INFORME DE AUDITORÍA

1. INFORMACIÓN BÁSICA DE LA AUDITORÍA

CÓDIGO AUDITORÍA:	AUD-1926	**TIPO DE AUDITORÍA:**	AUDITORÍA INTEGRAL
FECHA DE INFORME:	Diciembre 11 de 2019	**PROCESO / DEPENDENCIA AUDITADA:**	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
FECHA DE AUDITORÍA:	**Noviembre 19 al 28 de 2019** Sitio: Piso 5 Sede Central (Edificio "San Juan de Dios")	**AUDITORES:**	Auditor Líder: Ana Yancy Urbano Velasco Equipo Auditor: Eduardo Antonio Sanguinetti Romero / Jairo Tulande Collazos / Enrique Fernández Monsalve.

2. OBJETIVO DE LA AUDITORÍA

Evaluar la gestión integral del Proceso Gestión de Tecnologías de la Información en cumplimiento de los requisitos del – Modelo Integrado de Planeación y Gestión – MIPG (Decreto 1499 de 2017), atributos de calidad (ISO 9001:2008), y normatividad vigente aplicable al Proceso.

3. ALCANCE DE LA AUDITORÍA

La evaluación se realizará a la gestión adelantada por el Proceso de Gestión de Tecnologías de la Información del 01/09/2018 al 30/09/2019.

Nota aclaratoria: no se incluirá la verificación de la eficacia del Plan de Mejoramiento N° PM-19-00005 (AUD-1819), debido que este se encuentra aún en curso.

4. CRITERIOS DE LA AUDITORÍA

Se tendrán como criterios a tener en cuenta los siguientes:

- Ley 594 de 2000 "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".
- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública".
- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- Decreto Ley 897 de 2017 "Por el cual se modifica la estructura de la Agencia Colombiana para la Reintegración de Personas y Grupos Alzados en Armas y se dictan otras disposiciones".
- Decreto 4138 de 2011 "Por el cual se crea la Agencia Colombiana para la Reintegración de Personas y Grupos Alzados en Armas y se establecen sus objetivos y estructura".
- Decreto 1499 de 2017 (MIPG).
- Norma Técnica Colombiana NTC–ISO9001: 2008 (Sistemas de Gestión de la Calidad).

- Norma Técnica Colombiana NTIC – ISO27001:2015 (Tecnologías de la Información; Técnicas de Seguridad; Sistema de Gestión de la Seguridad de la Información).
- Caracterización y demás documentos inscritos en el Sistema Integrado de Gestión para la Reintegración – SIGER (procedimientos, instructivos, manuales y formatos).
- Normatividad del Proceso (leyes, decretos, resoluciones y acuerdos y demás normatividad que le aplique al proceso) y Planes de Mejoramiento del Proceso.

5. DESARROLLO DE LA AUDITORÍA

La Auditoría Integral al Proceso de Gestión de Tecnologías de la Información se ejecutó conforme a los procedimientos de auditoría previamente definidos en el Diseño de Pruebas y en el Plan de Auditoría. En el desarrollo de la misma se adelantaron los siguientes procedimientos:

- Cumplimiento del Protocolo de Solicitud de Información pactado con el auditado (efectuado entre el 21 de octubre y el 22 de noviembre de 2019).
- Reunión de Apertura de la Auditoría realizada el día 15 de noviembre de 2019.
- Charla de Autocontrol y Prevención de la Corrupción impartida por el Asesor de Control Interno de Gestión el día 20 de noviembre de 2019.
- Revisión *In Situ* de los temas y aclaraciones respecto de los aspectos evidenciados en las muestras de auditoría (12,13,14 y 18 de noviembre de 2019).
- Reunión de Cierre de la Auditoría realizada el día 2 de diciembre de 2019.

En este punto es importante resaltar que, debido a las limitaciones de cualquier estructura de control interno, puede incurrirse en imprecisiones e irregularidades que no hayan sido detectadas bajo la ejecución de los procedimientos de auditoría previamente planeados dado que la revisión efectuada corresponde a una muestra de la información tomada; conforme a ello, la Entidad y el Proceso son responsables de establecer y mantener un adecuado Sistema de Control Interno para prevenir irregularidades y materialización de riesgos.

5.1. TEMAS VERIFICADOS

5.1.1. Realizar seguimiento al Plan de Acción / Plan Estratégico / Indicador del Proceso

Durante la auditoría se procedió a revisar aleatoriamente una muestra de las evidencias así:

A. Plan de Acción Institucional (PAI)

- **Indicador 51. Sellos de Excelencia "Gobierno Digital"**

  - **Primer trimestre**
    Durante este periodo se evidenció el cargue de las comunicaciones (correos electrónicos) donde se hace la respectiva postulación ante el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) para obtener el Sello de Excelencia "Gobierno Digital".

  - **Segundo trimestre**
    Se observa la publicación de datos abiertos que hace la Entidad para continuar con el proceso de obtención del Sello de Excelencia "Gobierno Digital".

➢ **Tercer trimestre**
Se observa el cargue de la última actualización realizada con corte a 31/03/2019 del "Histórico de Personas Desmovilizadas", en formato Microsoft Excel; en el mismo orden de ideas, durante el mes de abril se observa el "Histórico de Personas Desmovilizadas con corte a abril de la Vigencia 2019, estos carecen de logo institucional, quien elaboró y quien revisó.

Adicionalmente, se observa el cargue del Reconocimiento del Sello de Excelencia "Gobierno Digital" en primer nivel para Datos Abiertos – La Reintegración en Cifras, así como el cargue del Reconocimiento Sello de Excelencia "Gobierno Digital", en primer nivel, para Datos Abiertos – Estadísticas de las Personas Desmovilizadas que han Ingresado al Proceso de Reintegración.

- **Indicador 52. Documento aprobado de diagnóstico de situación actual y plan de acción para la implementación de la política de "Gobierno Digital"**

➢ **Primer trimestre**
Se observó el plan para el dominio de servicios tecnológicos (Documento borrador), fechado 11 de marzo de 2019.

➢ **Segundo trimestre**
Sin observaciones en las evidencias.

➢ **Tercer trimestre**
Haciendo una verificación de las evidencias subidas en la carpeta compartida determinada para tal fin se hicieron las siguientes observaciones:

❖ Al documento "Plan de Dominio Gobierno TI, Política de Gobierno Digital", sin observaciones sobre la evidencia.
❖ Al documento "Matriz de Dominio consolidada" sin observaciones sobre la evidencia.
❖ A los documentos: a) "Plan de Acción Dominio de Sistemas de Información"; b) "Política de Gobierno Digital"; c) "Plan de Acción Dominio Uso y Apropiación, Política de Gobierno Digital"; y, d) "Plan de Acción para la Implementación de la Política de Gobierno Digital"; sin observaciones sobre la evidencia.

- **Indicador 53. Nivel de avance en la implementación del Plan Estratégico de Tecnologías de la Información (PETI) para la Vigencia 2019**

➢ **Primer trimestre**
Durante este periodo se realizó un muestreo de documentos cargados como evidencias de este indicador en los cuales se observó que estos corresponden a lo solicitado en el mismo.

