PROCESO: GESTIÓN TIC	**DEPENDENCIA AUDITADA: TIC**
FECHA: 18 de octubre de 2023	**Fecha de Inicio: 29 de marzo de 2023**
LUGAR: OFICINA DISTRISEGURIDAD	**Fecha de Finalización: 10 de septiembre de 2023**
TIPO DE INFORME: FINAL	**AUDITORIA No. 001**

1. OBJETIVO DE LA AUDITORÍA:

Verificar, a través de los procedimientos de auditoría, el cumplimiento del objetivo del proceso de Gestión TIC de "Proporcionar lineamientos y servicios tecnológicos en materia de gestiónde la información, mediante la administración de la infraestructura tecnológica, los sistemas deinformación y las comunicaciones en forma oportuna, eficiente y transparente que permita la interoperabilidad, el gobierno abierto, el fortalecimiento, integración e implementación de la innovación en tecnologías de información, para garantizar la disponibilidad, integridad y confidencialidad de la misma en la realización de las actividades y cumplimiento de losobjetivos estratégicos de Distriseguridad, en la toma de decisiones y el desarrollo institucional".

2. ALCANCE DE LA AUDITORÍA:

El periodo de evaluación comprende desde el 1 de enero al 28 de marzo de 2023 teniendo en cuenta lo establecido en:

- ✓ Plan Estratégico de Tecnologías de la Información y las Comunicaciones
- ✓ Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- ✓ Plan de Seguridad y Privacidad de la Información
- ✓ Procedimientos del Proceso de Gestión TIC
- ✓ Seguimiento a los Indicadores y Riesgos del proceso.

3. CRITERIOS DE LA AUDITORÍA:

- ✓ Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- ✓ Documentación interna (procedimiento, planes, políticas, directrices, etc.) del Proceso de Gestión TIC de la entidad.

4. RESUMEN EJECUTIVO:

La Oficina de Control Interno en ejercicio de su rol de Evaluación y Seguimiento, así como en cumplimiento del Plan Anual de Auditoría 2023, incluyó la realización de una auditoría al proceso de Gestión TIC, actividad que dio inicio el 29 de marzo de 2023, con la reunión de

apertura de esta, aplicando en su desarrollo las normas de auditoría generalmenteaceptadas, con el fin de verificar el cumplimiento del objetivo del proceso en procura de asegurar el cumplimiento de la misión encomendada y la visión proyectada de la entidad.

De acuerdo con los objetivos y alcances definidos, el desarrollo del trabajo se abordó siguiendo la metodología y etapas que se describen a continuación:

- Identificación del proceso de Gestión de Proyectos, sus riesgos y controles asociados.
- Identificación de los procedimientos del proceso y sus controles
- Solicitud de información y entrevista al líder del proceso
- Recolección de información
- Análisis de la información

Una vez dado inicio al proceso de auditoría de Control Interno, se solicitó información sobre el proceso a través de memorando No. 0484 de fecha 29 de marzo de 2023. Respondido mediante correo electrónico, anexando la información que se encontraba disponible.

Con fecha 9 de octubre de 2023 se realizó la reunión de cierre de la auditoría y se dio a conocer a los miembros del proceso de Gestión TIC el Informe Preliminar.

Con fecha 17 de octubre de 2023 el líder del proceso remite el memorando No. 1626 mediante el cual acepta todos los hallazgos de la auditoría y señala que estos serán analizados y tratados.

Con fecha 20 de octubre de 2023 se remite el Informe Final de la auditoría al proceso de Gestión TIC, para que se genere el correspondiente plan de mejoramiento a los hallazgos presentados.

5. OBSERVACIONES:

En desarrollo del proceso de auditoría, se solicitaron los documentos correspondientes a los riesgos del proceso y puntos de control de los procedimientos señalados en el Manual de Procesos y Procedimientos de Distriseguridad.

Tomando como base los documentos señalados se realizó la revisión correspondiente, de lo cual queda registro en las siguientes observaciones:

5.1 RIESGOS DEL PROCESO

La ISO 27001 define el evento en la seguridad de la información como Cualquier ocurrencia identificada en un sistema de información, servicio o estado de la red que indica una posible infracción en la seguridad de la información, en la política o fallo en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

Los riesgos asociados al proceso de Gestión TIC se encuentran contemplados en los mapas de riesgos Institucional (Código MDEYP-002 Versión 1) y de Corrupción (Código MDEYO-012 Versión1).

MAPA	RIESGOS	CONTROLES	ACCIONES
RIESGOS INSTITUCIONALES	Posibilidad de eventos que afecten la totalidad o parte de la infraestructura tecnológica interna o externa de la entidad	El P.U.E. Planeación e Ingeniero TICS elaborarán a principio de vigencia mes de enero un cronograma de todas las actividades que se deben tener en cuenta para obtener una seguridad digital oportuna y cumplir con los lineamientos de la política institucional de seguridad digital. El P.U.E. Planeación e ingeniero TICS se reunirán a principios de vigencia mes de enero con el fin de realizar diagnósticos de seguridad digital y actualizarán la política si se requiere.	Cronograma de Gestión TICS Diagnóstico de Seguridad Digital Actualización de Política de Seguridad Digital
RIESGOS INSTITUCIONALES	Posibilidad de ineficacia en los controles de acceso.	El P.U.E. Planeación e Ingeniero TICS elaborarán a principio de vigencia mes de enero un cronograma de todas las actividades que se deben tener en cuenta para obtener una seguridad digital oportuna y cumplir con los lineamientos de la política institucional de seguridad digital. El P.U.E. Planeación e ingeniero TICS se reunirán a principios de vigencia mes de enero con el fin de realizar diagnósticos de seguridad digital y actualizarán la política si se requiere.	Cronograma de Gestión TICS Diagnóstico de Seguridad Digital Actualización de Política de Seguridad Digital
RIESGOS INSTITUCIONALES	Posibilidad de inoperancia de la infraestructura tecnológica debido a escasez de recursos para la continuidad de la operación	El P.U.E. Planeación realizará un diagnóstico y presupuesto a principios de la vigencia de lo necesario para la operabilidad de la infraestructura tecnológica cumpliendo estándares de seguridad digital, oficiando a la Dirección General y Dirección Administrativa y Financiera	Diagnóstico TICS Presupuesto TICS Oficio a la Dirección General y Dirección Administrativa y Financiera
RIESGOS INSTITUCIONALES	Posibilidad de daños a los equipos debido a mal servicio de Soporte técnico externo.	El P.U.E. Planeación e ingeniero Tics elaboraran una lista de soportes técnicos requeridos y que cumplan con los requisitos necesarios para las necesidades de la entidad.	Lista de soportes técnicos
RIESGOS DE CORRUPCIÓN	Posibilidad que, por acción u omisión mediante el uso indebido del poder, de los recursos o de la información se lesionen los intereses de la entidad realizando acceso indebido a los sistemas para el uso no apropiado de la información contenida en los sistemas de un(os) colaborador(es) para el favorecimiento propio o de un	El profesional especializado de planeación como líder del proceso de gestión TIC e ingeniero TIC debe actualizar anualmente la política de seguridad digital y realizar seguimiento mensual del cumplimiento de las herramientas contenidas en la misma, en cuanto a hardware, software, redes, información, autenticación de usuarios, contraseñas para bases de datos con cambios periódicos estipulados, controles de los equipos informáticos, trazabilidad de la información y	Actualización de las políticas de seguridad creando controles para el fortalecimiento de la seguridad de la información

	tercero	responsables.	
		P.U.E. Planeación solicitará por medio de oficio a principio de la vigencia al proceso de gestión talento humano incluir en el plan de capacitación sensibilización a todo el personal sobre temas de corrupción y ética	Oficio para proceso GTH solicitando capacitaciones referentes a temas de ética.

5.1.1. Evaluación del diseño de estructura del riesgo

No.	Descripción del Riesgo	Impacto (¿Qué?)	Causa Inmediata (¿Cómo?)	Causa Raíz (¿Por qué?)	Resultado de la Evaluación
1	Posibilidad de eventos que afecten la totalidad o parte de la infraestructura tecnológica interna o externa de la entidad	**SIN INFORMACIÓN**	eventos que afecten la totalidad o parte de la infraestructura tecnológica interna o externa de la entidad	**SIN INFORMACIÓN**	Deficiencias en la estructura del riesgo de acuerdo con lo establecido por la Guía para la administración del riesgo y el diseño de controles en entidades públicas. En este sentido no contiene el riesgo el impacto generado ni la causa raíz.
2	Posibilidad de ineficacia en los controles de acceso.	**SIN INFORMACIÓN**	ineficacia en los controles de acceso.	**SIN INFORMACIÓN**	Deficiencias en la estructura del riesgo de acuerdo con lo establecido por la Guía para la administración del riesgo y el diseño de controles en entidades públicas. En este sentido no contiene el riesgo el impacto generado ni la causa raíz.
3	Posibilidad de inoperancia de la infraestructura tecnológica debido a escasez de recursos para la continuidad de la operación	**SIN INFORMACIÓN**	inoperancia de la infraestructura tecnológica	escasez de recursos para la continuidad de la operación	Deficiencias en la estructura del riesgo de acuerdo con lo establecido por la Guía para la administración del riesgo y el diseño de controles en entidades públicas. En este sentido no contiene el riesgo el impacto generado.
4	Posibilidad de daños a los equipos debido a mal servicio de Soporte técnico externo.	**SIN INFORMACIÓN**	daños a los equipos	Mal servicio de Soporte técnico externo.	Deficiencias en la estructura del riesgo de acuerdo con lo establecido por la Guía para la administración del riesgo y el diseño de controles en entidades públicas. En este sentido no contiene el riesgo el impacto generado.

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.

