MINISTERIO DE VIVIENDA, CIUDAD Y TERRITORIO 29-06-2018 09:29
Al Contestar Cite Este No.: 2018IE0007411 Fol:1 Anex:0 FA:0
ORIGEN 7120-OFICINA DE CONTROL INTERNO / DIANA PATRICIA GONZALEZ OSORIO
DESTINO 7000-DESPACHO DEL MINISTRO / WENDY JOHANNA MORALES ORDOÑEZ
ASUNTO SEGUIMIENTO SGSI
OBS ELABORÓ: LINA MORALES

2018IE0007411

GOBIERNO DE COLOMBIA

MINVIVIENDA

MEMORANDO

Bogotá, D.C.

PARA: **Dr. CAMILO SÁNCHEZ ORTEGA.**
Ministro de Vivienda, Ciudad y Territorio.

DE: **OFICINA CONTROL INTERNO**

ASUNTO: Informe de seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información SGSI, en el marco de la Estrategia de Gobierno en línea para el Ministerio de Vivienda, Ciudad y Territorio.

Cordial saludo,

En cumplimiento de las funciones establecidas en la Ley 87 de 1993, el Artículo 8 del Decreto 3571 de 2011, del Decreto 648 de 2017 y en cumplimiento del Rol de Evaluación y Seguimiento, específicamente del Plan Anual de Auditorías vigencia 2018 aprobado por el Comité Institucional de Coordinación de Control Interno en sesión virtual del pasado 30 de enero de 2018, Acta No. 01, atentamente me permito remitirles para su conocimiento y fines pertinentes, el Informe de Seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información SGSI, en el marco de la Estrategia de Gobierno en línea para el MVCT, el cual agradecemos socializarlo con el respectivo equipo de trabajo, a fin de que se analice su contenido y se tomen las respectivas acciones que a su consideración apliquen para el proceso evaluado.

Finalmente, agradecemos la mejor disposición y colaboración de su equipo de trabajo durante el proceso de evaluación y reiteramos nuestro compromiso en la asesoría y acompañamiento para contribuir al fortalecimiento de las políticas en materia de Seguridad de la Información en el MVCT.

De otra parte, me permito informar que el mismo se encuentra publicado en el link: http://www.minvivienda.gov.co/sobre-el-ministerio/planeacion-gestion-y-control/sistema-de-control-interno/auditorias-internas-independientes

Cordialmente,

OLGA YANETH ARAGÓN SANCHEZ
Jefe Oficina de Control Interno.

Anexos: Informes de seguimiento SGSI
Copia: Gestión de Proyectos de Tecnologías de la Información

Elaboró: Lina Alejandra Morales.
Revisó: Olga Yaneth Aragón.

FECHA DE REALIZACIÓN DEL SEGUIMIENTO: 27/06/2018

PROCESO: GESTION DE PROYECTOS DE TECNOLOGIAS DE LA INFORMACION.

RESPONSABLE DEL PROCESO:
MAURICIO FERNANDEZ CORREA – JEFE OFICINA TIC

TIPO DE SEGUIMIENTO:
Informe de seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información SGSI, en el marco de la Estrategia de Gobierno en línea para el Ministerio de Vivienda, Ciudad y Territorio.

OBJETIVO:
Realizar seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información SGSI, bajo los requisitos de la norma ISO 27001 de 2013.

ALCANCE:
Seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información SGSI, correspondiente al primer y segundo trimestre de la vigencia 2018.

CRITERIOS:

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*". Artículo 12: *Funciones de los auditores internos. Serán funciones del asesor, coordinador, auditor interno o similar las siguientes literal "e. Velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de la organización y recomendar los ajustes necesarios;".*

Decreto 3571 de 2011: *"Por el cual se establecen los objetivos, estructura, funciones del Ministerio de Vivienda, Ciudad y Territorio y se integra el Sector Administrativo de Vivienda, Ciudad y Territorio."* Artículo 8, *Oficina de Control Interno. Son funciones de la Oficina de Control Interno o quien haga sus veces, además de las señaladas en las leyes vigentes sobre la materia, las siguientes*: Numeral 4. "*Verificar el cumplimiento de las políticas, normas, procedimientos, planes, programas, proyectos y metas del Ministerio, así como recomendar los ajustes pertinentes y efectuar seguimiento a su implementación".*

ISO 27001 de 2013, *es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una organización.*

Decreto 648 de 2017 Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, Artículo 2.2.21.5.3 *De las Oficinas de Control Interno*. *Las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control*.

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"* Implementación del Modelo Integrado de Planeación y Gestión.

Resolución 0973 de 2017, *"Por la cual se adopta el Sistema de Gestión de Seguridad de la Información SGSI, la Política y los Objetivos de Seguridad de la Información en el Ministerio de Vivienda, Ciudad y Territorio, en el marco de la estrategia de Gobierno en Línea"*

Decreto 612 de 2018 "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado."

Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones."

INTRODUCCIÓN:

La Oficina de Control Interno –OCI- en cumplimiento de las funciones establecidas en la Ley 87 de 1993, el Artículo 8 del Decreto 3571 de 2011, del Decreto 648 de 2017 y en cumplimiento del Rol de Evaluación y Seguimiento y del Plan Anual de Auditorías vigencia 2018 aprobado por el Comité Institucional de Coordinación de Control Interno en sesión virtual del pasado 30 de enero de 2018, Acta No. 01, efectúa con el fin de realizar el seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información SGSI,

verificación de las evidencias presentadas a la OCI por parte del proceso TIC, de acuerdo a la solicitud de correo electrónico del pasado 13/06/2018.

En el marco de lo expuesto, se elabora el presente informe, teniendo en cuenta los requisitos de la norma ISO 27001 de 2013.

DESARROLLO

ANÁLISIS DE LA INFORMACIÓN:

Seguimiento al cumplimiento frente al estándar NTC ISO 27001:2013 – SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION – REQUISITOS.

La evaluación de los requisitos se calificó en una escala de 1 a 7 donde los niveles de aplicación del control se miden bajo las siguientes convenciones de valoración:

1. No contemplado
2. En proceso de elaboración
3. En Borrador
4. Documentado
5. Control Implementado
6. Control actualizado
7. Control auditado.

Capítulo 4. Contexto Organizacional

Ilustración 1. Análisis de la definición del Contexto Organizacional

Respecto al análisis del contexto organizacional en el cual se abordan 4 elementos en específico como lo son el análisis del contexto, el análisis de los requisitos, el análisis de la aplicabilidad del sistema de gestión y la definición en si del sistema de gestión de seguridad de la información, los documentos relacionados con la política, los procedimientos y estructura de la organización para establecer el plan de implementación, se evidencia los siguiente:

- En la verificación, no se evidenció, la fuente de la elaboración de dicho contexto y su alineación a las estrategias organizacionales, así como la interrelación con las partes interesadas, en el marco del Sistema Integrado del MVCT.
- No se puede evidenciar la documentación normativa, así como la identificación y el análisis de riesgos para la implementación del SGSI.

