

Políticas de Seguridad y Privacidad de la información en Función Pública implementada	100	100	Al respecto, la OTIC desarrolló las actividades efectuadas durante la vigencia, sobre las cuales se pudo validar su cumplimiento: -Actualizar la documentación asociada a la política de seguridad de la información: la OTIC implementó la Política de Seguridad y Privacidad de la Información, con el propósito de garantizar la protección, confidencialidad, integridad y disponibilidad de la información institucional. El documento denominado "Política General de Seguridad de la Información", versión 2 de octubre 2020, tiene como objetivo "...garantizar la confidencialidad, integridad y la disponibilidad de la información de la cual el OAPF es responsable, y esto lo logra con el diseño de una Política General de Seguridad de la información, con el establecimiento de políticas internas, la implementación de controles a la infraestructura, a los activos de información que componen la seguridad perimetral y demás activos". Cabe anotar que el diseño de esta política va acorde con los estándares que permiten evaluar el cumplimiento de los más altos niveles de seguridad de la información, como lo son ISO 27002:2022, ISO 27032:2019, ISO 27701: 2019, ISO 37001:2019 y las leyes colombianas que exigen a la OAPF brindar seguridad a la información que se resguarda en referencia a los documentos del Modelo de Seguridad y Privacidad de datos personales que se describen en el marco normativo. -Realizar jornadas de sensibilización en seguridad de la información para Función Pública: se efectuaron jornadas de sensibilización durante la vigencia, asociadas a las políticas de Seguridad y Privacidad de la información en Función Pública, se realizaron Capacitaciones en : - Ciberseguridad donde se socializa los peligros del Fishing - Confidencialidad en los servicios de información personal al grupo de la GREC - IA Para todos las capacitaciones se evidencia las actas de asistencia, grabación de las sesiones y presentación efectuada.	Vlaksa/0000061/2025/DOCUMENTOS_APOYO/SEGURIDAD/COMPROMISOS/CAPACITACIONES Vlaksa/0000061/2025/DOCUMENTOS_APOYO/SEGURIDAD/REPORTES/SGI/Mezes
Seguimiento a la ejecución presupuestal del proyecto de inversión de "Tecnologías"	100	100	La OTIC durante la vigencia 2025 estableció y gestionó la siguiente actividad: - Realizar el seguimiento a la ejecución presupuestal del proyecto, con respecto a lo comprometido frente a lo apropiado en el proyecto de inversión "Mejoramiento de las tecnologías de la información y las comunicaciones a nivel institucional para dar cumplimiento a las políticas de Gobierno Digital y transformación Digital Bogotá" Para ello, se evidencian mes a mes los reportes de avance proyecto TIC, my completos y debidamente estructurados, los cuales tienen el propósito de informar sobre el estado de avance del proyecto a cada corte mensual de 2025 con el fin de facilitar la toma de decisiones informada proporcionando una visión clara y objetiva del estado actual del proyecto de inversión. Vale la pena resaltar que los documentos de seguimiento contienen la siguiente información: -Apropiación Vigente -Ejecución mes correspondiente 2025 -Problemas durante la ejecución del mes -Ejecución Presupuestal -Apropiación disponible -Resumen avance financiero para el mes de diciembre por objetivos del proyecto -Avance Meta por producto -Avance acuerdo de desempeño -Tablero de control mes correspondiente 2025 Como resultado de la gestión a diciembre de 2025, la OTIC en su seguimiento concluyó: "En cuanto al avance de las Compromisos, se registra una ejecución por un valor total de \$ 2.891.816.723,57 que corresponde a un 96.4% sobre la apropiación vigente y un 100% de ejecución de las obligaciones sobre los compromisos. Es importante destacar que la naturaleza contractual de los compromisos adquiridos por la Oficina de Tecnología implica modalidades de pago periódicas y progresivas. La mayoría de los contratos del área contemplan pagos mensuales escalonados, no desembolsos de suma global única. Esta estructura de pagos genera naturalmente un porcentaje de ejecución que mes a mes va aumentando. Sin embargo, la proyección de cumplimiento para cierre de vigencia 2025 era del 100% el cual efectivamente se cumplió."	Vlaksa.dfile.local/0000061/2025/DOCUMENTOS_APOYO/PLANEACION/INFORMES/SGI
