INFORME DE AUDITORÍA

1. INFORMACIÓN BASICA DE LA AUDITORÍA			
CÓDIGO AUDITORÍA:	AUD-1819	**TIPO DE AUDITORÍA:**	AUDITORÍA INTEGRAL
FECHA DE INFORME:	Diciembre 19 de 2018	**PROCESO / DEPENDENCIA AUDITADA:**	Gestión de Tecnologías de la Información
FECHA DE AUDITORÍA:	Del 19 de noviembre al 14 de diciembre de 2018	**AUDITORES:**	Auditor Líder: Eduardo Antonio Sanguinetti Romero. Auditor Acompañante: Ana Yancy Urbano Velasco.

2. OBJETIVO DE LA AUDITORÍA

Evaluar la gestión integral del Proceso de Gestión de Tecnologías de la Información con el fin de verificar el cumplimiento de los requisitos del Modelo Integrado de Planeación y Gestión (MIPG); las Normas Técnicas de Calidad NTC ISO 270001:2013 y el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST), así como la Normatividad Vigente y los procedimientos establecidos para el mejoramiento del continuo del proceso.

3. ALCANCE DE LA AUDITORÍA

La evaluación se realizará a la gestión adelantada por la Oficina de Tecnologías de la Información desde el 01/01/2017 al 31/10/2018.

Nota aclaratoria: se incluirá dentro del alcance la verificación de la eficacia del Plan de Mejora PM-16-00094.

4. CRITERIOS DE LA AUDITORÍA

Se tendrán como criterios normativos los establecidos en la Ley 594 de 2000; la Ley 1474 de 2011; la Ley 1712 de 2014; la Ley 1755 de 2015; el Decreto Ley 897 de 2017; el Decreto Ley 1499 de 2017; el decreto 4138 de 2011; el capítulo 6 del decreto 1072 de 2015; la resolución 1893 de 2015; la resolución 1111 de 2017; la NTC ISO 27001:2013; el MIPG y todas las normas de calidad aplicables.

Igualmente, se tendrán en cuenta la caracterización, procedimientos, manuales e instructivos, inscritos en el Sistema Integrado de Gestión para la Reintegración (SIGER), así como las demás normas, documentos, circulares, procedimientos, manuales e instructivos que regulen y le apliquen al Proceso de Gestión de Tecnologías de la Información.

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 el Plan de Auditoría. En el desarrollo de la misma se adelantaron los siguientes procedimientos:

- Reunión de Apertura de la Auditoría el día 19 de noviembre de 2018 cumpliendo, de esta manera, con el protocolo establecido para tal fin.
- Charla de Autocontrol impartida por el Asesor del Grupo de Control Interno de Gestión la cual se efectuó el 19 de noviembre de 2018; la mencionada actividad fue efectuada en dos (2) jornadas así: una en la mañana y otra en la tarde con el fin de que todos los integrantes de este proceso asistieran.
- Se cumplió con el protocolo de solicitud de información pactado con el auditado.
- Revisión *In Situ* de temas y aclaraciones de aspectos evidenciados en las muestras de auditoría con los profesionales encargados.
- Se efectuó Reunión de Cierre con la asistencia del Líder del Proceso y el Coordinador del Grupo de Sistemas de Información el día 19 de diciembre de 2018.

Cabe resaltar que, debido a las limitaciones de cualquier estructura de control interno, puede incurrirse en errores e irregularidades que no hayan sido detectados bajo la ejecución de los procedimientos de auditoría previamente planeados; conforme a ello, la Entidad y el Proceso son responsables de establecer y mantener un adecuado Sistema de Control Interno y de prevenir irregularidades y materialización de riesgos.

5.1 TEMAS VERIFICADOS

Con el fin de poder validar información y cumpliendo con lo establecido en el Plan de Auditoría se procedió a verificar los siguientes temas:

- Políticas del Modelo Integrado de Planeación y Gestión – MIPG y SG-SST.
- Verificación del trámite de las Peticiones, Quejas, Reclamos, Sugerencias y/o Denuncias (PQRS-D).
- Verificación de la eficacia de los planes de mejoramiento cerrados a cargo del Proceso PM-16-00094.

5.1.1 Políticas del Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST)

Con el fin de validar el cumplimiento de las políticas establecidas en el MIPG y el SG-SST, se procedió a aplicar el siguiente cuestionario al Líder del Proceso y a los profesionales que atendieron la Auditoría:

- **Política de Gestión Política Direccionamiento y Planeación**

COMPONENTE	CATEGORÍA	PREGUNTA	RESPUESTA POR EL AUDITADO
CONTEXTO ESTRATÉGICO	Identificación de los Grupos de Valor y sus necesidades	¿Cómo ha el identificado el Proceso los grupos de valor y sus necesidades?	Se cuenta con un documento, el cual describe la caracterización de los usuarios de la Oficina de Tecnología de la Información (OTI). Este documento fue remitido, mediante correo electrónico, a la Oficina Asesora de Planeación el día 26 de septiembre y se encuentra en proceso de validación por parte de la mencionada oficina.

LIDERAZGO ESTRATÉGICO	Liderazgo estratégico	¿Qué lineamientos se han tomado desde el Proceso de Gestión de las Tecnologías de la Información para la implementación de MIPG?	Se evidencian reuniones de la OTI en las que se envía la información a su equipo en lo relacionado con los indicadores y nuevos lineamientos a cumplir. De igual manera, se replican correos de nuevos lineamientos enviados por otras entidades o por la Líder del Proceso, todo con el fin de que el grupo de trabajo se encuentre capacitado y con el conocimiento adecuado para cumplir con sus labores. Por otra parte, se emiten correos informativos a todo el equipo de la OTI. Igualmente, esta oficina ha adoptado el uso de carpetas compartidas donde se evidencia la documentación que es generada por sus miembros para cada uno de los temas objeto de trabajo por esta dependencia; esta información se encuentra a disposición del grupo de trabajo debidamente identificada.

- **Gestión Presupuestal**

POLÍTICA	CATEGORÍA	ACTIVIDADES DE GESTIÓN/ PREGUNTAS PARA EL PROCESO	RESPUESTA DEL AUDITADO
GESTIÓN PRESUPUESTAL	Programación Presupuestal	¿Qué presupuesto tiene asignada la OTI?	El presupuesto asignado para la Vigencia 2018 es de: $**18.381823.551**, y la distribución es: A-3-1-1-28 Conectividad y Comunicaciones $**4.613.089.500** A-3-1-1-28 Dotación de Equipos $**3.466.268.482** A-3-1-128 Renovación y Adquisición de Licenciamiento de la Entidad. $**3.190.381.739** A-3-1-1-28 Servicio Premier de Microsoft y conexos $**500.000.000** A-3-1-1-28 Servicios Tecnológicos para la ARN …$**6.570.583.830** A-3-1-1-28 Suministro de requerimientos tecnológicos $**41.500.000**
		¿Cómo se hace el seguimiento a la asignación presupuestal?	La Líder del Proceso, junto con una de sus colaboradoras, han elaborado un archivo, en formato Microsoft Excel, denominado

			"Proyección de pagos oct-nov-dic 2018". En este archivo se evidencia discriminación por: Descripción del Servicio (bien o servicio requerido); Modalidad de Selección; Descripción de la Actividad en el Presupuesto; Rubro Presupuesto (Reintegración); Valor estimado – asignado a contratar; Fuente de Recursos de Reintegración 2018; Fuente de Recursos de Reintegración 2018; Fuente de Recursos de Reincorporación 2018; Fuente de los recursos 2018 (Total Fuente de Recursos); Fuente de Recursos (Reintegración/Reincorporación); Estado; Estado Actual; y Observaciones y trazabilidad; en el campo de trazabilidad se tienen observaciones como aquellos rubros donde se liberaron dineros.
		¿Qué balance se tiene sobre la liquidación de los contratos que tiene a cargo la OTI?	Dentro de las actividades que la Jefe de la Oficina ha implementado se tiene el control de liquidación de los contratos que ya se encuentran en estado ejecutados; este control se lleva a cabo en un archivo, en formato Microsoft Excel, llamado "Liquidaciones 2018". En el mismo se evidencian las actividades adelantadas con el fin de dar cumplimiento a lo requerido por el Grupo de Gestión Contractual; igualmente, este archivo tiene pestañas marcadas con los nombres de Vigencias 2015, 2016, 2017 y 2018. Para la vigencia 2015, se cuenta con 16 registros de los cuales dos (2) se encuentran en revisión por parte del Grupo de Gestión Contractual. Para la vigencia 2016 se tienen 12 registros de los cuales dos (2) se encuentran en proceso de liquidación. Para la Vigencia 2017 se cuenta con nueve (9) registros de estos, tres (3) registros, se encuentran en proceso de liquidación.

			Para la vigencia 2018 se cuenta con ocho (8) registros de los cuales cinco (5) de estos no requieren liquidación de acuerdo a memorando enviado por el Grupo de Gestión Contractual y tres (3) se encuentran en proceso de generación de su acta de liquidación.