5.1.2. Evaluación de la estructura del control

No.	Riesgo	Descripción del Control	Responsable de Ejecutar el Control	Acción / Propósito (Verificar, validar, cotejar, comparar)	Como se hace / Como se ejecuta	Frecuencia	Fuente para el análisis	Acciones en caso de desviaciones	Evidencia del Control	Resultado de la Evaluación
1	Posibilidad de eventos que afecten la totalidad o parte de la infraestructura tecnológica interna o externa de la entidad	**CONTROL No. 1** El P.U.E. Planeación e Ingeniero TICS elaborarán a principio de vigencia mes de enero un cronograma de todas las actividades que se deben tener en cuenta para obtener una seguridad digital oportuna y cumplir con los lineamientos de la política institucional de seguridad digital.	P.U.E. Planeación e Ingeniero TICS	Elaborarán un cronograma de todas las actividades que se deben tener en cuenta para obtener una seguridad digital oportuna y cumplir con los lineamientos de la política institucional de seguridad digital	**SIN INFORMACIÓN**	A principio de vigencia mes de enero	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	Atributos de Eficiencia: Tipo - Preventivo Implementación - Manual Atributos Informativos: Documentación - Sin Información Frecuencia - Aleatoria Evidencia - Con registro Al revisar la estructura del control se pudo evidenciar debilidades en cuanto a su diseño: 1. La acción de elaborar un cronograma corresponde más con una actividad del proceso que con una acción de control, ya que estas deben involucrar verbos como verificar, validar, cotejar, comparar. Por ejemplo, para este caso el control podría estar dirigido a verificar el cumplimiento del cronograma. 2. La estructura del control no contiene los siguientes elementos: Cómo se hace, fuente para el análisis, acciones en caso de desviaciones. Finalmente se considera que el control no reduce o mitiga la materialización del riesgo.

No.	Riesgo	Descripción del	Responsable	Acción / Propósito	Como se hace	Frecuencia	Fuente para el	Acciones en	Evidencia del	Resultado de la Evaluación
1	Posibilidad de eventos que afecten la totalidad o parte de la infraestructura tecnológica interna o externa de la entidad	**CONTROL No. 2** El P.U.E. Planeación e ingeniero TICS se reunirán a principios de vigencia mes de enero con el fin de realizar diagnósticos de seguridad digital y actualizarán la política si se requiere.	P.U.E. Planeación e ingeniero TICS	Se reunirán con el fin de realizar diagnósticos de seguridad digital y actualizarán la política si se requiere.	**SIN INFORMACIÓN**	A principio de vigencia, mes de enero	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	Atributos de Eficiencia: Tipo - Preventivo Implementación – Manual Atributos Informativos: Documentación – Sin Información Frecuencia – Aleatoria Evidencia - Con registro Al revisar la estructura del control se pudo evidenciar debilidades en cuanto a su diseño: 1. La acción de realizar un diagnóstico corresponde más con una actividad del proceso que con una acción de control, ya que estas deben involucrar verbos como verificar, validar, cotejar, comparar. Por ejemplo, para este caso el control podría estar dirigido a verificar el cumplimiento de las acciones generadas con los resultados del diagnóstico. 2. La estructura del control no contiene los siguientes elementos: Cómo se hace, fuente para el análisis, acciones en caso de desviaciones. Finalmente se considera que el control no reduce o mitiga la materialización del riesgo.

No.	Riesgo	Descripción del	Responsable	Acción / Propósito	Como se hace	Frecuencia	Fuente para el	Acciones en	Evidencia del	Resultado de la Evaluación
2	Posibilidad de ineficacia en los controles de acceso.	**CONTRO No. 1** El P.U.E. Planeación e Ingeniero TICS elaborarán a principio de vigencia mes de enero un cronograma de todas las actividades que se deben tener en cuenta para obtener una seguridad digital oportuna y cumplir con los lineamientos de la política institucional de seguridad digital.	P.U.E. Planeación e Ingeniero TICS	elaborarán un cronograma de todas las actividades que se deben tener en cuenta para obtener una seguridad digital oportuna y cumplir con los lineamientos de la política institucional de seguridad digital	**SIN INFORMACIÓN**	A principio de vigencia mes de enero	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	<u>Atributos de Eficiencia:</u> Tipo - Preventivo Implementación – Manual <u>Atributos Informativos</u>: Documentación – Sin Información Frecuencia – Aleatoria Evidencia - Con registro Al revisar la estructura del control se pudo evidenciar debilidades en cuanto a su diseño: 1. La acción de elaborar un cronograma corresponde más con una actividad del proceso que con una acción de control, ya que estas deben involucrar verbos como verificar, validar, cotejar, comparar. Por ejemplo, para este caso el control podría estar dirigido verificar el cumplimiento del cronograma. 2. La estructura del control no contiene los siguientes elementos: Como se hace, fuente para el análisis, acciones en caso de desviaciones. Finalmente se considera que el control no reduce o mitiga la materialización del riesgo.

No.	Riesgo	Descripción del	Responsable	Acción / Propósito	Como se hace	Frecuencia	Fuente para el	Acciones en	Evidencia del	Resultado de la Evaluación
2	Posibilidad de ineficacia en los controles de acceso	**CONTROL No. 2** El P.U.E. Planeación e ingeniero TICS se reunirán a principios de vigencia mes de enero con el fin de realizar diagnósticos de seguridad digital y actualizarán la política si se requiere.	P.U.E. Planeación e ingeniero TICS	Se reunirán con el fin de realizar diagnósticos de seguridad digital y actualizarán la política si se requiere.	**SIN INFORMACIÓN**	A principio de vigencia mes de enero	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	Atributos de Eficiencia: Tipo - Preventivo Implementación – Manual Atributos Informativos: Documentación – Sin Información Frecuencia – Aleatoria Evidencia - Con registro Al revisar la estructura del control se pudo evidenciar debilidades en cuanto a su diseño: 1. La acción de realizar un diagnóstico corresponde más con una actividad del proceso que con una acción de control, ya que estas deben involucrar verbos como verificar, validar, cotejar, comparar. Por ejemplo, para este caso el control podría estar dirigido a verificar el cumplimiento de las acciones generadas con los resultados del diagnóstico. 2. La estructura del control no contiene los siguientes elementos: Como se hace, fuente para el análisis, acciones en caso de desviaciones. Finalmente se considera que el control no reduce o mitiga la materialización del riesgo.

No.	Riesgo	Descripción del	Responsable	Acción / Propósito	Como se hace	Frecuencia	Fuente para el	Acciones en	Evidencia del	Resultado de la Evaluación
3	Posibilidad de inoperancia de la infraestructura tecnológica debido a escasez de recursos para la continuidad de la operación	El P.U.E. Planeación realizará un diagnóstico y presupuesto a principios de la vigencia de lo necesario para la operabilidad de la infraestructura tecnológica cumpliendo estándares de seguridad digital, oficiando a la Dirección General y Dirección Administrativa y Financiera	P.U.E. Planeación	Realizará un diagnóstico y presupuesto de lo necesario para la operabilidad de la infraestructura tecnológica	Cumpliendo estándares de seguridad digital, oficiando a la Dirección General y Dirección Administrativa y Financiera	A principios de la vigencia	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	<u>Atributos de Eficiencia:</u> Tipo - Preventivo Implementación – Manual <u>Atributos Informativos</u>: Documentación – Sin Información Frecuencia – Aleatoria Evidencia - Con registro Al revisar la estructura del control se pudo evidenciar debilidades en cuanto a su diseño: 1. La acción de realizar un diagnóstico y presupuesto corresponde más con una actividad del proceso que a una acción de control, ya que estas deben involucrar verbos como verificar, validar, cotejar, comparar. Por ejemplo, para este caso el control podría estar dirigido a verificar la ejecución del presupuesto y al cumplimiento de las acciones generadas con los resultados del diagnóstico. 2. La estructura del control no contiene los siguientes elementos: fuente para el análisis, acciones en caso de desviaciones. Finalmente se considera que el control no reduce o mitiga la materialización del riesgo.

No.	Riesgo	Descripción del	Responsable	Acción / Propósito	Como se hace	Frecuencia	Fuente para el	Acciones en	Evidencia del	Resultado de la Evaluación
4	Posibilidad de daños a los equipos debido a mal servicio de Soporte técnico externo.	El P.U.E. Planeación e ingeniero Tics elaboraran una lista de soportes técnicos requeridos y que cumplan con los requisitos necesarios para las necesidades de la entidad.	El P.U.E. Planeación e ingeniero Tics	Elaborarán una lista de soportes técnicos requeridos y que cumplan con los requisitos necesarios para las necesidades de la entidad.	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	**SIN INFORMACIÓN**	<u>Atributos de Eficiencia:</u> Tipo - Preventivo Implementación – Manual <u>Atributos Informativos</u>: Documentación – Sin Información Frecuencia – Aleatoria Evidencia - Con registro Al revisar la estructura del control se pudo evidenciar debilidades en cuanto a su diseño: 1. La acción de elaborar una lista de soportes técnicos requeridos corresponde más con una actividad del proceso que a una acción de control, ya que estas deben involucrar verbos como verificar, validar, cotejar, comparar. 2. No contiene la estructura del control los siguientes elementos: Como se hace, frecuencia, fuente para el análisis, acciones en caso de desviaciones. Finalmente se considera que el control no reduce o mitiga la materialización del riesgo.

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.

5.1.3. Evaluación de la ejecución del control

Sobre el cumplimiento de los controles contemplados en la matriz de riesgos institucionales se puede observar, respecto a cada uno de ellos, lo siguiente:

- **RIESGO 1**. Posibilidad de eventos que afecten la totalidad o parte de la infraestructura tecnológica interna o externa de la entidad

Control. El P.U.E. Planeación e Ingeniero TICS elaborarán a principio de vigencia mes de enero un cronograma de todas las actividades que se deben tener en cuenta para obtener una seguridad digital oportuna y cumplir con los lineamientos de la política institucional de seguridad digital.

Resultado del análisis.

