MACROPROCESO/ PROCESO O ÁREA DEL SEGUIMIENTO		No. INFORME FINAL
INFORME FINAL DE AUDITORIA INTERNA MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		24-2021
		FECHA DE INICIO
		01/12/2021
		FECHA ENTREGA DE INFORME
		28/04/2022
EQUIPO AUDITOR		**DESTINATARIO LIDER Y/O RESPONSABLE DEL ÁREA O DEPENDENCIA:**
Auditor(es):	Julio Andrés Sánchez S.	**Dr. Orlando Alfonso Clavijo Clavijo** Superintendente de Vigilancia y Seguridad Privada **Ing. Miguel Ángel García Gómez** Jefe Oficina de Sistemas
ASPECTOS GENERALES DEL INFORME		
Objetivo General:	Verificar la implementación de Modelo de Seguridad y Privacidad de la Información (MSPI), en cumplimiento con lo establecido en la resolución 500 de marzo 10 de 2021 y su anexo.	
Objetivos Específicos:	➢ Analizar la implementación de la herramienta referente al autodiagnóstico en seguridad y privacidad de la información, documentada en el anexo 1 de la resolución 500/2021. ➢ Evaluar el cumplimiento de la política de seguridad de la información, soportada en con el manual de políticas específicas y procedimientos documentados. ➢ Revisar los aspectos referentes al levantamiento de activos de información ➢ Verificar el procedimiento realizado por la Supervigilancia para el desarrollo del tratamiento y valoración de riesgos en seguridad y privacidad de la información. ➢ Cotejar los documentos relacionados con el plan de comunicaciones, plan de control operacional y establecimiento de indicadores.	
Alcance:	El alcance de la presente auditoría se llevará a cabo para la vigencia 2021.	
Metodología:	Aplicación de los elementos y herramientas para la evaluación independiente en concordancia con las normas internacionales para el ejercicio profesional de la auditoría interna, así: - Análisis de la información suministrada - Verificación de la información cargada en el gestor documental eSigna y la Suite Visión Empresarial. - Realización de mesas de trabajo y entrevistas con los responsables.	

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Criterios de seguimiento:	• Ley 87 de 1993 • Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”. • Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital”. • Decreto 612 de 2018 integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. • Manual de la Política de Gobierno Digital Versión 7 de abril de 2019. • CONPES 3995 de 2020 Política Nacional de confianza y seguridad Digital • Resolución 500 de marzo 10 de 2021 “*por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”,* • Guía Modelo de Seguridad de la Información MSPI Versión 4 de febrero de 2021 e instrumentos relacionados.

RESUMEN EJECUTIVO

Dentro de la función de evaluación y seguimiento al sistema de control interno dispuesta en la Ley 87 de 1993, en especial el artículo 12 literal G, y de acuerdo a los lineamientos descritos en el Modelo Integrado de Planeación y Gestión – MIPG en la dimensión de “Control Interno”, donde se define la auditoría como *“una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la entidad; que ayuda a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno”*:

Esta dependencia, concordante con el Plan Anual de Auditorías aprobado por el Comité Institucional de Coordinación de Control Interno, presenta el informe preliminar de auditoría de seguimiento modelo de seguridad y privacidad de la información, el cual se ejecutó atendiendo las directrices establecidas para la tercera línea de defensa dentro del Modelo Integrado de Planeación y Gestión MIPG, alineado con el Modelo Estándar de Control Interno –MECI, por medio de la evaluación de la gestión de riesgos asociados al proceso y sus controles.

Como resultado del informe de auditoría, la OCI da las recomendaciones pertinentes en el marco del rol de asesoría a la Alta Dirección, con el fin de aportar al mejoramiento del Sistema de Control Interno Institucional.

En el desarrollo de la auditoria al MSPI-SGSI el equipo auditor logro evidenciar lo siguiente:

- El autodiagnóstico en la casilla de evidencias no contiene referencia a una ubicación web o del sistema de información institucional que permita evidenciar el documento que le otorga el porcentaje de cumplimiento del nivel de madurez del 74.8%. Es de anotar, que la información relacionada con el MSPI-SGSI debe ser cargada en el Sistema y ser de fácil acceso de consulta para entes externos e internos, y demás grupos interesados.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

- Las funciones asignadas al rol del Chieff Information Oficcer CIO y al rol del Oficial de Seguridad de la Información, no están acorde con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y los demás entes regulatorios, se precisa que las funciones del CIO están orientadas a cumplir tareas estratégicas, diseñar planes e implementar los dominios de arquitectura empresarial, mientras que el Oficial de Seguridad de la Información debe hacer parte de la implementación del sistema, el modelo y la arquitectura de referencia de la Seguridad de la Información. Ver ítem 5,2 del cuerpo del informe.

- La metodología desarrollada para la evaluación y clasificación de riesgos, a la fecha de la auditoria (31 de diciembre de 2021), no ha sido aplicada en lo referente a seguridad de la información, lo anterior teniendo en cuenta que la entidad no tiene identificados los riesgos y controles, situación que conlleva a comprometer los activos de la información documental. Lo anterior se puede observar en lo puntos 6,7 y 8 del presente informe de auditoría.

- El plan anual SGSI, registra fecha de elaboración en el mes de junio de 2021, lo que permite inferir que la Oficina de Sistemas no adelantó actividades relacionadas con la implementación del SGSI, durante el periodo comprendido de enero a mayo de la vigencia antes mencionada, situación que dificulta la integración de planes institucionales enunciada en el artículo 2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción del decreto 612 de 2018 que a la letra dice: "*Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año".*

DESARROLLO DE LA AUDITORÍA

Dentro de la función de evaluación y seguimiento al sistema de Control Interno dispuesta en la Ley 87 de 1993, en especial el artículo 12 literal G, concordante con los planes y objetivos trazados en el plan anual de auditoría vigencia 2021, la Oficina de Control Interno adelantó la auditoria al proceso de Gestión de Sistemas e Información, en lo referente a la implementación del Modelo de seguridad y privacidad de la información (MSPI).