- **Política de Gobierno Digital**

POLÍTICA	CATEGORÍA	ACTIVIDADES DE GESTIÓN/ PREGUNTAS PARA EL PROCESO	RESPUESTA DEL AUDITADO
TIC PARA GOBIERNO ABIERTO	Indicadores de Proceso Logro: Participación	De las actividades formuladas en la Estrategia de participación ciudadana, señale cuáles se realizaron por medios electrónicos: a. Rendición de cuentas. b. Elaboración de normatividad. c. Formulación de la planeación. d. Formulación de políticas, programas y proyectos. e. Ejecución de programas, proyectos y servicios. f. Ejercicios de innovación abierta para la solución de problemas relacionados con sus funciones. g. Promoción del control social y veedurías ciudadanas. e. Ninguno de los anteriores.	La Entidad ha adelantado tareas por medios electrónicos de la siguiente manera: • Rendición de Cuentas que fue transmitida también por medios electrónicos (Skype). • Formulación de políticas, proyectos y servicios: en este caso se conoce acerca de las capacitaciones en el tema de proyectos que aplicará la Entidad y en la cual los usuarios deben registrar información en el aplicativo dispuesto para esto. Aunque no se cuenta con las evidencias en la OTI se encuentra pendiente que, por parte de la Oficina Asesora de Planeación y el Grupo de Atención al Ciudadano, se alleguen las evidencia con el fin de subir el porcentaje de calificación. (En este momento se tiene un avance de un 43%).
TIC PARA LA GESTIÓN	Indicadores de Proceso Logro: Estrategia de TI	¿La arquitectura empresarial es una estrategia? ¿Qué procesos se han determinado para este punto?	En este punto se ha dado prelación a los procesos misionales; sin embargo, es importante que en la Entidad exista un replanteamiento de Misión, Visión, Objetivos y Planeación de acuerdo a lo contenido en el decreto 897 de 2017 dado que se modificó la estructura de la Entidad y esto

			requiere que sea ajustado y articulado con los requerimientos para la implementación del MIPG. (En la actualidad se tiene como calificación un 80% en su avance.)
	Indicadores de Proceso Logro: Información	Con relación a la gestión y planeación de los componentes de información, la Entidad: a. Definió un esquema de gobierno de los componentes de información. b. Definió una metodología para el diseño de los componentes de Información. c. Definió un esquema para el análisis y aprovechamiento de los componentes de Información. e. Ninguna de la anteriores.	Con respecto a este punto la Agencia ha generado los siguientes instrumentos: Una (1) matriz de activos de información; una (1) matriz de flujos de información y una (1) matriz de dominios de Información con el fin de consolidar el esquema de gobierno de los componentes de información. Es de anotar que la matriz de activos de información se encuentra bajo la responsabilidad de la Oficina Asesora de Planeación.
	Indicadores de Proceso	Durante el periodo evaluado, la Entidad implementó dentro de sus sistemas de información la Guía de Estilo y las especificaciones técnicas de usabilidad definidas por la Entidad y el Ministerio de las Tecnologías de la Información en sus: a. Sistemas de información misionales. b. Sistemas de información de soporte. c. Sistemas de información estratégicos. d. Portales digitales. e. Ninguna de las anteriores.	En revisión de los sistemas de información que actualmente maneja la Entidad se revisa y se obtiene el siguiente resultado: Literal a. Se aplica en el Sistema de Apoyo para la Reincorporación (SARA). Literal b. Impedimento contractual (propiedad de tercero) Literal c. Impedimento contractual (propiedad de tercero) Literal d. Se aplicó en la página electrónica de la Agencia y en la Intranet. En este punto es preciso indicar que los sistemas que se tienen en la Agencia, y que corresponden a un tercero, se validarán para verificar que cumplan las condiciones en las próximas renovaciones y/o nueva contratación.
SEGURIDAD Y PRIVACIDAD	Indicadores de resultado	La Entidad contó con un proceso de identificación	La Entidad ha realizado un trabajo detallado y, al interior

DE LA INFORMACIÓN	Seguridad y Privacidad de la Información	de infraestructura crítica; lo aplicó y comunicó los resultados a las partes interesadas.	de la ARN, se creó una matriz de activos de información. Este dio parámetros para identificar la infraestructura y la clasificación de su criticidad. Se cuenta con el formato diligenciado "Guía de Identificación ICC", tomado de la Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia. De igual manera la Oficina de Tecnologías de la Información generó una (1) presentación de Infraestructura crítica. Sin embargo, este tema se encuentra bajo la responsabilidad de las áreas de la Oficina Asesora de Planeación, dado que se encuentra la administración y custodia de la matriz de activos de información; en lo referente al tema de continuidad del negocio, este se encuentra bajo la responsabilidad de la Subdirección Administrativa.
		¿Qué aspectos resalta de esta política?	La Entidad ha venido implementando productos y servicios que generan valor por lo que ha venido aplicando mejores prácticas y estándares de calidad. De hecho, siguiendo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) que creó un modelo de Sello de Excelencia de Gobierno Digital con lo cual se evaluarán las Entidades Públicas, la OTI ha validado los 10 requisitos exigidos en esta guía y se evalúa que la Entidad los cumple. Así las cosas, la mencionada Oficina ha solicitado al Director, quien ha autorizado la postulación de la Entidad, con el fin de obtener este título de "Sello de la Excelencia".

			Por lo anterior, se verifica que la Entidad ha venido trabajando con el fin de obtener reconocimiento en el sector y, en general, con todas las entidades públicas generando, así, valor agregado a todas las actividades realizadas por esta oficina.

- **Política de Seguridad de la Información**

POLÍTICA	CATEGORÍA	ACTIVIDADES DE GESTIÓN/ PREGUNTAS PARA EL PROCESO	RESPUESTA DEL AUDITADO
SEGURIDAD DE LA INFORMACIÓN	Seguridad de la Información	¿Qué instrumentos ha aplicado con el fin dar cumplimiento a esta política?	La Entidad cuenta con el Instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información (MSPI) emitido por el MINTIC. En este documento se encuentra descrita la escala de evaluación y las políticas de seguridad de la información. Adicionalmente, se cuenta con mesas de trabajo de Seguridad donde se ha venido informando sobre los temas de seguridad de la Entidad; para este caso se evidenciaron las siguientes actas de reunión: Mesa de Trabajo de Seguridad de Información N° 1-2018 de abril de 2018; Acta N° 2 de octubre de 2018 y Acta N° 3 de octubre de 2018.
		¿Qué estrategia ha adoptado la Entidad con el fin de implementar la Política de Seguridad de la Entidad?	La Entidad, desde hace dos (2) años, contrató a un proveedor para que efectuará un diagnóstico de Continuidad del Negocio. Es por ello que, en la actualidad, la Agencia se encuentra trabajando bajo esas premisas y es por ello que se tiene un proyecto de Continuidad del Negocio el cual, a la fecha, se encuentra asignado al Subdirector Administrativo. De igual manera, se han generado unas mesas de trabajo para tratar

			diferentes frentes de acción sobre este tema. Al respecto, se evidencia Acta de Reunión de Continuidad del Negocio realizada el día el 6 de septiembre de 2018, en la misma se hizo la presentación a quien asumirá la dirección de este proyecto.
		Organización de la información	La OTI cuenta con una carpeta compartida que tienen en uso todos sus integrantes, allí se evidencia documentos elaborados en materia de Seguridad de la Información.
		¿Se han realizado campañas y/o sensibilizaciones a la Entidad sobre temas de Seguridad de la Información?	La oficina de Tecnologías de la Información ha venido redactando documentos sobre este tema y, por ende, ha socializado en la Agencia sobre los mismos. Al respecto, se evidencia correo electrónico del 9 de noviembre de 2018 donde, la Jefe de la OTI, envía información a los Asistentes de Información y sus colaboradores en Sede Central sobre una nota publicada en la Intranet acerca de la “Gestión de Incidentes de Seguridad de la Información”; esta noticia se encuentra a disposición de todos los funcionarios de la Entidad. De igual manera, se logró evidenciar una presentación acerca de las buenas prácticas para almacenar documentos digitales que la Agencia debe adoptar con el fin mantener coherencia con las tablas de retención e información generada en cada Dependencia.
		¿Cómo se tiene definida la participación de la Alta Dirección para apoyar el Sistema de Gestión de la Seguridad de la Información (SGSI)?	La Entidad cuenta con un Comité Institucional de Gestión y con una Mesa de Seguridad quienes están encargados de: • Definir y adoptar políticas para la gestión y tratamiento de los Riesgos

			de Seguridad de la Información. • Definir y adoptar políticas para el desarrollo del SGSI. • Solicitar al Responsable de Seguridad de la Información el resultado del Estado del Sistema de Gestión de Seguridad de la Información.

5.1.2 Seguimiento Aplicación NTC 27001 – Seguridad de la Información

Requisito		
4 Contexto de la Organización		
4.1 Entendiendo la Organización y su contexto		
ENUNCIADO DE LA NORMA	**EVIDENCIA**	**REVISIÓN CONTROL INTERNO**
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.	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Evidenciado metodología DOFA
4.2. Comprensión 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	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Evidenciado metodología DOFA
La organización debe determinar: b]los requisitos de las partes interesadas pertinentes a la seguridad de la información. (Debe incluir Requisitos Legales y reglamentarios, obligaciones contractuales.	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Se encuentra en proceso de actualización
4.3. Determinación del alcance del sistema de gestión de seguridad de la información		

La organización debe determinar los límites y aplicabilidad del sistema de gestión de seguridad de la información para establecer su ámbito de aplicación. Al determinar este ámbito, la organización debe considerar: a) los problemas externos e internos mencionados en el 4,1;	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información.	Evidenciado Manual de Gestión de Seguridad de la Información con Código TI-M-01 V-6 30/11/2018
b) los requisitos indicados en el punto 4.2, y	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Evidenciado metodología DOFA
c) las interfaces y las dependencias entre las actividades realizadas por la organización, y los que se llevan a cabo por otras organizaciones.	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Aspecto por mejorar: incluir en el Manual del Sistema de Gestión de Seguridad de la Información TI-M-01, la articulación
El alcance deberá estar disponible como información documentada.	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Evidenciado en SIGER - MÓDULO DE CONTROL DE DOCUMENTOS - LISTADO MAESTRO DE DOCUMENTOS - PROCESO DE Gestión e Tecnologías de la información - manual, PAGINA WEB
4.4. Sistema de gestión de seguridad de la información		
La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, de conformidad con los requisitos de esta Norma Internacional.	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Evidenciado Manual del Sistema de Gestión de Seguridad de la Información.
5. Liderazgo		
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	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información.	Evidenciado Manual del Sistema de Gestión de Seguridad de la Información.

información y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización;		
b) asegurando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización;	Reglamento Mesa de Seguridad	A través de la líder del proceso de Gestión de Tecnologías de la Información, se realiza capacitación, charlas y remisión de tips informativos para el cumplimiento de las políticas de seguridad de la información. Comité Institucional de Gestión y Desempeño y la Mesa de Seguridad tienen responsabilidades establecidas en el Manual SGSI. Aspecto por mejorar: incluir en las caracterizaciones de los procesos los requisitos que estos debe liderar y compromisos, dicha tarea debe ser liderada por la Oficina Asesora de Planeación.
c) asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;	Reglamento Mesa de Seguridad	Evidenciado con el presupuesto asignado a la ARN se destina en el plan anual de adquisiciones los recursos anuales y plan de acción.
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;	Reglamento Mesa de Seguridad	Se evidencia la labor que realiza la OTI; sin embargo, se requiere que en la Revisión por la Dirección, se deje constancia del resultado de esta revisión con el fin de dar cumplimiento a este requisito.
e) asegurando que el sistema de gestión de seguridad de la información logre los resultados previstos;	Reglamento Mesa de Seguridad	Se evidencia reglamento de la mesa de seguridad, sin embargo se requiere fortalecer este tema realizando la Revisión por la Dirección.
f)dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;	Reglamento Mesa de Seguridad	Reglamento Mesa de Seguridad
g) promoviendo la mejora continua ; y	Reglamento Mesa de Seguridad	Se requiere tener formulado planes de mejoramiento que permitan determinar cuál ha sido el mejoramiento continuo, ya que a través de la OTI se han implementado acciones de mejora.

