ARN AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN	**INFORME DE AUDITORÍA PROCESO DE GESTION DE TECNOLOGIAS DE LA INFORMACION 2021 (AUD – 2117)**

INFORMACIÓN BASICA			
FECHA DE INFORME	30 de septiembre de 2021	**PROCESO / DEPENDENCIA**	Gestión de Tecnologías de la Información
FECHA SEGUIMIENTO	10 de agosto a 17 de septiembre de 2021	**AUDITOR**	**Auditor Líder:** Sandra Paola Estupiñán **Grupo Auditor:** Derly Katherine Cubides

1. OBJETIVO

Evaluar el grado de cumplimiento de los requisitos de los Sistema de Gestión adoptados en la Agencia, así como la normatividad vigente y métodos de operación establecidos para el fortalecimiento de la operación y gestión institucional, del Proceso de Gestión de Tecnologías de la Información.

2. ALCANCE

La verificación se realizará a través de la herramienta Microsoft Teams. Para el Proceso de Gestión de Tecnologías de la Información, basados en la información recopilada entre el 01/09/2020 al 30/08/2021.

3. CRITERIOS

Se tuvieron en cuenta, entre otros, los siguientes criterios normativos: a)Ley 975 de 2005; b) Ley 1437 de 2011; c) Ley 1755 de 2015; d) Decreto 1391 de 2011; e) Decreto 1082 de 2015; f) Decreto 648 de 2017; g) Decreto Ley 899 de 2017; h) Decreto 1499 de 2017; i) Decreto 69 de 2018; j) Decreto 1212 de 2018; k) Decreto 1363 de 2018; l) Resolución 346 de 2012; m) Resolución 754 de 2013; n) Resolución 1724 de 2014; o) Resolución 0075 de 2016; p) Resolución 1356 de 2016; q) Resolución 3207 de 2018; r) Resolución 2536 de 2019; s) CONPES 3931 de 2018; t) NTC 6047:2013; u) NTC ISO 27001:2013; v) NTC ISO 9001:2015; w) NTC ISO 14001:2015; x) NTC PE 1000:2017; y) NTC ISO 45001:2018.

De igual manera, se tuvo en cuenta, entre otros, los siguientes procedimientos, manuales e instructivos inscritos en el Software para la Planeación y Gestión que apliquen a la unidad auditable, a saber:

•Caracterización proceso gestión de tecnologías de la información
• Manual Del Sistema De Gestión De Seguridad De La Información
•Procedimiento Atención A Requerimientos De Sistemas De Información
•Procedimiento Soporte A Usuarios
•Gestión De Incidentes De Seguridad
• Normograma Del Proceso De Gestión De Tecnologías De La Información

En lo relacionado con el tema presupuestal se tuvo en cuenta los siguientes aspectos:
• Asignación de recursos Presupuestales.
• Ejecución Plan Anual de Adquisiciones.
• Ejecución Presupuestal.

Finalmente, es importante dejar en claro que se tuvieron en cuenta las demás normas, documentos, circulares, procedimientos, manuales e instructivos que le apliquen a cada una de las unidades auditables.

4. DESARROLLO

La auditoría al Proceso de Gestión de Tecnologías de la Información se efectuó de acuerdo con las actividades planificadas en el Plan de Auditoría así:

- Reunión de apertura realizada el día 20 de septiembre de 2021.
- Verificación de los resultados del Plan de Acción Institucional y demás planes a los cuales aporta en su gestión la unidad auditable.
- Verificación la aplicación de los controles para los riesgos institucionales.
- Verificación el conocimiento y aplicación de las normas adoptadas por la Entidad. (ISOs 9001, 45001, 14001, 27001, PE 1000 y MIPG)
- Verificación de la Implementación de los métodos de operación del Proceso de Gestión de Tecnologías de la Información.
- Verificación la ejecución de traslados documentales al nivel central y el estado del archivo de gestión.
- Verificación el seguimiento y cumplimiento de PQRSD
- Verificación y evaluar la eficacia de las acciones correctiva y de mejoras de los planes de mejoramiento cerrados.
- Verificación la ejecución presupuestal.
- Reunión de cierre realizada el día 24 de septiembre de 2021.

En el ejercicio de este auditoria se pudo haber incurrido en imprecisiones debido a cualquier limitación frente a la información reportada y encontrada en los sistemas de información oficiales.

4.1 Aspectos Generales del Grupo

Para desarrollar la Gestión Institucional, en especial, para cumplir con las actividades de la Caracterización que son responsabilidad del Grupo, así como lo establecido desde el PAI, demás planes a los cuales aporta en su gestión, en la Gestión de los Riesgos, en la implementación de las acciones correctivas, preventivas y de mejoras de los planes de mejora y las acciones derivadas de los Proyectos de Inversión, el Proceso de Gestión de Tecnologías de la Información cuenta con el apoyo de veinticinco (25) funcionarios de Carrera Administrativa, de los cuales dos (2) se encuentran en encargo y cuatro (4) se encuentran vacantes, once (11) Contratistas los cuales pasaron en el mes de julio y septiembre a ser parte del proveedor de servicios tecnológicos, debido a una reestructuración donde se articularon nuevos servicios de TI; en el mismo orden de ideas, los costos mensuales totales proyectados para la Vigencia 2021 de este rubro son los siguientes:

EMPLEO GENERAL	ASIGNACIÓN BÁSICA	SITUACIÓN ADMINISTRATIVA
Jefe de oficina 0137 – 20	$ 8.646.847	Libre nombramiento y remoción
Técnico administrativo 3124 – 11	$ 1.836.730	Carrera administrativa
Profesional especializado 2028 – 24	$ 8.067.732	Carrera administrativa
Profesional especializado 2028 – 21	$ 6.583.507	Carrera administrativa
Profesional especializado 2028 – 19	$ 5.738.031	Carrera administrativa
Profesional especializado 2028 – 19	$ 5.738.031	Periodo de prueba
Profesional especializado 2028 – 19	$ 5.738.031	Carrera administrativa
Profesional especializado 2028 – 19	$ 5.738.031	Carrera administrativa
Profesional universitario 2044 – 11	$ 3.211.673	Provisional
Profesional universitario 2044 – 11	$ 3.211.673	Encargo carrera Admin.
Técnico administrativo 3124 – 17	$ 2.721.555	Provisional
Profesional especializado 2028 - 24	$ 8.067.732	Periodo de prueba
Profesional especializado 2028 - 21	$ 6.583.507	Carrera administrativa
Profesional especializado 2028 - 19	$ 5.738.031	Carrera administrativa
Profesional especializado 2028 - 13	$ 3.691.789	Carrera administrativa
Técnico administrativo 3124 - 17	$ 2.721.555	Carrera administrativa
Técnico administrativo 3124 - 17	$ 2.721.555	Carrera administrativa
Técnico administrativo 3124 - 17	$ 2.721.555	Carrera administrativa
Técnico administrativo 3124 - 11	$ 1.836.730	Encargo carrera Admin.
Profesional 3	$ 7.843.000	Contratista
Profesional 8	$ 3.863.000	Contratista
profesional 1	$ 9.774.000	contratista
Profesional 8	$ 3.863.000	Contratista
Profesional 2	$ 9.071.000	Contratista
Profesional 4	$ 6.790.000	Contratista
Profesional 4	$ 6.790.000	Contratista
Profesional 3	$ 7.843.000	Contratista
Técnico 1	$ 3.336.000	Contratista
Profesional 4	$ 6.790.000	Contratista
Profesional 8	$ 3.863.000	Contratista
Total, Anual Vigencia 2021	**$ 1.760.257.284**	

***El cálculo del valor de los contratistas fue calculado con 6 y 9 meses respectivamente, de acuerdo a lo contratado.

En lo que respecta a la ejecución presupuestal se verificó la ejecución de acuerdo al Informe de Seguimiento a la Disponibilidad presupuestal con corte a 31 de agosto de 2021, donde se identificó lo siguiente:

PRESIDENCIA DE LA REPÚBLICA
AGENCIA PARA LA REINCORPORACION Y LA NORMALIZACION ARN
SEGUIMIENTO A LA DISPONIBILIDAD PRESUPUESTAL VIGENCIA 2021

La paz con legalidad es de todos

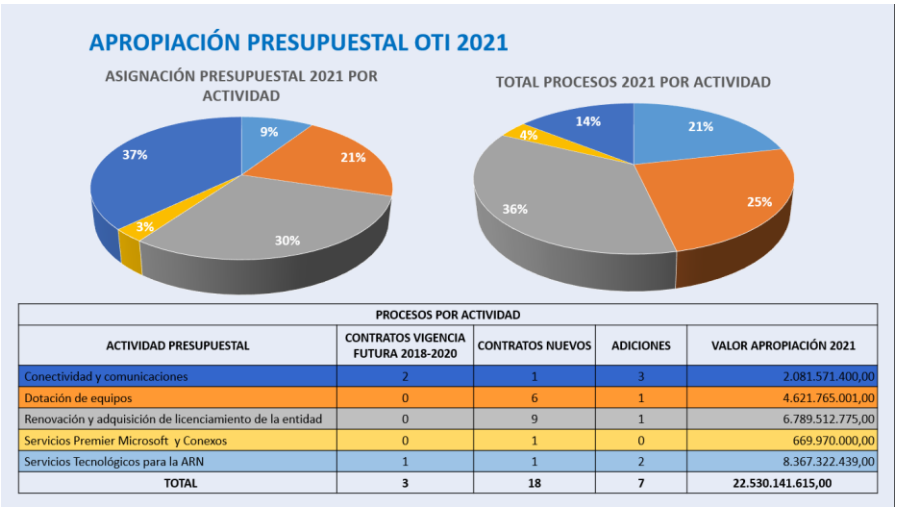
Seguimiento Ejecución del 1 al 31 de Agosto de 2021

			EJECUCION PRESUPUESTAL		PROCESOS ADJUDICADOS			
OFICINA – GRUPO	RUBRO	ACTIVIDAD	TOTAL APROPIACION	TOTAL RPs	Valor	Proceso	Valor	Proceso
a. Oficina Tecnologías Información	A-03-03-01-001	Conectividad y Comunicaciones	624.471.420	534.471.420	345.324.771	Cto 1551/20 – Nube privada	189.146.649	*Cto 1737/18 – Conectividad *Cto 1169 – Conectividad VF
	A-03-03-01-001	Servicio Premier de Microsoft y conexos	200.991.000	200.991.000	200.991.000	Cto 1224 – Soporte técnico Premier		
	A-03-03-01-001	Dotación de Equipos	1.019.986.617	418.733.989	118.747.388	*Cto 1211 – Librería de respaldo *Cto 1618/20 – Minidatacenter	299.986.600	*Cto 1535 – Diademas *Cto 1543 – Escáneres
	A-03-03-01-001	Servicios Tecnológicos para la ARN	2.510.196.731	2.510.196.731	2.474.818.031	Cto 1807/18 – Telefonía y centro de servicios y adición	35.378.700	Cto 1013 – Sharepoint
	A-03-03-01-001	Renovación y Adquisición de licenciamiento de la entidad	2.036.853.832	1.789.800.605	1.485.527.897	*Cto 1117 – Lic ArcGIS *Cto 1139 – Power BI Pro *Cto 1135 – Licencias Stata *Cto 1278 – Mailchimp *Cto 1279 – Microsoft	304.272.708	*Cto 1779/20 – Lic Adobe *Cto 1141 – Licencia Nvivo *Cto 1180 – Microsoft Azure *Cto 1229 – Lic solarwinds
a. Oficina Tecnologías Información	A-03-03-01-001	Conectividad y Comunicaciones	1.457.099.980	1.247.099.980	805.757.799	Cto 1551/20 – Nube privada	441.342.181	*Cto 1737/18 – Conectividad *Cto 1169 – Conectividad VF
	A-03-03-01-001	Servicio Premier de Microsoft y conexos	468.979.000	468.979.000	468.979.000	Cto 1224 – Soporte técnico Premier		
	A-03-03-01-001	Dotación de Equipos	3.601.778.384	977.045.973	277.077.239	*Cto 1211 – Librería de respaldo *Cto 1618/20 – Minidatacenter	699.968.734	*Cto 1535 – Diademas *Cto 1543 – Escáneres
	A-03-03-01-001	Servicios Tecnológicos para la ARN	5.857.125.708	5.857.125.708	5.774.575.408	Cto 1807/18 – Telefonía y centro de servicios y adición	82.550.300	Cto 1013 – Sharepoint
	A-03-03-01-001	Renovación y Adquisición de licenciamiento de la entidad	4.752.658.943	4.176.201.414	3.466.231.762	*Cto 1117 – Lic ArcGIS *Cto 1139 – Power BI Pro *Cto 1135 – Licencias Stata *Cto 1278 – Mailchimp *Cto 1279 – Microsoft	709.969.652	*Cto 1779/20 – Lic Adobe *Cto 1141 – Licencia Nvivo *Cto 1180 – Microsoft Azure *Cto 1229 – Lic solarwinds
			22.530.141.615	**18.180.645.820**				

Fuente: Informe Seguimiento Disponibilidad Presupuestal con corte agosto 2021. Subdirección Financiera ARN

Del total de la apropiación o asignación presupuestal asignada a la Oficina de Tecnologías de la Información, correspondiente a $22.530.141.615 = se ha contratado con corte a 31 de agosto de 2021 $18.180.645.820 = lo que corresponde al 81% del total presupuestado, y se identifican los procesos adjudicados de acuerdo a la contratación realizada.

Adicional a lo anterior la oficina de Tecnologías de la información aporto el siguiente gráfico en el cual se evidencia la apropiación presupuestal y el detalle de la contratación por cada actividad presupuestal



PROCESOS POR ACTIVIDAD				
ACTIVIDAD PRESUPUESTAL	CONTRATOS VIGENCIA FUTURA 2018-2020	CONTRATOS NUEVOS	ADICIONES	VALOR APROPIACIÓN 2021
Conectividad y comunicaciones	2	1	3	2.081.571.400,00
Dotación de equipos	0	6	1	4.621.765.001,00
Renovación y adquisición de licenciamiento de la entidad	0	9	1	6.789.512.775,00
Servicios Premier Microsoft y Conexos	0	1	0	669.970.000,00
Servicios Tecnológicos para la ARN	1	1	2	8.367.322.439,00
TOTAL	3	18	7	22.530.141.615,00

Fuente: Presentación Proceso de Gestión Tecnologías de la Información

En entrevista con la jefe de la Oficina de Tecnologías de la Información se identificó la apropiación del proceso de formulación y ejecución del presupuesto asignado, el cual corresponde al presupuesto de gasto de mediano plazo, que se le realizan ajustes anuales y es parte del presupuesto del funcionamiento debido a que no hay proyectos de inversión.

Frente a la programación y ejecución de acuerdo al Plan anual de adquisiciones se validó que de acuerdo a la circular que se emite por el Director de la ARN, se inicia un proceso de identificación de necesidades de las áreas de acuerdo a reuniones realizadas, que la Oficina de Tecnologías de la Información se rige principalmente por el acuerdo marco de precios y que las necesidades se alinean al Plan estratégico de Tecnologías de la Información (PETI), al Plan sectorial o al plan de segundo nivel en lo posible, de esta manera se establece el PAA de acuerdo a necesidades, se inician mesas de trabajo para evitar incumplimientos en los acuerdos definido, para confirmar la necesidad y afinar necesidad y el estudio de mercado para ajustar diferencias, hacer ajustes y destinarlos a otros temas si se requiere.

Para la ejecución contractual se realizan reuniones de seguimiento mensuales con los proveedores por parte de los supervisores de los contratos para validar el cumplimiento y la facturación, se hace seguimiento en la ejecución de los mismos, verificación de los servicios, se generan alertas y se solicita apoyo si se generan incumplimientos los cuales se informan, dentro de los seguimiento se ha identificado reprocesos por temas de facturación, especialmente por el tema de facturación electrónica y por la división de las facturas para su aprobación por SIIF Nación.

En cuanto a las liquidaciones de los contratos se indica que se hace revisión permanente de la gestión y consulta al grupo de Gestión Contractual y a la fecha solo tienen pendiente un contrato por liquidar debido a que no lo ha firmado el proveedor ya que la mayoría son contratos con servicios de tracto sucesivo o contratos de compraventa los cuales no requieren liquidación.

Se indica que los temas que se encuentran pendientes por contratar corresponden a mil millones de la SAN, la adquisición de cámaras, Una adición al contrato de Nube privada, el licenciamiento del antivirus y la adquisición de certificados digitales, y dentro de los puntos críticos está el no conseguir cámaras con mayor resolución para las estaciones fijas, los problemas con el simulador de Colombia compra eficiente y el acuerdo marco de precios y frente a los saldos pendientes se revisa el destino para realizar adiciones a algunos contratos y extender las vigencias.