Se pudo evidenciar la existencia del cronograma que contiene las actividades del área de TIC. Sin embargo, se pudo establecer que para el primer trimestre de 2023 el cumplimiento fue el que se detalla a continuación:

Número de actividades de Enero – Marzo: 14

Número de actividades ejecutadas de Enero – Marzo: 9

Cumplimiento: 64%

Por lo anterior, es necesario actualizar el control, debido que la sola existencia del cronograma no evita la materialización del riesgo, sino que es necesaria su ejecución y que las actividades programadas apunten a la prevención de eventos que afecten la infraestructura tecnológica de la entidad. De acuerdo con los resultados de la ejecución del cronograma TICS, se considera que el control no se ha cumplido.

Control. El P.U.E. planeación e ingeniero TICS se reunirán a principios de vigencia mes de enero con el fin de realizar diagnóstico de seguridad digital y actualizarán la política si se requiere.

Resultado del análisis. Solicitada la evidencia para este control, no se aportó acta de reunión de la revisión, ni autodiagnóstico de gobierno digital.

De acuerdo con los resultados obtenidos se considera que el control no se ha cumplido.

- **RIESGO 2.** Posibilidad de ineficacia en los controles de acceso**.**

El termino de ineficacia significa *"Incapacidad para producir el efecto deseado o para ir bien para determinada cosa"*. Las medidas de control de acceso están orientadas a controlar y monitorear los accesos a los medios de información de acuerdo con las políticas definidas por la organización. De acuerdo con lo anterior puede entenderse el riesgo como la posibilidad de que las medidas o políticas para el acceso a los medios de información de la entidad no permitan su control y/o monitoreo. Para el riesgo antes mencionado se encontraron definidos los siguientes controles en la matriz de riesgos:

Control. El P.U.E. Planeación e Ingeniero TICS elaborarán a principio de la vigencia, mes de enero, un cronograma de todas las actividades que se deben tener en cuenta para obtener una seguridad digital oportuna y cumplir con los lineamientos de la política institucional de seguridad digital.

Resultado del análisis. Se evidencia cronograma, pero en este no se encuentran detalladas actividades recurrentes respecto a la implementación de políticas, controles, validaciones respecto al control de acceso. Tampoco se han implementado los controles de acceso del MSPI. En este sentido el control no es acorde al riesgo identificado.

Control. El P.U.E. planeación e ingeniero TICS se reunirán a principios de vigencia, mes de enero, con el fin de realizar diagnósticos de seguridad digital y actualizarán la política si se requiere.

Resultado del análisis. No se evidencia acta de reunión de la revisión ni autodiagnóstico de gobierno digital. El control no es acorde al riesgo identificado.

- **RIESGO 3.** Posibilidad de inoperancia de la infraestructura tecnológica debido a escasez de recursos para la continuidad de la operación

La infraestructura tecnológica, es la estructura de hardware, software, los elementos de red, sistema operativo (SO) y el almacenamiento de datos, mediante la cual se soportan los servicios de Tecnología de la Información, requeridos para el funcionamiento de la entidad y elservicio que esta brinda a la ciudadanía en general. Al revisar la matriz de riesgos institucionales, se identificó el siguiente control para el riesgo:

Control. El P.U.E. planeación realizará un diagnóstico y presupuesto a principios de lavigencia de lo necesario para la operabilidad de la infraestructura tecnológica cumpliendo estándares de seguridad digital , oficiando a la Dirección General y Dirección Administrativa y Financiero.

Resultado del análisis. Solicitada la evidencia de la aplicación del control, no se suministraron copias del diagnóstico y presupuesto TIC; tampoco se suministraron copias de los oficios dirigidos a la Dirección General y Dirección Administrativa y Financiera remitiendo dichos documentos. De acuerdo con los resultados obtenidos se considera que el control nose ha cumplido.

- **RIESGO 4.** Posibilidad de daños a los equipos debido a mal servicio de Soporte técnico externo.

Control El P.U.E. Planeación e ingeniero TIC elaborarán una lista de soportes técnicos requeridos y que cumplan con los requisitos necesarios para las necesidades de la entidad.

Resultado del análisis. No se presenta evidencia de cumplimiento de este control.

- **RIESGO 5.** Posibilidad que, por acción u omisión mediante el uso indebido del poder, de los recursos o de la información se lesionen los intereses de la entidad realizando acceso indebido a los sistemas para el uso no apropiado de la información contenida en los sistemas de un(os) colaborador(es) para el favorecimiento propio o de un tercero.

Control. El profesional especializado de planeación como líder del proceso de gestión TIC e ingeniero TIC debe actualizar anualmente la política de seguridad digital y realizar seguimiento mensual del cumplimiento de las herramientas contenidas en la misma, en cuanto a hardware, software, redes, información, autenticación de usuarios, contraseñas para bases de datos con cambios periódicos estipulados, controles de los equipos informáticos, trazabilidad de la información y responsables.

Resultado del análisis. La política de seguridad digital aportada tiene fecha de noviembre de 2021. No evidencia actualización a marzo de 2023. No se evidencia implementación y seguimiento a las estrategias a implementar de la política.

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.

5.2 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (PETI)

De acuerdo con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano, el Plan Estratégico de las Tecnologías de la Información y Comunicaciones (en adelante PETI) es el artefacto que se utiliza para expresar la Estrategia de TI. El PETI hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI. Cada vez que una institución pública haceun ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.

5.2.1. Publicación de un Plan Estratégico de Tecnología de la Información.

El Decreto 1083 de 2015, establece en el artículo 2.2.22.3.14 lo siguiente: "*Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionalesy estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:*

(…)

10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI

11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

12. Plan de Seguridad y Privacidad de la Información

(…)"

Solicitada la evidencia de la existencia del PETI, esta fue entregada y al mismo tiempo se pudo evidenciar su publicación en la página web de la entidad en el siguiente enlace:

https://distriseguridad.gov.co/home/transparencia/planeacion-presupuestos-e-informes/

Se evidencia que la fecha de publicación del documento es 02 de enero de 2023.

5.2.2 Formulación del Plan Estratégico de Tecnología de la Información.

Establece el Decreto 1078 de 2015, en su artículo 2.2.9.1.2.2 lo siguiente: *"Lineamientos, Guías y Estándares. 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, los cuales harán parte integral de esta. La implementación de los lineamientos, guías y estándares se realizará en articulación con el Modelo Integrado de Planeación y Gestión - MIPG.*

Parágrafo 1. Los lineamientos y estándares son los requerimientos mínimos que todos los sujetos obligados deberán cumplir para el desarrollo y consecución de la Política de Gobierno Digital.

Parágrafo 2. Las guías corresponden a las recomendaciones que emita el Ministerio de Tecnologías de la Información y las Comunicaciones sobre temáticas que, por el desarrollo y evolución de la Política de Gobierno Digital, se considere oportuno informar a los sujetos obligados para promover las mejores prácticas utilizadas para su incorporación".

Analizado el documento publicado en la página web de la entidad, se pudo observar que este no se desarrolla ni detalla de acuerdo con las guías y modelos propuestos por el MINTIC, como, por ejemplo:

- Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI.

https://www.mintic.gov.co/arquitecturati/630/articles-15031_recurso_pdf.pdf

- Plan estratégico de tecnologías de la información - Producto tipo (Plantilla Tipo Cartilla PETI PLUS).

https://gobiernodigital.mintic.gov.co/portal/Transformate-con-Gobierno-Digital-/Caja-de-herramientas/#data=%7B%22filter%22:%2247263%22,%22page%22:3%7D

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, guíasy 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 propuestospor 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.

5.2.3. Alineación del PETI con la estrategia institucional.

De acuerdo con lo establecido por el Decreto 415 de 2016 artículo 2.2.35.3 numeral 1 la entidad debe liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan

Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado.

De igual manera el MGPTI.G.GEN.01 – Documento Maestro del Modelo de Gestión de Proyectos TI en el numeral 7.3.1 Liderazgo de proyectos de TI, establece: *"La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá supervisar el trabajo sobre el componente de TI conforme con los lineamientos de la Arquitectura Empresarial de la institución".*

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 el documento HOJA DE RUTA DE ARQUITECTURA EMPRESARIAL 2023, el cual contiene actividades que no se encuentran descritas en la sección de los proyectos priorizados en el PETI.

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 alos 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.

5.3 IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con el Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, la Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo.

Las entidades deben desarrollar las capacidades que permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación del habilitador Seguridad y Privacidad de la Información, el cual 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.

El artículo 2.2.9.1.2.2 del Decreto 1078 de 2015, estableció que el Ministerio de Tecnologías de la Información y las Comunicaciones debe expedir y publicar lineamientos, guías y estándares para facilitar la comprensión, sistematización e implementación integral de laPolítica de Gobierno Digital, los cuales harán parte integral de ésta, además, que la implementación de los lineamientos, guías y estándares se debe realizar en articulación con elModelo integrado de Planeación y Gestión - MIPG.

En ese sentido el Mintic expidió la resolución 500 de 2021 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, el cual en sus artículos 3 y 4 define:

*"**ARTÍCULO 3. Lineamientos generales.** Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales yformatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digitalque se relacionan en el Anexo 1 de la presente resolución.*

Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura critica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

ARTÍCULO 4. Sistema de gestión de seguridad de la información y seguridad digital. *Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia".*

De acuerdo con los lineamientos expedidos por MINTIC el Modelo de Seguridad y Privacidad de la Información "MSPI", contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Solicitada la información, registros y/o documentos que den cuentan de la implementación del modelo en la entidad no se suministran los soportes.