h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad .	Reglamento Mesa de Seguridad	Roles definidos en el manual de seguridad de la información
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;	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Se evidencia en el TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
b) incluya los objetivos de seguridad de la información (ver 6.2) o proporcione el marco para establecer los objetivos de seguridad de la información;	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Se evidencia en el TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
c) incluya un compromiso de cumplir con los requisitos aplicables en materia de seguridad de la información; y	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Se evidencia en el TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
d) incluya un compromiso de mejora continua del sistema de gestión de seguridad de la información.	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Se evidencia en el TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
La política de seguridad de la información debe: e) estar disponible como información documentada;	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Se evidencia en el TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información, y se encuentra publicado en el SIGER.
La política de seguridad de la información debe: f) ser comunicada dentro de la organización; y	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Se requiere fortalecer la comunicación de la política del SGSI al interior de la entidad y a las partes interesadas. Es importante indicar que hay evidencia de las actividades que adelanta permanentemente la OTI en el Comité Institucional pero que el fortalecimiento de la comunicación deberá ser adelantado por el Grupo de Talento Humano y La Oficina Asesora de Comunicaciones
La política de seguridad de la información debe: g) estar a disposición de	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Se requiere fortalecer aún más la divulgación de la política del SGSI al interior de la entidad y a las partes interesadas, esta actividad

las partes interesadas, según corresponda.		se debe coordinar con el Grupo de Talento Humano y la Oficina Asesora de Comunicaciones.
5.3. Roles de organización, responsabilidades y autoridades		
La alta dirección debe asegurarse de que las responsabilidades y autoridades para las funciones relevantes para la seguridad de información son asignados y comunicados.	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Roles establecidos en el TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información, sin embargo se requiere fortalecer este deber mediante comunicado del Director a los directivos.
La alta dirección debe asignar la responsabilidad y autoridad para: a) garantizar que el sistema de gestión de seguridad de la información se ajusta a los requisitos de esta Norma Internacional; y	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Roles establecidos en el TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información, sin embargo se requiere fortalecer este deber mediante comunicado del Director a los directivos.
La alta dirección debe asignar la responsabilidad y autoridad para: b) informar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Roles establecidos en el TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información, sin embargo se requiere fortalecer este deber mediante comunicado del Director a los directivos.
6 Planeación		
6.1 Acciones para abordar los riesgos y oportunidades		
6.1.1 Consideraciones generales		
Al planificar el sistema de gestión de seguridad de la información , la organización debe considerar las cuestiones mencionadas en los 4.1 y los requisitos a que hace referencia 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;	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Plan de acción SGSI versión 6 2018, metodología DOFA

b) prevenir o reducir los efectos no deseados ; y	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
c) lograr la mejora continua	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
La organización debe planificar : d) las acciones para tratar estos riesgos y oportunidades ; y	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
e) la manera de: 1) integrar e implementar las acciones en sus procesos del sistema de gestión de seguridad de la información; y	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
e) la manera de: 2) evaluar la eficacia de estas acciones.	Manual de Gestión del Riesgo	El Manual de Gestión del Riesgo, se requiere actualizar, con el fin de articular con el procedimiento de Acciones Correctivas, preventivas y de mejora del proceso de Evaluación, Control y Mejoramiento, esta actividad se debe articular con la Oficina Asesora de Planeación.
6.1.2 Evaluación de riesgos de seguridad de la información		
La organización debe definir y aplicar un proceso de evaluación 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	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
2) los criterios para la realización de las evaluaciones de riesgos de seguridad de la información;	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
b) se asegure de que las evaluaciones de riesgos de seguridad de la información repetida producen resultados consistentes, válidos y comparables;	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo

c) identifica los riesgos de seguridad de la información: 1) aplica el proceso de evaluación de riesgos de seguridad de información para identificar los riesgos asociados a la pérdida de confidencialidad , integridad y disponibilidad para obtener información dentro del alcance del sistema de gestión de seguridad de la información , y	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
2) identificar a los propietarios de los riesgos ;	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
d) análisis de los riesgos de seguridad de la información : 1) evaluar las posibles consecuencias que resultarían si los riesgos identificados en 6.1.2 c) 1) llegaran a materializarse;	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
2) evaluar la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
3) determinar los niveles de riesgo;	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
e) evalúa los riesgos de seguridad de la información : 1) comparar los resultados del análisis de riesgos a los criterios de riesgo establecidos en 6.1.2 a);	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo
2) clasificación de los riesgos analizados para el tratamiento de riesgos.	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo

La organización conservará información documentada sobre el proceso de evaluación de riesgos de seguridad de información .	Sistema de Gestión para la Reintegración SIGER, módulo Riesgos	En el módulo de riesgos SIGER, se requiere fortalecer la metodología de evaluación, esta actividad deberá estar articulada con la Oficina Asesora de Planeación.
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 a: a) seleccionar las opciones de tratamiento de riesgos de seguridad de información adecuados y teniendo en cuenta los resultados de la evaluación de riesgos;	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo y módulo de riesgo SIGER
b) determinar todos los controles que sean necesarios para implementar la opción de tratamiento de riesgos de seguridad de información(s) elegida;	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo y módulo de riesgo SIGER
c) Comparar los controles determinados en 6.1.3 b) anteriormente, con los del Anexo A y verifique que no hay controles necesarios que se han omitido;	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo y módulo de riesgo SIGER
d) producir una Declaración de aplicabilidad que contenga los controles necesarios (véase 6.1.3 b) y c)) y la justificación de las inclusiones, si estas se están aplicando o no, y la justificación de las exclusiones de controles del Anexo A;	Declaración de aplicabilidad	Declaración de aplicabilidad
e) formular un plan de tratamiento de riesgos de seguridad de la información; y	Mapa de riesgos Direccionamiento estratégico vigencia 2018	En el Manual de Gestión del Riesgo y módulo de Riesgos SIGER, se requiere fortalecer este tema , por lo que esta actividad que debe estar articulada con la Oficina Asesora de Planeación.

f) obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos de seguridad de la información residuales propietarios de los riesgos.	La OAP indica el documento "Respuesta compromisos Gobierno Digital"	En el Manual de Gestión del Riesgo y módulo de Riesgos SIGER, se requiere fortalecer este tema , por lo que esta actividad que debe estar articulada con la Oficina Asesora de Planeación.
La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de información.	Sistema de Gestión para la Reintegración SIGER, módulo Riesgos	En el Manual de Gestión del Riesgo y módulo de Riesgos SIGER, se requiere fortalecer este tema , por lo que esta actividad que debe estar articulada con la Oficina Asesora de Planeación.
6.2. los objetivos de seguridad de información y la planificación para alcanzarlos		
La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
Los objetivos de seguridad de la información deberán: a) ser coherentes con la política de seguridad de la información;	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
b) ser medibles (si es posible);	Documento de despliegue de la Política del SGSI	Documento de despliegue de la Política del SGSI
c) tener en cuenta los requisitos de seguridad de la información aplicable, así como los resultados de la evaluación de riesgos y el tratamiento del riesgo;	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
d) ser comunicados; y	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información, fortalecer la comunicación al interior y partes interesadas. Es importante indicar que hay evidencia de las actividades que adelanta permanentemente la OTI en el Comité Institucional y que el fortalecimiento de la comunicación deberá articularse entre el Grupo de Talento Humano y La Oficina Asesora de Comunicaciones

e) ser actualizados según sea apropiado	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información
La organización conservará información documentada sobre los objetivos de seguridad de la información.	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información. Sistema de Gestión para la Reintegración SIGER,	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información. Sistema de Gestión para la Reintegración SIGER,
Al planificar el marco para alcanzar sus objetivos de seguridad de la información, la organización debe determinar: f) qué se hará;	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional
g) los recursos que serán necesarios;	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional
h) que será responsable;	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional
i) cuando se complete; y	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional
j) cómo se evaluarán los resultados.	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 y los planes operativos alineados con el Plan de acción institucional
7. Apoyo		
7.1. Recursos		
La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.	TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Formulación y ejecución plan de acción, plan anual de adquisiciones, TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información

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;	La OTI a través del contrato 1176 de 2016 ha definido en el Anexo D Personal para la prestación del servicio. Hojas de vida profesionales asociados contrato 1176 de 2016. Hojas de vida colaboradores ARN	Contratos de prestación de servicios, personal de planta, manual de funciones, se requiere verificar este documento y los demás con el fin de asegurar la competencia, por lo que esta actividad se deberá articular entre el Grupo de Talento Humano y el Grupo de Gestión Contractual.
b) asegurar que todas las personas son competentes sobre la base de su caso educación, formación, o experiencia;	La OTI a través del contrato 1176 de 2016 ha definido en el Anexo D Personal para la prestación del servicio. Hojas de vida profesionales asociados contrato 1176 de 2016. Hojas de vida colaboradores ARN-SIGEP Revisar la resolución de cargos	Contratos de prestación de servicios, personal de planta, manual de funciones, se requiere verificar este documento y los demás con el fin de asegurar la competencia; por lo que esta actividad se deberá articular entre el Grupo de Talento Humano y el Grupo de Gestión Contractual.
c) cuando sea aplicable, tomar las acciones para adquirir la competencia necesaria, y evaluar la eficacia de las medidas adoptadas; y	Soportes de capacitaciones realizadas por la UT Open link Maicrotel 2016 a los funcionarios de la ARN ISO 20000, COBIT, ITIL	Contratos de prestación de servicios, personal de planta, manual de funciones, se requiere verificar este documento por lo que esta actividad se deberá articular entre el Grupo de Talento Humano y el Grupo de Gestión Contractual.
d) conservar la información documentada apropiada como evidencia de la competencia.	Programa de gestión documental ARN Control documental contrato 1176 de 2016	Contratos de prestación de servicios, personal de planta, manual de funciones, se requiere verificar este documento y los demás con el fin de asegurar la competencia, por lo que esta actividad se requiere articular con la Subdirección Administrativa.
7.3 Conciencia		
Las personas que realizan un trabajo bajo el control de la organización debe tener en cuenta: a) La política de seguridad de la información	Campañas de sensibilización a través de los canales definidos por la Oficina Asesora de Comunicaciones.	Plan de sensibilización y campañas
b) su contribución a la eficacia del sistema de gestión de seguridad de la información , incluyendo los beneficios de un mejor desempeño de la seguridad de la información; y	Encuesta de seguridad vigencia 2015 Encuesta de seguridad vigencia 2017	Aplicación de Encuesta de Seguridad