A continuación, se registra la valoración del capítulo 4:

CAPITULO 4								
ÍTEM	NORMA		CONTEXTO ORGANIZACIONAL					
	CAP.	TITU						
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES	
1	4	4.1.	CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO	La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.	Se cuenta con un borrador del contexto estratégico para el SGSI, el cual a la fecha no se encuentra articulado con el SIG.	3	Se recomienda articular con el contexto del MVCT.	
3		4.2.	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	La organización debe determinar: Las partes interesadas que son pertinentes al sistema de gestión de seguridad de la información	Se cuenta con un borrador de matriz de contexto de la organización, la cual establece unas partes interesadas vs requerimientos de seguridad de la información, sin embargo, la misma no contiene el 100% de dichas partes interesadas toda vez que el mismo no ha sido creado participativamente con los procesos del MVCT.	3	No se cuenta con análisis, ni priorización de las partes interesadas sus requisitos y su interacción con los procesos.	
4				los requisitos de estas partes interesadas pertinentes a seguridad de la información	Se cuenta con un borrador de matriz de contexto de la organización, sin embargo, No ha sido determinados de forma estructurada, no se cuenta con registro.	3	-	

CAPITULO 4								
ÍTEM	NORMA		CONTEXTO ORGANIZACIONAL					
	CAP.	TITU						
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES	
5		4.3.	DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance	Se cuenta con un borrador del contexto estratégico para el SGSI, en el cual establecen un alcance en el apartado No. 7, sin embargo, el mismo no determina el límite y la aplicabilidad.	3	-	
6				Cuando se determina este alcance, la organización debe considerar: las cuestiones externas e internas referidas en el numeral 4.1, y	No se determinan con claridad las partes internas y externas	3	menciona las partes sin embargo no se ha analizado su suficiencia	
7				los requisitos referidos en el numeral 4.2; y	No se determinan con claridad los requisitos de las partes interesadas	3	-	
8				las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones.	No es especifico a los servicios del MVCT.	1	-	
9				El alcance debe estar disponible como información documentada	No se encuentra disponible por no estar aprobado el documento	1	-	

CAPITULO 4								
ÍTEM	NORMA		CONTEXTO ORGANIZACIONAL					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
10		4.4.	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma.	se cuenta con la necesidad de establecer un Sistema de Seguridad de la Información documentado en términos generales, mediante la resolución 0973 del 28 de diciembre de 2017, sin embargo, este no ha sido implementado, toda vez que no se establece la aplicabilidad del sistema de gestión de seguridad de la información.	2	-

Conclusión

No se ha definido el contexto organizacional con base en los criterios normativos, no se evidencia el alcance y el estado actual de la organización, no tiene asociada la identificación y creación del modelo de seguridad a aplicar, no se ha dado claridad a los procesos críticos de la operación de la entidad, la identificación de vulnerabilidades y amenazas aplicando la metodología de riesgos acorde a las necesidades del contexto de la organización, los planes de tratamiento de riesgos y la generación del marco documental, la interrelación con las partes interesadas y sus requisitos; adicionalmente, de acuerdo a la norma, se debe asegurar que estén articulados los sistemas de seguimiento y medición con los requisitos de las partes interesadas.

Capítulo 5. Contexto Organizacional

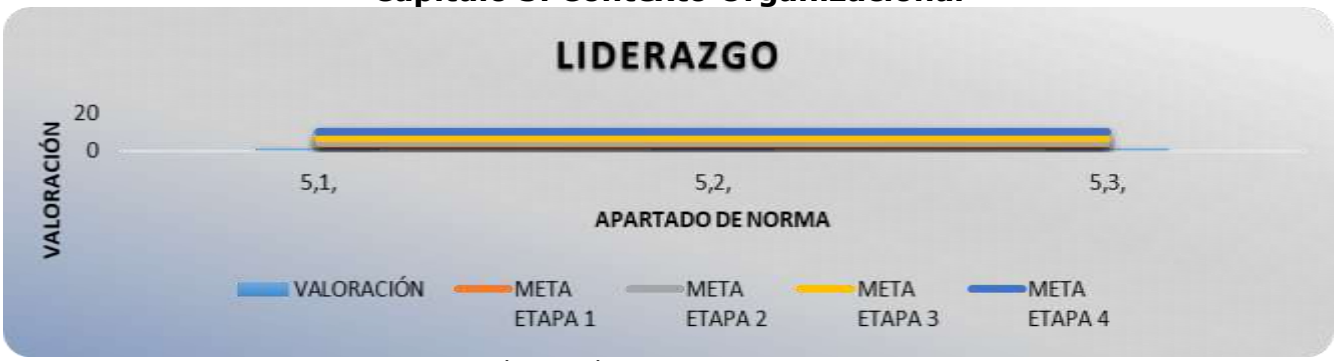


Ilustración 2. Análisis del Ejercicio de Liderazgo

En este capítulo se abordan tres temas específicos como lo son el ejercicio del liderazgo, la definición de políticas adecuadas a la gestión y la definición y empoderamiento de roles funciones y responsabilidades, así como la creación de compromiso.

Una vez establecido el ejercicio del liderazgo frente a la prevención se puede evidenciar que ha sido delegado únicamente en el Jefe de la Oficina de TIC, cuando es requerido que sea replegado y empoderado en todos los niveles de la organización, no se puede definir como ha sido divulgado y alineado a la gestión de las actividades de los servidores públicos de tal forma que se pueda generar sinergia y compromiso como factores claves en la generación de cultura.

Los criterios, funciones y responsabilidades de los servidores públicos, a pesar de que están definidos dentro de los perfiles de cargo, estos no abordan de forma clara las funciones y responsabilidades en materia de seguridad de la información.

Así mismo, no está claramente definido el rol de oficial de seguridad de forma que permee la responsabilidad y los resultados de su gestión.

A continuación, se registra la valoración del capítulo 5:

CAPITULO 5								
ÍTEM	NORMA		LIDERAZGO					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
11	5	5,1,	LIDERAZGO Y COMPROMISO	La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información: asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización	Se evidencia resolución 0973 del 28 de diciembre de 2017, "Por la cual se adopta el Sistema de Gestión de Seguridad de la Información SGSI, la Política y los Objetivos de Seguridad de la Información en el Ministerio de Vivienda, Ciudad y Territorio, en el marco de la estrategia de Gobierno en Línea"	4	-
12				asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización.	-	1	No se han establecido criterios para la articulación con el Sistema Integrado de Gestión
13				asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles	-	1	No se cuenta con presupuesto definido, adicionalmente no se ha asignado el oficial de seguridad de la información
14				comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información	-	1	A pesar de que se ha estructurado el sistema, no se ha realizado divulgación o capacitación.

CAPITULO 5							
ÍTEM	NORMA		LIDERAZGO				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
15				asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos	-	1	No se han generado revisiones al sistema ya que este no ha sido implementado, se han definido algunos controles, pero no han sido incluidos dentro del sistema de gestión
16				dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información	-	1	No se cuenta con la asignación de responsabilidades desde el SGSI
17				promoviendo la mejora continua	-	1	No se han involucrado en temas de revisión y análisis de la mejora.
18				apoyando otros roles pertinentes sus áreas de responsabilidad de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad	-	1	No está claramente definido si se han definido funciones y responsabilidades especificas en el manejo de información, TI o tratamiento de datos.
19		***5,2,***	**POLÍTICA**	La alta dirección debe establecer, una política de la seguridad de la información que: a) sea apropiada al propósito y contexto de la organización y apoye su dirección estratégica;	-	2	La política del SGSI, se encuentra en proceso de elaboración.

CAPITULO 5								
ÍTEM	NORMA		LIDERAZGO					
	CAP.	TITU						
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES	
20				proporcione un marco de referencia para el establecimiento de los objetivos de la seguridad de la información;	-	1	No se cuenta con un despliegue o interrelación definido	
21				incluya un compromiso de cumplir los requisitos aplicables con la seguridad de la información;	-	1	No se encuentra definido	
22				incluya un compromiso de mejora continua del sistema de gestión de la seguridad de la información.	-	1	No se encuentra definido	
23				La política de seguridad de la información debe: estar disponible como información documentada	-	2	La política del SGSI, se encuentra en proceso de elaboración.	
24				comunicarse dentro de la organización	-	1	No se encuentra definido	
25				Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes	-	2	La política del SGSI, se encuentra en proceso de elaboración.	

