INFORME DEFINITIVO DE AUDITORÍA INTERNA -GESTIÓN TECNOLÓGICA INVAMA 2025

https://www.gbtec.com/es/wiki/gestion-de-procesos/modelo-de-madurez-digital/[1]

[1] Fuente https://www.gbtec.com/es/wiki/gestion-de-procesos/modelo-de-madurez-digital/

Contenido

1. PRESENTACIÓN 3
2. CONCEPTOS 4
3. OBJETIVO 5
4. MARCO NORMATIVO APLICABLE 5
5. ALCANCE DE LA AUDITORÍA 6
6. METODOLOGÍA 6
7. RESULTADOS 7
7.1. FORTALEZAS 9
7.2 OPORTUNIDADES DE MEJORA 12
8. RESULTADO GRÁFICO DEL PROCESO AUDITOR 17
9.RECOMENDACIONES. 18
10.PLAN DE MEJORAMIENTO. 20

1. PRESENTACIÓN

La presente auditoría se realiza en ejecución al plan anual de auditoría interna vigencia 2025, aprobado por el comité coordinador de control interno en sesión del 17 de febrero de igual anualidad, las razones técnicas para evaluar internamente el proceso están orientadas al nivel de criticidad del riesgo en el cual se determinó que la gestión tecnológica permite a la entidad mejorar sus procesos internos, reduciendo costos operativos y aumentando la eficiencia de los servicios públicos. La automatización de trámites, el uso de plataformas digitales para la gestión de datos y la digitalización de procesos administrativos permite a la entidad trabajar de manera más ágil, y destinar recursos a áreas de mayor impacto social. Esto se traduce en una mejora continua de la calidad de los servicios ofrecidos a los ciudadanos.

La gestión tecnológica dentro del Modelo Integrado de Planeación y Gestión (MIPG) en entidades públicas se refiere a la forma en que se planifica, desarrolla y utiliza la tecnología para mejorar la eficiencia y el cumplimiento de los objetivos institucionales. MIPG, a través de sus dimensiones y políticas, promueve la gestión del conocimiento y la innovación, lo cual incluye la gestión tecnológica, para adaptar la entidad a las nuevas tecnologías y mejorar la prestación de servicios.

2. CONCEPTOS

En el proceso auditor se pueden encontrar resultados como fortalezas, hallazgos, debilidades y oportunidades de mejora, los cuales, se pasan a definir para un mayor entendimiento para un mayor entendimiento de los resultados aquí presentados:

FORTALEZA:

Se define como fortaleza a aquellos aspectos de una organización o entidad que son considerados positivos, en la medida en que permiten superar obstáculos, evitar problemas o sobreponerse a situaciones adversas.

HALLAZGO: En auditoría, un hallazgo es la discrepancia o situación identificada **al comparar la condición observada en un proceso** con los **criterios establecidos**, sustentada en evidencia suficiente, pertinente y válida, que puede constituir una debilidad, un incumplimiento o una oportunidad de mejora.

CRITERIO: Se trata del estándar contra el cual ha medido o comparado la condición. Es la norma contra la cual el auditor mide la condición.

DEBILIDAD: Se entiende como una deficiencia significativa en los controles internos que, en sí misma, o en combinación con otras deficiencias, dan como resultado más que una probabilidad remota de que no se podrán impedir o detectar los errores materiales.

OPORTUNIDAD DE MEJORA: Una oportunidad de mejora es la identificación de un aspecto, práctica o proceso dentro de la entidad que, aunque no constituya necesariamente una irregularidad o hallazgo

negativo, puede optimizarse para fortalecer la gestión, aumentar la eficiencia, reducir riesgos o mejorar el cumplimiento normativo.

3. OBJETIVO

Evaluar la eficiencia, eficacia y cumplimiento de la gestión tecnológica de la entidad, con el fin de verificar su alineación con los objetivos institucionales, el cumplimiento de la normativa vigente, y la implementación de los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG. Esto incluye la revisión de los procesos asociados al uso, administración y desarrollo de tecnologías de la información, así como su contribución al mejoramiento continuo, la innovación institucional y la toma de decisiones basada en datos.

