AREA O PROCESO EVALUADO	FECHA	AUDITOR LÍDER
ACCESIBILIDAD WEB Y MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Octubre de 2022	Jaime Acosta Zamudio Jefe Oficina Asesora Control Interno **Equipo Auditor:** Diego Escobar Profesional Apoyo
PERSONA(S) AUDITADA(S)	**CARGO**	**DEPENDENCIA**
Adriana Vargas Salazar	Subdirector Administrativo y Financiero	Subdirección Administrativa y Financiera

1. OBJETIVOS

OBJETIVO GENERAL:

Evaluar la gestión del modelo de seguridad y privacidad de la información, y el estado de accesibilidad de la página web del Instituto Municipal de Cultura y Turismo de Bucaramanga, mediante la calificación de los criterios señalados en norma NTC 5854 de 2011 y las herramientas de evaluación y diagnóstico MinTic, identificando su nivel de implementación y aspectos por mejorar del proceso.

Objetivos Específicos:

1. Evaluar el cumplimiento de los requisitos de accesibilidad en la página web del imct en los niveles de conformidad A, AA y AAA, mediante el análisis de la implementación de los criterios señalados en la NTC 5854 de 2011, verificando la observancia en las disposiciones legales contenidas en la estrategia de gobierno digital.

2. Evaluar el nivel de madurez del modelo de seguridad y privacidad de la información del imct, a través de la aplicación de las herramientas diagnóstico MinTic, con el fin de identificar mejoras en los estándares de Seguridad de la Información de la entidad.

2. ALCANCE

Evaluar la gestión actual del modelo de seguridad y privacidad de la información, y el estado vigente del grado de accesibilidad de la página web del Instituto Municipal de Cultura y Turismo de Bucaramanga, mediante la aplicación de listas de chequeo para la verificación de requisitos técnicos presentes en la norma NTC 5854 de 2011 y las herramientas de evaluación y diagnóstico MinTic, identificando su nivel de implementación y aspectos por mejorar de la estrategia de gobierno digital institucional.

3. CRITERIOS DE AUDITORIA

- Constitución Política de Colombia

- Ley 87 de 1993, Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
- NTC 5854 de 2011. Accesibilidad a páginas web.
- NTC ISO/IEC 27001:2013 Sistemas de Gestión de Seguridad de la Información.
- Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 1083 de 2015. Decreto único reglamentario de función pública.
- Decreto 1499 de 2017, por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1078 de 2015 por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.
- Manual Gobierno Digital MinTic. Versión 06 de 2018.
- Resolución MinTic 1519 de 2020, por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 de 2014 y se definen requisitos de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos.
- Decreto 767 de 2022, por el cual se establecen lineamientos generales de la política de gobierno digital.

4. DOCUMENTOS EXAMINADOS

- Autodiagnóstico Gobierno Digital, disponible en: https://autodiagnosticogobdigital.gov.co/dashboard
- Portal web institucional, disponible en : https://imct.gov.co/
- Seguimiento Anexo 1, Matriz Índice de Transparencia y de Acceso a la Información – ITA, Herramienta para la Vigilancia del Cumplimiento Normativo Ley 1712 - Versión 2021.
- Instrumento Evaluación Modelo de Seguridad y Privacidad de la Información – MSPI
- Calificación Anexo A, Norma Técnica Colombiana - NTC 5854.