Sistemas de información regionales de Función Pública actualizados e interoperando	100	100	Se evidencian también los correspondientes reportes efectuados por el responsable de FPP en la Plataforma Integrada de Inversión Pública - PIP del DNP- para cada mes de gestión, para cada proyecto de inversión, donde se gestionaron los requerimientos según solicitudes y/o planes de trabajo sobre los sistemas (SIGEP2, FURAD3, SLUT3) y el proceso de INTEROPERABILIDAD, el detalle se observa en el reporte del archivo adjunto como soporte. Este reporte permite evidenciar en resumen las acciones realizadas por la OTIC para los sistemas que se planearon actualizar y gestionar durante la vigencia 2025. Así mismo se hace reporte en el periodo que aplique de los temas de interoperabilidad. Los resultados según el último informe (Noviembre-diciembre) y validando previamente los debidos soportes fueron: SIGEP: Para el sistema SIGEP en el bimestre se continúa con el soporte a la versión 2.0 en los siguientes procesos: i) Requerimientos de consultas y ajustes de información. ii)Entregas de información del SIGEP i cada mes se entrega información a la Contraloría General, en cuanto a las hojas de vida, se registraron un total de 790.575 autenticaciones al sistema, de las cuales 485.586 resultaron en hojas de vida aprobadas y validadas correctamente. En relación con el módulo de bienes y rentas, se constataron 718.916 registros, de los cuales todos han sido confirmados. FURAD3: Para el presente periodo se realizaron sesiones para revisión de tareas para la próxima medición de desempeño, así como de seguimiento de avance en el desarrollo de los requerimientos enviados por la DGGI. Se realizó el borrado de usuarios en base de datos en ambiente preproductivo como parte del allanamiento para la próxima medición. Se elaboró acta de aceptación y entrega a la DGGI de los tableros de control en Power BI de MPM3 medición 2024. SLUT: Para el sistema SLUT en el periodo noviembre y diciembre de 2025 se continúa con el soporte a la versión 3.0. Incidentes y peticiones (requerimientos) gestionadas en la herramienta de la mesa de servicio proactiva por 52 casos. -Con relación a los requerimientos de consultas y ajustes de información, se resolvió el 83% de las solicitudes registradas en la herramienta proactiva. -Durante el periodo reportado, se presentaron modelos encubiertos, a la fecha el proceso se encuentra bajo monitoreo. -Monitoreo funcionamiento SLUT v3. -Se hace seguimiento al proceso de las mesas de trabajo con GOV.CO en el proceso de intercambio de información entre dicho portal y SLUT 3.0, se adelanta la revisión técnica de las actividades de comparación y ajuste de datos, en el marco del proceso de interoperabilidad con SLUT. INTEROPERABILIDAD: En la entidad se han venido trabajando los procesos de interoperabilidad con las entidades, donde se siguen los lineamientos del marco de interoperabilidad indicado por MIN TIC siguiendo los respectivos dominios del marco. SIGEP: i) CGR, se continúan los envíos de información periódicamente. Los planes de trabajo para el resto de los frentes se encuentran en organización y se están reajustando. Para más detalle ver el informe del grupo de interoperabilidad.	Vlaksa/0000071/2025/DOCUMENTOS_APOYO/REPORTES/SGI/INFORMES/SIGEP Vlaksa/0000071/2025/DOCUMENTOS_APOYO/REPORTES/SGI Vlaksa/0000071/2025/DOCUMENTOS_APOYO/INFORMES/INTEROPERABILIDAD Vlaksa/0001651/2025/DOCUMENTOS_APOYO/SIGEP/CONTRALORIA/10/OCTUBRE Vlaksa/0001651/2025/DOCUMENTOS_APOYO/INTEROPERABILIDAD/ASCC/COMPROBOS
