

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

1. INFORMACIÓN GENERAL

Tipo de Informe	Preliminar <input type="checkbox"/> Final <input checked="" type="checkbox"/> Fecha de la Auditoría: 28/09/2020 al 20/10/2020
Nombre de la Auditoría	Auditoría Gestión de la Información.
Objetivo	<ul style="list-style-type: none"> - Analizar el Sistema de Información de Tierras "SIT" de la entidad donde se evalué su diseño, arquitectura y demás componentes que permitan establecer el cumplimiento de las normativas asociadas a la elaboración e implementación de software y sistemas de información, así como también su uso y administración. - Evaluar el Plan de Continuidad del Negocio de la Entidad conforme a las normativas emitidas por el Ministerio de las Tecnologías y las Comunicaciones, sus avances e implementaciones efectuadas teniendo en cuenta la Circular No. 10 de la Vicepresidencia de la Republica.
Alcance	<p>Desde la implementación del sistema de información hasta los procesos y controles definidos por la Entidad en cuanto a:</p> <ul style="list-style-type: none"> - Diseño y Arquitectura del Sistema de Información - Seguridad de la Información - Controles de accesos - Almacenamiento de los datos - Operaciones de Red - Continuidad del Negocio - Plan de Recuperación ante desastres
Dependencia/Proceso Auditado	Dirección de Gestión del Ordenamiento Social de la Propiedad
Responsable de la dependencia/proceso auditado	Subdirector de Sistemas de Información de Tierras
Equipo Auditor	Auditores: Lilibeth Aguilera Pua (Auditor Líder). Basco German Ricaurte Guerra. Sergio Alejandro Matiz Parra
Criterios de Auditoría	Directiva Presidencial 002 de 2020 Circular 0018 de marzo 2020 Función Pública Circular Externa No. 10 2020 Vicepresidencia de la Republica G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI;



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>Guía técnica; Versión 1.0; 30 de marzo de 2016.</p> <p>G.GEN.02 Guía General de Adopción del Marco de Referencia de Arquitectura Empresarial.</p> <p>Guía técnica; Versión 1.2; 30 de noviembre de 2015.</p> <p>Modelo de Gestión IT4+ de Julio de 2016.</p> <p>Modelo de Seguridad y Privacidad de la Información.</p> <p>Guía para la Preparación de las TIC Para la Continuidad del Negocio.</p> <p>Guía para realizar el Análisis de Impacto de Negocios BIA.</p> <p>Definición estratégica de los sistemas de información - LI.SIS.01.</p> <p>Arquitecturas de referencia de sistemas de información - LI.SIS.03 Metodología de referencia para el desarrollo de sistemas de información - LI.SIS.05.</p> <p>Decreto 415 DE 2016.</p> <p>Decreto 2573 DE2014.</p> <p>MAE.G.GEN.01 – Documento Maestro del Modelo de Arquitectura Empresarial.</p> <p>Manual para la implementación de Gobierno Digital.</p> <p>Documentos establecidos por la Agencia para sobre arquitectura de TI (Caracterización, procedimientos , instructivos, sistema de gestión documental, mapa de riesgos, políticas, indicadores, proyectos de inversión entre otros).</p> <p>Demas Normativas Vigentes expedida por los entes regulatorios en materia de Tecnologías de la información y las Comunicaciones.</p> <p>Ley 594 de 2000 "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones" y sus normas reglamentarias.</p> <p>Decreto 1080 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura".</p> <p>Documentos establecidos por la Agencia para la operatividad de la gestión documental (caracterización, procedimientos, instructivos, sistema de gestión documental, mapa de riesgos, indicadores, planes de mejoramiento, proyectos de inversión, entre otros).</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2. METODOLOGÍA Y/O ACTIVIDADES DESARROLLADAS

El presente informe contiene la verificación y análisis realizado por la Oficina de Control Interno sobre la Gestión de la Información en cuanto a la revisión y evolución de uno de los sistemas de información de misión de crítica denominado **Sistema de Información de Tierras SIT**, que tiene como principal objetivo permitir gestionar y procesar de manera articulada y centralizada la información de los procesos misionales de la Agencia, facilitando a sus usuarios, la disponibilidad, visualización, acceso y uso de información para la toma de decisiones; observando que cumpla con las exigencias normativas, y que su implementación este acorde con las buenas prácticas asociadas a los sistemas de información.