El equipo auditor tomó como fuente de información, la documentación publicada en el sitio web de la entidad https://www.supervigilancia.gov.co/ y en el sistema de información Suite Visión Empresarial, tal como se ilustra en la tabla Numero 1.

Tabla No1. Información de Auditoria

No.	Criterio	Entregable	Medio
1	**Herramienta de Diagnostico Seguridad y Privacidad de la Información.**	Diligenciamiento de la herramienta autodiagnóstico MSPI	Correo Electrónico

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

	2	**Herramienta de Diagnostico Seguridad y Privacidad de la Información.**	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Correo Electrónico	
	3	**Herramienta de Diagnostico Seguridad y Privacidad de la Información.**	Documento con los hallazgos encontrados en las pruebas - matrices de vulnerabilidad.	Correo electrónico	
	4	**Política de Seguridad y Privacidad de la Información**	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Suite Visión Empresarial Página Web	
	5	**Política de Seguridad y Privacidad de la Información**	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Suite Visión Empresarial Página Web	
	6	**Política de Seguridad y Privacidad de la Información**	Procedimientos documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Suite Visión Empresarial	

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

	7	**Roles y responsabilidades de seguridad y privacidad de la información.**	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Suite Visión Empresarial Página Web	
	8	**Inventario de activos de información**	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.	Correo electrónico	
	9	**Inventario de activos de información**	Matriz con la identificación, valoración y clasificación de activos de información.	Suite Visión Empresarial	
	10	**Integración del MSPI con el Sistema de Gestión documental**	Integración del MSPI, con el sistema de gestión documental de la entidad.	Visita campo	

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

	11	**Identificación, Valoración y tratamiento de riesgo.**	Documento con la metodología de gestión de riesgos.	Página Web	
	12	**Identificación, Valoración y tratamiento de riesgo.**	Documento con el análisis y evaluación de riesgos.	NA	
	13	**Identificación, Valoración y tratamiento de riesgo.**	Documento con el plan de tratamiento de riesgos.	Página Web	
	14	**Identificación, Valoración y tratamiento de riesgo.**	Documento con la declaración de aplicabilidad.	Suite Visión Empresarial	
	15	**Plan de comunicaciones**	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Correo electrónico	
	16	**Planificación y Control Operacional.**	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	NA	
	17	**Implementación del plan de tratamiento de riesgos.**	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	NA	

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

18	**Indicadores De Gestión.**	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	NA	
19	**Plan de revisión y seguimiento, a la implementación del MSPI.**	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Correo electrónico	
20	**Plan de Ejecución de Auditorias**	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	NA	
21	**Plan de mejora continua**	Documento con el plan de mejoramiento.	NA	
22	**Plan de mejora continua**	Documento con el plan de comunicación de resultados	NA	

1. **Resultado del análisis correspondiente a la Herramienta de Diagnóstico Seguridad y Privacidad de la Información.**

Teniendo en cuenta que el objetivo fundamental del Diagnóstico Seguridad y Privacidad de la Información es la medición correspondiente al avance de la gestión en la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), la Oficina de Control Interno durante el desarrollo de la auditoría evidenció:

- El instrumento que actualmente tiene la Superintendencia de Vigilancia y Seguridad Privada para adelantar el autodiagnóstico del modelo de Seguridad y Privacidad de la Información, se encuentra desarrollado en la versión de la norma ISO 27001 2013 adoptada por la Alta Consejería Distrital de TIC, sin embargo, al cotejar la información de la guía expuesta por el Ministerio de Tecnologías de la Información y Comunicaciones, se observa que la entidad a la fecha de la auditoria (27 de diciembre de 2021) no está utilizando el instrumento de evaluación del MSPI definido por el MINTIC para evaluar el nivel de implementación del mismo, el cual se puede consultar en el siguiente

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

enlace https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/ y hace parte del Anexo 1 de la Resolución 00500 de marzo 10 de 2021.

- Una vez el equipo auditor revisa la herramienta autodiagnóstico para la implementación del SGSI, evidencia que en las pestañas GAP Logro1, GAP Logro2, GAP Logro3 se encuentran detalladas las actividades para la implementación de cada uno de los dominios del sistema, en ellos, a partir de una pregunta especifica se entrega una valoración (Cumple satisfactoriamente, Cumple parcialmente, no cumple), se especifica una evidencia y una recomendación. Sin embargo, la casilla evidencias no contiene referencia a una ubicación web o del sistema de información institucional donde se vea el documento, informe, herramienta, instrumento o similar que permita verificar su cumplimiento.

La situación anteriormente evidenciada constituye un riesgo para la implementación del SGSI y MSPI debido a que toda la información producida por el personal encargado debe reposar en un sistema unificado que permita su posterior consulta para entes externos e internos, de conformidad con las disposiciones señaladas en la Ley 1712 de 2014 y la Resolución 1519 de 2020, las cuales determinan los parámetros para la publicación y actualización de información pública.

La tabla numero 2 revela el nivel de madurez - instrumento autodiagnóstico realizado por la Oficina de Sistemas.

Tabla N° 2. Avance SGSI Logros – Fases – Metas

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	22,9%
LOGRO2	HACER	40%	30,6%
LOGRO3	VERIFICAR	15%	8,8%
	ACTUAR	15%	12,5%
	TOTAL	100%	74,8%

Fuente: Instrumento Autodiagnóstico Supervigilancia

Teniendo en cuenta que no existen soportes que evidencien el nivel de madurez de la implementación del MSPI, la Oficina de Sistemas debe realizar las acciones de mejora que subsanen lo evidenciado e incluirlo en el plan de mejoramiento para posterior seguimiento por parte de la Oficina de Control Interno.

