I. INFORMACIÓN GENERAL

1. LIDER DE PROCESO: Jefe de Oficina de Tecnologías de la Información

1.1 OBJETIVO DEL PROCEDIMIENTO: Brindar los lineamientos requeridos para identificar las brechas en el cumplimiento de las políticas de gobierno digital y seguridad digital, haciendo uso de los criterios establecidos por el MinTIC, a fin de formular las actividades que conduzcan al cumplimiento de los lineamientos exigidos en éstas.

1.2 ALCANCE DEL PROCEDIMIENTO: Va desde la identificación de la declaración de aplicabilidad hasta la proposición de actividades para reducción de las desviaciones de los planes Estratégico de TI, de Seguridad y Privacidad de la Información y de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la siguiente vigencia.

1.3 RESPONSABLE DEL PROCEDIMIENTO: Jefe de Oficina de Tecnologías de la Información

1.4 CORRESPONSABLES DEL PROCEDIMIENTO: Coordinador Grupo Interno de Trabajo de Infraestructura y Sistemas de Información (GITISI) y Profesionales de la OTI.

2. GLOSARIO:

El siguiente glosario es, en su mayoría, tomado de los términos definidos o adoptados por el Ministerio de Tecnologías de las Información y las Comunicaciones de la República de Colombia, disponible en: https://www.mintic.gov.co/arquitecturaempresarial/630/w3-propertyvalue-385289.html

Análisis de brechas: Corresponde a la identificación, comparación y análisis de las diferencias entre un estado o situación actual y el estado o situación objetivo. Dentro del contexto de Arquitectura Empresarial permite poder planear las arquitecturas de transición necesarias para implementar y alcanzar la arquitectura empresarial objetivo.

Arquitectura de Tecnologías de la Información: Describe la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de los servicios de tecnología Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).

Artefacto: Un producto de trabajo arquitectónico que describe un aspecto de la arquitectura.

Capacidades de TI: Son un subconjunto de las capacidades institucionales operativas que tienen como propósito asegurar el adecuado aprovisionamiento del talento humano, los recursos y los procesos que se necesitan para ofrecer los servicios de TI definidos en su catálogo.

Componente de TI: Hace referencia a cualquier elemento de TI (software, hardware o componente de información) de una institución, lo mismo que a sus procesos, capacidades y servicios.

Ejercicios de Arquitectura Empresarial: Definen la situación objetivo de la entidad, son iterativos, tienen un alcance y unas necesidades claras que deben solucionar.

Gestión de proyectos: La aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del proyecto. La gestión de proyectos se refiere a guiar el trabajo del proyecto para obtener los resultados esperados. Los equipos de proyecto pueden lograr los resultados utilizando una amplia gama de enfoques (por ejemplo, predictivo, híbrido y adaptativo)

Gerente del proyecto: Persona asignada por la entidad para liderar el equipo del proyecto que es responsable de lograr los objetivos del proyecto. Los gerentes de proyecto realizan una variedad de funciones, como facilitar el trabajo del equipo del proyecto para lograr los resultados y administrar los procesos para entregar los resultados esperados.

Información: Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.

Interoperabilidad: Habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y

sistemas de información. (Gobierno de Australia). Habilidad de dos o más sistemas (computadoras, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar y de intercambiar datos de acuerdo con un método definido, con el fin de obtener los resultados esperados. (ISO). El ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades. (Marco de Interoperabilidad para el Gobierno en línea, Versión 2010). (Fuente: Glosario MinTIC)

Lineamiento: Es una orientación de carácter general. Corresponde a una disposición o directriz que debe ser implementada en las instituciones del Estado colombiano.

Mapa de ruta: Un mapa de ruta es un conjunto estructurado de acciones que define la manera de lograr los objetivos fijados en una estrategia. Un mapa de ruta está expresado en términos de programas o proyectos, que son agrupadores de las acciones, y tiene asociados estimaciones de tiempo, costos y riesgos.