Se destaca el seguimiento que se realiza a la parte contractual y las reuniones de seguimiento con los proveedores frente a la supervisión de los contratos a cargo del proceso.

4.2 Seguimiento al Plan de Acción Institucional y demás planes a los cuales aporta en su gestión.

Se identifica en el Proceso de Gestión de Tecnologías de la Información, se reportan los siguientes indicadores:

- Plan de Acción Institucional (PAI) y Plan Estratégico Sectorial (PES) – 7 indicadores.

COD_ IND.	INDICADOR	FORMULA	Validación
PAI_61	Nivel de ajuste y avance en la implementación del	{Nivel de avance en la implementación del	El indicador se incumplió en el año 2020 debido a que no se oficializo el documento según lo evidenciado en la evaluación por dependencias

	Plan de preservación digital 2021	Plan de preservación digital}	de Gestión documental, se identifica que este fue asignado en abril a la OTI, sin embargo según lo manifestado en este momento se va a reconstruir la hoja de ruta del proyecto, por lo tanto, se identifica un posible riesgo en el cumplimiento del indicador toda vez que la implementación no ha iniciado , debido a que el documento no está culminado aún, igualmente es importante que para soportar el avance en la implementación del plan se identifiquen los temas planeados y los que se han ejecutado para garantizar la adecuada implementación del mismo.
PAI_63	Cantidad de sello de la Excelencia en Gobierno Digital 2021	{# Sellos de Excelencia otorgados a la Agencia por el cumplimiento de las estrategias de Gob. Digital}	Hace parte del plan sectorial indicador (SEC_4), Para el tercer trimestre se dio cumplimiento con la obtención de un nuevo sello de excelencia en el mes de agosto relacionado con la categoría de datos abiertos.
PAI_64	Implementación del Plan de la Política de Gobierno Digital, teniendo en cuenta la evaluación del FURAG vigente o autodiagnóstico de MinTic ARN y las últimas disposiciones normativas 2021	{% avance en la implementación plan de la política de Gobierno Digital}	Hace parte del plan sectorial indicador (SEC_5), En el año 2020 se realizó ajuste a las metas establecidas en el plan estratégico sectorial que fue definido de la siguiente manera: 2020 (20%), para el 2021 (30%) y para 2022 (30%). Para un total de 80%.
PAI_65	Nivel de avance en la implementación del PETI 2021	{Porcentaje de cumplimiento de avance en la implementación del PETI}	Indicador anual para cumplir el 40% este año, de cara al 100% de los proyectos identificados en el PETI, 2019-10% 2020 el 8%- 2021-13 proyectos con 40%% - 13 proyectos 2021, se ajustaron según las necesidades los cuales se deben ejecutar en 2021. Cumplimiento último trimestre. Hace parte del plan de segundo nivel.
PAI_67	Nivel de cumplimiento del Plan de Seguridad y Privacidad de la Información 2021	{# actividades realizadas /# actividades planeadas}	Se tiene plan de trabajo para el avance de las actividades, socializado en comité institucional, no todas las actividades tienen fechas definidas, se encuentran pendientes retroalimentaciones y definir fechas por algunas dependencias, por lo tanto, Se recomienda ampliar la información de seguimiento al cumplimiento del indicador mencionando en el registro trimestral el detalle de las actividades planeadas y las actividades ejecutadas efectivamente.
PAI_68	Porcentaje de tareas de desarrollo realizadas en el	{#tareas desarrollo software apoyo finalizadas /#tareas	Se manejan dos (2) rutas, un registro en Aranda y el proceso de desarrollo que es el más largo el cual se registran y desarrollan en Azure DevOps.

	periodo de Sistema de Apoyo 2021	desarrollo software apoyo planeadas}	Se mide las tareas de desarrollo según un ajuste solicitado, cuantas tareas planearon y cuantas cumplieron.
PAI_69	Porcentaje de tareas de desarrollo realizadas en el periodo en el Sistema Misional 2021	{#tareas desarrollo software misional finalizadas /#tareas desarrollo software misional planeadas}	Se recomienda no duplicar los archivos que soportan el indicador se encuentran en formato Word y .pdf.

- Plan de Anticorrupción y de Atención al Ciudadano 2021 (PAC) - 1 indicador.

COD_ IND.	INDICADOR	FORMULA	Validación
PAC_19	Evaluación de cumplimiento a página web mediante aplicación de herramienta diagnóstico de usabilidad y accesibilidad 2021	{Evaluación de la herramienta de diagnóstico de usabilidad y accesibilidad de la página web}	Se usan herramientas de accesibilidad a personas con discapacidad, limitación visual, el software va etiquetando la información, subtitulo, imagen, Se está realizando el análisis 2 veces al año, en el mes de junio se hizo con la recomendación sugerida de la W3C en la página https://www.w3.org/WAI/ER/tools/. actualmente la página está en calificación AA según la norma WCAG 2.0.

- Plan de segundo nivel – 2 indicadores.

INDICADOR	FORMULA	VALIDACION
Diseño e Implementación de los proyectos identificados que hacen parte los componentes del PETI	{% avance de ejecución de los proyectos PETI con tipología Sistemas de Información 2021} + {% avance de ejecución de los proyectos PETI con tipologías Infraestructura y transversal 2021} |2 * 1	Alineado con el indicador del PAI indicador (PAI_65) se reportan los 13 proyectos que se van a ejecutar en el 2021, Se validó el documento con el porcentaje de avance.
Actualización del Documento del Plan Estratégico de Tecnologías de la Información	{% Ejecución en el Diseño y Actualización del documento PETI 2020}	Se identificó dentro del proceso de direccionamiento Estratégico, PETI ya cargado el 20/09/2021 en SIG.

De la validación de los planes que se manejan en la entidad, asociados al Proceso de Gestión de Tecnologías de la Información se identifica que los indicadores a la fecha se han reportado con oportunidad y los ajustes de calidad se han subsanado de acuerdo a lo indicado por planeación y Control interno en los casos que aplican.

- Plan Indicadores de Proceso (PIP) - 2 indicadores

De acuerdo a los resultados de evaluación de dependencias se observa que el Proceso de Gestión de Tecnologías de la Información ha obtenido los siguientes resultados durante las siguientes vigencias:

DEPENDENCIA	2017		2018		2019		2020	
	RESULTADO SIGER	EVALUACION CONTROL INTERNO DE GESTIÓN	RESULTADO SIGER	EVALUACION CONTROL INTERNO DE GESTIÓN	RESULTADO SIGER	EVALUACION CONTROL INTERNO DE GESTIÓN	RESULTADO SIGER	EVALUACION CONTROL INTERNO DE GESTIÓN
Oficina de Tecnologías de la Información	100,00	100,00	100,00	95,00	100,00	98,12	100,00	97,32

Como observación general en los mencionados periodos se tiene que el Proceso de Gestión de Tecnologías de la Información debe f**ortalecer el tema de elaboración y administración de evidencias.**

Para lo corrido de la Vigencia 2021 en lo que respecta al primer semestre (corte al 30 de junio), el Grupo obtuvo una calificación del **100%** de cumplimiento en SIGER, correspondiente al cumplimiento del avance en los dos (2) indicadores del proceso. Se procedió a dar revisión a los resultados obtenidos en dicho periodo, así mismo, se exploró sobre los controles aplicados desde el Proceso con el fin de dar cumplimiento a las metas planteadas, así:

Indicador 1: Nivel de satisfacción de los servicios de información y tecnología 2021

Para el periodo el Proceso de Gestión de Tecnologías de la Información indica que: el cumplimiento de lo programado para el primer trimestre se recibieron un total de 2.506 de usuarios que respondieron la encuesta y se contestaron como usuarios satisfechos con el servicios de la OTI un total 2.429, equivalentes al 96.93%., y para el segundo trimestre se recibieron un total de 2.228 encuestas en las cuales 2.136 usuarios manifestaron encontrarse satisfechos con el servicios de la OTI, lo que corresponde al 95.87%.

Resultados de evaluación de Dependencias 1er Semestre de 2021 (realizado por el Grupo de Control Interno de Gestión):

Resultado 3%: Se observa el cumplimiento de la meta para este indicador.
Calidad de información 5%: Los documentos cumplen con los lineamientos establecidos en el Manual de Seguimiento a la Planeación y Gestión Institucional.
Oportunidad 2%: los registros realizados en el software administrador del SIGER se evidencian que fueron efectuados dentro de los tiempos establecidos.

Indicador 2: Oportunidad y eficacia en la atención de solicitudes de servicios 2021

Para el periodo el Proceso de Gestión de Tecnologías de la Información indica que: Para el primer trimestre se recibieron 2.480 solicitudes y se respondieron dentro del término (ANS) 2.413, equivalentes

al 97.3%. y para el segundo trimestre se recibieron 2.346 solicitudes y se respondieron dentro del término (ANS) 2.212, equivalentes al 94.29%. Como resultado se ha cumplido con la meta del 75%.

Resultados de evaluación de Dependencias 1er Semestre de 2021 (realizado por el Grupo de Control Interno de Gestión):

Resultado 3%: Se observa el cumplimiento de la meta para este indicador.
Calidad de información 5%: Los documentos cumplen con los lineamientos establecidos en el Manual de Seguimiento a la Planeación y Gestión Institucional.
Oportunidad 2%: los registros realizados en el software administrador del SIGER se evidencian que fueron efectuados dentro de los tiempos establecidos.

Por lo tanto, frente a la evaluación por dependencias del 1er trimestre se obtuvo una calificación del 100% debido a que se observa el cumplimiento de la meta para los indicadores, los documentos cumplen con los lineamientos establecidos en el Manual de Seguimiento a la Planeación y Gestión Institucional, y los registros realizados en el software administrador del SIGER se evidencian que fueron efectuados dentro de los tiempos establecidos. No obstante, se recomienda dejar los archivos de las evidencias en un solo formato cuando se trata de la misma información en los casos de los documentos en Word, Excel y pdf, para evitar duplicidad de información en el repositorio.

4.3 ACCIONES EN MAPAS DE RIESGOS

Para la Vigencia 2021, el Proceso de Gestión de Tecnologías de la Informació se encuentra vinculado a dos (2) riesgos propios del Proceso de Tecnología, dos (2) de Seguridad de la Información y tres (3) transversales. Después de revisadas las evidencias ubicadas en las carpetas compartidas dispuestas para este fin, se verificó lo siguiente:

1. Proceso de Gestión de Tecnologías de la Información

- **Riesgo 1:** Indisponibilidad de los servicios TI.
  Clasificación del Riesgo: Tecnología
  Controles:

  1.El líder del servicio hace seguimiento a los resultados del monitoreo de la disponibilidad de la infraestructura tecnológica de los servicios de TI que se realiza 7x24x365 a través de varias herramientas automáticas; cuando se presenta un evento adverso el servicio de monitoreo lo registra y documenta en la herramienta de gestión Aranda para su atención. Evidencia: Informe de monitoreo de servicios.
  2. Cada supervisor de cada contrato realiza seguimiento mensual de acuerdo con el Manual de contratación, supervisión e interventoría a los servicios prestados por los proveedores de conectividad, nube privada y servicios tecnológicos, cuando se presenta un incumplimiento se solicita formalmente al proveedor para que tome las acciones pertinentes. Evidencia: Informes de seguimiento de contratos
  3. El líder del servicio revisa y gestiona de acuerdo con los recursos disponibles los boletines de recomendaciones que mensualmente emiten los centros de respuesta de atención a incidentes,

cuando se genere una recomendación se registra y documenta en la herramienta de gestión Aranda para su atención. Evidencia: Informe de boletines.

Acciones:
Control1: Se reciben las recomendaciones de centros de respuestas, (8 boletines de Csirt), con los cuales se ajustan las observaciones, y adicional a esto se tiene verificación de seguridad por capas, perimetral, IPS, Proxy, WAF, firewall interno o de Core, controles a nivel de aplicación y D.A, SIEM (Apliance. Logs de Windows y plataformas monitoreadas, aplicación de firmas o comportamiento) administrado por Indra, se tiene un SOC, análisis de lo expuesto en internet, URL sospechosas monitoreo constante y recomendaciones de bloqueo preventivo (se boquea el remitente, IPs, y URLs) Se abre caso con el proveedor si es necesario.
Control 2: Ya se incluyeron las evidencias en la carpeta para el segundo trimestre, y se verifican los informes mensuales de seguimiento, y no se ha superado el ANS, se hace seguimiento de los servicios mensualmente.
Control 3: Informes de proveedores de conectividad (media commerce), nube privada (century link) y servicios Tecnológicos, reporte de los seguimiento y monitoreos. Se confirma que los controles son suficientes y no necesitan ajustes por el momento.

De manera simultánea a la revisión de los controles y las acciones de cada riesgo, el auditor expone el resultado de la revisión efectuada por el Grupo de Control Interno de Gestión a la gestión de los riesgos con base en los seguimientos realizados en el Aplicativo dispuesto para este fin, resaltando los siguientes aspectos:

Resultado: Se observa el cumplimiento de las actividades propuestas para mitigar el riesgo.
Calidad de la Información: Las evidencias aportadas en la carpeta compartida cumplen con los lineamientos establecidos en el Manual de Seguimiento a la Planeación y Gestión Institucional (Codigo:DE-M-03), no se identifican soportes del segundo trimestre en la carpeta compartida para la acción 2, (tema que ya fue subsanado para la fecha de la auditoria).
Oportunidad: Se observó que los seguimientos y análisis se realizaron de manera extemporánea para el primer trimestre. (El seguimiento de las acciones se realizó en los tiempos definidos, el análisis es el que se realiza extemporáneo)

- **Riesgo 2:** Infraestructura de TI Insuficiente.
  Clasificación del Riesgo: Tecnología

  Controles:
  1. El líder del servicio hace seguimiento a los resultados del monitoreo de la capacidad de la infraestructura tecnológica de los servicios de TI que se realiza 7x24x365 a través de varias herramientas automáticas; El líder del servicio hace seguimiento a la gestión de activos que se realiza a través de la herramienta de gestión Aranda. Cuando se presenta un evento fuera de los parámetros establecidos se registra y documenta en la herramienta de gestión Aranda para su atención. Evidencia: Informe de gestión de capacidad de servicios monitoreados.
  2.El líder del servicio hace seguimiento y monitoreo mensual al plan anual de adquisiciones, a través del Marco de Gasto de Mediano Plazo, los resultados de dicho monitoreo quedan descritos en el acuerdo de desempeño, si se presenta un evento adverso, se realiza el respectivo ajuste a plan

mediante solicitud al comité de contratación. Evidencia: Seguimiento a la ejecución del Plan Anual de Adquisición.

Acciones:
Se realiza la verificación por parte del líder del servicio, se genera el informe de capacidad, se hace validación con solarwinds para gestión de la capacidad, se presentan alertas en 75 o 80, y hasta 95 umbrales críticos pero el esquema permite maniobrar, se realiza el análisis de gestión de capacidad, para definir el PAA y robustecer las capas, No se ha materializado este riesgo. Se tiene Control de Capacidad, Control de gestión de activos: parque computacional, seguimiento control de software, se usa la herramienta Aranda y la ficha técnica de las características del equipo y se validan los inventarios con Aldino de forma mensual, como parte del monitoreo, adicional a esto se hace Seguimiento a la ejecución del PAA, con lo que se identifica que los controles son suficientes para este riesgo.

De manera simultánea a la revisión de los controles y las acciones de cada riesgo, el auditor expone el resultado de la revisión efectuada por el Grupo de Control Interno de Gestión a la gestión de los riesgos con base en los seguimientos realizados en el Aplicativo dispuesto para este fin, resaltando los siguientes aspectos:

Resultado: Se observa el cumplimiento de las actividades propuestas para mitigar el riesgo.
Calidad de la Información: Las evidencias aportadas en la carpeta compartida cumplen con los lineamientos establecidos en el Manual de Seguimiento a la Planeación y Gestión Institucional (Codigo:DE-M-03).
Oportunidad: Se observa el registro dentro de las fechas establecidas del seguimiento y análisis realizados en el software administrador del SIGER.