2. Informe técnico autodiagnóstico modelo SGSI.

Considerando que el objetivo principal del autodiagnóstico de Seguridad y Privacidad de la información es definir en su primera fase la Evaluación del desempeño del Modelo (MSPI), el cual me permite identificar el estado de avance de implementación que tiene la entidad con respecto a los requerimientos exigidos en la resolución 00500 de marzo 10 de 2021 y demás normas reglamentarias, a continuación, se hacen las siguientes observaciones:

Una vez analizado el "*INFORME TÉCNICO AUTODIAGNOSTICO MODELO DE SGSI 2021",* realizado por la entidad, el cual fue remitido a la Oficina de Control Interno a través de correo electrónico institucional por el área auditada, el equipo auditor

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

observó que el mismo contiene un apartado de recomendaciones y conclusiones, en las cuales se resume el trabajo desarrollado en términos de implementación del SGSI en la Supervigilancia; sin embargo, las actividades que describen hacen alusión a las acciones de mejora para cada uno de los dominios del sistema, los cuales no se encuentran enmarcados en un plan tipo matriz que permita realizar el seguimiento y control por parte tanto de la dependencia como de la Oficina de Control Interno o entes externos de control.

Por otra parte, y teniendo en cuenta la imagen Numero 1, por medio de la cual la entidad expone el grado de avance por dominios de control:

Imagen No 1. Avances por dominio de control

Fuente: Informe técnico autodiagnóstico modelo SGSI Supervigilancia.

Según los dominios definidos por la herramienta autodiagnóstico para la implementación del SGSI, se indica que las franjas de color amarillo representan el avance en términos de cada uno de estos y su aproximación a la meta estimada, representada en color gris.

La imagen No 2 muestra los controles establecidos por cada uno de los dominios señalados por herramienta autodiagnóstico de SGSI:

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Imagen 2. Controles establecidos por dominio

POR DOMINIO DE CONTROL						
NOMBRE DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	PESO CONTROLES IMPLEMENTADOS Y PARCIALMENTE IMPLEMENTADOS	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	2	2	2	0	0	0
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7	5	3	4	0	0
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	6	5	4	2	0	0
DOMINIO 8 - GESTIÓN DE ACTIVOS	9	5,5	2	7	0	1
DOMINIO 9 - CONTROL DE ACCESO	14	10	6	8	0	0
DOMINIO 10 - CRIPTOGRAFÍA	2	1,5	1	1	0	0
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	15	15	15	0	0	0
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	14	10	6	8	0	0
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	7	4	1	6	0	0
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	13	11	9	4	0	0
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	5	2,5	0	5	0	0
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA	7	7	7	0	0	0
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	4	2	0	4	0	0
DOMINIO 18 - SEGURIDAD DE LAS COMUNICACIONES	8	6	4	4	0	0
	113		**60**	**53**	**0**	**1**

Fuente: Informe técnico autodiagnóstico modelo SGSI Supervigilancia.

De acuerdo con lo anterior, se observa que la Supervigilancia tiene aplicados un total de 113 controles según cada uno de los dominios para la implementación del SGSI, sin embargo, se observa que la implementación de 60 controles está en un 100%, 53 controles con implementación parcial y 1 control relacionado con la gestión de activos no aplica.

La Oficina de Sistemas debe gestionar a través del plan de seguridad de la información, el plan estratégico de TI (PETI), el plan de tratamiento de riesgos y demás instrumentos una hoja de ruta que permita realizar el seguimiento y el control de las actividades referenciadas, permitiendo encauzar en un solo mapa la búsqueda de implementación del sistema SGSI y el MSPI, lo anterior teniendo en cuenta que el informe no permite realizar seguimientos ni establecer los controles adecuados que conlleven a la implementación satisfactoria del modelo.

La situación anteriormente evidenciada debe ser incluida en el plan de mejoramiento para posterior seguimiento por parte de la Oficina de Control Interno.

3. Política de seguridad de la información

El equipo auditor revisó y analizó la política general de seguridad de la información expedida por la Supervigilancia a través de la resolución *20171400016907,* la cual se encuentra disponible en el sistema Suite Vision Empresarial y en la página web de la Supervigilancia, sin embargo, la misma se encuentra desactualizada teniendo en cuenta los nuevos desafíos que desde el Estado se proponen con documentos como el CONPES 3995, política nacional de confianza y seguridad digital y demás normas vigentes reglamentarias que rigen la materia.

Así mismo, es importante que el funcionario y/o contratista asignado a desempeñar funciones o actividades relacionadas con el rol de oficial de seguridad de la información, no haga parte del equipo de trabajo de la Oficina de Sistemas, lo anterior teniendo en cuenta que las funciones del mismo se encuentran claramente definidas en la guía de Gobierno Digital actualizada por MINTIC en el 2019, que a la letra dice: *"Responsable de Seguridad de la Información: Atendiendo a la necesidad de articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación*

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

de las políticas en materia de Seguridad de la Información, incluyendo la Seguridad Digital, en la respectiva entidad, se debe designar un Responsable de Seguridad de la Información que a su vez responderá por la Seguridad Digital en la entidad, el cual debe pertenecer a un área que haga parte del direccionamiento estratégico o Alta Dirección (MIPG, 2017); Así mismo, *"El responsable de Seguridad de la información será el líder del proyecto, escogido dentro del equipo designado en cada entidad y tendrá las responsabilidades establecidas en la guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información (Guía 4 - Roles y Responsabilidades), quien, a su vez, tiene responsabilidades asignadas dentro de cada dominio del Marco de Arquitectura Empresarial.* ***El responsable de seguridad de la información deberá participar en los comités de desempeño institucional****." (Negrilla y subrayado fuera de texto)*

La situación presentada genera un hallazgo el cual debe ser incluido en el plan de mejoramiento para posterior seguimiento por parte de la Oficina de Control Interno, toda vez que la Supervigilancia debe actualizar su política general para la implementación de la seguridad de la información como parte integral de los procesos, teniendo en cuenta las nuevas disposiciones emitidas por el Estado en ocasión de los cambios en transformación digital, la nueva realidad de las tecnologías emergentes, entre otras sucedidas desde 2017, fecha de firma del documento en mención. Adicionalmente, el oficial de seguridad debe hacer parte del comité institucional de Gestión y Desempeño.