CAPITULO 5							
ÍTEM	NORMA		LIDERAZGO				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
26				las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas	-	1	No está definido la periodicidad de evaluación
27				estar disponible para las partes interesadas según sea disponible	-	1	No se encuentra definido
28		5,3,	ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen, se comuniquen y se entiendan en toda la organización.	-	1	No es claro como en los perfiles se han definidos funciones, responsabilidades y competencias enfocadas a seguridad d de la información
29				La alta dirección debe asignar la responsabilidad y autoridad para: a) asegurarse de que el sistema de gestión de la seguridad de la información es conforme con los requisitos de esta Norma Internacional;	-	1	No se encuentra definido
30				asegurarse de que los procesos están generando y proporcionando las salidas previstas;	-	1	No se encuentra definido

CAPITULO 5							
ÍTEM	NORMA		LIDERAZGO				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
31				informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información	-	1	No se encuentra definido
32				La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la organización	-	1	No es claro como en los perfiles se han definidos funciones, responsabilidades y competencias enfocadas a seguridad d de la información.

Conclusión

No está claramente definido el ejercicio del liderazgo de tal forma que se pueda evidenciar un compromiso y empoderamiento de las actividades en pro de obtener los resultados de conformidad y control sobre los riesgos de la seguridad de la información. El Jefe de la oficina TIC no tiene definido el plan director para dar los lineamientos requeridos para la implementación del SGSI, no existe un sistema de gestión documental que permita documentar lo referente al SGSI que contenga la política del SGSI, la declaración de aplicabilidad, los documentos (procedimientos, formatos) asociados al SGSI, la metodología de riesgos, los documentos (procedimientos, formatos) asociados a riesgos.

Capítulo 6. Planificación

Ilustración 3. Análisis de Planificación de la Gestión

En las actividades de planificación nos enfocamos en 2 temas específicos como lo son el análisis de riesgos y las oportunidades, la valoración de los riesgos definiendo planes de acción para tratarlos de forma preventiva, así como abordar las oportunidades para mejorar la gestión, y los objetivos que pretende la organización alcanzar a través de la implementación de actividades, controles, planes y programas para evitar la materialización de los impactos que pueden generar los riesgos.

Las actividades enfocadas a planificar y dirigir la gestión a la prevención y el control de riesgos no se encuentran alineadas, se realizan actividades de control de forma independiente y a pesar de que se cuenta con algunas herramientas, estas no han sido implementadas o su implementación no es trazable.

La gestión del proceso de TIC ha desarrollado una serie de controles orientados a proteger la información y los datos, sin embargo, dicha planificación no ha sido aprobada o alineada a la estrategia de implementación, lo que limita la gestión preventiva del proceso de TIC.

En este contexto, no es claro cómo establecer o asegurar una gestión eficiente, ya que los documentos no han sido aprobados, divulgados, socializados y puestos

en ejecución, con el propósito de evidenciar de forma trazable su gestión, monitoreo, control, evaluación, análisis y mejora.

No es claro, cómo han sido alineados los objetivos a la gestión de los procesos, a las políticas y a la estrategia de implementación, y no se define como estos van a ser medidos para establecer su efectividad y los esfuerzos organizacionales en pro de la mejora continua.

No han sido evaluadas o abordadas las oportunidades para mejorar los controles o la seguridad de la información en forma trazable, por lo cual no se puede realizar un análisis del impacto y la mejora obtenida a través de los resultados.

Los objetivos no establecen metas y planes o programas alineados para desarrollarlos, de tal forma que se pueda medir o evaluar el desempeño del MVCT frente a la seguridad de la información.

A continuación, se registra la valoración del capítulo 6:

CAPITULO 6								
ÍTEM	NORMA		PLANIFICACIÓN					
	CAP.	TITU						
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES	
33	6	6.1.	ACCIONES PARA ABORDAR RIESGOS Y OPORTUNIDADES	Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario abordar con el fin de:	-	1	No se cuenta con documento para establecer los riesgos, lo que dificulta la definición del método para establecer las oportunidades y generar acciones de mejora.	

CAPITULO 6								
ÍTEM	NORMA		PLANIFICACIÓN					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
34					asegurar que el sistema de gestión de la seguridad de la información pueda lograr sus resultados previstos;	se cuenta con matriz de riesgos de seguridad de la información definida por procesos del pasado 12/04/2018, sin embargo, no se evidencia la participación de los procesos en la construcción de la misma.	3	Matriz borrador, sin aprobación, sin metodología
35					prevenir o reducir efectos no deseados;	Están definido los controles, pero no han sido implementados, de acuerdo a la matriz borrador presentada	3	Matriz borrador, sin aprobación, sin metodología
36					lograr la mejora continua	-	1	Matriz borrador, sin aprobación, sin metodología
37					La organización debe planificar: las acciones para tratar estos riesgos y oportunidades; y	-	1	Matriz borrador, sin aprobación, sin metodología
38					la manera de: 1) integrar e implementar estas acciones en sus procesos del sistema de gestión de la seguridad de la información,	-	1	Se definen las acciones para abordar los riesgos y las oportunidades, sin embargo, las actividades definidas no han sido implementadas.
39					2) evaluar la eficacia de estas acciones.	-	1	No se cuenta con una metodología documentadas y debidamente aprobada

CAPITULO 6								
ÍTEM	NORMA		PLANIFICACIÓN					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
40					La organización debe definir y aplicar un proceso de valoración de riesgos de la seguridad de la información que	-	1	A la fecha no se ha documentado
41					establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan : 1) Los criterios de aceptación de riesgos	-	1	A la fecha no se ha documentado
42					2) los criterios para realizar valoraciones de riesgos de la seguridad de la información	-	1	A la fecha no se ha documentado
43				**VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN**	asegure que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables	-	1	A la fecha no se ha documentado
44					identifique los riesgos de la seguridad de la información	-	1	A la fecha no se ha documentado
45					1) aplicar el proceso de valoración de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información	-	1	A la fecha no se ha documentado

CAPITULO 6								
ÍTEM	NORMA		PLANIFICACIÓN					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
46					2) identificar a los dueños de los riesgos	-	1	A la fecha no se ha documentado
47					d) analice los riesgos de la seguridad de la información	-	1	A la fecha no se ha documentado
48					1) Valorar las consecuencias potenciales que resultaran si se materializaran los riesgos identificados en 6.1.2 c) 1);	-	1	A la fecha no se ha documentado
49					2) Valorar la probabilidad realista de que ocurran los riesgos identificados en 6.1.2c) 1); y	-	1	A la fecha no se ha documentado
50					3) determinar los niveles de riesgo	-	1	A la fecha no se ha documentado
51					e) evalúe los riesgos de seguridad de la información	-	1	A la fecha no se ha documentado
52					comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en 6,2,1 A) y	-	1	A la fecha no se ha documentado
53					Priorizar los riesgos analizados para el tratamiento de riesgos	-	1	A la fecha no se ha documentado
54				**TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**	la organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para:	-	1	A la fecha no se ha documentado

CAPITULO 6								
ÍTEM	NORMA		PLANIFICACIÓN					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
55					seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la valoración de riesgos	-	1	A la fecha no se ha documentado
56					determinar los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información	-	1	A la fecha no se ha documentado
57					comparar los controles determinados en 6,1,3 b) con los del Anexo A, y verificar que no sean omitidos controles necesarios	-	1	A la fecha no se ha documentado
58					d) producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A	-	1	A la fecha no se ha documentado
59					e) formular un plan de tratamiento de riesgos de la seguridad de la información; y	-	1	A la fecha no se ha documentado

