| | | |
|---|---|---|
| **PROCESO**<br>**GESTIÓN DEL SERVICIOS TIC** | **SUBPROCESO**<br>**N/A** | |
| **TIPO DE PROCESO**<br><br>**MISIONAL _____ APOYO __X___ ESTRATÉGICO _____ EVALUACIÓN Y CONTROL _____** | | |
| **ÁREA AUDITADA**<br><br>**OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN** | | |
| **NIVEL: CENTRAL __X__ SECCIONAL ____** | | |
| **UNIDAD AUDITABLE**<br><br>**EVALUAR LA ADOPCIÓN E IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI** | | |
| **TIPO DE AUDITORÍA:**<br><br>**Auditoría Interna __X__ Auditoría de Cumplimiento ___ Auditoría de seguimiento ____**<br>**Auditorías específicas: ____ Auditorías de sistemas o de TIC: ____¿Cuál? _____** | | |
| **LUGAR DE DESARROLLO DE LA AUDITORÍA**<br><br>**Oficinas Nacionales __X__ Gerencia Seccional ____ Oficina Local ____ PAPF ____ Otro ____**<br>**¿Cuál?_____** | | |
| **FORMA DE DESARROLLO DE LA AUDITORÍA: Presencial ____ Remota ____ Mixta __X__** | | |
| **VIGENCIA: 2024** | | |
| **FECHA DE INICIO: 08/04/ 2024** | **FECHA DE FINALIZACIÓN: 30/05/2024** | |
| **TIPO DE INFORME:** | Preliminar ____ Definitivo __X___ | Fecha: 02 de Julio 2024 |

## 1. OBJETIVO

Evaluar la gestión del proceso Gestión de Servicios TIC del Instituto Colombiano Agropecuario (ICA), principalmente el Modelo de Seguridad y Privacidad de la Información –MSPI y la Política de Gobierno Digital, en el marco del Modelo Integrado de Planeación y Gestión -MIPG, conforme a los lineamientos establecidos por el MinTIC.

## 2. ALCANCE

El alcance se definió para el proceso Gestión de Servicios TIC, como responsable de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), desde el periodo comprendido entre el 01 de Enero 2023 al 31 Diciembre 2023 en el del Instituto Colombiano Agropecuario (ICA), teniendo en cuenta los procedimientos del proceso.

*Nota:*
*"Este alcance puede ser extendido a otras vigencias o procedimientos, cuando la Oficina de Control Interno lo considere necesario y podrá verse limitado cuando no se suministre la información solicitada, o se haga de manera parcial"*

## 3. LIMITACIONES AL ALCANCE

No se presentó limitación al alcance frente al periodo comprendido, en evaluar el Modelo de Seguridad y Privacidad de la Información (MSPI) en el marco de la presente auditoría.

**4. CRITERIOS**

- 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 1499 de 2017. "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".
- Decreto 767 de 2022 “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”
- Decreto 338 de 2022 - por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Guía Modelo de Seguridad de la Información MSPI MinTIC Versión 3.0.2 del 29/07/2016 y guías relacionadas.
- Fortalecimiento de la Gestión TI en el Estado - Instrumentos MSPI Modelo de Seguridad y Privacidad de la Información (MSPI)
- Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), tiene por objetivo brindar un marco de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta al momento de llevar a cabo actividades socio económicas en el entorno digital (prestación de trámites, servicios internos y externos, transacciones en línea entre otros) para así, fomentar y mantener la confianza de las múltiples partes interesadas (proveedores, ciudadanos, entidades públicas y privadas) en el uso del entorno digital en su interacción con Estado, impulsando así la prosperidad económica y social del país.
- Guía para la administración del riesgo y el diseño de control en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital Versión 4 del Departamento Administrativo de la Función Pública (DAFP) octubre de 2018.
- Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, Ministerio de Tecnologías de la Información y las Comunicaciones y Departamento Administrativo de la Función Pública (DAFP) 2018.
- Manual de la Política de Gobierno Digital Versión 7 de abril de 2019.
- Norma ISO 27001:2013. Técnicas de seguridad: Sistemas de gestión de la seguridad de la información. Requisitos.
- Resolución No. 500 de 2021 del MinTIC “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”
- Resolución No. 742 de 2022 del MinTIC "Por al cual se fortalece el Modelo de Seguridad y Privacidad de al Información yse definen lineamientos adicionales alos establecidos en al Resolución No. 500 de 2021".