Marco de Referencia de Arquitectura Empresarial - MRAE: Es un modelo de referencia puesto a disposición de las instituciones del Estado colombiano para ser utilizado como orientador estratégico de sus arquitecturas empresariales, tanto sectoriales como institucionales. El Marco establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza una ruta de implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información. El propósito final de este Marco es habilitar la política de Gobierno Digital del país.

Modelo de Arquitectura Empresarial - MAE: Es un instrumento para implementar el habilitador de Arquitectura de la Política Gobierno Digital del Estado Colombiano que establece el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Modelo Integrado de planeación y gestión - MIPG: Es un modelo que articula el quehacer institucional, mediante el establecimiento de cinco políticas de desarrollo administrativo, el monitoreo, evaluación de los avances en la gestión institucional y sectorial, el talento humano y los recursos administrativos, tecnológicos y financieros se convierten en el soporte para el cumplimiento de las metas institucionales y de gobierno.

Modelo de Gestión y Gobierno de TI - MGGTI: Es un modelo que orienta a las entidades públicas a generar las capacidades de gestión y gobierno de TI que les permitan responder a las necesidades que demandan los escenarios de economía digital.

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PETI: Plan Estratégico de Tecnologías de la Información y las Comunicaciones

Plan de comunicación de la Estrategia de TI: Toda estrategia debe ser comunicada de manera adecuada a los distintos interesados, dentro y fuera de una institución. El plan de comunicación define los tipos de usuarios a los que se informará, los tipos de contenido y medios de comunicación por usar, para divulgar la Estrategia de TI. Este plan es uno de los componentes de un PETI.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de TI: Es una directriz u orientación que tiene el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Las políticas son usadas para dirigir las decisiones, para asegurar la consistencia y el apropiado desarrollo e implementación de los procesos, estándares, roles, actividades y servicios de TI.

Principios: Son un conjunto de enunciados expresados en forma de reglas de alto nivel, que guían una institución, permitiéndole tomar decisiones sobre una base sólida. Reflejan los valores y convicciones de una entidad, y deben ser interpretados y usados como un conjunto. Los principios de TI definen la esencia estratégica de un PETI.

Proyecto: Es un conjunto estructurado de actividades relacionadas para cumplir con un objetivo definido, con unos recursos asignados, con un plazo y un presupuesto acordados.

Proyecto de TI: Es el proceso de planear, organizar y delimitar la responsabilidad de la realización de las metas específicas de TI de una organización. Incluye la supervisión de los proyectos de desarrollo de software, instalaciones de hardware, actualizaciones de red, despliegues de computación en nube y virtualización, proyectos de gestión de datos y análisis de negocios, y la implementación de servicios de TI.

PSPI: Plan de Seguridad y Privacidad de la Información

PTRSPI: Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Racionalizar: Organizar los trámites, procesos y procedimientos de tal manera que se reduzcan a su mínima expresión, con el menor esfuerzo y costo para el ciudadano, a través de estrategias efectivas de simplificación, estandarización, mejoramiento continuo, supresión y automatización de los mismos. (Fuente: Glosario MinTIC)

Requisito o requerimiento: Una declaración de necesidad que debe ser satisfecha por la arquitectura o un paquete de trabajo en particular.

Riesgo: Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Riesgo en un proyecto: Un riesgo es un evento o condición incierta que, si ocurre, puede tener un efecto positivo o negativo .

Rol: La función habitual o esperada de un actor, o el papel que alguien o algo desempeña en una acción o evento en particular. Un actor puede tener varios roles.

Roles: Conjunto de responsabilidades y actividades asignadas a una persona o grupo de personas para apoyar la adopción y aplicación del Marco de Referencia de Arquitectura Empresarial para la gestión de TI.

Seguridad de la información
Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital.

