad entre otros. No se entregaron soporte	PENDIENTE
8	Seguimiento a los compromisos adquiridos por las unidades de trabajo relacionados con la seguridad de la información.	SI	30%	Dentro del seguimiento realizado a los compromisos esta la circular 056 emitida por la unidad de sistemas donde se socializan los requisitos para el el uso de portátiles por parte de contratistas;	Documento soporte compartido por la unidad de sistemas, el cual indica los controles al acceso de red. No se evidencia algún tipo de seguimiento a dichos controles)	PENDIENTE
9	Plan de sensibilización de seguridad de la información, vigencia 2023-2025	NO	0%	Este plan se debe diseñar, se debe considerar el personal especializado para realizar la actividad	Sin soportes	PENDIENTE

10	Valoración de riesgos asociados a los activos de información y servicios misionales de la gobernación de Caldas				Se encuentra la evaluación de riesgo de la unidad de sistemas, pero no es posible identificar la fecha yversión en que fue realizado o actualizado. El documento se encuentra en proceso de actualización.	PENDIENTE
11	Plan de tratamiento de riesgos				Se encuentra publicado en la pagina de la gobernación con fecha de 23 enero de 2023 (Se identifican incumplimientos de algunas acciones planeadas)	CUMPLIDO
12	Herramientas para el cifrado de la información crítica misional de la	No	0%	No se cuenta con una herramienta para cifrar la información.	No se evidencian herramientas	PENDIENTE
13	Cláusulas de seguridad en los contratos	SI	100%	En los contratos de prestación de servicio, mínima cuantía, se incluye la obligación especifica de seguridad de la información.	dentro de los soportes suministrados, se refleja una clausula de contrato donde se especificaba las obligaciones con respecto a la seguridad de la información	CUMPLIDO
14	Evidencias de la verificación realizada al acceso a los sistemas mediante logs de auditoria	SI	100%	Se cuenta con un contrato de Noc + Soc que realiza monitoreo a 18 servicios, se realizan reportes de manera semanal además de reportes de ataques bloqueados por la infraestructura Fortinet.	Se hizo validación del contrato y las evidencias de su ejecución	CUMPLIDO
15	Acuerdos de confidencialidad con los empleados, proveedores y terceros	SI	80%	El procedimiento se encuentra en la oficina de calidad para su codificación correspondiente, actualmente se utiliza, pero no para todos los contratos.	En el documento adjunto se puede observar los acuerdos de confidencialidad con los proveedores, terceros y empleados	CUMPLIDO

16	Controles implementados para el acceso a los centros de datos.	SI	100%	Todos los centros de datos cuentan con control de acceso biométrico, actualizado en el mes de Agosto del 2023	En la visita técnica a las instalaciones se logró identificar los controles de acceso biométrico en todos los cuartos eléctricos	CUMPLIDO
17	Políticas y procedimientos para el mantenimiento y cuidado de los centros de cableado y el centro de datos principal	SI	100%	El procedimiento y los formatos se encuentran en la unidad de calidad para realizar la asignación del código correspondiente en la plataforma Almera	Se evidencian los procedimientos en los documentos compartidos por la unidad.	CUMPLIDO
18	Procesos y procedimientos para dar cumplimiento a cada una de las políticas de seguridad diseñadas.	SI	100%	Se cuenta con los procesos y procedimientos que dan cumplimiento a cada una de las políticas planteadas desde la unidad de sistemas.	Se presentan cada uno de los procedimientos a las actividades realizadas en la unidad de sistemas	CUMPLIDO
19	Actualización plan de mantenimiento preventivo y parchado de los sistemas informáticos, servidores, aplicaciones y software en general	SI	100%	Se realizan las actualizaciones, parchado y mantenimiento de los servicios incluidos en el catalogo de servicios de la unidad; cuando se liberan por parte del fabricante actualizaciones se realiza la instalación correspondiente.	se observa el plan de mantenimiento preventivo(Enero 17 del 2023 – versión 2). No se evidencia el plan de parchado (ya que no se sabe cuando el fabricante habilita actualizaciones para la entidad)	CUMPLIDO
20	Plan de Continuidad del Negocio (BCP), para la Gobernación de Caldas.	NO	0%		No se encuentran soportes de evidencia. Es recomendable dejar establecida la necesidad del plan de continuidad del negocio.	PENDIENTE
21	Plan de recuperación ante desastres (DRP), para el área de TI de la Gobernación de Caldas	SI	30%	El plan está en proceso de revisión ajuste.	El plan de recuperación ante desastres se encuentra dentro de los documentos anexados	CUMPLIDO
22	Planes de pruebas para el DRP y el BCP	NO	0%	Este plan se debe diseñar, se debe considerar el personal especializado para realizar la actividad	No se encuentran evidencias	PENDIENTE
23	Simulacros realizados del DRP y el BCP.	NO	0%	Este plan se debe diseñar, se debe considerar el personal especializado para realizar la actividad	No se encuentran evidencias	PENDIENTE

