INFORME DE EVALUACIÓN Y SEGUIMIENTO AL CUMPLIMIENTO DE LA NTC-27001 DE 2013

CORPORACIÓN AUTÓNOMA REGIONAL DEL MAGDALENA – CORPAMAG

OFICINA CONTROL INTERNO

DICIEMBRE DE 2023

INFORME DE EVALUACIÓN Y SEGUIMIENTO

1. INTRODUCCIÓN

De acuerdo con lo establecido en 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 teniendo en cuenta los roles definidos para la tercera línea de defensa –Oficina de Control Interno dentro del Modelo Integrado de Planeación y Gestión – MIPG, se realizó el seguimiento al cumplimiento de los requisitos de la Norma Técnica Colombiana NTC-27001 de 2013.

2. OBJETIVO

Evaluar el cumplimiento de la Norma Técnica NTC-ISO/IEC Colombiana 27001 por parte de CORPAMAG y el avance de las acciones de mejora propuestas a los hallazgos producto de la auditoría realizada por la Revisoría Fiscal en la vigencia 2022.

3. CRITERIOS

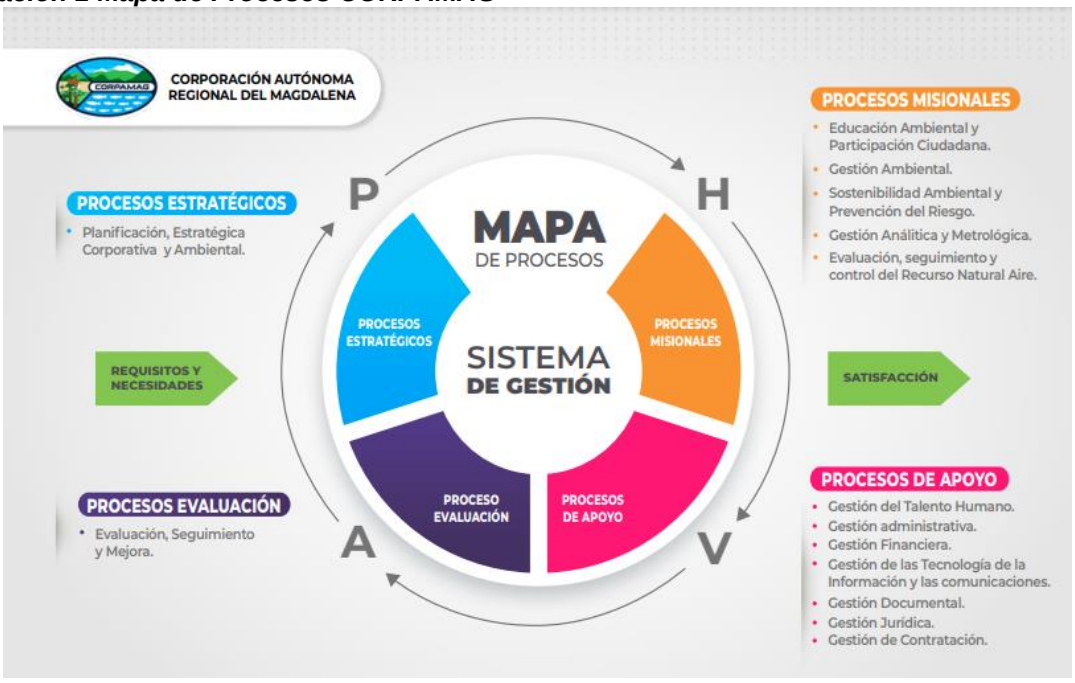
- **Ley 87 de 1993** *"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones".*

- **Norma Técnica Colombiana NTC-ISO/IEC 27001 "**Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos".