4. Organización documentos SGSI-MSPI

El equipo auditor realizó el cotejo y análisis de los documentos relacionados con la implementación del Sistema de Seguridad de la Información SGSI, frente a lo que se encuentra publicado a través del sistema Suite Visión Empresarial, es de aclarar que los documentos deben estar incluidos dentro del proceso denominado SGSI, lo anterior teniendo en cuenta que hacen parte integral de dicho sistema y no como actualmente que se evidencia su ubicación en dos procesos: en gestión de sistemas e información y en Sistema de Gestión y Seguridad de la información, situación que refleja desorden conceptual en cuanto a que la Oficina de Sistemas tiene a su cargo unos componentes enfocados a la gestión tecnológica desde la visión de sistemas, servicios, infraestructura, estrategia, gobierno y proyectos TI y por otra parte, la seguridad de la información está enfocada en los activos de información, gestión de riesgos, controles, aplicabilidad, entre otros aspectos, situación que evidencia duplicidad y desorden en el cargue de la información en virtud de que los documentos no se encuentran archivados de acuerdo a los lineamientos establecidos en el sistema de Gestión de Calidad implementado por la Supervigilancia.

A continuación, se relacionan los documentos que se describen en la imagen No 4, la cual hace alusión a lo anteriormente descrito:

- Declaración de aplicabilidad
- Documento de confidencialidad APO, SEVEN, RENOVA Y ESIGNA
- Instructivo - Aplicativo
- Matriz de roles y privilegios
- Registro de incidencias aplicativos livianos
- Registro general de incidentes de seguridad de información
- Reporte de incidente de seguridad de la información
- Solicitud de cambio – RFC
- Manual de política de gestión de disponibilidad respecto a los servicios TI
- Manual de política de seguridad de la información
- Política de protección de datos personales GSI
- Política de seguridad de la información
- Activos de seguridad de la información

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Imágen 4. Documentos proceso gestión de sistemas e información

Fuente: Suite Visión empresarial

5. Manual de políticas de seguridad de la información

El equipo auditor evidenció que la entidad cuenta con el manual de políticas de seguridad y privacidad de la información, el cual cumple con los lineamientos establecidos en la Guía No.2 Elaboración de la política general de seguridad y privacidad de la información V2 del MSPI, que a la letra dice: "*establecer, implementar, mantener, mejorar y socializar el Sistema de Gestión de Seguridad de Información - SGSI basado en la política de Gobierno Digital y la norma ISO/IEC 27001:2013, alineado al cumplimiento de los objetivos estratégicos de la Supervigilancia."* Así mismo, el documento "*define los criterios y comportamientos que deben seguir todos los funcionarios, contratistas, terceros o cualquier persona que tenga una relación contractual con la Supervigilancia, o que tenga acceso a los activos de información y al SGSI.".* Se precisa, que el documento se encuentra actualizado en su versión N° 10 aprobado por el Sistema de Gestión de Calidad MAN-GSI-140-029, y el mismo se encuentra en la página web de la Supervigilancia y en el sistema Suite Visión Empresarial.

5.1 Sanciones por incumplimiento que se ven reflejadas en el manual de la política de seguridad de la información.

Es de anotar que según lo estipulado en el numeral 3 del Manual de Política de Seguridad de la Información, el cual describe: *"Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente política de seguridad, conforme a lo dispuesto por las normas estatutarias escalafonarias y convencionales que rigen al personal del Sector Defensa y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes. Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga, cumpliendo las formalidades impuestas por los preceptos constitucionales, la ley de procedimientos administrativos y demás normativas específicas aplicables. Además de las sanciones disciplinarias o administrativas, la persona que no da debido cumplimiento a sus obligaciones puede incurrir*

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

también en responsabilidad civil o patrimonial, cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el código penal y leyes especiales."

Aunque la entidad cuenta con el manual de política de seguridad de la información, el mismo no contiene la descripción de las sanciones, protocolos y responsables en caso de que se presente un incumplimiento por las partes interesadas.

Por otra parte, es de señalar que una vez realizada la trazabilidad en las diferentes plataformas que tiene establecidas la Supervigilancia para consulta, no se evidenció la resolución de implementación del manual, el cual se encuentra desactualizado.

Lo evidenciado genera un hallazgo el cual debe ser incluido en el plan de mejoramiento para posterior seguimiento por parte de la Oficina de Control Interno.

5.2 Roles y responsabilidades de seguridad y privacidad de la información.

Siguiendo con el análisis del manual, se evidencia que el numeral 7 contiene los roles y responsables de la implementación y puesta en marcha del sistema así:

- Comité Institucional de Gestión y Desempeño
- Alta Dirección
- Jefes
- CIO (jefe de la Oficina de Informática y Sistemas)
- Oficial de Seguridad de la Información
- El Gestor de Información
- Todos los funcionarios
- Custodios de información
- El propietario de la Información (El líder o propietario del proceso)
- Oficina de Recursos Humanos
- Oficina de Control Interno
- Funcionarios, contratistas y terceros

5.3 Confusión de roles y responsabilidades

Cabe señalar que el Manual de Política de Seguridad de la Información que tiene implementado la Supervigilancia, no contempla la independencia en lo referente al rol y responsabilidad que tiene tanto el Oficial de Seguridad de la Información como el Jefe de la Oficina de Sistemas (CIO), contexto que tiende a confundir dichos roles y responsabilidades en la implementación de la estrategia TI y del SGSI-MSPI, tal como se mencionó en el punto 5 del cuerpo del presente informe.