CAPITULO 6								
ÍTEM	NORMA		PLANIFICACIÓN					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
60					f) obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información	-	1	A la fecha no se ha documentado
61					La organización debe conservar información documentada acerca del proceso de tratamiento de riesgos de la seguridad de la información	-	1	A la fecha no se ha documentado
62		6,2,		OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANIFICACIÓN PARA LOGRARLOS	La organización debe establecer objetivos de la seguridad de la información para las funciones y niveles pertinentes	La política de SGSI se encuentra en proceso de elaboración en la cual se establecen los objetivos.	2	Sin revisión de OAP
63					Los objetivos de la seguridad de la información deben: a) ser coherentes con la política de la seguridad de la información;	La política de SGSI se encuentra en proceso de elaboración en la cual se establecen los objetivos.	2	Sin revisión de OAP
64					ser medibles (si es posible);	-	1	No se han definido sistemas de seguimiento y medición de los objetivos
65					c) tener en cuenta los requisitos de la seguridad de la información aplicables, y los resultados de la valoración y del tratamiento de los riesgos	-	1	A la fecha no se ha documentado
66					d) ser comunicado; y	-	1	No han sido comunicados

CAPITULO 6								
ÍTEM	NORMA		PLANIFICACIÓN					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
67					e) ser actualizado, según sea apropiado.	-	1	No han sido evaluados o actualizados
68					La organización debe conservar información documentada sobre los objetivos de la seguridad de la información	-	1	A la fecha no se ha documentado
69					Cuando se hace la planificación para lograr sus objetivos de la seguridad de la información, la organización debe determinar: f) lo que se va a hacer	-	1	No es claro como se ha alineado la gestión a través de las actividades en aras de cumplir los objetivos.
70					g) que recursos se requerirán	-	1	A la fecha no se ha documentado
71					h) quién será responsable	-	1	A la fecha no se ha documentado
72					i) cuándo se finalizará; y	-	1	A la fecha no se ha documentado
73					j) cómo se evaluarán los resultados	-	1	A la fecha no se ha documentado

Conclusión

No se cuenta con una metodología para abordar los riesgos, lo cual dificulta la trazabilidad de la eficacia de la gestión y el desempeño de los procesos, que este alineada con el contexto de la metodología implementada por la organización.

El Jefe de la oficina TIC no tiene definida la metodología de riesgos para ser utilizada como MAGERIT, Octave, ISO31000, ISO27005, ITIL, COBIT, el modelo de seguridad y privacidad de la información asociados a buenas prácticas para mitigar los riesgos.

La falta de identificación de riesgos y por siguiente la carencia de controles, impacta significativamente el Sistema de seguridad de la información y por ende los sistemas de información del MVCT y FNV.

Capítulo 7. Apoyo

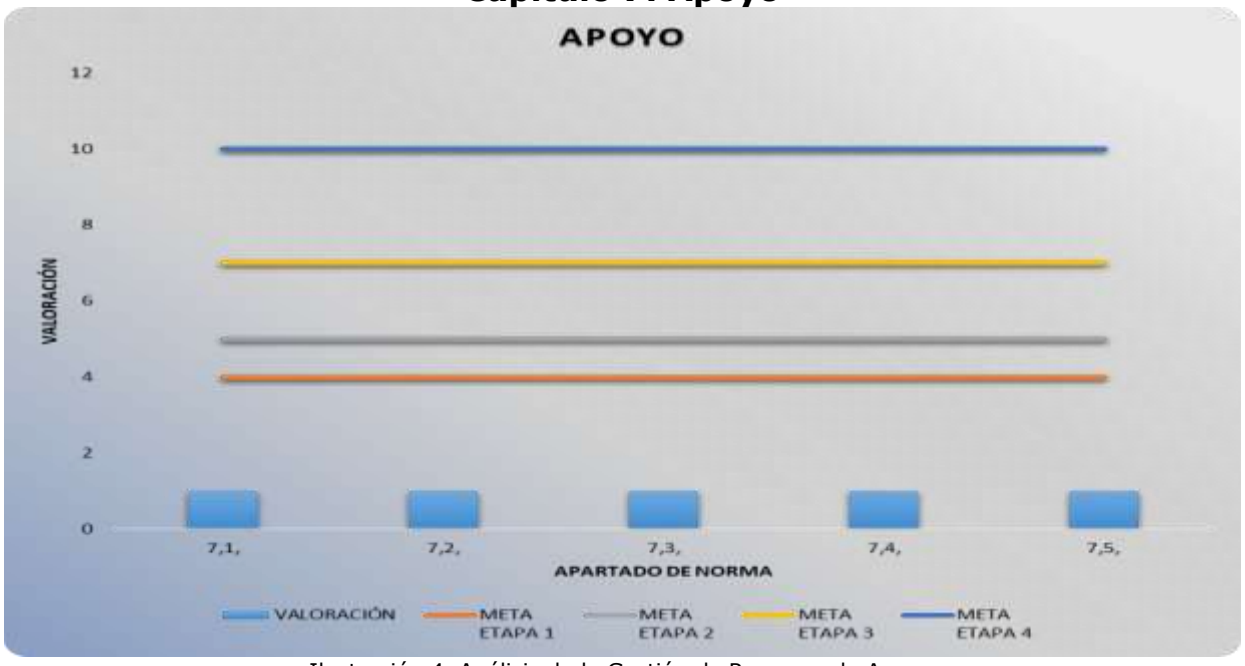


Ilustración 4. Análisis de la Gestión de Recursos de Apoyo

Frente a los requisitos normativos de los recursos de apoyo, la norma aborda 5 temas en específico, los cuales son recursos, comunicaciones, creación de cultura, gestión del conocimiento y documentación, los cuales son herramientas que apoyan una operación efectiva de los procesos.

La aplicación de estos criterios, obedece a la asignación por necesidad de tal forma que se cuente con los recursos para la operación de las actividades, sin embargo, esta asignación se realiza más por necesidad, que porque exista una estructura definida para la operación de los procesos y las operaciones de los planes o actividades de control.

No es claro cómo abordar una metodología para gestionar el conocimiento a través del cual se pueda hacer uso de este, y el proceso de capacitación se ha limitado a las condiciones generales de los sistemas de gestión y las actividades,

más que al desarrollo y la creación de cultura preventiva enfocada a la seguridad de la información. No se cuenta con una base documental definida, lo que dificulta dar cumplimiento a los requerimientos normativos.

A continuación, se registra la valoración del capítulo 7:

CAPITULO 7							
ÍTEM	NORMA		APOYO				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
74		*7,1,*	**RECURSOS**	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento , implementación , mantenimiento y mejora continua del sistema de gestión de la seguridad de la información .	-	1	No se cuenta con presupuesto definido, adicionalmente no se ha asignado el oficial de seguridad d de la información
76	*7*	*7,2,*	**COMPETENCIA**	La organización debe: a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño de la seguridad de la información;	-	1	No es claro cómo han sido tenidos en cuenta los criterios de seguridad de la información para definir las competencias del personal. No se realizan estudios de confiabilidad al personal ni ingreso ni periódicos
77				asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas;	-	1	No se han definido competencias con base en los perfiles enfocados a seguridad de la información

CAPITULO 7							
ÍTEM	NORMA		APOYO				
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
78					cuando sea aplicable, tomar acciones para adquirir la competencia necesaria	-	1	A la fecha no se ha documentado
79					y evaluar la eficacia de las acciones tomadas;	-	1	A la fecha no se ha documentado
80					conservar la información documentada apropiada como evidencia de la competencia.	-	1	A la fecha no se ha documentado
81			7,3,	TOMA DE CONCIENCIA	Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de: a) la política de la seguridad de la información;	-	1	No se ha realizado divulgación de la política.
82					su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios de una mejora del desempeño;	-	1	No se ha realizado divulgación de los criterios y la aplicabilidad del SGSI
83					las implicaciones de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información.	-	1	No se ha realizado divulgación de los criterios y la aplicabilidad del SGSI