4. RESULTADOS DE EVALUACIÓN Y SEGUIMIENTO

La Corporación tiene definido desde 2008 un **modelo de operación basado en procesos** bajo el ciclo Planear, Hacer, Verificar y Actuar – PHVA y estos son: (misionales, de apoyo, estratégicos y evaluación) y a la fecha se sigue implementando. El mapa de procesos vigente se encuentra disponible en el siguiente enlace:
https://www.corpamag.gov.co/transparencia/informacion-de-la-entidad/a-mapa-y-cartas-de-procesos.

Ilustración 1 Mapa de Procesos CORPAMAG



Fuente: sede virtual de CORPAMAG.

En la ilustración anterior, se puede observar que la entidad tiene establecido 14 procesos y cada uno cuenta con su ficha de caracterización en la cual se establece su propósito u objetivo, alcance, responsables, interrelación con los demás procesos, entradas, salidas, indicadores, procedimientos relacionados, como también la información de todo aquello que este realiza.

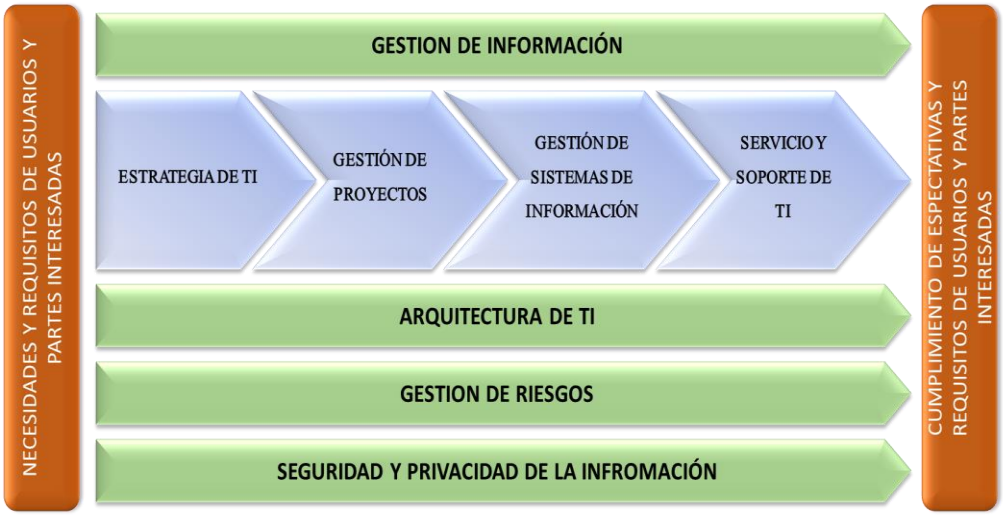
El proceso *Gestión de Tecnologías de la Información y las Comunicaciones* de CORPAMAG está identificado en el Sistema Integrado de Gestión con el código **FC.GT.009,** y su objetivo es "*Implementar soluciones tecnológicas para optimizar los procesos y procedimientos de la Corporación, haciéndoles más eficientes, transparentes y participativos, gracias al uso de las Tecnologías de la Información y las Comunicaciones*", y contiene 5 procedimientos

1. PR.GT.001 Formulación y seguimiento del plan estratégico de las Tecnologías de la Información y la Comunicaciones – TIC.
2. PR.GT.002 Gestión de proyectos y planes de las Tecnologías de la Información y la Comunicaciones – TIC.
3. PR.GT.003 Mantenimientos preventivos y correctivos
4. PR.GT.004 Gestión de la Seguridad de la Información.
5. PR.GT.005 Soporte a usuarios de TI.

Con respecto al cumplimiento de los requisitos establecidos en la norma NTC-27001 se evidenció lo siguiente:

1. Que el Plan Estratégico de Tecnología de la Información y las Comunicaciones PETI 2020-2023 de la Corporación (https://www.corpamag.gov.co/archivos/planes/PETI_Corpamag_2020-2023_v2023.pdf) incluye el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el cual fue ajustado en la vigencia 2023, en donde se plantea la cadena de valor sugerida para el proceso de Gestión de la Información de la entidad, como se muestra representada en la ilustración No. 2.