## 5. DESARROLLO DE LA AUDITORÍA

El Instituto Colombiano Agropecuario -ICA, en concordancia con lo dispuesto en el Plan Anual de Auditoria 2024, realizó una evaluación al proceso Gestión del Servicio TIC, principalmente el Modelo de Seguridad y Privacidad de la Información –MSPI y la política de gobierno Digital, en el marco del Modelo Integrado de Planeación y Gestión -MIPG, de acuerdo con los lineamientos y directrices dispuestos por el MinTIC para la adopción del MSPI.

Para el desarrollo de la auditoría, se emplearon técnicas de auditoría, tales como verificación documental del repositorio **(Evidencias MSPI)**, indagación y revisión del avance de la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI en el instituto, teniendo en cuenta los procedimientos de seguridad de la información asociados al proceso, como las directrices y lineamientos de las guías de la biblioteca virtual del MinTIC para fortalecer la gestión TI del ICA. Este análisis se efectuó, de acuerdo con la *ISO 27001:2013 "Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de seguridad de la información*", los criterios y la normatividad vigente del componente de seguridad en la adopción de la Política de Gobierno Digital, en su elemento habilitador "seguridad de la información", verificando el estado y avance efectuado por la entidad en el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el MinTIC, entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en el ICA, alineados con la Resolución 500 de 2021 del MinTIC.

De acuerdo con las anteriores consideraciones, se organizó reunión de apertura el 8 de abril del año que discurre, donde fue presentado el Plan de la Auditoría MSPI y se solicitó información al proceso mediante memorando No.20243107157 de fecha 8 de abril del 2024.

Seguidamente en el marco de la auditoría y dando cumplimiento a las fechas establecidas del Plan de Auditoría MSPI, el 7 de mayo del 2024, se coordinó reunión con el líder del proceso y/o delegados para presentar los ***resultados parciales*** de la evaluación realizada al Modelo de Seguridad y Privacidad de la Información - MSPI en el ICA, permitiendo validar las evidencias y soportes allegados, de conformidad al requerimiento *(Memorando No.20243107157)* y al análisis de los procedimientos del proceso, como las guías, manuales aplicados para adoptar los lineamientos del MSPI en el ICA, de conformidad con las directrices impartidas el MinTIC en la Resolución No. 500 del 2021.

Finalmente, se realizó reunión de cierre de la Auditoría MSPI el 30 de mayo del 2024, donde se presentó los ***resultados finales***, a través de un Papel de Trabajo MSPI, que permitió evaluar el porcentaje de cumplimiento de las metas y resultados del ciclo de operación del Modelo de Seguridad y Privacidad de la Información – MSPI.

### ✓Resultado Evaluación Fina del MSPI ICA

Se realizó una evaluación del modelo (MSPI), evidenciando un 24,444% de avance en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI como se detalla a continuación:

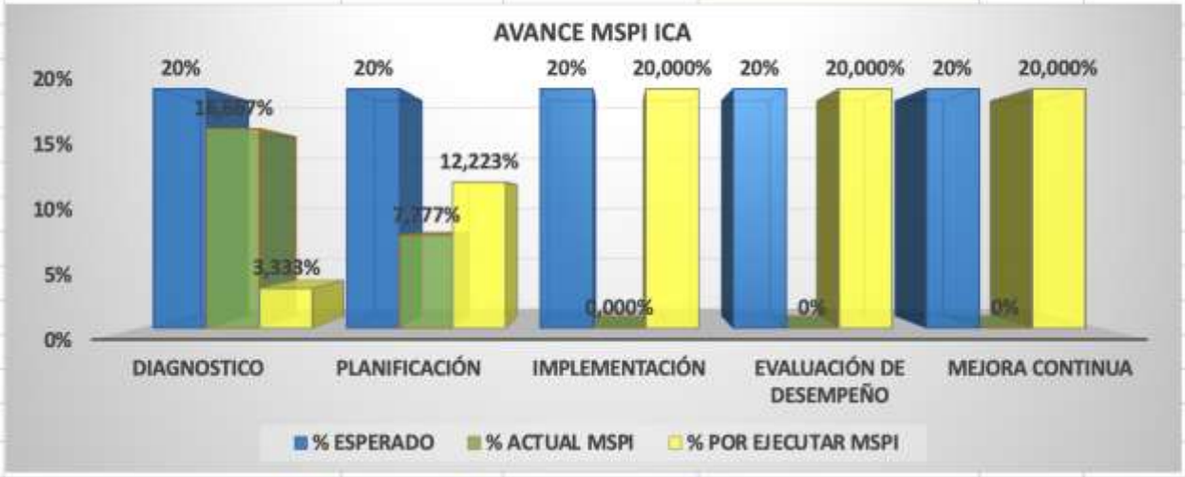
ICA Instituto Colombiano Agropecuario

| CICLOS | FASES MSPI | CUMPLE | | META | % ESPERADO | % ACTUAL MSPI |
|---|---|---|---|---|---|---|
| 1 | DIAGNOSTICO | 1.1 | | 20% | 6,667% | 6,667% |
| | | 1.2 | | | 6,667% | 6,667% |
| | | 1.3 | | | 6,667% | 3,333% |
| 2 | PLANIFICACION | 2.1 | | 20% | 2,222% | 2,222% |
| | | 2.2 | | | 2,222% | 0,000% |
| | | 2.3 | | | 2,222% | 1,111% |
| | | 2.4 | | | 2,222% | 1,111% |
| | | 2.5 | | | 2,222% | 1,111% |
| | | 2.6 | | | 2,222% | 0,000% |
| | | 2.7 | | | 2,222% | 0,000% |
| | | 2.8 | | | 2,222% | 0,000% |
| | | 2.9 | | | 2,222% | 2,222% |
| 3 | IMPLEMENTACIÓN | 3.1 | | 20% | 5% | 0,000% |
| | | 3.2 | | | 5% | 0,000% |
| | | 3.3 | | | 5% | 0,000% |
| | | 3.4 | | | 5% | 0,000% |
| 4 | EVALUACION DE DESEMPEÑO | 4.1 | | 20% | 10% | 0,000% |
| | | 4.2 | | | 10% | 0,000% |
| 5 | MEJORA CONTINUA | 5.1 | | 20% | 20% | 0,000% |
| RESULTADOS MSPI | | | | 100% | 100,00% | 24,444% |

También se observa que el proceso, presenta un porcentaje del **75,556% pendiente por ejecutar** en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI como se detalla a continuación:

**ESTADISTICA FINAL**
**MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI**

| FASES MSPI | % ESPERADO | % ACTUAL MSPI | % POR EJECUTAR MSPI |
|---|---|---|---|
| DIAGNOSTICO | 20% | 16,667% | 3,333% |
| PLANIFICACIÓN | 20% | 7,777% | 12,223% |
| IMPLEMENTACIÓN | 20% | 0,000% | 20,000% |
| EVALUACIÓN DE DESEMPEÑO | 20% | 0% | 20,000% |
| MEJORA CONTINUA | 20% | 0% | 20,000% |
| RESULTADOS MSPI | 100% | 24,444% | 75,556% |