4. MARCO NORMATIVO APLICABLE

Ley 87 de 1993 – Por la cual se establecen normas para el ejercicio del control interno en las entidades del Estado, Artículos Art. 2 y Art. 9.

Ley 489 de 1998 – Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional.

Modelo Integrado de Planeación y Gestión – MIPG (Decreto 1499 de 2017)

Decreto 648 de 2017 – Por el cual se reglamenta el rol del jefe, asesor o director de control interno.

Normatividad y Lineamientos TIC en Colombia

Gobierno Digital (antes Estrategia de Gobierno en Línea).

Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC, en la Parte 2, Título 9, el marco del Gobierno Digital.

Resolución 1519 de 2020 del MinTIC define los lineamientos para la implementación de la Política de Gobierno Digital en entidades públicas.

Ley 1581 de 2012 – Protección de Datos Personales

Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública.

Ley 1341 de 2009 – Principios y régimen general de las TIC

Ley 1266 de 2008 – Habeas Data

Ley 527 de 1999 – Comercio Electrónico y firma digital

Resolución 500 de 2021, Modelo de Seguridad y Privacidad de la Información (MSPI), Seguridad TI y 2277 de 2025

5. ALCANCE DE LA AUDITORÍA

El alcance de la presente auditoria corresponde a la vigencia 2024 y 2025.

6. METODOLOGÍA

a) La Observación o Inspección

b) Análisis de datos

c) Entrevista

7. RESULTADOS

El proceso de Gestión de Tecnologías de la Información se encarga de planificar, administrar y dar soporte a los recursos y servicios tecnológicos de la entidad. Su objetivo es implementar nuevas soluciones que provean información oportuna, eficiente y transparente, contribuyendo a la transformación digital. Además, garantiza la confiabilidad, disponibilidad, integridad y accesibilidad de la infraestructura tecnológica y de comunicaciones, siguiendo las directrices institucionales y normativas para cumplir con los objetivos del INVAMA.

Este proceso comienza identificando las necesidades tecnológicas de la entidad. Luego se crean planes, políticas y directrices para implementar soluciones y proyectos de TI, se establecen controles de seguridad para proteger la información (disponibilidad, integridad y confidencialidad). Finalmente, se monitorean y evalúan los recursos y servicios tecnológicos para aplicar mejoras continuas y asegurar el cumplimiento de los objetivos.

Para el desarrollo de la presente auditoría se analizaron diversas fuentes de formación, entre ellas el catálogo de servicios ofrecidos por GT[2] formatos, procesos y procedimientos[3], Matriz de Riesgos e Indicadores[4] los cuales se relacionan a continuación;

1. Estructura proceso PT
2. Lista de chequeo configuración de equipo de cómputo V2
3. Monitoreo gestión servicios tecnológicos
4. Bitácora bacukp y o restauración de la información

[2] Gestión Tecnológica
[3] Carpeta SGC
[4] Carpeta SGC

5. Sistemas de información
6. Asignación de cuentas de usuario y contraseñas
7. Políticas TIC´S_ V2
8. Planeación estratégica tecnologías de la información
9. Cuentas de usuario
10. Configuración recurso tecnológico
11. Actualización e implementación sistemas de información
12. Gestión de servicios tecnologías de la información.
13. Soporte técnico
14. Copia seguridad y restauración de la información
15. Caracterización del proceso Gestión.
16. Decreto 767 de 2022 Plan estratégico de tecnología y sistemas de información PETI.
17. Inventario de recursos tecnológicos (hardware, software, redes, etc.)
18. Indicadores del proceso
19. Gestión del riesgo

En desarrollo de la presente auditoría se identificaron 49 servicios ofrecidos por GT, una vez revisadas todas las fuentes antes señaladas se procede a presentar los siguientes resultados así;

7.1. FORTALEZAS

7.1.1. Talento Humano

Talento Humano Se evidencia que el equipo humano responsable de la gestión tecnológica en el INVAMA cuenta con trayectoria y conocimientos previos en el área, lo cual constituye un valor estratégico para la entidad. Esta experiencia se traduce en una ejecución más eficiente de las actividades, una toma de decisiones más acertada y una mayor capacidad para anticipar y resolver situaciones técnicas o administrativas complejas, aspectos que favorecen la continuidad operativa y el cumplimiento de los objetivos institucionales en materia tecnológica.

