DISTRISEGURIDAD TECNOLOGÍA, PREVENCIÓN, ARTICULACIÓN	**ACTA DE REUNIONES**	**CÓDIGO:** FDEYP-010 **VERSIÓN:** 1.0 **FECHA:** 18/11/2021

FECHA: 9 de septiembre de 2023 **LUGAR** OFICINA DE CONTROL INTERNO

MOTIVO DE REUNION

COMITÉ CONSULTIVO	☐	**REUNIONES CON LA COMUNIDAD**	☐
REUNIONES DE GREMIOS	☐	**CONSEJO DE GOBIERNO**	☐
		MEDIOS DE COMUNICACIÓN	☐
CONSEJO DE SEGURIDAD	☐	**OTROS**	X **Reunión de Cierre Auditoría 001-2023 Proceso Gestión TIC**

TEMAS TRATADOS

Siendo las 10:41 a.m. del 09 de septiembre de 2023 se da inicio a la reunión de cierre de auditoría al proceso de Gestión TIC, convocada por el doctor Gildardo Pérez Torres, Asesor de Control Interno.

En la reunión participan el doctor Gildardo Pérez Torres, asesor de Control Interno; Enrique Nicolás Brieva Jurado, líder proceso Gestión TIC; Victor Santis, Ingeniero apoyo Gestión TIC; Giovana Venegas, asesora implementación MIPG y Francisco Murillo Zabala, apoyo Oficina de Control Interno.

Se procede a señalar las observaciones que se presentaron en desarrollo de la auditoría al proceso de Gestión TIC, en los siguientes términos:

1. RIESGOS DEL PROCESO

HALLAZGO No. 1 La Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5, actualiza y precisa elementos metodológicos para mejorar el ejercicio de identificación, estructuración y valoración del riesgo. Requerida la matriz de riesgos se observan deficiencias en la estructura de los riesgos. Esto pudo obedecer a falta de conocimiento y aplicación de la guía establecida. Como consecuencia, se posibilita la materialización de los riesgos del proceso.

Señala Giovana Venegas que la matriz que envía la alcaldía no está estructurada de acuerdo con la Función Pública.

HALLAZGO No. 2 La Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5, actualiza y precisa elementos metodológicos para mejorar el ejercicio de identificación, diseño, estructuración y valoración del riesgo y sus controles. Requerida la matriz de riesgos se observan debilidades en la estructura del diseño de los controles al no contar con la totalidad de los criterios establecidos para ellos. Esto pudo obedecer a falta de conocimiento y aplicación de la guía establecida. Como consecuencia se incrementa la posibilidad de materialización de los riesgos del proceso.

HALLAZGO No. 3 Los mapas de riesgos Institucional (código MDEYP-002 Versión 1) y de Corrupción (código MDEYO-012 versión 1), presentan unos controles que pretenden mitigar la posibilidad de ocurrencia. Requeridas las evidencias de los controles realizados no se recibe información y/o no son satisfactorias para considerar el cumplimiento de éstos. Esto pudo obedecer a debilidades en la programación y planeación de las actividades del proceso. Como consecuencia, se incrementa la posibilidad de materialización de los riesgos definidos en la matriz.

2. FORMULACIÓN DEL PLAN ESTRATÉGICO DE TECNOLOGÍA DE LA INFORMACIÓN (PETI)

HALLAZGO No. 4 Establece el Decreto 1078 de 2015, en su artículo 2.2.9.1.2.2, que el Ministerio de Tecnologías de la Información y las Comunicaciones expedirá y publicará lineamientos, guías y estándares para facilitar la comprensión, sistematización e implementación integral de la Política de Gobierno Digital, en articulación con el Modelo Integrado de Planeación y Gestión - MIPG. Revisado el documento PETI publicado en la página web de la entidad se pudo evidenciar que este no se desarrolla ni detalla de acuerdo con las guías y modelos propuestos por el MINTIC. Esto pudo obedecer a desconocimiento de la normatividad y/o falta de personal idóneo en el área. Como consecuencia, se dificulta avanzar en temas relacionados con TIC en la entidad, permaneciendo con debilidades en la implementación de requerimientos legales.