Sistemas y servicios de apoyo actualizados	3	100	Dentro de la única actividad especificada "hacer seguimiento al funcionamiento de las herramientas tecnológicas utilizadas". Se gestionaron y atendieron requerimientos de soporte técnico o mejoramiento funcional según solicitudes y/o planes de trabajo sobre los Aplicativos de apoyo interno del Grupo de Servicios de Tecnológicos para KACTUS y PROACTIVANET dado que para NEON no se presentó ninguna solicitud funcional de mejora y ajuste al servicio. El detalle se observa en el reporte adjunto últimas páginas del archivo adjunto: Para la herramienta KACTUS- Nómina: para el tercer trimestre : -Se revisa la configuración de correo electrónico para el envío de los desprendibles de nómina del usuario Diana Vargas. -Se destilquea el módulo de ingresos y retenciones -a)Se revisa la configuración de Kactus en el PC del usuario Diana Vargas ya que los módulos no estaban cargando. Para la herramienta Mesa de Servicio PROACTIVANET que se encuentra en producción, se evidencian los debidos informes mensuales de seguimiento, y en específico para las tres herramientas mencionadas. El sistema de Nómina KACTUS, opero con normalidad y los casos presentados durante la vigencia han sido atendidos y resueltos. En relación con el sistema de inventarios NEON, se incluyó dicho sistema en la categoría de "Sistemas de Información Internos" de la mesa de servicio. Observación: La meta programada (3) no va en relación con la meta ejecutada (100)	Vlaksa/0002941/2025/DOCUMENTOS_APOYO/MEGA_SERVICIOS/INFORMES Vlaksa/0001651/2025/DOCUMENTOS_APOYO/VERIFICAS/SGI/VERIFICAS-APLICATIVOS Vlaksa/0000071/2025/DOCUMENTOS_APOYO/REPORTES/SGI/INFORMES/GP/ETI
ESTADO RIESGOS				
La OTIC con el apoyo de la OAP identifica siete (7) riesgos en la vigencia, relacionados en la matriz de riesgos del SGI, clasificados así: EJECUCION Y ADMINISTRACION DE PROCESOS - RIESGO 1: "Posibilidad de afectación reputacional por sanciones de entes de control, debido al incumplimiento de las obligaciones en materia de protección de datos personales " Controles: - El encargado de seguridad de la información valida la efectividad y vulnerabilidad de los controles existentes en el sistema, reportando las fallas encontradas, a través de pruebas o inspecciones técnicas de seguridad implementadas. - RIESGO 2: "Posibilidad de afectación reputacional por aumento de peticiones de servicio o imposibilidad para prestar el servicio en la capacidad comprometida debido a la gestión inadecuada de los servicios requeridos por la entidad (concentración de conocimiento, retraso en las entregas de proyectos de software, heterogeneidad en el desarrollo de software, falta de formalización de las metodologías de desarrollo de software)" Controles: - El coordinador y/o líder técnico verifica los requerimientos solicitados por líderes funcionales con el fin de identificar si es viable y definir los tiempos de entrega. Para ello se gestionaron todas las incidencias relacionadas durante los meses de enero y febrero; se recibieron y gestionaron los requerimientos recibidos por parte de los usuarios relacionados con los cursos virtuales, el Gestor Normativo y los procesos. - El Coordinador y/o líder técnico verifica el cumplimiento de requisitos mediante pruebas de funcionamiento para garantizar que el desarrollo correspondió a los requerimientos especificados. El reporte de este control en el SGI no es muy reciente respecto a su gestión, en el mismo no se especifica las pruebas de funcionamiento que determina, por ejemplo. - El coordinador y/o líder verifica el cumplimiento del cronograma y/o actas de reunión con el fin de hacer seguimiento al cumplimiento de compromisos y tiempos definidos en el cronograma. El reporte de este control en el SGI no es muy reciente respecto a su gestión, en el mismo no se especifica el seguimiento que debe hacer el coordinador al cumplimiento de compromisos y tiempos en el cronograma, así como sus debidos soportes. A su vez el registro es el mismo que en el control anterior. CORRUPCION - RIESGO 3: "Posibilidad de recibir o solicitar cualquier dádiva durante la construcción de la ficha técnica y la identificación de necesidades para la adquisición de bienes y servicios del proceso de tecnologías con el fin de beneficiarse a nombre propio o de terceros " Controles: - El profesional encargado de la Oficina de TIC valida los estudios de mercado sobre las fichas técnicas con el fin de establecer la viabilidad y presupuesto requerido para la contratación. Se evidencia el respectivo reporte mensual, donde se soporta la gestión a través de los reportes mensuales de contratación. - El responsable de la Oficina de TIC revisa los estudios previos para ser presentados al grupo de gestión contractual con el fin de analizar y ajustar la viabilidad de la contratación. Se evidencia el respectivo reporte mensual, donde se soporta la gestión a través de los reportes mensuales de contratación, en el ajuste de				