- **Riesgo 3:** Pérdida de la información.
  Tipo de Riesgo: Seguridad de la información.
  Acción No.1: Verificar mensualmente por parte de líder del servicio que las copias de respaldo se realicen de acuerdo con las tareas programadas, para garantizar la disponibilidad de la información centralizada. Evidencias: Informe mensual de backups. Frente a esta acción se indica que se realizan los backups de información, respaldo a discos y cintas de manera mensual, información de disco de usuario final (retención de 10 meses), y a cinta se realizan semanal y se rescriben surtido el mes, se va a alinear con áreas para definir la nueva política de los tiempos de retención alineado con la preservación de la información.
  Acción No.2: Verificar mensualmente por parte de líder del servicio la restauración de las copias de respaldo, a través de la herramienta de recovery backups, para garantizar la disponibilidad e integridad de la información centralizada. Evidencia: Informes de pruebas de restauración. Para esta acción se han realizado pruebas de restauración, se prueba en la BD de centro alterno, la BD del nodo principal se restaura en el centro alterno, solo con las pruebas del DBA, adicional se realizan pruebas de restauración de solicitudes por demanda y todas han sido satisfactorias.
  Acción No.18: El profesional designado por parte del proceso de Gestión de Tecnologías de la Información debe realizar la revisión y actualización de los activos de información de su dependencia, teniendo en cuenta los criterios de actualización establecidos en el DE-I-03 Instructivo para la Actualización de la matriz de activos de información. Frente a esta acción se realizó la actualización de

los activos de información de la dependencia, y realización del plan de trabajo, seguimiento de los requisitos en el instructivo de Matriz y la validación de gestión documental jurídica y tecnología.

Sin embargo se recomienda fortalecer el control, y revisar que el control realmente mitigue el riesgo de Pérdida de Información, a lo que el proceso indica que se debe madurar el control porque hasta ahora se dió inicio con las áreas y se identificó el medio debido a que se propusieron unos riesgos transversales para cada proceso y no fue posible asociarlo en cada proceso por temas de la herramienta, eso está pendiente de revisión hasta que se resuelva el tema de la prospectiva, y que se separe el tema de seguridad de la Información y no se asocien todos los riesgos de seguridad a la OTI.

- **Riesgo 4:** Uso indebido de la información.
  Clasificación del Riesgo: Seguridad de la información.
  Acción No. 2: Realizar de forma mensual por parte del líder del servicio las actividades de verificación (depuración) de usuarios en los sistemas de información y aplicativos misionales y directorio activo, con el fin de realizar el control de acceso a la información. Evidencia: Informe de seguimiento.

  Acción No. 3: Verificar mensualmente por parte del líder del servicio, los informes de monitoreo de seguridad y tomar las acciones pertinentes, con el fin de asegurar la información frente a las amenazas. Evidencia: Informe de seguimiento.

  Acción No. 6: El líder del servicio realiza la sensibilización a los funcionarios y colaboradores de la ARN, de acuerdo al cronograma del plan de sensibilización, en temas asociados a servicios de TI, con el fin de propender el uso y apropiación de las buenas prácticas de seguridad de la información. Evidencia: Informe de seguimiento.

  Acción No. 7: Verificar de forma mensual por parte del líder del servicio, los informes del administrador de la solución DLP y tomar las acciones pertinentes de ser necesario, con el fin de asegurar la información frente a las amenazas. Evidencia: Informe de seguimiento.

  Acción No. 18: El profesional designado por parte del proceso de Gestión de Tecnologías de la Información debe realizar la revisión y actualización del índice de información clasificada y reservada y de la matriz de flujos de información, teniendo en cuenta los lineamientos establecidos.

De las acciones definidas se el proceso indica que se están realizando las actividades de depuración, mensualmente del directorio activo, y aplicativos misionales(SIRR-ALADINO),así como las sensibilización de seguridad de la información según el cronograma, la verificación del DLP y la plataforma de TrendMicro se hace con mesas de trabajo para verificar y ajustar las reglas, sin embargo se identifica un falencia frente a la línea que se debe generar desde el Oficial de Seguridad en estos temas, y en cuanto a la actualización del índice de información clasificada y reservada, se indica que para el primer trimestre se estableció el plan y en el tercer se hará la actualización.

2. Proceso Gestión del Talento Humano.

Riesgo: Contagios de COVID-19 por el retorno a la presencialidad en todas las sedes de la ARN.
Clasificación del Riesgo: Cumplimiento.
Acción No. 14: 14. El líder del proceso de Gestión de Tecnologías de la información promueve la apropiación de acuerdo a las notas informativas que se generen desde Talento Humano de manera

trimestral. Evidencias: Listas de asistencia, actas de reunión, registros fotográficos o correos electrónicos, que den cuenta de la sensibilización de las notas informativas

El Proceso de Gestión de Tecnologías de la Información indica que por el momento aún se encuentran en trabajo en casa salvo algunos temas en sitio dependiendo de la necesidad del servicio, están con alternancia y el personal de soporte en sitio si está en la sede, frente a la acción indica que se hacen sensibilización de las notas recibidas, se reenvian las notas internamente, y se participa en las capacitaciones, además se les recuerda sobre el registro en Alissta diariamente.

3. Proceso Direccionamiento Estratégico

Riesgo 1: Incumplimiento de la ley de transparencia y acceso a la información pública
Clasificación del Riesgo: Estratégico
Acción No. 9: El profesional designado por parte del proceso de Gestión de Tecnologías de Información debe realizar la revisión y actualización de la información publicada a través de la página web de la ARN y el espacio de transparencia, de acuerdo al Instructivo de Cumplimiento Ley 1712 de 2014 para la Transparencia y el Acceso a la Información Pública en la ARN (DE-I-04) y su Anexo No.1 Matriz de Cumplimiento, según le aplique, registrando el seguimiento en acta de revisión trimestral. Dicha acta debe reportar todas las acciones adelantadas para el tratamiento del riesgo y, en caso de materialización, debe determinar las acciones de mitigación y planes de mejora adelantados, remitiendo copia de la misma a la Oficina Asesora de Planeación para seguimiento y retroalimentación. Frente a esta acción el proceso indica que el Instructivo se encuentra actualizado de acuerdo al anexo 1 de la ley de transparencia según lo que le aplicaba a la OTI.

Riesgo 2: Incumplimiento de políticas de protección de datos personales
Clasificación del Riesgo: Estratégico
Acción No. 11: El profesional designado por parte del proceso de Gestión de Tecnologías de la información debe realizar la revisión trimestral de los inventarios de bases de datos a cargo (registradas y derivadas), el estado de autorizaciones de uso de datos personales capturadas y custodiadas, los procesos de transmisión de datos definidos y formalizados, las respuesta a PQRSD relacionadas con información personal, las sensibilizaciones realizadas en el tema, según le aplique, lo cual se consignará en acta de revisión consolidada por las dependencias y grupos territoriales involucrados en el proceso. Dicha acta debe reportar todas las acciones adelantadas para el tratamiento del riesgo y, en caso de materialización, debe determinar las acciones de mitigación y planes de mejora adelantados, remitiendo copia de la misma a la Oficina Asesora de Planeación para seguimiento y retroalimentación. Frente a este control se indica viene adelantando con las bases de datos transaccionales el proceso de ofuscación de datos y se han realizado reuniones para definir los campos y columnas que contienen datos sensibles.

4. **Proceso Atención al Ciudadano.**

Riesgo: Incumplimiento en los tiempos de respuesta de las PQRSD de acuerdo con la normatividad vigente.
Clasificación del Riesgo: Cumplimiento.
Acción No. 14: Identificar el porcentaje de incumplimiento (Numerador: cantidad de PQRSD vencidas en el periodo a reportar / Denominador: cantidad de PQRSD tramitadas y finalizadas en el

periodo a reportar) *100 Especifique razones del incumplimiento en caso de que aplique. OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN, se indica por parte del proceso que frente a los tiempos de respuesta a la fecha todos se han cumplido y se maneja una plantilla para seguimiento interno, en la cual se incluyo el campo de datos personales desde el mes de agosto.

Posterior, el auditor expone el resultado de la revisión efectuada por el Grupo de Control Interno de Gestión a la gestión de los riesgos con base en los seguimientos realizados en el Aplicativo dispuesto para este fin, resaltando los siguientes aspectos:

Resultado: Se observa el cumplimiento de las actividades propuestas para mitigar el riesgo.
Calidad de la Información: Las evidencias aportadas cumplen con los lineamientos emitidos en el Manual de Seguimiento a la Planeación y Gestión (CODIGO:DE-03).
Oportunidad: Se observa el cumplimiento en la fecha de seguimiento, sin embargo, no se registra análisis para ningún trimestre de este riesgo.

Se observa el cumplimiento por parte de la OTI en registro del seguimiento, sin embargo, la fecha de los análisis realizada por parte del grupo de Atención al Ciudadano se observa que se están realizando de manera extemporánea.

Sin embargo, se recomienda incluir en el formato la Fuente de la información como lo define el Manual de Seguimiento a la planeación y Gestión institucional (Codigo:DE-M-03) en los archivos cargados como evidencias del cumplimiento de las acciones para mitigar el riesgo y no duplicar los mismos archivos en diferentes formatos para evitar duplicidad de información.

4.4 TRASLADOS DOCUMENTALES AL NIVEL CENTRAL Y ARCHIVO DE GESTIÓN

Se realizó una verificación de la organización del archivo de gestión y aplicación de la Tabla De Retención Documental – TRD de acuerdo con lo establecido en el MANUAL DE ORGANIZACIÓN DE ARCHIVOS DE GESTIÓN, Código GD-M-03, versión 01 del 17/02/2020 y demás documentos asociados. Se aclara que por motivos de la emergencia sanitaria por cuenta del COVID-19, durante la vigencia 2020 no se realizaron traslados documentales y seguimientos por parte del Grupo de Gestión Documental.

Teniendo en cuenta que el Grupo de Gestión Documental realizó una verificación y seguimiento a los Archivos de Gestión e Implementación de la TRD el 21 de junio de 2021, se verificó el cumplimiento de los compromisos establecidos, observando lo siguiente:

- El Proceso de Gestión de tecnologías de la Información, llevó a cabo las actividades de aplicación del formato hoja de control documental, foliación y rotulado de las carpetas, identificación de las cajas o gavetas donde se almacenan los archivos en concordancia con las series documentales específicas, para los 16 expedientes revisados los cuales se encontraron conformes a los criterios definidos con un porcentaje de aprobación del 100% en los criterios definidos por el grupo de Gestión documental.

No obstante, se identifica que se acordaron los siguientes compromisos:

1. Actualizar el método de organización de los expedientes correspondientes a la subserie documental ACTAS DE CASOS DE USO DE DESARROLLO DE SISTEMA DE INFORMACIÓN, de las vigencias 2017en adelante, tanto para soportes físicos como electrónicos, con base a lo acordado en el presente seguimiento.

2. Actualización los demás instrumentos de descripción (FUID, Hoja control, Índice expediente electrónico, rotulo de carpeta, entre otros), que garanticen la adecuada administración y custodia del archivo de gestión de la unidad administrativa. Una vez actualizados los FUID, realizar envió mediante correo electrónico hacia el grupo de gestión documental.

De estos compromisos establecidos con el Grupo de Gestión Documental se identificó un avance en la organización de las carpetas, y la foliación en un 40%, generando el rótulo, y un avance del 30% de toda la documentación que se debe ajustar, por lo anterior se dejara como recomendación dentro del presente informe la culminación de los compromisos adquiridos en el seguimiento del grupo de gestión documental.

Dado que la auditoría se realizó a través de la herramienta Microsoft Teams, se informa que no se tuvo acceso de forma física al archivo de gestión y a los expedientes documentales limitando la verificación y evaluación del cumplimiento de los lineamientos en materia de gestión documental.

4.5 SEGUIMIENTO Y CUMPLIMIENTO DE PQRSD

De acuerdo con la base de datos suministrada por el Grupo de Atención Ciudadana, durante el primer semestre del 2021 el Proceso de Gestión de Tecnologías de la Información recibió y atendió 12 PQRSD registradas en SIGOB, de las cuales siete (7) se encontraban en el reporte de PQRSD remitido por atención al ciudadano y cinco (5) no se encontraban relacionadas en el reporte pero si estaban en el control de PQRSD de la OTI; no obstante se verificaron y se evidenció que fueron atendidas en los términos establecidos, los PQRSD recibidas fueron las siguientes:

OBJETO DE LA PETICIÓN	FECHA DE RADICACIÓN	FECHA DE RESOLUCIÓN	DURACIÓN DEL TRÁMITE	DURACIÓN PERMITIDA	CÓDIGO DE RADICACIÓN	CANAL DE ATENCIÓN	OBSERVACIONES
Petición de Información (E)	8/01/2021	19/01/2021	6	20	EXT21-000208	Virtual	Información entregada Oficio OFI21-000422
Petición de Información (E)	1/02/2021	3/02/2021	2	20	EXT21-001268	Virtual	Información entregada Oficio OFI21-001496
Petición de Información (E)	4/03/2021	10/03/2021	4	20	EXT21-003280	Virtual	Información entregada Oficio OFI21-005121
Petición de Información (AT)	8/03/2021	10/03/2021	2	40	EXT21-003385	Virtual	Información entregada Oficio OFI21-005120
Petición de Información (E)	11/03/2021	17/03/2021	4	20	EXT21-003731	Virtual	Información entregada Oficio OFI21-005986
Petición de Información (E)	11/03/2021	11/03/2021	1	20	EXT21-003736	Virtual	Información entregada Oficio OFI21-005296
Petición de Documentos	15/06/2021	17/06/2021	2	20	EXT21-009055	Virtual	Información entregada Oficio OFI21-013747
Petición de Información (AT)	21/01/2021	27/01/2021	4	20	EXT21 – 000676*	Virtual	Información entregada Oficio OFI21-000962
Derecho de Petición (E)	26/01/2021	8/03/2021	30	30	EXT21- 000905*	Virtual	Información entregada Dos Oficios OFI21-004847 y OFI21-004571.
Petición de Información (AT)	11/02/2021	N/A	N/A	N/A	EXT21 – 001874*	Virtual	No requiere respuesta, gestión interna con MEM21-003640
Derecho de Petición (E)	10/03/2021	21/04/2021	29	30	EXT21 – 003639*	Virtual	Información entregada Oficio OFI21-009046.
Derecho de Petición (E)	24/03/2021	26/04/2021	23	30	EXT21 – 004682*	Virtual	Información entregada Oficio OFI21-009394.

Fuente: Informe PQRSD Atención al ciudadano y Registro PQRSD 2021 -OTI

*comunicaciones que, si se identifican en SIGOB, pero no en el reporte generado por Atención al ciudadano.

Frente a la atención a PQRSD, el Proceso de Gestión de Tecnologías de la Información menciona que una vez llega la solicitud, diligencian un archivo de Excel que mantienen como control para realizar su seguimiento y cumplir con los tiempos de respuestas, adicional se realiza la validación de las respuesta remitidas y se identifica que se dieron en los términos de ley, que fue clara y en lenguaje sencillo, acorde a lo solicitado y fueron remitidas por certimail dentro de los términos establecidos.

Teniendo en cuenta lo anterior, se identifica conformidad frente al cumplimiento en los tiempos de respuesta de las PQRSD, y el seguimiento que realizan internamente debido a que no se identifica ninguna extemporaneidad asociada el Proceso de Gestión de Tecnologías de la Información.

4.6 EFICACIA Y CUMPLIMIENTO DE LOS PLANES DE MEJORAMIENTO

Una vez verificada la información del Módulo de Mejoramiento del SIG, se observó que el Proceso de Gestión de Tecnologías de la Información, con corte al 20 de septiembre de 2021, contaba con cinco (5) planes de mejora para la verificación de eficacia como son el PM-15-00026 (5 acciones), PM-19-00005 (8 acciones), PM-19-00023 (1 acción), PM-20-00001 (7 acciones) y PM-20-00014 (3 acciones).

A continuación, se presentan los resultados de la verificación y evaluación de la eficacia de los planes de mejoramiento en los cuales sus acciones fueron revisadas y cerradas como mínimo hace cuatro meses de acuerdo a lo establecido en el Procedimiento Gestión de Acciones Correctivas y de Mejora (código EM-P-01 V-5 del 15/07/2021).

Plan de Mejora PM-15-00026: Este plan de mejora está constituido por cinco (5) No Conformidades cada una con una acción, las cuales se detallan a continuación junto con los resultados de la verificación.