7.1.2 Herramientas Tecnológicas

La entidad cuenta con una solución tecnológica robusta a través del uso del sistema GLPI recientemente implementado, lo que permite administrar de manera centralizada y eficiente los servicios tecnológicos, los activos, los contratos y demás componentes relacionados con la gestión TI.

Esta herramienta facilita el control, el seguimiento de procesos y la generación de información clave para la toma de decisiones.

7.1.3 Calidad En el Servicio

El área de tecnología ha adoptado prácticas efectivas para garantizar la calidad del servicio, al establecer con los proveedores compromisos formales que definen tiempos de atención diferenciados según la gravedad de los incidentes. Esta estrategia, acompañada de un seguimiento permanente por parte del equipo de sistemas, permite controlar el cumplimiento de los acuerdos y fomentar una mejora continua en la prestación de los servicios tecnológicos.

7.1.4. Capacitación y Culturización

La entidad ha establecido un esquema sostenido de formación en seguridad de la información, mediante la ejecución de campañas de sensibilización que se difunden regularmente a través del canal oficial de correo electrónico y charlas. Estas acciones promueven el fortalecimiento de la cultura organizacional en torno a la protección de los activos de información, mediante la divulgación de recomendaciones técnicas y buenas prácticas que refuerzan el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información institucional.

7.1.5. Respaldo de la información

Se evidenció la implementación de un sistema de respaldo automatizado en la nube, mediante el uso de la herramienta Acronis, el cual permite realizar copias de seguridad de forma diaria.

Esta práctica contribuye a la protección de la información clasificada como crítica para la operación institucional y garantiza la disponibilidad y recuperación de los datos en caso de fallos o incidentes. Asimismo, el mecanismo adoptado está alineado con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en materia de seguridad y gestión de la información.

7.1.6. Transparencia y acceso a la información pública.

El Índice de Transparencia y Acceso a la Información Pública (ITA) constituye un mecanismo de medición que permite valorar en qué medida las entidades cumplen con su obligación de publicar información de carácter público. Más allá de verificar la divulgación de datos, este índice facilita identificar avances y oportunidades de mejora en la gestión institucional, al mismo tiempo que impulsa la rendición de cuentas y fortalece las acciones orientadas a la prevención de la corrupción.

Para el caso del Invama la calificación obtenida por las ultimas tres vigencias es del 100 %

PROCURADURIA GENERAL DE LA NACION

Reporte de Cumplimiento ITA para el Periodo 2025

Número de documento: NI 800002916
Sujeto obligado: INSTITUTO DE VALORIZACION DE MANIZALES
Nivel de cumplimiento: 100 sobre 100 puntos

Lo que evidencia que la entidad cumple en su totalidad con las obligaciones normativas establecidas en la Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública Nacional, así como con los lineamientos de la Procuraduría General de la Nación y demás entes de control.

Este resultado refleja:

- Alta disposición para garantizar el derecho fundamental de acceso a la información pública.
- Cumplimiento en la publicación proactiva de información en medios institucionales (web y demás canales oficiales).
- Existencia de procedimientos claros de atención a solicitudes de información de la ciudadanía.
- Cultura institucional orientada hacia la transparencia y el gobierno abierto.

7.2 OPORTUNIDADES DE MEJORA

7.2.1 Riesgos y Controles

Si bien en el Plan de Seguridad y Privacidad de la Información se contempla la definición de un Plan de Continuidad del Negocio y Recuperación de Desastres (BCP/DRP)[5], actualmente este aún no se encuentra formalizado ni aprobado.

[5] Plan de Continuidad del Negocio (BCP) / Plan de Recuperación ante Desastres (DRP)

Esto representa una oportunidad de mejora para que en la entidad se diseñe, documente y apruebe el plan de continuidad tecnológica y recuperación de desastres, en concordancia con la normatividad MinTIC y los estándares internacionales (ISO 22301 – continuidad de negocio, ISO 27031 – continuidad de servicios TI).