riesgos se encuentran las observaciones, las rutas y los nombres de los archivos relacionados con los procesos para este periodo					
SEGURIDAD DIGITAL					
RIESGO 4: "Posibilidad de afectación reputacional por divulgación no autorizada debido a pérdida de confidencialidad de la información reservada o clasificada almacenada en las bases de datos del aplicativo por la integridad pública ." (Periodicidad trimestral)					
Controles:					
- El profesional encargado de la Oficina de Tecnologías de la Información y las Comunicaciones, valida que la información remitida al grupo de valor atienda el protocolo para el intercambio de información segura.					
- El profesional encargado solicita a la OTIC la información requerida por el grupo de valor, con las características de seguridad de la información necesaria atendiendo el protocolo para el intercambio de información segura. Como soporte se tienen unos documentos en word que establece el protocolo que soporta el control o política frente al riesgo, algunos					
documentos apuntan a Políticas para tratamiento de datos personales.					
- El profesional encargado solicita a la OTIC la información requerida por el grupo de valor, con las características de seguridad de la información necesaria atendiendo el protocolo para el intercambio de información segura.					
- El profesional encargado valida que el requerimiento por parte del grupo de valor cumpla con el protocolo para el intercambio de información segura, con el fin de atender la solicitud de entrega de información.					
RIESGO 5: "Posibilidad de afectación reputacional por queja, demanda o sanción de los grupos de valor y/o entes de control debido a pérdida de confidencialidad en activos que contiene información con carácter personal administrados por la OTIC " (Periodicidad trimestral)					
Controles:					
- El jefe de la Oficina de TIC convoca el comité de emergencia, cuando se presente un incidente o evento potencial de seguridad de la información para gestionar de manera efectiva y oportuna los incidentes de seguridad.					
- El profesional designado para cada sistema de información institucional implementa y/o parametriza los componentes de seguridad con el fin de prevenir accesos no autorizados a nivel de sistema de información y base de datos.					
- El profesional encargado del manejo de los firewal de Función Pública verifica que el proveedor de los servicios de conectividad, configure las reglas de seguridad, con el fin de prevenir accesos no autorizados.					
RIESGO 6: "Posibilidad de afectación reputacional por quejas de grupos de valor y/o sanciones de entes de control debido a pérdida de integridad (modificación no autorizada) de la información o configuración de los servicios gestionados por la OTIC causados por posible ataque informático, falla eléctrica, errores de configuración, error humano en la aplicación de procedimientos, falta tecnológica, vulnerabilidades conocidos o desconocidos en el software y hardware "					
Controles					
- El coordinador del grupo de servicios de TI en conjunto con los líderes técnicos de los sistemas o servicios de información evalúan y ajustan las solicitudes de cambio para garantizar que estos cuando se implementen no afecten la integridad y disponibilidad de la información.					
- El jefe de la Oficina de TIC convoca el comité de crisis, cuando se presente un incidente o evento potencial de seguridad de la información para gestionar de manera efectiva y oportuna los incidentes de seguridad					
- El jefe de la Oficina de TIC convoca el comité de crisis, cuando se presente un incidente o evento potencial de seguridad de la información para gestionar de manera efectiva y oportuna los incidentes de seguridad					
- El profesional encargado del manejo de los certificados digitales asociados a los sistemas de información y portales, verifica oportunamente la vigencia e implementación de los mismos, con el fin de mantener la autenticidad, integridad y garantizar la confidencialidad de la información de las plataformas tecnológicas en I					
Las que están instalados los sistemas.					