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Simplificar: Adoptar estrategias que implican: reducción de costos operativos en la entidad, reducción de costos para el usuario, reducción de documentos, reducción de pasos, reducción de pasos en el trámite interno, reducción de requisitos, reducción del tiempo de duración del trámite, reducción del tiempo en los puntos de atención, aumento en la vigencia del trámite, aumento de puntos de atención, fusión del trámite. (Fuente: Glosario MinTIC)

TAIP: Transparencia y Acceso a la Información Pública.

Tecnologías de la información - TI: Es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas. El término se utiliza como sinónimo para los computadores y las redes de computadoras, pero también abarca otras tecnologías de distribución de información, tales como la televisión y los teléfonos. Múltiples industrias están asociadas con las tecnologías de la información: hardware y software de computadoras, electrónica, semiconductores, internet, equipos de telecomunicación, el comercio electrónico y los servicios computacionales.

Valor: En un contexto organizacional, generar y entregar valor significa, en general, proveer un conjunto de servicios y productos para facilitarle a alguien el logro de un objetivo. TI genera y entrega valor a una institución mediante la implementación de los

servicios de TI. La entrega de valor es una medida abstracta, difícil de cuantificar directamente, pero que se puede calcular con el ahorro en esfuerzo o el aumento en la calidad del objetivo institucional que apoya.

Visión estratégica: Es la definición de alto nivel de los objetivos que se pretenden lograr y de la manera de hacerlo. Es uno de los componentes del PETI. En el caso de TI, la visión estratégica debe contemplar el impacto de las nuevas tecnologías, los cambios en las necesidades y expectativas de los ciudadanos, usuarios y actores de la entidad.

3. POLÍTICAS DE OPERACIÓN:

El análisis de cumplimiento de las políticas mediante artefactos de autodiagnóstico debe realizarse por lo menos una vez en cada semestre a fin de actualizar la línea base de cumplimiento.

El desarrollo completo del procedimiento debe realizarse por lo menos una vez al año, a fin de formular las actividades de los planes del Decreto 612 de 2018, asignados a la OTI, para la siguiente vigencia.

El procedimiento se ejecutará de manera adicional, por cambios en los lineamientos de alguna de las políticas analizadas o por solicitud generada por necesidad institucional o sectorial.

4. RELACIÓN CON OTROS PROCEDIMIENTOS Y PROCESOS:

Procesos que se requieren como proveedor	Qué insumos requiere del proveedor	Procedimiento	Que se obtiene del procedimiento	Para quien va dirigido el servicio o producto
Gestión de Tecnologías de Información y las Comunicaciones	Según las actividades registradas, Declaración de aplicabilidad publicada en los medios electrónicos de la SCRD.	Consolidación y Gestión de las Políticas de Gobierno Digital y Seguridad Digital	Planes publicados, Informe de seguimiento a los planes y Documento con actividades para reducción de desviaciones	Toda la entidad