RESPUESTA DE LA UNIDAD DE SISTEMAS

Sobre implementación del Modelo de Seguridad y Privacidad de la Información, es importante aclarar, que el Comité de Seguridad de la Información, en las reuniones realizadas para el análisis del respectivo informe, se redactó la siguiente conclusión:

Acta No. 1, del 29 de marzo de 2023: "El Comité analizó y acepta las observaciones registradas en el informe presentado por la firma EVIDENCE y acogerá las recomendaciones sobre las actividades que le corresponden a la Jefatura de Gestión de la Información, la Unidad de Sistemas y el grupo de informática de la Secretaría de Educación, sin embargo consideramos como comité que el proceso adelantado por parte de la firma EVIDENCE en el año 2022 en la Gobernación de Caldas y de acuerdo al tiempo estimado para la implementación del proceso de acuerdo a lo estipulado en el contrato,no contempla el contenido completo de la implementación del modelo de seguridad y privacidad de la información de acuerdo a las directrices del MinTIC, el contrato no contempló el ciclo de seguridad de la información que está compuesto por 5 fases, solo desarrolló la fase de Diagnóstico".

Acta No.2 del 14 de abril de 2023: "Se hace una lectura general de la primer acta, y se aclara que el Comité de seguridad acepta las observaciones registradas en el informe presentado por la firma EVIDENCE, y acatará las recomendaciones que le corresponden a la Jefatura de Gestión de la Información, unidad de sistemas y Secretaría de Educación, aclarando que no se conocen las obligaciones contractuales de la firma en mención, pero será un insumo para elaborar un plan de acción que permite incrementar el nivel de madurez en la implementación del Modelo de Seguriad y Privacidad de la información".

De igual forma, la firma EVIDENCE en su informe, contextualiza lo siguiente: "Con base en el Análisis Indicado, se propone el siguiente mapa de ruta del plan de seguridad y privacidad de la información para 2023, 2025 a fin de ir adoptando progresivamente las recomendaciones:

Teniendo en cuenta esto, se Definió un Plan de Acción Correctivo, el cual se enfocó enestructurar el Cronograma de Trabajo mediante el cual, se logrará para el año 2023,contar con el MSPI y su Incorporación"

Por lo anterior, se tendrá en cuenta las observaciones realizadas por la firma EVIDENCE, para elaborar un plan de acción,con actividades alcanzables desde la Jefatura de Gestión de la Información y la Unidad de Sistemas, que permitan incrementar el nivel de madurez en la implementación del Modelo de Seguridad y

Privacidad de la Información de la entidad, en el cronograma propuesto por ellos y las observaciones realizadas por la oficina de Control Interno:

Item	Actividad	Acción Propuesta	Responsable	Fecha de Implementación
1	Diseño y diagnóstico del MSPI y crear el comité de ciberseguridad de la información	Se cuenta con la herramienta de diagnóstico para evaluar el nivel de madurez en la implementación del MSPI	Unidad de Sistemas	Actualizada
		La entidad cuenta con el Comité de Seguridad de la Información, el cual tiene funciones similares a las de un Comité de Ciberseguridad. Decreto 0381 de 2018. En proceso de actualización.	Unidad de Sistemas	Implementado
2	Actualización de los activos de información.	Se cuenta con la identificación de los activos de información.	Unidad de Sistemas	Implementado
		Clasificación y etiquetado de los activos de información	Gestión Documental	Sin Definir
3	Elaboración del manual de políticas de Seguridad basado en el MSPI.	Se cuenta con la actualización del manual de políticas de seguridad y privacidad de la información	Unidad de Sistemas	Acta de aprobación del 20 de septiembre de 2023
4	Socialización y divulgación del manual de MSPI.	Las políticas contenidas en el manual se han socializado	Unidad de Sistemas	Circular 56 de 2022 Circular
5	Definición de la estrategia de seguridad de la información para la Gobernación de Caldas	La entidad cuenta con el Decreto de adopción del SGSI, el manual de políticas de seguridad y privacidad de la información y el Plan Estratégico de Tecnologías de la Información con vigencia 2020-2023	Unidad de Sistemas	Implementado
6	Diseño del plan de inteligencia de amenazas	Se cuenta con un plan para ejecutar con la firma Data&Service, para ejecutar en la presente vigencia	Unidad de Sistemas	Inicia el mes de octubre de 2023
7	Diseño del plan de recuperación de desastres	Se cuenta con un borrador del plan, en estado de revisión	Jefatura Gestión de la Información Unidad de Sistemas	Diciembre 20 de 2023
8	Diseño del plan anual de concientización de ciberseguridad	Documentar el plan de concientización de ciberseguridad	Unidad de Sistemas	Octubre de 2023
		Política de Retiro de equipos de la entidad Política ante posibles hurtos Acceso a seguridad	Secretaría General	