Además, se establezca responsables, tiempos de recuperación (RTO/RPO[6]), estrategias de respaldo y mecanismos de comunicación ante incidentes, programe y ejecute pruebas periódicas de simulación; ejemplo caída de servidores, indisponibilidad de red, que permitan validar la eficacia del plan y realizar ajustes.

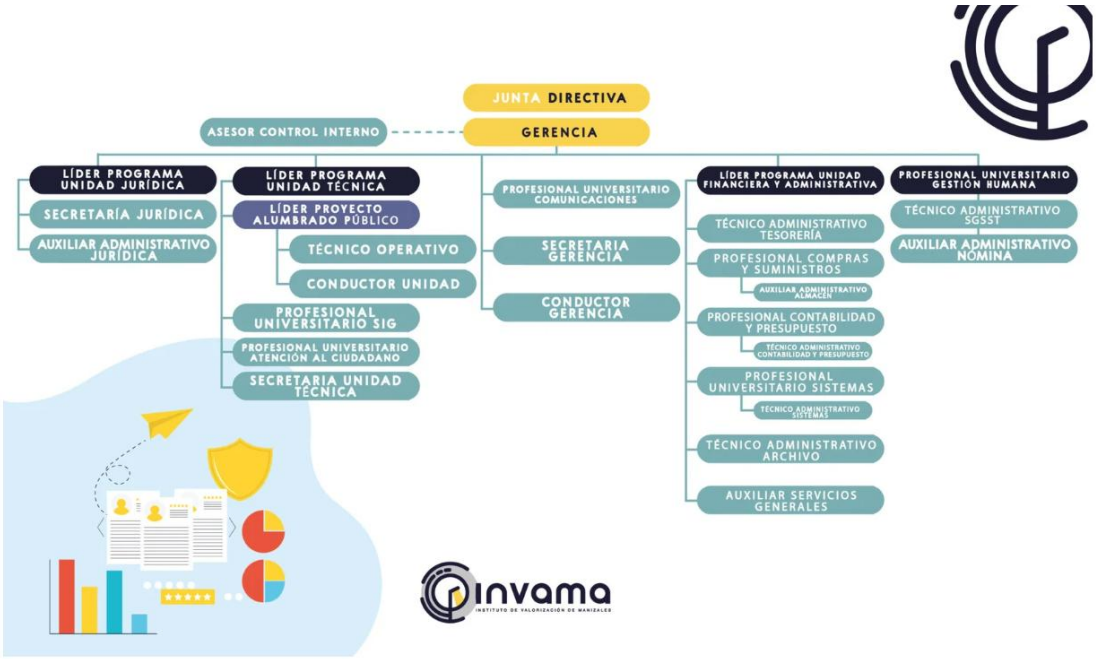
7.2.2 Fortalecimiento Institucional.

Una vez revisada la estructura orgánica de la entidad se observa que no se está dando cumplimiento al Decreto 415 de 2016 “"Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones”, en su artículo 2.2.35.4 que señala;

“(…) Nivel Organizacional. Cuando la entidad cuente en su estructura con una dependencia encargada del accionar estratégico de las Tecnologías y Sistemas de la Información y las Comunicaciones, hará parte del comité directivo y dependerán del nominador o representante legal de la misma (…)”