➢ **Segundo trimestre**
Realizada la auditoría, se pudo observar que, la evidencia cumple con el producto descrito en la acción.

➢ **Tercer trimestre**

Las evidencias subidas para este periodo cumplen con lo establecido en el Manual de Seguimiento a la Planeación y Gestión

B. Plan Anticorrupción

- **Indicador 18. Evaluación de cumplimiento a página web mediante aplicación de herramienta *Tawdis* 2019**

  - **Primer trimestre**
    Haciendo una verificación de las evidencias subidas en las carpetas compartidas determinadas para tal fin se observa lo siguiente:
    - Al documento: "Plan de trabajo de remediación" sin observaciones sobre la evidencia.

  - **Segundo trimestre**
    Su evidencia cumple con los descrito en el Manual de Seguimiento a la Gestión Institucional.

  - **Tercer trimestre**
    - Su evidencia cumple con los descrito en el Manual de Seguimiento a la Gestión Institucional.

- **Indicador 20. Actividades de sensibilización y concienciación sobre los temas relacionados con las políticas de seguridad de la información y políticas de uso de la información 2019**

Las evidencias cargadas para el cumplimiento de este indicador en las carpetas dispuestas para tal fin cumplen con lo establecido en el Manual de Seguimiento a la Planeación y Gestión Institucional de la ARN en cada uno de los trimestres objeto de análisis.

5.1.2. Revisar la aplicación y/o atributo del Control de los Documentos al Proceso de Gestión de Tecnologías de la Información

Dentro de la Auditoria se revisaron los siguientes documentos que se encuentran publicados en el SIGER así:

- **Caracterización proceso Gestión de Tecnologías de la Información:** documento vigente desde el 11 de noviembre de 2016 y, a la fecha, se encuentra en su versión N° 5. En él se observa que: a) en el campo de "Producto" del Planear se menciona Plan Operativo pero, en la actualidad, se manejan Planes de Acción; b) en el campo "Proveedor" y "Cliente" del documento en general se mencionan "Procesos ACR" y deben escribirse "Procesos ARN"; c) en el campo "Actividad" del Hacer se menciona "[…]plataforma tecnológica de la ACR[...], pero debe escribirse ARN; y, d) en el campo de "Requisitos" se hace referencia a la NTC GP 1000:2009

- **Documentos Complementarios**
  - **Manual de Gobierno Digital:** documento externo del MinTIC que contiene información sobre la Implementación de la Política de Gobierno Digital (decreto 1078 de 2015, Título 9, Capítulo 1). Este documento se visualiza en su Versión N° 5 y está fechado el 2018–09–24.

- **Matriz de Recursos Tecnológicos:** documento que detalla los recursos Tecnológicos de la Agencia; al consultar en la descripción de la ficha del documento se visualiza "Matriz de información detallada sobre los Aplicativos (Sistemas de información y Aplicaciones) utilizados en la ACR", pero lo correcto es escribir ARN; por otra parte, al interior del documento se observa que el logo hace referencia a la ACR, pero lo correcto es escribir ARN; adicionalmente, en el campo "Proveedor" se indica ACR, pero lo correcto es escribir ARN; y, finalmente, en el campo "Administrador del Sistema" se observa los nombres de personas que ya no laboran en la Entidad y se hace referencia a correos electrónicos con dominio: "acr.gov.co", pero lo correcto es escribir: "reincorporacion.gov.co".
- **Plan Operativo (PO) Oficina Tecnologías de la Información:** documento interno en el que se observa el Plan Operativo de la Vigencia 2015 por lo que, en consecuencia, este es un documento que no se está aplicando y, en consecuencia, es necesario que se solicite su inactivación al Administrador del SIGER.

- **Formatos:**
  - **Caso de uso (Código N° TI–F–03, Versión N° 3 y de fecha 2018–08–17)**: formato interno que, en su ficha de Documentos de SIGER, no tiene diligenciados los campos: "Documento"; "Tipo de Documento", y "Proceso". Sin el diligenciamiento de estos campos, no es posible determinar si este formato se encuentra asociado con otro documento y, en consecuencia, en el momento de modificarlo o eliminarlo se puede evaluar el impacto en el proceso; tal y como se observa a continuación:

  - **Acta de Aceptación de Funcionalidad (Código N° TI–F–02, Versión N° 3 y de fecha 2017–11–24)** este es un formato interno y, en su ficha de Documentos de SIGER, no tiene diligenciados los campos: "Documento"; "Tipo de Documento", y "Proceso". Sin el diligenciamiento de estos campos, no es posible determinar si este formato se encuentra asociado con otro documento y, en consecuencia, en el momento de modificarlo o eliminarlo se puede evaluar el impacto en el proceso; tal y como se observa a continuación:

FORMATO ACTA DE ACEPTACIÓN DE FUNCIONALIDAD

DATOS DOCUMENTO

Tipo de documento:	Formato				
Proceso:	Gestión de Tecnologías de la información				
Código:	TI-F-02	Versión:	V-3	Vigencia:	2017-11-24
Control de cambios:	Actualización de la sigla ACR por ARN, cambio de formato a la plantilla vigente de procedimiento dispuesta en el SIGER. Actualizado a logo azul ARN 28/08/2018.				
Dimensión:					
Palabras clave:					
Generar PDF:	NO				
Anexo:	Ver anexo	TI-F-02 Formato Acta de Aceptacion de Funcionalidad V3.docm			

DOCUMENTOS ASOCIADOS

Documento:	
Tipo documento:	
Proceso:	

- ❖ **Solicitud de usuario y/o recursos tecnológicos (Código N° TI–F–01, Versión N° 7 y de fecha 2019–07–09):** formato interno que tiene como finalidad que el Jefe de Dependencia, o Coordinador de GT, lo diligencie para solicitar los permisos de usuario o recursos tecnológicos que necesite; finalmente, después de la revisión efectuada, no se dejan observaciones.

- **Guías:**
  - ❖ **Guía de intercambio de información (Código N° TI–G–01, Versión N° 1 y de fecha 2019–09–02)**: documento Interno que ofrece lineamientos para la ejecución de intercambios de información tanto a escala interna como a otras entidades, proveedores o terceros de forma adecuada; lo anterior promueve la cultura de seguridad entre los interesados internos y externos; finalmente, después de la revisión efectuada, no se dejan observaciones.

- **Manuales:**
  - ❖ **Manual del Sistema de Gestión de Seguridad de la Información – SGSI (Código N° TI–M–01, Versión N° 7 y de fecha 2019–09–24):** documento interno que establece las directrices, lineamientos de seguridad y protección de la información, a través de la gestión segura de los activos de información, del Sistema de Gestión de Seguridad de la información que contribuya al cumplimiento de las metas estratégicas de la Agencia incluyendo, también, lo referente a Protección de Datos Personales. Finalmente, después de la revisión efectuada, no se dejan observaciones.

- **Normograma (Código N° TI–N–01, Versión N° y de fecha 201 9–10–29):** documento interno que indica las diferentes normas que aplican al proceso. Finalmente, después de la revisión efectuada, no se dejan observaciones.