5. RESULTADO DE AUDITORÍA

ACCESIBILIDAD WEB

Se observó la expedición de la Resolución MinTic 1519 de 2020, *"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"*, la cual define en al Artículo 3: *"Directrices de accesibilidad web. A partir del 1 de enero del 2022, los sujetos obligados deberán dar cumplimiento a los estándares AA de la Guía de Accesibilidad de Contenidos Web (Web Content Accesibillity Guidelines - WCAG) en la versión 2.1, expedida por el World Web Consortium (W3C), conforme con el Anexo 1 de la presente resolución aplicable en todos los procesos de actualización, estructuración, reestructuración, diseño, rediseño de sus portales web y sedes electrónicas, así como de los contenidos existentes en ésas."*, y el Artículo 8 menciona: *"…el artículo 3 se deberá implementar a más tardar el 31 de diciembre del 2021, conforme con los términos referidos en el anexo 1 de esta misma Resolución…"*

En este sentido se revisaron los nueve (9) ítems señalados en el Anexo 1 de la Resolución MinTic 1519 de 2020, de los cuales se requería contar con un enlace o URL donde se pueda visualizar un certificado emitido por el representante legal de la entidad, o de cualquiera de sus funcionarios o empleados responsables del cumplimiento regulatorio

que tenga capacidad para emitirlo, en el que se acredite el cumplimiento de estos criterios en el portal web institucional, sin embargo, no se cumplía con dicho requerimiento. Así mismo tampoco se evidenció cumplimiento respecto a:

El numeral “a” que menciona que los elementos no textuales (p. ej. imágenes, diagramas, mapas, sonidos, vibraciones, etc.) que aparecen en el sitio web deben tener texto alternativo, de la cual se recomienda coordinar con comunicaciones para las publicaciones no textuales y generar lineamientos desde Subdirección Administrativa y Financiera para el manejo de este tema.

El numeral “b”, que menciona que los videos o elementos multimedia deben tener subtítulos y audio descripción (cuando no tiene audio original), como también su respectivo guion en texto, de lo que se recomienda implementar audio descripción y guion en este tipo de material.

El numeral “e”, que menciona que los formularios o casillas de información deben tener advertencias e instrucciones claras con varios canales sensoriales (p. ej. Campos con asterisco obligatorios, colores, ayuda sonora, mayúscula sostenida), de lo que se recomienda generar las instrucciones previas de diligenciamiento en los Formularios de PQRS, Afiliación Biblioteca y demás que se identifiquen.

El numeral “h”, que menciona que el lenguaje de los títulos, páginas, sección, enlaces, mensajes de error, campos de formularios, es en español claro y comprensible (siguiendo la guía de lenguaje claro del DAFP, en el caso de las entidades públicas, disponible en: https://www.portaltributariodecolombia.com/wp-content/uploads/2015/07/portaltributariodecolombia_guia-de-lenguaje-claro-para-servidores-publicos.pdf), de lo que se recomienda complementar las instrucciones iniciales señaladas en el formulario PQRS e implementar multilenguaje (Varios idiomas).

En el numeral “i”, que menciona que los documentos (Word, Excel, PDF, PowerPoint, etc.) deben cumplir con los criterios de accesibilidad establecidos en el Anexo 1 de la Resolución 1519 de 2020 para ser consultados fácilmente por cualquier persona, de lo que se sugiere verificar la Resolución 1519 de 2020 MinTIC, Anexo 1, capítulo 3, accesibilidad en documentos digitales para publicación, e implementar dichas disposiciones.

Hallazgo 1:

Teniendo en cuenta lo anterior, se configura como hallazgo la inobservancia del cumplimiento del artículo 3 y 8 de la Resolución MinTic 1519 de 2020.

De forma complementaria, se evaluó el cumplimiento de los requisitos de accesibilidad en la página web del imct en los niveles de conformidad A, AA y AAA, mediante la implementación de los criterios señalados en la NTC 5854 de 2011, por lo que se analizó el diagnóstico proporcionado por el responsable del portal web, y se observó el siguiente resultado:

Criterios	Cumple	No Cumple	Total
A	30	7	37
AA	10	4	14
AAA	10	12	22
Total	**50**	**23**	**73**

Es importante señalar que la NTC 5854 de 2011, tomó como documento de referencia las pautas de accesibilidad para el contenido web (WCAG) 2.0 recomendación del W3C del

11 de diciembre de 2008 disponibles en: http://www.w3.org/TR/2008/REC-WCAG20-20081211/.