10	Implementación del plan de sensibilización de seguridad de la información, vigencia 2023- 2025	Para la presenta vigencia se cuenta con el plan de capacitación institucional, con temas en seguridad digital	Unidad de Capacitación y Bienestar Unidad de Sistemas	Implementado
11	Identificación de los riesgos asociados a los activos de información y servicios misionales de la Gobernación de Caldas	Se cuenta con la identificación y valoración de los riesgos de seguridad de la información que pueden ser controlados por la unidad de sistemas	Unidad de Sistemas	Implementado
12	Formular el plan de tratamiento de riegos	Se cuenta con el plan de tratamiento de riesgos	Unidad de Sistemas	Implementado
13	Gestionar herramientas para el cifrado de la Información crítica misional de la entidad.	Definida la política de cifrado de información	Unidad de Sistemas	Aprobada
		Se cuenta con el cifrado del correo electrónico con el certificado SSL	Unidad de Sistemas	Implementado
		Se cuenta con cifrado para la conexión VPN	Unidad de Sistemas	Implementado
		Token en la Secretaría de Hacienda para los servicios de tesorería	Secretaría de Hacienda	Implementado
14	Identificar las cláusulas de seguridad en los contratos	En las obligaciones de los contratos de prestación de servicios y mínima cuantía, se especifican las acciones en relación con la seguridad de la información.	Unidad de Contratación Unidad de sistemas	Implementado
15	Verificar el acceso a los sistemas mediante los logs de auditoría	Se cuenta con un contrato con la firma DATA&SERVICE para llevar a cabo el servicio NOC + SOC, para el monitoreo de los servicios de red	Unidad de Sistemas Proveedor DATA & SERVICE	Implementado
16	Generar y/o actualizar los acuerdos de confidencialidad con los empleados, Proveedores y terceros.	Se cuenta con acuerdos de confidencialidad, para algunos contratos con proveedores	Unidad de Sistemas	Implementado
		El formato de acuerdos de confidencialidad de información está en proceso de validación por la unidad de Calidad	Unidad de Calidad	En proceso
17	Implementar los controles adecuados para el acceso a los centros de datos.	Centros de datos tiene implementado el acceso con biométrico	Unidad de Sistemas	Implementado
18	Generar políticas y procedimientos para el Mantenimiento y cuidado de los centros de cableado y el centro de datos principal.	Se cuenta con la política de seguridad física y del entorno	Unidad de Sistemas	Aprobada
		El procedimiento seguridad y privacidad de la información, cuenta con el manual operativo de acceso seguro, se encuentra en la unidad de	Unidad de Sistemas Unidad de Calidad	En proceso

		calidad, para la asignación del código y validación		
19	Generar los procesos y procedimientos para dar cumplimiento a cada una de las políticas de seguridad diseñadas.	Se creó el procedimiento seguridad y privacidad de la información, para el cual se elaboraron los manuales respectivos para los diferentes servicios, los cuales se encuentran en la unidad de calidad para la inclusión en el sistema de gestión de calidad y la codificación respectiva	Unidad de Sistemas Unidad de Calidad	En proceso
20	Generar planes de mantenimiento preventivo y parchado de los sistemas informáticos, servidores, aplicaciones y software en general.	Se cuenta con el plan de mantenimiento preventivo y correctivo de los equipos de cómputo de la entidad para la vigencia	Unidad de sistemas	Implementado
		Para los sistemas de información y aplicaciones, se cuenta con contratos de renovación de licencias	Unidad de sistemas	Implementado
		Para el parchado de sistemas de información, se realizan cuando el proveedor pone a disposición una actualización	Unidad de Sistemas	Implementado
21	Diseñar el Plan de Continuidad del Negocio (BCP), para la Gobernación de Caldas.	No se cuenta con talento humano especializado y recursos económicos	Alta dirección	
22	Diseñar el Plan de recuperación ante desastres (DRP), para el área de TI de la Gobernación de Caldas	Se cuenta con un documento borrador, en proceso de revisión y aprobación	Unidad de Sistemas	Noviembre de 2023
23	Generar los planes de pruebas para el DRP el BCP	No se cuenta con talento humano especializado y recursos económicos	Alta dirección	
24	Realizar simulacros del DRP y el BCP.	No se cuenta con talento humano especializado y recursos económicos	Alta dirección	
25	Generar la declaración de aplicabilidad para el MSPI.	Se cuenta con un borrador en proceso de validación	Unidad de Sistemas	Noviembre de 2023