- **Procedimientos:**
  - **Atención a requerimientos de sistemas de información (Código N° TI–P–01, Versión N° 04 y de fecha 2017–12–07):** documento interno que establece las actividades para atender todo tipo de requerimientos del Sistema de Información de la ARN. Finalmente, después de la revisión efectuada, no se dejan observaciones.
  - **Soporte a usuarios (Código N° TI–P–02, Versión N° 5 y de fecha 2017–12–07):** documento interno que define las actividades a realizar con el fin de atender una solicitud que llega a la Mesa de Soporte de la ARN Finalmente, después de la revisión efectuada, no se dejan observaciones.

Teniendo en cuenta lo anterior, se observa que 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 registrados en el sistema SIGER con el fin de dar cumplimiento a la Actividad N° 6 "Elaborar o ajustar los documentos" del Procedimiento Control de Documentos (Código N° GD–P–04, Versión N° 7 y de fecha 18/03/2019).

Nota: La actualización de Caracterización del Proceso se debe validar frente al Plan de Mejora que tiene el Proceso de Direccionamiento Estratégico.

5.1.3. Revisión de la aplicación y atributo del Control de Registros del Proceso de Gestión de Tecnologías de la Información.

Para efectos de esta auditoria se tomó para revisión el Procedimiento "Atención a requerimientos de Sistemas de Información (Código N° TI–P–01, Versión N° 4 y de fecha 07–12–2017); posteriormente, se solicitó una (1) carpeta donde se encontrara información de casos de uso al azar y el auditado suministró la carpeta de casos de uso correspondientes al mes de mayo de la Vigencia 2019; la misma contiene 31 formatos de casos de uso.

Así las cosas, se procedió con la revisión de la documentación de la carpeta suministrada por el auditado donde se observó que existen tres (3) actas que se encuentran firmadas el Ingeniero Hernán Alonso Lotero Rojas, como Coordinador de Sistemas de la OTI, pues su nombramiento quedó en firme en el mes de noviembre para los siguientes casos de uso: CU–SIR–FINANCIERA–0005-2; CU–SIR–PLANDETRABAJO-0002 y CU–SIR –B IE–0013.

De los 31 casos contenidos en esta carpeta se observa que 12 de ellos no cuentan con el formato "Acta de Aceptación de Funcionalidad" (Código N° TI–F–02, Versión N° 3 y de fecha 2017–11–24), tal como se observó en los siguientes casos de uso:

1. CU-SIR-FINANCIERA-0005-2
2. CU-SIRJURIDIA-0001
3. CU-SIR-PLANDETRABAJO-0001
4. CU-SIR-PLANDETRABAJO-0010
5. CU-SIR-BIE-0001
6. CU-SIR-FINANCIERA-0054
7. CU-SIR-JURIDICAA-0013
8. CU-SIR-JURIDICA-0033

9. CU-SIR-BIE-0003
10. CU-SIR-JURIDICA-0031
11. CU-SIR-BIE-0013
12. CU-SIR-JURIDICA-0038

Acto seguido, se revisaron ocho (8) casos (TFS 3180, CASO TFS 3287, teniendo énfasis en el paso a paso de las actividades contenidas en el Procedimiento "Atención a requerimientos de Sistemas de Información (Código N° TI–P–01, Versión N° 4 y de fecha 07–12–2017); estos casos representan una muestra de los casos contenidos en la carpeta descrita anteriormente. Producto de esta actividad se arrojaron los siguientes resultados:

N° ACTIVIDAD	FLUJOGRAMA	DESCRIPCION DE LA ACTIVIDAD	CUMPLE	NO CUMPLE
1	Recibir requerimiento del Sistema de Información	Recibir requerimiento de sistemas de información: Recibir solicitud del Jefe de Dependencia o delegado del área que realiza el requerimiento de nuevos desarrollos, ajustes a los sistemas de información o elaboración de reportes. La solicitud debe incluir mínimo la siguiente información: a) Delegado del área solicitante responsable durante la atención del requerimiento. b) Tipo de la solicitud: Se debe indicar si es un ajuste a una funcionalidad existente o un nuevo desarrollo. c) Descripción del requerimiento: Especificar qué se requiere, indicando si es una pantalla, un reporte, un proceso, instructivo, cambio de rol o creación de uno nuevo, etc.	**1.** CU–SIR–BIE– 0013 **2**. CU–SIR–BIE–0046 **3**. CU–SIR–BIE–0045 **4**. CU–SIR–JURIDICA–0031 **5**. CU–SIR–JURIDICA–0038	**1**. CU-SIR-BIE-0046 (CASO TFS 3287); **2**. CU-SIR-BIE-0045 (CASO TFS 3287); **3**. CU-SIR-JURIDICA-0038 (CASO TFS 3648)
2	Se atiende solicitud con (SI – Actividad 4) (No – Actividad 3)	Analizar solicitud y determinar la viabilidad del requerimiento y si puede ser atendida con un desarrollo interno.	No exige registro	N/A
3	Informar la No Viabilidad	Informar la No Viabilidad: Enviar correo electrónico al jefe de la dependencia solicitante informando la No Viabilidad del requerimiento con desarrollo interno.	No aplica para los casos revisados	No aplica para los casos revisados
4	Asignar profesional de sistemas de información	Asignar profesional para atender el requerimiento: Crea registro del requerimiento al profesional delegado a través de la herramienta establecida.	**1.**CU– SIR–BIE –0013 (TFS 3180); **2**. CU-SIR-JURIDICA-0031 (CASO TFS 3253); **3**. CU-SIR-REPORTE-0016(CASO Q38094) **4.** CU-SIR-PLANDETRABAJO-0010 (CASO TFS 2973)	**1**. CU-SIR-BIE-0046 (CASO TFS 3287); **2**. CU-SIR-BIE-0045 (CASO TFS 3287); **3**. CU-SIR-JURIDICA-0038 (CASO TFS 3648) **4**. CU-SIR-CULMINACION-0005(CASO TFS 2962)
5	Analizar requerimiento y establecer el Plan de Trabajo	Analizar requerimiento: analizar solicitud, establecer alternativa de solución, definir plan de trabajo e informar al Coordinador de Sistemas de Información el estado del requerimiento a través del registro en la herramienta establecida.	No exige registro	N/A

