



1. Fecha: Enero 2021		2. Dependencia a evaluar: Oficina de Tecnologías de la Información y las Comunicaciones - OTIC	
3. Objetivos Institucionales relacionados con la dependencia: Consolidar una gestión pública moderna eficiente, transparente, focalizada, participativa y al servicio de los ciudadanos. Consolidar a Función Pública como un Departamento eficiente, técnico e innovador.			
4. PRODUCTO SGI	5. MEDICIÓN DE PRODUCTOS		
	5.1. Avance producto SGI (%)	5.2. Análisis de Resultados	
Política de Gobierno Digital ejecutada	100	<p>Este producto fue ejecutado mediante la gestión de 4 actividades, las cuales fueron gestionadas como se muestra a continuación:</p> <p>1. Diseñar el modelo de datos maestros de la entidad:</p> <p>Se evidencia el anexo técnico y el estudio previo para la implementación del Modelo de Datos Maestros – MDM, elaborados por la OTIC. No obstante, una vez expuesto el tema a la Subdirección y a la Oficina Asesora de Planeación - OAP de los productos esperados en la implementación del MDM, se estimó conveniente no contratar este producto por el proyecto de políticas de inversión, siendo así, la Oficina de TIC no realizó dicha contratación y la iniciativa se coordinó a través de un Contratista Asesor de la Dirección, bajo la supervisión de la OAP (se anexa link de la reunión virtual).</p> <p>Se realizó la explicación del alcance esperado en la implementación del MDM al contratista asignado al tema y se entregó la documentación respectiva.</p> <p>Se realizó el seguimiento a la implementación del proyecto MDM, con la participación de la OAP, Subdirección y OTIC (Soporte: 2020-09-29_Acta_proyecto_mdm).</p> <p>Ruta de soportes:</p> <p>\\yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\GOBIERNO_DIGITAL\ARQUITECTURA\PROYECTOS\MDM</p>	

Además, la OTIC orientó y explicó al equipo institucional sobre lineamientos de gobierno y gestión de datos, que permitan avanzar metodológicamente entorno a la administración de datos maestros (MDM). Se evidencia constancia de la citación de la reunión efectuada en el mes de noviembre, **sin embargo, no se adjunta evidencia del registro de la reunión, así como del contenido expuesto y/o temas tratados en la misma.**

Ruta de soportes:

\\yaksa\10031GSI\2020\DOCUMENTO_APOYO\GENERALES\TECNICO\EVIDENCIAS

2. Diseñar la propuesta de PMO en la entidad

En el segundo trimestre, la OTIC elaboró el estudio de mercado para la implementación de la Oficina de Proyectos - PMO. Se presentó a la subdirección y a la OAP los productos esperados en la implementación de la PMO. Al respecto, la subdirección estimó conveniente no contratar este producto por el proyecto de políticas de inversión, por tanto la OTIC no realizó dicha contratación y los productos fueron asumidos por la entidad en cabeza de la OAP. **Sobre este aspecto, en los archivos registrados en el SGI, no se evidencia(n) el(los) soporte(s) de la toma de esta decisión por parte de la Subdirección.**

Se evidencia el archivo implementación_pmo que corresponde a las actividades que a implementar lideradas por la OAP y los productos esperados.

Ruta de red:

\\yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\GOBIERNO_DIGITAL\ARQUITECTURA\PROYECTOS\PMO

En el tercer trimestre, Función Pública – FP tomó la decisión de implementar una PMO para la entidad. En reunión entre el equipo de la OAP y personal asesor de la alta dirección se definió el tipo de oficina de gestión de proyectos para el DAFP y se determinó el cronograma de acción para el resto de la vigencia, así como los productos esperados. Para esta gestión, se evidenció como soporte la presentación del proyecto, el cronograma, el documento guía para la implementación en FP, y el plan de Gestión del cambio (Ruta: <\\Yaksa\10020oap\2020\TRD\PROYECTOS\PMO>)

Para el último trimestre, bajo el cronograma de trabajo para la vigencia, y con el apoyo de la OTIC, se recomendó la construcción de (2) dos productos:

- Documento guía para la implementación de la PMO en FP, el cual fue finalizado y socializado con los miembros del equipo de la OAP para su respectiva retroalimentación.
- Plan de Gestión del Cambio, donde se concluyó la exploración de bibliografía y se implementó en producción el documento que contiene las fases para la gestión del cambio en el DAFP.

Los respectivos soportes de esta gestión se encuentran en la Ruta:

\\Yaksa\10020oap\2020\DOCUMENTOS_APOYO\PMO

3. Implementar la política de seguridad y privacidad de la información a cargo de la OTIC, según lo establecido en el Plan de Seguridad y Privacidad de la Información 2020

		<p>Durante la vigencia se efectuaron las siguientes tareas:</p> <ul style="list-style-type: none"> • Se efectuaron pruebas de ingeniería social, enfocadas a realizar ataques de seguridad dirigidos a Servidores, Contratistas y Pasantes de Función Pública. • Se adelantó el proceso pre-contractual para la contratación de la firma que debía realizar el diagnóstico, actualización y evaluación del modelo de Seguridad y Privacidad de la Información. • Se actualizó la Política de Seguridad y Privacidad de la Información de Función Pública, la cual se encuentra publicada en el Sistema Integrado de Planeación Gestión – SIPG <p>Los soportes de la gestión se evidencian en las rutas:</p> <p>\\yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\SEGURIDAD\INGENIERIA_SOCIAL</p> <p>\\yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\CONTRATOS_CONVENIOS\INVERSION\SEGURIDAD_PRIVACIDAD</p> <p>\\yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\SEGURIDAD\POLITICA</p> <p>Archivos:</p> <p>2020-07-02_Dafp_gms_gis_junio2020 2020-08-11_Dafp_gis_reporte_menusal_julio_2020 2020-08-12_Dafp_gis_reportemensual_julio_2020 2020-06-26_Analisis_del_sector 2020-06-26_Comparativo_economico_seguridad 2020-06-26_Estudio_previo_seguridad_digital_rev_idc 2020-07-15_Estudios_previos_seguridad_digital_revldc 2020-05-26_Propuesta_dafp_seguridad 2020-05-26_Propuesta_qvision_seguridad_privacidad_fp_v2 2020-03-30_Politica_seguridad_informacion_vp</p> <ul style="list-style-type: none"> • Se dio inicio a la ejecución del contrato para la Implementación de la Seguridad y Privacidad de la Información con la firma MNEMO (CONTRATO 234-2020). • Se consolidan y entregan los documentos base para iniciar con el análisis de seguridad de los componentes establecidos en la ficha. Así mismo, se cuentan con las actas de reunión a la fecha realizadas. <p>Los soportes de la gestión se evidencian en la ruta:</p> <p>\\Yaksa\10030otic\2020\DOCUMENTOS_APOYO\SEGURIDAD\CONTRATO_234_2020</p> <p>Archivos:</p> <p>2020-09-01_Acta_inicio_contrato_234_2020 2020-09-11_Checklist_entrega_informacion_mnemo 2020-09-11_Reunion_seguimiento_seguridad_informacion_cto_mnemo 2020-09-18_Reunion_seguimiento_seguridad_informacion_cto_mnemo 2020-09-25_Reunion_seguimiento_seguridad_informacion_cto_mnemo 2020-10-02_Reunion_seguimiento_seguridad_informacion_cto_mnemo</p> <ul style="list-style-type: none"> • Entrega por parte del contratista del Informe de evaluación y recomendaciones en materia de seguridad de la información, ciberseguridad y datos personales. <p>El soporte de la gestión se evidencian en la ruta:</p> <p>\\Yaksa\10030otic\2020\DOCUMENTOS_APOYO\SEGURIDAD\CONTRATO_234_2020\AVANCE</p>
--	--	---