II. ACTIVIDADES Y PUNTOS DE CONTROL

NO.	Actividad	Descripción	Responsable	Tiempo	Documento o Registro
1.	Identificar la declaración de aplicabilidad	El responsable de seguridad de la información identifica la última versión de la declaración de aplicabilidad publicada en los medios electrónicos de la SCRD	Responsable de Seguridad de la Información	1 día	No aplica
2.	Revisar la declaración de aplicabilidad de la SCRD	El responsable de seguridad de la información debe revisar la declaración de aplicabilidad a fin de identificar los controles aplicables a la SCRD. ¿Se requiere ajustar la declaración? Sí: Continuar con la actividad 3. No: Continuar con la actividad 4.	Responsable de Seguridad de la Información	1 día	Declaración de aplicabilidad revisada
3.	Ajustar la declaración de aplicabilidad	El responsable de seguridad de la información ajusta la declaración de aplicabilidad y presenta a la jefatura de la OTI para gestionar la aprobación y publicación.	Responsable de Seguridad de la Información.	2 días	Declaración de aplicabilidad actualizada
4.	Realizar autodiagnóstico MPSI	El Responsable de Seguridad de la Información de la OTI, junto con las dependencias responsables de controles, realiza levantamiento de información del cumplimiento de los lineamientos descritos en el Modelo de Privacidad y Seguridad de la Información.	Responsable de Seguridad de la Información Dependencias responsables de controles	30 días	Autodiagnóstico MSPI
5.	Presentar autodiagnóstico del MSPI	El responsable de seguridad de la información presenta resultado del autodiagnóstico del MSPI a la jefatura de la OTI	Responsable de Seguridad de la Información	1 día	Autodiagnóstico MSPI
6.	Identificar y verificar necesidades de formulación o actualización de planes.	El responsable de seguridad de la información verifica si se requiere formular o actualizar el Plan de Seguridad de la Información y/o el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de las Información por obligación del Decreto 612 de 2018, por cambio normativo o de lineamientos estatales o decisión estratégica institucional o sectorial. **Punto de control:** El ingeniero designado como responsable de seguridad de la información, debe verificar si existen cambios normativos, lineamientos a nivel estatal, distrital o institucional que impliquen la actualización de los Planes de Seguridad y Privacidad de la Información y de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. ¿Se requiere actualizar el PSPI y el PTRSPI? Sí: Continuar con la actividad 7. No: Continuar con la actividad 20.	Responsable de Seguridad de la Información	2 días	

7.	Identificar las brechas responsabilidad de la OTI	El responsable de seguridad de la información, conforme al autodiagnóstico del MPSI, identifica los controles que corresponden a la responsabilidad de la OTI y que no se cumplen en su totalidad y describe la brecha entre la situación actual y la esperada.	Responsable de Seguridad de la Información	3 días	**No aplica**
8.	Identificar brechas otras dependencias	El responsable de seguridad de la información, conforme al autodiagnóstico del MPSI, identifica los controles que corresponden a la responsabilidad de otras dependencias y que no se cumplen en su totalidad y remite la información, vía correo electrónico, a cada responsable a fin de que se identifiquen las brechas correspondientes.	Responsable de Seguridad de la Información Dependencias responsables de controles	3 días	Correos electrónicos a las dependencias responsables
9.	Presentar informe de brechas a jefatura de la OTI	El responsable de seguridad de la información presenta el autodiagnóstico del MPSI y el análisis de brechas a la jefatura de la OTI para su conocimiento	Responsable de Seguridad de la Información	1 día	Informe de brechas de seguridad de la información
10.	Proponer actividades para reducción de las brechas	El responsable de seguridad de la información propone a la jefatura de la OTI, las actividades necesarias para la reducción de brechas encontradas a partir del autodiagnóstico del MPSI, conforme a los controles que corresponden a la Oficina en el instrumento.	Responsable de Seguridad de la Información	2 días	Documento con actividades propuestas para reducción de brechas en tecnología
11.	Identificar recursos para la reducción de brechas	El jefe de la OTI lidera reunión para identificar los recursos que exigen las actividades propuestas para la reducción de brechas y si es viable atenderlas en el corto o mediano plazo con los recursos disponibles	Jefe de la OTI Responsable de Seguridad de la Información Persona de apoyo en la planificación y ejecución presupuestal de la OTI	3 días	Documento con actividades propuestas para reducción de brechas en tecnología con contraste de financiación
12.	Realizar reunión de reducción de brechas otras dependencias	El jefe de la OTI y el responsable de seguridad de la información, realizan reunión con las demás dependencias responsables de reportar cumplimiento de controles a través del MPSI a fin de establecer cuáles actividades se llevarán a cabo en la siguiente vigencia para reducir las brechas encontradas	Jefe de la OTI Responsable de Seguridad de la Información Dependencias responsables de controles	1 día	Acta de reunión
13.	Priorizar actividades para el PSPI y el PTRSPI	El responsable de seguridad de la información en conjunto con el jefe de la OTI, establecen las actividades que conforme al análisis de recursos fueron viabilizadas, serán realizadas en la siguiente vigencia	Jefe de la OTI Responsable de Seguridad de la Información	2 días	Documento con actividades priorizadas para reducción de brechas en tecnología
14.	Formular/actualizar el PSPI	El responsable de seguridad de la información, conforme a las actividades priorizadas realiza formulación o actualización, según corresponda, del Plan de Seguridad y Privacidad de la Información para ser presentado a la jefatura de la OTI	Responsable de Seguridad de la Información	5 días	PSPI proyectado