N° ACTIVIDAD	FLUJOGRAMA	DESCRIPCION DE LA ACTIVIDAD	CUMPLE	NO CUMPLE
6	Analizar Información	Realizar las actividades establecidas en el plan de trabajo de acuerdo a las siguientes etapas: 1. Etapa de análisis – Se realiza el Levantamiento del o los Caso(s) de Uso; 2. Etapa de desarrollo – Implementación de requerimientos solicitados, con control de código en herramienta establecida. (si aplica); 3. Etapa de Pruebas – Realizar pruebas internas a la nueva funcionalidad – Elaborar o actualizar el Instructivo de Usuario que explique cómo opera la funcionalidad.	**1.** CU-SIR-BIE-0013 (CASO TASK 3180) **2.** CU-SIR-JURIDICA-0031 (CASO TFS 3253) **3.** CU-SIR-REPORTE-0013 (CASO Q38094) **4**. CU-SIR-CULMINACION-0005 (CASO TFS 2962) **5**. CU-SIR-PLANDETRABAJO-0010 (CASO TFS 2973) **6**. CU-SIR-BIE-0046 (CASO TFS 3287) **7**. CU-SIR-BIE-0045 (CASO TFS 3287) **8.** CU-SIR-JURICA-0038 (CASO TFS 3648)	
7	Funcionalidad cumple con (Si va con Actividad 10) (No con Actividad 8)	Verificar la solución o la Funcionalidad Desarrollada según lo establecido en el o los Caso(s) de Uso.	No se exige registro	No se exige registro
8	Solicitar ajustes a la solución	Solicitar ajustes a la solución: Solicitar los ajustes a la solución del requerimiento o del instructivo de usuario.	No se exige registro	No se exige registro
9	Realizar ajustes solicitados	Realizar los ajustes solicitados. (Se devuelve a Actividad 7)	No se exige registro	No se exige registro
10	Firmar acta y solicitar puesta en producción	Firmar Acta Aceptación de la funcionalidad por el profesional de Sistemas de Información y el delegado de la dependencia solicitante, solicitar la puesta en producción de la funcionalidad.	**1.** CU-SIR-REPORTE-0016 (CASO Q38094)	1. CU-SIR-BIE-0013 (CASO TFS 3180) 2.CU-SIR-BIE-0045 (CASO TFS 3287) 3.CU-SIR-BIE-0046 (CASO TFS 3287); 4. CU-SIR-JUERIDICA-0031 (CASO TFS 3253) 5. CU-SIR-JURIDICA-0038 (CASO TFS 3648) 6. CU-SIR-PLANDETRABAJO-0010 (CASO TFS 3529) 7. CU-SIR-CULMINACION-0005 (CASO TFS 2962)

De acuerdo con lo anterior se observa que la OTI 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 12–07–2017), específicamente, en su Actividad 1 “Recibir requerimiento del Sistema de Información” y en su Actividad 10 “Firmar acta y solicitar puesta en producción”.

5.1.4. Verificar la Implementación del MIPG (Autodiagnóstico; Formulario Único Reporte de Avances de la Gestión – FURAG y Plan de Acción)

El día 20–11–2019 se indagó al entrevistado sobre el resultado del FURAG y el Plan de Acción / Plan de Mejora del MIPG que la Agencia está trabajando para su posterior implementación; resultado de la entrevista realizada se obtuvo la siguiente información:

- **Resultados FURAG:** La OTI conoce el resultado obtenido por la Entidad frente a esta evaluación así:

Índice de Desempeño Institucional	D1: Talento Humano	D2: Direccionamiento Estratégico y Planeación	D3: Gestión para Resultados con Valores	D4: Evaluación de Resultados	D5: Información y Comunicación	D6: Gestión del Conocimiento
88,5	87,9	83,3	88,1	89,2	92,6	89,6

Como se puede observar en la tabla anterior, el resultado del Índice de Desempeño Institucional fue del **88,5%** y, disgregando, la Dimensión 3 "Gestión para Resultados con Valores" obtuvo una calificación del 88,1%.

De igual manera, el auditado presenta un instrumento del Modelo de Seguridad y Privacidad de la Información (MSPI), que permite visualizar el nivel de implementación de acciones en la Entidad, mismas acciones que aplican a las políticas de Gobierno Digital y de Seguridad Digital.

Por otra parte, la Dimensión de Información y Comunicación obtuvo una calificación del 92,6 frente a 100 que es lo máximo.

Finalmente, se observa el conocimiento que tiene el auditado frente a las dos (2) políticas que se aplican en el proceso en lo referente a la implementación del MIPG; adicionalmente, cada semestre se está aplicando el autodiagnóstico con el fin de validar los aspectos a fortalecer y como estos se engranan con lo solicitado por MinTIC.

5.1.5. Seguimiento a la Implementación de la Norma ISO NTC–27001:2013

Del día 25 al día 28 de noviembre de 2019 se procedió a efectuar una revisión en la implementación de la Norma NTC–27001:2013 obteniendo los siguientes resultados:

REQUISITO	DESCRIPCIÓN	CALIFICACIÓN	C	NC	OP	OBSERVACIÓN DEL AUDITOR (25/11/2019 AL 28/11/2019)
4. CONTEXTO DE LA ORGANIZACIÓN		**92,50**				
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	La organización debe determinar las cuestiones externas e internas que son relevantes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su Sistema de Gestión de Seguridad de la información.	90,00			X	Se tiene un Plan para el Mantenimiento del Sistema de Gestión de Seguridad de la Información que fue aprobada en marzo de 2019; el contexto legal se debe articular con el Normograma. Buscar el instrumento; de igual manera se debe buscar la articulación con el Sistema de Gestión.

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	La organización debe determinar: a) las partes interesadas que son pertinentes para el Sistema de Gestión de Seguridad de la Información; y b) los requisitos de las partes interesadas pertinentes a la seguridad de la información. **NOTA:** los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.	90,00			X	Este punto de la norma se debe articular con el contexto de la Planeación Estratégica de la Agencia.
4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN	La organización debe determinar los límites y aplicabilidad del Sistema de Gestión de Seguridad de la Información para establecer su alcance. Cuando se determina este alcance, la organización debe considerar: a) las cuestiones externas e internas referidas en el numeral 4,1, y b) los requisitos indicados en el punto 4.2, y c) las interfaces y dependencias entre las actividades realizadas por la organización y las que realizan otras organizaciones. El alcance deberá estar disponible como información documentada.	90,00			X	En el Alcance se debe actualizar la Resolución N° 0335 de 2017 dado que, en el Manual del Sistema de Gestión de Seguridad de la Información (Código N° TI–M–01, Versión N° 7 y de fecha 24–09–2019) se describe un alcance diferente. Por otra parte, se recomienda que el Alcance se encuentre relacionado con el objeto de la Entidad y, asimismo, es preciso que se ajuste según las necesidades y expectativas de las partes interesadas y, también, según su contexto.
4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	La organización debe establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, de acuerdo con los requisitos de esta Norma.	100,00	X			La Entidad adoptó el Sistema de Seguridad de la Información mediante la Resolución N° 0335 del 24 de febrero de 2017 y el Manual del Sistema de Gestión de la Seguridad de la información de fecha 24 de septiembre de 2019.