Archivo:
2020-10-30_Informe_evaluacion_recomendacion_final

4. Socializar la política de Gobierno digital

A lo largo de la vigencia, se gestionaron las siguientes tareas:

- Socialización de la política de Gobierno Digital a la Subdirección y Oficina de Planeación, para el habilitador ámbito de Gobierno de TI y los ámbitos relacionados con el Plan Estratégico de TI – PETI, la Oficina de Proyectos – PMO y el Modelo de Datos Maestros MDM.

Archivos:

2019-06-05_Anexo_tecnico_gobierno_digital
2020-06-10_Diagnostico_final_gobierno_digital
2020-04-27_Revisar_estrategia_gobierno_digital_fp
2020-04-27_Presentacion_mdm
2020-04-27_Presentacion_pmo
2020-05-13_Master_data_services_fp
2020-05-29_Implementacion_pmo
2020-06-12_Presentacion_pmo
2020-06-12_Productos_implementation_2020_pmo
2020-06-25_Mdm_version_trabajo
2020-06-25_Registro_reunion_interna_gobierno_digital
2020-06-30_Reunion_datos_maestros_mdm
2020-07-17_Mdm_pmo, 2020-07-23_Reunion_proyecto_pmo

- Socialización al Jefe de TI del estado de la implementación de la Política de Gobierno Digital – componente de Arquitectura para las siguientes iniciativas:

1. Dominio de Gobierno de TI mediante la gestión integral de proyectos con la implementación de la PMO.
2. Dominio Gestión de Información mediante la Implementación del Modelo de Gestión de Datos Maestros – MDM.

Archivos: 2020-09-18_Acciones_a_implementar_gd_v3 y 2020-09-15_Gobierno_digital_v3

- Socialización de la política de Gobierno Digital.

Archivos: 2020-11-25_Gobierno_digital y 2020-11-25_Acta_socializacion_gobierno_digital

Los soportes de la gestión de las anteriores tres actividades se encuentran en la ruta de red:

<\\yaksa\10030OTIC\2020\DOCUMENTOS APOYO\GOBIERNO DIGITAL\SOCIALIZACION>

- Realización mesa de trabajo con la ESAP para la socialización del avance del PETI Sectorial, soportada en los archivos “2020-10-14_Documento_discusion_peti_sectorial” y “2020-10-08_Acta_peti_sectorial_esap_fp”, en la ruta de red: <\\yaksa\10030OTIC\2020\DOCUMENTOS APOYO\PETI\PETI-SECTORIAL>

<p>Proyecto de inversión coordinado y gestionado</p>	<p>4</p>	<p>Este producto fue ejecutado mediante la gestión de 4 actividades, las cuales fueron gestionadas como se muestra a continuación:</p> <p>1. Actualización de las metas de producto, actividades y costos asociados, en la cadena de valor del proyecto de inversión</p> <p>A través de los reportes mensuales de avance de la ejecución de los recursos en el SPI, la OTIC mantiene el registro de la actualización de las metas de producto, actividades y costos asociados.</p> <p>Ruta de red:</p> <p>\\Yaksa\10030otic\2020\DOCUMENTOS_APOYO\CONTRATOS_CONVENIOS\INVERSION\INFORMES</p> <p>Al 31 de diciembre se contó con la ejecución a nivel de compromisos del 97% y a nivel de obligación del 92%, logrando el cumplimiento de las metas propuestas.</p> <p>Ruta de red:</p> <p>\\Yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\CONTRATOS_CONVENIO\SINVERSION\INFORMES\DICIEMBRE\FINANCIERA</p> <p>Archivo:</p> <p>2020-12-31_Tablero_control_ejecucion</p> <p>2. Adelantar reuniones de seguimiento con los responsables de los entregables, asegurando la coherencia entre lo planeado y lo ejecutado – Trimestral</p> <p>Durante la vigencia, la OTIC asistió a las reuniones convocadas para el seguimiento del plan anual de adquisiciones y del proyecto de inversión, se realizaron además reuniones de seguimiento con el equipo de coordinación de TIC para revisar avances respecto a la ejecución del Proyecto de Inversión de TIC.</p> <p>Ruta de red:</p> <p>\\YAKSA\10030OTIC\2020\DOCUMENTOS_APOYO\SEGUIMIENTO_OTIC</p> <p>Archivos:</p> <p>2020-10-02_Avance_proyectos_tic 2020-09-18_Acta_seguimiento_semanal_coordinadores 2020-09-01_Avance_proyectos_tic_2 2020-09-25_Acta_seguimiento_semanal_coordinadores</p> <p>Finalmente, al finalizar la vigencia se revisó la ejecución al acuerdo de desempeño. Según se verificó, para el mes de noviembre, hubo una ejecución a nivel de compromisos del 90% frente al 88% planeado en el acuerdo de desempeño. Así mismo se evidencia una ejecución del 66% en obligaciones frente al 65% planeado en el mismo acuerdo</p> <p>Ruta de red:</p> <p>\\Yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\CONTRATOS_CONVENIO\SINVERSION\INFORMES\CONTRALORIA</p> <p>Archivo:</p> <p>2020-11-30_Ejecucion_cualitativa_presupuestal_noviembre</p>
--	----------	---

3. Asegurar el cumplimiento de la programación presupuestal establecida en el acuerdo de desempeño

A lo largo del año, se realizaron procesos precontractuales según lo planificado, con el fin de cumplir con el acuerdo de desempeño. Mensualmente, la OTIC generó el reporte de seguimiento, verificando el cumplimiento del acuerdo.