3. ALINEACIÓN DEL PETI CON LA ESTRATEGIA INSTITUCIONAL

HALLAZGO No. 5 Establece el Decreto 415 de 2016, en el artículo 2.2.35.3, que la entidad debe liderar la gestión estratégica con un PETI que esté alineado a la estrategia y modelo integrado de gestión de la entidad. De igual manera, el Documento Maestro del Modelo de Gestión de Proyectos TI - MGPTI.G.GEN.01 – determina que quien haga las veces de líder de Tecnologías y Sistemas de la Información debe dirigir la planeación, ejecución y seguimiento a los proyectos de TI. Verificado el PETI de Distriseguridad, se pudo evidenciar que carece de un componente que analice y alinee la estrategia, objetivos y/o metas institucionales con la estrategia de tecnología de la información. También se pudo evidenciar que el documento HOJA DE RUTA DE ARQUITECTURA EMPRESARIAL 2023, contiene actividades que no se encuentran descritas en la sección de los proyectos priorizados en el PETI. Esto pudo obedecer a desconocimiento de la normatividad y/o falta de personal idóneo en el área. Como consecuencia, se dificulta avanzar en temas relacionados con TIC en la entidad, mostrando debilidades en la implementación de requerimientos legales.

El líder del proceso de Gestión TIC sugiere la necesidad de involucrar al proceso de entrega y supervisión para la formulación del plan

4. IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

HALLAZGO No. 6 El artículo 3 de la Resolución 500 de 2021 del Ministerio de las Tecnologías y las Comunicaciones establece que los sujetos obligados "*…deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución"*. Solicitada la información y practicado el diagnóstico con el ingeniero apoyo del proceso se pudo determinar que el modelo de seguridad y privacidad no se encuentra implementado en la entidad. Esto pudo obedecer a desconocimiento de la normatividad y/o falta de personal idóneo en el área. Como consecuencia, se dificulta avanzar en temas relacionados con la seguridad y privacidad de la información, permaneciendo vulnerables ante cualquier amenaza sobre seguridad de la información que se presente en la entidad.

5. MARCO DE ARQUITECTURA EMPRESARIAL DE LA ENTIDAD

HALLAZGO No. 7 Establece el Decreto 1083 de 2015 en el numeral 2 del artículo 2.2.35.3. que las entidades del Estado del orden nacional y territorial, los organismos autónomos y de control deberán *"Liderar la definición, implementación y mantenimiento de la arquitectura empresarial de la entidad …"*. En el mismo sentido el Min TIC expidió la Resolución 1878 de 2023 mediante la cual "*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.* Teniendo en cuenta que el Marco de Referencia Empresarial está conformado por tres componentes se solicitan las evidencias de la estructuración, definición e implementación del Modelo de Arquitectura Empresarial (MAE), el Modelo de Gestión y Gobierno de TI (MGGTI) y el Modelo de Gestión de Proyectos de TI (MGPTI) en la entidad. Sin embargo, se informa por parte del proceso auditado que el Marco de Arquitectura Empresarial no se ha implementado en Distriseguridad. Esto pudo obedecer a desconocimiento de la normatividad y/o falta de personal idóneo en el área. Como consecuencia, se dificulta avanzar en temas relacionados con TIC en la entidad, permaneciendo con debilidades en la implementación de requerimientos legales.

6. PROCEDIMIENTOS DEL PROCESO DE GESTIÓN TIC

HALLAZGO No. 8 La GUÍA PARA LA GESTIÓN POR PROCESOS EN EL MARCO DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG), Versión 1, del Departamento Administrativo de la Función Pública, establece unos lineamientos para la adecuada adopción de los procedimientos. Revisado el documento donde se presentan los procedimientos de la entidad, se puede observar que los registrados con los códigos PGTICS-004 y PGTICS-005 no cumplen a cabalidad con las características definidas por el Departamento Administrativo de la Función Pública, al no presentar un ordenamiento de las tareas necesarias para el cumplimiento de la operación. Esto puede obedecer a desconocimiento de la normatividad y/o falta de personal idóneo en el área. Como consecuencia, se dificulta avanzar en temas relacionados con TIC en la entidad, permaneciendo con debilidades en la implementación de requerimientos legales.

HALLAZGO No. 9 Los procedimientos de la entidad presentan en su construcción unos puntos de control, de los cuales se infiere que tienen como propósito garantizar que el procedimiento esté siendo ejecutado correctamente y que el objetivo de éste se alcance. Requeridas las evidencias sobre el cumplimiento de los puntos de control, no se obtiene información ni evidencias. Esto puede obedecer a la inadecuada implementación o definición de los procedimientos o falta de control para ejecutar los procedimientos del proceso. Como consecuencia, se pueden materializar riegos que dificulten el cumplimiento del objetivo del proceso de Gestión TIC.