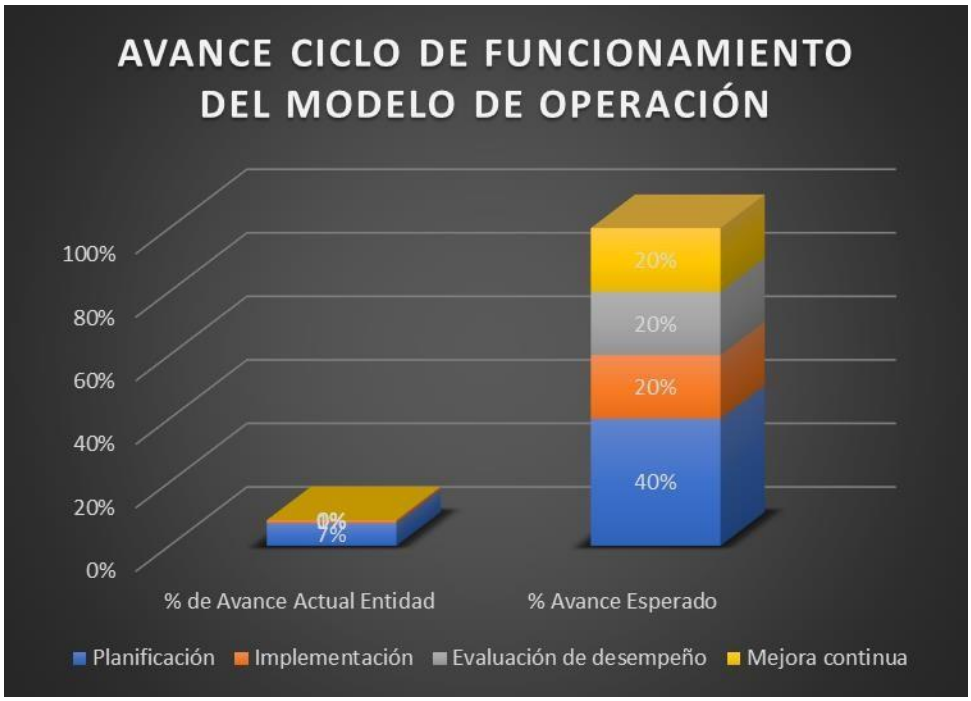
De igual manera se procedió a la aplicación del instrumento de evaluación dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC - en el enlace https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/ para diagnosticar el estado de la seguridad y privacidad de la información en la entidad, de lo cual se obtuvo el siguiente resultado:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Actual	Calificación Objetivo	Evaluación de Efectividad de Control
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	100	**REPETIBLE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	24	100	**REPETIBLE**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	23	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	22	100	**REPETIBLE**
A.9	CONTROL DE ACCESO	0	100	**INEXISTENTE**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	29	100	**REPETIBLE**
A.12	SEGURIDAD DE LAS OPERACIONES	9	100	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	24	100	**REPETIBLE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	7	100	**INICIAL**
A.15	RELACIONES CON LOS PROVEEDORES	20	100	**INICIAL**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	**INEXISTENTE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	24	100	**REPETIBLE**
A.18	CUMPLIMIENTO	41,5	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**19**	**100**	**INICIAL**

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	7%	40%
	Implementación	1%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		8%	100%



NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	INTERMEDIO
Repetible	CRÍTICO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

De acuerdo con el análisis de la anterior información se puede establecer que respecto a la implementación de los controles del modelo de seguridad y privacidad de la información la entidad se encuentra en un nivel inicial (19/100) y respecto al avance del ciclo de funcionamiento del modelo de operación (PHVA) la entidad se encuentra en 8%, lo cual es crítico.

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.

5.4 MARCO DE ARQUITECTURA EMPRESARIAL DE LA ENTIDAD

El Decreto número 1083 de 2015*, "por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública"* establece en el artículo 2.2.35.3. que para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades del Estado del orden nacional y territorial, los organismos autónomos y de control deberán: "… *Numeral 2. Liderar la definición, implementación y mantenimiento de la arquitectura empresarial de la entidad y/o sector en virtud de las definiciones y lineamientos establecidos en el marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información y las Comunicaciones (TIC) del Estado, la estrategia GEL y según la visión estratégica, las necesidades de transformación y marco legal específicos de suentidad o sector".*).

El Ministerio de Tecnologías de la Información y las Comunicaciones Mediante la Resolución 1978 del 26 de mayo de 2023 "*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".

El artículo 2.2.9.1.1.1 del Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, establece "… *los lineamientos generales de la Política de Gobierno Digital, entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio*".

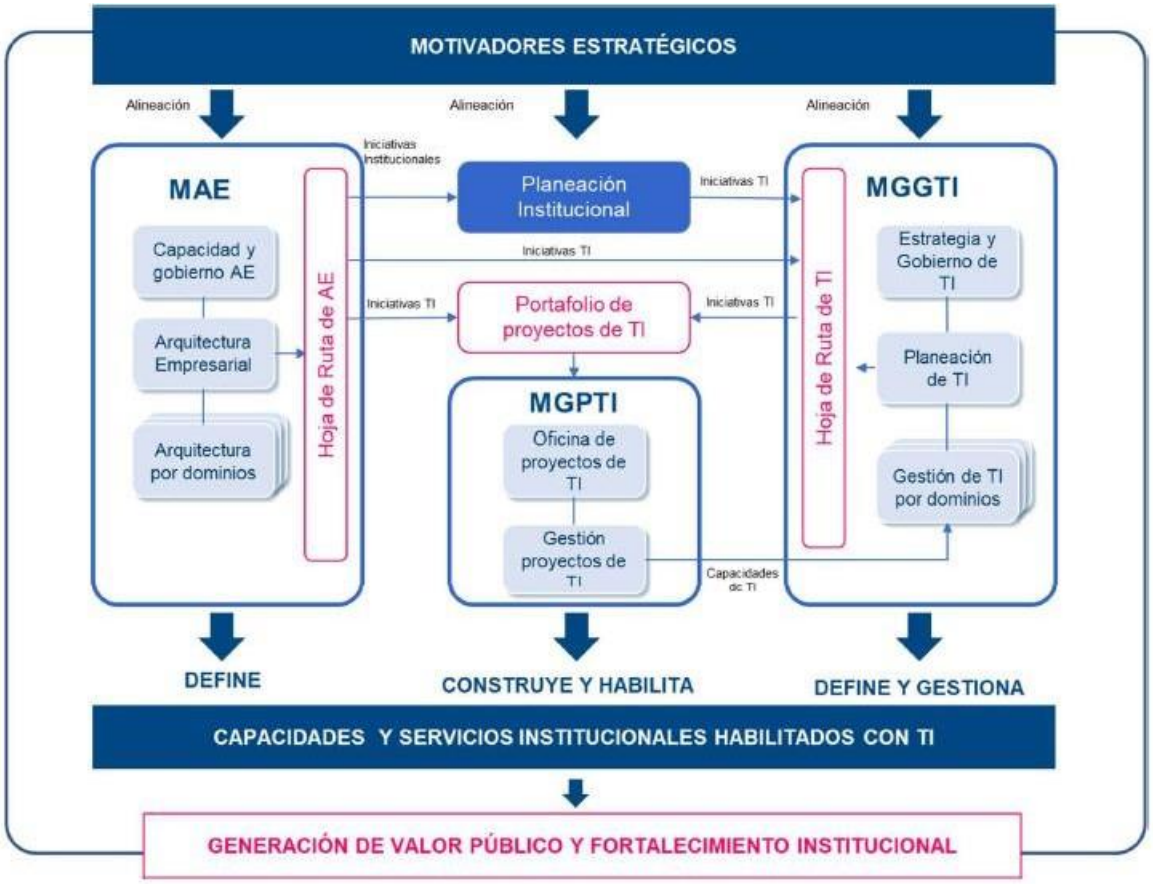
Así mismo, el parágrafo de este artículo señala que, *"para efectos de la aplicación, los Grupos de Interés de la Política de Gobierno Digital los conforman las entidades públicas, la academia, el sector privado, las organizaciones de la sociedad civil, los ciudadanos y, en general, los habitantes del territorio nacional".*

El numeral 3 del artículo 2.2.9.1.2.1. del Decreto 1078 de 2015 establece que los sujetos obligados desarrollarán las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación de los siguientes habilitadores: Arquitectura, Seguridad y Privacidad de la Información, Cultura y Apropiación y Servicios Ciudadanos Digitales. Donde el habilitador de Arquitectura tiene como propósito que *"los sujetos obligados desarrollen capacidades para el fortalecimiento institucional implementando el enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de proyectos con componentes de Tecnologías de la Información. Los sujetos obligados deberán articular su orientación estratégica, su modelo de gestión, su plan de transformación digital, y su estrategia de Tecnologías de Información y las Comunicaciones, con el objetivo de dar cumplimiento a la Política de Gobierno Digital".*

En ese sentido el MINTIC, en su objetivo de impulsar y facilitar la adopción del enfoque de Arquitectura Empresarial (AE) como un habilitador para el fortalecimiento institucional, creó el Marco de Referencia de Arquitectura Empresarial del Estado Colombiano (MRAE) como una herramienta que orienta el desarrollo y evolución de las arquitecturas empresariales institucionales y sectoriales; apoya la Gestión y Gobierno de las tecnologías de información en las entidades y el desarrollo de los proyectos con componentes de TI, buscando maximizar la generación de valor público.

El Marco de Referencia de Arquitectura Empresarial del Estado Colombiano (MRAE), se encuentra compuesto por tres modelos: el Modelo de Arquitectura Empresarial (MAE), el Modelo de Gestión y Gobierno de TI (MGGTI) y el Modelo de Gestión de Proyectos de TI (MGPTI), los cuales guían la aplicación de un enfoque de Arquitectura Empresarial para

facilitar la articulación entre la estrategia y planeación institucional, el modelo operativo y gestión de la entidad, y la gestión de TI.



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.

Se informa, por parte del sujeto de auditoría, que el Marco de Referencia de Arquitectura Empresarial no se ha implementado en Distriseguridad en concordancia con las guías establecidas por el MINTIC.