Lo anterior genera un riesgo, toda vez que el CIO debe ejercer dentro de los roles y responsabilidades funciones estratégicas en el cumplimiento de los dominios de arquitectura empresarial que en su versión 2. ha definido MINTIC como una arquitectura de seguridad de la información, mientras que el Oficial de Seguridad de la Información, hace parte de la implementación de todo el sistema, el modelo y la arquitectura de referencia.

La entidad debe establecer directrices que permitan a estos dos roles ser complemento para apalancar las estrategias de TI y del SGSI-MPSI.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

Es de señalar que lo observado genera un hallazgo, el cual deberá ser incluido en el plan de mejoramiento para posterior seguimiento de la Oficina de Control Interno.

6. Matriz Inventario de activos de información

Resultado del análisis correspondiente a la matriz de inventarios de activos de información, se observa que la misma contiene los campos reflejados en la imagen No 5, sin embargo, la matriz no detalla la información relacionada con la infraestructura crítica, situación que contraviene con lo estipulado en el numeral 11.3 Guía inventario clasificación de activos e infraestructura critica, que hace parte del anexo 1, que contempla la Resolución 00500 de 2021.

Imagen 5. Encabezados matriz de activos de información

REGISTRO DE ACTIVOS DE INFORMACION SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA							
CATEGORÍAS O SERIES DE INFORMACIÓN:	NOMBRE O TÍTULO DE LA INFORMACIÓN	DESCRIPCIÓN DE LA INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE:	FORMATO	INFORMACIÓN	
						DISPONIBLE	PUBLICO

Fuente: Matriz de inventario de activos de información

Es de señalar que lo observado genera un hallazgo, el cual deberá ser incluido en el plan de mejoramiento para posterior seguimiento de la Oficina de Control Interno.

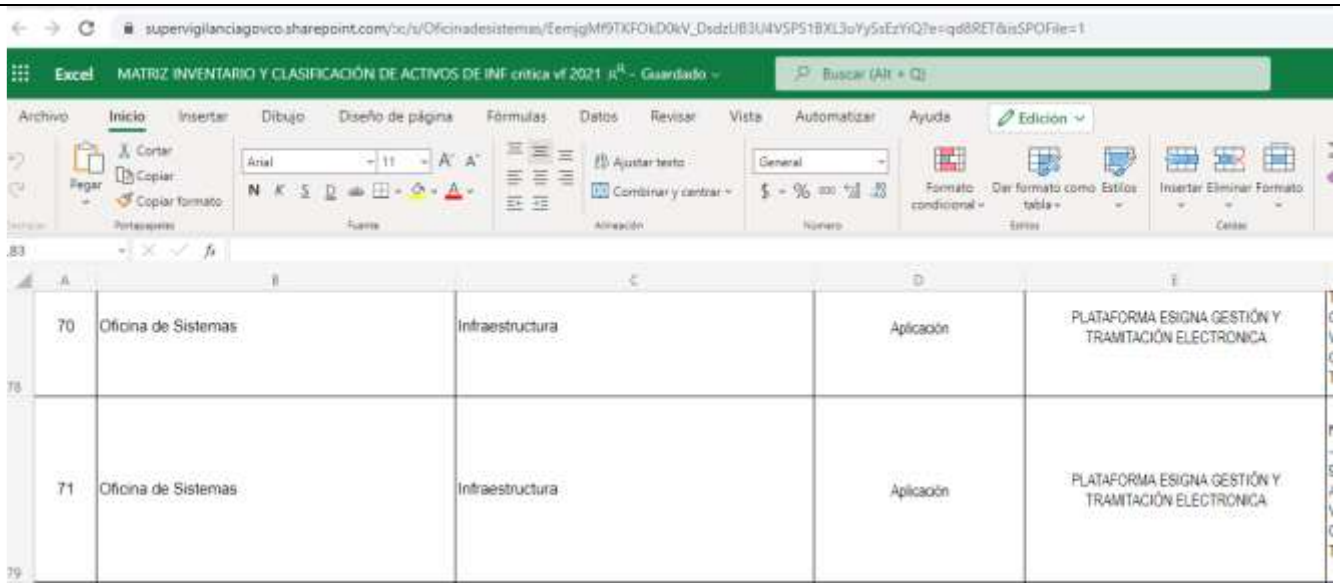
Respuesta dada por la Oficina de Sistemas.

Durante la auditoria se dio a conocer al Sr. auditor que sí contamos con la matriz de activos de información infraestructura crítica de la entidad 2021, esta información no está publicada por temas de seguridad. La matriz se encuentra en la documentación de Oficina de Sistemas - Seguridad de la Información. En la siguiente dirección.

https://supervigilanciagovco.sharepoint.com/:x:/s/Oficinadesistemas/EemjgMf9TKFOkD0kV_DsdzUB3U4VSPS1BXL3uYySsEzYiQ?e=qd8RET&isSPOFile=1

Puesto que esta matriz es confidencial, se adjunta pantallazo a continuación del contenido del enlace y de que si existe.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	



70	Oficina de Sistemas	Infraestructura	Aplicación	PLATAFORMA ESIGNA GESTIÓN Y TRAMITACIÓN ELECTRONICA
71	Oficina de Sistemas	Infraestructura	Aplicación	PLATAFORMA ESIGNA GESTIÓN Y TRAMITACIÓN ELECTRONICA

Respuesta Oficina de Control Interno

Frente al argumento planteado por la Oficina de Sistemas, el equipo auditor afirma que en la visita de auditoria en campo realizada el día 01 de diciembre de 2021, no se logró evidenciar el detalle de la Infraestructura critica de la Superintendencia de Vigilancia y Seguridad Privada en la matriz de activos de información expuesta en esa reunión por parte de la Oficina de Sistemas a los auditores de la Oficina de Control Interno.