7. IPv6 (Internet Protocol Versión 6)

HALLAZGO No. 10 El Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Resolución No. 2710 de 2017 generó los lineamientos para la adopción del protocolo IPv6. Mediante la Resolución 1126 de 2021 estableció como plazo máximo para la transición de IPv4 a IPv6 el 31 de diciembre de 2022. Requerida la información al proceso auditado se informó que la entidad no ha realizado ninguna acción encaminada a la adopción del protocolo IPv6. Esto pudo obedecer a desconocimiento de la normatividad. Como consecuencia, se dificulta avanzar en temas relacionados con TIC en la entidad, permaneciendo con debilidades en la implementación de requerimientos legales.

8. GOBIERNO EN LÍNEA – PÁGINA WEB

HALLAZGO No. 11 La 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 establece la información que se debe publicar por las entidades en sus páginas web. Revisada la página web de la entidad se encuentra que esta, aunque contiene los módulos para cargar la información, carece de ella y en algunos casos es incompleta y/o desactualizada. Esto puede generarse por falta de supervisión sobre el contratista encargado de la página web de la entidad. Como consecuencia, se acrecientan debilidades en la implementación de requerimientos legales.

9. POLÍTICA DE GOBIERNO DIGITAL

HALLAZGO No. 12 El Ministerio de Tecnologías de la Información y las Comunicaciones presenta el documento MANUAL DE GOBIERNO DIGITAL Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2). Señalando aspectos como la planeación de los habilitadores de la política e inicio de la ejecución de la política. Revisado el documento denominado POLÍTICA INSTITUCIONAL DE GOBIERNO DIGITAL, Código: PIDEYP - 001 Versión: 1.0 Fecha: 18/11/2021, se puede evidenciar la falta de cumplimiento y/o seguimiento de la política, debido que de 27 estrategias definidas solo se ha dado cumplimiento a 3 de ellas. Esto puede generarse por falta de liderazgo en el proceso de Gestión TIC. Como consecuencia, se presentan debilidades en la implementación de requerimientos legales.

HALLAZGO No. 13 – PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN Establece el Procedimiento código PDEYP-006 “Control de Registros y Documentos”, que el líder del proceso debe: elaborar el formato del

registro (documento), solicitar al proceso de Direccionamiento Estratégico y Planeación la asignación del código, diligencia el formato de solicitud de elaboración, actualización o anulación de documentos y envía a planeación el formato de solicitud diligenciado y el documento para su archivo, para que el responsable de la administración del SIG realice control de los registros y/o documentos por medio del listado maestro de registros y listado maestro de documentos. En desarrollo de las actividades de auditoría se recibe copia de la POLÍTICA DE SEGURIDAD DIGITAL Código: PIDEYP - 001 Versión: 1.0 Fecha: 18/11/2021 y de la POLÍTICA INSTITUCIONAL DE GOBIERNO DIGITAL, Código: PIDEYP - 001 Versión: 1.0 Fecha: 18/11/2021, de lo que se pudo evidenciar que las dos políticas presentan el mismo código, versión y fecha. Esto puede generarse por fallas en la ejecución del procedimiento *Control de Registros y Documentos* en el Proceso de Direccionamiento Estratégico y Planeación. Como consecuencia, se presenta duplicidad de códigos en los documentos del SIG.

Manifiesta la asesora de implementación MIPG que el formato de las políticas es el mismo código para todas ellas. Sin embargo, señala el P.U.E. Planeación que efectivamente las políticas deben tener códigos diferentes al ser documentos distintos.

10. POLÍTICA DE SEGURIDAD DIGITAL

HALLAZGO No. 14 Se presenta, por parte del proceso auditado, el documento denominado POLÍTICA INSTITUCIONAL DE SEGURIDAD DIGITAL, Código: PIDEYP – 001, Versión: 1.0, Fecha: 18/11/2021, el cual establece una política y unas estrategias a implementar. Realizada la verificación de estos aspectos (política y estrategias) se establece que no se cumple con ninguno de ellos. Esto puede ocurrir por falta de liderazgo y control por parte del responsable del proceso y/o falta de personal idóneo en el área. Como consecuencia, se está generando la ralentización en el avance de temas estratégicos TIC.

11. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

HALLAZGO No. 15 El Ministerio de Tecnologías de la Información y las Comunicaciones presenta la Guía de Gestión de Riesgos – Seguridad y Privacidad, Guía No. 7, en la que se establece que se debe diseñar un plan de tratamiento de riesgos incluyendo los de Seguridad de la información, en el cual se defina qué tratamiento se dará a los riesgos, qué acciones se implementarán, quienes serán los responsables de ésta implementación, además, que el plan debe plantear claramente cada acción, etapa y procedimientos que se ejecutarán para poder ser monitoreado. Requerido el PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION de la entidad, el proceso Gestión TIC presenta el documento con ese nombre, Código: MGTICS – 002 Versión: 1.0 Fecha: 18/11/2021, en él que se pudo evidenciar que no se cumple con los parámetros y lineamientos establecidos en la Guía de Gestión de Riesgos – Seguridad y Privacidad. Guía No. 7, al no contemplar estrategias encaminadas a la adopción del Modelo de Seguridad y Privacidad de la Información, a la elaboración de una Matriz de Inventario y Clasificación de Activos de Información, al levantamiento de la Infraestructura Tecnológica Crítica, al tratamiento y monitoreo de riesgos de Seguridad de la información. Esto puede ocurrir por falta de idoneidad por parte del responsable del proceso y/o falta de personal idóneo en el área. Como consecuencia, no se gestionan los riesgos de Seguridad de la información de acuerdo con los lineamientos establecidos por las autoridades lo que podría generar alteración, mal uso y pérdida de la información.

Luego de revisar los hallazgos de la auditoría, el asesor de Control Interno procede a indicar cuales son las recomendaciones derivadas de lo observado en esta auditoría, así:

RECOMENDACIONES

- ✓ Desarrollar las acciones necesarias encaminadas a ejercer los controles establecidos en los mapas de riesgos institucional y de corrupción.
- ✓ Desarrollar el Plan Estratégico de Tecnologías de la Información – PETI – de la entidad, de acuerdo con las guías y modelos propuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- ✓ Establecer en el PETI de Distriseguridad un componente que analice y alinee la estrategia, objetivos y/o metas institucionales con la estrategia de tecnología de la información.
- ✓ Implementar el Modelo de Seguridad y Privacidad de la Información en la entidad, como habilitador de la Política de Gobierno Digital, siguiendo los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- ✓ Implementar el Modelo de Arquitectura Empresarial de la entidad, con base en los preceptos establecidos en el Marco de Referencia de Arquitectura Empresarial del Estado Colombiano.
- ✓ Replantear los procedimientos de la entidad, de acuerdo con lo establecido en La GUÍA PARA LA GESTIÓN POR PROCESOS EN EL MARCO DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG), Versión 1, del Departamento Administrativo de la Función Pública.
- ✓ Desarrollar acciones encaminadas a realizar la transición del protocolo IPv4 a la implementación del protocolo IPv6, para dar cumplimiento a lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Resolución No. 2710 de 2017 y 1126 de 2021
- ✓ Tomar medidas de impacto sobre la información que debe estar publicada en la página web institucional y que a la fecha no se encuentra alojada en el portal o se encuentra desactualizada.
- ✓ Revisar los enlaces de la página web de la entidad que no contienen información o que se encuentran dañados.
- ✓ Orientar los esfuerzos de la entidad para lograr implementar los habilitadores de la POLÍTICA INSTITUCIONAL DE GOBIERNO DIGITAL.
- ✓ Restructurar los planes estratégicos de TIC, con el propósito que se establezcan actividades, indicadores y estrategias de implementación a las que se les haga seguimiento efectivo.
- ✓ Revaluar la matriz de riesgos institucional y de corrupción, con el propósito de alcanzar que los riesgos, y en consecuencia los controles, impacten de manera clara sobre el objetivo del proceso, de acuerdo con lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones en la Guía de Gestión de Riesgos – Seguridad y Privacidad, Guía No. 7
- ✓ Incluir en el cronograma del proceso las actividades que se establezcan para la implementación de las políticas y planes institucionales adoptados por la entidad.
- ✓ Realizar el inventario de sistemas de información con que cuenta Distriseguridad.
- ✓ Crear la tabla de retención documental del proceso, adoptarla y utilizarla.
- ✓ Fortalecer institucionalmente el área de TIC para que esta cuente con un responsable vinculado de manera formal a la planta de personal de la entidad.