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.

5.5 PROCEDIMIENTOS DEL PROCESO DE GESTIÓN TIC

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, señala que *"Los procedimientos son el conjunto de especificaciones, relaciones y ordenamiento de las tareas requeridas para cumplir las actividades de un proceso, controlando las acciones que requiere la operación de la entidad en la medida en que especifican paso a paso qué se debe hacer en el proceso".*

Señala el mismo documento que, son características de los procedimientos las siguientes:

- *"Deben elaborarse en un formato amigable, es decir, que sea fácil de entender, interpretar y consignar.*
- *Las actividades que describen en los procedimientos deben ser muy claras.*
- *Las actividades deben describir una secuencia.*
- *Cada actividad debe tener un responsable.*
- *Los procedimientos deben de ser únicos, exclusivos.*
- *Debe tener un diagrama de flujo de las actividades descritas.*
- *El manual de procedimientos es la suma de los procedimientos de cada área.*
- *Los procedimientos deben ser descritos por las personas que más saben acerca de la operación.*
- *Los procedimientos deben de ser susceptibles de mejora".*

De igual manera, la guía indica: *"Recuerde que el objetivo principal de la gestión procesos es reducir el papeleo innecesario y, a su vez, dar una documentación precisa y concisa sobre qué se hace y cómo se hace en cada uno de los procesos de la entidad para que cualquier persona (independientemente de su conocimiento) se familiarice con él fácilmente".*

De acuerdo con la información suministrada por el proceso auditado en el documento denominado Procedimientos Gestión TIC, se tienen los siguientes:

No.	Procedimiento	Código	Versión
1	MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE ELEMENTOS TECNOLÓGICOS (HARDWARE Y SOFTWARE)	PGTICS-001	1.0
2	BACKUPS O RESPALDO DE LA INFORMACIÓN INSTITUCIONAL	PGTICS-002	1.0
3	ADMINISTRACIÓN DE CUENTAS Y ACTIVIDADES EN LA RED	PGTICS-003	1.0
4	GOBIERNO EN LÍNEA EN COLOMBIA	PGTICS-004	1.0
5	ADMINISTRACIÓN DE SEGURIDAD DIGITAL	PGTICS-005	1.0
6	TRATAMIENTO DE DATOS	PGTICS-006	1.0
7	DETERMINACIÓN DE NECESIDADES TECNOLÓGICAS Y REQUERIMIENTOS	PGTICS-007	1.0

De los procedimientos señalados, no se halla evidencia del cumplimiento de los puntos de control, por lo que se infiere que no se está efectuando ninguno de ellos, en los términos establecidos.

De igual manera, los procedimientos códigos PGTICS-004 y PGTICS-005, no cumplen a cabalidad con las características definidas por el Departamento Administrativo de la Función Pública en la GUÍA PARA LA GESTIÓN POR PROCESOS EN EL MARCO DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG), Versión 1, principalmente al no presentar un ordenamiento de las tareas necesarias para el cumplimiento de una operación, alno describir una secuencia, sino una serie de acciones independientes.

El procedimiento código PGTICS-006 carece de la característica de ser único y exclusivo, al documentar en el SOPORTE LEGAL y en la actividad No. 5 información pertinente a la Superintendencia de Industria y Comercio.

Sumado a lo anterior, se observa que el documento suministrado por el proceso auditado denominado PROCEDIMIENTOS GESTIÓN TIC, carece de código, versión y fecha, por lo que se considera que no ha sido incluido oficialmente en el Manual de Procesos y Procedimientos de la entidad.

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.

5.6 IPv6 (Internet Protocol Versión 6)

El Protocolo de Internet (IP) es un elemento de direccionamiento de Internet que permite por medio de conmutación de paquetes la interacción de toda clase de dispositivos y aplicaciones conectados a la red, el protocolo confiere a cualquier dispositivo conectado un número que representa su dirección en la red mundial de internet.

El agotamiento de las direcciones IPv4 conlleva a un estancamiento en el desarrollo de nuevos servicios, aplicaciones y tecnologías basadas en internet, dado que el número de dispositivos conectados a la red crece exponencialmente y no habría direcciones disponibles que soporten dicha demanda.

El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Resolución No. 2710 de 2017, estableció los lineamientos para la adopción del protocolo IPv6 señalando que para el proceso de transición se utilizarían como referencia los documentos denominados: *"Guía de transición de IPv4 a IPv6 para Colombia"* y *"Guía para el aseguramiento del Protocolo IPv6"*, expedidos por el ministerio.

Mediante la Resolución 1126 de 2021 se estableció que *"Las entidades estatales del orden nacional que trata el artículo segundo de la presente resolución, deberán culminar el proceso de transición al protocolo IPv6 en convivencia con el protocolo IPv4 a más tardar el 30 de junio de 2022. Por su parte,* ***las entidades territoriales deberán finalizar dicho proceso a más tardar el 31 de diciembre del año 2022****. En todo caso, dicha adopción deberá ser acorde al plan de diagnóstico formulado por cada entidad"*

Requeridas las evidencias del cumplimiento de lo establecido en las Resoluciones 2710 de 2017 y 1126 de 2021 se informa por parte del proceso auditado que la entidad no ha realizadoninguna acción encaminada a la adopción del protocolo IPv6.

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.

5.7 GOBIERNO EN LÍNEA – PÁGINA WEB

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 y se dictan otras disposiciones, tiene como objeto "… *regular el derecho de acceso a la información pública, los procedimientos para el ejercicioy garantía del derecho y las excepciones a la publicidad de información"*.

El ARTÍCULO 7 de la referida Ley 1712 de 2014 establece: "***Disponibilidad de la Información.*** *En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten*".

Se establece en la Ley 1712 de 2014 la información mínima obligatoria que se debe publicar, así:

- ***Información respecto a la estructura del sujeto obligado. (Artículo 9º)***

  a) La descripción de su estructura orgánica, funciones y deberes, la ubicación de sus sedes y áreas, divisiones o departamentos, y sus horas de atención al público;

b) Su presupuesto general, ejecución presupuestal histórica anual y planes de gasto público para cada año fiscal, de conformidad con el artículo 74 de la Ley 1474 de 2011;

c) Un directorio que incluya el cargo, direcciones de correo electrónico y teléfono del despacho de los empleados y funcionarios y las escalas salariales correspondientes a las categorías de todos los servidores que trabajan en el sujeto obligado, de conformidad con el formato de información de servidores públicos y contratistas;

d) Todas las normas generales y reglamentarias, políticas, lineamientos o manuales, las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos y los resultados de las auditorías al ejercicio presupuestal e indicadores de desempeño;

e) Su respectivo plan de compras anual, así como las contrataciones adjudicadas para la correspondiente vigencia en lo relacionado con funcionamiento e inversión, las obras públicas, los bienes adquiridos, arrendados y en caso de los servicios de estudios o investigaciones deberá señalarse el tema específico, de conformidad con el artículo 74 de la Ley 1474 de 2011. En el caso de las personas naturales con contratos de prestación de servicios, deberá publicarse el objeto del contrato, monto de los honorarios y direcciones de correo electrónico, de conformidad con el formato de información de servidores públicos y contratistas;

f) Los plazos de cumplimiento de los contratos;

g) Publicar el Plan Anticorrupción y de Atención al Ciudadano, de conformidad con el artículo 73 de la Ley 1474 de 2011.

- ***Publicidad de la contratación. (Artículo 10º)***

En el caso de la información de contratos indicada en el artículo 9 literal e), tratándose de contrataciones sometidas al régimen de contratación estatal, cada entidad publicará en el medio electrónico institucional sus contrataciones en curso y un vínculo al sistema electrónico para la contratación pública o el que haga sus veces, a través del cual podrá accederse directamente a la información correspondiente al respectivo proceso contractual, en aquellos que se encuentren sometidas a dicho sistema, sin excepción.

- ***Información respecto a servicios, procedimientos y funcionamiento del sujeto obligado*. *(Artículo 11º)***

a) Detalles pertinentes sobre todo servicio que brinde directamente al público, incluyendo normas, formularios y protocolos de atención;

b) Toda la información correspondiente a los trámites que se pueden agotar en la entidad, incluyendo la normativa relacionada, el proceso, los costos asociados y los distintos formatos o formularios requeridos;

c) Una descripción de los procedimientos que se siguen para tomar decisiones en las diferentes áreas;

d) El contenido de toda decisión y/o política que haya adoptado y afecte al público, junto con sus fundamentos y toda interpretación autorizada de ellas;

e) Todos los informes de gestión, evaluación y auditoría del sujeto obligado;

f) Todo mecanismo interno y externo de supervisión, notificación y vigilancia pertinente del sujeto obligado;

g) Sus procedimientos, lineamientos, políticas en materia de adquisiciones y compras, así como todos los datos de adjudicación y ejecución de contratos, incluidos concursos y licitaciones;

h) Todo mecanismo de presentación directa de solicitudes, quejas y reclamos a disposición del público en relación con acciones u omisiones del sujeto obligado, junto con un informe de todas las solicitudes, denuncias y los tiempos de respuesta del sujeto obligado;

i) Todo mecanismo o procedimiento por medio del cual el público pueda participar en la formulación de la política o el ejercicio de las facultades de ese sujeto obligado;

j) Un registro de publicaciones que contenga los documentos publicados de conformidad con la presente ley y automáticamente disponibles, así como un Registro de Activos de Información;

k) Los sujetos obligados deberán publicar datos abiertos, para lo cual deberán contemplar las excepciones establecidas en el título 3 de la presente ley. Adicionalmente, para las condiciones técnicas de su publicación, se deberán observar los requisitos que establezca el Gobierno Nacional a través del Ministerio de las Tecnologías de la Información y las Comunicaciones o quien haga sus veces.