Adicionalmente se evaluó el Plan de Continuidad del Negocio BCP (sus siglas en ingles) en donde se verifico entre otros aspectos, que el plan haya sido elaborado teniendo en cuenta las normativas que el Ministerio de las Tecnologías de la Información y las Comunicaciones para este tipo de documentos, de igual forma fue objeto de análisis los avances propuestos para el año 2020 y los programados con base a la planeación efectuada por las dependencias responsables.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Para el logro del objetivo propuesto en la auditoría, se realizaron actividades tales como:

- Mesas de Trabajo con los recursos que hacen parte del proceso auditado quienes, de acuerdo con los temas de su competencia, aportaron información adicional y aclararon inquietudes del equipo auditor, las cuales fueron ejecutadas de la siguiente manera:

Objetivo Mesa de Trabajo	Fecha	Hora Inicio	Hora de Finalización
Revisión Diseño y Arquitectura Sistema de Información de Tierras SIT	19/10/2020	10:00 a. m.	11:00 a. m.
Gestión de Control de Cambios Sistema de Información de Tierras SIT	19/10/2020	4:00 p. m.	5:00 p. m.
Seguridad de la Información Sistema de Información de Tierras SIT	20/10/2020	10:00 a. m.	11:00 a. m.
Gestión documental Sistema de Información de Tierras SIT	20/10/2020	9:30 a. m.	11:00 a. m.
Controles de Acceso, Administración de Roles Sistema de Información de Tierras SIT	20/10/2020	4:00 p. m.	5:00 p. m.
Arquitectura de Red SIT - Estructura de Seguridad Perimetral	21/10/2020	10:00 a. m.	11:00 a. m.
Almacenamiento de Datos - Backups de la Información, Contingencias SIT	22/10/2020	10:00 a. m.	11:00 a. m.
Continuidad del Negocio - Plan de Recuperación de Desastres	22/10/2020	4:00 p. m.	5:30 p. m.

- Consulta de información publicada en el sitio web de la entidad y la intranet institucional.
- Consulta de la información a través de repositorios como SharePoint y One Drive.
- Revisión y consulta de la Información gestionada por el área auditada en cumplimiento de las normativas emitidas por los entes competentes en materia de Tecnologías de la Información y las comunicaciones.
- Verificación de las funcionalidades de la aplicación mediante un usuario de consulta.

En las actividades relacionadas anteriormente, se realizó el cotejo de los criterios de auditoría establecidos, frente a los soportes, información y evidencias suministradas, lo que arrojó como resultado, los hallazgos y opciones de mejora descritos en este informe.

Mediante correos electrónicos enviados a los enlaces establecidos por la Subdirección de Sistemas de Información de Tierras, se realizó la solicitud de información de la siguiente manera:

Descripción	Fecha de Envío Solicitud	Fecha de Respuesta SSIT	Observaciones
Solicitud de Información No. 1	29/09/2020	05/10/2020	El Auditado envió la parte de la información solicitada, en algunos casos no la posee y en otros solicito aclaración.
Solicitud de Información No. 2	07/10/2020	12/10/2020	El Auditado envió la información solicitada, se presenta la necesidad de realizar mesas de trabajo para la aclaración y explicación de la documentación.
Solicitud de Información No. 3	19/10/2020	21/10/2020	De acuerdo con la mesa de trabajo realizada el día 19 de octubre se realizó una nueva solicitud de Información.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Solicitud de Información No. 4	20/10/2020	26/10/2020	De acuerdo con la mesa de trabajo realizada el día 20 de octubre se realizó una nueva solicitud de Información
Solicitud de Información No.5	20 de octubre de 2020	21 de octubre de 2020	De acuerdo con la mesa de trabajo realizada el día 20 de octubre se realizó una nueva solicitud de Información
Solicitud de Información No.6	23 de octubre de 2020	23 de octubre de 2020	De acuerdo con la mesa de trabajo realizada el día 22 de octubre se realizó una nueva solicitud de Información

INTRODUCCION

Teniendo en cuenta la importancia que representan las Tecnologías de la Información y las Comunicaciones en las organizaciones públicas, y siendo estas, uno de los pilares fundamentales para el cumplimiento de sus objetivos y metas propuestas, es necesario realizar evaluaciones periódicas que garanticen que la Entidad se desarrolle bajo procesos evolutivos y actualizados, con miras al mejoramiento en la prestación de los servicios, situación que hoy día cobra mucha importancia debido a los constante cambios que la tecnología sufre día a día en las organizaciones.