c) las consecuencias de que no cumplan con los requisitos del sistema de gestión de seguridad de la información	Manual Del Sistema Integrado De Gestión Para La Reintegración: TH-P-08 Procedimiento control disciplinario verbal TH-P-06 Procedimiento control disciplinario ordinario TI-M-01 Manual del Sistema de Gestión de Seguridad de la Información	Manual de SGSI, SIGER y Procedimientos disciplinarios Manual de contratación
7.4 Comunicación		
La organización debe determinar la necesidad de las comunicaciones internas y externas pertinentes para la sistema de gestión de seguridad de la información que incluye: a) El contenido de las comunicaciones;	Se evidencia Acta de reunión Campaña de sensibilización SGSI 2018	Canales, temática y medios definidos en el documento complementario Matriz de Flujo de Información, sin embargo, se requiere fortalecer el instrumento que permita identificar todo el proceso de comunicación del sistema de información integrado con el SIGER. Esta actividad debe estar articulada con la Oficina Asesora de Planeación. Y Oficina Asesora de Comunicación.
b) cuando comunicarlo;	Se evidencia Acta de reunión Campaña de sensibilización SGSI 2018	Canales, temática y medios definidos en la matriz de flujo de información, sin embargo, se requiere definir un instrumento que permita identificar todo el proceso de comunicación del sistema de información integrado con el SIGER.
c) a quien comunicarlo;	Se evidencia Acta de reunión Campaña de sensibilización SGSI 2018	Canales, temática y medios definidos en la matriz de flujo de información, sin embargo, se requiere definir un instrumento que permita identificar todo el proceso de comunicación del sistema de información integrado con el SIGER.
d) quien debe comunicar ; y	Se evidencia Acta de reunión Campaña de sensibilización SGSI 2021	Canales, temática y medios definidos en la matriz de flujo de información, sin embargo, se requiere definir un instrumento que permita identificar todo el proceso de comunicación del sistema de información integrado con el SIGER.
e) los procesos por los que la comunicación se efectuará	Se evidencia Acta de reunión Campaña de sensibilización SGSI 2022	Canales, temática y medios definidos en la matriz de flujo de información, sin embargo, se requiere definir un instrumento que permita identificar todo el proceso de comunicación del sistema de información integrado con el SIGER.

7.5 Información documentada		
7.5.1 Consideraciones generales		
El Sistema de gestión de seguridad de la información de la organización debe incluir: a) la información documentada requerida por esta Norma Internacional; y	• Políticas y objetivos de seguridad de la información – Manual SGSI • Metodología de evaluación y tratamiento de riesgos – Manual Gestión del Riesgo • Declaración de Aplicabilidad – Declaración • Plan de tratamiento del riesgo – SIGER • Informe sobre evaluación y tratamiento de riesgos – SIGER • Definición de funciones y responsabilidades de seguridad – Manual SGSI • Inventario de activos – Matriz activos de información • Uso aceptable de los activos – Manual SGSI/ Activos de información • Política de control de acceso – Manual SGSI • Procedimientos operativos para gestión TI- Documentos de Gestión de tecnologías de la información. • Política de seguridad para proveedores – Manual SGSI • Procedimiento para gestión de incidentes - Guía para la gestión de incidentes y Procedimiento de gestión de incidentes • Requisitos legales, normativos y contractuales – Nomograma • Registros de capacitación, habilidades, experiencia y calificaciones – Anexo D Contrato 1176 (Personal para la prestación del servicio). Hoja de vida Gestor de Seguridad de la Información y Apoyo Sistema de Gestión de Seguridad de la Información • Registros sobre actividades de los usuarios, excepciones y eventos de seguridad – SOC Procedimientos internos de desarrollo.	Se requiere fortalecer estos temas de documentación articulados con la documentación del SIGER y los procesos de la organización.
b) la información documentada que la organización determina como necesarias para la efectividad del sistema de gestión de seguridad de la información. 1- El tamaño de la organización y a su tipo de actividades, proceso, productos y servicios. 2- La complejidad de los procesos y sus interacciones y. 3- La competencia de personas.		
7.5.2 Creación y actualización		
Al crear y actualizar la información documentada de la organización debe asegurarse apropiado: a) la identificación y descripción (por ejemplo,	GD-P-04 Control de documentos.	Se cumple con la información documentada, Se requiere fortalecer estos temas de documentación articulados con la documentación del SIGER y los procesos de la organización.

un título, fecha, autor, o el número de referencia);		
b) formato (por ejemplo, idioma, versión de software, gráficos) y los medios de comunicación (por ejemplo, papel, electrónico); y	GD-P-04 Control de documentos.	
c) la revisión y aprobación de la idoneidad y adecuación.	GD-P-04 Control de documentos.	
7.5.3. Control de la información documentada		
La información documentada requerida por el sistema de gestión de seguridad de la información y de esta Norma internacional se deben controlar para asegurar: a) que está disponible y adecuada para su uso, donde y cuando sea necesario; y	GD-P-03 Control de registros	Procedimiento de Control de documento y de registros, sin embargo, se recomienda revisión de estos para determinar si cumplimos y si se requiere actualización.
b) está protegido de forma adecuada (por ejemplo, de la pérdida de confidencialidad, uso inadecuado, o la pérdida de la integridad)	GD-P-03 Control de registros	
Para el control de la información documentada, la organización debe responder a las siguientes actividades, según sea el caso; c) acceso a la distribución, recuperación y uso;	GD-P-03 Control de registros	
d) almacenamiento y conservación, incluyendo la preservación de la legibilidad;	GD-P-03 Control de registros	
e) el control de cambios (por ejemplo, control de versiones); y	GD-P-03 Control de registros	
f) la retención y disposición.	GD-P-03 Control de registros	

Información documentada de origen externo, que la organización determina que son necesarios para la planificación y operación del sistema de gestión de seguridad de la información, se debe identificar apropiadamente, y ser controlada.	Nomograma Direccionamiento Estratégico Nomograma Tecnologías de la Información	Se requiere verificación y si es el caso actualización de la documentación de origen externo. Nomograma de los procesos, por lo que esta actividad se debe coordinar con la Oficina Asesora.
8 Operación		
8.1 Planificación y control operacional		
La organización debe planificar , ejecutar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y poner en práctica las acciones determinadas en el apartado 6.2	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018 Manual de Supervisión e interventoría.	16 procesos y se implementa SGSI
La organización debe implementar también planes para lograr los objetivos de seguridad de la información determinada en el apartado 6.2 .	Plan para la implementación del Sistema de Gestión de Seguridad de la Información vigencia 2018	Plan de acción SGSI
La organización debe mantener la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo previsto.	Sistema de Gestión para la Reintegración SIGER	Información SIGER, SIR, TRD y Carpetas compartidas
La organización debe controlar los cambios planificados y examinar las consecuencias de los cambios no deseados , la adopción de medidas para mitigar los posibles efectos adversos , según sea necesario.	La OAP indica el documento "Respuesta compromisos Gobierno Digital"	Procedimiento gestión del cambio TI, se requiere verificar este tema, con el fin de determinar la aplicación de controles.
La organización debe asegurarse de que los procesos externalizados se determinan y controlan .	Manual de Supervisión e interventoría.	Manual de contratación. Se requiere verificar con todos los contratos de la entidad.

8.2 Evaluación de riesgos de seguridad de la información		
La organización debe llevar a cabo las evaluaciones de riesgos de seguridad de la información a intervalos planificados cuando se produzcan o propongan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2 a).	Manual de Gestión del Riesgo	Manual de Gestión del Riesgo y módulo de riesgo SIGER
La organización conservará información documentada de los resultados de las evaluaciones de riesgos de seguridad de información.	Sistema de Gestión para la Reintegración SIGER	Manual de Gestión del Riesgo y módulo de riesgo SIGER
8.3 Tratamiento de riesgos de seguridad de la información		
La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información.	Mapa de riesgos Direccionamiento estratégico vigencia 2018	Módulo de riesgos SIGER, sin embargo se requiere articular todo el plan de tratamiento con los riesgos de los procesos de la entidad, actividad que debe ser coordinada con la Oficina Asesora de Planeación.
La organización conservará la información documentada de los resultados del tratamiento de los riesgos de seguridad de información.	Sistema de Gestión para la Reintegración SIGER, módulo Riesgos	Módulo de riesgos SIGER, sin embargo se requiere articular todo el plan de tratamiento con los riesgos de los procesos de la entidad
9 Evaluación del desempeño		
9.1 Seguimiento, medición, análisis y evaluación		
La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información.	La entidad ha planeado realizar auditorías en el año 2018 Se ha definido indicadores para el SGSI	Se han aplicado instrumentos para el seguimiento, medición, análisis y evaluación, sin embargo; Sin embargo, se requiere presentar dicha información en el Acta de Comité institucional de Gestión y Desempeño como prueba de la revisión por la Dirección respecto a la evaluación del SGSI.

la organización debe determinar que se debe hacer a) seguimiento y que es necesario medir, incluyendo los procesos de seguridad de la información y los controles;	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.. Sin embargo, se recomienda revisar estos instrumentos y determinar cuál sería la medición del SGSI. (Incluyendo que indicadores son los que darán cuenta)
la organización debe determinar b) los métodos de seguimiento, medición, análisis y evaluación, en su caso, para garantizar la validez de los resultados;	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.. Sin embargo, se recomienda revisar estos instrumentos y determinar cuál sería la medición del SGSI. (Incluyendo que indicadores son los que darán cuenta)
la organización debe determinar c) cuando se llevará a cabo el seguimiento y medición;	La entidad ha planeado realizar auditorías en el año 2018 DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.. Sin embargo, se recomienda revisar estos instrumentos y determinar cuál sería la medición del SGSI. (Incluyendo que indicadores son los que darán cuenta)
la organización debe determinar d) quien debe hacer seguimiento y medir;	La entidad ha planeado realizar auditorías en el año 2018 DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.. Sin embargo, se recomienda revisar estos instrumentos y determinar cuál sería la medición del SGSI. (Incluyendo que indicadores son los que darán cuenta)

la organización debe determinar e) cuando se deben analizar y evaluar los resultados de seguimiento y medición; y	La entidad ha planeado realizar auditorías en el año 2018 DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.. Sin embargo, se recomienda revisar estos instrumentos y determinar cuál sería la medición del SGSI. (Incluyendo que indicadores son los que darán cuenta)
la organización debe determinar f) quien debe analizar y evaluar los resultados.	La entidad ha planeado realizar auditorías en el año 2018 DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.. Sin embargo, se recomienda revisar estos instrumentos y determinar cuál sería la medición del SGSI. (Incluyendo que indicadores son los que darán cuenta)
La organización conservará información documentada apropiada como prueba de los resultados del monitoreo y medición.	Sistema de Gestión para la Reintegración SIGER, módulo auditoría. DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.	EM-M-01 Manual de Auditoría Interna DE-M-03 Manual de Seguimiento a la Planeación y Gestión Institucional.. Sin embargo, se recomienda revisar estos instrumentos y determinar cuál sería la medición del SGSI. (Incluyendo que indicadores son los que darán cuenta)
9.2 Auditoría Interna		
La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:	EM-M-01 Manual de Auditoría Interna	Desde el proceso de Gestión de Tecnologías de la información, se viene realizando auditorías, sin embargo se requiere ejecutar auditorías institucional al SGSI, con el fin de verificar su conformidad y posterior seguimiento, medición y análisis.
a) cumple 1) los propios requisitos de la organización para su sistema de gestión de seguridad de la información; y 2) los requisitos de esta norma internacional;	EM-M-01 Manual de Auditoría Interna	Desde el proceso de Gestión de Tecnologías de la información, se viene realizando auditorías, sin embargo se requiere ejecutar auditorías institucional al SGSI, con el fin de verificar su conformidad y posterior seguimiento, medición y análisis.

