ICA
Instituto Colombiano Agropecuario

ICA 27/09/2024 07:39
Al Contestar cite este No.: **20243126716**
Origen: Oficina de Control Interno
Destino: Gerencia General
Anexos: Fol:9

MEMORANDO

11.100.4
Bogotá,

PARA: **PAULA ANDREA CEPEDA RODRIGUEZ**
Gerencia General (E)

DE: OFICINA DE CONTROL INTERNO

ASUNTO: FUNCIÓN PREVENTIVA - AUDITORIA GOBIERNO DIGITAL 2024

Doctora Paula Andrea, reciba un cordial saludo.

En atención al cumplimiento de las funciones de la Oficina de Control Interno, establecidas por el ordenamiento jurídico a través del ***Articulo No.12 de la 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"* y en especial los literales:

> *d)Verificar que los controles asociados con todas y cada una de las actividades de la organización, estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad;*
> *e) Velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de la organización y recomendar los ajustes necesarios;*
> *f) Servir de apoyo a los directivos en el proceso de toma de decisiones, a fin de que se obtengan los resultados esperados.*
> *g) Verificar los procesos relacionados con el manejo de los recursos, bienes y los sistemas de información de la entidad y recomendar los correctivos que sean necesarios;*
> *j. Mantener permanentemente informados a los directivos acerca del estado del control interno dentro de la entidad, dando cuenta de las debilidades detectadas y de las fallas en su cumplimiento;*

Por lo anterior y en concordancia con la Circular No. 1 del 09 de julio de 2015 "Fortalecimiento del sistema de control interno frente a su funcion preventiva" del Consejo Asesor del Gobierno Nacional, la Oficina de Control Interno se permite emitir la presente función preventiva, en relación con el seguimiento y la evaluacion de las actividades desarroladas en el Mapa de Ruta "2023-2025" del ICA, frente a la implementacion de la Politica de Gobieno Digital en el ICA 2024.

Y en concordancia con la normatividad establecida en la implementación de la Política de Gobierno Digital, como lo son:

- Decreto 1078 de 2015 Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno en Línea. Art.2.2.9.1.1.3, literal 10. *"10. Proactividad: Los sujetos obligados a la Política de Gobierno Digital desarrollarán capacidades que les permitan anticiparse a las necesidades de los ciudadanos y, en general, los habitantes del territorio nacional, en la prestación de servicios de calidad y mitigar riesgos asociados a la continuidad y disponibilidad de estos, así como la identificación de riesgos asociados a la regulación del sector."*
- Decreto No.767 del 16 de mayo 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"*
- Manual de la Política de Gobierno Digital Versión 7 de abril de 2019.
- Resolución 1978 de 2023 "*Por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones"*
- *Resolución 500 de 2021 establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el Modelo de Seguridad y Privacidad de la Información (MSPI).*
- *Resolución No. 742 de 2022 del MinTIC "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a lo establecido en la Resolución No. 500 de 2021".*
- Norma ISO 27001:2013. Técnicas de seguridad: Sistemas de gestión de la seguridad de la información. Requisitos.
- *CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa, donde el ICA deberá fortalecer las capacidades en su habilitador "Seguridad de la Información" para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.*
- 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 entreotros) 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.
- Decreto 620 de 2020**,** *"Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"*
- *Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.*
- *Resolución 1519 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece los estándares y directrices para la publicación de información, así como los requisitos para el acceso a la información pública, la accesibilidad web, la seguridad digital y los datos abiertos.*
- *El artículo 147 de la Ley 1955 de 2019, establece que las entidades del Estado nacional deben incluir el componente de transformación digital en sus planes de acción. Además, hace hincapié en la importancia de que las entidades territoriales incorporen estrategias de ciudades y territorios inteligentes.*
- Resolución 01117 de 5 de abril de 2022 *"Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios*

inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital" o *Plan Nacional de Desarrollo (PND) 2022 - 2026 "Colombia Potencia Mundial de la Vida". Artículo 143. Transformación digital como motor de oportunidades e igualdad.*