5. LIDERAZGO		**83,33**				
5.1. LIDERAZGO Y COMPROMISO	La Alta Dirección debe demostrar liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información: a) asegurando que se establezcan la Política de Seguridad de la Información y los Objetivos de Seguridad de la Información y que estos sean compatibles con la dirección estratégica de la organización;	80,00			X	La Política se encuentra descrita en la Resolución N° 0335 del 24 de febrero de 2017; sin embargo, es importante que esta política contenga la Misión de la Entidad.
	b) asegurando la integración de los requisitos del Sistema de Gestión de Seguridad de la Información en los procesos de la organización;					Para que exista integración entre los requisitos del Sistema se debe actualizar la Caracterización de todos los procesos para que, así, se contemple el Sistema de Seguridad de la Información.
	c) asegurando que los recursos necesarios para el Sistema de Gestión de Seguridad de la Información estén disponibles;					En la Resolución N° 335 del 24 de febrero de 2017 se describen los recursos que se tendrán disponibles.
	d) comunicando la importancia de la gestión de la Seguridad de la Información eficaz y la conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información;					Al interior de la Agencia, se hacen campañas de sensibilización; adicionalmente, en los Comités de Desempeño Institucional la Jefe de la OTI lleva los avances del Sistema de Seguridad de la Información; en el mismo orden de ideas, la Mesa técnica colabora en la revisión de los temas de seguridad física y demás. Al respecto, es preciso indicar que el Director es quien asume la información que se debe divulgar al interior de la Entidad.
	e) asegurando que el Sistema de Gestión de Seguridad de la Información logre los resultados previstos;					En la actualidad se cuentan con instrumentos como el Autodiagnóstico del MIPG; la matriz MSPI y el FURAG para ir revisando el nivel de avance en la implementación del Sistema de Seguridad de la Información.
	f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del Sistema de Gestión de la Seguridad de la Información;					La OTI durante la Vigencia 2019 generó al interior de la Entidad, comunicaciones, notas de publicaciones, así como disposiciones y lineamientos con el fin de que la Alta Dirección genere información dirigida a los funcionarios y contratistas. De otra parte, en lo referente a intercambio de información, brindan el acompañamiento, por lo que el brazo técnico de la Entidad es la OTI para apoyar en lo relacionado con temas tecnológicos.
	g) promoviendo la mejora continua ; y					La OTI generó una guía de intercambio de información con el fin de que las dependencias que lo requieren apliquen dichas directrices.

	h) apoyando otros roles pertinentes de la Dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.					En lo referente a los temas de tecnología, la Dirección de la Entidad, ha definido que todas las dependencias de la ARN, en caso de requerir apoyo en lo referente a temas de tecnología, deben solicitar el apoyo y acompañamiento de los integrantes del Equipo de Tecnología con el fin de brindar la asesoría correspondiente.
5.2 POLÍTICA	La Alta Dirección debe establecer una política de seguridad de la información que: a) sea apropiada para el propósito de la organización; b) incluya los objetivos de Seguridad de la Información (véase el numeral 6.2) o proporcione el marco para establecer los objetivos de Seguridad de la Información; c) incluya el compromiso de cumplir con los requisitos aplicables en materia de seguridad de la información; y d) incluya el compromiso de mejora continua del Sistema de Gestión de Seguridad de la Información; y La Política de Seguridad de la Información debe: e) estar disponible como información documentada; f) comunicarse dentro de la organización; y g) estar disponible para las partes interesadas, según sea apropiado.	90,00			X	La Política del Sistema de Seguridad de la Información, definida en la Resolución N° 335 del 24 de febrero de 2017 menciona "Artículo 5, Política del SGSI. La Política del SGSI es la declaración general que representa la posición de la Dirección de la ACR con respecto a la protección de los activos de información, a la implementación del Sistema de Gestión de Seguridad de la Información – SSI y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos, los cuales deben estar articulado con el Sistema Integrado de Gestión para la Reintegración – SIGER." Por otra parte, el Manual del Sistema de Gestión de Seguridad de la Información (Código N° TI–M–01, Versión N° 7 y de fecha 2019–09–24) indica: "3.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – "Toda impresión física de este documento se considera Documento No Controlado." La versión vigente se encuentra en el *software* del SIGER (Página 25 de 51). La ARN reconoce la importancia de identificar y proteger sus activos de información; igualmente, se encuentra comprometida con la preservación de la confidencialidad, integridad, disponibilidad, legalidad y no repudio de toda información relacionada con su estrategia, gestión, bases de conocimiento y otros conceptos comprometiéndose, de esta manera, a desarrollar, implantar, mantener y mejorar continuamente el SGSI. De igual manera, la ARN tiene un compromiso con la seguridad de la información a través de la implantación de un conjunto adecuado de controles tales como: políticas, prácticas, procedimientos, estructuras organizativas y funciones tecnológicas; dichos controles establecidos permiten asegurar que se cumplen los objetivos de seguridad de la información de la Entidad. Teniendo en cuenta lo anterior se observa que la Resolución se debe actualizar con el fin de mantener homogénea la información ya descrita.
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	La Alta Dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen. La Alta Dirección debe asignar la responsabilidad y autoridad para:	80,00			X	En el Artículo 8 "Responsables" de la Resolución N° 335 del 24 de febrero de 2017 se describen unos responsables; por otra parte, en el Numeral 2.3 "Roles y Responsabilidades para los Sistemas de Información, Aplicativos, Portales y/o Servicios de Tecnologías de la Información" del Manual del Sistema de Gestión de Seguridad de la Información (Código N° TI–M–01, Versión N° 7 y de fecha 2019–09–24) se indican otros responsables; por lo anterior, se solicita que se efectué la actualización respectiva en la Resolución mencionada.

	a) asegurarse de que el Sistema de Gestión de la Seguridad de la Información sea conforme con los requisitos de esta Norma;					
	b) informar a la Alta Dirección sobre el desempeño del Sistema de Gestión de la Seguridad de la Información. **NOTA:** la Alta Dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del Sistema de la Seguridad de la Información dentro de la organización.					
6. PLANIFICACIÓN **6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES**		**75,00** **50,00**				
6.1.1 Generalidades	Al planificar el Sistema de Gestión de Seguridad de la Información, la organización debe considerar las cuestiones mencionadas en el numeral 4.1 y los requisitos a que hace referencia en el numeral 4.2 y determinar los riesgos y oportunidades que es necesario tratar, con el fin de: a) asegurarse de que el Sistema de Gestión de Seguridad de la Información puede lograr su resultado previsto;	50,00		X		Al hacer verificación no se visualiza la integración e implementación de las acciones de riesgos de Seguridad de la Información en todos los procesos. Adicionalmente, no se encuentra descrito, en instrumento alguno, como se evaluará la eficacia de las acciones de los Mapas de Riesgos de la Entidad.
	b) prevenir o reducir los efectos no deseados; y					
	c) lograr la mejora continua					
	La organización debe planificar: d) las acciones para tratar estos riesgos y oportunidades ; y					
	e) la manera de: 1) integrar e implementar las acciones en sus procesos del Sistema					

	de Gestión de Seguridad de la Información; y e) la manera de: 2) evaluar la eficacia de estas acciones.					
6.1.2 Valoración de riesgos de seguridad de la información	La organización debe definir y aplicar un proceso de valoración de riesgos de Seguridad de Información que: a) establezca y mantenga los criterios de riesgo de la información de seguridad que incluyen: 1) los criterios de aceptación del riesgo; y 2) los criterios para realizar valoraciones de riesgos de Seguridad de la Información; b) asegure que las valoraciones repetidas de los riesgos de la Seguridad de la Información produzcan resultados consistentes, válidos y comparables; c) identifique los riesgos de Seguridad de la Información: 1) aplicar el proceso de valoración de riesgos de Seguridad de Información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del Sistema de Gestión de Seguridad de la Información; e 2) identificar a los dueños de los riesgos; d) analice los riesgos de la Seguridad de la Información: 1) Valorar las consecuencias potenciales que resultarán si se materializan los riesgos identificados en 6.1.2 c) 1);	50,00		X		De acuerdo a lo descrito en el Manual de Gestión del Riesgo (Código DE–M–02, Versión N° 6 y de fecha 2019–06–18), Numeral 9.2.2 “Pauta para la Valoración del Riesgo", Literal b) Para los riesgos de Seguridad Digital, en el campo de "Impacto (Consecuencias) Cuantitativo", se indica X%, pero esto no se encuentra definido ni se indica cómo se debe calcular lo que, en consecuencia, no se ajusta al momento de aplicar el tema de valoración de los riesgos pues, al no tener esta variable definida, no se puede calcular el riesgo. Por otra parte, no se indica que los indicadores de Seguridad de la Información van a tener el mismo tratamiento.