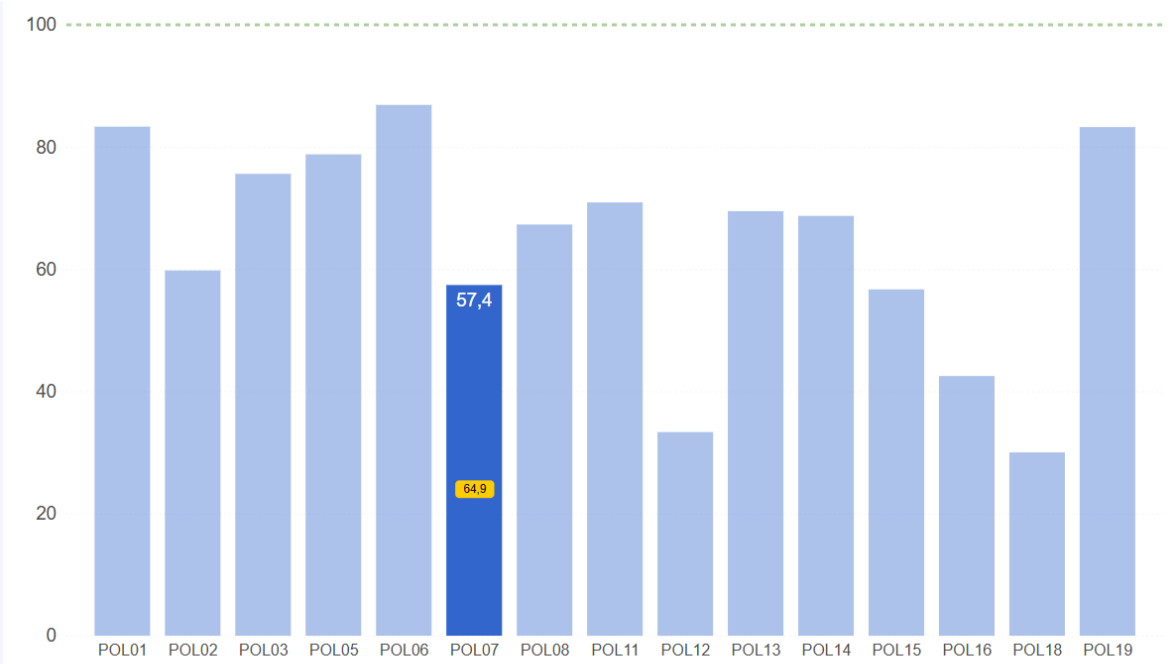
[6] Objetivo de Tiempo de Recuperación / Objetivo de Punto de Recuperación

Lo anterior indica que las entidades públicas deben ajustar su estructura orgánica a los lineamientos establecidos para garantizar el fortalecimiento en materia de TIC, y su no aplicación puede generar debilidades en el fortalecimiento institucional, limitando la capacidad de la entidad para alinear sus procesos tecnológicos con la normatividad vigente y con las políticas de modernización del Estado.