Ilustración 2 Cadena de valor de TI



Fuente: PETI 2020-2023 de CORPAMAG

2. Se evidenció la publicación de la resolución 5846 del 28 de diciembre de 2021 *"por medio de la cual se adoptan el modelo de seguridad y privacidad de la Información (MSPI), la política general de seguridad y privacidad de la Información y la política de seguridad digital de la Corporación Autónoma Regional del Magdalena-CORPAMAG*" en la sede virtual de la entidad, además su socialización. https://www.corpamag.gov.co/archivos/planes/PoliticaSeguridadyPrivacidaddelaInformacion.pdf.

3. Durante la vigencia 2023 se realizó la revisión del Modelo de Seguridad y Privacidad de la Información-MSPI y se formuló la Política de Copias de Seguridad y Gestión de Almacenamiento, la cual fue socializada a los servidores públicos durante los meses de septiembre y octubre del año en curso.

4. En la intranet de la entidad se encuentra definido y publicado el plan de mantenimiento preventivo de infraestructura de tecnologías de la información y las comunicaciones correspondiente a la vigencia 2023, sin embargo en el numeral 5.*8 cronograma de ejecución*, el título del cuadro está errado, dado que hace referencia al 2020, por lo que se sugiere se realice la corrección. https://www.corpamag.gov.co/intranet/gestionTIC/2023-Plan-de-mantenimiento-CORPAMAG.pdf

5. La entidad tiene inventariado sus activos informáticos, y actualmente se está efectuando por parte del área de Almacén como mecanismo de control su verificación, una vez se termine se realizará la respectiva conciliación de la información con el grupo de las TIC.

6. La Corporación cuenta con el personal idóneo con responsabilidades definidas en el sistema de seguridad de la información.

7. Cada año, se establece un plan de mantenimiento preventivo y correctivo de las instalaciones físicas.

5. SEGUIMIENTO A ACCIONES DE MEJORA PARA SUBSANAR HALLAZGOS DE LA AUDITORÍA REALIZADA POR LA REVISORÍA FISCAL - VIGENCIA 2022

Con respecto a los tres (3) hallazgos encontrados por la revisoría fiscal de la entidad, se lograron los siguientes avances:

Tabla 1 Porcentaje de cumplimiento hallazgos de la revisoría fiscal

Hallazgo		% cumplimiento
5	Se debe definir en conjunto de las políticas de seguridad de la información de acuerdo a las necesidades identificadas en el análisis de riesgos, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes. Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	100%
6	Para el cumplimiento de los requerimientos establecidos en el Anexo A de la norma ISO 27001 es necesario elaborar un diagrama de red de alto nivel o arquitectura de TI, con el objetivo de identificar físicamente y lógicamente incidentes que afecten el correcto funcionamiento de los sistemas de información	0%
7	El área responsable del proceso debe realizar el debido control y mantenimiento al inventario de activos de tecnología e información, para establecer responsabilidad sobre la tenencia de los mismos y la información sobre estos, incluido el control al licenciamiento de software, mantenimientos preventivos/correctivos y las acciones necesarias para mejorar las condiciones de control de humedad en el cuarto de servidores principales.	100%

6. RECOMENDACIONES

1. Continuar realizando las gestiones necesarias para cumplir con las acciones propuestas en el plan de mejoramiento y subsanar los hallazgos identificados.

2. Procurar la mejora continua del proceso con la aplicabilidad y cumplimiento del 100% de la NTC-27001 y estar preparados para los cambios del entorno (internos y externos), con el propósito de seguir manteniendo un Sistema Seguridad de la Información efectivo.

LILIANA HIDALGO GARCIA
Jefe Oficina de Control Interno

LUZ PIEDAD ECHAVARRÍA LÓPEZ
Contratista