Para el mes de diciembre, hubo una ejecución del proyecto TIC a nivel de compromisos del 97% frente al 98% planeado en el acuerdo de desempeño. Así mismo, se evidenció una ejecución del 92% en obligaciones, al 31 de diciembre.

Los soportes se evidenciaron en las siguientes rutas:

\\Yaksa\Calidad_OS\Proyectos 2020\Gestion de la Inversión TIC\Informes

Archivos:

2020-01-31_Proyecto_tic_curva_s
2020-03-31_Proyecto_tic_curva_s
2020-04-30_Proyecto_tic_curva_s
2020-05-29_Proyecto_tic_curva_s

\\yaksa\10030otic\2020\DOCUMENTOS_APOYO\CONTRATOS_CONVENIOS\INVERSION

Archivos:

2020-03-12_Paa_2020_seguimiento
2020-07-06_Ejecucion_cualitativa_presupuestal_junio
2020-07-30_Acuerdo_desempeno_tics
2020-08-30_Ejecucion_cualitativa_presupuestal_agosto
2020-10-05_Ejecucion_cualitativa_presupuestal_septiembre
2020-11-04_Ejecucion_cualitativa_presupuestal_octubre
2020-11-30_Ejecucion_cualitativa_presupuestal_noviembre
2020-12-31_Ejecucion_cualitativa_presupuestal_diciembre

4. Reportar mensualmente los avances en la ejecución de recursos y entregables asociados a los productos de los proyectos de inversión

Durante el año se celebraron los siguientes contratos establecidos en el plan anual de adquisiciones:

- Soporte y mantenimiento Sigep I.
- Contratación del talento recurso humano de apoyo para gestión documental (Línea 214 PAA).

Se elaboraron los estudios previos a contratos de los siguientes procesos:

- Nómina
- Pruebas de Entidades (Línea 161PAA)
- CRM
- Soporte SIGEP II

Ruta:

\\yaksa\10030otic\2020\DOCUMENTOS_APOYO\CONTRATOS_CONVENIOS\INVERSION

Archivo:

2020-03-12_Paa_2020_seguimiento

		<p>Se realizaron entre otros, los siguientes pagos periódicos:</p> <ul style="list-style-type: none">• Direccionamiento Ipv 6• Planta temporal y contratistas de apoyo a la gestión de los sistemas de apoyo y misionales• Oficial de seguridad, el apoyo jurídico y financiero. <p>Ruta:</p> <p>\\Yaksa\Calidad_OS\Proyectos 2020\Gestion de la Inversión TIC\Informes</p> <p>Archivo:</p> <p>2020-03-31_Proyecto_tic_curva_s</p> <p>Se realizó mensualmente el seguimiento a la ejecución de recursos y entregables asociados a los proyectos de inversión.</p> <p>Ruta:</p> <p>\\Yaksa\Calidad_OS\Proyectos 2020\Gestion de la Inversión TIC\Informes</p> <p>Archivos:</p> <p>2020-04-30_Proyecto_tic_curva_s 2020-05-29_Proyecto_tic_curva_s 2020-07-30_Proyecto_tic_curva_s 2020-07-08_Proyecto_tic_curva_s 2020-08-30_Proyecto_tic_curva_s 2020-09-30_Proyecto_tic_curva_s 2020-10-30_Proyecto_tic_curva_s 2020-11-30_Proyecto_tic_curva_s 2020-12-31_Proyecto_tic_curva_s</p>
--	--	--

<p>Servicios ciudadanos digitales actualizados</p>	<p>3</p>	<p>Este producto fue ejecutado mediante la gestión de 7 actividades, las cuales fueron gestionadas como se muestra a continuación:</p> <p>1. Coordinar el diagnóstico para la incorporación de servicios ciudadanos digitales para SIGEP, gestor normativo, Eva y portal institucional</p> <p>Se efectuó la elaboración del documento de diagnóstico de implementación, el cual tuvo el propósito de “realizar el diagnóstico para la incorporación de los Servicios Ciudadanos Digitales en el Sistema de Gestión del Empleo Público SIGEP, Gestor Normativo, Espacio Virtual de Asesoría EVA y el Portal Institucional del Departamento Administrativo de la Función Pública”. Al respecto, se evidencia el debido soporte en el archivo “2020-05-29_Diagnostico” en la ruta de red: \\yaksa\10033GPETI\2020\DOCUMENTOS_APOYO\EVIDENCIAS_SGISERVICIOS_CIUDADANOS_DIGITALES</p> <p>2. Documentar e implementar controles de seguridad digital para el tratamiento de riesgos en sistemas de información digitales</p> <p>Como parte de la implementación de controles de seguridad en la celebración de contratos, se recomendó a la OTIC el uso de la cláusula de confidencialidad para contratistas, la cual reza así:</p> <p>“SEGURIDAD DE LA INFORMACIÓN: El contratista se obliga a cumplir las disposiciones normativas de la política de Tratamiento de datos personales, Manual de políticas de seguridad de la información de Función Pública y las políticas de seguridad digital adoptadas por la Entidad. Adicionalmente deberá guardar absoluta reserva sobre la información PÚBLICA RESERVADA, PÚBLICA CLASIFICADA, DATOS SENSIBLES, DATOS PRIVADOS, DATOS SEMIPRIVADOS, SECRETO EMPRESARIAL COMERCIAL, durante toda la vigencia del contrato y hasta 2 años después de la liquidación (si aplica) del mismo”, el soporte se evidencia en el archivo “2020-06-08_Correo_clausula_seguridad_proveedor_actualizacion_eva”.</p> <p>Por otro lado, en el mes de septiembre se verificaron los requerimientos para el cumplimiento del dominio político legal del marco de interoperabilidad, el soporte se evidencia en el archivo “2020-08-26_Orientaciones_cumplimiento_dominio_interoperabilidad”</p> <p>Durante el mes de noviembre se realizaron mesas de trabajo con la Contraloría General de la República, para formalizar el intercambio seguro de información en caso de investigaciones fiscales. Se evidencia presentación del procedimiento para transferencia segura de información, presentada por la OTIC (Archivo: 2020-11-30_Presentacion_flujo_trabajo_petition_contraloria”)</p> <p>Los soportes de la gestión de las anteriores actividades se encuentran en la ruta de red: \\Yaksa\10020oap\2020\DOCUMENTOS_APOYO\SEGURIDAD_INFORMACION</p> <p>3. Documentar y socializar lineamientos para la preservación de la seguridad y privacidad de la información gestionada por los sistema de información digitales</p> <p>Durante el mes de abril se adelantaron campañas de sensibilización en materia de seguridad de la información, para todos los servidores y contratistas de la Entidad, con el fin de prevenir ataques informáticos durante el confinamiento obligatorio a causa de la emergencia sanitaria por el COVID19. Se evidencia el respectivo informe de sensibilización, donde se describen las actividades en materia de sensibilización en seguridad de la información realizadas durante el</p>
--	----------	--

periodo 1 al 30 de abril (Soporte "2020-04-30_Informe_sensibilizacion_sgsi", ruta:

\\Yaksa\10020oap\2020\DOCUMENTOS APOYO\SEGURIDAD INFORMACIÓ N\ABRIL\9_sensibilizacion_seguridad)

Durante el mes de junio se completó la primera fase del plan de sensibilización en seguridad y se realizan las pruebas a los usuarios para evaluar socialización de los controles divulgados (Soporte: 2020-06-26_Informe_pruebas_vulnerabilidades_junio, ruta de red: \\Yaksa\10020oap\2020\DOCUMENTOS APOYO\SEGURIDAD INFORMACIÓ N\JUNIO\PRUEBAS_VULNERABILIDADES_13)

4. Identificar, analizar y formular planes de tratamiento de riesgos de seguridad digital para los sistemas de información digitales

Durante la vigencia 2020, se efectuaron las siguientes tareas:

- Identificación de riesgos asociados a los sistemas de información de la entidad, contenidos en el mapa de riesgos institucional publicado en el portal web de Función Pública, el seguimiento a sus controles y planes de acción se reportan a través del SGI módulo de riesgos.
- Como parte de la implementación de controles de seguridad en los contratos, se recomendó a la OTIC, el uso de la cláusula de confidencialidad para contratistas.
- Actualización del mapa de riesgos de todas las actividades del proceso de gestión de talento humano (Octubre). Se soporta en el archivo: 2020-10-26_Plantilla_riesgo_gth_rev6, ruta de red: \\Yaksa\10020oap\2020\DOCUMENTOS APOYO\SEGURIDAD INFORMACIÓ N\OCTUBRE\ACTUALIZAR RIESGOS SEGURIDAD_5
- Identificación de riesgos asociados a la Continuidad del Negocio, para los Sistemas de Información con que cuenta la Entidad, bajo la nueva metodología de Riesgos 2020, para el Proceso de Tecnologías de la Información y las Comunicaciones (Archivo: 2020-12-01_Matriz_riesgos_prd_gth, ruta de red: <\\yaksa\10021GMI\2020\TRD\PLANES\RIESGOS INSTITUCIONALES>

5. Incorporar gradualmente el concepto de ciudadano digital en el SUIT y FURAG a partir de las definiciones establecidas por MinTIC

- Se adelantaron las mesas de trabajo de Historias de Usuario en el proyecto de SUIT 4, con el objeto de incorporar los lineamientos de ciudadanos digitales en este proyecto. Se soportan en el correo-informe otorgado por la Gerente del Proyecto (Archivos: 2020-08-30_Correo_informe_avance_scd_suit4, 2020-08-30_Correo_informe_avance_scd_suit4_anexo, ruta: \\yaksa\10031GSI\2020\DOCUMENTO APOYO\SUIT_IVINFORMES).
- Los Proyectos de SUIT 4 y FURAG 3.0 se prorrogaron hasta la vigencia 2021, según justificaciones de la Agencia Nacional Digital - AND y aprobación de los supervisores. Dentro de este marco, se implementó el servicio de autenticación, de conformidad a la estrategia de realizarlo internamente en los sistemas (Soportes evidenciados en los archivos: 2020-11-30_Documento_arquitectura y 2020-12-23_Informe_supervision_gestion_210_2020_corte_noviembre_diciembre_original, rutas de red: <\\yaksa\10031GSI\2020\DOCUMENTO APOYO\FURAG III2 EJECUCION\DOCUMENTOS TECNICOS> y \\yaksa.dafp.local\10030OTIC\2020\DOCUMENTOS APOYO\CONTRATOS_C ONVENIOS\CONVENIOS\SUIT4 AND\8_CIERRE\INFORMES)

		<p>6. Proveer servicios de información para la estrategia de servicios ciudadanos digitales</p> <ul style="list-style-type: none"> • Se adelantaron las mesas técnicas con la AND, para conectar el servicio de autenticación de segundo nivel de SIGEP I, con los servicios de Ciudadanos Digitales de la AND. • Se efectuó el proceso de configuración de la conexión entre los dos servidores XROAD, terminando las pruebas de conexión del servicio de autenticación de segundo nivel con la AND a través del XROAD. <p>Los soportes de la gestión se evidenciaron en la ruta:</p> <p>\\Yaksa\10031GSI\2020\DOCUMENTO_APOYO\INTEROPERABILIDAD\TECNICO</p> <p>7. Sensibilizar a usuarios y responsables de sistemas de información digitales en lineamientos, controles y planes de tratamiento de riesgos de seguridad digital</p> <ul style="list-style-type: none"> • Actualización de la matriz de riesgos del proceso de Direccionamiento Estratégico mediante el formato de caracterización de procesos. • En lo referente al plan de seguridad y privacidad, se ejecutó la campaña de sensibilización en seguridad de la información. incluyendo piezas digitales de alertas, campaña de cambio de claves y socialización de eventos externos en materia de seguridad digital. • Sensibilización en seguridad de la información para el Comité Directivo institucional. <p>Rutas de red:</p> <p>\\Yaksa\10020oap\2020\DOCUMENTOS_APOYO\SEGURIDAD INFORMACION\MAYO\ELABORAR ACTUALIZAR DOCUMENTOS SGSI_1</p> <p>\\Yaksa\10020oap\2020\DOCUMENTOS_APOYO\SEGURIDAD INFORMACION\MAYO\SENSIBILIZACION_SEGURIDAD_9</p> <p>Archivos:</p> <p>2020-05-28_Caracterizacion_direccionamiento_estrategico 2020-05-30_Informe_sensibilizacion_sgsi 2020-08-30_Informe_sensibilizacion_sgsi_agosto 2020-11-30_Informe_sensibilizacion_sgsi_noviembre</p>
--	--	---