No Conformidad No.1. 1. De acuerdo al análisis de la base de datos de backup diarios proporcionada por Gestión Tecnológica y de la Información se evidenció que no se tiene registro diario del mes de abril incumpliendo el numeral 4.2.4 control de registros de la NTCGP1000

Acciones	**Verificación de la Eficacia**
Registro de incidente en la herramienta de mesa de ayuda con copia a la jefatura y coordinaciones de la OTI, a partir de noviembre de 2015.	Se identifica que mediante la herramienta Aranda se realiza el registro de los incidentes o solicitudes de backups por demanda en la herramienta, adicional a esto en el Manual de seguridad se encuentra definida la política en el numeral 3.12.2 Respaldo de la Información pag- 48, y adicional a esto se cuenta con dos acciones de riesgo donde se realizan los informes de los backups Programados y esta información se encuentra centralizada. Las acciones son: 1. Verificar mensualmente por parte de líder del servicio que las copias de respaldo se realicen de acuerdo con las tareas programadas, para garantizar la disponibilidad de la información centralizada. Evidencias: Informe mensual de backups. 2.Verificar mensualmente por parte de líder del servicio la restauración de las copias de respaldo, a través de la herramienta de recovery backups , para garantizar la disponibilidad e integridad de la información centralizada. Evidencia: Informes de pruebas de restauración. Frente a lo anterior, tanto en el desarrollo de la auditoría como en la validación de la documentación, por parte del Grupo de Control Interno se evidenció que no se han presentado situaciones similares a las identificadas en la No Conformidad. Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.

No Conformidad No.2 De acuerdo al análisis de la base de datos de backup mensual proporcionada por Gestión Tecnológica y de la información se evidenció que el registro del backup del mes de marzo de 2015 se realizó el día lunes 6 de abril de la presente anualidad incumpliendo el numeral 5.3.2 respaldo de la información del manual del sistema de gestión de la seguridad de la Información – SGSI, el cual enuncia lo siguiente: Backup Mensual: Corresponde a la copia mensual completa en cinta de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza el primer día hábil de cada mes

Acciones	**Verificación de la Eficacia**

Se realiza ajuste al esquema de backups en el Manual SGSI Literal _ 5.3.2 Respaldo de la información (...La copia se realiza los primeros diez (10) días hábiles de cada mes. …)	Se identifica que en el Manual de seguridad se encuentra definida la política en el numeral 3.12.2 Respaldo de la Información pag- 48, se define que: "La Oficina de Tecnologías de la Información efectúa copias de la Información contenida en los Sistemas de Información de acuerdo con el siguiente esquema: Backup Mensual: Corresponde a la copia mensual completa en cinta de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza los últimos diez (10) días hábiles de cada mes, adicional a esto se cuenta con dos acciones de riesgo donde se realizan los informes de los backups Programados y las restauraciones realizadas y esta información se encuentra centralizada. Frente a lo anterior, tanto en el desarrollo de la auditoría como en la validación de la documentación, por parte del Grupo de Control Interno se evidenció que no se han presentado situaciones similares a las identificadas en la No Conformidad. Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.

No conformidad No.3. Revisada la Política de control de accesos, numeral 5.4.1 "cuando un colaborador termina su relación laboral, sus permisos de acceso deberán ser revocados de forma inmediata" de acuerdo a la entrevista realizada al grupo coordinador de gestión Tecnológica y de la Información, se tiene establecido el procedimiento con Talento Humano, de informar en forma inmediata a gestión Tecnológica y de la Información, la novedad de personal "retiro" pero con el caso del funcionario Javier Alonso Cárdenas Díaz, se evidenció que dicho procedimiento no se está cumpliendo por parte de Talento Humano, incumpliendo el procedimiento THP05 desvinculación de personal numeral 7 que enuncia: Enviar novedades de personal a jefes Enviar correo electrónico a los responsables de las siguientes dependencias y/o grupos, informando la novedad de retiro del funcionario para hacer seguimiento a:... .Tecnología de la información: Desactivación de cuentas a Jefe de Oficina De Tecnologías de la Información y al correo soporteacr@acr.gov.co.

Acciones	**Verificación de la Eficacia**
Se implementa el envío de la solicitud a través de un correo de parte de Talento Humano con copia al Coordinador del Grupo de Infraestructura y Soporte a soporteacr@acr.gov.co, para el registro, control y seguimiento de la gestión a través de la Herramienta de la Mesa de Ayuda	Se identifica que en el documento TI-G-12 Guía Creac Gest Usuarios en los ST V1, en el numeral 6.2. INACTIVACIÓN DE CUENTAS DE USUARIO. - La Oficina de Tecnologías de la Información elabora reportes de los usuarios deshabilitados y usuarios para eliminar. Estos reportes son actualizados con la información proporcionada por Talento Humano y el Grupo de Gestión Contractual. - Guía de gestión de usuarios, adicional se implementó el control mensual de depuración de usuarios así: Realizar de forma mensual por parte del líder del servicio las actividades de verificación (depuración) de usuarios en los sistemas de información (SIGOB- SIGER-ALADINO), sistemas de información y aplicativos misionales y directorio activo con el fin de realizar el control de acceso a la información Frente a lo anterior, tanto en el desarrollo de la auditoría como en la validación de la documentación, por parte del Grupo de Control Interno se evidenció que este control fue optimizado. Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.

No Conformidad No.4. Revisada la Política de control de accesos, numeral 5.4.1: cuando un colaborador termina su relación laboral, sus permisos de acceso deberán ser revocados de forma inmediata y de acuerdo a la entrevista realizada al grupo coordinador de gestión Tecnológica y de la Información, se
evidenció el área de gestión Contractual no tiene establecido el procedimiento de informar en forma inmediata a gestión Tecnológica y de la Información, la novedad de (retiro) de los contratistas con terminación anticipada del contrato, incumpliendo el numeral 4.2.1 generalidades de la NTCGP:1000 literal c que enuncia: los procedimientos documentado.

Acciones	**Verificación de la Eficacia**
Verificar el procedimiento relacionado con la etapa post contractual (liquidación de convenios o contratos), para incluir como actividad la notificación a la Oficina de	El Proceso de Gestión de Tecnologías de la Información ha establecido estrategias para terminación de contratistas, el sistema se parametrizo y automatizo para que se inhabilite el día que termine el contrato, adicional a esto la Oficina de Tecnologías de la Información elabora reportes de los usuarios deshabilitados y usuarios para eliminar. Estos reportes son actualizados con la información proporcionada por Talento Humano y el Grupo de Gestión Contractual. - Guía de gestión de usuarios.

Tecnologías de la Información, las desvinculaciones de los contratistas por vencimiento del contrato o terminación anticipada del mismo.	Frente a lo anterior, tanto en el desarrollo de la auditoría como en la validación del Informe de inhabilitados, por parte del Grupo de Control Interno se evidenció que no se han presentado situaciones similares a las identificadas en la No Conformidad. Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.
No Conformidad No.5. Verificado el Normograma del proceso de Gestión Tecnológica y de la Información se evidenció que se encuentra desactualizado, toda vez que no contempla la nueva versión del decreto 2573 de diciembre de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones incumpliendo el numeral 4.2.3 control de documentos de la NCTGP:1000 literal b que enuncia, revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.	
Acciones	**Verificación de la Eficacia**
Se remite para publicación en el SIGER el normograma con las normas vigentes, decreto 2573 de 2014 y Decreto 1078 de 2015. Se debe verificar cada cuatrimestre y actualizar por lo menos una vez al año si se requiere. El Normograma actualizado es publicado el 27 de noviembre de 2015 en el SIGER	Se identifica que el ultimo normograma fue actualizado el 2021-04-14 y para la construcción de este se realizan validaciones en Min TIC - CsIRT y conceptos técnicos. Frente a lo anterior, tanto en el desarrollo de la auditoría como en la validación de la documentación, por parte del Grupo de Control Interno se evidenció que no se han presentado situaciones similares a las identificadas en la No Conformidad. Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.

Plan de Mejora PM-19-00005: Este plan de mejora está constituido por una (1) No Conformidad con ocho (8) acciones, como se detallan a continuación junto con los resultados de la verificación.

No Conformidad No.1. "El Proceso de Gestión de Tecnologías de la Información presenta deficiencia en la eficacia en una (1) de las acciones Plan de Mejora PM-16-00094, toda vez que las acciones: a. H14- AC1 – "Usar el software Microsoft Project para el manejo de cronogramas y complementar la información de los proyectos en la herramienta actual para seguimiento de proyectos (Team Foundation Server - TFS) – Toda vez que no se logra evidenciar, el registro de la tareas del ciclo en algunos de los desarrollos casos revisados como es el paso a pruebas o producción.	
Acciones	**Verificación de la Eficacia**
AC1. Elaborar una propuesta de modificación al proceso de Desarrollo de Software que incluya los controles e instrumentos de seguimiento y evaluación de las diferentes etapas del proceso.	Se realizado la elaboración de la Guía de desarrollo de SW- Código: TI-G-06 actualizada el 31/05/2021 en la cual se incluyen las 4 fases de desarrollo y los lineamientos para cada fase, así como el Procedimiento atención a requerimientos de sistemas de Información – código: TI-P-01 actualizado el 31/05/2021 para cada etapa de desarrollo. •Se incluyo acta de definición del caso de uso, un requerimiento puede tener varios casos de uso, se nombran los casos de uso utilizados. • Se realizan Mesas de trabajo de SIRR donde se plantean los temas y definen acuerdos.
AC2. Presentación y socialización de la propuesta a todos los colaboradores de la OTI.	Se realizo la socialización de la Guía de desarrollo de Software y el Procedimiento atención a requerimientos de sistemas de Información.
AC3. Diseño de los controles de calidad, instrumentos y mecanismos de seguimiento a las etapas del proceso.	Se realiza la validación con el Caso Q89974- Caso GAO – Se inicio con la validación del registro del caso en Aranda y desde ahí se enlazo con la herramienta Azure DevOps, donde se identifica que solo los coordinadores de seguimiento pueden solicitar los casos, se genera la tarea, que se asocia en DEVOPS, se utiliza metodología propia (Scrum - RUP), se identificaron Puntos de Control - Generar tareas de backlog y Control con el cuadro de mando de la herramientas Azure DevOps,

	adicional se realizan reuniones semanal de SCRUM y se puede validar el estado de los desarrollos
AC4. Diseño de indicadores de calidad del proceso.	Se tienen definidos los indicadores plan de acción de los desarrollos misionales y de apoyo en el PAI así: “Porcentaje de tareas de desarrollo realizadas en el periodo de Sistema de Apoyo 2021” y “Porcentaje de tareas de desarrollo realizadas en el periodo en el Sistema Misional 2021”
AC5. Implementación de controles de calidad y formatos.	Se realizan pruebas funcionales que realiza el técnico de la OTI, antes de pasar al usuario final
AC6. Mediciones de Calidad y seguimiento.	Se identifican indicadores del plan de acción y de seguimiento por porta del coordinador de desarrollo.
AC7. Evaluación de la articulación de las herramientas existentes para gestión del ciclo de desarrollo.	Se identifica la articulación de las herramientas desde Aranda se genera la tarea y se enlaza con Azure a la tarea asignada. Se diligencia el plan de pruebas de manera manual, sin embargo, se seguirá evolucionando en el uso de la herramienta para automatizar las pruebas.
AC8. Identificar oportunidades de mejora y realizar las acciones que correspondan.	Posterior a la prueba se valida la pertinencia y si se requieren mejoras en el desarrollo se propone ante las mesas del SIRR y se aprueban los ajustes o mejoras.
Frente a lo anterior, tanto en el desarrollo de la auditoría como en la validación de la documentación, por parte del Grupo de Control Interno se evidenció que no se han presentado situaciones similares a las identificadas en la No Conformidad y que fue optimizado y automatizado el proceso de desarrollo. Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.	

Plan de Mejora PM-19-00023: Este plan de mejora está constituido por una (1) Oportunidad de Mejora con una (1) acción respectivamente, la cual se detalla a continuación junto con los resultados de la verificación.

Oportunidad de Mejora No. 1. Se presentan algunos incumplimientos de acuerdo al Autodiagnóstico de MIPG realizado en el último trimestre del 2018 en donde el puntaje de las actividades es inferior al 100% y a los resultados de la medición del Formulario único Reportes de Avances de la Gestión (FURAG) de la ARN a 31-12-2018, realizado en el primer trimestre de 2019.	
Acciones	**Verificación de la Eficacia**
Analizar, definir e implementar certificaciones y constancias en línea que puede tener la Entidad.	De acuerdo a las necesidades se ha realizado el desarrollo para las personas, en la página web de la entidad en las siguientes URLs: certificaciones de retención: https://sara.reincorporacion.gov.co/es-CO/OtherServices/CertificadoIngresos Debido a que se define una acción puntual cumplida, se establece que el plan de mejoramiento fue **EFICAZ**.

Plan de Mejora PM-20-00001: Este plan de mejora está constituido por dos (2) No conformidades con cuatro (4) y tres (3) acciones respectivamente, la cual se detalla a continuación junto con los resultados de la verificación.

No Conformidad No.1. El Proceso de Gestión de Tecnologías de la Información incumple con la actualización de los documentos: ¡a) CARACTERIZACIÓN PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN; b) Matriz de Recursos Tecnológicos; y, c) PO Oficina Tecnologías de la Información que se tienen registrado en el Sistema SIGER con el fin de dar cumplimiento a la Actividad 6 “Elaborar o ajustar los documentos” del Procedimiento Control de Documentos

(Código N° GD–P–04, Versión N° 7 y de fecha el 18/03/2019). Nota: la actualización de la Caracterización del Proceso se debe validar frente al Plan de Mejora que tiene el Proceso de Direccionamiento Estratégico (PM1900023).	
Acciones	**Verificación de la Eficacia**
AC1. Solicitar a la OAP la eliminación del documento Matriz de Recursos Tecnológicos en la parte de documento complementario, por lo que es un documento de apoyo a la gestión que permanentemente se viene actualizando y presentando en el Comité Institucional de Gestión y Desempeño en la carpeta compartida COMINS.	1. Ultima actualización de la caracterización fue el 30/11/2020, no se identifica la matriz de recursos tecnológicos en la documentación del proceso, se maneja como documento interno de trabajo denominado: "Inventario sistemas de información" 2. Se realizan internamente capacitaciones continuas al personal que ingresa a la dependencia. 3. El plan operativo de la oficina de tecnología se eliminó de la documentación del proceso. 4. Se identifica que la última actualización de los documentos fue realizada en el 2021, identificando que el 89% de los documentos fueron actualizados o creados en el año 20021. 33 de los 37 existentes. Se encuentran 2 pendientes de actualización por ser temas trasversales, dos documentos externos y uno en el 2020. Frente a lo anterior, tanto en el desarrollo de la auditoría como en la validación de la documentación, por parte del Grupo de Control Interno se evidenció que no se han presentado situaciones similares a las identificadas en esta No Conformidad. Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.
AC2. Solicitar a la Oficina Asesora de Planeación capacitación en el SIGER a los funcionarios de la OTI.	
AC3. Solicitar a la OAP la eliminación del PO Oficina Tecnologías de la Información que se encuentra ubicado en la Sección del SIGER: Documento Complementario.	
AC4. Realizar monitoreo y seguimiento periódico a los documentos publicados en el SIGER relacionados con el proceso de Gestión de tecnologías de la información.	

No Conformidad No. 2: La Oficina de Tecnología de la Información se encuentra incumpliendo lo descrito en el PROCEDIMIENTO ATENCIÓN A REQUERIMIENTOS DE SISTEMAS DE INFORMACIÓN (Código N° TI–P–01, Versión N° 4 y de fecha 07–12–2017) en sus Actividades 1 “Recibir requerimiento del Sistema de Información” y Actividad 10 “Firmar acta y solicitar puesta en producción” de acuerdo a la muestra de los casos revisados durante la Auditoria.	
Acciones	**Verificación de la Eficacia**
AC1: Realizar un análisis del procedimiento actual “Atención a Requerimientos de Sistemas de Información” para identificar los ajustes que se requiere realizar sobre el mismo, incluir los roles y responsabilidades sobre cada actividad, así como, agregar puntos de control que permitan verificar la ejecución correcta del flujo completo del procedimiento.	Se identifica que el Procedimiento atención a requerimientos de sistemas de Información – código: TI-P-01 actualizado el 31/05/2021 publicados en SIG, el cual fue divulgado en los boletines de la ARN, dentro del documento se identifican los responsables de las actividades como los registros que se deben mantener en cada etapa Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.
AC2: Proyectar la versión ajustada del procedimiento Atención a Requerimientos de Sistemas de Información y gestionar su aprobación de acuerdo con el Sistema Administrador SIGER.	
AC3: Socializar los ajustes al procedimiento Atención a Requerimientos de Sistemas de Información, con los líderes funcionales de los sistemas de información, funcionarios y contratistas de la OTI y otros actores involucrados en el procedimiento.	