Por último, se dan a conocer las conclusiones a las que se llegaron de la auditoría realizada:

CONCLUSIONES

De acuerdo con la evaluación realizada al cumplimiento de las disposiciones, lineamientos, normativa y procedimientos vigentes, asociados a la Gestión del área TIC, se puede resaltar como aspecto positivo la publicación de los planes institucionales y estratégicos de los que trata el decreto 612 de 2018, correspondientes al área de Tecnología de la Información y Comunicación "TIC" (Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad y Privacidad de la Información). De igual forma se resalta que en el tema de gobierno digital, se cuenta con una pagina web que cumple con los lineamientos técnicos de accesibilidad web requeridos por el anexo 1 de la Resolución 1519 de 2020 emitida por MINTIC. No obstante, se identificaron deficiencias relacionadas con cumplimientos normativos, al no hallar evidencias de la implementación del Modelo de Seguridad y Privacidad de la Información "MSPI", del Marco de Arquitectura Empresarial, de la implementación del protocolo IPv6. Además, se identificaron temas por fortalecer, relacionados con las diferentes políticas, la formulación de los diferentes planes estratégicos, la gestión de riesgos y la gestión documental relacionada con TIC.

En la actualidad las oficinas de TIC desempeñan un rol estratégico en la modernización y la eficiencia de las operaciones de una entidad pública. En ese sentido, el Decreto 415 de 2016, a través del cual se definen lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones", establece en su artículo 2.2.35.4 que 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.

Por tal motivo, debido a criticidad de las debilidades encontradas, se hace necesario el fortalecimiento institucional del área de TIC de la entidad, para que esta cuente con un responsable vinculado de manera formal a la entidad y de esta manera:

- ✓ Garantizar que haya una persona claramente identificada y responsable de la gestión de las tecnologías de la información y comunicación dentro de la entidad. Esto promueve la responsabilidad y la coordinación eficiente de los recursos y actividades relacionadas con la tecnología.
- ✓ Asegurar, que las iniciativas de TIC estén alineadas con los objetivos estratégicos de la entidad y contribuyan al logro de sus metas.
- ✓ Desempeñar un papel clave en la gestión de recursos humanos y presupuestarios relacionados con la tecnología. Esto incluye la planificación y asignación de recursos para proyectos tecnológicos y la supervisión del gasto en tecnología.
- ✓ Liderar la implementación de políticas y medidas de seguridad de la información para proteger los datos sensibles y garantizar el cumplimiento de las regulaciones relacionadas con la privacidad y la ciberseguridad.
- ✓ Identificar oportunidades para mejorar la eficiencia operativa a través de la implementación de soluciones tecnológicas adecuadas (automatización de procesos y optimización de sistemas).

- ✓ Coordinar eficazmente proyectos de tecnología complejos, para asegurar que se entreguen a tiempo y dentro del presupuesto.
- ✓ Liderar la interacción con proveedores de tecnología y otras entidades externas de manera eficiente.
- ✓ La implementación efectiva del marco de arquitectura empresarial.

Se informa que una vez terminada la reunión de cierre, se enviara via correo el informe preliminar de la auditoria proceso gestión TIC para su conocimiento y observaciones, para lo cual se da un plazo de 3 dias. Luego de vencido el termino si no se recibe respuesta u observaciones el informe quedara en firme.

Siendo las 12:05 se da por finalizada la reunión de cierre de la auditoría.

ACCIONES	CUMPLIMIENTO SI O NO	RESPONSABLE	FECHAS
Enviar informe preliminar de auditoria proceso gestión TIC		Asesor de Control Interno	10/10/2023
Dar respuesta al informe preliminar de auditoria proceso gestión TIC en caso de tener alguna observación		PUE Planeación	13/10/2023

FIRMAS:

GILDARDO PÉREZ TORRES
Asesor Control Interno

ENRIQUE NICOLÁS BRIEVA JURADO
P.U.E Planeación

VICTOR SANTIS
Ingeniero apoyo Gestión TIC

GIOVANA VENEGAS
Asesora Implementación MIPG

FRANCISCO MURILLO ZABALA
Apoyo Control Interno