Hallazgo 2:

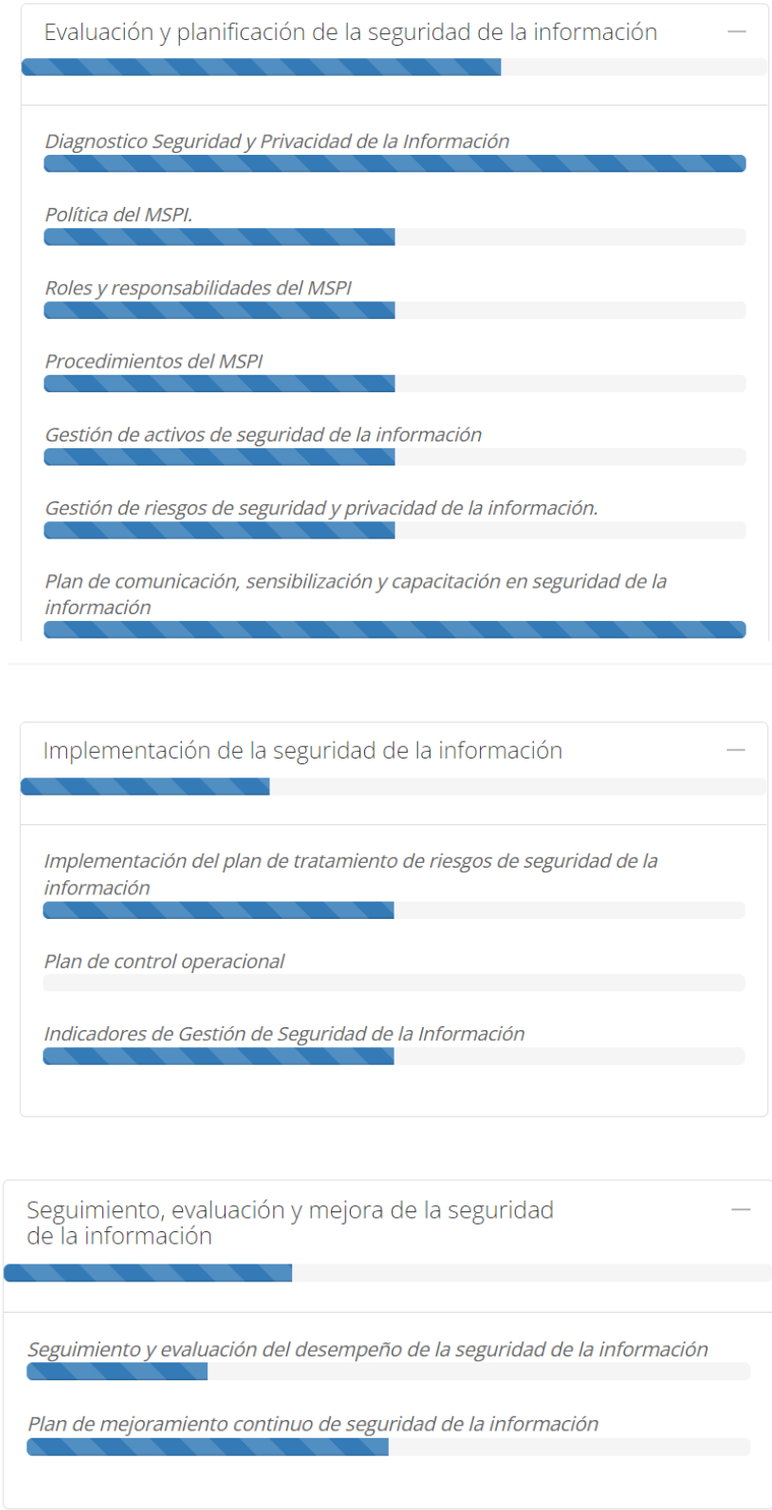
Como se observa en la anterior tabla, el imct no cumple con la totalidad de requisitos mínimos para siquiera alcanzar el nivel de conformidad A en su página web institucional, atendiendo la NTC 5854 de 2011.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La estrategia de Gobierno digital, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, eficiente y transparente.