RIESGO 7: "Posibilidad de afectación reputacional por quejas y sanciones de entes de control debido a pérdida de disponibilidad o incumplimiento de los ANS (acuerdos de niveles de servicio) de los servicios y sistemas de información administrados por la OTIC, causados por incidentes de seguridad fuera de control "					
Controles:					
- El líder técnico de cada sistema de información o plataforma tecnológica activa el plan de continuidad y recuperación con el fin de restablecer la prestación de los servicios afectados					
- El supervisor de los contratos de nube, verifica mensualmente el cumplimiento y disponibilidad de los ANS firmados con el proveedor, garantizando su prestación hacia los grupos de valor de manera continua.					
- El supervisor del contrato de conectividad verifica mensualmente el cumplimiento y disponibilidad de los ANS firmados con el proveedor, garantizando su prestación hacia los grupos de valor de manera continua.					
Este riesgo se materializó el 28 de marzo 2025, en el informe de gestión de riesgos del SGI no se registra dicha materialización (Fecha, Acontecimiento), tampoco se evidencia en la página de materialización la información relacionada con la causas generadora la descripción del evento, la fecha del evento, el producto afectado y tipo de pérdida.					
ESTADO INDICADORES					
Consultado el Sistema de Gestión Institucional - SGI, y el SPG, se observaron los siguientes indicadores para la vigencia 2025:					
1.Acceso al aplicativo por la integridad pública:					
Variable(s): "Viabilidad_uso_sistema_integridad_publica"					
Medición: Trimestral.					
- La ficha del indicador se observa publicada en el SGP (V8, feb 2025).					
En el SGI se registra la siguiente gestión: ingreso al aplicativo por la integridad pública:					
primer trimestre: 695.810 vs 611.000 usuarios de la vigencia 2024					
segundo trimestre: 432.989 vs 461.000 usuarios de la vigencia 2024					
tercer trimestre:590723 vs 458,000 usuarios					
cuarto trimestre: al menos 795286 vs 372,000 usuarios					
A nivel general, con relación a la vigencia 2024, se denota un incremento del 67% en la cantidad de usuarios que accedieron al aplicativo.					
2. Atención oportuna de incidencias y peticiones nivel especializado:					
Variable(s): "Atencion_nivel_especializado"					
Medición: Mensual.					
- La ficha del indicador se observa publicada en el SGP (V8, feb 2025).					
- En el SGI se registra la siguiente gestión: Se atendieron 85 peticiones, de las cuales solo dos (2) quedaron pendientes de atención.					
3.Disponibilidad de los servidores:					
Variable:"Horas_servicio_disponible"					
Medición: Trimestral					
- La ficha del indicador esta debidamente publicada en el SGP - V8 feb 2025					
- Según registros del SGI, se evidencia un registro en el reporte cualitativo y sus soportes no acorde con la naturaleza del indicador, se registro el nivel de acceso al Sistema de Rendición de Cuentas para la implementación de la Par - SIRCAP.					