También se observa que de 19 actividades del MSPI, el proceso cumplió cuatro (4), cuatro (4) parcialmente y once (11) no cumplió de acuerdo con la implementación del Modelo de Seguridad y Privacidad de la Información, como se detalla a continuación:

| MSPI | CUMPLE | META | % ESPERADO | % FINAL EJECUTADO | % PENDIENTE POR EJECUTAR | MSPI | ACTIVIDADES MSPI | CUMPLIO | CUMPLIO PARCIAL | NO CUMPLIO |
|---|---|---|---|---|---|---|---|---|---|---|
| 1.1 | SI | 20% | 6,667% | 6,667% | 0,000% | 1.1 | 1 | 1 | | |
| 1.2 | SI | | 6,667% | 6,667% | 0,000% | 1.2 | 2 | 1 | | |
| 1.3 | PARCIAL | | 6,667% | 3,333% | -3,334% | 1.3 | 3 | | 1 | |
| 2.1 | SI | 20% | 2,222% | 2,222% | 0,000% | 2.1 | 4 | 1 | | |
| 2.2 | NO | | 2,222% | 0,000% | -2,222% | 2.2 | 5 | | | 1 |
| 2.3 | PARCIAL | | 2,222% | 1,111% | -1,111% | 2.3 | 6 | | 1 | |
| 2.4 | PARCIAL | | 2,222% | 1,111% | -1,111% | 2.4 | 7 | | 1 | |
| 2.5 | PARCIAL | | 2,222% | 1,111% | -1,111% | 2.5 | 8 | | 1 | |
| 2.6 | NO | | 2,222% | 0,000% | -2,222% | 2.6 | 9 | | | 1 |
| 2.7 | NO | | 2,222% | 0,000% | -2,222% | 2.7 | 10 | | | 1 |
| 2.8 | NO | | 2,222% | 0,000% | -2,222% | 2.8 | 11 | | | 1 |
| 2.9 | SI | | 2,222% | 2,222% | 0,000% | 2.9 | 12 | 1 | | |
| 3.1 | NO | 20% | 5% | 0,000% | -5,000% | 3.1 | 13 | | | 1 |
| 3.2 | NO | | 5% | 0,000% | -5,000% | 3.2 | 14 | | | 1 |
| 3.3 | NO | | 5% | 0,000% | -5,000% | 3.3 | 15 | | | 1 |
| 3.4 | NO | | 5% | 0,000% | -5,000% | 3.4 | 16 | | | 1 |
| 4.1 | NO | 20% | 10% | 0,000% | -10,000% | 4.1 | 17 | | | 1 |
| 4.2 | NO | | 10% | 0,000% | -10,000% | 4.2 | 18 | | | 1 |
| 5.1 | NO | 20% | 20% | 0,000% | -20,000% | 5.1 | 19 | | | 1 |
| RESULTADOS MSPI | | 100% | 100,00% | 24,444% | -75,554% | | 19 | 4 | 4 | 11 |

De acuerdo con lo anterior, se presentan los resultados generales de la evaluación al Modelo de Seguridad y Privacidad de la Información – MSPI, implementado en el ICA el siguiente cuadro:

| CICLO | FASES MSPI | MSPI | ACTIVIDADES | META | RESULTADO | EVIDENCIA | CUMPLIO | CUMPLIO PARCIAL | NO CUMPLIO |
|---|---|---|---|---|---|---|---|---|---|
| 1 | DIAGNOSTICO | 1.1 | 1 | Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. | Diligenciamiento de la herramienta. | SI | 1 | 0 | 0 |
| | | 1.2 | 2 | Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad | Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad. | SI | 1 | 0 | 0 |
| | | 1.3 | 3 | Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación | Documento con los hallazgos encontrados en las pruebas de vulnerabilidad. | PARCIAL | 0 | 1 | 0 |
| 2 | PLANIFICACION | 2.1 | 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. | SI | 1 | 0 | 0 |
| | | 2.2 | 5 | Políticas 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. | NO | 0 | 0 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **2.3** | 6 | Procedimientos de seguridad de la información. | Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional. | PARCIAL | 0 | 1 | 0 |
| | | **2.4** | 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. | PARCIAL | 0 | 1 | 0 |
| | | **2.5** | 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.<br>Matriz con la identificación, valoración y clasificación de activos de información.<br>Documento con la caracterización de activos de información, que contengan datos personales<br>Inventario de activos de IPv6 | PARCIAL | 0 | 1 | 0 |
| | | **2.6** | 9 | Integración del MSPI con el Sistema de Gestión documental | Documento de Integración del MSPI, con el sistema de gestión documental de la entidad. | NO | 0 | 0 | 1 |
| | | **2.7** | 10 | Identificación, Valoración y tratamiento de riesgo. | Documento con la metodología de gestión de riesgos.<br>Documento con el análisis y evaluación de riesgos.<br>Documento con el plan de tratamiento de riesgos.<br>Documento con la declaración de aplicabilidad.<br>**Documentos revisados y aprobados por la alta Dirección.** | NO | 0 | 0 | 1 |
| | | **2.8** | 11 | Plan de Comunicaciones. | Documento con el plan de comunicación, sensibilización y capacitación para la entidad. | NO | 0 | 0 | 1 |
| | | **2.9** | 12 | Plan de diagnóstico de IPv4 a IPv6. | Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. | SI | 1 | 0 | 0 |
| 3 | IMPLEMENTACIÓN | **3.1** | 13 | Planificación y Control Operacional | Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. | NO | 0 | 0 | 1 |
| | | **3.2** | 14 | Implementación del plan de tratamiento de riesgos. | Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. | NO | 0 | 0 | 1 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 3.3 | 15 | Indicadores De Gestión. | Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. | NO | 0 | 0 | 1 |
| | | 3.4 | 16 | Plan de Transición de IPv4 a IPv6 | Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI. | NO | 0 | 0 | 1 |
| 4 | EVALUACION DE DESEMPEÑO | 4.1 | 17 | 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. | NO | 0 | 0 | 1 |
| | | 4.2 | 18 | 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. | NO | 0 | 0 | 1 |
| 5 | MEJORA CONTINUA | 5.1 | 19 | Plan Mejora Continua | Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados. | NO | 0 | 0 | 1 |
| RESULTADOS MSPI (ACTIVIDADES) | | | | | | | 4 | 4 | 11 |

De acuerdo con el anterior análisis estadístico, se evidenció un cumplimiento del 24,444% de ejecución con respecto al desarrollo del ciclo de operación del Modelo de Seguridad y Privacidad de la Información - MSPI implementado en el ICA, lo correspondiente a 19 actividades establecidas en el MSPI, con un cumplimiento de cuatro (4) actividades, cuatro (4) parcialmente y once (11) no cumplidas.

### 5.1 METODOLOGÍA

El Instituto Colombiano Agropecuario-ICA, adoptó el Modelo de Seguridad y Privacidad de la Información – MSPI de MinTIC, el cual define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior del Instituto un Sistema de Gestión de Seguridad de la Información – SGSI y Seguridad Digital, que contemple su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

El Modelo de Seguridad y Privacidad de la Información – MSPI consta de cinco (5) fases las cuales permiten al Instituto gestionar y mantener adecuadamente la seguridad y privacidad de los activos de información. Por ello, el ICA debe abordar las siguientes fases:

1. **Diagnóstico:** Se debe iniciar con un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.
2. **Planificación:** Determina las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

3. **Operación:** La entidad implementa los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. **Evaluación de desempeño:** la entidad determina de qué manera va a ser evaluado la adopción del modelo.
5. **Mejoramiento Continuo**: se establecen procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.


La metodología que se utilizó en el marco de la auditoría, estuvo orientada en evaluar las actividades desarrolladas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información MSPI, lo que le permitirá al ICA mejorar la planeación, administración y gestión de riesgos de seguridad, como la implementación de controles físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno del Instituto, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos.