CAPITULO 7							
ÍTEM	NORMA		APOYO				
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
84		*7,4,*		**COMUNICACIÓN**	La organización debe determinar las comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan: a) el contenido de la comunicación; b) cuándo comunicar; c) a quién comunicar; d) quién debe comunicar; e) los procesos para llevar a cabo la comunicación	-	1	No se han establecido los parámetros de comunicación o las características para comunicar de tal forma que se asegure un control
85		*7,5,*		**INFORMACIÓN DOCUMENTADA**	El sistema de gestión de la seguridad de la información de la organización debe incluir: a) la información documentada requerida por esta Norma Internacional;	-	1	Se cuenta con el borrador de 3 documentos, sin embargo, no ha sido aprobado y no se ha establecido la suficiencia de los mismos. No se han definido procedimientos para desarrollar actividades, generales del SGSI
86					la información documentada que la organización determina como necesaria para la eficacia del sistema de gestión de la seguridad de la información.	-	1	A la fecha no se ha documentado

CAPITULO 7							
ÍTEM	NORMA		APOYO				
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
87				CREACIÓN Y ACTUALIZACIÓN	Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado: a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia)	-	1	A la fecha no se ha documentado
88					b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico)	-	1	A la fecha no se ha documentado
89					c) la revisión y aprobación con respecto a la idoneidad y adecuación	-	1	A la fecha no se ha documentado
90				CONTROL DE LA INFORMACIÓN DOCUMENTADA	La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta Norma se debe controlar para asegurarse de que: a) esté disponible le y adecuada para su uso, donde y cuando se necesite; y	-	1	A la fecha no se ha documentado

CAPITULO 7								
ÍTEM	NORMA		APOYO					
	CAP.	TITU	APARTADO DE NORMA	REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
91					b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad)	-	1	A la fecha no se ha documentado
92					Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda: a) distribución, acceso, recuperación y uso;	-	1	A la fecha no se ha documentado
93					almacenamiento y preservación, incluida la preservación de la legibilidad;	-	1	A la fecha no se ha documentado
94					control de cambios	-	1	A la fecha no se ha documentado
95					retención y disposición.	-	1	A la fecha no se ha documentado
96					La información documentada de origen externo, que la organización determina como necesaria para la planificación y operación del sistema de gestión de la seguridad de la información, se debe identificar, según sea apropiado, y controlar.	-	1	A la fecha no se ha documentado

Conclusión

Los recursos organizacionales no se encuentran asignados por un adecuado proceso de planificación, sino por necesidad de contingencia y no es claro como los ejercicios de creación de cultura se desarrollan en materia de prevención de la seguridad y control de los riesgos del manejo de datos e información. No existe un nivel de estructuración que identifique las necesidades del sistema y como implementar alternativas de socialización y sensibilización para garantizar el flujo de información que se requiere, como el mapa de ruta para las iniciativas del SGSI.

Capítulo 8. Operación

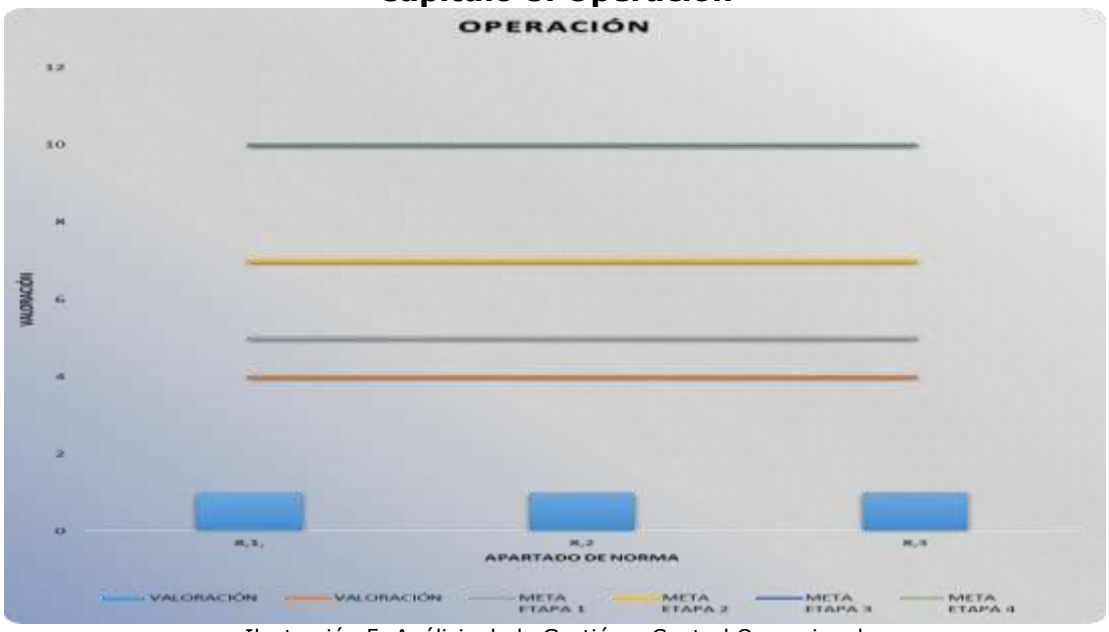


Ilustración 5. Análisis de la Gestión y Control Operacional

Los controles operacionales abordan 3 temas específicos, la planificación y el control de la operación, el control de las vulnerabilidades y el tratamiento de los riesgos, enfocado a mantener bajo condiciones controladas todas las actividades que puedan poner en riesgo la información o los datos.

Frente a este tema, principalmente resaltamos la importancia de las herramientas organizacionales como son los firewalls, los antivirus, los protocolos de control de software implementados y controlados, sin embargo, no se cuenta con un plan

para cierre de brechas en temas de planificación y control de la operación, ya que no se mantienen registros de estas actividades.

Se requiere el establecimiento de políticas con las condiciones que deben cumplir los servidores públicos para asegurar un control efectivo sobre la información, incluyendo criterios como los protocolos de trabajo seguro, los procedimientos operativos normalizados de seguridad entre otros.

El análisis de las vulnerabilidades, obedece al análisis de los riesgos y su contexto (documentos borrador), más que al de una vulnerabilidad, enfocada en los históricos y en la ocurrencia de eventos, teniendo en cuenta que la vulnerabilidad es el nivel de preparación del MVCT, para actuar ante una emergencia o evento adverso.

Los controles a los riesgos han sido definidos (matriz borrador), pero estos no han sido implementados y no han sido divulgados a los procesos y sus equipos de trabajo, los mismos son solo de conocimiento de los responsables de la actividad en el proceso TIC y Administración del SIG.

A continuación, se registra la valoración del capítulo 8:

CAPITULO 8								
ÍTEM	***NORMA***		***OPERACIÓN***					
	CAP.	***TITU***						
	APARTADO DE NORMA		**REQUISITO**	***ESPECIFICACIÓN***	***EVIDENCIA***	***VALORACIÓN***	***OBSERVACIONES***	
97	***8***	***8,1,***	**PLANIFICACIÓN Y CONTROL OPERACIONAL**	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el numeral 6.1	-	1	A la fecha no se ha documentado	

CAPITULO 8								
ÍTEM	NORMA		OPERACIÓN					
	CAP.	TITU						
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES	
98				La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en el numeral 6.2.	-	1	A la fecha no se ha documentado	
99				La organización debe mantener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado.	-	1	A la fecha no se ha documentado	
100				La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario.	-	1	A la fecha no se ha documentado	
101				La organización debe asegurar que los procesos contratados externamente estén controlados	-	1	A la fecha no se ha documentado	
102		*8,2,*	**VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN**	La organización debe llevar a cabo valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando se produzcan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el numeral 6,1,2 a).	-	1	A la fecha no se ha documentado	
103				la organización debe conservar información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información	-	1	A la fecha no se ha documentado	

CAPITULO 8							
ÍTEM	NORMA		OPERACIÓN				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
104		8,3,	TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	La organización debe implementar el plan de tratamiento de riesgos de la seguridad de la información	-	1	A la fecha no se ha documentado
105				La organización debe conservar información documentada de los resultados del tratamiento de riesgos de la seguridad de la información	-	1	A la fecha no se ha documentado

Conclusión

Dentro del control operacional de la organización, no se han implementado acciones que permitan responder y evaluar las situaciones que se puedan presentar, no se cuenta con protocolos de seguridad, lo cual incumple con los requisitos normativos; así mismo, no se evidencia la planificación que permita una adecuada evaluación a la operación bajo condiciones controladas tomando en cuenta las actividades desarrolladas en la implementación del SGSI. De igual manera, no se identifican estrategias para la presentación de los resultados y las fases que deben implementarse en cada uno de procesos de gestión definidos en el SGSI para generar, producir e implementar el sistema.