ESTADO PLAN DE MEJORAMIENTO					
HALLAZGO	FECHA	ESTADO	DEPENDENCIA(S)	ORIGEN	ANALISIS DE CAUSA(S) Y ACTIVIDADES
521	19/05/2022	ABIERTO	Grupo de Gestión Contractual, Grupo de Gestión Documental, Grupo de Gestión Humana, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u> , Secretaría General	Mejora - Autoevaluación	SI, 4 actividades definidas con fecha de finalización 31/07/2024
570	4/06/2024	ABIERTO	Dirección de Empleo Público, Dirección de Gestión y Desempeño Institucional, Dirección de Participación Transparencia y Servicio al Ciudadano, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	SI, 7 actividades definidas con fecha de finalización 31/07/2025
591	22/11/2024	ABIERTO	Dirección de Desarrollo Organizacional, Dirección de Empleo Público, Oficina de Relación Estado Ciudadanas, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	NO SE HA EFECTUADO AUN
594	22/11/2024	ABIERTO	<u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	SI, 3 actividades definidas con fecha de finalización 30-05-2025
629	29/07/2025	ABIERTO	Dirección de Participación Transparencia y Servicio al Ciudadano, Dirección Gestión del Conocimiento, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Resultados FURAG	SI, 5 actividades definidas con fecha de finalización 15-Dic-2025
630	29/07/2025	ABIERTO	Dirección de Desarrollo Organizacional, Dirección de Empleo Público, Dirección de Gestión y Desempeño Institucional, Dirección de Participación Transparencia y Servicio al Ciudadano, Dirección Gestión del Conocimiento, Grupo de Apoyo a la Gestión Merritorífica, Oficina Asesora de Planeación, Oficina de Relación Estado Ciudadanas, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Resultados FURAG	SI, 11 actividades definidas con fecha de finalización 15-Dic-2025
640	18/11/2025	ABIERTO	Grupo de Gestión Documental, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	SI, 3 actividades definidas con fecha de finalización : 30/05/2026
641	18/11/2025	ABIERTO	Grupo de Gestión Documental, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	SI, 3 actividades definidas con fecha de finalización: 30/06/2026
642	18/11/2025	ABIERTO	Grupo de Gestión Documental, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	SI, 4 actividades definidas con fecha de finalización : 30/06/2026
650	18/11/2025	ABIERTO	Grupo de Gestión Documental, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	SI, 4 actividades definidas con fecha de finalización : 30/07/2027
294	13/12/2017	PARA CERRRE	Dirección de Participación Transparencia y Servicio al Ciudadano, Grupo de Servicio al Ciudadano Institucional, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	SI, 12 actividades definidas con fecha de finalización en las vigencias 2018 y 2019
515	8/03/2022	PARA CERRRE	Dirección de Desarrollo Organizacional, Dirección de Empleo Público, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Mejora - Autoevaluación	SI, 6 actividades definidas con fecha de finalización en la vigencia 2022
516	9/03/2022	PARA CERRRE	Dirección de Participación Transparencia y Servicio al Ciudadano, Oficina Asesora de Planeación, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Mejora - Autoevaluación	SI, 6 actividades definidas con fecha de finalización en la vigencia 2022
518	23/03/2022	PARA CERRRE	Dirección de Empleo Público, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Mejora - Autoevaluación	SI, 3 actividades definidas con fecha de finalización en la vigencia 2022
524	12/07/2022	PARA CERRRE	Dirección de Empleo Público, Oficina Asesora de Planeación, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Desempeño del proceso - SGI	SI, 7 actividades definidas con fecha de finalización en la vigencia 2022
589	17/10/2024	PARA CERRRE	Oficina Asesora de Comunicaciones, Oficina Asesora de Planeación, Oficina de Relación Estado Ciudadanas, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Seguimiento OCI	SI, 7 actividades definidas con fecha de finalización meses de diciembre 2024 y abril 2025
593	22/11/2024	PARA CERRRE	Dirección de Empleo Público, <u>Oficina de Tecnologías de la Información y las Comunicaciones</u>	Auditoría de Gestión	SI, 2 actividades definidas con fecha de finalización 30/06/2025

CONCLUSIONES Y RECOMENDACIONES