15.	Presentar el PSPI a la jefatura de la OTI para aprobación	El responsable de seguridad de la información presenta la proyección del Plan de Seguridad y Privacidad de la Información a la jefatura de la OTI para su aprobación. ¿El plan es aprobado? Si: Continuar con la actividad 17. No: Continuar con la actividad 16.	Jefe de la OTI Responsable de Seguridad de la Información	1 día	Correo electrónico o acta de reunión con definición de aprobación
16.	Ajustar el PSPI proyectado	El responsable de seguridad de la información realiza los ajustes definidos por la jefatura de la OTI al PSPI.	Responsable de Seguridad de la Información	2 días	PSPI ajustado
17.	Formular/actualizar el PTRSPI	El responsable de seguridad de la información, conforme a las actividades priorizadas realiza formulación o actualización, según corresponda, del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para ser presentado a la jefatura de la OTI	Responsable de Seguridad de la Información	5 días	PTRSPI proyectado
18.	Presentar el PTRSPI a la jefatura de la OTI para aprobación.	El responsable de seguridad de la información presenta la proyección del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información a la jefatura de la OTI para su aprobación. **Punto de control:** El responsable de seguridad de la información debe presentar la proyección del PTRSPI a la jefatura de la OTI para su aprobación o recomendaciones ¿El plan es aprobado? Sí: Continuar con la actividad 30. No: Continuar con la la actividad 19.	Jefe de la OTI Responsable de Seguridad de la Información	1 día	Correo electrónico o acta de reunión con definición de aprobación
19.	Ajustar el PTRSPI proyectado	El responsable de seguridad de la información realiza los ajustes definidos por la jefatura de la OTI al PTRSPI.	Responsable de Seguridad de la Información	2 días	PTRSPI ajustado
20.	Verificar si se requiere formular/actualizar PETI	El responsable de formulación y seguimiento al PETI verifica si se requiere formular o actualizar el Plan de Tecnologías de la Información por obligación del Decreto 612 de 2018, por cambio normativo o de lineamientos estatales o decisión estratégica institucional o sectorial. **Punto de Control:** El ingeniero designado como responsable de la reformulación y seguimiento del PETI, debe verificar si existen cambios normativos, lineamientos a nivel estatal, distrital o institucional que impliquen la actualización del Plan Estratégico de Tecnologías de la Información. ¿Se requiere actualizar el PETI? Sí: Continuar con la actividad 21. No: Continuar con la actividad 30.	Responsable de formulación y seguimiento al PETI	3 días	No aplica