RESPUESTA CONTROL INTERNO

De acuerdo con la información emitida por parte de la Unidad de Sistemas, se dan como cumplidas las actividades 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13. Debido a que se presentaron sus respectivas evidencias, con relación a la actividad 8 (Plan anual de concientización de ciberseguridad) se deberá hacer la suscripción del plan de

mejoramiento y las actividades 21, 23 y 24, se recomienda realizar propuestas o alternativas de solución para que la alta dirección las pueda considerar.

3.2.3 PLAGIO EN MANUAL DE PROCESOS Y PROCEDIMIENTOS

Criterio: Ley 23 de 1982 artículo 31

Observaciones: Al momento de hacer la revisión del manual de procesos y procedimientos de la unidad de sistemas, se pudo evidenciar que hubo transcripciones de imágenes y texto de otro manual ya creado sin referencia alguna, dando lugar a posible plagio; ya que según la Ley 23 de 1982 en su artículo 31, establece lo siguiente:

"Es permitido citar a un autor transcribiendo los pasajes necesarios, siempre que éstos no sean tantos y seguidos que razonablemente puedan considerarse como una reproducción simulada y sustancial, que redunde en perjuicio del autor de la obra de donde se toman. En cada cita deberá mencionarse el nombre del autor de la obra citada y el título de dicha obra. Cuando la inclusión de obras ajenas constituya la parte principal de la nueva obra, a petición de parte interesada, los tribunales fijarán equitativamente y en juicio verbal, la cantidad proporcional que corresponda a cada uno de los titulares de las obras incluidas […]".

En la siguiente imagen en el documento denominado manual de procesos y procedimientos de la Unidad de Sistemas se pudo observar que frente al documento de manual de procedimientos y procesos de la Cámara de Representantes versión 3, con fecha de 30 de abril del 2018, hay similitudes desde la página 27 hasta la 33, sin tener en cuenta si los conceptos se adaptan de manera integral a la Gobernación de Caldas, prueba de ello, se presenta en el mapa de procesos, puesto que en el de la Gobernación de Caldas cuenta con macro procesos, procesos y procedimientos mas no con subprocesos como si se observa en el mapa de procesos de la Cámara de Representantes.

MANUAL DE PROCEDIMIENTOS Y PROCESOS CAMARA DE REPRESENTANTES	MANUAL DE PROCESOS Y PROCEDIMIENTOS DE LA UNIDAD DE SISTEMAS (GOBERNACION DE CALDAS)
Conviene repasar los principales conceptos partiendo de la definición de proceso, los niveles de operación o descomposición en niveles, el operar por procesos, la articulación basada en las funciones de las dependencias y la operación basada en los proyectos de la Entidad, la caracterización, los tipos de procesos, el ciclo PHVA, la cadena de valor, el mapa de procesos, la identificación de los procesos y sus interacciones, la forma cómo se agrupan y desdoblan (macro procesos, procesos, subprocesos, procedimientos), lo cual depende de la complejidad de cada organización. "El hecho de identificar, entender, mantener, mejorar y, en general, gestionar los procesos y sus interrelaciones como un sistema contribuye a la eficacia, eficiencia y efectividad de las entidades en el logro de sus objetivos" NTCGP 1000:2009.	Conviene repasar los principales conceptos partiendo de la definición de proceso, los niveles de operación o descomposición en niveles, el operar por procesos, la articulación basada en las funciones de las dependencias y la operación basada en los proyectos de la Entidad, la caracterización, los tipos de procesos, el ciclo PHVA, la cadena de valor, el mapa de procesos, la identificación de los procesos y sus interacciones, la forma cómo se agrupan y desdoblan (macro procesos, procesos, subprocesos, procedimientos), lo cual depende de la complejidad de cada organización. "El hecho de identificar, entender, mantener, mejorar y, en general, gestionar los procesos y sus interrelaciones como un sistema contribuye a la eficacia, eficiencia y efectividad de las entidades en el logro de sus objetivos" NTCGP 1000:2009.
	