<p>Servicios tecnológicos y de información actualizados</p>	<p>7</p>	<p>Este producto fue ejecutado mediante la gestión de 4 actividades así:</p> <p>1. Estabilizar el sistema de información SIGEP II</p> <p>Durante la vigencia, se realizaron las actividades de estabilización según cronograma establecido, así como de preparación para la migración del segundo paquete de entidades, según la estrategia de la Dirección de Empleo Público (Prueba Beta 2).</p> <p>Ruta de red soportes:</p> <p>\\yaksa\10031GSI\2020\DOCUMENTO_APOYO\SIGEP\I\01_GESTION_PROY_CRONOGRAMAS</p> <p>Archivos: 2020-03-30_Cronograma_estabilizacion 2020-05-26_Seguimiento_estabilizacion_sigepii_v11_oap 2020-06-27_Estabilizacion_sigep_ii_v15</p> <p>2. Formular los requerimientos técnicos y adelantar el proceso pre-contractual</p> <p>Se generaron las fichas técnicas y estudios previos para los procesos planteados en el Plan Anual de Adquisiciones-PAA.</p> <p>Ruta de red soportes:</p> <p>\\Yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\CONTRATOS_CONVENIO_S\INVERSION</p> <p>2020-03-31_Proyecto_tic_curva_s 2020-05-30_Proyecto_tic_curva_s 2020-07-30_Avance_proyectos_tic</p> <p>En el mes de septiembre se generaron las fichas técnicas y estudios previos para la adquisición de equipos de cómputo para el Departamento Administrativo de la Función Pública, de conformidad con las especificaciones de la ficha técnica del Acuerdo Marco de Precios. Se evidencia el archivo “2020-09-03_Estudios_previos_computadores” como soporte.</p> <p>En el mes de noviembre se realizan entre otros los siguientes pagos:</p> <ul style="list-style-type: none"> • Adquisición de memorias RAM DDR3, DDR4 y disco de estado sólido para equipos de cómputo de escritorio y portátiles de Función Pública • Adquisición de la video una cámara y sus accesorios, para el uso en cubrimiento de eventos virtuales o televisivos, de reuniones, asesorías y capacitaciones ofrecidas por Función Pública • Personas de planta temporal del proyecto TIC, así como los contratistas que apoyan el mejoramiento y actualización de los sistemas de información de apoyo y misionales • Chat a Natura software y de los servicios de la solución de gestión humana Kactus a DIGITAL WARE. • Contrato firma MNEMO, para la implementación de controles de seguridad de la información en los sistemas de información y centro de datos de Función Pública <p>Los soportes se evidencian en la ruta de red:</p> <p>\\Yaksa\10030OTIC\2020\DOCUMENTOS_APOYO\CONTRATOS_CONVENIO_S\INVERSION\INFORMES</p>
---	----------	---

3. Implementar los requerimientos planteados por las Direcciones para los sistemas misionales de SUIT, FURAG y SIGEP

La OTIC desarrollo las siguientes actividades:

- Gestión de soporte y mantenimiento de los sistemas misionales de información, especificada en los informes periódicos de avance, los cuales permiten evidenciar las acciones realizadas por el grupo de servicios de información de la Oficina de Tecnologías de la información y las comunicaciones, dando alcance a la planeación institucional en cuanto la atención de los requerimientos funcionales y no funcionales de los sistemas misionales SUIT, SIGEP y FURAG. Se ubican en la ruta de red: <\\yaksa\10031GSI\2020\TRD\INFORMES\GENERAL>
- Implementación y liberación en producción de requerimientos del sprint 3 y 4 del sistema SUIT 3.0, el acta de aceptación se encuentra en proceso de aprobación. Se atienden los casos de soporte.
- Para el sistema SUIT 4.0, en el mes de noviembre se presentó un avance real del 67.1% sobre el planeado del 77.8% de línea base, con un desfase del -10.7%, con lo cual se aplicó el plan de choque para recuperar el desfase.
- Para el sistema FURAG 3.0, se realizaron las reuniones de seguimiento del Comité Técnico, se terminaron y aceptaron los entregables para los pagos respectivos.
- Para SIGEP I, fueron gestionados los casos de soporte que se cumplieron o solucionaron con la intervención del proveedor. También, se atendieron y respondieron los casos recibidos a través de Orfeo. Finalmente se cumplió con las tareas planeadas y descritas en el cronograma y se realizó el despliegue de la nueva versión del sistema el 28 de diciembre de 2020.

Se evidencia como soporte a esta gestión los informes periódicos del Grupo de Servicios de Información para el presente periodo, donde se indican las actividades realizadas sobre requerimientos y casos de soporte para los sistemas misionales SUIT, SIGEP y FURAG.

Ruta:

<\\yaksa\10031GSI\2020\TRD\INFORMES\GENERAL>

4. Realizar el acompañamiento técnico a la implementación del sistema de nómina de la entidad

Durante la vigencia, la OTIC acompañó en el proceso de los estudios previos para la prestación del servicio de soporte, mantenimiento preventivo, correctivo y evolutivo de la solución KACTUS-HCM, a través de la empresa DIGITAL WARE (Se evidencian los estudios previos definitivos en el archivo: 2020_04_03_Estudio_previo_digital_ware_2020_final, ruta de red: \\Yaksa\10033gpeti\2020\DOCUMENTOS_APOYO\SUPERVISION_CONTRATOS\NOMINA_KACTUS\CONTRATO)

Las actividades de acompañamiento efectuadas fueron:

- Entrega al Grupo de Gestión Humana de la información complementaria para la migración de la nómina SIGEP a la nueva nómina.
- Otorgamiento de la VPN (Virtual Private Network), para los empleados del proveedor DIGITAL WARE y para los nuevos servidores del GGH que van a administrar la nueva aplicación de nómina.
- Acompañamiento técnico a través del trámite con el proveedor HEINSOHN de la tabla de descuentos de nómina de los servidores.