	2) Valorar la probabilidad realista de que ocurran los riesgos identificados en 6.1.2 c) 1);					
	3) determinar los niveles de riesgo;					
	e) evalúe los riesgos de Seguridad de la Información: 1) comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a); y					
	2) priorizar los riesgos analizados para el tratamiento de riesgos.					
	La organización conservará información documentada acerca del proceso de valoración de riesgos de la Seguridad de la Información.					
6.1.3 Tratamiento de riesgos de Seguridad de la Información	La organización debe definir y aplicar un proceso de tratamiento de riesgos de Seguridad de la Información para: a) seleccionar las opciones apropiadas de tratamiento de riesgos de Seguridad de Información teniendo en cuenta los resultados de valoración de riesgos;	50,00		X		El Manual de Gestión del Riesgo (Código N° DE–M–02, Versión N° 6 y de fecha 2019–06–18) se debe ajustar con el fin de que este de una mejor línea para los riesgos de Seguridad de la información.
	b) determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de Seguridad de la Información; **NOTA:** las organizaciones pueden diseñar los controles necesarios, o identificarlos de cualquier fuente.					
	c) Comparar los controles determinados en 6.1.3 b) con los del Anexo A y verificar que no sean omitidos controles necesarios; **NOTA 1:** el Anexo A					

	contiene una lista amplia de objetivos de control y controles. Se invita a los usuarios de esta Norma a consultar el Anexo A, para asegurar que no se pasen por alto los controles necesarios. **NOTA 2:** los objetivos de control están incluidos implícitamente en los controles escogidos. Los objetivos de control y los controles enumerados en el Anexo A no son exhaustivos, y pueden ser necesarios objetivos de control y controles adicionales.					
	d) producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya que se implementen o no y la justificación para las exclusiones de controles del Anexo A;					
	e) formular un plan de tratamiento de riesgos de la Seguridad de la Información; y					
	f) obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de Seguridad de la Información y la aceptación de los riesgos residuales de la Seguridad de la Información.					
	La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de Seguridad de Información. **NOTA:** el proceso de valoración y tratamiento de riesgos de la Seguridad de la Información que se					

	presenta en esta Norma se alinea con los principios y directrices genéricas suministradas en la ISO 31000[5].					
6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS	La organización debe establecer los objetivos de Seguridad de la Información en las funciones y niveles pertinentes. Los objetivos de Seguridad de la Información deben: a) ser coherentes con la política de Seguridad de la Información; b) ser medibles (si es posible); c) tener en cuenta los requisitos de la Seguridad de la Información aplicables, y los resultados de la valoración y del tratamiento de los riesgos; y el tratamiento del riesgo; d) ser comunicados; y e) ser actualizados, según sea apropiado. La organización debe conservar información documentada sobre los objetivos de la Seguridad de la Información. Cuando se hace la planificación para lograr sus objetivos de Seguridad de la Información, la organización debe determinar: f) lo que se va hacer; g) los recursos que se requerirán; h) quién será responsable; i) cuándo se finalizará; y j) cómo se evaluarán los resultados.	100,00	X			La Entidad describe el Objetivo en la Resolución N° 335 del 24 de febrero de 2017 en los siguientes términos: "Garantizar que los riesgos asociados a la Seguridad de la Información sean identificados, valorados, controlados y administrados de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que produzcan en el entorno y las tecnologías". Por otra parte. los objetivos que se describen en el Manual del Sistema de Gestión de Seguridad de la Información (Código N° TI–M–01, Versión N° 7 y de fecha 2019–09–24) son: * Garantizar la continuidad de los servicios de gestión de la Entidad y tecnología de la información frente a incidentes. * Fortalecer en los servidores públicos y colaboradores de la Agencia para la Reincorporación y la Normalización las buenas prácticas y comportamientos seguros en el manejo de información. * Gestionar los riesgos de Seguridad de la Información para que sean conocidos y, según su impacto, sean atendidos de una forma documentada, repetible, eficiente y adaptada al entorno y a la tecnología. * Proteger la información de la gestión y la tecnología utilizadas para el procesamiento de la información de la Agencia para la Reincorporación y la Normalización, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información. Teniendo en cuenta lo anterior, se encuentra pendiente por articular esta información y dejar una sola versión y, de igual manera, indicar como se van a evaluar estos resultados.
7. SOPORTE		**82,00**				
7.1 RECURSOS	La organización debe determinar y proporcionar los	80,00				La Entidad cuenta anualmente con recursos definidos en el Plan Anual de Adquisiciones de Tecnología de la Información; sin embargo, se requiere fortalecer el talento

	recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.					humano para apoyar la implementación y mantenimiento del Sistema de Seguridad de la Información de la ARN.
7.2 COMPETENCIA	La organización debe: a) determinar la competencia necesaria de las personas que realizan, bajo su control un trabajo que afecta su desempeño de la Seguridad de la Información; y b) asegurarse de que estas personas sean competentes, basándose en la educación, formación, o experiencia adecuadas; c) cuando sea aplicable, tomar las acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y d) conservar la información documentada apropiada como evidencia de la competencia. **NOTA:** las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de las personas competentes.	80,00		X		De acuerdo con lo descrito en el Acta de Comité Institucional de Gestión y Desempeño N° 9, efectuada el 27 septiembre de 2018, se observa la designación como Oficial de Seguridad a una Asesora de la Dirección General; posteriormente, se procedió a revisar la Hoja de Vida de esta Asesora, pero se observó que tiene formación profesional en Psicología; por lo que su formación no está acorde con las responsabilidades del Oficial de Seguridad, tampoco, cuenta con la experiencia desempeñar este rol. Por otra parte, la Entidad se encuentra formando auditores en la Norma NTC–27001:2013 para que estos apoyen la implementación y seguimiento al Sistema de Seguridad de Información. Es importante tener en cuenta que todos los perfiles de cargo de la entidad deben incluir responsabilidades frente al SGSI y definir la competencia. Esta observación debe ser indicada al Grupo de Talento Humano
7.3 TOMA DE CONCIENCIA	Las personas que realizan un trabajo bajo el control de la organización debe tomar conciencia de: a) La política de Seguridad de la Información b) su contribución a la eficacia del Sistema de Gestión de Seguridad de la Información, incluyendo los beneficios de una mejora del desempeño	80,00				Se requiere fortalecer este tema para que los servidores públicos y los contratistas de la Agencia para que tomen conciencia acerca de la importancia de la implementación del SGSI. Por otra parte, la Entidad se encuentra formando auditores en la Norma NTC–27001:2013 para que estos apoyen la implementación y seguimiento al Sistema de Seguridad de Información.