**5.2 MUESTRA**

*El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales (ISO 27001:2013 "Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de seguridad de la información"), con el objetivo de orientar la gestión e implementacion adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.*

En consecuencia de lo anterior, **no se aplica el muestreo** en esta auditoría, ya que se validaron la totalidad de actividades de las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información - MSPI, teniendo en cuenta las directrices y dispociones dadas en la *Resolución No. 500 de 2021 del MinTIC "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".*

**5.3 FORTALEZAS**

- ✓ Se resalta la disposición, responsabilidad y compromiso de parte de los miembros del proceso de Gestión del Servicio TIC en la ejecución de las diferentes actividades propuestas, así como el acompañamiento en todas las reuniones realizadas para aclarar dudas e inquietudes frente a los requerimientos del auditoria MSPI.
- ✓ Se resalta el sentido de pertenencia y el esfuerzo de los miembros del proceso Gestión del Servicio TIC, en el desarrollo de diseños de artefactos y borradores de procedimientos para avanzar en el proceso de adopción e implementación del MSPI.

**5.4 RESULTADOS**

**Observación No.1**

- ✓ Incumplimiento del *Decreto No. 767 de 2022*, *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital"*, Artículo 2.2.9.1.2.1. Estructura – Habilitadores: 3.*2. Seguridad y Privacidad de la Información, "Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos".* Debido al nivel bajo de ejecución de las actividades desarrolladas por el proceso Gestión del Servicio TIC, de acuerdo con las metas y resultados esperados del ciclo de operación del Modelo de Seguridad y Privacidad de la Información – MSPI, obteniendo un porcentaje total de avance de 24,444%. El porcentaje citado, refleja avances parciales para las fases de diagnóstico y planificación, para el caso de las fases de implementación, evaluación de desempeño y mejora continua no se registró avances, reflejando un bajo nivel de adopción e implementación de lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI en el ICA.

**Recomendación No. 1**

- ✓ Se recomienda al proceso Gestión del Servicio TIC, dar cumplimiento a actividades establecias en las metas y resultados esperados del ciclo de operación de las cinco (5) fases del Modelo de Seguridad y Privacidad de la Información MSPI, lo que permitirá al ICA la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno del Instituto, gestionando de manera eficaz, eficiente y efectiva los activos

de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en el modelo de operación por procesos.

**Observación No. 2**

- ✓ Incumplimiento de la **Resolución No. 500 del 10 de marzo de 2021 de MinTIC**, en su *ARTICULO No. 3. Lineamientos generales "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",* debido a la ausencia y debilidades en los soportes presentados, lo que no permite evaluar de manera integral, la eficacia, eficiencia, calidad de las metas y resultados propuestos en el MSPI.

**Recomendación No. 2**

- ✓ Se recomienda al proceso Gestión del Servicio TIC atender los lineamientos y directrices de las guías 1-21, manuales, instructivos, normatividad y demás documentación relacionada para la adopción y la implementación del MSPI (Biblioteca virtual), con el proposito de fortalecer las capacidades del habilitador de la Politica de Gobierno Digital "Seguridad de la Información" en el ICA, en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

**Observación No. 3**

- ✓ Incumplimiento de la **Resolución No. 500 del 10 de marzo de 2021 del MinTIC**, en su *ARTICULO No. 6 "La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la Entidad"*, de acuerdo con la identificación, valoración y tratamientos de riesgos técnicos (seguridad informática, seguridad digital) y riesgos administrativos del ICA, identificados en las fase de Diagnóstico y Planeación del MSPI, como la declaración de la aplicabilidad y la implementación del plan de tratamiento de riesgos, teniendo en cuenta la definición de controles para mitigar su materialización, de acuerdo con los lineamientos y directrices del MSPI en las guías de Gestión del Riesgo de MinTIC ;Controles de seguridad digital de MinTIC, lo que puede generar materializaciones o afectaciones por debilidades en la administración y gestión de riesgos, como el diseño, ejecución y efectividad de controles de la seguridad de la información y la seguridad digital.