Es así que, el Instituto al no tener implementado las actividades del Mapa de Ruta "2023-2025", de acuerdo con los lineamientos de la Política de Gobierno Digital, en los componentes: *Gobernanza, Innovación Pública Digital, Habilitadores, Líneas de acción e iniciativas dinamizadoras*, no está garantizando una transformación digital integral como mecanismo para el desarrollo, la sostenibilidad, la inclusión y el bienestar económico y social e integral, con las posibles consecuencias:

1. Imposibilidad para evaluar de manera integral, la eficacia, eficiencia, calidad de las metas y resultados propuestos en el Mapa de Ruta "2023-2025" del ICA, de acuerdo con los lineamientos de la Política de Gobierno Digital implementada en la Entidad.
2. Afectación de riesgos tecnológicos del ICA 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.
3. Posibilidades de materializaciones de riesgos en la Arquitectura de TI del ICA, a falta de implementación de los lineamientos del MAE en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información.
4. Posibilidad de afectación reputacional por vulnerabilidades tecnológicas en el ámbito de seguridad informática y ciberseguridad no identificadas en el ICA, que pueden causar incidentes de seguridad a los activos de información, sistemas operativos, aplicaciones, redes inalámbricas y/o Infraestructuras críticas, etc., de acuerdo con los principios fundamentales de la triada *CIA o CID en la "confidencialidad, integridad y disponibilidad"*. Estos tres pilares son fundamentales para la protección de los datos y sistemas en un entorno cibernético cada vez más amenazante, lo anterior, debido al nivel bajo de ejecución de las actividades desarrolladas por el proceso Gestión del Servicio TIC, en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI
5. Posibilidad de afectación en los Servicios de TI del ICA por vulnerabilidades administrativas no identificadas.
6. Desconocimiento y/o falta de articulación con los dueños de cada proceso (funcionales) de las herramientas diseñadas para facilitar la planificación,

administración y mejora de los servicios relacionados con la tecnología de la información en el Instituto.

7. Posibilidad de incumplimiento del Anexo 2 (Estándares de publicación y divulgación de información) de acuerdo con los lineamientos dados en la Resolución 1519 de 2020 de MinTIC, toda vez que la información pública del sitio web https://www.ica.gov.co/ debe estar actualizada, por ejemplo: el contenido del sitio, los datos básicos los funcionarios y contratistas de las 32 seccionales, oficinas locales, redes de laboratorios de diagnóstico veterinario, entre otras áreas y dependencias del nivel central y nacional.
8. Afectación reputacional por quejas ocasionada al no poder ofrecer servicios digitales de calidad y confianza en el ICA
9. Afectación reputacional por quejas ocasionada al no mejorar la calidad de vida de los ciudadanos en la oferta y automatización de trámites que permitan hacer valer los derechos de los ciudadanos, cumplir con obligaciones o ejercer actividades, como también los servicios ofrecidos por el ICA haciendo uso de tecnologías emergentes.
10. Posibilidad de incumplimiento de proyectos o iniciativas que no puedan lograr la transformación digital pública del ICA.
11. Afectación reputacional, por no poder mejorar la cometitividad de ICA derivado del Plan Estratégico 2023 – 2026 "ICA Más Cerca del Campo", frente al proceso de modernización de los servicios tecnológicos y el fortalecimiento de la seguridad de la información de los sistemas que soportan el trabajo por la sanidad agropecuaria y la inocuidad agroalimentaria del campo colombiano.

Teniendo en cuenta las posibles consecuencias identificadas en el marco de la auditoria de la Politica de Gobierno Digital implementada en la vigenvia 2024 y considerando las recomendaciones dadas por la Oficina de Control Interno en la auditoria de seguimiento a la Politica de Gobierno Digital en la vigencia 2023, se observó lo siguiente:

Vigencia 2023

Se realizó Informe Seguimiento A Gobierno Digital Marco De Arquitectura Empresarial , mediante memorando No. 20233126360, radicado el pasado 17 de noviembre del 2023 a la Gerencia General, cuyo objetivo, fue presentar los resultados finales del avance y/o cumplimiento de las actividades programadas en el Mapa de Ruta de Gobierno Digital 2023-2025 con las siguientes recomendaciones:

- *Ajustar la matriz de madurez, a los lineamientos establecidos en el "Marco de Referencia de Arquitectura Empresarial MRAE V3.3 con la matriz de nivel de madurez.*