Revisada la página web de la entidad https://distriseguridad.gov.co/, se evidencian las siguientes situaciones:

- Valores. no se halla la información actualizada.
- Directorio de Servidores Públicos, Empleados o Contratistas. No se encuentra el Listado de Contratistas.
- Directorio de Agremiaciones o Asociaciones en las que participe. No hay información.
- Calendario de Actividades y Eventos. No se tiene
- Entes y Autoridades que lo Vigilan. No hay información
- Contratación - Publicación de la ejecución de los contratos No hay información
- Manual de contratación, adquisición y/o compras. Manual de contratación desactualizado, se tiene el de 2015
- Formatos o modelos de contratos o pliegos tipo No se halla información al respecto.
- Planeación, Presupuesto e Informes

- Ejecución Presupuestal: No se evidencia ejecución presupuestal 2023.
- Proyectos de Inversión
- Informe sobre Defensa Pública y Prevención del Daño Antijurídico
- Plan Anual de Adquisiciones Se encuentra desactualizado
- Mecanismo de presentación de PQRSD No permite anexar documentación
- Estructura orgánica Desactualizada

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.

5.8 POLÍTICA DE GOBIERNO DIGITAL

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).

En este documento, en el ítem 2.1 se plantea: *¿Como planear la política en la entidad?*

2.1.1. Lineamientos de Planeación Estratégica

Entidades públicas de nivel territorial:

Con el fin de generar capacidades institucionales en la administración pública territorial y asumir la transformación digital a futuro, las entidades territoriales deberán vincularse a los proyectos estratégicos de transformación digital siguiendo los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC, e implementar el Modelo de Ciudades y Territorios Inteligentes para impulsar proyectos con enfoque de transformación digital para sus ciudades y territorios, a través de las herramientas e instrumentos que el Ministerio de las Tecnologías de la Información y las Comunicaciones defina para la formulación y cofinanciación de los mismos.

2.1.2. Articulación de la política

Con el objetivo de alinear la política de Gobierno Digital con la misión, las políticas de gestión y desempeño institucional y los procesos y servicios de la entidad; se deben desarrollar las siguientes actividades para determinar los proyectos estratégicos y el estado de implementación de los habilitadores de la política de Gobierno Digital:

- ✓ *Alinear Gobierno Digital con la planeación estratégica de la entidad*
- ✓ *Revisar el estado de implementación de las políticas de gestión y desempeño institucional:*
- ✓ *Priorizar Iniciativas:*

2.1.3. Planeación de los habilitadores de la política

El proceso de transformación digital de las entidades públicas se encuentra estrechamente ligado al fortalecimiento de la seguridad y la privacidad de la información, a la identificación, valoración y gestión de los riesgos de seguridad digital, al desarrollo de la arquitectura T.I. en articulación con la arquitectura institucional y a la prestación de servicios digitales basados en el Modelo de Servicios Ciudadanos Digitales. A partir de ello, es necesario que la entidad determine el estado de implementación de estos elementos y establezca un plan para iniciar o continuar con su desarrollo. Para ello, desarrolle las siguientes acciones:

- ✓ *Revisar el estado de implementación del Modelo de Seguridad y Privacidad de la Información -MSPI*
- ✓ *Revisar el estado de implementación del Marco de Referencia de Arquitectura Empresarial*
- ✓ *Revisar las condiciones de la entidad para la implementación de Servicios Ciudadanos Digitales (título 17, parte 2, libro 2 del DUR-TIC)*

El ítem 3.1 señala: ¿Cómo iniciar la ejecución de la política?

Una vez la entidad cuente con el PETI, el plan de seguridad y privacidad de la información y el plan de acción para la implementación de Servicios Ciudadanos Digitales, ésta debe desarrollarlos y aplicar los lineamientos que corresponden a los componentes TIC para el Estado y TIC para la Sociedad...

Se hace entrega, por parte del proceso auditado, del documento denominado POLÍTICA INSTITUCIONAL DE GOBIERNO DIGITAL, Código: PIDEYP - 001 Versión: 1.0 Fecha: 18/11/2021.

Analizada la información consignada en la política de seguridad digital de Distriseguridad, en concordancia con el documento MANUAL DE GOBIERNO DIGITAL y la Implementación de la Política de Gobierno Digital Decreto 1008 de 2018, se observa que:

- ✓ Respecto a la Planeación de los habilitadores de la política

  - No se halla evidencia de que se adelanten acciones encaminadas a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI.
  - No se adelantan acciones para la implementación del Marco de Referencia de Arquitectura Empresarial

- ✓ Respecto al inicio de la ejecución de la política

  - La entidad presenta un PETI que no ha sido desarrollado ni detallado de acuerdo con las guías y modelos propuestos por el MINTIC
  - No se cuenta con un plan de acción para la implementación de Servicios Ciudadanos Digitales.

En el mismo documento denominado POLÍTICA INSTITUCIONAL DE GOBIERNO DIGITAL, Código: PIDEYP - 001 Versión: 1.0 Fecha: 18/11/2021 se establecen una serie de acciones en el acápite correspondiente a estrategias a implementar, dentro de la política de gobierno digital de Distriseguridad, sobre las cuales se evidencia lo siguiente:

1. ***El Equipo de Gestión TIC, realizará el autodiagnóstico de la Política de Gobierno Digital, de acuerdo con la herramienta que el Ministerio de TIC o el Departamento de la Función Pública DAFP, establezca para ello****.*

   No se ha realizado, en la actual vigencia, el autodiagnóstico de la Política de Gobierno Digital

2. ***El Equipo de Gestión TIC, implementará la arquitectura TI y establecerá la estrategia de TI a través de la construcción del Plan Estratégico de Tecnologías de Información –PETI- y realizará seguimiento a su implementación*****.**

   No se documenta la implementación de la arquitectura TI. De igual forma, revisado el documento PETI publicado en la página web se evidenció que este no se desarrolla ni detalla de acuerdo con las guías y modelos propuestos por el MINTIC

3. ***El Equipo de Gestión TIC, mantendrá actualizado sus procedimientos y lineamientos en materia tecnológica*****.**

   Revisados los procedimientos del proceso Gestión TIC se evidencia que no todos cumplen con lo dispuesto 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,

4. ***El Equipo de Gestión TIC, definirá indicadores que permitan medir su operación***.

   En la caracterización del proceso se establecen tres indicadores.

5. ***El Equipo de Gestión TIC, construirá y mantendrá actualizados los catálogos de servicios de TI y de sistemas de información de la Entidad.***

   No se encuentran actualizados catálogos de servicios TI y de sistemas de información.

6. ***El Equipo de Gestión TIC, contará con un inventario de su infraestructura tecnológica.***

   No se encuentra actualizado el inventario de activos de información al no verse reflejados en una *Matriz de Inventario y Clasificación de Activos de Información*. (Guía para laGestión y Clasificación de Activos de Información – Ministerio de Tecnologías de la Información y las Comunicaciones. V5)

7. ***El Equipo de Gestión TIC, mantendrá actualizada la herramienta para atención de soportes tecnológicos (requerimientos e incidentes).***

   No existe en la entidad una herramienta para atención de soportes tecnológicos

8. ***El Equipo de Gestión TIC, elaborará una Metodología para el Desarrollo de Sistemas de Información y Buenas Prácticas*.**

   No se evidencia la presentación de esta metodología

9. ***El Equipo de Gestión TIC, establecerá acuerdos de niveles de servicio con los proveedores de tecnología, de acuerdo con el objeto del contrato.***

   No se tienen establecidos acuerdos de niveles de servicio con los proveedores de tecnología.

10. ***El Equipo de Gestión TIC, realizará un diagnóstico del uso y apropiación de las Tecnologías de Información en la Entidad, e implementará estrategias de gestión del cambio.***

    No se evidencia la realización de un diagnóstico del uso y apropiación de las Tecnologías de Información en la entidad.

11. ***El Equipo de Gestión TIC, socializará los proyectos que tenga en materia tecnológica.***

    No se evidencia la socialización de proyectos en materia tecnológica en la entidad.

12. ***El Equipo de Gestión TIC, realizará acciones para gestionar los documentos electrónicos de la Entidad.***

    No se observa que en la entidad se realicen acciones para gestionar los documentos electrónicos, ni se tienen definidos lineamientos.

13. ***El Equipo de Gestión TIC, realizará el diagnóstico de la implementación del Modelo de Seguridad y Privacidad de la Información MSPI con las herramientas que el Ministerio de TIC destine para ello.***

    Sólo durante la realización de la auditoría el equipo de auditor realizó un diagnóstico del MSPI, aplicando la herramienta diagnóstica dispuesta por el Ministerio de Tecnologías dela Información y las Comunicaciones.

14. ***El Equipo de Gestión TIC, mantendrá actualizada la Política de Seguridad y Privacidad de la Información.***

    Distriseguridad cuenta con un documento denominado Política de Seguridad Digital, no obstante, ninguno de los aspectos señalados como política y estrategias a implementar se desarrolla en la entidad.

15. ***El Equipo de Gestión TIC, identificará y mantendrá actualizados los activos de información de la Entidad.***

    La entidad no cuenta con un inventario integral de activos de información, desarrollado de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.

16. ***El Equipo de Gestión TIC, identificará, valorará y realizará un plan de tratamiento de riesgos de seguridad digital que afecten la plataforma tecnológica y la información de la Entidad****.*

    Verificado el contenido del PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN de la entidad**,** en lo referente a la gestión de riesgos, se evidencia que no se cumple con los parámetros y lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Guía de Gestión de Riesgos – Seguridad y Privacidad. Guía No. 7.

17. ***El Equipo de Gestión TIC, implementará controles para proteger la información que se produce y gestiona en la Entidad.***

    No se tiene implementado el MSPI, el cual establece los controles definidos en la ISO 27001.