	de la Seguridad de la Información; y c) las implicaciones de la no conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información					
7.4 COMUNICACIÓN	La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al Sistema de Gestión de Seguridad de la Información que incluyan: a) el contenido de las comunicación; b) cuándo comunicar; c) a quién comunicar; d) quién debe comunicar ; y e) los procesos para lleva a cabo la comunicación.	90,00				La Agencia cuenta con la Matriz de Flujos de Información Componente de Comunicación Pública (Código N° DE–F–25, Versión 1 y de fecha 2019–11–12); en este documento se presentan los lineamientos para generar la comunicación de la información; sin embargo, se debe verificar el documento complementario: "COMPONENTE COMUNICACIÓN PÚBLICA – MATRIZ DE FLUJOS DE INFORMACIÓN" (fechado el 2016–12–22) que se encuentra en el Proceso de Gestión de Comunicaciones, pues es necesario mantener una sola versión en la Entidad.
7.5 INFORMACIÓN DOCUMENTADA		**80,00**				
7.5.1 Generalidades	El Sistema de Gestión de Seguridad de la Información de la organización debe incluir: a) la información documentada requerida por esta Norma; y b) la información documentada que la organización ha determinado que es necesaria para la eficacia del Sistema de Gestión de Seguridad de la Información. **NOTA:** el alcance de la información documentada para un Sistema de Gestión de la Seguridad de la Información puede ser diferente de una organización a otra debido a: a) el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios, b) la complejidad de los	80,00		X		En el SIGER se observa el Manual de Seguridad de la Información (Código N° TI–M–01, Versión N° 7 de fecha 2019 –09–24); la Guía de Intercambio de Información (Código N° TI–G–01, Versión N° 1 y de fecha 2019–09– 02); y, en lo referente a riesgos se cuenta con el Manual de Gestión de Riesgos (Código DE–M–02, Versión N° 6 y de fecha 2019–06–18). De otra parte, la Oficina de Tecnología cuenta con un repositorio digital donde se observa documentación del Sistema de Seguridad de la Información en la carpeta /otidoc / soporte documentos / Sin embargo, es importante observar que documentación como, por ejemplo, la Declaración de Aplicabilidad, debe estar publicada en el SIGER, pues es información documentada necesaria.

	procesos y sus interacciones, y c) la competencia de las personas.					
7.5.2 Creación y actualización	Cuando se crea y se actualiza la información documentada de la organización debe asegurarse de que lo siguiente sea apropiado: a) la identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);	80,00		X		Los documentos que se han creado para el SGSI deben estar publicados en el SIGER.
	b) formato (por ejemplo, idioma, versión de *software*, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);					
	c) la revisión y aprobación con respecto a la idoneidad y adecuación.					
7.5.3 Control de la información documentada	La información documentada requerida por el Sistema de Gestión de Seguridad de la Información y por esta Norma se deben controlar para asegurarse de que: a) esté disponible y adecuada para su uso, donde y cuando se necesite; y	80,00				Los documentos que se han creado para el SGSI deben estar publicados en el SIGER.
	b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad)					

	Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable: c) distribución, acceso, recuperación y uso;					
	d) almacenamiento y preservación, incluida la preservación de la legibilidad;					
	e) control de cambios (por ejemplo, control de versiones); y					
	f) retención y disposición.					
	La Información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del Sistema de Gestión de Seguridad de la Información se debe identificar y controlar, según sea adecuado. **NOTA:** el acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.					
8. OPERACIÓN		**66,67**				
8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de Seguridad de la Información y para implementar las acciones determinadas en el numeral 6.1. La organización también debe implementar planes para lograr los objetivos de la Seguridad de la Información	100,00				

	determinados en el numeral 6.2.					
	La organización debe mantener información documentada en la medida necesaria para tener la confianza en que los procesos se han lleva a cabo según lo planificado					Se tiene un documento de Seguimiento a los indicadores del Sistema de Seguridad de la Información donde se lleva el registro de dos (2) indicadores mensuales y uno (1) anual.
	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.					Se tiene programada una (1) reunión con la Oficina Asesora de Planeación para dar lineamientos de TI Gestión de Cambios bajo el esquema ITIL.
	La organización debe asegurar que los procesos controlados externamente estén controlados.					Muchos de los procesos se encuentran regulados con la parte contractual; en este sentido, se tienen designados a varios supervisores quienes se encargan de efectuar el respectivo seguimiento.
8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	La organización debe llevar a cabo valoraciones de riesgos de Seguridad de la Información a intervalos planificados cuando se propongan u ocurran cambios significantes, teniendo en cuenta los criterios establecidos en el numeral 6.1.2 a).	50,00		X		La Entidad no cuenta con la información documentada de los resultados de las evaluaciones de los riesgos de seguridad y de los resultados en el tratamiento de los mismos para todos los riesgos.
	La organización conservará información documentada de los resultados de las evaluaciones de riesgos de Seguridad de Información.					
8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	La organización debe implementar el plan de tratamiento de riesgos de la Seguridad de la Información.	50,00		X		
	La organización debe conservar información documentada de los resultados del tratamiento de riesgos de la Seguridad de la Información.					
9. EVALUACIÓN DEL DESEMPEÑO		**60,00**				
9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	La organización debe evaluar el desempeño de la seguridad de la	100,00				La Entidad cuenta con mecanismos internos y externos como MSPI, Autodiagnóstico, FURAG, que apoyan el seguimiento y medición de la implementación del Sistema de Seguridad de

	información y la eficacia del Sistema de Gestión de Seguridad de la Información.					la Información; igualmente, cuenta con indicadores que deben ser revisados para verificar el cumplimiento del Sistema junto con la documentación que se ha implementado del mismo.
	La organización debe determinar: a) a qué es necesario hacer seguimiento y qué es necesario medir, incluyendo los procesos y controles de Seguridad de la Información;					
	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.					
	c) cuándo se debe llevar a cabo el seguimiento y medición;					
	d) quién debe llevar a cabo el seguimiento y la medición;					
	e) cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición; y					
	f) cuándo deban analizar y evaluar estos resultados.					
	La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y la medición.					
9.2 AUDITORÍA INTERNA	La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el Sistema de Gestión de Seguridad de la Información:	80,00				La Entidad no cuenta con un grupo de auditores que tengan la competencia y experiencia para evaluar el Sistema. En el mes de octubre la Agencia adelantó la formación de un grupo de auditores en la Norma ISO 27001:2013 los cuales, para la Vigencia 2020, deben adquirir la experiencia en el tema de auditoria y así apoyar en la implementación del Sistema al interior de la ARN.