Partiendo de la base de la implementación de la política de gobierno digital en el imct, se utilizó la herramienta de autodiagnóstico disponible en el portal https://autodiagnosticogobdigital.gov.co/dashboard, donde el responsable del proceso generó calificación del avance en la misma, en consecuencia, es importante resaltar los resultados de los indicadores de cumplimiento respecto a la seguridad de la información, los cuales se presentan a continuación:

Indicadores de cumplimiento:



La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

En este sentido, de forma paralela, se evaluó el nivel de madurez del modelo de seguridad y privacidad de la información del imct, a través de la aplicación del

Instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información – MSPI – proporcionado por el Ministerio de las Tecnologías de la Información y Comunicación, con el fin de identificar mejoras en los estándares de Seguridad de la Información de la entidad.

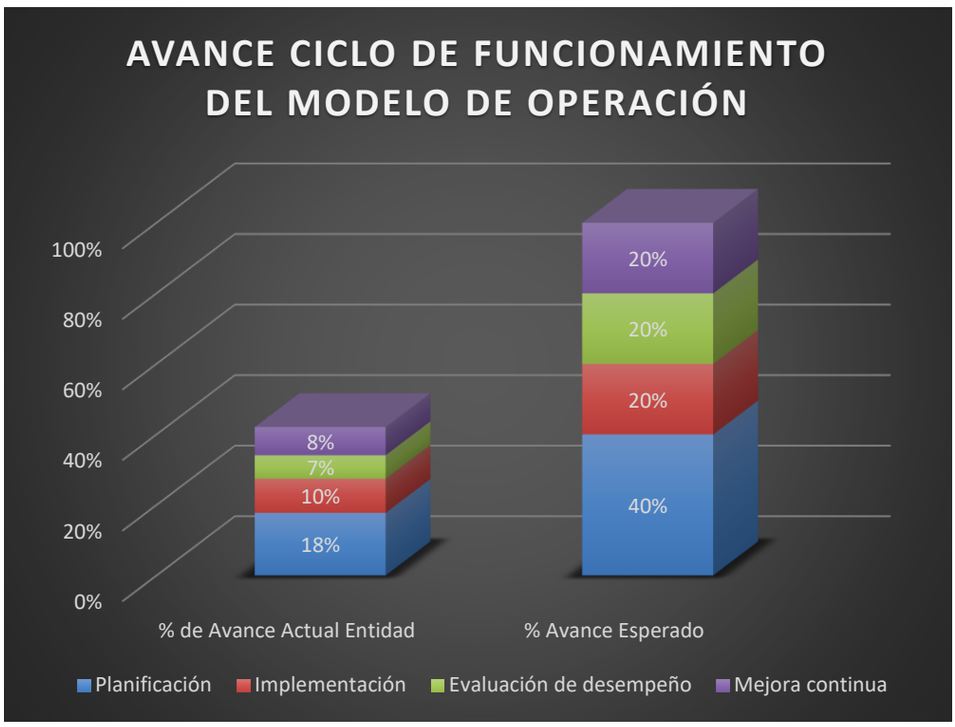
Respecto a la evaluación de la efectividad de los controles se evidenció la siguiente calificación, teniendo en cuenta la tabla de escala de valoración de controles.