1. De acuerdo con los registros del Sistema de Planeación y Gestión Institucional, se observó el cumplimiento de los ocho (8) entregables propuestos para la vigencia 2025. No obstante se especifican algunos aspectos susceptibles de mejora para algunos de ellos, que se recomienda tener en cuenta para la gestión futura: a) Actualización del Sistema Integrado de Planeación y Gestión en lo correspondiente al proceso de Tecnologías de la Información: Se resalta el esfuerzo impreso en esta actividad y el apoyo de la OAP para su gestión. Sin embargo, se evidencian en el SIGP para el proceso algunos protocolos e instructivos que mantienen versiones de vigencias 2023 y 2024, los cuales deben ser revisados y posiblemente actualizados. b) Estrategia de Continuidad Institucional en Función Pública implementada: Se generó por parte de la OTIC un documento bien importante y debidamente estructurado como lo es la "ESTRATEGIA DE CONTINUIDAD INSTITUCIONAL EN LA FUNCIÓN PÚBLICA DE LAS APLICACIONES MISIONALES, SISTEMA SIGEPI, SISTEMA FURAG y SISTEMA SUIT" versión 1 junio 2025, no obstante no ha sido publicado en el SIGP como parte de su implementación. c) Sistemas y servicios de apoyo actualizados: La meta programada se definió con un valor cuantitativo de tres (3), mientras la meta ejecutada fue de cien (100), importante unificar el criterio de medición en la planeación institucional para los entregables como lo establece el procedimiento. 2. Se resalta la gestión efectuada en los entregables: Proyectos de inversión gestionados y consolidados y Seguimiento a la ejecución presupuestal del proyecto de inversión de "Tecnologías", por cuanto en los soportes de gestión se evidencian reportes periódicos con información financiera detallada y estructurada sobre el estado de avance periódico del proyecto de inversión. 4. La Oficina de Tecnologías de la Información y las Comunicaciones, definió tres (3) indicadores para la vigencia 2025 a los cuales se les realizó el respectivo seguimiento; sin embargo, se sugiere que la OTIC cuando efectúe el registro en el SGI incluya la información correspondientes al indicador y a su variable. Caso evidenciado para el indicador "Disponibilidad de los servidores", donde el registro en el reporte cuantitativo y sus soportes no está acorde con la naturaleza del indicador, se registró el nivel de acceso al Sistema de Rendición de Cuentas para la Implementación de la Paz - SIRCAP, pero no de evidencia el indicador de disponibilidad para todos los servidores. 5. Respecto al plan de mejoramiento, se evidenciaron para la vigencia 2025 y anteriores, diez (10) hallazgos (521, 570, 591, 594, 629, 630, 640, 641, 642 y 650) en estado "ABIERTO" y siete (7) en estado "PARA CIERRE" (294, 515, 516, 518, 524, 589 y 593) con vigencias de finalización desde 2018, 2019 y 2022. Por lo anterior, se recomienda efectuar la gestión oportuna para los hallazgos ABIERTOS en pro de aplicar un mejoramiento continuo y oportuno al interior de la entidad. De otro lado, para los hallazgos en estado PARA CIERRE gestionar prioritariamente su cierre con el apoyo de la OAP. Se acentúa que algunos de los hallazgos para cierre ya habían sido mencionados en el ejercicio de seguimiento efectuado por esta oficina para la vigencia 2024. 6. Se destaca la oportunidad y efectividad en el reporte de riesgos, controles asociados a los riesgos institucionales. Durante la vigencia 2025 la OTIC realizó a tiempo todos los reportes en el SGI, de manera clara y oportuna. No obstante, se evidencio en uno de los riesgos detallados en la sección correspondiente de este informe, un reporte no muy claro y orientado a la gestión del control especificado, por ello es importante que el reporte de gestión este acorde con la naturaleza del control y los soportes apoyen las acciones determinadas. De otro lado, no se evidencia la trazabilidad del riesgo materializado en marzo de la vigencia 2025, donde se registre el detalle del acontecimiento y que tratamiento fue dado para minimizar dicha materialización. La información contenida en la sábana de materialización de riesgos es básica y no registra el detalle informativo necesario de la causa, evento origen, fecha y producto o servicio afectado, entre otras. Por ello, es importante aportar toda la trazabilidad técnicooperativa y efectuar el tratamiento respectivo frente a los riesgos que se materialicen en la vigencia respectiva, gestionando a su vez un plan de mejoramiento sobre la(s) causa(s) que dio (deron) origen a la materialización.
Elaboró: Mauricio Corrajo Rodríguez Revisó: Aprilidis Jorge León de Castro B.