	

RESPUESTA DE LA UNIDAD DE SISTEMAS

Se acepta la observación, y será ajustado el documento, incluyendo en la imagen, la fuente de la misma

RESPUESTA CONTROL INTERNO

Se deberá anexar la acción correspondiente en el plan de mejoramiento.

3.2.4 INCUMPLIMIENTO DE ACTIVIDADES DEL PLAN DE TRATAMIENTO DE RIESGOS

Criterio: Procedimientos

Observaciones: Dentro del plan de tratamiento de riesgos se puede evidenciar que las actividades presentes no fueron ejecutadas para sus respectivas fechas, ya que no se encontraban los soportes al momento de solicitarlos.

La presente imagen corresponde al plan de tratamiento de riesgos de la seguridad y privacidad de la información de la Gobernación de Caldas, actualizado el 23 de enero de 2023, versión 2, el cual se encuentra publicado en la página oficial de la Gobernación de Caldas.

- **Plan de tratamiento de riesgos**

Item	Actividad	Tarea	Responsable	Fecha de Inicio	Fecha Fin
1	Identificación de los Activos de información	Actualizar los activos de información	Gestión Documental Unidad de Sistemas	1-feb-23	28-abr-23
2	Adopción de Lineamientos inherentes a la gestión del riesgo	Crear y/o actualizar la política, metodología y procedimiento de gestión del riesgo	Jefatura Gestión de la Información Unidad de Sistemas	1-feb-23	28-abr-23
3	Identificación y valoración de los Riesgos de Seguridad y Privacidad de la Información	Identificación y valoración de nuevos riesgos de seguridad de la información	Jefatura Gestión de la Información Unidad de Sistemas	1-mar-23	28-abr-23
		Actualizar los riesgos de seguridad de la información ya registrados	Jefatura Gestión de la Información Unidad de Sistemas	1-mar-23	28-abr-23

RESPUESTA UNIDAD DE SISTEMAS

Item	Actividad	Tarea	Responsable	Fecha de Inicio	Fecha Fin	Fecha Real de Implementación	Fecha Implementación
1	Identificación de los Activos de información	Actualizar los activos de información	Unidad de Sistemas	1-feb-23	28-abr-23	30-sep-23	
		Clasificación y etiquetado	Gestión Documental	Sin definir			
2	Adopción de Lineamientos inherentes a la gestión del riesgo	Crear y/o actualizar la política, metodología y procedimiento de gestión del riesgo	Jefatura Gestión de la Información Unidad de Sistemas	1-feb-23	28-abr-23		dic-23
3	Identificación y valoración de los Riesgos de Seguridad y Privacidad de la Información	Identificación y valoración de nuevos riesgos de seguridad de la información	Jefatura Gestión de la Información Unidad de Sistemas	1-mar-23	28-abr-23	30-jun-23	
		Actualizar los riesgos de seguridad de la información ya registrados	Jefatura Gestión de la Información Unidad de Sistemas	1-mar-23	28-abr-23	30-jun-23	

RESPUESTA CONTROL INTERNO

Se acepta la evidencia enviada, puesto que el cuadro adjunto permite visualizar la fecha de implementación de las actividades, garantizando mayor claridad de la ejecución de las mismas.

4. SUSCRIPCIÓN DEL PLAN DE MEJORAMIENTO

Si se ejerce el derecho de contradicción en el plazo estipulado en el numeral anterior por parte del auditado**,** la oficina de Control Interno se pronunciará sobre el mismo y correrá traslado del informe final de la auditoría interna con el fin de que se suscriba el plan de mejoramiento respectivo, el mismo, contará con un término cinco (5) días hábiles para su presentación ante esta oficina, el cual empezará a contar a partir del día siguiente de la entrega del documento en mención.

4.1 SEGUIMIENTO AL CUMPLIMIENTO DEL PLAN DE MEJORAMIENTO

Es un deber de la Secretaría auditada, llevar a cabo el seguimiento periódico de las acciones propuestas en el plan de mejoramiento, conforme las fechas de culminación establecidas para cada una de las acciones con las cuales se pretende corregir la situación evidenciada.

A la oficina de Control Interno deberá remitirse a solicitud de la misma en las fechas que para el efecto se establezcan, el avance de las acciones suscritas en el plan de mejoramiento con los soportes que permitan evidenciar el cumplimiento de dichas acciones.

Manizales, 27 de septiembre de 2023.

JULIETA TORO GÓMEZ
Jefe Oficina de Control Interno

CARLOS ALBERTO OSORIO
Practicante
Jefatura Control Interno