Plan de Mejora PM-20-00014: Este plan de mejora está constituido por cuatro (4) No conformidades de las cuales solo tres están asociadas a la OTI, y serán las cuales se validen cada una con una (1) acción respectivamente, la cual se detalla a continuación junto con los resultados de la verificación:

No Conformidad No. 1: H1: Hallazgo Transversal Auditoria Oficina Tecnologías de la Información AU-1926. La Agencia no cumple con los requisitos de la Norma ISO 27001: 2013 – SGSI abajo descritos, tal y como se evidenció en la revisión de la implementación de dicha norma en la evaluación que se realizó al Proceso de Gestión de Tecnología de la Información (resultado presentado en el informe de auditoría). Los numerales de la norma que se incumplen son los siguientes, a saber: 6.1.2 Valoración de riesgos de Seguridad de la Información; 6.1.3 Tratamiento de riesgos de Seguridad de la Información; 8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN; 8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN.	
Acciones	**Verificación de la Eficacia**
AC1: AC1: Apoyar en la actualización del Manual de Gestión de Riesgos Institucional, dando los aportes técnicos en la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información, de acuerdo con lo exigido por la norma ISO 27001:2013. Producto: Acta de reunión con los lineamientos de valorización y tratamiento de riesgos de Seguridad de la Información.	El manual de riesgo se publicó la última versión el 17/09/2021, donde se incluyen la gran mayoría de los lineamientos incluido por la OTI y se inicia la implementación del mismo. Por lo anterior, se establece que la acción fue **EFICAZ**.

No Conformidad No. 3: Hallazgo Transversal Auditoria Oficina Tecnologías de la Información AU-1926. La Agencia no cumple con los requisitos de la Norma ISO 27001: 2013 – SGSI abajo descritos, tal y como se evidenció en la revisión de la implementación de dicha norma en la evaluación que se realizó al Proceso de Gestión de Tecnología de la Información (resultado presentado en el informe de auditoría). Los numerales de la norma que se incumplen son los siguientes, a saber: 7.2 COMPETENCIA, 9.3 REVISIÓN POR LA DIRECCIÓN y 10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS de la norma NTC ISO 27001:2013.	
Acciones	**Verificación de la Eficacia**
AC1: Adelantar sesión de la Mesa de Seguridad, en la que se deben presentar las competencias con las que debe cumplir el servidor designado por el Director General para cumplir el rol de Oficial de Seguridad y definir terna de posibles servidores de la ARN aspirantes a Oficial de Seguridad que cumplen las competencias. Producto: Acta de reunión	Se identifica que la acción planteada se cumplió de acuerdo con lo definido. Por lo anterior, se establece que la acción fue **EFICAZ**. **NOTA:** a pesar que la acción a cargo de la OTI se cumplió, se observa que no se ha nombrado el oficial de seguridad que cumpla con los requisitos exigidos por la normatividad, como se manifiesta en el acta N° 008 de 2020 del Comité Institucional de Gestión y Desempeño realizado el 19 de noviembre de 2020, donde se indica que se autorizó la contratación para un Profesional grado 2.
No Conformidad No. 4: Hallazgo Transversal Auditoria Oficina Tecnologías de la Información AU-1926. La Agencia no cumple con los requisitos de la Norma ISO 27001: 2013 – SGSI abajo descritos, tal y como se evidenció en la revisión de la implementación de dicha norma en la evaluación que se realizó al Proceso de Gestión de Tecnología de la Información (resultado presentado en el informe de auditoría). Los numerales de la norma que se incumplen son los siguientes, a saber; 7.5.2 Creación y actualización. .	
Acciones	**Verificación de la Eficacia**
AC1: Seleccionar, definir y coordinar con la OAP, estableciendo la documentación que debe estar en el Software para la Administración de la planeación y la Gestión que harían parte del Sistema de Gestión Integral sobre la documentación de la OTI de Sistema de Gestión de Seguridad de la Información Producto: Documentos aprobados y publicados en SIGER	Se identifica que la última actualización de los documentos fue realizada en el 2021, identificando que el 89% de los documentos fueron actualizados o creados en el año 2021. 23 documentos generados nuevos para el SGSI para 2021. Por lo anterior, se establece que el plan de mejoramiento fue **EFICAZ**.

Teniendo en cuenta los resultados de la verificación y evaluación de la eficacia de los planes de mejoramiento en los cuales sus acciones fueron revisadas y cerradas como mínimo hace cuatro meses

se concluye que los planes de mejora asociados al Proceso de Gestión de Tecnologías de la Información se consideran eficaces.

4.7 MÉTODOS DE OPERACIÓN

Respecto a los métodos de operación y documentación del proceso se validó en el aplicativo SIG y se indagó al Líder Proceso y equipo de trabajo, respecto a lo cual señalaron la totalidad de documentos del proceso así: 1 Caracterización, 1 Normograma, 5 Formatos, 1 Manual, 19 Guías, 2 instructivos, 3 procedimientos y 5 documentos de apoyo, para un total de 37 (treinta y siete) documentos asociados al Proceso de Gestión de Tecnologías de la Información.
De otra parte, en lo referente a la actualización de los Documentos del Proceso, se indicó y se observó la matriz de actualización y elaboración de documentos del grupo alineado al proceso de actualización de documentos del Sistema Integrado de Gestión.
La validación documental se llevo a cabo a medida que se realizaba la validación de los numerales de la norma ISO 27001:2013, durante la validación se revisó la aplicación de los siguientes documentos principalmente:

• Caracterización del Proceso Gestión de Tecnologías de la Información:
El líder del proceso con su equipo de trabajo informó que se realizó la actualización de la caracterización a finales del año 2020, la validación realizada fue basada en este documento denominado: CARACTERIZACIÓN PROCESO GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN con código: TI-C-01 - V-6 de 2020-11-30, con el cual se validó que las actividades asociadas a el PHVA se encuentran alineadas a los indicadores que se reportan por parte del proceso, así como el seguimiento y monitoreo de las actividades encaminadas a la mejora continua del proceso.

• Manual del Sistema de Gestión de Seguridad de la Información

Se realizó la validación del MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN registrado en SIG con código: TI-M-01, VERSIÓN V-8 de fecha 2020-10-02,

donde se identificó dentro del manual el detalle de los numerales 4. Contexto – 5. Liderazgo y 6.2 Objetivos de Seguridad de la información de la norma ISO 27001:2013, se indaga por la actualización y alineación de definiciones, y lineamientos de etiquetado y clasificación de la información que se deben incluir en el manual, a lo que el proceso menciona que el manual se encuentra en proceso de actualización y antes de finalizar el año 2021 se publicará la versión 9.0, no obstante, se dejará como parte de las recomendaciones del presente informe que se realice una revisión integral del mismo con el fin de ajustar los temas asociados a la nueva documentación generada por el proceso .

- **Guía de Gestión de Cambios de Tecnologías de la Información**

Se realizo la validación del GUÍA DE GESTIÓN DE CAMBIOS DE TECNOLOGÍAS DE LA INFORMACIÓN registrado en SIG con código: TI-G-09, VERSIÓN V-1 de fecha 2021-06-08, donde se identifica como parte del control de los cambios tecnológicos del numeral 8.1 Planificación y Control Operacional, en este documento se identifica la solicitud por medio del formato TI-F-05 Formato RFC, el equipo de control de cambios, los tipos de cambios que se pueden presentar así como la reunión de

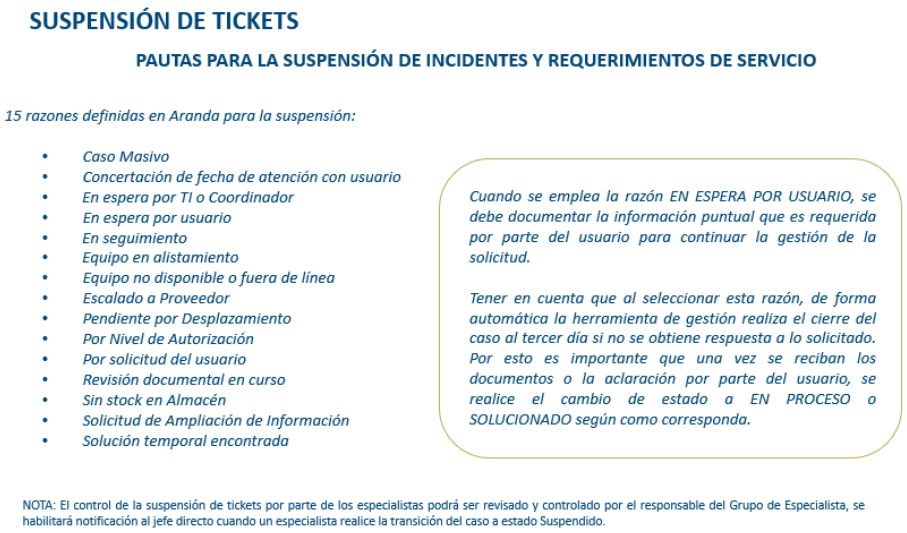
control de cambios realizada los días miércoles, lo cual queda documentando en la herramienta Aranda y se realiza un informe mensual de Control de cambios, se identifica su indicador y los roles y responsabilidades dentro del proceso de gestión de cambios.

- **Guía para la creación y gestión de usuarios en los servicios tecnológicos**

Se realizo la validación del GUÍA PARA LA CREACIÓN Y GESTIÓN DE USUARIOS EN LOS SERVICIOS TECNOLÓGICOS registrado en SIG con código: TI-G-12, VERSIÓN V-1 de fecha 2021-06-10, donde se identificaron las consideraciones y gestión para la creación, modificación o eliminación de usuarios de dominio y correo electrónico, así como las notificaciones para las novedades de personal, dentro del ejercicio de validación se revisaron los casos Q 113600 – Q113661 - QQ115080 – Q115716 – Q115767 y Q115758, casos asociados a las acciones realizadas a la novedad de vacaciones de un funcionario, donde se identificaron algunos aspectos por mejorar como la calidad en las respuestas suministradas al usuario final debido a que en el caso Q115080 se solicito un pantallazo en donde se identificaba el usuario activo y la respuesta fue: "***Solución:*** *Buen día, De manera atenta se informa que la cuenta de dominio referenciada, se encuentra activa y sin fecha de expiración debido a su vinculación como funcionaria"* y durante la validación realizada en la auditoria se remitieron nuevos soportes donde se indica que: "fue error en la interpretación de la imagen suministrada por el especialista que atendió el caso en Aranda" y que se remitía la imagen del informe del mes de agosto 2021 donde se evidencia que el usuario estaba deshabilitado sin embargo es un pantallazo de un archivo Excel no de la herramienta directamente.

Adicional, en el caso 112007, se identifica la suspensión del mismo y no se identifican los motivos de esta suspensión como lo evidencia la imagen:

y de acuerdo a la presentación suministrada donde se definen las pautas para la suspensión de incidentes y requerimientos se identifican 15 razones para realizar la suspensión y se indica que se debe documentar la acción puntual por la cual se realiza la suspensión, adicional en la nota se identifica que este puede ser revisado por el especialista y tampoco se evidencia esta revisión.



SUSPENSIÓN DE TICKETS

PAUTAS PARA LA SUSPENSIÓN DE INCIDENTES Y REQUERIMIENTOS DE SERVICIO

15 razones definidas en Aranda para la suspensión:

- *Caso Masivo*
- *Concertación de fecha de atención con usuario*
- *En espera por TI o Coordinador*
- *En espera por usuario*
- *En seguimiento*
- *Equipo en alistamiento*
- *Equipo no disponible o fuera de línea*
- *Escalado a Proveedor*
- *Pendiente por Desplazamiento*
- *Por Nivel de Autorización*
- *Por solicitud del usuario*
- *Revisión documental en curso*
- *Sin stock en Almacén*
- *Solicitud de Ampliación de Información*
- *Solución temporal encontrada*

Cuando se emplea la razón EN ESPERA POR USUARIO, se debe documentar la información puntual que es requerida por parte del usuario para continuar la gestión de la solicitud.

Tener en cuenta que al seleccionar esta razón, de forma automática la herramienta de gestión realiza el cierre del caso al tercer día si no se obtiene respuesta a lo solicitado. Por esto es importante que una vez se reciban los documentos o la aclaración por parte del usuario, se realice el cambio de estado a EN PROCESO o SOLUCIONADO según como corresponda.

NOTA: El control de la suspensión de tickets por parte de los especialistas podrá ser revisado y controlado por el responsable del Grupo de Especialista, se habilitará notificación al jefe directo cuando un especialista realice la transición del caso a estado Suspendido.

Se resalta que durante la auditoria se remitieron algunos soportes donde indican que, de los temas de documentación de los casos por parte de los especialistas, se están trabajando con el líder de calidad para mejorar estos aspectos en la herramienta Aranda (se adjunta borrador de propuesta para mejorar la calidad de la documentación). En el mismo orden, también se realiza medición en la calidad de la información de la documentación de los casos y este es el insumo para plantear todas las acciones encaminadas a la mejora.
Sin embargo, teniendo en cuenta lo identificado se considera un aspecto por fortalecer la documentación de los casos suspendidos debido a que, aunque se encuentra pautas definidas para documentarlos en los casos actualmente no se ven reflejadas.

•Procedimiento Atención a Requerimientos de Sistemas de Información

Se identifica que el Procedimiento atención a requerimientos de sistemas de Información – código: TI-P-01 actualizado el 31/05/2021 publicados en SIG, dentro del documento se identifican los responsables de las actividades como los registros que se deben mantener en cada etapa, la asignación de tareas en cada etapa del diseño y diferentes puntos de control como lo son el registro en Aranda para trazabilidad del caso y la interacción y relación del caso en la herramienta de desarrollo AzureDeVops, donde se crea el backlog con sus respectivas tareas de desarrollo, y se controla el despliegue de los cambios en producción así como las tareas de pruebas, lo cual se encuentra alineado con la guía de desarrollo de software. Para la verificación de este procedimiento y la guía de desarrollo se realiza la trazabilidad con los casos de desarrollo Q96615 y Q89974, sin embargo, se identifica como recomendación que se culmine con la implementación de las pruebas automatizadas en la herramienta AzureDeVops con el fin de optimizar el uso de la herramienta.

•Gestión De Incidentes De Seguridad

Se identifica que el Procedimiento de Gestión de Incidentes de Seguridad – código: TI-P-03 actualizado el 03/06/2021 publicados en SIG, dentro del documento se identifican las actividades, responsables y registros para la atención a los incidentes o eventos de seguridad en conjunto con la Guía para la gestión de incidentes de seguridad – código TI-G-04 del 31/05/2021, identificando las etapas para la atención de los incidentes, la clasificación y categorización de los incidentes, los roles en cada caso y la forma de realizar los reportes a entidades pertinentes según corresponda lo cual se documenta en la herramienta Aranda, para dar a conocer los eventos identificados en las herramientas del SOC se usa el documento de Reporte de eventos de Seguridad, en el cual se recomienda incluir los campos de las lecciones aprendidas y posible causa raíz con el fin de evitar posibles eventos futuros.

• Normograma del Proceso de Gestión de Tecnologías de la Información

Se realiza la validación del documento cargado en SIG como Normograma con código: TI-M-01, en su V-9, del 14 de abril de 2021, en lo referente se indicó que se realiza la actualización de manera anual y la última versión actualizada fue para la vigencia de 2021 y que constantemente se encuentran consultando Mintic y las diferentes fuentes con el fin de mantenerlo actualizado permanentemente.

4.8 SISTEMAS ADOPTADOS POR LA ARN

Se procedió a la verificación de las responsabilidades que tiene el Proceso de Gestión de Tecnologías de la Información en la implementación los Sistemas de Gestión adoptados por la Entidad, como son, el Sistema de Gestión de Calidad, el Sistema de Seguridad y Salud en el Trabajo, el Sistema de Seguridad de la Información, el Sistema de Gestión Ambiental y el Proceso Estadístico - PE1000. Esta verificación se realizó, por una parte, a través de la indagación y verificación de evidencias con la Coordinadora del Grupo y con el personal asignado para el apoyo en la implementación por cada uno de los Sistemas; y, por otra parte, a través del diligenciamiento y análisis de un formulario por parte de los funcionarios y contratistas que hacen parte del Grupo.

El formulario se realizó a través de la herramienta Forms y está constituido por 30 preguntas de conocimiento y percepción sobre los Sistemas de Gestión adoptados por la Entidad. A la fecha de la auditoria el Grupo cuenta con veintiún (21) funcionarios y once (11) contratistas de los cuales la totalidad diligenciaron el formulario. Con base en los resultados obtenidos se describen las principales fortalezas y oportunidades de mejora que debe tener en cuenta el Grupo. El detalle de los resultados para cada una de las preguntas se remite como anexo al presente informe.