Capítulo 9. Evaluación del Desempeño.

Ilustración 6. Análisis del Ejercicio de Evaluación del Desempeño en la Gestión

La evaluación del desempeño en la gestión se enfoca en 3 actividades, como lo son el monitoreo y seguimiento del desempeño, las auditorías y la revisión por la dirección; las cuales deben estar estructuradas y contar con los recursos y la información adecuada, frente a este criterio, la organización no cuenta con la definición de las herramientas para dar cumplimiento a los requisitos.

Como sistemas de monitoreo y control, no se han definido indicadores y algunas actividades de revisión, lo cual no permite medir el desempeño de la seguridad de la información, en pro de la toma de acciones que permitan la mejora en los resultados.

No se han realizado auditorías al sistema de gestión de seguridad de la información, así mismo no se evidencia la documentación del procedimiento para evaluar los criterios que deben ser evaluados dentro de la auditoria concernientes a las actividades de seguridad de la información.

El proceso o las actividades de revisión por la dirección no se han definido o ejecutado de tal forma que se evidencie un seguimiento apropiado y una toma de decisiones por parte de los líderes de los procesos para prevenir incidentes con la información suministrada.

A continuación, se registra la valoración del capítulo 9:

CAPITULO 9							
ÍTEM	NORMA		EVALUACIÓN DEL DESEMPEÑO				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
106	9	9,1,	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información	-	1	A la fecha no se ha documentado
107				La organización debe determinar: a) A que es necesario hacer seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados validos	-	1	A la fecha no se ha documentado
108				b) los métodos de seguimiento y medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos. Para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles	-	1	No han sido definido sistemas estructurados de seguimiento y medición
109				c) cuándo se deben llevar a cabo el seguimiento y la medición	-	1	No han sido definido sistemas estructurados de seguimiento y medición
110				d) quién debe llevar a cabo el seguimiento y la medición	-	1	A la fecha no se ha documentado
111				e) cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición; y	-	1	A la fecha no se ha documentado
112				La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición	-	1	No se cuenta con métodos de seguimiento y medición definidos

CAPITULO 9							
ÍTEM	NORMA		EVALUACIÓN DEL DESEMPEÑO				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
113				La organización debe llevar a cabo auditorías internas a intervalos planificados , para proporcionar información acerca de si el sistema de gestión de la seguridad de la información	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI
114				a) es conforme con: 1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información ; y	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI
115				2) los requisitos de esta Norma;	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI
116				b) está implementado y mantenido	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI
117		9,2,	AUDITORIA INTERNA	La organización debe: c) planificar , establecer , implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia , los métodos, las responsabilidades , los requisitos de planificación , y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI
118				d) para cada auditoría , definir los criterios y el alcance de ésta	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI
119				e) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI

CAPITULO 9							
ÍTEM	NORMA		EVALUACIÓN DEL DESEMPEÑO				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
120				asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI
121				conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta	-	1	No se han definido métodos o protocolos para ejecutar auditorias de SGSI
122		9,3,	REVISIÓN POR LA DIRECCIÓN	La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados , para asegurarse de su conveniencia , adecuación y eficacia continuas	-	1	No se ha definido métodos o registros o se ha planificado
123				La revisión por la dirección debe planificarse y llevarse a cabo incluyendo consideraciones sobre: a) el estado de las acciones de las revisiones por la dirección previas;	-	1	No se ha definido métodos o registros o se ha planificado
124				b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;	-	1	No se ha definido métodos o registros o se ha planificado

CAPITULO 9								
ÍTEM	NORMA		EVALUACIÓN DEL DESEMPEÑO					
	CAP.	TITU						
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES	
125				c) retroalimentación sobre el desempeño de la seguridad de la información , incluidas las tendencias relativas a: 1) no conformidades y acciones correctivas ; 2) seguimiento y resultados de las mediciones ; 3) resultados de la auditoría ; y 4) cumplimiento de los objetivos de la seguridad de la información ;	-	1	No se ha definido métodos o registros o se ha planificado	
126				d) retroalimentación de las partes interesadas	-	1	No se ha definido métodos o registros o se ha planificado	
127				e) resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y	-	1	No se ha definido métodos o registros o se ha planificado	
128				f) las oportunidades de mejora.	-	1	No se ha definido métodos o registros o se ha planificado	
129				Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información	-	1	No se ha definido métodos o registros o se ha planificado	
130				La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.	-	1	No se ha definido métodos o registros o se ha planificado	

Conclusión

No se cuenta con un enfoque claro de la medición, monitoreo y control del desempeño de la seguridad de la información, toda vez que las actividades de control no están siendo monitoreadas, analizadas y evaluadas con medios trazables; este criterio cuenta con un bajo grado de implementación frente a los requisitos normativos.

Capítulo 10. Mejora.

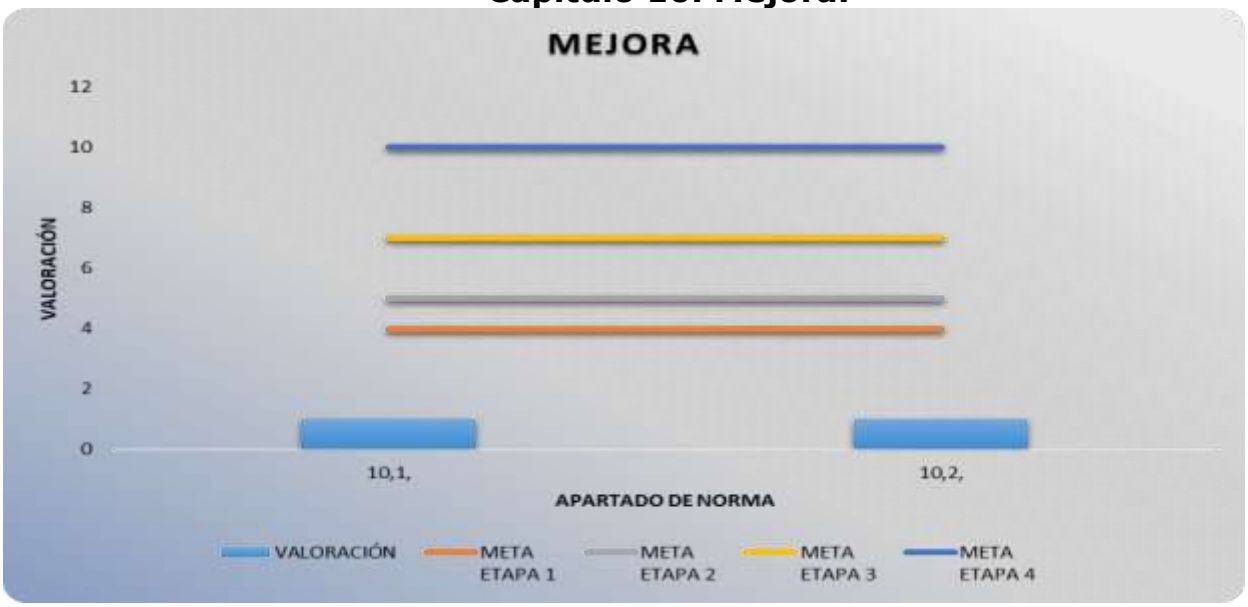


Ilustración 7. Análisis del Ejercicio de Evaluación del Desempeño en la Gestión

La mejora está enfocada en aquellas actividades o acciones que implementa la organización, para desarrollar y mejorar su sistema de manera sistemática, con base en los resultados organizacionales, teniendo en cuenta dos aspectos específicos, las acciones de mejora, el aprovechamiento de estas y su registro y el control de los eventos adversos.