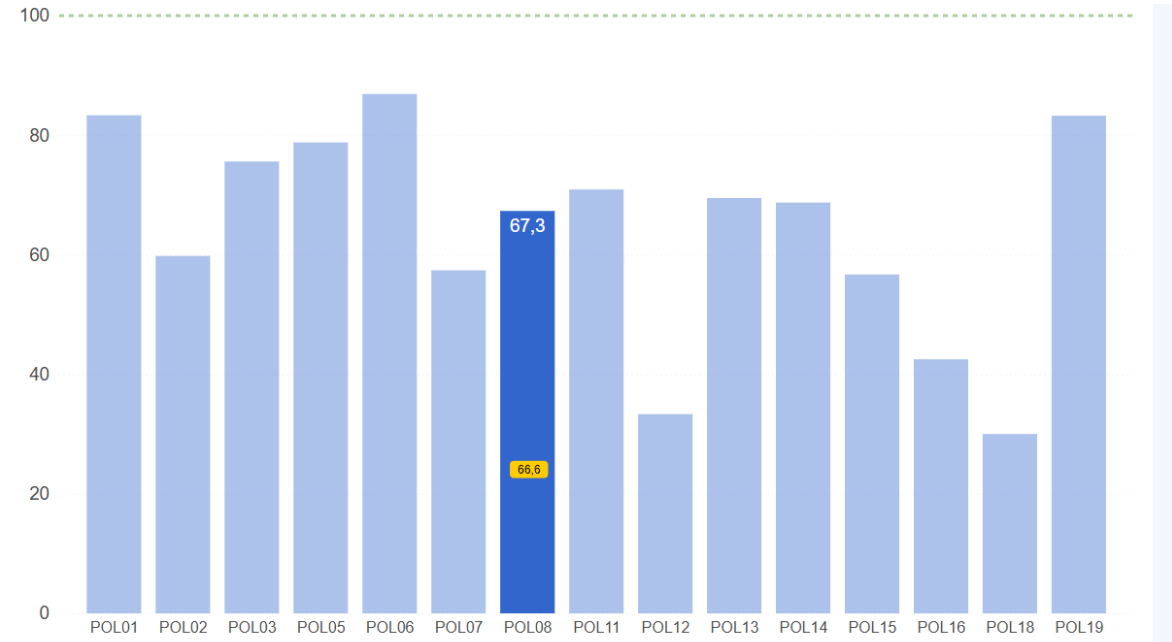


7.2.3 Avance Políticas MIPG

Dentro de las actividades del proceso se encuentra Evaluar el Avance en la Implementación de las políticas de Gestión y Desempeño Institucional que hacen parte de MIPG. Al evaluar el avance de la política de No POL7 Índice de Gobierno Digital y POL8 Índice de Seguridad Digital, las que atañen de manera directa con el proceso auditado, se encuentran los siguientes resultados para la vigencia 2024.



Nota 1: La etiqueta de valores en amarillo en cada columna indica el valor promedio obtenido en la política específica consultada.



Nota 1: La etiqueta de valores en amarillo en cada columna indica el valor promedio obtenido en la política específica consultada.

En el Índice de Gobierno Digital POL7 la entidad presento un resultado de 57,4% mientras que la línea del grupo par 64,7%, lo anterior indica que la entidad se encuentra por debajo del promedio del grupo par (–7,3 puntos porcentuales), lo cual refleja brechas en la implementación de políticas y estrategias orientadas a la transformación digital. Esto indica posibles debilidades en la adopción de herramientas tecnológicas, en la gestión de datos, en la interoperabilidad de sistemas y en la oferta de trámites y servicios digitales accesibles al ciudadano.

De otro lado el Índice de Seguridad Digital (POL 8) donde la entidad presento un resultado de 67,3% posicionándose la línea del grupo par en 66,6% superando ligeramente el instituto de valorización a las entidades promedio en (+0,7 puntos porcentuales). Si bien esto demuestra avances en la implementación de políticas de seguridad de la información, protección de datos y ciberseguridad, el resultado aún es moderado y evidencia la necesidad de fortalecer los controles, la gestión de riesgos digitales y los planes de continuidad del negocio.

La entidad muestra fortalezas en Seguridad Digital al ubicarse por encima del grupo par, aunque con un margen mínimo que exige consolidación y sostenibilidad de los avances. En contraste, presenta rezagos significativos en Gobierno Digital, que demandan un plan de acción inmediato para superar la media nacional y evitar el riesgo de rezago en transformación digital, eficiencia institucional y percepción ciudadana.

7.2.4 Planta Física

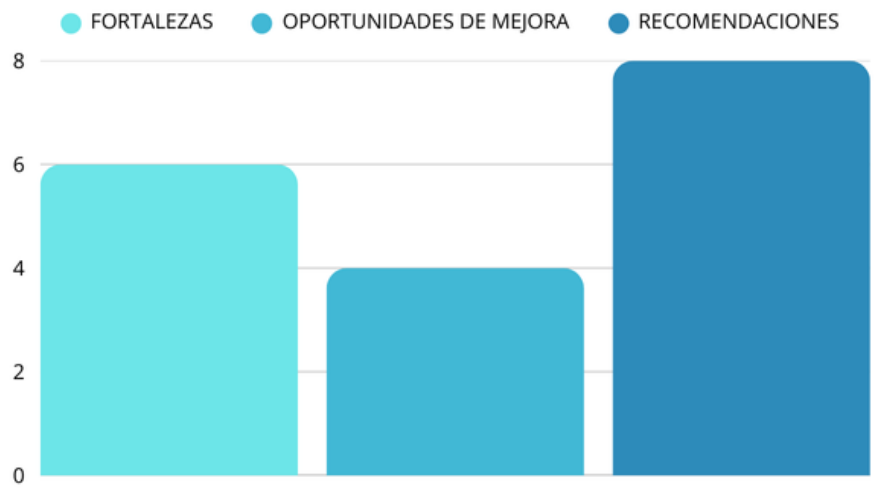
Se identifica limitación en la planta física que impactan tanto las condiciones de trabajo de los funcionarios como el espacio destinado a la

data center, lo que puede generar riesgos asociados a la continuidad operativa, la seguridad de la información y la infraestructura tecnológica.