b) se ha implementado y mantiene de manera eficaz.	EM-M-01 Manual de Auditoría Interna	Desde el proceso de Gestión de Tecnologías de la información, se viene realizando auditorías, sin embargo se requiere ejecutar auditorías institucional al SGSI, con el fin de verificar su conformidad y posterior seguimiento, medición y análisis.
La organización debe: c) planificar, establecer, implementar y mantener un programa(s) de auditoría, incluida la periodicidad, los métodos, responsabilidades, requisitos de planificación y presentación de informes. El programa(s) de auditoría deberá tener en cuenta la importancia de los procesos en cuestión y los resultados de auditorías anteriores;	EM-M-01 Manual de Auditoría Interna	Desde el proceso de Gestión de Tecnologías de la información, se viene realizando auditorías, sin embargo se requiere ejecutar auditorías institucional al SGSI, con el fin de verificar su conformidad y posterior seguimiento, medición y análisis.
d) definir los criterios de auditoría y el alcance de cada auditoría;	EM-M-01 Manual de Auditoría Interna	Desde el proceso de Gestión de Tecnologías de la información, se viene realizando auditorías, sin embargo se requiere ejecutar auditorías institucional al SGSI, con el fin de verificar su conformidad y posterior seguimiento, medición y análisis.
e) selección de los auditores y realizar auditorías que garanticen la objetividad e imparcialidad del proceso de auditoría;	EM-M-01 Manual de Auditoría Interna	Se requiere fortalecer los auditores de certificación de SGSI.
f) asegurarse de que los resultados de las auditorías se reportan a la gerencia pertinente; y	EM-M-01 Manual de Auditoría Interna	Comité de coordinación de control interno y los informes que se presentan a la Dirección y líder del proceso.
g) retener información documentada como pruebas del programa (s) de auditoría y los resultados de la auditoría.	EM-M-01 Manual de Auditoría Interna	Módulo de auditorías SIGER
9.3 Revisión por la dirección		
La alta dirección debe revisar el sistema de gestión de seguridad de las organizaciones de información a intervalos	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño	A través del líder del proceso de Tecnologías de la Información se realiza presentación de avances del SGSI, sin embargo, es importante realizar la Revisión por

planificados para asegurarse de su conveniencia, adecuación y eficacia.		la Dirección según requisito de la norma ISO 27001. De igual forma, tiene un recurso compartido (COMINS) que es gestionado por la Oficina Asesora de Planeación y allí se comparte la información con los integrantes del Comité.
La revisión por la dirección debe incluir la consideración de: a) el estado de las acciones de las revisiones por la dirección previas;	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño	A través del líder del proceso de Tecnologías de la Información se realiza presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001
b) los cambios en los problemas externos e internos que son relevantes para el sistema de gestión de seguridad de la información;	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño y Actas de las mesas de Seguridad.	A través del líder del proceso de Tecnologías de la Información se realizar presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001
c) la retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en: 1) las no conformidades y acciones correctivas;	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño	A través del líder del proceso de Tecnologías de la Información se realizar presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001
2) seguimiento y medición a los resultados;	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño y Actas de las Mesas de Seguridad.	A través del líder del proceso de Tecnologías de la Información se realizar presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001
3) resultados de las auditorías; y	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño	A través del líder del proceso de Tecnologías de la Información se realizar presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001

4) el cumplimiento de los objetivos de seguridad de la información;	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño y Actas de las Mesas de Seguridad.	A través del líder del proceso de Tecnologías de la Información se realizar presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001
d) la retroalimentación de las partes interesadas;	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño	A través del líder del proceso de Tecnologías de la Información se realizar presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001
e) los resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos; y	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño	A través del líder del proceso de Tecnologías de la Información se realiza presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001
f) las oportunidades de mejora continua.	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño y Actas de las Mesas de Seguridad.	A través del líder del proceso de Tecnologías de la Información se realiza presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001. También se requiere documentar la mejoras en el SIGER, como evidencia de su mejoramiento
Las salidas de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y de cualquier necesidad de cambios en el sistema de gestión de seguridad de la información.	Manual del Sistema Integrado de Gestión para la Reintegración Actas de Comité Institucional de Gestión y Desempeño y Actas de las Mesas de Seguridad.	A través del líder del proceso de Tecnologías de la Información se realiza presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001
La organización conservará información documentada como evidencia de los resultados de las revisiones por la dirección.	Actas de Comité Institucional de Gestión y Desempeño	A través del líder del proceso de Tecnologías de la Información se realiza presentación de avances del SGSI, sin embargo es importante realizar la Revisión por la Dirección según requisito de la norma ISO 27001

10. Mejora		
10.1 No conformidad y Acción Correctiva		
Cuando se produce una no conformidad, la Organización debe; a) reaccionar a la no conformidad, y según sea el caso: 1) tomar medidas para controlar y corregir; y 2) hacer frente a las consecuencias;	EM-P-01 Procedimiento Gestión de Acciones Correctivas, Preventivas y de Mejora	Se han formulados planes de mejoramiento, sin embargo se requiere establecer estos requisitos institucionalmente.
b) evaluar la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o se producen en otros lugares, a través de: 1) la revisión de la no conformidad; 2) determinar las causas de la no conformidad; y 3) determinar si existen incumplimientos similares o podrían producirse;	EM-P-01 Procedimiento Gestión de Acciones Correctivas, Preventivas y de Mejora	Se han formulados planes de mejoramiento, sin embargo se requiere establecer estos requisitos institucionalmente.
c) Implementar cualquier acción necesaria	EM-P-01 Procedimiento Gestión de Acciones Correctivas, Preventivas y de Mejora	Se han formulados planes de mejoramiento, sin embargo se requiere establecer estos requisitos institucionalmente.
d) revisar la eficacia de las medidas correctivas adoptadas; y	EM-P-01 Procedimiento Gestión de Acciones Correctivas, Preventivas y de Mejora	Se revisa al eficacia de los planes de mejora, sin embargo se requiere establecer estos requisitos institucionalmente.
e) realizar cambios en el sistema de gestión de seguridad de la información, si es necesario.	EM-P-01 Procedimiento Gestión de Acciones Correctivas, Preventivas y de Mejora	Se revisa al eficacia de los planes de mejora, sin embargo se requiere establecer estos requisitos institucionalmente.
Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.	EM-P-01 Procedimiento Gestión de Acciones Correctivas, Preventivas y de Mejora	Se revisa al eficacia de los planes de mejora, sin embargo se requiere establecer estos requisitos institucionalmente.
La organización conservará información documentada como evidencia de:	Sistema de Gestión para la Reintegración SIGER, módulo Plan de mejoramiento	Módulo de mejora SIGER, sin embargo se requiere ajustar dicho aplicativo, esta actividad se debe articular con la Oficina Asesora de Planeación.

f) la naturaleza de las no conformidades y de cualquier acción tomada posteriormente, y	Sistema de Gestión para la Reintegración SIGER, módulo Plan de mejoramiento	Módulo de mejora SIGER, sin embargo se requiere ajustar dicho aplicativo.
g) los resultados de cualquier acción correctiva.	Sistema de Gestión para la Reintegración SIGER, módulo Plan de mejoramiento	Módulo de mejora SIGER, sin embargo se requiere ajustar dicho aplicativo.
La organización debe mejorar continuamente la convivencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.	EM-P-01 Procedimiento Gestión de Acciones Correctivas, Preventivas y de Mejora	Se debe realizar la Revisión por la dirección para tomar dichas acciones

5.1.3 Revisión de los tiempos de respuesta de las PQRS-D

Con el fin de validar el cumplimiento en los tiempos de respuesta de las PQRS-D, recibidas por la OTI, se procedió a tomar la base de PQRS-D generada por el Grupo de Atención al Ciudadano correspondiente al Primer Semestre de la Vigencia 2018 así:

Fecha de registro	Tipo	Área Responsable	Días hábiles permitidos respuesta	Fecha Vencimiento	Fecha Terminación de la gestión	Días trámite con fecha de Terminación de la gestión	Caso Vencido / A tiempo
27/02/2018	Peticiones de Información	Oficina de Tecnologías de la Información	10	13/03/2018	5/03/2018	4	A Tiempo
5/06/2018	Petición	Oficina de Tecnologías de la Información	15	27/06/2018	19/06/2018	9	A Tiempo
6/06/2018	Petición	Oficina de Tecnologías de la Información	15	28/06/2018	22/06/2018	11	A Tiempo

Como se evidencia, se tienen todos los registros con estado “A Tiempo”; de igual manera se efectuó revisión a usuario de la Jefe de Oficina de Tecnologías de la Información de SIGOB, donde se logró observar que no se tienen ninguna comunicación por tramitar y como resultado de revisión de las solicitudes de PRQs ha sido acorde a los tiempos de respuesta; se recomienda continuar manteniendo el buen habito de contestar las solicitudes dentro de los tiempos respectivos.