A continuación, se describen los aspectos identificados por cada uno de los sistemas:

4.8.1 GESTIÓN DE CALIDAD (NTC ISO 9001:2015)

En el desarrollo de la entrevista con la líder del proceso se logró identificar que, en lo relacionado con la Norma NTC ISO 9001:2015, los miembros del Equipo de Trabajo conocen los siguientes temas:

- Se evidenció que se tiene claridad sobre los sistemas de gestión en los cuales se encuentra certificada la ARN y en cuáles se va a certificar, lo genera comprensión de la Organización y su Contexto (4.1.).
- Como Grupo apoyan los procesos de certificación de la Agencia participando de los procesos de capacitación y sensibilización brindados, trabajando en apoyo de los líderes de los sistemas, principalmente en Seguridad de la Información., cabe aclarar que es un sistema transversal que debe ser estratégico, se ha jalonado desde OTI para lograr la certificación y controlar adecuadamente los riesgos de los activos de la información y datos personales, generando conciencia y manejo adecuado de toda la información, en todos los procesos están involucrados.
- Se cuenta con los recursos para ejecutar las actividades de su proceso, dado que se evidencia que cuenta con un Talento Humano multidisciplinario, cuentan con las adecuadas instalaciones e infraestructura para poder operar. Se cuenta con el conocimiento de la ejecución de presupuesto y el Plan Anual de Adquisiciones dando, así, cumplimiento al Numeral 7.1. “Recursos”.
- Manifiestan que las personas que conforman el Grupo cuentan con la competencia e idoneidad necesario para el desarrollo de las actividades, sin embargo, se aclara que el personal no es suficiente, especialmente en los temas de desarrollo de la parte misional debido a las múltiples solicitudes diarias, así como al entorno y la normatividad cambiante, Lo anterior, da cumplimiento a lo establecido en el Numeral 7.2. “Competencia”.
- Hacen uso del Página web de la entidad y la Intranet Institucional con el fin de estar al día con la información que es comunicada adiciona a esto que se manejan unas listas de distribución de la OTI, donde se incorpora la información más relevante, y la información de los comités en los que se participan se comparte con el equipo de trabajo, de esta manera, se da cumplimiento al numeral 7.4. “Comunicaciones”.
- En el portal de la pagina Web indican que el proceso publica lo relacionado con la ley de transparencia, la política de protección de datos, sin embargo, indica que se esta realizando un ejercicio con Comunicaciones y Planeación Con el propósito de que la información publicada en la página web cuente con los mismos controles de la tabla de retención documental para los documentos físicos., al ejercicio de las TRD, sin embargo está pendiente que se revise con las áreas que tiene más injerencia sobre ley de transparencia y acceso a la información.
- La jefe de la oficina demuestra conocimiento y apropiación sobre las funciones que desempeña, resaltando las funciones de seguimiento a los temas a cargo, la interlocución con otras áreas, así como presentar propuestas a la dirección general para el uso de las tecnologías de la información de manera estratégica, asistir al director en estrategias tecnológicas representar ante MinTIC a la Agencia, promover de los servicios y buenas prácticas, en Seguridad de la Información, promoviendo mesas de Seguridad, intercambio información, verificar el mejoramiento del servicio, actividades con las cuales se da cumplimiento de esta manera, al Numeral 8.5. “Producción y Prestación del Servicio”

- Manifiestan que el proceso del cual hacen parte contribuye al cumplimiento del objeto misional a través del apalancamiento de servicios tecnológicos para cumplir la misión, con los controles de acceso, los servicios y plataforma de los servicios, garantía de equipos, brindando soporte técnico al parque computacional de la entidad, planeación con las mejoras, manifiestan que es un proceso transversal y fundamental, dando cumplimiento de esta manera, al Numeral 8.5. “Producción y Prestación del Servicio”

- Frente a la gestión del Grupo en la implementación de los Sistema de Gestión adoptados por la ARN informan que han atendido las solicitudes de información y orientaciones dadas por las dependencias líderes de cada Sistema, apoyando a verificación de mejoras en los procesos, por medio de la interacción con otras dependencias para propuestas de articulación, en la mejora de desarrollo de software, con los resultados de indicadores y acciones a tomar de manera preventiva, con lo menores tiempos de atención a los servicios, sin embargo, no se evidencia un análisis integral de los sistemas adoptados por la Entidad de manera integral y, en consecuencia, hacer este tipo de análisis se considera una oportunidad de mejora para dar cumplimiento al Numeral 9.1.1. “Generalidades”.
- Para el análisis y evaluación de riesgos de los sistemas adoptados por la entidad, indica el proceso que lo realiza con el reporte de las actividades realizadas en el mapa de riesgos institucional.
- Frente a la aplicación de algún mecanismo para evaluar la satisfacción de nuestro principal cliente, el proceso manifiesta que se realizaron las encuestas de la prestación del servicio de Seguridad de la Información, la cual se realiza a final de año y la verificación del avance frente a los resultados se valida en las mesas de seguridad con el fin de mejorar el SGSI, adicional a esto se realizan las evaluaciones de los servicios con Aranda, y las encuestas de satisfacción que aplica el proceso misional Teniendo en cuenta lo anterior se verifica el cumplimiento del Numeral 9.1.2. “Satisfacción del Cliente”.
- En relación con los controles aplicados para el cumplimiento de las actividades propias de la dependencia se resalta que realizan autocontrol en el seguimiento y verificación de las actividades que desarrollan mediante un plan de compromisos donde se va chequeando el compromiso y los soportes generados, se realizan reuniones de seguimiento para validar en que van y que está pendiente, Igualmente, realizan las evaluaciones del desempeño y las supervisiones a cargo a través de acompañamiento e informes mensuales, con controles de cumplimiento de la facturación, y mesas de trabajo con otras áreas, sin embargo aunque se generan acciones de mejora estas no son registradas en el Sistema Integrado de Gestión (SIG) lo que no permite visualizar la mejora aplicada; registrar estas acciones de mejora se considera como una oportunidad de mejora para cumplir con el Numeral 10.3. “Mejora Continua”.

En relación con los resultados obtenidos en el formulario se destacan los siguientes aspectos:

- El Grupo tiene claridad y conocimiento que la ARN presta un servicio, sin embargo, no se encontró un consenso sobre el servicio que se presta, en donde el 50% establece que el servicio es el acompañamiento de la población objeto, y, el otro 50% presentó respuestas variadas que como tal no identifican un servicio claro. Por otra parte, se evidenció que tienen claridad que pertenecen al proceso misional conforme se tiene establecido en el mapa de procesos de la ARN.
- Frente a las responsabilidades que tiene los empleados públicos y contratistas en cuanto a los Sistemas de Gestión adoptados por la ARN se evidenció respuestas variadas, motivo por el cual es importante identificar las responsabilidades y roles establecidos por cada sistema de gestión dependiendo sin son empleados públicos con personal a cargo y supervisores, o empleados públicos sin personal a cargo, o contratistas.
- El 53% del Grupo manifiesta haber participado en la identificación y gestión de los riesgos institucionales.

- El 94% del Grupo tiene conocimiento sobre la documentación que aplica a las actividades que realiza y dónde está publicada.
- Del total de encuestados el 38% identificó la línea de defensa a la que hacen parte de acuerdo con el esquema establecido por la ARN, por lo cual es importante su retroalimentación y apropiación para que la totalidad de integrantes del proceso tengan claridad frente a la línea de defensa a la cual pertenecen.
- Se observó que el 84% de los encuestados realizó la capacitación impartida por el DAFP sobre el Modelo Integrado de Planeación y Gestión.
- En relación con los conocimientos sobre el Sistema de Gestión de Calidad se observó que el 100% de los encuestados conocen su política; el 62% saben cómo están asignados los Roles y Responsabilidades; el 78% considera que se promueve la toma de conciencia; el 78% han recibido capacitaciones sobre este Sistema de Gestión; el 81% conoce que el Grupo tiene definido un enlace (delegado) para la implementación de este Sistema de Gestión.
- Sobre la percepción del grado de conocimiento de cada encuestado frente al Sistema de Gestión de calidad– SGC, de manera porcentual según las 32 personas que contestaron se observó que el 44% de los encuestados correspondiente a 14 encuestados consideran que su grado de conocimiento esta entre 0 – 6, y el 47% correspondiente a 15 encuestados, considera que su grado de conocimiento esta entre 7 – 8 y el 9% correspondiente a 3 encuestados considera que su grado de conocimiento esta entre 9 – 10.
- Por último, se observa que el valor ponderado de grado de conocimiento del SGC es de **6,1** en una escala de 0 a 10 de acuerdo a las respuestas obtenidas en esta encuesta lo que indica que no se tiene un conocimiento sólido sobre el Sistema de Gestión de Calidad de la Entidad; por lo tanto, se requiere que se tomen acciones para mejorar el conocimiento del Grupo de Trabajo acerca de este tema. Lo anterior con miras a fortalecer este aspecto al momento de la certificación de la norma NTC ISO 9001:2015.

4.8.2 Sistema de Gestión de Seguridad y Salud en el Trabajo (NTC/ISO 45001:2018)

En el desarrollo de la Auditoría se verificó el cumplimiento de las disposiciones en materia de seguridad y salud en el trabajo en el Proceso de Gestión de Tecnologías de la Información con base en lo establecido en el Manual del Sistema de Gestión de Seguridad y Salud en el Trabajo con código TH-M-02, versión 1 del 28/04/2020, documentación asociada y requisitos de la norma ISO 45001:2018, observando lo siguiente:

- La líder del proceso demuestra conocimiento y apropiación del compromiso, así como, la asignación de roles y responsabilidades con respecto al Sistema de GS-SST, lo que genera cumplimiento del numeral 5.1 Política de la SST.
- La líder del proceso demuestra conocimiento que la ARN ha identificado los peligros y la evaluación de riesgos en materia de SST, y reconoce sus principales riesgos, al respecto ha realizado la solicitud de informes del talento Humano para dar abordaje a situaciones puntuales o mejoras en sus condiciones, lo cual genera cumplimiento del numeral 6.1 Acciones para abordar riesgos y oportunidades;
- El proceso conoce que el Sistema de SST cuenta con una manual que esta publicado en SIGER en donde están asignados los roles y responsabilidades identificando la líder del Sistema.

- Demuestran conocimiento sobre los riesgos y peligros de SST asociados al Grupo. Como control para evitar la materialización de estos riesgos y peligros participan en las pausas activas.
- El Brigadista del Grupo manifiesta haber participado en procesos de formación y en simulacros de evacuación.

En relación con los resultados obtenidos en el formulario se destacan los siguientes aspectos:

- En relación con los conocimientos sobre el Sistema de Gestión de SST se observó que, del total de encuestados, el 75% conoce su política, el 65% sus roles y responsabilidades y el 85% han recibido capacitaciones sobre este Sistema de Gestión; el 87% considera que se promueve la toma de conciencia.
- Por otra parte, el 87% de los encuestados conocen que es un incidente de SST y un accidente de SST, conocen como se reporta un incidente de SST y un accidente SST; el 85% sabe cómo proceder en una situación de emergencia de SST; el 94% reporta que la ARN realizó una evaluación de su sitio de trabajo; y el 60%, reporta haber participado en ejercicios de simulacros de emergencias de SST en los últimos dos años.
- El 41% de los encuestados informa conocer que la Entidad ha establecido un proceso para la eliminación de peligros, sustitución a materiales ecológicos y/o procesos o equipos menos peligrosos.
- Sobre la percepción del grado de conocimiento de cada encuestado frente al Sistema de Gestión de SST, de manera porcentual según las 32 personas que contestaron se observó que el 34% correspondiente a 11 encuestados consideran que su grado de conocimiento esta entre 0 – 6 y el 63% correspondiente a 20 encuestados considera que su grado de conocimiento esta entre 7 – 8 y el 3% correspondiente a 1 encuestado considera que su grado de conocimiento esta entre 9 – 10.
- Por último, se observa que el valor ponderado de grado de conocimiento del SGSST es de **6,7** en una escala de 0 a 10 de acuerdo a las respuestas obtenidas en esta encuesta lo que indica que no se tiene un conocimiento sólido sobre el Sistema de Gestión de Seguridad y Salud en el Trabajo; por lo tanto, se recomienda elevar el porcentaje de participación de los empleados públicos y contratistas del proceso en las actividades de Seguridad y Salud en el Trabajo. Lo anterior con miras a fortalecer este aspecto al momento de la certificación en la norma NTC ISO 45001:2018.

4.8.3 Sistema de Gestión Ambiental (Norma NTC ISO 14001:2015)

En el desarrollo de la Auditoría se verificó el cumplimiento de las disposiciones en materia ambiental en el Proceso de Gestión de Tecnologías de la Información de acuerdo con lo establecido en el Manual de Gestión Ambiental con código GA-M-05, versión 1 del 25/09/20219; documentación asociada y requisitos de la norma ISO 14001, específicamente los numerales 5.1 Liderazgo y compromiso, 6.2.2 Planificación de acciones para lograr los objetivos ambientales, 8.1. Planificación y control operacional, observando lo siguiente:

- El Coordinador del Grupo y el Guardian Ambiental, roles dentro del SGA, demostró conocimiento sobre las responsabilidades y compromisos frente al Sistema, establecidas en el numeral 6.5 Roles y responsabilidades del Manual de Gestión Ambiental.
- Frente a la ejecución y seguimiento al Plan de Gestión Ambiental se evidenció que el Guardian Ambiental participa del plan de capacitaciones establecido, así como, retroalimenta al Grupo haciéndolos participes de las actividades que se desarrollan. Igualmente, se reporta la información necesaria sobre las personas que asisten por ocasionalmente a las instalaciones de la ARN, sobre las buenas prácticas establecidas, sobre el manejo de residuos, los controles establecidos, materias primas e insumos utilizados y demás información solicitada para la implementación del SGA.

En relación con los resultados obtenidos en el formulario se destacan los siguientes aspectos:

- En relación con los conocimientos sobre el Sistema de Gestión Ambiental se observó que del total de encuestados el 15% conoce su política; el 31% sabe cómo están asignados los Roles y Responsabilidades; el 53% considera que se promueve la toma de conciencia; el 37% ha recibido capacitaciones sobre este Sistema de Gestión; el 71% conoce que el Grupo tiene definido un enlace (delegado) para la implementación de este Sistema de Gestión.
- Por otra parte, el 43% conoce que es una contingencia ambiental; el 18% conoce como se reporta una contingencia ambiental; el 15% sabe cómo proceder en una situación de emergencia Ambienta; el 21% ha participado en ejercicios de simulacros de emergencia Ambiental en los últimos dos años.
- Sobre la percepción del grado de conocimiento de cada encuestado frente al Sistema de Gestión Ambiental, de manera porcentual según las 32 personas que contestaron se observó que el 78% correspondiente a 25 encuestados, considera que su grado de conocimiento esta entre 0 – 6 y el 22% correspondiente a 7 encuestados considera que su grado de conocimiento esta entre 7 – 8 y ningún encuestado considero que su conocimiento esta entre 9 y 10.
- Por último, Se observa que el valor ponderado de grado de conocimiento del SGA es de **4,2** sobre 10 de acuerdo a las respuestas obtenidas en esta encuesta lo que indica que no se tiene conocimiento sobre el Sistema de Gestión Ambiental; teniendo en cuenta lo anterior, es preciso elevar el porcentaje de participación de los empleados públicos y contratistas en las actividades de Gestión Ambiental. Lo anterior con miras a fortalecer estos aspectos al momento de la certificación en la Norma NTC ISO 14001:2015

4.8.4 Sistema de Seguridad de la Información (Norma NTC ISO 27001:2013)

En el desarrollo de la Auditoría se verificó el cumplimiento de las disposiciones en materia de seguridad de la información en el Proceso de Gestión de Tecnologías de la Información, de acuerdo con lo establecido en el Manual del Sistema de Gestión de Seguridad de la Información con Código TI-M-01, versión 08 del 02/10/2020, documentación asociada, y requisitos de la norma ISO 27001, observando lo siguiente:

- En la entrevista realizada con la jefe del proceso se evidenció el compromiso de apoyo y servicio que tiene el Grupo de Trabajo en lo referente al manejo seguro de la información y los protocolos de manejo de la misma, así como el conocimiento sobre las responsabilidades y compromisos frente a este Sistema de Gestión, expresan un compromiso de apoyo y servicio de manera total

en todos los temas del SGSI, lo anterior cumple con lo establecido en el Numeral 5.1.1 “Liderazgo y compromiso” de la mencionada norma.