La Oficina de Control Interno valora que la Oficina de Sistemas cuente al día de hoy con la evidencia para dar cumplimiento a la situación planteada, pero la misma no fue aportada en los tiempos establecidos, por lo tanto, se ratifica el hallazgo identificado en el cuerpo del informe, el cual debe ser incluido en el plan de mejoramiento para posterior seguimiento de la OCI.

6.1 Diligenciamiento de la matriz de activos de información

Siguiendo con el análisis de la matriz de activos de Información, se evidencia que no han sido tenidas en cuenta algunas consideraciones y definiciones expuestas en el anexo 1, complemento de la resolución 00500 de 2021, modelo de seguridad y privacidad de la información, versión 4 con fecha 22/02/2021, numeral 11.3 Guía inventario clasificación de activos e infraestructura critica. Sobre esto se debe hacer énfasis en la información básica del activo, su tipificación, este aspecto es muy importante porque activos de información no hace referencia únicamente a documentos físicos o digitales, existe hardware, software, recurso humano, servicios e instalaciones que se pueden considerar en esta clasificación, incluyendo además la infraestructura critica cibernética nacional.

Así mismo los activos deben tener incluida en la matriz una clasificación con los niveles de protección adecuados, con base en sus características particulares. La guía cita lo siguiente: *"Para cada propiedad se establecieron criterios específicos y lineamientos para el tratamiento adecuado del activo. Así mismo en esta guía se definieron tres (3) niveles que permiten determinar el valor general o criticidad del activo en la entidad (es importante aclarar que los niveles pueden ser definidos a*

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

*criterio de la entidad): Alta, Media y Baja, con el fin identificar qué activos deben ser tratados de manera prioritaria."*Para ello se deben especificar los tipos de información: publica reservada, publica clasificada o información pública, definidas en el anexo y en la ley 1712 de 2014.

La situación anteriormente evidenciada constituye un riesgo, toda vez que, si no están identificados los activos de información, el ejercicio de gestión de riesgos y especificación de controles no tiene consistencia ya que no están siendo protegidos en su totalidad. De igual forma el equipo auditor sugiere hacer uso de los instrumentos divulgados por MINTIC para la formulación del inventario de activos de información siguiendo los parámetros que permitan tener equilibrio en cada uno de los tipos de clasificación para la información, unido a los conceptos derivados de arquitectura de información donde se especifican componentes, ciclos de vida y procesos para la gestión de estos como parte fundamental para la Supervigilancia.

Es de señalar que lo observado genera un hallazgo, el cual deberá ser incluido en el plan de mejoramiento para posterior seguimiento de la Oficina de Control Interno.

6.2 Aplicación Instructivo activos de información

Una vez que el equipo auditor revisa el instructivo diligenciamiento matriz inventario y clasificación de activos de información, y el formato matriz identificación, valoración, clasificación y etiquetado de la información, se evidencia que el mismo no tiene relación con la matriz de activos de la información previamente expuesta. Lo anterior genera un riesgo toda vez que el instrumento que debe ser usado es el que acompaña la resolución 500 de 2021 para la identificación de activos.

Es de señalar que los documentos en referencia, deben ser puestos en uso lo más pronto posible ya que al no tener claridad con el levantamiento de activos de información, difícilmente podrán ser protegidos a través de controles logrados por el análisis de riesgo, comprometiendo imagen, reputación, información de la entidad y los ciudadanos usuarios de esta.

Respuesta dada por la Oficina de Sistemas

El instructivo de diligenciamiento presentado esta realizado de acuerdo a lo estipulado en el anexo 1 de la resolución 500 de 2021 para identificación de activos, siendo esta la misma metodología que se indica en Guía para la Gestión y Clasificación de Activos de Información. Guía No. 5 MINTIC. La idea de la elaboración y publicación del instructivo, es facilitar el entendimiento y dar claridad al usuario de como diligenciar la matriz de activos de información explicando campo por campo y cuál debe ser su contenido.

Respuesta Oficina de Control Interno

Se aceptan las explicaciones dadas por el área auditada y se recomienda que la Oficina de Sistemas actualice el instructivo cada vez que se modifique la matriz.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

7. Metodología de gestión de riesgos

Revisada y cotejada la metodología implementada por la Supervigilancia para la administración de riesgos, el equipo auditor observa que la misma se encuentra acorde con los lineamientos emitidos por el Departamento Administrativo de la Función Pública y el Ministerio de Tecnologías de la Información y las comunicaciones

Es de señalar que el documento contiene las responsabilidades enmarcadas en las líneas de defensa, los escenarios de riesgos donde se incluyen desastres tecnológicos y ciberataques y los criterios para definir el nivel de probabilidad e impacto sobre el nivel de ocurrencia y su porcentaje, además determinan las afectaciones económicas y reputacionales. Señalan además, las frecuencias de probabilidad y su porcentaje, miden el nivel de aceptación del riesgo y su tratamiento. Además de esto, indican el plan de acción para desarrollar la política de administración sobre los riesgos, el proceso de seguimiento y evaluación. Por último, definen las herramientas para su gestión.

8. Plan de tratamiento de riesgos en seguridad de la información.

Revisado y analizado el plan de tratamiento de riesgos en seguridad de la información, que tiene implementado la Supervigilancia, el equipo auditor evidenció que este documento no cumple con la estructura que debe tener un plan institucional, lo anterior teniendo en cuenta que el mismo no identifica las actividades correspondientes al componente de SGSI y/o MSPI. Cabe señalar, que el plan implementado actualmente en la entidad está diseñado como una matriz y no como un documento que permita establecer herramientas para realizar el seguimiento, control y cumplimiento del mismo. (Ver imagen N° 6)

Imagen N° 6. Plan de tratamiento de riesgos en seguridad de la información

ENTIDAD	SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA
PLAN ESTRATÉGICO INSTITUCIONAL	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