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

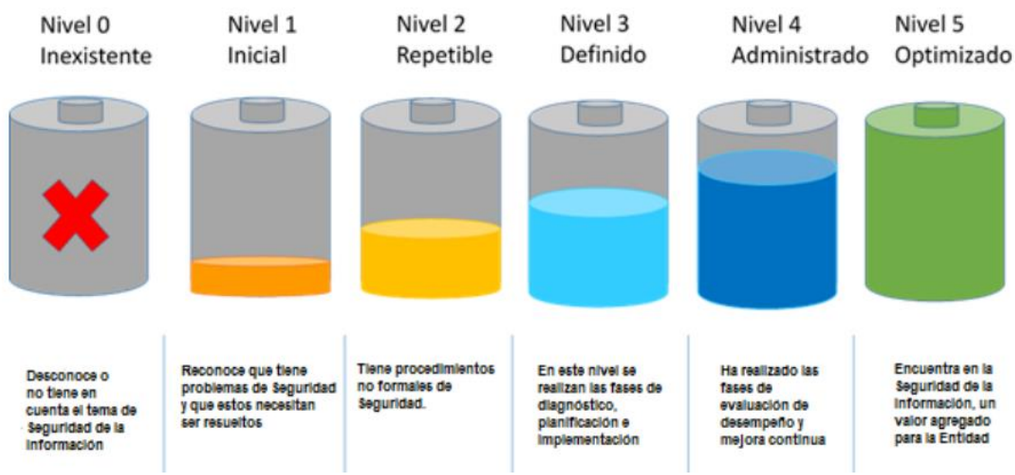
No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	100	**REPETIBLE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	44	100	**EFECTIVO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	48	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	59	100	**EFECTIVO**
A.9	CONTROL DE ACCESO	31	100	**REPETIBLE**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	31	100	**REPETIBLE**
A.12	SEGURIDAD DE LAS OPERACIONES	31	100	**REPETIBLE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	38	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	10	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	30	100	**REPETIBLE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	29	100	**REPETIBLE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	**REPETIBLE**
A.18	CUMPLIMIENTO	45	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**33**	**100**	**REPETIBLE**

Respecto del avance del ciclo de funcionamiento del modelo de operación (PHVA) se observaron los siguientes resultados:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	18%	40%
	Implementación	10%	20%
	Evaluación de desempeño	7%	20%
	Mejora continua	8%	20%
TOTAL		42%	100%



En el Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.



Respecto del nivel de madurez de modelo de seguridad y privacidad de la información se observó el siguiente resultado, teniendo en cuenta las siguientes escalas de calificación:

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Hallazgo 3:

Teniendo en cuenta los anteriores resultados, se configura como hallazgo el bajo nivel de madurez en la implementación del ciclo de operación del modelo de seguridad y privacidad de la información en el imct, lo que le imposibilita a la entidad gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Se observó vigente el proceso de “Gestión Tecnológica” en el mapa de procesos institucional, como proceso de apoyo del imct, el cual menciona dentro de sus actividades: “Administrar, configurar y mantener el acceso y la información de las plataformas web del imct”; “Establecer e implementar controles y/o acciones que minimicen los riesgos de seguridad de la información, según políticas definidas”; estas acciones definen como proveedores a todos los procesos del imct, y la caracterización del proceso define como responsable a profesional de apoyo, con la participación de contratistas de apoyo, sin embargo no se señala a ninguna de las áreas, dependencias u oficinas de la entidad definidas en el organigrama y/o manual de funciones, como responsables de liderar, coordinar u operar en la consecución y desarrollo de las mismas.

Hallazgo 4:

En este sentido se configura como hallazgo la falta de documentación, aunado a falencias en la designación de responsabilidades de coordinación y de operación en el proceso de gestión tecnológica del imct.

Considerando los anteriores hallazgos, se recomienda presentar un plan de mejoramiento con las acciones que estén encaminadas a dar solución a las falencias expuestas.

Como resultado de la presente auditoría, el proceso responsable deberá elaborar un Plan de Mejoramiento, con acciones y metas de tipo correctivo y/o preventivo, dirigidas a subsanar las causas administrativas que dieron origen a los hallazgos identificados por la Oficina Asesora de Control Interno como resultado del ejercicio de evaluación independiente que se describe en este informe.

FIRMA AUDITORES	**FIRMA AUDITADO**