- El proceso manifiesta que para garantizar la confidencialidad de la información cumplen con las pautas de transferencia para encriptación de datos, la verificación de procedimientos establecidos para solicitudes de permisos y control de accesos, controles de creación de las cuentas y perfiles de las cuentas.; para la disponibilidad de la información se realiza a través del cargue de la información de su proceso en SIG, las copias de respaldo, la verificación de D.A y controles de permisos; y frente a la integridad de la información toman las medidas de control establecidas en la Matriz de Activos de Información, se controla el manejo de accesos a la administración, se manejan contraseñas de administrador y usuarios privilegiados, cada plataforma maneja diferentes administradores, cada uno tiene su propia contraseña independiente todo este control en cabeza del oficial de seguridad informática, lo cual cumple con los tres pilares de la política de Seguridad de la Información.
- El proceso demuestra que tiene conocimiento sobre el proceso de notificación acerca de la eliminación de permisos de acceso a sistemas, carpetas y entrada a las sedes para las personas con novedades o que se desvinculan de la Agencia, indica que los usuarios de los empleados públicos y contratistas retirados se realiza una validación de que el correo no se encuentre activo y que en los sistemas ya se encuentran debidamente bloqueados. Lo anterior, da cumplimiento a lo establecido en el Anexo A: Control A.9.2. de la mencionada Norma.
- El proceso demuestra tener conocimiento sobre el protocolo para el manejo de los permisos a las carpetas compartidas y sobre los controles determinados para el manejo de la información confidencial, Lo anterior da cumplimiento a lo establecido en el Anexo A: Control A.9.3.
- Se demuestra conocimiento sobre los activos de información identificados y manejados en el Grupo, así como los riesgos de Seguridad de la Información asociados, el riesgo de protección de datos personales y la perdida de información.
- El responsable del proceso indica que el activo más importante para la gestión es el SIRR; adicionalmente, los aplicativos SIG y los Sistemas de Información también son usados de forma extensiva en el Grupo, así como las Carpetas Compartidas. Lo anterior da cumplimiento a lo establecido en el Anexo A: Control A.8.1.

En relación con los resultados obtenidos en el formulario se destacan los siguientes aspectos:

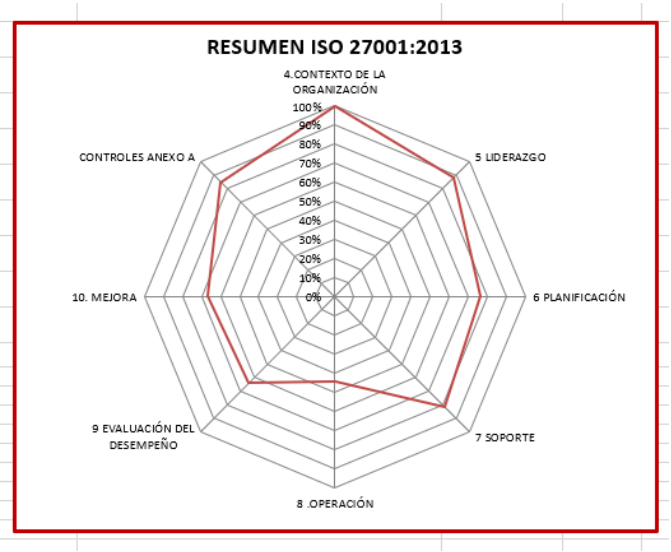
- En relación con los conocimientos sobre el Sistema de Gestión de Seguridad de la Información se observó que del total de encuestados el 75% conoce su política; el 90% sabe cómo están asignados los Roles y Responsabilidades; el 100% consideran que se promueve la toma de conciencia; el 100% han recibido capacitaciones sobre este Sistema de Gestión; el 96% conoce que el Grupo tiene definido un enlace (delegado) para la implementación de este Sistema de Gestión.
- Por otra parte, el 93% de los encuestados conoce que es un incidente y el 87% conoce que es un evento de seguridad; el 87% conoce como se reporta un incidente de seguridad y el 78% un evento de seguridad.
- El 78% de los encuestados informa que le han socializado la Declaración de Aplicabilidad del SGSI de la ARN.
- Por último, sobre la percepción del grado de conocimiento de cada encuestado frente al Sistema de Seguridad de la Información, de manera porcentual según las 32 personas que contestaron se observó que el 6% de los encuestados correspondiente a 2 encuestados consideran que su

grado de conocimiento esta entre 0 – 6 y el 50% correspondiente a 16 encuestados consideran que su grado de conocimiento esta entre 7 – 8, y el 44% correspondiente a 14 encuestados consideran que su grado de conocimiento esta entre 9 – 10.

- Por último, Se observa que el valor ponderado de grado de conocimiento del SGSI de **8,2** en una escala de 0 a 10 de acuerdo a las respuestas obtenidas en esta encuesta lo que indica que se tiene conocimiento sobre el Sistema de Gestión de Seguridad de la Información; sin embargo, es preciso elevar el porcentaje de participación de los empleados públicos y contratistas en las actividades del Sistema de Gestión de Seguridad de la Información. Lo anterior con miras a fortalecer estos aspectos al momento de la certificación en la Norma NTC ISO 27001:2013

Diagnóstico de la implementación de la Norma ISO 27001:2013

Como parte de la auditoria se realizó la validación de los soportes que apoyan el cumplimiento de los numerales de la norma ISO 27001: 2013 así como los controles del Anexo A, a los cuales se les asigno un porcentaje de acuerdo al cumplimiento si este es completo, parcial o no cumple la evidencia según lo solicitado por la norma, con el fin de determinar el porcentaje de la implementación de la norma en la ARN, resultado de la aplicación de la herramienta de autodiagnóstico se obtienen los siguientes resultados y observaciones:



NUMERALES	%
4.CONTEXTO DE LA ORGANIZACIÓN	100%
5 LIDERAZGO	89%
6 PLANIFICACIÓN	76%
7 SOPORTE	82%
8 .OPERACIÓN	44%
9 EVALUACIÓN DEL DESEMPEÑO	64%
10. MEJORA	67%
CONTROLES ANEXO A	85%
TOTAL GENERAL	76%

Como resultado del diagnóstico se identifica un porcentaje de implementación del **76%** sobre el 100% que se debería lograr, identificando en cada uno de los numerales los siguientes aspectos por fortalecer:

4. Contexto de la organización: Se identifica cumplimiento del **100%** de los numerales correspondientes al contexto desde el 4.1 al 4.4, debido a que cuenta con los documentos que soportan lo requerido en estos numerales, para el cumplimiento se relacionan los documentos Marco Estratégico y Plan Estratégico 2019-2022 v4, Manual del Sistema de Gestión de Seguridad de la Información con Código TI-M-01, versión 08 del 02/10/2020, y el documento Borrador Plan de seguridad y privacidad v4, con respecto al Plan de seguridad y Privacidad que aún se encuentra en borrador se identifica un aspecto por mejorar con respecto al cronograma que se tiene definido frente al tema de Plan de Continuidad del Negocio, se encuentra pendiente definir las fechas programadas de estas actividades para la vigencia 2021 y 2022, y por ende este tema se encuentra atrasada su definición e implementación.

5. Liderazgo: Se identifica un cumplimiento del **89%** debido a que en el numeral *5.1.1 Liderazgo y compromiso para el sistema de gestión de la seguridad de la información literal e) asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos*; y para el cumplimiento de este ítem no se han asegurado el cumplimiento de los resultados del sistema ya que se encuentra pendiente realizar la revisión por la dirección donde se determinan los resultados obtenidos del SGSI, como soportes para el cumplimiento del numeral se identifican las actas de reunión del comité de Gestión y desempeño y la mesa de Seguridad.

6.Planificación: Se identifica un cumplimiento del **76%** debido a que en la validación de las evidencias se identifica para los numerales 6.1.2 Valoración de riesgos de la seguridad de la información y 6.1.3 Tratamiento de riesgos de la seguridad de la información el cumplimiento parcial, debido a que el nuevo manual fue publicado en el mes de septiembre y la implementación se encuentra pendiente, adicional a esto la identificación de riesgos de seguridad de la información en todos los procesos hasta ahora se está iniciando y está muy prematura su implementación, lo cual genera un aspecto por mejorar.
Así mismo, la Oficina de Tecnologías de la Información ha definido el documento Despliegue de la política del Sistema de Gestión de Seguridad de la Información con el propósito de identificar en una solo vista la relación de la política con los objetivos del SGSI y los mecanismos de medición.

7.Soporte: Se identifico un cumplimiento del **82%** debido a que se identifica cumplimientos parciales en los siguiente numerales 7.2 Competencia, toda vez que a la fecha no se logra evidenciar, que por parte de la Alta dirección se realice la asignación del oficial de Seguridad de la Información acorde a las competencias definidas, y por parte de talento humano no se remitió el documento o acto administrativo con el cual se establecen las responsabilidades a la persona asignada como Oficial de Seguridad de la Información para la ARN, con el fin de poder validar los demás mencionar literales de este numeral, lo cual genera un NC en el presente informe. Adicional a esto en el numeral 7.3 Toma de Conciencia se recomienda realizar una evaluación de las capacitaciones con el fin validar la apropiación de los temas impartidos, y para mejorar el porcentaje de participación en las capacitaciones es importante que Talento Humano y el Grupo de Gestión Contractual analicen la viabilidad de incluir parámetros en la evaluación de desempeño para empleados públicos y en las obligaciones contractuales para contratistas.

8.Operacion: Se identifico un cumplimiento de **44%** debido a que un cumplimiento parcial para el numeral *8.1 Planificación y Control Operacional con respecto a que la organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario*. Dado que la Oficina de Tecnologías de la Información ha establecido las pautas para el tratamiento y control de cambios de tecnologías de la información, las cuales se encuentran descritas en el documento TI-G-09- Guía de gestión de cambios de tecnologías de la información dispuesto en SIG. Sin embargo, en este ítem se identifica que está pendiente la definición de las disposiciones para la gestión del cambio institucional por parte de Planeación o el área encargada, adicional a esto en los numerales 8.2 valoración de riesgos de la seguridad de la información y 8.3 tratamiento de riesgos de la seguridad de la información se encuentran con cumplimiento parcial debido a que el nuevo manual fue publicado en el mes de septiembre y la implementación se encuentra pendiente, adicional a esto la identificación de riesgos de seguridad de la información en todos los procesos hasta ahora se está iniciando.

9.Evaluacion del desempeño: Se identifico un cumplimiento de **64%** debido a que se identifica un cumplimiento parcial para el numeral 9.1 *Seguimiento, Medición, Análisis y Evaluación en lo que respecta al literal b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos; Nota: para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles*, actualmente los métodos identificados son el indicador de nivel de avance de implementación del Plan de seguridad y privacidad y los criterios de medición del MSPI, los cuales aunque generan mediciones se pueden fortalecer alineándolos a los objetivos del SGSI para que sean comparables y generen beneficios al sistema. Adicional es esto se identifica un incumplimiento del numeral 9.3 Revisión por la Dirección, ya que a la fecha se encuentra pendiente realizar la revisión por la dirección donde se determinan los resultados obtenidos del SGSI, lo cual genera No Conformidad en este numeral.

10.Mejora: Se identifico un cumplimiento de **67%** debido a que se identifica un incumplimiento en el numeral *10.2 Mejora Continua- La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.* Ya que a la fecha no se cuenta con los insumos para definir esa conveniencia, adecuación y eficacia del sistema.

Anexo A: Se identifico un cumplimiento de **85%** en la implementación de los controles del anexo A debido a que se tiene un grado de implementación parcial en los siguientes 25 controles del anexo:

CONTROLES ANEXO A ISO 27001:2013			
Control	**Descripcion**	**QUÉ TIENE?**	**QUE NOS FALTA**
A6.1.5	Seguridad de la información en la gestión de proyectos.	*Manual de Gestión de proyectos *Seguimiento a la gestión de proyectos -2021	Pendiente lo de SI solo esta de manera general, hay que revisar con planeacion, solo se tiene lo de OTI.
A6.2.2	Teletrabajo	*Manual del Sistema de Gestión de Seguridad de la Información *Manual de Teletrabajo https://klein.reincorporacion.gov.co/FSSIGER/DOCS/2020/10/84/A47DBB28-9F97-42ED-857F-329C5F73F646.pdf	Pendiente actualizacion de Talento Humano del Manual de Teletrajo y generando las disposiciones de Trabajo en casa teniendo en cuenta la nueva normativa
A8.2.2	Etiquetado de la información	*Guia de Etiquetado de la Informacion	Documento en codificacion, pendiente implementacion de los Lineamientos de etiquetado.
A8.3.2	Disposición de los medios	*GUÍA PARA LA GESTIÓN DE EQUIPOS DE USUARIO FINAL https://klein.reincorporacion.gov.co/FSSIGER/DOCS/2021/5/	Recomendación incluir el tema de borrado seguro cuando se dejen de usar los equipos.
A8.3.3	Transferencia de medios físicos	*Instructivo de embalaje de paquetería y encomiendas *Guía para la gestión de equipos de usuario final https://klein.reincorporacion.gov.co/FSSIGER/DOCS/2020/12	Pendiente validar la encripcion de medios extraibles.
A10.1.1	Política sobre el uso de controles criptográficos	*Manual del sistema de gestión de seguridad de la información *Acta CIGD de la revisión del manual del SGSI *Guía de intercambio de información *Reporte de Bitlocker *Guía para la gestión de equipos de usuario final	Pendiente en la documentacion incluir el tema del manejo de las llaves.
A10.1.2	Gestión de llaves	*Custodia de llaves criptográficas http://otidocs.acr.int/sites/OTI/Soporte%20de%20Instrumentos/2021/Soportes%20Seguridad%20Digital/MSPI-	Pendiente Armonizar documentalmente los lineamientos para las llaves criptográficas, responsable de la evidencia dependencias usuarias
A11.1.6	Áreas de despacho y carga	*Manual de Seguridad Preventiva *Procedimiento entrada y salida de bienes *Contrato de prestación de servicios de nube privada (Centro de datos) *Políticas de Ingreso y Permanencia Datacenter CenturyLink nuevo *Registro de ingreso al Datacenter *Contrato de prestación de servicios de vigilancia y seguridad privada	Pendiente fortalecer la implementacion de los controles en estas areas.
A12.1.2	Gestión de cambios	*Guía de gestión de cambios de tecnologías de la información *Informe mensual de la gestión de cambios de TI	Pendiente incluir lo relacionado con los lineamientos para el Cambio institucional.
A12.1.3	Gestión de capacidad		Pendiente revisar la documentacion con Gestor de Capacidad, para incluir en lo que se tiene en este control.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Guia desarrollo de software https://klein.reincorporacion.gov.co/FSSIGER/DOCS/2021/5/	Pendiente asegurar la implementacion de los tres ambientes.
A13.2.1	Políticas y procedimientos de transferencia de información	*TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información *Guía Intercambio de información *Instructivo_cifrado_documentos_7zip *Instructivo_cifrado_documentos_PGP	Pendiente validar la implementación del cifrado en todos los equipos de la agencia.
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	*Logs de transacciones SIR, SARA, ARPA (verificar en el sistema de información) *Contrato de certificado digitales 1778 de 2020 GESTION_TI\Gestion Oficina TI\CONTRATOS\CONTRATOS 2020\1778-20_CertifDigitales	Pendiente validar el monitoreo y resultado de la revisoin de logs
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	*Procedimiento interno de desarrollo *Guía Operacional de Gestión de Cambios http://otidocs.acr.int/sites/OTI/Soporte%20de%20Instrume	Pendiente lo relacionado con los planes de continuidad del negocio. (Gestión Administrativa)
A.14.2.8	Pruebas de seguridad de sistemas	*Tarea de pruebas Azure DevOps (test de pruebas) *Pruebas de control de acceso- roles	Pendiente validar los resultados de las pruebas de seguridad realizadas.