- *Realizar un plan para cubrir el 30% de actividades que no se han iniciado, en donde se tengan presupuestados recursos presupuestales y capital humano para poder realizarlos.*
- *El próximo PETI – Plan Estratégico de Tecnologías de Información debe estar articulado con el Marco de Arquitectura Empresarial y el Mapa de Ruta de Gobierno Digital 2023-2025.*
- *Actualizar procedimientos, guías, manuales o instructivos asociados al Marco de Arquitectura Empresarial y/o el Mapa de Ruta 2023-2025.*

Vigencia 2024

Se realizó la Auditoría al *Modelo de Seguridad y Privacidad de la Información (MSPI)*, mediante *memorando No 202443117225*, el cual fue radicado a la Gerencia General el pasado 3 de julio 2024, donde se evaluó el habilitador de la ***Politica de Gobierno Digital "Seguridad de la Información"***, con los siguientes incumplimientos:

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.*
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

*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.*

Riesgos identificados del habilitador de la Política de Gobierno Digital – Habilitador "Seguridad de la Información":

- *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.*

Es importante manifestar que, pese a lo mencionado anteriormente, los riesgos que tiene el proceso Gestión del Servicio TIC, no se han materializado.

Por lo anterior, la Oficina de Control Interno eleva ante la Gerencia General función preventiva asociada a la Política de Gobierno Digital para el Instituto y plantea las siguientes recomendaciones:

- Revisar y ajustar los documentos y/o entregables en la implementación de la Política de Gobierno Digital en el ICA 2024.
- Apropiar y aplicar los instrumentos del manual de la Política de Gobierno Digital para fortalecer la gestión TI del instituto y dar cumplimiento en la estructuración de los entregables y/o productos definidos y propender la transformación digital pública en el ICA.
- Desarrollar capacidades para el fortalecimiento institucional implementando el enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de los proyectos con componentes de Tecnologías de la información del ICA
- Desarrollar 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 datos.
- Desarrollar mediante soluciones tecnológicas, las capacidades para mejorar la interacción con la ciudadanía y organizar su derecho a utilización de medios digitales ante la administración pública.
- Desarrollar capacidades para el acceso, uso y aprovechamiento de Tecnologías de la Información y las Comunicaciones del ICA, promoviendo el uso y apropiación de estas entre las personas en situación de discapacidad y fomenta la inclusión con enfoque diferencial.
- Realizar capacitaciones y actividades de socialización encaminadas a que se fortalezcan los conocimientos y competencias institucionales en la adopción y la implementación de la Política de Gobierno Digital en el ICA 2024.
- Desarrollar servicios y procesos digitales, automatizados, accesibles, adaptativos y basados en criterios de calidad a partir del entendimiento de las necesidades del usuario y su experiencia, implementados esquemas de atención productiva y el uso de tecnologías emergentes.
- Promover el desarrollo económico y social del ICA impulsado por datos, como infraestructura y activos estratégicos, a través de mecanismos de gobernanza para el acceso, intercambio reutilización y explotación de datos.
- Promover la transparencia en la gestión pública con un enfoque de apertura por defecto, y el fortalecimiento de escenarios de dialogo que promuevan la confianza.
- Implementar proyectos de transformación digital que aporten a la generación

de valor público mediante aprovechamiento de las capacidades que brindan el uso y la apropiación de las Tecnologías de la Información y las comunicaciones para alcanzar los objetivos institucionales.

 Actualizar políticas, procedimientos, guías, manuales o instructivos asociados al Marco de Arquitectura Empresarial y/o el Mapa de Ruta 2023-2025.

La Oficina de Control Interno, recomienda realizar el analisis pertinente de la función preventiva y tomar las acciones correspondientes para mitigar las posibles consecuencias que se plantean en este documento y que estas sean comunicadas a esta oficina para el seguimiento que nos corresponde como tercera linea de defensa. Igualmente, reiterar el compromiso de esta oficina en el acompañamiento que se requiera de conformidad con nuestras competencias.

Atentamente,

JUAN FERNANDO PALACIO ORTIZ
Jefe Oficina Control Interno

Elaboró: Sergio Andres Castro Londoño