21.	Realizar autodiagnóstico Gobierno Digital	El responsable de formulación y seguimiento al PETI, realiza autodiagnóstico del cumplimiento de los lineamientos descritos en la Política Gobierno Digital y analiza las brechas para cumplimiento de cada uno.	Responsable de formulación y seguimiento al PETI	15 días	Autodiagnóstico Gobierno Digital
22.	Identificar las brechas responsabilidad de la OTI	El responsable de formulación y seguimiento al PETI realiza un análisis de los lineamientos que no se cumplen totalmente e identifica las brechas de lo requerido frente a la situación actual.	Responsable de formulación y seguimiento al PETI	4 días	No aplica
23.	Presentar informe de brechas a la OTI	El responsable de formulación y seguimiento al PETI presenta el informe de los lineamientos que no se cumplen totalmente a la jefatura de la OTI para su conocimiento.	Responsable de formulación y seguimiento al PETI	1 día	Informe de brechas Gobierno Digital
24.	Proponer actividades para reducción de las brechas	El responsable de formulación y seguimiento al PETI propone a la jefatura de la OTI, las actividades necesarias para la reducción de brechas encontradas a partir del autodiagnóstico para cumplir con los lineamientos exigidos.	Responsable de formulación y seguimiento al PETI	2 días	Documento con actividades propuestas para reducción de brechas
25.	Identificar recursos para reducción de brechas	El jefe de la OTI lidera reunión para identificar los recursos que exigen las actividades propuestas para la reducción de brechas y si es viable atenderlas en el corto o mediano plazo con los recursos disponibles	Jefe de la OTI Responsable de formulación y seguimiento al PETI Apoyo en la planificación y ejecución presupuestal de la OTI	2 días	Documento con actividades propuestas para reducción de brechas en contraste con financiación
26.	Priorizar actividades para el PETI	El responsable de la formulación y seguimiento al PETI en conjunto con el jefe de la OTI, establecen las actividades que conforme al análisis de recursos fueron viabilizadas, serán realizadas en la siguiente vigencia.	Jefe de la OTI Responsable de formulación y seguimiento al PETI	2 días	Documento con actividades priorizadas para reducción de brechas
27.	Formular/actualizar el PETI	El responsable de la formulación y seguimiento al PETI, conforme a las actividades priorizadas realiza formulación o actualización, según corresponda, del Plan Estratégico de TI para ser presentado a la jefatura de la OTI	Responsable de formulación y seguimiento al PETI	10 días	PETI proyectado
28.	Presentar el PETI a la jefatura de la OTI para aprobación	El responsable de la formulación y seguimiento al PETI presenta la proyección del Plan Estratégico de TI a la jefatura de la OTI para su aprobación. ¿El plan es aprobado? Si: Continuar con la actividad 30. No: Continuar con la actividad 29.	Jefe de la OTI Responsable de formulación y seguimiento al PETI	2 días	Correo electrónico o acta con decisión de aprobación

29.	Ajustar el PETI	El responsable de la formulación / actualización del PETI, realiza los ajustes solicitados por la jefatura de la OTI al plan.	Responsable de formulación y seguimiento al PETI	3 días	PETI ajustado
30.	Presentar los planes al Comité Institucional de Gestión y Desempeño para aprobación	El jefe de la OTI realiza presentación de los planes de Seguridad y Privacidad de la Información, de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Estratégico de Tecnologías de la Información y las Comunicaciones, según corresponda, ante el Comité Institucional de Gestión y Desempeño para su aprobación. ¿Los planes presentados son aprobados? Sí: Continuar con la actividad 32. No: Continuar con la actividad 31.	Jefe de la OTI Comité Institucional de Gestión y Desempeño	1 día	Presentación de Planes
31.	Ajustar los planes según recomendaciones del Comité Institucional de Gestión y Desempeño	Los responsables de cada uno de los planes que requieren ajustes solicitados por el Comité Institucional de Gestión y Desempeño, realizan los cambios en los planes presentados y no aprobados, de conformidad con las recomendaciones.	Responsable de Seguridad de la Información Responsable de formulación/actualización PETI	3 días	Planes ajustados
32.	Realizar publicación de los planes en sección TAIP	El designado para publicaciones en la sesión Transparencia Acceso a la Información Pública realiza la publicación de los planes actualizados en la sede electrónica de la SCRD	Responsable de publicaciones de la OTI	1 día	Planes publicados
33.	Realizar seguimiento de los planes	El responsable de seguimiento de los planes realiza de manera trimestral el cumplimiento de las actividades, dispuestas en los planes.	Responsable de Seguimiento a lo planes	2 días	No aplica
34.	Presentar seguimiento a la OTI	El responsable de seguimiento de los planes presenta el seguimiento a la jefatura de la OTI para dar a conocer el resultado.	Responsable de Seguimiento a lo planes	3 días	Informe de seguimiento
35.	Elaborar y presentar informe de seguimiento	El responsable de seguimiento de los planes, elabora y presenta informe de seguimiento de los planes y mediante el aplicativo Orfeo.	Responsable de Seguimiento a lo planes	3 dìas	Radicado Orfeo
36.	Proponer actividades para reducción de las desviaciones	El Jefe de la OTI y el responsable de seguimiento de los planes proponen a la jefatura de la OTI, las actividades necesarias para la reducción de las desviaciones encontradas, para cumplir el desarrollo de los planes.	Jefe de la OTI Responsable de Seguimiento a lo planes	2 dìas	Documento con actividades para reducción de desviaciones