A.14.2.9	Prueba de aceptación de sistemas	*Tarea de pruebas Azure DevOps (test de pruebas) *Pruebas unitarias *Pruebas de funcionalidad según caso de uso	Pendiente validar los resultados de las pruebas de seguridad realizadas.
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	*Manual del Sistema de gestión de seguridad de la información-3.18 POLÍTICA DE RELACIÓN CON PROVEEDORES pag.56 *Manual de contratación y supervisión e interventoría	Pendiente la alineacion de la politica de proveedores con los controles realizados por los supervisores de los contratos.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Manual del Sistema de gestión de seguridad de la información-3.18 POLÍTICA DE RELACIÓN CON PROVEEDORES pag.56 *Manual de contratación y supervisión e interventoría	Pendiente la alineacion de la politica de proveedores con los controles realizados por los supervisores de los contratos.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	*Manual del Sistema de gestión de seguridad de la información-3.18 POLÍTICA DE RELACIÓN CON PROVEEDORES pag.56 *Manual de contratación y supervisión e interventoría *Manual para la Identificación y Cobertura del Riesgo en los	Pendiente la alineacion de la politica de proveedores con los controles realizados por los supervisores de los contratos.
A15.2.2	Gestión del cambio en los servicios de los proveedores	*Manual del Sistema de gestión de seguridad de la información-3.18 POLÍTICA DE RELACIÓN CON PROVEEDORES pag.56 *Manual de contratación y supervisión e interventoría *Manual para la Identificación y Cobertura del Riesgo en los	Pendiente la alineacion de la politica de proveedores con los controles realizados por los supervisores de los contratos.
A16.1.2	Reporte de eventos de seguridad de la información	*GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD *Procedimiento gestión de incidentes de seguridad *GUÍA DE GESTIÓN DE EVENTOS DE TECNOLOGÍAS DE LA	Pendiente la articulación con la gestión ITIL de mejora.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	*GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD *Procedimiento gestión de incidentes de seguridad https://klein.reincorporacion.gov.co/FSSIGER//DOCS/2021/5	Pendiente la articulación con la gestión ITIL de mejora.
A17.1.1	Planificación de la continuidad de la seguridad de la información	*Plan de continuidad de negocio *Lista de chequeo para contingencia de servicios de TI \PLAN_CONTINUIDAD_NEGOCIO	Pendiente documento de continuidad del negocio
A17.1.2	Implementación de la continuidad de la seguridad de la información	*Plan de continuidad de negocio *Lista de chequeo para contingencia de servicios de TI \PLAN_CONTINUIDAD_NEGOCIO	Pendiente Evidencia de la implementación del Plan de continuidad del negocio
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Plan de continuidad de negocio *Lista de chequeo para contingencia de servicios de TI \PLAN_CONTINUIDAD_NEGOCIO	Pendiente Evidencia de la implementación del Plan de continuidad del negocio y ejercicios de simulacion.

Teniendo en cuenta lo identificado para dar cumplimiento a los numerales de la norma y los controles de anexo A se evidencia un aspecto por fortalecer encaminado a completar y mejorar la información documentada que soportan el cumplimiento e implementación de los controles mencionados y que aplican a SGSI de la Agencia para cumplir con la implementación de los numerales de la norma y del Anexo A de la Norma ISO 27001:2013.

4.8.5 Norma Técnica de la Calidad del Proceso Estadístico (NTC PE 1000:2017)

La jefe del proceso entrevistada en el ejercicio de la presente Auditoría indica que se encuentra muy familiarizado con el tema de las Operaciones Estadísticas; porque hacen parte de la auditoria y apoyo en los reportes.

Después de consultar y verificar, no se cuenta con evidencia sobre sensibilizaciones en esta materia. Por lo anterior, se recomienda solicitar capacitaciones respecto del Proceso Estadístico para, así, dar cumplimiento al Numeral 7.1.2. “Sensibilización” de la mencionada Norma.
En el desarrollo de la Auditoría a través del cuestionario se indagó sobre la Norma Técnica de la Calidad del Proceso Estadístico (NTC PE 1000), observando que el 38% tiene conocimiento que la ARN tiene dos operaciones estadísticas certificadas; el 3% conoce su política; el 6% conoce como están asignados los roles y responsabilidades; el 12% considera que se promueve la toma de conciencia; el 3% ha recibido capacitaciones; el 25% conoce que el Grupo tiene definido un enlace (delegado) para la implementación de este norma y el 28% conoce en que consiste la Operación Estadística de la Entidad.

- Sobre la percepción del grado de conocimiento de cada encuestado frente al proceso estadístico de la ARN, de manera porcentual según las 32 personas que contestaron se observó que el 88% correspondiente a 28 encuestados considera que su grado de conocimiento esta entre 0 – 6 y el 9% correspondiente a 3 encuestados considera que su grado de conocimiento esta entre 7 – 8 y el 3% correspondiente a 1 encuestado considera que su grado de conocimiento esta entre 9 – 10.
- Por último, se observa que el valor ponderado de grado de conocimiento del Proceso Estadístico en la ARN es de **2,8** en una escala de 0 a 10 de acuerdo a las respuestas obtenidas en esta encuesta lo que indica que no se tiene conocimiento sobre el Proceso estadístico; teniendo en cuenta lo anterior, es preciso elevar el porcentaje de participación de los empleados públicos y contratistas en las capacitaciones sobre el proceso estadístico y de esta manera, aportar al mantenimiento de la certificación de la Norma NTC PE 1000:2017.

5. CONCLUSIÓN GENERAL

La Auditoría al Proceso de Gestión de Tecnologías de la Información se ejecutó de acuerdo con lo previsto en el Plan de Auditoria y cumplió con el objetivo y alcance previsto gracias a la disposición de los profesionales que conforman el Proceso. Adicionalmente, este ejercicio de auditoría se realizó bajo un enfoque basado en riesgos y oportunidades.
Finalmente, y resultado de la auditoria adelantada se observó que la gestión adelantada por el Proceso se realiza de manera razonable dentro del marco regulatorio aplicable y vigente; adicionalmente, aplica los procedimientos que se han establecido en lo referente a sus políticas de operación y, también, aplica controles y seguimiento a las actividades que se desarrollan para dar cumplimiento al objetivo misional de la Agencia.

5.1 Conformidades - Fortalezas.

- El desarrollo y gestión con respecto a los temas de competencia del Proceso de Gestión de Tecnologías de la Información, es una labor a resaltar por el compromiso y diligencia que se tienen, al acometer estos asuntos.
- La organización documental y administración del archivo físico y digital de acuerdo a los lineamientos de la Entidad dado que obtuvieron una excelente valoración.

- La disposición en la atención de los requerimientos en el ejercicio auditor por parte del líder del proceso y el equipo de trabajo.
- Se destaca la relevancia que tienen los empleados públicos y contratistas en el proceso y el abordaje a personas con algún tipo de afectación, así como el apoyo por parte del líder.
- Se identifica que como parte del autocontrol del proceso de Tecnología se maneja un tablero de control, el plan de compromisos y reuniones de seguimiento periódicas, las cuales fortalecen el proceso.
- Se destaca el seguimiento que se realiza a la parte contractual y las reuniones de seguimiento con los proveedores frente a la supervisión de los contratos a cargo del proceso de Tecnologías de la información.

5.2 No Conformidades

5.2.1 No conformidades Transversales

- **NC1 : Direccionamiento Estratégico:** Contratación del oficial de seguridad: se evidencia que la Agencia no ha contratado una persona que tenga las competencias para realizar las obligaciones que tiene que desempeñar el Oficial de seguridad para el sistema de Gestión de Seguridad de la información; tal como se verificó en la revisión del Plan de Mejora PM-20-00001 Hallazgo 3, que a pesar de ejecutar las acciones no se cumplió con el objetivo final de tener la persona competente, generando un incumplimiento del numeral 7.2 competencia de la norma 27001:2013, lo cual materializa el riesgo de la no obtención de la certificación ISO 27001:2013 por incumplimiento de las competencias del oficial de Seguridad de acuerdo con los requisitos definidos.
  Nota: En reunión con la Alta Dirección se determinó el compromiso de contratar al Oficial de Seguridad acorde a las competencias necesarias para desempeñar el cargo para el mes de enero de 2022 y revisión de la planta de personal de la agencia para incorporar este cargo.

- **NC2: Atención al ciudadano:** Los reportes de PQRSD del primer y segundo trimestre, generados por el Sistema de Información SIGOB y analizados por el Grupo de Atención al Ciudadano, no contienen la totalidad de PQRSD recibidas y gestionadas durante el primer semestre de 2021, dado que en la revisión de PQRSD del proceso de Gestión de Tecnologías de la Información, se dejaron de reportar tres (3) PQRSD, afectando la integridad de la información reportada y analizada para realizar el seguimiento y evaluación del Sistema de PQRSD en la ARN, lo cual genera un incumplimiento en el Manual de Seguridad de la Información con respecto al objetivo del SGSI de : "*Proteger la información de la gestión de la Agencia para la Reincorporación y la Normalización y la tecnología utilizada para su procesamiento, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información*". y materialización del riesgo de entrega de información imprecisa para la toma de decisiones.

5.3 Aspectos por Fortalecer

5.3.1 Proceso de Gestión de Tecnologías de la Información

A continuación, se presentan los siguientes aspectos que podrían ocasionar No conformidades; no cumplimientos en el PAI, no cumplimiento o ineficacia en los Planes de Mejora y/o materialización de riesgos:

- Dentro de la validación de los controles definidos para el establecimiento e implementación de los requisitos de seguridad de la información pertinentes con los proveedores, se identificó que se cuenta con el seguimiento por parte de los supervisores de los contratos, no obstante, es importante mejorar las evidencias que soportan el cumplimiento de acuerdo a lo definido en la numeral 3.18 Política de Relación Con Proveedores del Manual de Seguridad de la Información CÓDIGO: TI-M-01.

- Para el indicador “Nivel de ajuste y avance en la implementación del Plan de preservación digital 2021” es importante para soportar el porcentaje en la implementación de este plan que se identifiquen los temas planeados y los que se han ejecutado a la fecha, con el fin de tener claridad en la medición del indicador y el avance de la implementación.

- Se considera un aspecto por fortalecer la documentación de los casos suspendidos debido a que, aunque se encuentra pautas definidas para documentarlos en los casos actualmente no se ven reflejadas, así como la calidad en las respuestas remitidas al usuario final de acuerdo a lo casos evidenciados.

- Se identifica que actualmente los métodos de medición usados son el indicador de nivel de avance de implementación del Plan de seguridad y privacidad y los criterios de medición del MSPI, los cuales, aunque generan mediciones se pueden fortalecer incluyendo los objetivos del SGSI y sus indicadores para que sean comparables, medibles y generen beneficios al sistema.

- Completar y mejorar la información documentada que soportan el cumplimiento e implementación de los controles mencionados y que aplican a SGSI de la Agencia para cumplir con la implementación del Anexo A de la Norma ISO 27001:2013.

- Aunque se generan acciones de mejora frente al proceso, estas no son registradas en el SIG lo que, en consecuencia, no permite visualizar la mejora continúa aplicada; teniendo en cuenta lo anterior, es importante registrar las oportunidades de mejora que se presentan en el Grupo en el Módulo de Mejora del mencionado Sistema. De esta manera se dará cumplimiento al numeral 10.3. “Mejora Continua” de la Norma ISO 9001:2015.

- Aunque constantemente se hace seguimiento a la gestión que se realiza en el Proceso, esta no queda soportada, es importante dejar el registro incluyendo el análisis integral de los sistemas adoptados por la Entidad; de esta manera se dará cumplimiento al Numeral 9.1.1. “Generalidades” de la Norma ISO 9001:2015.

5.3.2 Transversales

- Se identificó que la alta dirección aún no ha realizado la revisión por la dirección del sistema de gestión de seguridad de la información como lo indica el numeral 9.3. de la norma 27001:2013 y según lo observado en el proceso de auditoría, se pudo constatar en la revisión y evaluación de la eficacia del plan de mejora PM-20-00014, donde no de formularon acciones, que aun no se ha

efectuado, por tal motivo se requiere que esta sea desarrollada con el fin de poder cumplir con este requisito.

- Se identifica en la validación del documento “Borrador Plan de Seguridad y Privacidad de la Información” que se encuentran pendientes por definir las fechas en las cuales se cumplirán las actividades relacionadas con la implementación de plan de continuidad que se encuentra en cabeza de la **Subdirección Administrativa**, adicional a esto se identifica un cumplimiento parcial a los controles del anexo A con respecto a los temas de continuidad del negocio por la falta de documentación e implementación del plan de continuidad en la ARN.

- Para el numeral 7.3 Toma de Conciencia de la norma ISO 27001:2013 y demás capacitaciones, se considera un ítem importante a tratar con **Talento Humano**, realizar una evaluación de las capacitaciones con el fin validar la apropiación de los temas impartidos debido a que actualmente solo se evalúan los temas logísticos principalmente, adicional a esto es importante mejorar el porcentaje de participación en las capacitaciones definiendo una estrategia para que se participe en las capacitaciones y esto se pueda evaluar dentro de las obligaciones de los contratos y evaluaciones de desempeño si es posible.

- Fortalecer los procesos de capacitación y sensibilización por parte de **la Oficina Asesora de Planeación, Talento Humano, Subdirección de seguimiento, Subdirección administrativa y la Oficina de Tecnologías de la Información** frente a los sistemas de gestión adoptados por la Entidad y el MIPG con el fin, primordial de apropiar el conocimiento por parte de los miembros del Grupo, toda vez que los resultados obtenidos en la encuesta realizada indican que el grado de conocimiento frente a estos sistemas es bajo.

- Para la definición de riesgos transversales como por ejemplo los riesgos de **Tecnologías de la Información, Talento Humano y Direccionamiento Estratégico,** se identifica la necesidad de incluir a los líderes de los procesos en la definición de los mismos desde el inicio; debido a que al revisar el seguimiento de los riesgos transversales que se están gestionando en la agencia, se identificó que lo reportado se limita a lo que el responsable del riesgos transversal definió como control y no se describen controles propios asociados a la necesidad identificada en cada proceso.

- Frente a los numerales 8.2 valoración de riesgos de la seguridad de la información y 8.3 tratamiento de riesgos de la seguridad de la norma ISO 27001:2013, está pendiente la definición de las disposiciones para la gestión del cambio institucional por parte de **Planeación o el área encargada**, adicional a esto la identificación de riesgos de seguridad de la información en todos los procesos hasta ahora se está iniciando y está muy prematura la implementación, debido a que el nuevo manual fue publicado en el mes de septiembre y la implementación se encuentra en proceso, adicional a esto para el riesgo de Pérdida de Información es importante fortalecer el control, y revisar que el control realmente mitigue el riesgo asociándolo a los activos de información propios de cada dependencia, dado que cada uno maneja una particularidad diferente.

- Frente al numeral 9.3 Revisión por la Dirección de la norma 27001:2013, es importante mejorar y preparar los insumos para realizar la revisión por la dirección, así como la gestión para que esta se realice, teniendo en cuenta que se deben documentar los aspectos como: los cambios en cuestiones

internas y externas, la retroalimentación sobre el desempeño de la seguridad de la información, la retroalimentación de las partes interesadas, y las oportunidades de mejora.

5.4 Recomendaciones

- Se recomienda para el indicador “Nivel de cumplimiento del Plan de Seguridad y Privacidad de la Información 2021” ampliar la información de seguimiento al cumplimiento del indicador mencionando en el registro trimestral el detalle de las actividades planeadas y las actividades ejecutadas efectivamente, las cuales tengas fechas definidas.

- Se recomienda al momento de almacenar las evidencias que soportan el cumplimiento de los indicadores o las acciones de los riesgos no duplicar los archivos que soportan el indicador debido a que se encuentran en formato Word, Excel y pdf siendo el mismo archivo, para evitar duplicidad de información en el repositorio.

- Se recomienda incluir en los formatos y archivos cargados como evidencias del cumplimiento de las acciones para mitigar el riesgo o evaluar los indicadores, la fuente de la información como lo define el Manual de Seguimiento a la planeación y Gestión institucional (Codigo:DE-M-03).

- Se recomienda culminar de los compromisos adquiridos en el seguimiento del grupo de gestión documental con respecto a la organización de las carpetas, la foliación, el rótulo, de toda la documentación que se debe ajustar.

- Se recomienda que se realice una revisión integral del Manual de Seguridad de la Información con el fin de ajustar los temas asociados a la nueva documentación generada por el proceso, así como la actualización y alineación de definiciones, y lineamientos de etiquetado y clasificación de la información que se deben incluir en este manual.

- Se recomienda incluir en el documento de Reporte de eventos de Seguridad (usado para dar a conocer los eventos identificados con las herramientas del SOC), los campos de lecciones aprendidas y posible causa raíz con el fin de evitar posibles eventos futuros.

- Se recomienda tener en cuenta para el indicador “Nivel de ajuste y avance en la implementación del Plan de preservación digital 2021” los tiempos para la implementación del documento, toda vez que la implementación no ha iniciado, debido a que el documento no está culminado aún, y el año anterior se incumplió el indicador ya que el documento no se finalizó.

Elaborado por: Sandra Paola Estupiñán García – Auditora Líder
Derly Katherine Cubides Jaime – Equipo Auditor
Revisado y Aprobado: Eduardo Antonio Sanguinetti Romero – Asesor del Grupo de Control Interno de Gestión
Fecha de elaboración: septiembre 30 de 2021