	a) es conforme con: 1) los propios requisitos de la organización para su Sistema de Gestión de Seguridad de la Información; y, 2) los requisitos de esta Norma;					
	b) está implementado y manteniendo eficazmente.					
	La organización debe: c) planificar, establecer, implementar y mantener uno o varios programa(s) de auditoría, incluida la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programa(s) de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de auditorías previas;					
	d) para cada auditoria, definir los criterios y el alcance de ésta;					
	e) seleccionar auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;					
	f) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y					
	g) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.					
9.3 REVISIÓN POR LA DIRECCIÓN	La Alta Dirección debe revisar el Sistema de Gestión de Seguridad de la Información a intervalos planificados para asegurarse de su	0,00		X		La Alta Dirección, a la fecha de esta auditoría, no ha realizado la revisión del Sistema de Seguridad de la Información; de acuerdo con lo anterior, se deben efectuar revisiones continúas con el fin de tomar medidas de apoyo en la implementación y responsabilidades de todos los funcionarios

	conveniencia, adecuación y eficacia continuas.					y contratistas de la Agencia frente a la implementación de este Sistema.
	La Revisión por la Dirección debe incluir consideraciones sobre: a) el estado de las acciones con relación a las revisiones previas por la Dirección;					
	b) los cambios en las cuestiones externas e internas que sean pertinentes al Sistema de Gestión de Seguridad de la Información;					
	c) retroalimentación sobre el desempeño de la Seguridad de la Información, incluidas las tendencias relativas a: 1) no conformidades y acciones correctivas;					
	2) seguimiento y resultados de las mediciones;					
	3) resultados de la auditoría; y					
	4) cumplimiento de los objetivos de Seguridad de la Información;					
	d) retroalimentación de las partes interesadas;					
	e) resultados de la valoración de riesgos y el estado del plan de tratamiento de riesgos; y					
	f) las oportunidades de mejora continua.					
	Los elementos de salida de la revisión por la Dirección deben incluir decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el Sistema de Gestión de Seguridad de la Información.					
	La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la Dirección.					

10. MEJORA		**60,00**				
10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS	Cuando ocurra una no conformidad, la organización debe: a) reaccionar ante la no conformidad, y según sea el caso aplicable: 1) tomar acciones para controlarla y corregirla; y, 2) hacer frente a las consecuencias;	60,00		X		Se observa que el Sistema si ha tenido mejoramiento ejecutado, pero no documentado, en el Módulo de Mejoras del SIGER para su evaluación.
	b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el fin de que no vuelva a ocurrir ni ocurran en otra parte mediante: 1) la revisión de la no conformidad; 2) la determinación de las causas de la no conformidad; y, 3) la determinación de si existen no conformidades similares o que potencialmente podrían ocurrir;					
	c) Implementar cualquier acción necesaria					
	d) revisar la eficacia de las medidas correctivas tomadas; y					
	e) hacer cambios al Sistema de Gestión de Seguridad de la Información, si es necesario.					
	Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.					
	La organización debe conservar información documentada adecuada, como evidencia de:					
	f) la naturaleza de las no conformidades y cualquier acción posterior tomada; y					
	g) los resultados de cualquier acción correctiva.					
	La organización debe mejorar continuamente					

	la conveniencia, adecuación y eficacia del Sistema de Gestión de la Seguridad de la Información.					

De acuerdo a lo anterior se evidenció que la Agencia incumple los Numerales: a) 6.1.2 (Valoración de riesgos de Seguridad de la Información; b) 6.1.3 (Tratamiento de riesgos de Seguridad de la Información); c) 7.2 (COMPETENCIA); d) 7.5.1 (Generalidades); e) 7.5.2 (Creación y actualización); f) 8.2 (VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN); g) 8.3 (TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN; h) 9.3 REVISIÓN POR LA DIRECCIÓN; y, j) 10.1 (NO CONFORMIDADES Y ACCIONES CORRECTIVAS) de la Norma NTC – ISO 27001:2013.

5.2. CONFORMIDADES

Dentro del ejercicio de auditoría practicada al Proceso de Gestión de Tecnologías de la Información se encontraron las siguientes conformidades:

- Cuenta con personal calificado para implementar y sostener el MIPG en la Entidad.
- Cuenta con un personal que se encuentra receptivo a las observaciones efectuadas dentro de la auditoria.
- Cuenta con el conocimiento sobre la Gestión Institucional e Indicadores a los cuales hacen reporte y seguimiento a la administración.
- Se observó el cumplimiento en la organización de archivos digitales manejado por esta oficina.

5.3. NO CONFORMIDADES

NC1. 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: Como ya se estableció el Plan de Mejora PM-19-00023 de la Implementación de MIPG; donde una de las acciones corresponde a las actualizaciones de las caracterizaciones de los procesos; este documento no se tendrá en cuenta en la formulación del plan de mejora de esta auditoría.

NC2. 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.

NO CONFORMIDADES TRANSVERSALES – DIRECCIÓN GENERAL:

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; 7.2 COMPETENCIA; 7.5.1 Generalidades; 7.5.2 Creación y actualización; 8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN; 8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORAMCIÓN; 9.3 REVISIÓN POR LA DIRECCIÓN y 10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS de la norma NTC ISO 27001:2013.

6. OBSERVACIONES

No aplica.

7. ASPECTOS POR FORTALECER – DIRECCION GENERAL

Dentro de la revisión efectuada en esta auditoria se recomienda fortalecer los siguientes puntos de la Norma ISO 27001:2013 con el fin de contribuir a completar la implementación de la misma al interior de la Entidad:

- 4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO
- 4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS
- 4.3 DETERMINACION DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- 5.1. LIDERAZGO Y COMPROMISO
- 5.2 POLÍTICA
- 5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN
- 7.1 RECURSOS
- 7.3 TOMA DE CONCIENCIA
- 7.4 COMUNICACIÓN
- 7.5.3 Control de la información documentada
- 9.2 AUDITORÍA INTERNA

8. ASPECTOS A FORTALECER DEL PROCESO DE GESTIÓN DE TECNOLOGIAS.

De la revisión de los documentos que tiene el proceso de Gestión de Tecnologías, se observa que se puede fortalecer la ficha referencial de los documentos que se tienen registrados en SIGER, con el fin que, en el momento de efectuar actualizaciones, estas no queden obsoletas y no afecten el fin del documento.

En cuanto al tema de evidencias, se observa en la muestra obtenida para esta auditoría que se aplican los lineamientos impartidos en el Manual de Seguimiento a la Planeación; sin embargo, se sugiere que se revise en su totalidad los documentos no que no fueron objeto de esta auditoría, con el fin de garantizar el cumplimiento con los lineamientos.

9. CONCLUSIONES

- La auditoría se ejecutó de acuerdo con lo previsto en el Plan de Auditoría y, a la vez, se cumplió con el objetivo y alcance programado gracias a la disposición de los funcionarios y contratistas del Proceso de Gestión de Tecnologías de la Información.
- Finalmente, y resultado de la Auditoría, se observó que la gestión adelantada por los funcionarios y contratistas se realiza de manera satisfactorio dentro del marco regulatorio aplicable y vigente. En el Proceso se aplican procedimientos y formatos que le permiten adelantar su función; cuenta con funcionarios públicos competentes y comprometidos con el cumplimiento de los objetivos institucionales y con la mejora continua.

9.1. ANEXOS

No Aplica.

Nota: el presente informe no requiere firma por parte del Auditor Líder ni del Auditado teniendo en cuenta que su aprobación se realiza a través del Sistema de Gestión para la Reintegración (SIGER).