III. DOCUMENTOS ASOCIADOS Y ANEXOS

DOCUMENTOS ASOCIADOS:	
CÓDIGO	**NOMBRE**
	No aplica
ANEXOS (Si aplica)	
1	Diagrama de flujo del procedimiento
2	
3	

IV. CONTROL DE CAMBIOS Y APROBACIONES

CONTROL DE CAMBIOS		
Versión	**Fecha de Emisión**	**Cambios realizados**
1	06/12/2024	Versión inicial. Ver solicitud de creación, modificación o eliminación de documentos radicada en GLPI con el consecutivo número 108021 de fecha 31/10/2024 **Nota**: Con la creación de este documento se procede la eliminación del procedimiento GOT-PR-03 “Análisis seguimiento y evaluación de resultados del proceso”, teniendo en cuenta que las actividades que se encontraban en él, fueron incluidas en esta versión

FLUJO DE ELABORACIÓN, REVISIÓN Y APROBACIÓN			
Elaboró *Persona(s) responsable(s) de crear, proyectar la modificación y/o ajuste del documento*	**Aprobó** *Líder del Proceso quién debe hacer cumplir el contenido establecido en el documento*	**Validó** *Persona(s) de la OAP responsable(s) de verificar que el documento contenga los lineamientos establecidos*	**Avaló** *Jefe de la Oficina Asesora de Planeación*
NOMBRE: Jairo Enrique León León	NOMBRE: Javier Enrique Mariño Navarro	NOMBRE: Nelson Velandia	NOMBRE: Luis Fernando Mejía C.
CARGO:Contratista	CARGO: Jefe de Oficina OTI	CARGO: Profesional universitario	CARGO: Jefe Oficina Asesora de Planeación
FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente

Radicado: **20241600504603**
Fecha 05-12-2024 14:14

El Documento 20241600504603 fue firmado electrónicamente por:	
Vilma Rosa Villarraga Gongora	**Profesional Universitario 219 Grado 10**, Oficina Asesora de Planeación, ID: 51650932, vilma.villarraga@scrd.gov.co, Fecha de Firma: 06-12-2024 15:03:13
Luis Fernando Mejia Castro	**Jefe Oficina Asesora de Planeación**, Oficina Asesora de Planeación, ID: 79558456, luis.mejia@scrd.gov.co, Fecha de Firma: 06-12-2024 14:18:52
Nelson Javier Velandia Castro	**Profesional Universitario**, Oficina Asesora de Planeación, ID: 79905104, nelson.velandia@scrd.gov.co, Fecha de Firma: 06-12-2024 14:12:13
Javier Enrique Mariño Navarro	**Jefe Oficina de Tecnologías de la Información**, Oficina de Tecnologías de la Información, ID: 91474000, javier.marino@scrd.gov.co, Fecha de Firma: 06-12-2024 10:03:04
Jairo Enrique Leon Leon	**Contratista**, Oficina de Tecnologías de la Información, ID: 79952194, jairo.leon@scrd.gov.co, Fecha de Firma: 05-12-2024 14:39:09
Revisó:	Nidia Patricia Rodriguez Rodriguez - Profesional Especializado - Oficina de Tecnologías de la Información

8a300996bc62245170a8219debda8e437c78575679cc7f645134be2203d5c163
Codigo de Verificación CV: f6245