18. El Equipo de Gestión TIC, establecerá el diagnóstico de transición de IPV4 a IPV6.

No se ha realizado ninguna gestión encaminada a realizar la transición de IPV4 a IPV6

19. El Equipo de Gestión TIC, habilitará en la página web de la Entidad canales de contacto para atender las Peticiones, Quejas, Reclamos, Solicitudes y Denuncias PQRSD.

Se evidencia la existencia de un canal en la página web de la entidad para atender PQRSD. No obstante, no permite recibir documentos anexos, a pesar de contar con esta opción.

20. Entidad Descentralizada Distriseguridad hará parte del Sistema Integral de PQRSD del Distrito.

Se desconoce la existencia del Sistema Integral de PQRSD del Distrito.

21. Entidad Descentralizada Distriseguridad contará con ventanilla única de recepción y envío de correspondencia.

Existe en la entidad una ventanilla única de recepción y envío de correspondencia.

22. El Equipo de Gestión TIC, acogerá herramientas tecnológicas que permitan tener usabilidad y accesibilidad a la información por parte de usuarios internos y externos.

No se cuenta con herramientas que permitan tener usabilidad y accesibilidad de la información.

23. El Equipo de Gestión TIC, generará herramientas a través del uso de las tecnologías, para evaluar la satisfacción del servicio a nivel interno y externo.

La entidad no cuenta con herramientas a través del uso de las tecnologías, para evaluar la satisfacción del servicio a nivel interno y externo.

24. En la Entidad Descentralizada Distriseguridad Distrital cumplirán los requisitos que se establezcan en la Ley de Transparencia y acceso a la información pública Ley1712 del 2014.

En el desarrollo de la auditoría se establece el grado de cumplimiento de la normatividad por parte del proceso Gestión TIC

25. El Equipo de Gestión TIC y el Equipo de Comunicaciones Estratégicas harán uso de las herramientas tecnológicas (redes sociales, página web) para dar a conocer la gestión de la Entidad, difundir convocatorias, conocer opiniones y/o sugerencias.

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

26. El Equipo de Gestión TIC, identificará la información producida, útil para ciudadanos y entidades, con características de datos abiertos, para ser publicada.

No se ha realizado identificación de la información producida por la entidad con características de datos abiertos, útil para los ciudadanos y demás entidades.

27. El Equipo de Gestión TIC, habilitará herramientas tecnológicas colaborativas con otras Entidades para realizar control de la gestión y/o control ciudadano.

La entidad se encuentra en un nivel muy básico de implementación de herramientas tecnológicas colaborativas.

Revisadas las evidencias que conllevan a determinar el cumplimiento de las estrategias a implementar para la adecuada implementación de la política digital de Distriseguridad, se puede determinar que, de las 27 estrategias definidas solamente se evidencia cumplimiento de3, es decir que solamente se tiene un 11% de cumplimiento, lo que nos lleva a concluir que a pesar de contar con un documento aprobado y estandarizado de política digital esta no ha sido gestionada.

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 puedeevidenciar la falta de cumplimiento y/o seguimiento de la política, debido que de 27 estrategiasdefinidas 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.

5.9 POLÍTICA DE SEGURIDAD DIGITAL

Se pone de presente, por parte del proceso auditado, el documento denominado POLÍTICA INSTITUCIONAL DE SEGURIDAD DIGITAL, Código: PIDEYP – 001, Versión: 1.0, Fecha: 18/11/2021.

De acuerdo con el documento el objetivo es *“Diseñar la Política de Seguridad Digital en la Entidad descentralizada Distriseguridad, en un marco de gestión de los riesgos de Seguridad Digital en el que la Entidad pueda estar expuesta desde la perspectiva de entorno cibernético y siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información”.*

En este documento, en el acápite denominado POLÍTICA, se establecen siete (7) aspectos que se desarrollarán y serán liderados por parte del Equipo de Gestión TIC, de la entidad, a saber:

- ✓ La Entidad descentralizada Distriseguridad establecerá la seguridad digital como una responsabilidad institucional y un compromiso de todo el personal, liderada por el Equipo de Gestión TIC.
- ✓ La Oficina Asesora de Planeación, el Equipo de Gestión Documental y El Equipo de Gestión TIC, revisará y actualizará los activos de información y en ello tendrá en cuenta la clasificación según su naturaleza, como, por ejemplo, información, software, hardware y/o componentes de red.
- ✓ El Equipo de Gestión TIC, hará el levantamiento de la Infraestructura Tecnológica Crítica de la Entidad.

- ✓ El Equipo de Gestión TIC, actualizará los riesgos de seguridad digital, siguiendo la metodología dispuesta por el DAFP y el Ministerio de TIC.
- ✓ El Equipo de Gestión TIC implementará el Modelo de Seguridad y Privacidad de la Información MSPI con las herramientas que el Ministerio de TIC destine para ello, el cual integra en cada una de sus fases asociadas a la gestión de riesgos de seguridad digital.
- ✓ El Equipo de Gestión TIC establecerá los controles definidos en el Anexo A de la ISO 27001:2013, que en el MSPI se define como la Declaración de Aplicabilidad.
- ✓ El Equipo de Gestión TIC evaluará el desempeño del Modelo de Seguridad y Privacidad de la Información MSPI, a través de la aplicación de la política de seguridad y privacidad de la información, la ejecución de los controles definidos en la declaración de aplicabilidad y el monitoreo de los indicadores de seguridad de la información.

En el ítem correspondiente a ESTRATEGIAS A IMPLEMENTAR se presentan las acciones para dar cumplimiento a esta política, estableciendo diez (10) aspectos que se desarrollarán y serán liderados por el por parte del Equipo de Gestión TIC, según el documento.

- ✓ La Entidad descentralizada Distriseguridad establecerá la seguridad digital como una responsabilidad institucional y un compromiso de todo el personal, liderada por el Equipo de Gestión TIC.
- ✓ La Oficina Asesora de Planeación, el Equipo de Gestión Documental y El Equipo de Gestión TIC, revisará y actualizará los activos de información y en ello tendrá en cuenta la clasificación según su naturaleza, como, por ejemplo, información, software, hardware y/o componentes de red.
- ✓ El Equipo de Gestión TIC, hará el levantamiento de la Infraestructura Tecnológica Crítica de la Entidad.
- ✓ El Equipo de Gestión TIC, actualizará los riesgos de seguridad digital, siguiendo la metodología dispuesta por el DAFP y el Ministerio de TIC.
- ✓ El Equipo de Gestión TIC implementará el Modelo de Seguridad y Privacidad de la Información MSPI con las herramientas que el Ministerio de TIC destine para ello, el cual integra en cada una de sus fases asociadas a la gestión de riesgos de seguridad digital.
- ✓ El Equipo de Gestión TIC establecerá los controles definidos en el Anexo A de la ISO 27001:2013, que en el MSPI se define como la Declaración de Aplicabilidad.
- ✓ El Equipo de Gestión TIC evaluará el desempeño del Modelo de Seguridad y Privacidad de la Información MSPI, a través de la aplicación de la política de seguridad y privacidad de la información, la ejecución de los controles definidos en la declaración de aplicabilidad y el monitoreo de los indicadores de seguridad de la información.
- ✓ El Equipo de Gestión TIC desarrollará el Procedimiento de Gestión de Incidentes de Seguridad de la Información y en él se establecerá como actividad el reporte de los incidentes a las autoridades como el CSIRT o COLCERT.
- ✓ El Equipo de Talento Humano, brindará capacitación técnica, tecnológica para atender riesgos de seguridad digital y fortalecerá la capacidad humana.
- ✓ El Equipo de Gestión TIC sensibilizará a usuarios internos en el uso de medios digitales y en buenas prácticas para mitigar los riesgos de seguridad digital que puedan afectar a la Entidad.

Es importante señalar que los siete (7) primeros puntos de las ESTRATEGIAS A IMPLEMENTAR son idénticos a los señalados como POLÍTICA.

Solicitadas las evidencias del cumplimiento de los puntos establecidos en la POLÍTICA y ESTRATEGIAS A IMPLEMENTAR, se establece que:

- ✓ No se encuentra actualizado el inventario de activos de información al no verse reflejados en una *Matriz de Inventario y Clasificación de Activos de Información*. (Guía para laGestión y Clasificación de Activos de Información – Ministerio de Tecnologías de la Información y las Comunicaciones. V5)
- ✓ No se evidencia el levantamiento de la Infraestructura Tecnológica Crítica de la Entidad. (Decreto 338 de 2022 - ARTÍCULO 2.2.21.1.4.1. *Infraestructuras críticas cibernéticas y servicios esenciales).*
- ✓ Se encuentran debilidades en la gestión de riesgos de seguridad digital. No se sigue la metodología dispuesta por el DAFP y el Ministerio de TIC.
- ✓ No existe evidencia de la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, el cual, de acuerdo con la Política de Seguridad Digital de Distriseguridad, integra en cada una de sus fases asociadas a la gestión de riesgos de seguridad digital. (Decreto 1078 de 2015)
- ✓ No se halla evidencia de que el Equipo de Gestión TIC haya establecido los controles definidos en el Anexo A de la ISO 27001:2013, que en el MSPI se define como laDeclaración de Aplicabilidad.
- ✓ No se evalúa el desempeño del Modelo de Seguridad y Privacidad de la Información MSPI, al no encontrarse implementado en la entidad.
- ✓ No se videncia que el equipo de Gestión TIC haya desarrollado el Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- ✓ No se evidencia que el equipo de Talento Humano haya brindado capacitación técnica y/o tecnológica para atender riesgos de seguridad digital.
- ✓ No se halla evidencia de que el equipo de Gestión TIC sensibilice a usuarios internos en el uso de medios digitales y en buenas prácticas para mitigar los riesgos de seguridad digital que puedan afectar a la Entidad.

Se hace evidente el planteamiento de una política y unas estrategias a implementar que no se cumplen, lo que deja a la entidad con un documento denominado Política de Seguridad Digital que no se desarrolla en ninguno de sus aspectos.

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.