		<p>Estas actividades se soportaron en los siguientes archivos:</p> <ul style="list-style-type: none">2020-05-07_Tablas_solicitadas_nomina_kactus2020-05-19_Solicitud_vpn_digital_ware2020-05-27_Usuarios_conexion_dafp2020-06-26_Prioridad_req_2020_033488_dimensionamiento_migrar_descuentos_Nomina <p>Ruta de red:</p> <p>\\Yaksa\10033gpeti\2020\DOCUMENTOS_APOYO\NOMINA</p>
--	--	--

<p>Sistemas de información interoperando</p>	<p>1</p>	<p>Este producto fue ejecutado mediante la gestión de 4 actividades así:</p> <p>1. Adecuar la interoperabilidad de un sistema de información:</p> <p>La OTIC realizó las pruebas de carga a los servicios de exposición de SIGEP II y de igual forma se prestó el acompañamiento a Colombia Compra Eficiente-CCE, para el consumo de nuestro servicio en ambiente de pruebas (Soportes “2020-04-30_Informe_pruebas_carga” y “2020-04-30_Informe_pruebas_cce”, en la ruta: \\yaksa\10031GSI\2020\DOCUMENTO APOYO\INTEROPERABILIDAD)</p> <p>Además, se llevaron a cabo las pruebas de interoperabilidad del servicio de autenticación de segundo nivel con la Agencia Nacional Digital (AND), con información tomada desde el SIGEP II. De igual forma se inició plan de trabajo para interoperar SIGEP II con el SIDEAP (Sistema de información Distrital del Empleo y la Administración Pública). Se evidencia el informe denominado “2020-08-30_Informe_grupo_interoperabilidad”, donde se encuentra el detalle de esta gestión (Ruta: \\yaksa\10031GSI\2020\DOCUMENTO APOYO\INTEROPERABILIDAD\TECNICO)</p> <p>Se resalta que el detalle de las actividades para este proceso, se relacionó en los informes periódicos generados durante la vigencia por el Grupo de Servicios de Información de la OTIC, en el ítem de interoperabilidad. (Ruta de red: \\yaksa\10031GSI\2020\TRD\INFORMES\GENERAL)</p> <p>2. Adoptar la guía de interoperabilidad definida por Mintic</p> <p>Función Pública adoptó la guía de interoperabilidad definida por MINTIC en el Sistema SIGEP II (Base datos de consulta), interoperando con la AND. Según el servicio de autenticación de segundo nivel. Donde se realizaron las siguientes actividades:</p> <ul style="list-style-type: none"> • Instalación y configuración de la plataforma de interoperabilidad X-ROAD versión Colombia, de conformidad con los parámetros establecidos por guía de interoperabilidad de MinTIC. • Disposición de los servicios Web en esta plataforma para consumo de la AND <p>Ruta: \\yaksa\10031GSI\2020\DOCUMENTO APOYO\INTEROPERABILIDAD\AND</p> <p>Archivos:</p> <p>2020-06-30_Evidencia_pruebas_consumo 2020-06-30_Nivel_garantias_evidencia_pruebas_postman_collection 2020-06-30_Gestion_instalacion_xroad</p> <p>3. Coordinar la definición del mapa de ruta de interoperabilidad</p> <p>La OTIC elaboró la presentación del marco de interoperabilidad y el catálogo de servicios. Se evidencian en los soportes: 2020-02-05_Intrucccion_marco_interoperabilidad y 2020-03-31_Catalogo_servicios en la ruta de red: \\yaksa\10031GSI\2020\DOCUMENTO APOYO\INTEROPERABILIDAD\DOCUMENTACION.</p> <p>4. Coordinar la ejecución mesas de trabajo técnicas interinstitucionales para la interoperabilidad</p> <p>A lo largo del año, se realizaron mesas de trabajo técnicas con las entidades con las cuales se tienen convenios de interoperabilidad. En los informes periódicos</p>
--	----------	---

		<p>generados durante la vigencia por el Grupo de Servicios de Información de la OTIC, se reportan las actividades con las entidades en el marco de las mesas de trabajo adelantadas, en las cuales se han desarrollado tareas técnicas para interoperar y/o intercambiar información, reflejando el estado actual del proceso, los temas logrados y los pendientes para próximas vigencias y las recomendaciones técnicas correspondientes.</p> <p>Ruta de red: \\yaksa\10031GSI\2020\TRD\INFORMES\GENERAL</p> <p>Archivos:</p> <p>2020-05-30_Informe_avance_gsi 2020-07-30_Informe_avance_gsi 2020-09-30_Informe_avance_gsi 2020-11-30_Informe_avance_gsi</p> <p>Ruta de red: \\yaksa\10031GSI\2020\DOCUMENTO_APOYO\INTEROPERABILIDAD\TECNICO</p> <p>Archivo:</p> <p>2020-09-30_Informe_grupo_interoperabilidad</p> <p>Ruta de red: \\yaksa\10031GSI\2020\DOCUMENTO_APOYO\INTEROPERABILIDAD\TECNICO\CRONOGRAMA</p> <p>Archivo:</p> <p>2020-12-10_Presentacion_convenios_interoperabilidad_dep</p>
--	--	---

6. Evaluación de la Oficina de Control Interno a los compromisos de la dependencia:

Indicadores: Revisado el Sistema de Gestión Institucional – SGI, la OTIC reporta los siguientes indicadores:

a) *Atención oportuna de incidencias y peticiones nivel especializado:*

Variable: Atencion_nivel_especializado

Este indicador está diseñado con una frecuencia de reporte mensual y una meta de cumplimiento del 100%.

Durante la vigencia se evidencian las mediciones mensuales de enero a diciembre que fueron efectuadas por la Dependencia, soportadas en los correspondientes informes de la mesa de servicio (Ruta: \\yaksa\10032GST\2020\TRD\INFORMES\SERVICIOS_ESPECIALIZADOS\MESA_SERVICIO). **No obstante, la meta de cumplimiento arrojó en promedio para la vigencia el 89% de cumplimiento, solo se pudo cumplir al 100% en los meses de mayo y agosto.**

b) Disponibilidad de los servidores

Variable: Horas_servicio_disponible

Este indicador está diseñado con una frecuencia de reporte mensual y una meta de cumplimiento del 100%. Durante la vigencia se evidencian las mediciones mensuales de enero a diciembre que fueron efectuadas por la Dependencia, soportadas en los correspondientes informes de disponibilidad de la nube y de los servidores (Ruta: [\\yaksa\OSI_POA\EVargas\2019\supervision\247-2019-Orden-Compra-44027](#)). **La meta fue cumplida durante toda la vigencia.**

Riesgos: El proceso de Tecnologías de la Información definió en el mapa de riesgos de la vigencia 2020, los siguientes bajo la responsabilidad de la OTIC:

Riesgo	Causa	Acción de control	fecha inicio	Fecha fin	Reporte avances SGI
Favorecimiento de un privado durante la identificación de necesidades en los procesos de selección de proveedores (Corrupción)	Falta de Información sobre el proceso a contratar.	El líder del proceso cada vez que se requiera atender solicitudes de contratación, formaliza en el comité de contratación, las fichas técnicas asociadas a las necesidades de contratación. En caso que el comité tenga alguna observación sobre la ficha, el líder realizará la sustentación. Se evidencia por medio de actas de comité y las fichas técnicas.	1-01	31-12	Durante la vigencia se generaron las respectivas fichas técnicas, estudios de mercado y estudios previos para los procesos de contratación que cursaron en su momento y son sustentadas en el Comité de Contratación cuando hay observaciones sobre las mismas. En la ruta registrada se observan los soportes respectivos.
	Interpretación técnica y subjetividad en términos.	El líder del proceso cada vez que se requiera atender solicitudes de contratación, formaliza en el comité, las fichas técnicas asociadas a las necesidades de contratación. En caso que el comité de contratación tenga alguna observación sobre la ficha, el líder realizará la sustentación. Se evidencia por medio de actas del comité de contratación y las fichas técnicas.			Durante la vigencia se generaron las respectivas fichas técnicas, estudios de mercado y estudios previos para los procesos de contratación que cursaron en su momento y son sustentadas en el Comité de Contratación cuando hay observaciones sobre las mismas. En la ruta registrada se observan los soportes respectivos.

	Uso excesivo del poder	El líder del proceso cada vez que se requiera atender solicitudes de contratación, formaliza en el comité, las fichas técnicas asociadas a las necesidades de contratación. En caso que el comité tenga alguna observación sobre la ficha, el líder realizará la sustentación. Se evidencia por medio de actas de comité y las fichas técnicas.			Se realizan estudios previos que son enviados y expuestos en el Comité de Contratación que incluyen las fichas técnicas respectivas. <u>Verificando la evidencia relacionada en el SGI, no se relacionan las actas del Comité de Contratación, tal y como lo establece la acción de control especificada.</u>
Pérdida de confidencialidad (Seguridad Digital)	Debilidades en la clasificación de los activos de información	Los responsables de los activos de información de la Oficina de Tecnologías de la Información y las Comunicaciones, semestralmente, con el propósito de mantener actualizada la calificación de la información y prevenir accesos no autorizados a la misma, realizan la revisión del índice de información. Cuando se identifique un nuevo activo se informará al grupo de Gestión Documental. Como evidencia se tienen el índice y correos electrónicos.	1-01	31-12	Durante la vigencia no se presentó la necesidad de actualizar el índice de información, se mantuvo publicado en la página web de Función Pública. (Ruta: https://www.funcionpublica.gov.co/gestion-documental#registro-de-activos-de-informacion).
	Debilidades en la gestión de roles y privilegios a servicios	El responsable del servicio de información donde la administración de los usuarios este a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones, cada vez que lo solicita el líder funcional, asigna los roles y privilegios, verificando que en Proactivanet se apliquen los Checklist con parámetros de seguridad establecidos. En caso de no cumplir con la aplicación de los parámetros se devuelve. Como evidencia se tienen los Proactiva Net.			En la aplicación de mesa de servicio ProactivaNET, se tiene parametrizado el control de ejecución de la solicitud o requerimiento de creación de usuarios de red; el Grupo de Gestión Humana lo hará para el caso de los usuarios de planta y el Grupo de Gestión Contractual para el caso de contratistas.
	Debilidades en las gestión de contraseñas	El líder del proceso y el responsable de seguridad de la información, semestralmente, con el fin de asegurar el manejo adecuado de las políticas de control de acceso, realizan campañas de sensibilización. De no cumplirse con las políticas se presenta el caso en el Comité de Gestión y Desempeño Institucional. Como evidencia se tienen las campañas, correos electrónicos o actas de comité.			Desde el mes de febrero se dio inicio a la campaña de sensibilización en seguridad de la información, la cual fue constante durante toda la vigencia. Se evidencian los informes mensuales denominados "Labores ejecutadas en materia de sensibilización de seguridad de la información", donde se describen las actividades en materia de sensibilización en seguridad de la información realizadas durante cada periodo A nivel general, se enviaron mensajes de alerta sobre suplantación de correos, se socializó la guía de web locales, se realizó capacitación en Arquitectura Empresarial, se

					adelantaron recomendaciones sobre el adecuado manejo de la seguridad de la información a nivel de confidencialidad, se publicaron recomendaciones, alertas y mensajes para prevenir ataques informáticos, entre otros.
Pérdida de la disponibilidad de los activos (Seguridad Digital)	Entorno inseguro digital	El profesional de apoyo en seguridad de la información periódicamente, con el fin de verificar reportes y alertas de seguridad e identificar amenazas potenciales, realiza diagnósticos internos y externos de las plataformas o verifica reportes de entes externos. Cuando se identifican amenazas el profesional de apoyo en seguridad de la información junto con el líder del proceso identifican acciones a realizar y se establece la viabilidad de su aplicación, sujeta a las restricciones presupuestales y de contratación. Como evidencia se tienen los reportes de comunicaciones por mensajes instantáneos o correos electrónicos de proveedores o reportes de grupos de interés o registro de pruebas de vulnerabilidades realizadas.	1-01	31-12	<p>Durante la vigencia:</p> <ul style="list-style-type: none"> - Se verificaron las alertas sobre suplantación de correo institucional reportadas por COLCERT (Grupo de respuesta a emergencias cibernéticas de Colombia) y CAI Virtual. - Se identificaron y reportaron las amenazas por el Oficial de Seguridad, relacionadas con la seguridad de la información. - Se monitorizaron eventos y ataques informáticos reportados por el Centro de respuesta a incidentes del Mindefensa y Policía Nacional. - Se atendieron potenciales incidentes de robo de datos personales mediante Phishing. - Se identificaron intentos de robo de datos personales mediante correos suplantando a entidades bancarias, alertando a los usuarios con infografías preventivas. - Se ejecutaron pruebas de análisis de vulnerabilidades en las plataformas institucionales en coordinación con la OTIC.
	Incumplimiento en los acuerdos de nivel de servicio en el soporte por parte de los proveedores.	El supervisor del contrato cada vez que se presente una indisponibilidad del servicio con el fin de llevar un control de cada caso, registra en ProactivaNet la indisponibilidad, la causa y su solución. En caso de presentarse incumplimiento se validarán las cláusulas del contrato. Como evidencia se tienen los informes mensuales de seguimiento y el registro en ProactivaNet.			<p>Las indisponibilidades y ventanas de mantenimiento programadas durante la vigencia están registradas en la Herramienta Mesa de Servicio "ProactivaNet". A nivel general, no se presentaron indisponibilidades por parte de los proveedores de infraestructura durante el año.</p> <p>Se evidencian los reportes de indisponibilidades y ventanas de mantenimiento generados mensualmente por ProactivaNet.</p>