5.1.4 Eficacia de Planes de Mejoramiento cerrados a cargo del proceso PM-16-00094 (AUD-1668)

Hecha la revisión del SIGER, y con el acompañamiento de los coordinadores de la OTI, desde el día 28 de noviembre de 2018 hasta el día 6 de diciembre de 2018 se revisó la eficacia de un (1) Plan de Mejora que cuenta con 19 hallazgos y contenidos en 20 acciones discriminadas de la siguiente manera:

- **NO CONFORMIDAD 1**: "Se observó que los riesgos de TI son de carácter muy general para toda la función y que el cumplimiento de las medidas o acciones sobre su tratamiento tiene una periodicidad anual y en otros casos semestral, lo que no permite ejercer un monitoreo más riguroso sobre la evolución del manejo de dichos riesgos".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir descrita así:

  - ✓ **Acción 1.**" Evaluar cada riesgo para determinar las acciones y la periodicidad".

  En el momento de cierre de la acción se evidencia en el SIGER que se registra con mejor periodicidad el seguimiento a los riesgos de la Oficina de Tecnologías de la Información.

  Ahora bien, en la revisión del seguimiento de riesgos de la Vigencia 2018, se observa que se continua con un registro periódico de seguimiento a los riesgos que se tienen planteados en el Mapa de Riesgos de la OTI. Teniendo en cuenta lo anterior, se considera **Eficaz** esta acción.

- **NO CONFORMIDAD 2**: "En el momento de nuestra revisión se evidencia que aunque se cuenta con un Datacenter externo, con muy buenas características de seguridad y operación y está en etapa final de alistamiento y aseguramiento de un centro alterno de operaciones fuera de Bogotá, no se cuenta con un plan de continuidad de negocios para la ACR, (corresponde al denominado Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP)), que incluya el impacto (BIA) desde el punto de vista de recursos humanos, físicos y financieros, debidamente documentado, actualizado y probado".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Remitir requerimiento al Comité Institucional de Desarrollo Administrativo para su consideración".

  En su momento se generó el Memorando registrado con el número MEM16-012639 fechado el día 21 de noviembre de 2016 y dirigido al Secretario General; el mismo tenía como fin hacer conocer los hallazgos que son de orden transversal a la Agencia, este documento fue la evidencia con la que se procedió al cierre de la acción. A la fecha, el tema de asignación de Continuidad del Negocio ha sido delegado al Subdirector Administrativo de la ARN quien se encuentra conociendo el tema y trabajando para dar continuidad al plan de trabajo establecido; en este punto es importante aclarar que esta asignación no se ha realizado formalmente pues se encuentra en proceso de reglamentación.

  De igual manera se evidencia que, por parte de la Subdirección Administrativa, se ha venido trabajando en la identificación de algunos riesgos que podrían generar problemas serios para el cumplimiento del objeto de la Agencia.

  Teniendo en cuenta lo anterior, se observa que la actividad para cumplir con esta acción es **Eficaz**; sin embargo, se recomienda al ser un tema transversal que la Dirección de la Agencia debe asumir en el tema de seguridad de la información y

continuidad del negocio con el fin primordial, de mitigar los riesgos que a futuro puedan presentarse en la Agencia; es por ello que, el grupo de trabajo que liderará estos temas deberán contar con la participación un representante de las diferentes áreas de la Agencia, entre ellas OTI.

- **NO CONFORMIDAD 3: "**Se encuentran definidos como usuarios en producción, tres funcionarios desarrolladores que tienen privilegios de lectura y escritura sobre la base de datos de producción del aplicativo SIR. Estos usuarios son: Claudiaposada, Julianmadrid, Jerssonbetancourt".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Eliminar los permisos de los funcionarios desarrolladores con privilegios de escritura sobre las bases de datos en producción de todos los aplicativos y portales".

  En su momento esta acción fue reportada y cerrada con evidencias de correos electrónicos a los desarrolladores; en los mismos se notifica el nuevo perfil en las bases de datos. En la actualidad, se procede a hacer una prueba aleatoria de algunos usuarios desarrolladores como:

  - BD CRM- Claudia Posada y Diana Bobadilla no tiene permisos; Mariana Moreno y Mariano Carreno León, solo tienen permisos de lectura.
  - BD DWH – Claudia Posada, Hinna Luz Garavito, Diana Bobadilla, Norberto Pupo solo tienen permisos de lectura.
  - BD Huellas Sipas (Arpa) – Claudia Posada, Norberto Pupo, Hinna Luz Garavito Mariana Carreño y Diana Bobadilla solo tienen permisos de lectura y Mariana Moreno no tiene permisos.
  - BD AKRAB/SHI (Intranet), no hay permisos para los desarrolladores de la Entidad.

  Después de la revisión realizada en esta auditoría se considera que la acción es **Eficaz.**

- **NO CONFORMIDAD 4: "**Se observó que no se tiene implementada la auditoría sobre las bases de datos".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Establecer Plan de trabajo para la implementación de la auditoría sobre las bases de datos de producción".

  En su momento se cerró la acción con la generación de un documento denominado "Plan de Auditoría de Bases de Datos", en este se observa un (1) plan de trabajo. A la fecha se evidencia que se implementaron las auditorías a las bases de datos de: SIR (LYNX\SIR) (Log exitosos y log fallidos, modificación de estructuras).

  Por otra parte, se presentan informes mensuales; para este caso se evidenció que en los meses de septiembre y octubre de la Vigencia 2018 se reportan novedades JOBS, asociadas a las tareas del negocio del SIR, los cuales son informados al programador encargado del módulo al cual se encuentra vinculada dicha actividad.

En el periodo anterior, no se evidenciaron más informes debido a la rotación del personal, por la posesión del personal de carrera.

En esta auditoría se inició la prueba en la base de datos de prueba y desarrollo y ahora en la de producción, desde el mes de septiembre, con el fin de que no afecte el desempeño; los resultados arrojados evidencian que esta medida ha funcionado sin afectar el servicio ofrecido a los diferentes usuarios. Por lo anterior se considera que la acción es **Eficaz** a pesar que, durante unos meses, no se realizó el respectivo informe dado que los resultados arrojados son satisfactorios y no hay alarmas graves.

- **NO CONFORMIDAD 5: "**Para la instancia del aplicativo SIGOB se evidenció que para cada funcionario que va a ingresar en este aplicativo, se crea un usuario directamente en la base de datos".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Solicitar mediante correo electrónico al supervisor del contrato de SIGOB gestionar un ajuste en el software para que no se creen tantos usuarios en la base de datos como funcionarios que ingresan al aplicativo".

  Se envió un correo, por parte de la OTI, al supervisor del contrato de SIGOB en el que informaba que estaba pendiente por revisar qué se adelantó con respecto a esta solicitud. El día 26 de diciembre de 2016 se envió correo por parte de la Jefe de la OTI a la encargada del Grupo de Gestión Documental; posteriormente, en entrevista verbal se manifestó que en su momento se remitió correo al Programa de las Naciones Unidas para el Desarrollo (PNUD), pero informan que las respuestas se ofrecieron de manera verbal a la Subdirectora Administrativa del momento en la Entidad; la respuesta ofrecida es que el ajuste solicitado no se podría realizar. De otra parte, la Directora de OTI aportó evidencias de las gestiones realizadas con respecto al tema y en respuesta a ello se encuentra a la espera de las actualizaciones que están pendientes por realizar con el fin de revisar si el tema de creación de usuarios se encuentra ya cubierto. Por lo anterior, se considera que la acción es **Eficaz,** en temas de gestión al respecto; sin embargo, por ser un aplicativo de un tercero se encuentra sujeto a que el dueño de este aplicativo aplique las mejoras requeridas.

  Finalmente, en la presente auditoría se aprovechó y se revisó el tema de administración de usuarios; en la revisión se constata la presencia de más de 20 registros de personas retiradas de la Entidad que aún se encuentran activas en la base de datos de usuarios del Sistema de Información y Gestión para la Gobernabilidad (SIGOB); teniendo en cuenta lo anterior se requiere fortalecer el tema de administración de usuarios.

- **NO CONFORMIDAD 6: "**En el momento de nuestra revisión se pudo comprobar que a pesar que se realizan actividades de la administración, monitoreo y mantenimiento de las bases de datos, no existen documentos formales sobre las políticas y procedimientos relacionadas con funciones realizadas por el funcionario encargado de ejecutar estas tareas".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

- ✓ **Acción 1:** “Elaborar un documento de trabajo interno del área que incluya la descripción de las actividades de administración, monitoreo y mantenimiento de las bases de datos de la ACR”.

En su momento se elaboró el documento “A1 Actividades de Administración Base de Datos ACR V1 – abril de 2017”, el cual se ha venido aplicando; sin embargo, como parte del proceso de provisión de los cargos en la carrera administrativa, y cuando la persona asignada a esta labor surta el periodo prueba, se efectuarán los ajustes y/o actualización a que haya lugar con la persona que quedará a cargo de esta actividad. Por lo anterior, se considera **Eficaz** la acción.

- ❖ **NO CONFORMIDAD 7:** “De acuerdo a lo evidenciado actualmente no se cuenta con un mecanismo de cifrado de las bases de datos en su totalidad. Sin embargo, se pudo establecer que si hay alguna información que se cifra, en particular cuando va dirigida a entidades externas”.

Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

- ✓ **Acción 1:** “Establecer lineamiento para cifrado de información en la ACR, lo cual se incluirá en el manual de seguridad de la información de la ACR”.

Se evidencia que se tiene actualizado el Manual de Seguridad en su versión número seis; específicamente en el numeral 3.15 (Políticas de Criptografía) se describe el detalle de lo tratado en este tema, el mismo se está aplicando para la transferencia de información con entidades como: Fiduprevisora (pagos Apoyo Económico para la Reintegración); Ministerio de Salud; Ministerio del Interior; Banco Caja Social (ofrece servicios financieros a la población objeto de la Agencia). Por otra parte, se realizan consultas que hacen los fiscales a través de SARA, Centro de Memoria Histórica y Asobancaria.

Se manifiesta que la entidad ya cuenta con un 15% de convenios cubiertos en relación al cifrado de la información y además se tiene previsto que, para la Vigencia 2019, se aumente un 5% dado que se encuentra sujeto a la aprobación de la contraparte del convenio. Por lo anterior, se observa que la acción es **Eficaz**; sin embargo, se recomienda continuar en la ejecución de esta labor con el fin de mantener la transferencia de información segura de la población objetivo de la Agencia.

- ❖ **NO CONFORMIDAD 8: “**Se realizó una comprobación en el módulo de seguridad del aplicativo SIR, en el cual se evidencia que existen los siguientes usuarios asignados al rol de administrador: CRM Implementador Production, Gloria Isabel Montoya Navarro, Jaime Eduardo Santafé Patino, Julian Andrés Madrid Caballero, Luis Alberto Duarte Moreno, Soporte SIR”.

Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

- ✓ **Acción 1:** “Revisar los permisos para los ajustes correspondientes y la política para asignación del rol de Administrador del SIR, la cual se consignará en el catálogo de servicios en el numeral 6.1.8. Roles y Responsabilidades SIR”.

En su momento se elaboró un documento denominado “Catálogo de Servicios V1”; hoy día, este se encuentra en su versión número 9 fechado en agosto de 2018; en el numeral 5.1.8. (Roles y Responsabilidades) de este texto se describen los roles y responsabilidades de los usuarios con respecto al aplicativo SIR.

Igualmente, se establece una tabla de privilegios con los diferentes usuarios autorizados y con permisos en el SIR. De acuerdo a esta tabla se hizo una verificación de los usuarios creados en el Aplicativo SIR y se observan como Usuarios Administradores del Sistema a: Deisy Liliana Catano Albarracin; Julian Andrey Puerto Corral y Oscar Fernando Romero Villanueva, usuarios que no tienen el rol de desarrolladores.

Se generó una consulta y lo cual arrojó que existen un total de 1252 usuarios del SIR, por lo que se recomienda hacer la depuración de roles de acuerdo a las funciones de los colabores de la Entidad, es importante continuar depurando esta información y garantizar la seguridad de la información.

Después de la revisión realizada en esta auditoría se comprueba que esta acción es **eficaz**.

- **NO CONFORMIDAD 9:** “Se evidenció que la Entidad no dispone de políticas ni procedimientos documentados, dirigidos a administrar y monitorear en forma controlada y segura la creación, inactivación y eliminación de las cuentas de usuario registradas en los sistemas de información. Se identificaron funcionarios y contratistas que están retirados definitivamente o se encuentran en vacaciones, que están activos en el Dominio de Windows Server 2012”.

Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

- ✓ **Acción 1:** “Revisar el procedimiento de terminación anticipada y liquidación de contratos, a fin de garantizar la devolución y control de elementos informáticos intangibles (licencias), y administración de usuarios (creación y eliminación), lo cual se verá reflejado en acta de reunión”.

Al respecto, se hizo una prueba aleatoria a los usuarios que existen en la base de datos de SIR y allí se hizo revisión de aleatoria a casos así:

- A una (1) persona que trabaja con el tema de Mambrú que de ser funcionaria pasó a contratista, le liquidan un contrato y le efectúan otro; dentro de las solicitudes recibidas a Soporte no se ubica la solicitud de usuario en SIR para esta persona. No se encuentra el correo de solicitud de permisos de SIR.
- Se revisa la base de usuarios de SIGOB y allí se identifican ex – funcionarios de la Agencia, pero que se encuentran activos en este Sistema.
- En la base de datos Aladino de la Agencia, en una pasada auditoría realizada al Grupo de Almacén e Inventarios, se evidenció que existen usuarios activos cuando estos ya no trabajan en la Entidad.

Teniendo en cuenta lo anterior, se considera **Eficaz** esta acción, dado que se evidencia por parte de la OTI que se han aplicado acciones con el fin de depurar la base de usuarios; sin embargo se recomienda que desde la Dirección se emitan directrices al respecto, tomando concientizando a todos que el reporte a tiempo y las medidas con las personas que salgan

de licencia o vacaciones afectan la seguridad de la información y los riesgo que detecte la entidad, por lo que este tema se convierte en una acción transversal a la entidad.

NO CONFORMIDAD 10: "Se observó que en el Directorio Activo se tiene como política de bloqueo = 0, lo anterior deriva en la posibilidad de poder realizar intentar accesos de forma ilimitada para ingresar a la red sin la autorización requerida".

Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

- ✓ Acción 1: "Verificar la pertinencia de esta recomendación y realizar las recomendaciones que apliquen en el manual de seguridad de la información".

La OTI optó por configurar, dentro de sus políticas del Directorio Activo, que el usuario se bloquee después de cinco intentos; lo anterior generó que los casos de soporte se aumentaran y es por ello que se habilitó la política configurada en el mencionado Directorio; este se configuró con 50 intentos, una vez supere este número se bloquea el usuario.

De igual manera, se tienen configurados en la red otros dispositivos que ayudan a la identificación de los usuarios que ingresan a la red; esto se ha venido fortaleciendo y, hasta el momento, no se ha identificado la suplantación de usuarios. En la revisión hecha para esta auditoría se evidenció que la Oficina efectúa más campañas acerca del uso del correo institucional en los dispositivos móviles que no son de la Entidad y que, además, es responsabilidad del usuario su administración y seguridad de la información que allí se maneje.

Por lo anterior, se considera **Eficaz** la acción.

- ❖ **NO CONFORMIDAD 11**: "En el momento de nuestra revisión se observó que, tras las pruebas de penetración, existen 10 vulnerabilidades en progreso de remediación y 4 aún pendientes por resolver".

Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

- ✓ **Acción 1:** "Realizar seguimiento a las acciones de remediación lo cual se verá reflejado en el documento respectivo".

Se revisa el caso de la herramienta de gestión "Aranda" de número Q37859 de Carolina Cetina – Cundinamarca Boyacá fechado el 30 octubre de 2018. Este sistema registra por número de intentos de ingreso al sistema y el respectivo informe de inconvenientes; en el caso mencionado se informa que, por intentos de ingreso al Sistema, se vuelve reiterativo el tema de esta funcionaria. En el mismo orden de ideas se verifica el caso del Sistema "Aranda" de número Q38753 correspondiente al usuario Juan Carlos Estupiñán quien, también, reporta bloqueo por usuario por intentos de ingreso al Sistema.

Teniendo en cuenta la revisión hecha en esta auditoría se considera **Eficaz** la acción.

- **NO CONFORMIDAD 12**: “Se comprobó que existe un usuario en el área de seguimiento que ejecuta comandos SQL para la consulta de información de la base de datos de réplica de SIR (ACRP_MSCRM) la cual está en el nodo CETUS/DWH”.

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** “Crear formato para manejo de cuentas especiales y diligenciamiento para colaboradores con ese perfil”.

  En la auditoría se evidencia que se tienen cuatro (4) llaves para cuatro (4) funcionarios y, en esa caja de seguridad, se verificaron 10 sobres debidamente sellados con los usuarios de diferentes servicios tecnológicos.

  El formato contiene la fecha; el servicio autorizado; nombre y cargo; usuario y clave, firma y párrafo de seguridad de la información.

  Se evidencia, también, un correo de la doctora María Paola Molina Guerrero autorizando al usuario Juan Dueñas. Por lo anterior se considera **eficaz** la acción; sin embargo, se recomienda continuar monitoreando y conocer más sobre el tema con el objetivo de tener un usuario suscrito a la base de datos por parte de los procesos misionales.

- **NO CONFORMIDAD 13**: “En la revisión del proceso de copias de seguridad, se observó que no se cuenta con un procedimiento formal para la restauración”.

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** “Elaborar procedimiento interno para restaurar copias de seguridad e implementarlo. El procedimiento quedará descrito en el documento respectivo”.

  Al respecto se informa que se replanteó el documento en septiembre de 2018; el mismo cuenta con una nueva estructuración como tipos de copias de respaldo de aplicativos y de bases de datos; las herramientas para la generación de copias de respaldo de la información; disposición de recursos para las copias de seguridad; creación y generación de copias de respaldo, denominación y nomenclaturas de las copias de respaldo.

  Igualmente, se evidencia el caso de número Q39364 (Adriana Rojas), para la recuperación de archivos en la carpeta compartida; al respecto, se evidenció que un (1) funcionario de esta dependencia eliminó estos archivos por lo que se procedió con los ajustes de los permisos necesarios.

  Por otra parte, se verifica el caso de la herramienta “Aranda” de número Q36510 y relacionado con la recuperación de archivos de carpetas compartidas; este fue solicitado por el Grupo de Gestión Contractual y cumplió con los protocolos respectivos.

  En el mismo orden de ideas, se evidencia otro caso, vìa correo electrónico, para la recuperación de correos a Ligia Fernández, pero este no cuenta con el caso de soporte de la herramienta “Aranda”.

Después de la auditoría realizada se considera **Eficaz** la acción; sin embargo, se recomienda reforzar el tema de registro de casos a través de la herramienta “Aranda”.

- ✓ **Acción 2:** “Realizar y documentar las pruebas de restauración de backups”.

Después de realizada la auditoría se verifica que el formato se mantiene en la carpeta de nombre: “Grupo de Infraestructura\Software\ Backups\ Restauraciones”, en ella se cuenta con evidencia de cinco (5) formatos donde se evidencia la tarea de restauración.

Teniendo en cuenta lo anterior se considera **Eficaz** la acción.

- ❖ **NO CONFORMIDAD 14**: “Se observó que no existen cronogramas ni manejo formal como proyecto para desarrollos de gran complejidad”.

Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

- ✓ **Acción 1:** “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)”.

Se verificó el caso de número Q39832 registrado en la herramienta “Aranda”: “Modificación requisitos y reglas para Aprobación de un BIE; de esta solicitud se registraron tres (3) tareas en Team Foundatión Server; al respecto se generaron las tareas 2979 para documentar el análisis y requerimiento; 2980 para elaborar el desarrollo; y 2843 para la realización de pruebas.

Se verificó el caso de número Q38094 registrado en la herramienta “Aranda” “Para registrar los beneficios jurídicos de la Ley 1820”; al respecto, se generaron las tareas 2964 para la documentación de análisis y 2965 para ejecutar el desarrollo.

En lo relacionado con el caso de número Q20536 registrado en la herramienta “Aranda” y fechado el día 26 de febrero de 2018), “Control de cambios de ajuste a acuerdo de contribución” se generaron las tareas 2495 para análisis y 2496 para desarrollo. El mencionado caso se terminó el día 9 de marzo, pero se encontró pendiente el caso de pruebas.

Para el caso de numero Q22305 registrado en la herramienta “Aranda” y fechado el día 04 de abril de 2018 se crearon las tareas 2580 para el análisis; 2582 para el desarrollo; y 2583 para la realización de pruebas.

Frente al caso de número Q2214 registrado en la herramienta “Aranda” el día 19 de abril de 2018 “Ajuste de Alertas en el proceso Administrativo Sancionatorio” se crearon las tareas 2073 para análisis y 2075 para desarrollo.