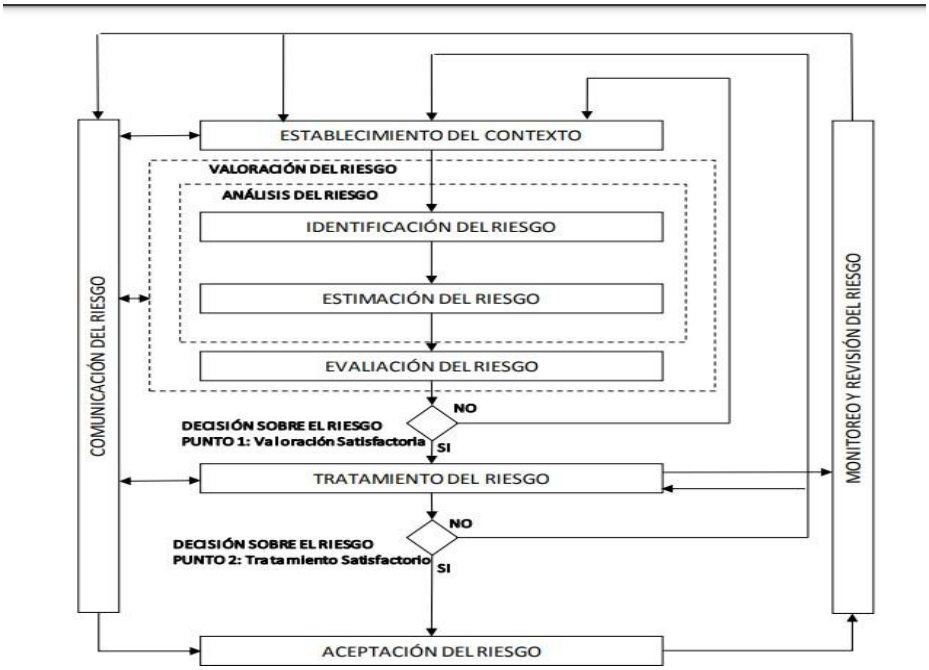
5.10 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Ministerio de Tecnologías de la Información y las Comunicaciones presenta la Guía de Gestión de Riesgos – Seguridad y Privacidad, Guía No. 7, la cual *"...busca orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP".*

Indica el documento que *"… dentro del Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (MSPI), un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones…"*

"Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación…"

La Guía de Gestión de Riesgos – Seguridad y Privacidad, presenta el proceso para la administración del riesgo en seguridad de la información, así:



Para la generación del análisis de riesgos se presenta una serie de etapas, basadas en la norma ISO27005:

- Identificación del Riesgo
- Identificación de los activos
- Identificación de las amenazas
- Identificación de Controle Existentes
- Identificación de las vulnerabilidades

Luego de elegir cuáles controles son los más adecuados para tener un nivel de riesgoaceptable para el o los procesos incluidos en el alcance del MSPI, 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 de acuerdo con las opciones entregadas en la guía, qué acciones se implementarán, quienes serán los responsables de esta implementación.

Este plan debe plantear claramente cada acción, etapa y procedimientos que se ejecutarán para poder ser monitoreado y lograr el seguimiento a la ejecución de este.

En desarrollo de la auditoría, el proceso Gestión TIC presenta el documento PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, Código: MGTICS – 002 Versión: 1.0 Fecha: 18/11/2021

El documento presenta los siguientes riesgos:

ID	ESCENARIO DE RIESGO	AMENAZA	VULNERABILIDAD
R1	Posibilidad de eventos que afecten la totalidad o parte de la infraestructura tecnológica interna o externa de la entidad	Tecnológico	Cronograma de Gestión TICS Diagnóstico de Seguridad Digital Actualización de Política de Seguridad Digital
R2	Posibilidad de inoperancia de la infraestructura tecnológica debido a escasez de recursos para la continuidad de la operación	Tecnológico	Diagnóstico TICS Presupuesto TICS Oficio a la Dirección General y Dirección Administrativa y Financiera

ID	ESCENARIO DE RIESGO	AMENAZA	VULNERABILIDAD
R3	Posibilidad de ineficacia en los controles de acceso.	Seguridad Digital	Cronograma de Gestión TICS Diagnostico de Seguridad Digital Actualización de Política de Seguridad Digital
R4	Posibilidad de inoperancia de la infraestructura tecnológica debido a escasez de recursos para la continuidad de la operación	Financiero	Diagnostico TICS Presupuesto TICS Oficio a la Dirección General y Dirección Administrativa y Financiera

Al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se le hace seguimiento, por parte de la Oficina de Control Interno, a través de la verificación del cumplimiento de las actividades señaladas como Plan de Acción, obteniendo el siguiente resultado:

PLAN DE ACCION DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DESDE EL ENFOQUE DE SEGURIDAD INFORMATICA SOBRE LOS ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN						
No	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE**	**TIEMPO**	**Seguimiento Primer Trimestre 2023**	**Seguimiento Segundo Trimestre 2023**	**Cumplimiento**
1	Diagnósticos de necesidades de TICS y solicitud de compra de bienes y soluciones TICS	TIC	feb-23		Pendiente diagnóstico de necesidades tic	0,5
2	Elaboración Cronograma proceso de TICS	TIC	feb-23			1
3	Adquisición de Controles de Seguridad informática frente a Ciber amenazas	PLANEACION	may-23	Se deben realizar acciones para la implementación de las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MINTIC.	Contratado con TIGO	1
4	Implementación de Controles de Seguridad Informática frente a Ciber amenazas	TIC	may-23	Se deben realizar acciones para la implementación de las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MINTIC.	Se deben realizar acciones para la implementación de las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MINTIC.	1

5	Actualizar la matriz de riesgo	TIC	ANUAL	Se deben realizar acciones para la implementación de las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MINTIC.	Se deben realizar acciones para la implementación de las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MINTIC.	0
				ACTIVIDADES REALIZADAS		**3,5**
				PORCENTAJE DE CUMPLIMIENTO DEL PLAN		**70%**

No obstante, haber alcanzado un porcentaje de cumplimiento del plan de 70%, es pertinente señalar que no se halla evidencia del cumplimiento de lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Guía de Gestión de Riesgos – Seguridad y Privacidad, Guía No. 7.

Además de lo anterior, se debe enfatizar en el hecho que la entidad no adelanta acción alguna encaminada a la adopción del Modelo de Seguridad y Privacidad de la Información, nopresenta una Matriz de Inventario y Clasificación de Activos de Información, no cuenta con un marco de arquitectura empresarial de TIC, ni presenta un levantamiento de la Infraestructura Tecnológica Crítica, elementos fundamentales para el desarrollo de los lineamientos establecidos por Ministerio de Tecnologías de la Información y las comunicaciones para una adecuada gestión de riesgos.

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 eldocumento con ese nombre, Código: MGTICS – 002 Versión: 1.0 Fecha: 18/11/2021, en élque se pudo evidenciar que no se cumple con los parámetros y lineamientos establecidos enla 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.

6 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 yPrivacidad, 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.

7 RESUMEN DE HALLAZGOS

Hallazgo No.	DESCRIPCIÓN
1	Deficiencias en la estructura de los riesgos.
2	Debilidades en la estructura del diseño de los controles al no contar con la totalidad de los criterios establecidos para ellos.
3	No se presentan evidencias y/o no son satisfactorias, sobre los controles realizados a los mapas de riesgos.
4	El PETI publicado en la página web de la entidad no se desarrolla ni detalla de acuerdo con las guías y modelos propuestos por el MINTIC.
5	El PETI carece de un componente que analice y alinee la estrategia, objetivos y/o metas institucionales con la estrategia de tecnología de la información. Además, la HOJA DE RUTA DE ARQUITECTURA EMPRESARIAL 2023, contiene actividades que no se encuentran descritas en la sección de los proyectos priorizados en el PETI.
6	El modelo de seguridad y privacidad de la información no se encuentra implementado en la entidad.
7	El Marco de Arquitectura Empresarial no se ha implementado en Distriseguridad.
8	Los procedimientos 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.
9	No se obtiene información ni evidencia del cumplimiento de los puntos de control establecidos en los procedimientos del proceso TIC.
10	No se ha realizado ninguna acción encaminada a la adopción del protocolo IPv6.
11	La página web de la entidad, aunque contiene los módulos para cargar la información, carece de ella y en algunos casos es incompleta y/o desactualizada.
12	Se evidencia falta de cumplimiento y/o seguimiento de la POLÍTICA INSTITUCIONAL DE GOBIERNO DIGITAL debido a que de 27 estrategias definidas solo se ha dado cumplimiento a 3 de ellas.
13	Los documentos POLÍTICA DE SEGURIDAD DIGITAL y POLÍTICA INSTITUCIONAL DE GOBIERNO DIGITAL presentan el mismo código, versión y fecha.
14	La POLÍTICA INSTITUCIONAL DE SEGURIDAD DIGITAL no cumple con los criterios de implementación de una política y unas estrategias.

15	El PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION no 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.

8 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.

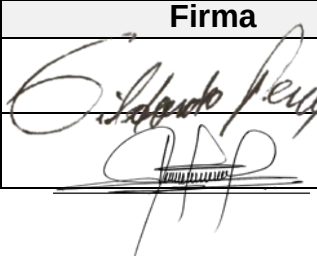
En la actualidad las oficinas de TIC desempeñan un rol estratégico en la modernización y la eficiencia de las operaciones de una entidad pública. En ese sentido, el Decreto 415 de 2016, a través del cual se definen lineamientos para el fortalecimiento institucional en materia de tecnologías de la información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

Para constancia se firma en Cartagena de Indias, a los días 20 días del mes de octubre de2023.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad**	**Firma**
GILDARDO PÉREZ TORRES	ASESOR DE CONTROL INTERNO	
FRANCISCO MURILLO ZABALA	APOYO CONTROL INTERNO	