**Recomendación No. 3**

- ✓ Se recomienda al proceso Gestión del Servicio TIC atender los lineamientos y directrices para la administración y gestión del riesgo, como el diseño de controles de seguridad en entidades públicas, este modelo pertenece al habilitador transversal de *Seguridad y Privacidad de la Información*, de la Política de Gobierno Digital y se desarrolla mediante el documento maestro del Modelo de Seguridad y Privacidad de la Información - MSPI y sus guías de orientación. Lo debe desarrollar el líder o encargado de seguridad de la información con el apoyo de toda la estructura organizacional.

## 6. RIESGOS DE LA UNIDAD AUDITABLE:

Los riesgos que tiene el proceso Gestión del Servicio TIC no se materializaron.

En el marco de la auditoria, desde la Oficina de Control Interno (OCI) recomendamos analizar y tener en cuenta los siguientes riesgos que se podrían identificar para actualizar el mapa de riesgo de la unidad auditable y con ello mitigar la posible materialización de situaciones que pueden afectar la buena gestión del proceso, en consecuencia de lo anterior, se detallan los siguientes riesgos a considerar:

- ✓ Afectación reputacional por quejas ocasionadas por la Indisponibilidad de la información necesaria para el cumplimiento de las actividades desarrolladas por los procesos del ICA.
- ✓ Afectación reputacional por quejas ocasionadas por la falta de identificación, clasificación de vulnerabilidades técnicas y administrativas, en la identificación de riesgos su prevención, protección, detección, respuesta, comunicación, recuperación y aprendizaje de los incidentes de seguridad digital que se presenten sobre los activos de información del ICA.
- ✓ Perdida de disponibilidad y confidencialidad de información alojada en activos tipo software o servicios (internos y/o externos).
- ✓ Indisponibilidad de las plataformas tecnológicas del ICA
- ✓ Perdida, daño o fuga de información digital del ICA
- ✓ Incumplimiento de los proyectos y actividades definidas en el Plan Estratégico de Tecnología (PETI)
- ✓ Afectación de la infraestructura tecnológica que soporta los tramites y servicios de la Entidad, asociados con la pérdida de disponibilidad, afectando la continuidad del negocio.

## 7. RECOMENDACIONES GENERALES Y CONCLUSIONES

- ✓ Revisar y ajustar los documentos y/o entregables de implementación del Modelo de Seguridad y Privacidad de la Información -MSPI.
- ✓ Apropiar y aplicar los instrumentos del MSPI (guías) para fortalecer la gestión TI del instituto y dar cumplimiento en la estructuración de los entregables y/o productos definidos.
- ✓ Documentar y/o ajustar los procedimientos, formatos, manuales y política relacionados con el Modelo de Seguridad de la Información (MSPI) de forma transversal a todos los procesos del instituto y en concordancia con las guías, instrumentos técnicos y requisitos del Modelo.
- ✓ Realizar capacitaciones y actividades de socialización encaminadas a que se fortalezcan los conocimientos y competencias de los colaboradores del Instituto en Seguridad y Privacidad de la Información, Seguridad Informática y Seguridad Digital.
- ✓ Parametrizar la herramienta CERESO - Mesa de Servicios, de tal forma que permita identificar que el incidente generado este asociado a la seguridad de la información, lo anterior para poder generar estadísticas más reales y realizar un análisis del estado de vulnerabilidad de los sistemas en el ICA.

| **FIRMA DE APROBACIÓN** | **NOMBRE Y FIRMA DEL(LOS) AUDITOR(ES)** | **FECHA DE APROBACIÓN** |
|---|---|---|
| *JUAN FERNANDO PALACIO ORTIZ*<br>**Jefe Oficina Control Interno** | SERGIO ANDRÉS CASTRO LONDOÑO | 02 de julio 2024 |