Al respecto, no es claro cómo se asegura que la mejora continua pueda ser analizada a través de la trazabilidad y los registros.

Por otra parte, no es claro cómo se mide el enfoque preventivo organizacional, y como se pueden analizar los resultados de las acciones tomadas frente a lo

planificado, de igual manera, no se cuenta con las herramientas para monitoreo de riesgo y de vulnerabilidad.

A continuación, se registra la valoración del capítulo 10:

CAPITULO 10							
ÍTEM	NORMA		MEJORA				
	CAP.	TITU					
	APARTADO DE NORMA		REQUISITO	ESPECIFICACIÓN	EVIDENCIA	VALORACIÓN	OBSERVACIONES
131	10	10,1	NO CONFORMIDADES Y ACCIONES CORRECTIVAS	cuando ocurra una no conformidad, la organización debe: a) reaccionar ante la no conformidad, y según sea aplicable 1) Tomar acciones para controlarla y corregirla, y	-	1	No se cuenta con método definido, lo que no permite generar una reacción y un control oportuno.
132				2) hacer frente a las consecuencias	-	1	A la fecha no se ha documentado
133				b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no volviera a ocurrir ni ocurra en otra parte, mediante:	-	1	A la fecha no se ha documentado
134				1) la revisión de la no conformidad	-	1	A la fecha no se ha documentado
135				2) la determinación de las causas de la no conformidad, y	-	1	A la fecha no se ha documentado
136				3) la determinación de si existen no conformidades similares, o que potencialmente	-	1	A la fecha no se ha documentado

				podrían ocurrir;			
137				c) implementar cualquier acción necesaria	-	1	A la fecha no se ha documentado
138				d) revisar la eficacia de las acciones correctivas tomadas , y	-	1	A la fecha no se ha documentado
139				e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario .	-	1	A la fecha no se ha documentado
140				Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas	-	1	A la fecha no se ha documentado
141				La organización debe conservar información documentada adecuada , como evidencia de: f) la naturaleza de las no conformidades y cualquier acción posterior tomada; y	-	1	A la fecha no se ha documentado
142				g) los resultados de cualquier acción correctiva	-	1	A la fecha no se ha documentado
143		***10,2***	**MEJORA CONTINUA**	La organización debe mejorar continuamente la conveniencia , adecuación y eficacia del sistema de gestión de la seguridad de la información.	-	1	A la fecha no se ha documentado

Conclusión

No se cuenta con un enfoque a la mejora de manera formal, no se pueden hacer trazabilidad o análisis y no se monitorean los resultados de gestión y la mejora alcanzada, lo que impide en algunos casos, adoptar buenas prácticas o cambiar las acciones que no surgen el efecto esperado.

De otra parte, el proceso presenta un plan de trabajo, el cual no se encuentra aprobado por el comité institucional de Gestión y Desempeño, el mismo no presenta avance significativo y las actividades documentadas no son acordes a los requerimientos de la norma ISO 27001:2013.

RIESGOS IDENTIFICADOS:

En los seguimientos a los mapas de Riesgos Integrados de Gestión y Corrupción, específicamente en los relacionados con el Proceso de "Gestión de Proyectos de Tecnologías de la Información", se verificó la identificación de los Riesgos de Gestión - Tecnología "**Pérdida de confidencialidad, disponibilidad y integridad de la información."** y **"Incumplimiento de la Política de gobierno Digital"**; en el monitoreo de los mismos, de manera mensual se observa que los controles implementados no permiten disminuir el nivel del Riesgo inherente permaneciendo en una zona EXTREMA, sin que a la fecha se tomen acciones por parte del proceso.

TIPO DE RIESGO	CLASE DE RIESGO	ZONA DE RIESGO INHERENTE	ZONA DE RIESGO RESIDUAL	No. CONTROLES
GESTION	TECNOLOGIA Pérdida de confidencialidad, disponibilidad e integridad de la información	EXTREMA	EXTREMA	2
	TECNOLOGIA Incumplimiento de la Política de gobierno Digital	EXTREMA	EXTREMA	3

VERIFICACIÓN DE CONTROLES:

El Grupo de Tecnologías de la Información y las Comunicaciones del Ministerio de Vivienda, Ciudad y Territorio, no evidencia cumplimiento de la operatividad de los controles asociados a los riesgos 4 y 5 de la matriz de riesgos del proceso; así mismo no se evidencia toma de acciones de mejora frente al informe generado por la OCI en el mes de mayo, comunicado al proceso mediante memorando 2018IE0006151 DEL 29/05/2018 y publicado en el link http://www.minvivienda.gov.co/sobre-el-ministerio/planeacion-gestion-y-

control/sistema-de-control-interno/rol-de-evaluaci%C3%B3n-de-gesti%C3%B3n-del-riesgo.

ACCIONES DE MEJORAMIENTO:

Al verificar el Plan de Mejoramiento del MVCT suscrito con la Contraloría General de la República, se observa el incumplimiento en el siguiente hallazgo, el cual, a la fecha no presenta toma de acciones de mejora por parte del proceso, así:

CÓDIGO HALLAZGO	DESCRIPCIÓN DEL HALLAZGO	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / FECHA DE TERMINACIÓN	Porcentaje de Avance físico de ejecución de las Actividades
40(2015)	Procedimientos seguridad de la información. Deficiencias en la formalización de mecanismos de control para mitigar la ocurrencia de eventos de seguridad que afecten la infraestructura tecnológica y la información a cargo del Ministerio.	Definir los siguientes procedimientos: 1. Recepción o intercambio de información con aplicativos de entidades externas. 2. Aprobación / adquisición de los recursos de TI para el MVCT 3. Implementación de proyectos del portafolio de proyectos del PETIC	**2018-03-31 El proceso incumplió la fecha programada para el cumplimiento de la actividad.**	0%

Así mismo, verificado el Plan de Mejoramiento del Sistema Integrado de Gestión del MVCT no se encuentran establecidos hallazgos relacionados con el tema objeto de verificación; ni acciones de un ejercicio de autocontrol que contribuya al mejoramiento del proceso.

RECOMENDACIONES:

Capítulo 4. Contexto Organizacional:

- ✓ Definir el método para realizar la evaluación de contexto organizacional.
- ✓ Realizar análisis de las partes interesadas y priorizar los requisitos, así como evaluar los sistemas de seguimiento y medición que se van a aplicar a cada uno de estos requisitos.

- ✓ Definir claramente el alcance, para cada uno los servicios y las condiciones de seguridad de la información.
- ✓ Documentar el plan director de seguridad y sensibilizar el mapa de ruta para la implementación del SGSI.
- ✓ Estructurar dentro del análisis de las partes interesadas, las internas y externas que son primarias o secundarias, así mismo establecer el análisis de oportunidades con estas.
- ✓ Divulgar el análisis del contexto, así como su aplicabilidad, el alcance de los controles y el sistema Integrado de gestión a todos los involucrados como medio de creación de conciencia y de generación de cultura.
- ✓ Estructurar un manual del sistema de gestión de seguridad de la información de tal forma que se cuente con la definición de la aplicabilidad de los criterios en la organización, articulado con el SIG.
- ✓ Definir metas e indicadores para evaluar que el sistema está operando correctamente, con el fin de establecer acciones preventivas y correctivas, según sea el caso.