POLITICA INSTITUCIONAL	OBJETIVO INSTITUCIONAL	RESPONSABLE OBJETIVO	ESTRATEGIA	ACTIVIDAD	META ANUAL	SEGUNDO TRIMESTRE		TERCER TRIMESTRE		CUARTO TRIMESTRE		FECHA DE INICIO	FECHA FIN	RESPONSABLE	PRESUPUESTO
						TAREA	ENTREGABLES	TAREA	ENTREGABLES	TAREA	ENTREGABLES				
3. EFICIENCIA ADMINISTRATIVA Y GESTION FINANCIERA	3.3. Realizar la integración de los sistemas de información para la reducción en el consumo de papel, fortalecer la seguridad, oportunidad en el uso de información y trazabilidad	Oficina de Sistemas	Gobierno Digital / ISO 27001:2013 / Gestión de riesgos	Elaborar matriz de riesgos de Seguridad de la Información	Monitorar exposición de riesgos de seguridad de la información	Actualizar matriz de riesgos de SI	Matriz de riesgos de SI actualizada	Actualizar matriz de riesgos de SI	Matriz de riesgos de SI actualizada	Actualizar matriz de riesgos de SI	Matriz de riesgos de SI actualizada	15/03/2022	31/12/2022	OSI (Oficial de Seguridad de la Información)	
				Realizar el levantamiento de riesgos de seguridad de la información	Monitorar exposición de riesgos de seguridad de la información	Identificar riesgos de SI	Riesgos identificados y actualizados	Identificar riesgos de SI	Riesgos identificados y actualizados	Identificar riesgos de SI	Riesgos identificados y actualizados	15/03/2022	31/12/2022	OSI (Oficial de Seguridad de la Información)	
				Elaborar el plan de tratamiento de riesgos de seguridad de la información	Monitorar exposición de riesgos de seguridad de la información					Realizar y aplicar plan de tratamiento de riesgos	Plan de riesgos ejecutado	15/03/2022	31/12/2022	OSI (Oficial de Seguridad de la Información)	
				Revisar del plan de tratamiento de riesgos de seguridad de la información	Monitorar exposición de riesgos de seguridad de la información	Actualizar planes de tratamiento de riesgos		Actualizar planes de tratamiento de riesgos		Actualizar planes de tratamiento de riesgos	Plan de riesgos actualizado	15/03/2022	31/12/2022	OSI (Oficial de Seguridad de la Información)	
				Actualizar los activos de información	Monitorar la exposición de activos de información			Actualizar activos de información y designar sus responsables	Matriz de activos de información actualizada	Solicitar a las áreas la presentación y cambios en los responsables de los activos	Matriz actualizada con los responsables de los activos	15/03/2022	31/12/2022	OSI (Oficial de Seguridad de la Información)	
				Realizar la clasificación de confidencialidad, integridad y disponibilidad de la información	Información de la SVSP clasificada y actualizada			Revisar privilegios y clasificación de la información	Matriz con privilegios revisados			15/03/2022	31/12/2022	OSI (Oficial de Seguridad de la Información)	

Fuente: Plan de tratamiento de riesgos

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

El plan de tratamiento de riesgos está definido por la norma ISO 27001:2013, en el se muestran las actividades que permitan elaborar una matriz de información tomando como entrada la definición de activos de información, para luego desarrollar un listado de riesgos los cuales deben generar diferentes acciones desde el punto de vista de controles para garantizar su confidencialidad, integridad y disponibilidad.

Lo anterior debe ser incluido en el plan de mejoramiento para posterior seguimiento por parte de la Oficina de Control Interno.

9. Declaración de aplicabilidad

Una vez que el equipo auditor revisa el plan de tratamiento de riesgos en seguridad de la información, se evidencia que la no existe una materialización de controles a partir de actividades detalladas y evidencias que muestren su implementación, así como la definición de una estrategia de comunicaciones a partir de piezas gráficas, capacitaciones, entre otros, para la apropiación de los controles dentro de la supervigilancia, además no se observa una conexión entre la definición de los riesgos y los controles especificados en la declaración de aplicabilidad, lo cual puede generar confusión al momento de crear sinergias entre los diferentes instrumentos que están siendo desarrollados por el equipo de trabajo en materia de seguridad de la información.

Adicionalmente, la matriz denominada declaración de aplicabilidad versión 1.0 de junio de 2018, que se encuentra publicada en el sistema Suite Visión empresarial, debe ser ajustada y actualizada de acuerdo a las nuevas disposiciones en materia de seguridad de la información dispuestas al interior de la Supervigilancia y los demás entes reguladores.

Lo anterior debe ser incluido en el plan de mejoramiento para posterior seguimiento por parte de la Oficina de Control Interno.

10. Gestión y tratamiento de vulnerabilidades

Se llevó a cabo la revisión de los documentos entregados vía correo electrónico el jueves 09 de diciembre de 2021 por parte de la oficina de sistemas relacionados con la gestión de vulnerabilidades adelantada por la Supervigilancia. El primer documento revisado con nombre *“acta con resumen de actividades y evidencias de las actividades realizadas para prevención de seguridad de la información – paro nacional mayo 4 de 2021”*, da cuenta de un ejercicio preventivo en ocasión a los sucesos presentados por la intrusión de sitios gubernamentales durante las jornadas de protesta. De acuerdo a lo señalado en el documento, se realizaron cierre de puertos, aplicación de factores de doble autenticación y monitoreo a la infraestructura en búsqueda de actividades sospechosas.

En este mismo sentido, el equipo auditor revisó el documento con nombre informe de equipo financiera, en este se muestra la revisión sobre el acceso físico a las oficinas del equipo de financiera y revisión de los equipos de cómputo, destinados para pagos virtuales. En esta actividad se verifica que se tenga el sistema operativo de los equipos actualizado, así como el agente antivirus. Además, activación de aplicativos, borrado de cookies, verificación de programas instalados, bloqueo a registro del sistema operativo, así como puertos usb y verificación de conexión a Internet.