	Obsolescencia tecnológica	El responsable del activo de información, cada vez que el fabricante libere versiones de software base para corregir vulnerabilidades, debe realizar el análisis de su impacto y si es viable aplicarlas. Los coordinadores realizan seguimiento a la estrategia. Como evidencia se tiene el registro en ProactivaNet de la respectiva actualización.			Se evidencian los reportes mensuales de actualizaciones del software base de servidores de impresión y de correo electrónico, así como del controlador de dominio. En la actualidad, se usa WSUS (Windows Server Update Services), el cual controla centralizadamente las actualizaciones de seguridad críticas para equipos y servidores. <u>No se evidencia el soporte de los análisis de impacto de las versiones de software liberadas, tal y como lo especifica la acción de control.</u> <u>No se evidencia reporte de los meses de octubre y noviembre.</u>
	Pérdida de servicios esenciales.	El responsable del activo de información semestralmente, con el fin de detectar variaciones en el comportamiento de la plataforma tecnológica y en los servicios de información, realiza la verificación de la información de registro de eventos generados por los diferentes sistemas y/o dispositivos. En caso de observar eventos, se debe convocar una reunión de control de cambios para evaluar y tomar decisiones. Como evidencia se tienen las actas de reunión de control de cambios o registro en ProactivaNet o correos electrónicos.			Durante la vigencia se presentaron algunas indisponibilidades, como el movimiento de datacenter, la entrada en operación de los servicios de nube privada en IFX y la realización de algunas actualizaciones de software base y plataforma Windows. <u>El avance registrado no refleja la gestión especificada en la acción de control, no pudiéndose evidenciar la verificación del registro de eventos de los sistemas y/o dispositivos, así como las actas de reunión de control de cambios o los casos registrados en Proactivanet.</u>
	Restricciones presupuestales para contar con infraestructura de alta disponibilidad.	El líder del proceso mensualmente realiza seguimiento al Plan de Adquisiciones de la oficina de TIC. Cuando sesione el Comité Institucional de Gestión y Desempeño reporta el avance. Como evidencia se tienen correos electrónicos y los informes de supervisión.			Se realizan reuniones mensuales con la Secretaría General, la Oficina Asesora de Planeación y/o la Subdirección para el seguimiento y ajuste al Plan de adquisiciones (PAA) de la oficina TIC.
Pérdida de la integridad	Ataques informáticos	El profesional a cargo de la plataforma tecnológica junto con los líderes técnicos de los servicios de información, periódicamente deben ejecutar un plan de pruebas de restauración de backups, con el fin de asegurar que el control está siendo efectivo. Cuando la	1-01	31-12	Se realizó entre otra la siguiente gestión durante la vigencia: -Se generó el cronograma de respaldo y recuperación de base de datos y aplicación de SIGEP I, SIGEP II, SUIT III y Portales por migración de datacenter externo.

	Error humano	plataforma tecnológica o servicios de información fallen, se debe recurrir a los planes de contingencia. Como evidencia se tienen los resultados de las pruebas de restauración de backups.			<ul style="list-style-type: none"> - Estableciendo la información y los servicios a migrar. - Se solicitó y realizó la restauración del backup de FURAG II, Se realizaron copas de seguridad del servidor de archivos Yaksa. -Para el proceso de migración a la nueva infraestructura de Hiperconvergencia, se realizó la restauración de Backups satisfactoriamente, dando como resultado que los servicios migrados se encuentran operando correctamente. -Se realizaron pruebas de restauración de backups de SIGEP 1 y 2, SGI en ambiente de producción, Proactivanet en producción, ORFEO en producción, VMWare, Backup del Gestor Normativo, del formulario de gerencia pública y del sistema Kactus.
	Fallas tecnológicas				

7. Recomendaciones de mejoramiento de la Oficina de Control Interno:

1. Con el fin de fortalecer la trazabilidad de la gestión efectuada en el tratamiento de los riesgos de la dependencia, se sugiere que en el SGI a futuro:
 - Se registre el nombre del archivo o archivos que soportan cada una de las tareas que se detallan, acorde con lo especificado por la dependencia en el comentario de avance de la actividad. Esto debido a que en el riesgo *“Favorecimiento de un privado durante la identificación de necesidades en los procesos de selección de proveedores”* causa *“Uso excesivo del poder”*, no se relacionaron las actas del Comité de Contratación.
 - Se registre oportunamente el avance de las acciones de control, definidas en el mapa de riesgos. Lo anterior, en razón a que para el riesgo *“Pérdida de la disponibilidad de los activos”* causa *“Obsolescencia tecnológica”*, no se evidenció el reporte de avance para los meses de octubre y noviembre.
 - Se registre el avance y sus respectivas evidencias acorde con la acción de control especificada para el riesgo. Esto debido a que en el riesgo *“Pérdida de la disponibilidad de los activos”* causas *“Obsolescencia tecnológica”* y *“Pérdida de servicios esenciales.”*, no se está reflejando en el avance la gestión y sus soportes acorde con la acción de control.
2. Para los próximos ejercicios de planeación, se revise la metodología para definir las metas de los indicadores en el SGI, específicamente para el indicador *“Atención oportuna de incidencias y peticiones nivel especializado”*, en el cual como lo pudo evidenciar la Oficina de Control Interno, solo se pudo cumplir la meta establecida en los meses de mayo y agosto de la vigencia 2020.
3. Con el fin de evidenciar toda la gestión y trazabilidad en la ejecución de las actividades registradas para cada uno de los productos en la Planeación Institucional, se sugiere a futuro que, al relacionar los avances en el SGI, se tengan en cuenta todos los archivos correspondientes que soportan su cumplimiento.

Casos puntuales en los que se observó esta debilidad fue en el producto *“Política de Gobierno Digital ejecutada”*, actividades:

- Diseñar el modelo de datos maestros de la entidad
 - Diseñar la propuesta de PMO en la entidad
4. La Oficina de Control Interno pudo evidenciar el cumplimiento de las metas propuestas en la Planeación Institucional. Adicional al oportuno registro de los avances en el aplicativo SGI, se evidencia una mejora en la claridad y pertinencia de estos.

8. Firmas:

Auditor (es)

Jefe Oficina de Control Interno