Las condiciones inadecuadas del entorno pueden generar fallas prematuras en los equipos, sobrecostos por mantenimientos correctivos y dificultades para ampliar la capacidad instalada conforme a las necesidades futuras.

Este entonces más que un problema de espacio físico, se trata de un riesgo estratégico para la entidad, porque compromete la continuidad de sus procesos misionales, la protección de la información institucional y la sostenibilidad de su infraestructura tecnológica.

8. RESULTADO GRÁFICO DEL PROCESO AUDITOR



Descripción;

El número de fortalezas es superior al de oportunidades de mejora, lo cual evidencia que el Instituto de Valorización de Manizales Invama cuenta con prácticas sólidas en la gestión tecnológica. Esto refleja un nivel de madurez favorable, donde existen más aspectos consolidados que debilidades por atender.

En desarrollo el proceso auditor se genera un mayor número de recomendaciones frente al número de oportunidades de mejora buscando no solo corregir las oportunidades de mejora, sino en potenciar buenas prácticas.

Por lo que, tal como se puede apreciar en el siguiente titulo la mayoría de recomendaciones están orientadas a fortalecer procesos ya existentes (por ejemplo, consolidar seguridad digital, culturización, adecuación de infraestructura).

Este panorama refleja que la gestión tecnológica del INVAMA no presenta fallas críticas, pero sí necesita ajustes estratégicos para garantizar sostenibilidad y alineación con las políticas nacionales de transformación digital.

9.RECOMENDACIONES.

1. Diseñar, formalizar y aprobar el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación de Desastres (DRP), alineados con estándares establecidos en la Ley 1523 de 2012 sobre la política nacional de gestión del riesgo de desastres, las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y normas concordantes.

2. Establecer responsables claros, tiempos de recuperación (RTO/RPO), protocolos de comunicación y roles ante incidentes.
3. Realizar simulacros de contingencia (caída de servidores, indisponibilidad de red, pérdida de datos) para validar la efectividad del plan.
4. Documentar y mejorar continuamente los resultados de dichas pruebas.
5. Gestionar con la alta dirección la adecuación de la estructura orgánica para dar cumplimiento al Decreto 415 de 2016, garantizando que el área de Gestión Tecnológica tenga representación ante el comité estratégico de la entidad[7]. Buscando con lo anterior establecer mecanismos formales de articulación entre GT[8] y las demás dependencias para asegurar la alineación de la estrategia digital con los objetivos misionales.
6. Elaborar un plan de acción específico para superar las brechas en el Índice de Gobierno Digital (POL7), priorizando, Interoperabilidad de sistemas, Gestión y analítica de datos, Implementación de trámites y servicios digitales accesibles al ciudadano.
7. Consolidar y mantener los avances en el Índice de Seguridad Digital (POL8) con mayor énfasis en ciberseguridad preventiva, monitoreo continuo de riesgos digitales, protección avanzada de datos personales.
8. Implementar un plan de adecuación progresiva de la planta física que albergue la infraestructura tecnológica, asegurando condiciones óptimas de seguridad, ventilación, energía eléctrica regulada y crecimiento futuro.

[7] Comité de gerencia

[8] Gestión Tecnológica

10.PLAN DE MEJORAMIENTO.

Con el propósito de dar cumplimiento a las disposiciones en materia de control interno y de fortalecer los mecanismos de seguimiento y mejora continua, se establece que, una vez recibido el informe definitivo que contenga **acciones de mejora o recomendaciones** derivadas de evaluaciones o auditorías, el proceso evaluado deberá formular y adoptar un Plan de Mejoramiento en un término no superior a **diez (10) días hábiles**, contados a partir de la fecha de recibo del informe.

Dicho plan deberá adoptarse en el formato "CG-AM-FO-01 Plan MejoramientoV4" disponible en la carpeta del SGC, proceso evaluación y control. Con lo anterior se busca garantizar la implementación de medidas orientadas al fortalecimiento institucional y a la mitigación de los riesgos identificados.

El cumplimiento oportuno de esta disposición será objeto de seguimiento por parte de Control Interno, en el marco de sus funciones de evaluación y acompañamiento.

Las evidencias reposan en la carpeta digital del proceso auditor.

ANYELA ANDREA HENAO LONDOÑO
Asesora de control interno