Una vez que el equipo auditor revisa los documentos relacionados con ejercicios para el análisis y mitigación de vulnerabilidades, se evidencia que esto debe ser llevado a una matriz de vulnerabilidades que permita en el tiempo, trazar un mapa de ruta para la prevención a partir de ejercicios como los realizados y expuestos en los documentos por el equipo de trabajo. La Supervigilancia debe utilizar los instrumentos brindados por las normas internacionales y en este caso, por MINTIC, con relación a la gestión de vulnerabilidades a través de la identificación de activos, riesgos, amenazas,

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

vulnerabilidades y controles de forma unificada y a través de planes que tracen las actividades que permitan un mayor control sobre la operación del SGSI y el MSPI. Los detalles al respecto pueden ser consultados en la Guía de gestión de riesgos publicada por MINTIC, versión 3.0.0 del 01/04/2016.

Lo evidenciado debe ser incluido en el plan de mejoramiento para posterior seguimiento por parte de la Oficina de Control Interno.

11. Plan de comunicaciones

Una vez que el equipo auditor revisa las evidencias suministradas por la Oficina de Sistemas a través de correo electrónico tales como: Actas correspondientes a las diferentes capacitaciones realizadas a través de la plataforma Ms Teams, las cuales hacen alusión al plan de comunicaciones para el SGSI-MSPI, se observa que estas no tienen relación con el plan de comunicaciones, teniendo en cuenta que el mismo debe contener la estrategia y actividades para la socialización y apropiación de la seguridad de la información en la entidad, describiendo las actividades que permitan lograr el objetivo del plan en mención, recursos y responsables

Lo anterior debe ser incluido en el plan de mejoramiento para posterior seguimiento por parte de la Oficina de Control Interno.

12. Plan anual de trabajo SGSI 2021

Revisado y analizado el Plan de trabajo SGSI, el equipo auditor evidenció que el encabezado del formato contiene:

- Actividades
- Responsables
- Periodicidad (meses de cumplimiento)
- Recursos
- Entregables
- Observaciones.

Se precisa que la fecha de elaboración del documento es del mes de junio de 2021, lo que permite observar que la Oficina de Sistemas entre el periodo comprendido de enero a mayo de 2021, no realizó ninguna actividad relacionada con la implementación del SGSI, de igual manera, el mismo no tiene actividades de apropiación y sensibilización de los temas de seguridad de la información.

Cabe señalar, que el plan de acción debe ser trazado y publicado al inicio del año, con el fin de medir el porcentaje de avance de las actividades formuladas y realizar el seguimiento a través de informes de ejecución, lo anterior en cumplimiento de lo establecido el artículo 2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción del decreto 612 de 2018 que a la letra dice: "*Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año"*

Lo observado genera un hallazgo, el cual deberá ser incluido en el plan de mejoramiento para posterior seguimiento de la Oficina de Control Interno.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

13. Observación Final

Revisada la documentación, instrumentos y demás elementos entregados por la Oficina de sistemas al equipo auditor, se evidencia que no fue suministrado lo siguiente:

- Documento con el análisis y gestión de riesgos
- Integración del MSPI con el sistema de gestión documental
- Informe de la ejecución del plan de tratamiento de riesgos
- Indicadores de gestión de seguridad y privacidad de la información
- Plan de ejecución de auditorias
- Plan de mejoramiento
- Plan de comunicación de resultados

Al no contar con el insumo de la información, la Oficina de Control Interno no pudo validar si la entidad tiene implementado el sistema SGSI-MSPI de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la información y las comunicaciones y el Departamento Administrativo de la Función Pública.

RECOMENDACIONES

La Oficina de Control Interno, recomienda:

- Realizar los ajustes a que haya lugar de acuerdo con los lineamientos establecidos en la Resolución 500 de 2021 y el anexo 1 de la misma, con relación a la implementación del MSPI.
- Desarrollar un plan de trabajo unificado para los temas de seguridad de la información, seguridad digital y seguridad informática, el cual incluya un método para realizar seguimiento y control periódico, evidenciado en entregables.
- Se deben hacer los ajustes a que haya lugar, con el fin de que el Oficial de Seguridad de la información forme parte de la alta dirección o del proceso de planeación.
- Establecer los riesgos del proceso, de acuerdo con las directrices establecidas en la Guía Modelo de Seguridad de la Información MSPI Versión 4 de febrero de 2021.
- Capacitar a funcionarios y/o contratistas, en los temas referentes a seguridad de la información.
- Desarrollar indicadores de gestión del proceso de privacidad y seguridad de la información
- Elaborar el mapa de riesgos de Seguridad Digital.

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	

CONCLUSIONES
• Durante el desarrollo de la auditoría, se evidenciaron presuntos incumplimientos normativos en relación con la implementación del MSPI a través de la normatividad vigente, así mismo, la gestión de riesgos y el levantamiento de activos de información debe ser una de las principales tareas del equipo de trabajo, puesto que son el pilar para el establecimiento de controles y la definición de políticas específicas. • La entidad debe implementar mecanismos que visualicen el trabajo en equipo del rol del oficial de seguridad de la información y el CIO (Chief Information Officer), puesto que cada uno es complemento a partir de las acciones del área de sistemas en relación con los conceptos y acciones que desde seguridad de la información deben permear los proyectos, los sistemas, los servicios y la infraestructura de la entidad, lo cual genera valor en la operación de sistemas, lo anterior en virtud que la transformación digital se convierte en piedra angular para el “nuevo trabajo” que afrontan las entidades estatales.
 **JULIO ANDRES SANCHEZ S.** Auditor Oficina de Control Interno    **MÓNICA AMPARO VARÓN AGUIRRE** Jefe Oficina de Control Interno

FUNCIONARIO O CONTRATISTA	NOMBRE
Tramitado y Proyectado por	Julio Andrés Sánchez S. - Auditor OCI
Revisado para firma por	Mónica Amparo Varón Aguirre – Jefe OCI
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.	