Capítulo 5. Liderazgo:

- ✓ Aprobar por parte de la alta dirección las directrices organizacionales enfocadas a la seguridad de la información.
- ✓ Divulgar las políticas a todos los niveles del MVCT y las partes interesadas.
- ✓ Integrar el SGSI al Sistema Integrado de Gestión del MVCT.
- ✓ Definir el plan de gobierno del SGSI.
- ✓ Asignar un oficial de seguridad de la información, el cual tenga rol independiente dentro de esta gestión y no pertenezca a proceso o actividades que tengan influencia directa sobre la seguridad de la información.
- ✓ Crear el comité técnico de seguridad.
- ✓ Definir los roles y responsabilidades del comité de seguridad.
- ✓ Aprobar la estructura y documentos del SGSI, en lo posible por parte de la alta dirección.
- ✓ Capacitar al personal sobre los criterios claves del SGSI y su estructura.
- ✓ Establecer el rol de la alta dirección dentro de los sistemas de asignación, responsabilidad, seguimiento, control y mejora del SGSI.

- ✓ Divulgar a todos los niveles del MVCT, las responsabilidades y funciones frente a la seguridad de la información previamente aprobados por la alta dirección.
- ✓ Actualizar las políticas en donde se especifique el compromiso de la organización, con el cumplimiento, el control, el seguimiento, la evaluación y la mejora de la gestión en temas de manejo de datos e información.
- ✓ Establecer la periodicidad y el método a través de cual se debe realizar la evaluación del cumplimiento de las políticas y los objetivos organizacionales del SGSI.
- ✓ Alinear las actividades de cada uno de los procesos a las actividades de control y de seguimiento al manejo y tratamiento de los datos e información a través de las caracterizaciones.
- ✓ Establecer la gestión del oficial de seguridad, así como los métodos de rendición de cuentas.

Capítulo 6. Planificación:

- ✓ Documentar la metodología, articulada con la establecida por el SIG para la administración del riesgo y realizar el ejercicio para asegurar la identificación y la definición de planes de acción para las oportunidades en temas de mejora en seguridad de la información.
- ✓ Actualizar la matriz de riesgos con base en los cambios organizacionales y de la gestión.
- ✓ Priorizar e implementar de forma gradual las actividades definidas para el control de los riesgos.
- ✓ Establecer plazos para la implementación de los controles y planes definidos para controlar los riesgos.
- ✓ Establecer métodos y frecuencia para evaluar la efectividad de los controles implementados.
- ✓ Realizar análisis comparativo entre los riesgos obtenidos en la evaluación inicial y la mejora obtenida con la implementación de los controles.
- ✓ Establecer métodos estructurados y alineados para evaluar el cumplimiento de los objetivos y las necesidades de cambio o ajuste en estos o sus metas.
- ✓ Realizar despliegue de las directrices organizacionales de tal forma que se asegure el conocimiento y la toma de conciencia.

Capítulo 7. Apoyo:

- ✓ Asignar un presupuesto para la ejecución de los planes, programas y actividades de control.
- ✓ Designar al oficial de seguridad de la información y mantener un registro de esta en el cual se especifiquen funciones, responsabilidades y niveles de autoridad.
- ✓ Actualizar los perfiles de cargo asegurando que se definen competencias frente a la seguridad de la información.
- ✓ Asegurar que se realizan los estudios de confiabilidad al personal, sobre todo a aquellos que cuentan con manejo de datos o información relevante.
- ✓ Incluir en plan de capacitación actividades enfocadas a seguridad de la información, herramientas controles planes y programas.
- ✓ Diseñar un programa de gestión del conocimiento enfocado a asegurar la creación de cultura y la toma de conciencia, el aprovechamiento del conocimiento organizacional e individual.
- ✓ Establecer registros de las actividades de formación y desarrollo realizadas.
- ✓ Asegurar que las actividades de formación y desarrollo son evaluadas y mantener un registro que permita la trazabilidad de los resultados de la eficacia de estas.
- ✓ Definir los medios, canales, elementos, registro e involucrados en las comunicaciones organizacionales enfocadas a la seguridad de la información a través de herramientas como la matriz de comunicaciones.
- ✓ Asegurar que se cuenta con protección de la información de forma periódica a través de los backups y se analiza el riesgo de mantener backups periódicos, así como mantener backups de respaldo como medio de protección.

Capítulo 8. Operación:

- ✓ Alinear los controles actuales (borrador) a la gestión de planificación y control operacional, a través del análisis de los riesgos y las vulnerabilidades.
- ✓ Realizar priorización de los planes y actividades de control, e implementar aquellas que son prioritarias.

- ✓ Realizar estructuración y divulgación de los planes, programas o actividades definidas para controlar y gestionar los riegos y reducir la vulnerabilidad organizacional.
- ✓ Asegurar que cualquier proceso tercerizado enfocado a la creación, desarrollo o manejo de información y sus herramientas cuente con métodos de control definidos incluyendo verificaciones y auditorías a proveedores.
- ✓ Realizar evaluación independiente de las vulnerabilidades con base en los históricos de eventos, y definir los planes operativos de actuación ante la ocurrencia, así mismo divulgar al personal involucrado.
- ✓ Realizar seguimiento periódico a los riesgos y su gestión, así como a la eficacia de los planes o actividades implementadas para controlar los riesgos y las vulnerabilidades.
- ✓ Evaluar las necesidades de controles frente a su definición, implementación, control y mejora, e implementar los requeridos.

Capítulo 9. Evaluación del Desempeño:

- ✓ Estructurar las actividades y herramientas de seguimiento y medición, con base en los objetivos de la gestión de seguridad de la información.
- ✓ Establecer y alinear las responsabilidades del seguimiento y medición a cada uno de los procesos y a los líderes de procesos.
- ✓ Establecer una alineación directa entre las políticas, los objetivos, los indicadores y las actividades. (realizar un cuadro de despliegue de políticas).
- ✓ Realizar medición y análisis de los indicadores, y generar las acciones correctivas o preventivas respecto a los resultados que se obtengan.
- ✓ Estructurar el procedimiento de auditorías internas teniendo en cuenta los criterios de seguridad de la información.
- ✓ Elaborar perfil de cargo de auditor de seguridad de la información con base en los requerimientos que se establezcan para el MVCT.
- ✓ Establecer el método o métodos para realizar por parte de la alta dirección revisiones periódicas a la eficacia y el desempeño de la gestión de seguridad de la información.
- ✓ Programar y ejecutar auditoria interna una vez se ha implementado el sistema de seguridad de la información.
- ✓ Realizar revisión por la dirección inicial y establecer la periodicidad con la que se van a desarrollar.

Capítulo 10. Mejora:

- ✓ Documentar e implementar el procedimiento de acciones en sus etapas para aquellas acciones que se requieran o que han generado un impacto o cambio en la organización.
- ✓ Establecer análisis de tendencia en la mejora a través de los resultados alcanzados por la implementación de mejoras o acciones de mejora en los procesos de seguridad de la información.
- ✓ Registrar las acciones de mejora tomadas y realizar análisis de los resultados.

PAPELES DE TRABAJO:

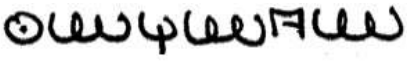
Documentos suministrados por el proceso a través de la carpeta compartida \\DOMUSFILE\Evidencias_SIG$

CUMPLIMIENTO DE LOS PRINCIPIOS DE AUDITORIA Y LIMITACIONES

Para el presente informe de evaluación se aplicaron por parte del auditor los principios de Integridad, Objetividad, Confidencialidad, Competencia y Conflicto de Interés y en el desarrollo del mismo no se presentaron limitaciones.

FIRMAS:

LINA ALEJANDRA MORALES
AUDITOR



OLGA YANETH ARAGON SANCHEZ
JEFE OFICINA DE CONTROL INTERNO