Al finalizar la revisión de los casos no se evidenció en todos ellos la realización de las diferentes etapas de desarrollo como son análisis, desarrollo, pruebas y producción; teniendo en cuenta lo anterior se considera **Ineficaz** esta acción.

- **NO CONFORMIDAD 15**: "En los desarrollos y/o mantenimiento de software, se utilizan datos reales para las pruebas, lo cual dada la naturaleza de la agencia y el tipo de información (sensible) de la ACR, se puede ver afectada la confidencialidad de los datos".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Establecer procedimiento para el manejo de datos en ambiente de pruebas, lo cual quedará registrado en el documento: Procedimientos internos de desarrollo y será socializado con el Grupo de Sistemas de Información mediante acta".

  Se elaboró un documento de trabajo denominado "Procedimientos internos de desarrollo Grupo de Sistemas de Información V-5" fechado en septiembre de 2018.

  Este documento, en su numeral 5 (Plan de Calidad de Software) y en el subnumeral y 5.6. "Manejo de Datos en Ambientes de Pruebas", describe el proceso para contar con los datos necesarios en los ambientes de pruebas; se indica en este texto, igualmente, que se realiza copia de la base de datos del ambiente productivo cada cuatro (4) meses, o cuando el grupo de desarrollo lo considere necesario para lo cual se realiza solicitud al Administrador de Bases de Datos a través de SoporteACR, la herramienta establecida para tal fin.

  Dentro del procedimiento de replicar la base de datos de producción a pruebas se realizará una reducción de esta excluyendo documentos adjuntos relacionados a las PPR; igualmente, se realiza un *shrink* y se correrá un procedimiento encargado de enmascarar o modificar los datos sensibles de las PPR como son nombre, identificación y datos de ubicación. Adicionalmente, se correrá procedimiento para modificar los new_name de las entidades donde se reflejan los datos de las PPR.

  A raíz de la revisión realizada se pueden evidenciar los controles que se han definido para los datos en la base de pruebas, lo cual ha funcionado y se ha maneja de la mejor manera por parte de los programadores. Por lo anterior se considera **Eficaz** esta acción.

- **NO CONFORMIDAD 16**: "No hay un Quality Assurance en el ciclo de vida del software".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Fortalecer el procedimiento interno de desarrollo para evidenciar el aseguramiento de calidad durante el ciclo de vida del software, lo cual quedará registrado en el documento: Procedimientos internos de desarrollo y será socializado con el Grupo de sistemas de Información mediante acta".

  En el documento de trabajo denominado "Procedimientos internos de desarrollo Grupo de Sistemas de Información" V-5 de septiembre de 2018, específicamente en su numeral 5. "Plan de Calidad de Software", se evidencian los lineamientos establecidos con el fin del Aseguramiento de Calidad de Software junto con los respectivos lineamientos en la etapa de pruebas; manejo de datos en ambiente de pruebas y los usuarios definidos en ambientes de pruebas. Igualmente, en este segmento del manual

en mención, se observa que se abarca lo referente a la calidad del Software y posterior puesta en producción lo cual, efectivamente, garantiza el ciclo de vida del software; es de resaltar que este documento se ha venido actualizando a medida que la Entidad requiera los ajustes necesarios. Por lo anterior se considera que esta acción es **Eficaz.**

- **NO CONFORMIDAD 17:** "En el procedimiento de desarrollo o modificación a programas, se utilizan usuarios finales en las pruebas del aplicativo en un ambiente similar al de producción, en el cual dichos usuarios finales, no se retiran posterior a las pruebas".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Establecer procedimiento para el manejo de usuarios para ambiente de pruebas, lo cual quedará registrado en el documento: Procedimientos internos de desarrollo y será socializado con el Grupo de Sistemas de información mediante acta".

  En el documento de trabajo denominado "Procedimientos internos de desarrollo Grupo de Sistemas de Información V-5" fechado en septiembre de 2018, específicamente en en su numeral 5. "Plan de Calidad de Software" y en el subnumeral 5.7. "Usuarios de Prueba", se evidencia que se han creado usuarios genéricos para realizar las pruebas; asimismo, se denota el manejo y cambio de clave de estos usuarios.

  Por lo anteriormente mencionado se considera **Eficaz** esta acción.

- **NO CONFORMIDAD 18**: No hay una aplicación de un modelo o metodología de gestión de proyectos tipo PMI".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Fortalecer los conocimientos de la OTI en gestión de proyectos - PMI, lo cual se evidenciará con las certificaciones de asistencia de 3 funcionarios al curso de Dirección de Proyectos Alineado al PMBOK Guide edition 5".

  En su momento se dictó una (1) capacitación sobre *Project Management Institute* (PMI) a la cual acudieron cerca de 20 funcionarios de la ARN; sin embargo, por el aprovisionamiento del personal de carrera, muchos de los que tomaron el curso ya no se encuentran en laborando Agencia.

  Ahora bien, en la Coordinación de Sistemas, se manejan la metodología *Scrum* (método para trabajar en equipo a partir de iteraciones o *Sprints*), por el tipo de casos a manejar en la Entidad, pues se tiene como regla documentar todo situación que se presenta, pero, al momento, no se lleva a cabo un proceso bajo la metodología PMI.

  La metodología *Scrum* se basa en la calidad del resultado y el conocimiento táctico de los ejecutores; los *sprint* son tareas rápidas a realizar. La mencionada metodología se verifica, en su desarrollo, a través de reuniones con el equipo de trabajo realizadas con el fin, primordial, de hacer seguimiento a las tareas designadas; así las cosas, el

Coordinador de Sistemas realiza esta actividad una (1) vez a la semana en la OTI para revisar los avances presentados.

Teniendo en cuenta la anterior revisión se considera **Eficaz**, esta acción; sin embargo, se recomienda que se implemente la metodología de trabajo PMI.

- **NO CONFORMIDAD 19:** "Se pudo establecer con el coordinador de sistemas de información de la OTI, que a pesar que la entidad ha establecido el acompañamiento de la OTI para cualquier aspecto que involucre adquisición de elementos tecnológicos, software, hardware o similares; desde las áreas usuarias, no siempre se solicita ese acompañamiento".

  Este hallazgo se encuentra registrado con una (1) acción a cumplir así:

  - ✓ **Acción 1:** "Remitir requerimiento mediante memorando al Comité Institucional de Desarrollo Administrativo, para su consideración, en los temas transversales detectados en la auditoría interna".

  Como parte de esta acción, la Entidad, ha comprendido la importancia de contar con el acompañamiento y criterio técnico en los productos y servicios a adquirir; en esta auditoría se evidencia correo electrónico de fecha noviembre 15 de 2018 en donde se evidencia el acompañamiento para el Software "SISGESTIÓN".

  Por otra parte, se verifican los correos electrónicos del 9 de agosto y del 5 de diciembre de 2018 en donde se evidencian los comentarios sobre la ficha técnica y el concepto técnico de Control de Acceso.

  Por lo anteriormente revisado se considera **Eficaz** esta acción.

5.2 FORTALEZAS

Dentro del ejercicio de auditoría practicada al proceso de Gestión de Tecnologías de la Información se identificaron las siguientes conformidades, las cuales son informadas en el momento del cierre de la auditoría:

- Se cuenta con un equipo de trabajo multidisciplinario y receptivo a la información que se les entrega y, además, son idóneos para desarrollar las actividades generadas en este proceso de auditoría.
- El equipo de trabajo cuenta con el conocimiento y plan de trabajo adecuados para implementar el MIPG y la NTC ISO 27001 en la entidad.
- Tiene su información, en la carpeta compartida, debidamente identificada y organizada con el fin de que el grupo de trabajo acceda y haga uso dicha información a tiempo real.
- Cuenta con planes que permiten llevar y ejecutar el objetivo misional de la Entidad.
- Se evidencia el gran compromiso de todos y se resalta, también, el compromiso por parte de la Líder del Proceso con el fin de dar cumplimiento a la normatividad vigente.
- Se resalta la claridad con la se cuenta para abordar todos los temas que son de su competencia, por parte del Líder del Proceso.

- Se cuenta con documentación sobre los temas de trabajo ya estructurados con el fin de dar apoyo a las actividades que se realizan.
- Se resalta el liderazgo y las acciones implementadas del Sistema de Gestión de Seguridad de la Información por parte de la OTI, acordes con los debes de la NTC ISO 27001 SSGSI.
- Postulación de la Entidad, con el fin de obtener este título de “Sello de la Excelencia”.

5.3 HALLAZGOS DE LA AUDITORÍA

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:
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 las tareas del ciclo de desarrollo en algunos de los casos revisados como es el paso a pruebas o a producción. Incumpliendo la NTC ISO 9001:2008 en su punto 8.5.2. Acción Correctiva literal f.

5.4 RECOMENDACIONES

- Fortalecer la distribución de tareas cuando haya ausencia del responsable como, por ejemplo, en el caso de la auditoría de las bases de datos.
- Documentar y fortalecer el Proceso de Continuidad del Negocio por parte de la Dirección de la Agencia.
- Fortalecer el Proceso de Implementación de la NTC ISO 27001 en toda la Entidad y los procesos que la conforman teniendo en cuenta el resultado de la revisión de la auditoría en el punto 5.1.2 de este documento, pues es responsabilidad de todos que esto se lleve a cabo.
- Emitir Directrices por parte de la Dirección que involucren a todas las dependencias de la Entidad, con el fin de mantener la base de datos de usuarios actualizadas y de esta manera mitigar posibles riesgos de pérdida y uso de información no autorizada.
- Formalizar por parte de la Dirección de la Entidad, la asignación de responsables que liderarán los Planes de Continuidad del Negocio y Seguridad de la Información.

5.5 CONCLUSIONES

La auditoría se ejecutó de acuerdo a lo previsto en el Plan de Auditoría y se cumplió con el objetivo y alcance gracias a la disposición de los colaboradores del Proceso de Tecnologías de la Información; sin embargo esta auditoría se amplió dos (2) semanas dado que se alternó con los compromisos del Grupo de Control Interno de Gestión en cuanto a la auditoría realizada por la Contraloría General de la Nación a la ARN y, también, por el Encuentro de Coordinadores que se desarrolló en este mismo periodo.

Finalmente, y resultado de la auditoría, se observó que la gestión adelantada por los miembros de la OTI se realiza de manera razonable dentro del marco regulatorio aplicable y vigente; también, aplica procedimientos y formatos que le permiten adelantar su función;

aplica controles y seguimientos; y, además, cuenta con colaboradores competentes y comprometidos con el cumplimiento de los objetivos institucionales y con la mejora continua en la Agencia.

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