La Oficina de Control Interno en su planeación de auditorias a desarrollarse en la vigencia 2020, dispuso realizar tres (3) auditorias concernientes a las Tecnologías de la Información y la Comunicaciones, con el propósito de poder determinar el estado de diferentes puntos estratégicos para la Entidad que conlleven a un analisis inicial de la infraestructura tecnológica que tiene implementada para la atención de los servicios tanto internos como externos; enfocados en tres grandes aspectos:

- 1. Arquitectura Empresarial:** Es el componente que está encaminado a que todas las Entidades Publicas a través de lineamientos estratégicos estén acordes con los procesos del negocio para la construcción de unas Tecnologías de la Información y las Comunicaciones adecuadas y ordenadas con las demás Entidades Públicas, de igual manera que sea el mapa de ruta en la toma de decisiones de la alta gerencia.
- 2. Disposición de la Información:** En atención a que la información es uno de los activos más importantes para las organizaciones y mas para las Entidades Públicas por su pertenencia, es necesario verificar que los datos o información que sea generada por la entidad, cuenten con todos los elementos que garanticen un buen manejo, administración, respaldo y seguridad sobre sus procesos internos y externos.
- 3. Gestión de la Información:** Este aspecto está enfocado a la revisión de los sistemas de información de misión crítica de la entidad, en donde su principal propósito es el de validar los entornos generales como son: su diseño, administración, seguridad, continuidad y demás aspectos necesarios para proveer aplicativos que cumplan con los objetivos del negocio de una manera oportuna y eficiente.

Con lo anteriormente expuesto. la Oficina de Control Interno pretende de una manera apropiada, revisar de forma integral, los principales aspectos de las Tecnologías de la Información y las Comunicaciones de la Entidad, esto como un analisis inicial a todo el proceso que con lleva la revisión y evaluación de la Infraestructura Tecnológica de la ANT.



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

De la información recibida, analizada y obtenida de las mesas de trabajo, a continuación, se presentan los requisitos con cumplimiento e incumplimiento observados por el equipo auditor:

3. HALLAZGOS

3.1 REQUISITOS CON CUMPLIMIENTO – CONFORMIDADES – DISEÑO Y ARQUITECTURA DEL SISTEMA DE INFORMACIÓN.

El objetivo de este análisis es revisar los aspectos mas importantes de la conformación técnica del Sistema de Información de Tierras teniendo en cuenta las normativas y buenas prácticas asociadas a las entidades públicas que conforman su arquitectura, adicionalmente identificar los puntos de seguridad de la información que se están abordando teniendo en cuenta que se presta servicios a nivel interno y externo de la entidad.

Criterio	Observación
<p>Manual de Gobierno Digital - Arquitectura y Diseño - La Entidad tiene documentada la arquitectura de referencia y de solución para los Sistemas de información - Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p>	<p>1. La entidad cuenta con un repositorio de Sharepoint en la siguiente dirección URL : http://srvsider02:81/sites/SSIT/AE/SitePages/Arquitectura%20Empresarial.aspx. donde gestiona todo lo relacionado con los dominios de información, en esta carpeta esta alojada un dominio denominado “DOMINIO DE SISTEMAS DE INFORMACIÓN”, en este dominio se encuentra toda la documentación relacionada con los sistemas de información, donde se presentan dos módulos denominados de la siguiente manera:</p> <ul style="list-style-type: none"> - Arquitectura de Soluciones: Se describe la Arquitectura de las Soluciones y el Catálogo de los sistemas de información que posee la Entidad. - Soluciones: Este módulo cuenta con una subcarpeta denominada S.I. Misional, donde se describe cada Sistema de Información Misional con su respectiva documentación, en este caso se evidencia una carpeta denominada Sistemadelnfromación: SIT SISTEMA INTEGRADO DE TIERRAS el cual contiene cuarenta y dos (42) documentos distribuidos de la siguiente manera: <ul style="list-style-type: none"> - - Configuración: Un (1) documento - - Diseño Tecnología de Arquitectura: Seis (6) documentos - - Étnicos: Un (1) documento - - Historia de Usuarios: Quince (15) documentos - - Manuales: Nueve (9) documentos - - Necesidades Generales: Un (1) Documento



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<ul style="list-style-type: none"> - - Plan de Pruebas Iniciales: Cuatro (4) - - Requerimientos: Cinco (5) documentos <p>De acuerdo con los análisis efectuados por el equipo de auditoría, se evidencia que la documentación cumple con el criterio dispuesto por el manual de gobierno digital, donde se clasifica la información técnica del Sistema de Información de Tierras SIT describiendo los aspectos más importantes en cuanto su arquitectura, sin embargo sugiere realizar la inclusión de información que son importantes en la arquitectura de la aplicación, los cuales son necesarios para determinar en conjunto su composición de la siguiente manera:</p> <p>Opciones de mejora:</p> <p>1.1 Seguridad de la Información: Se sugiere incluir dentro de la carpeta donde están alojados los documentos de arquitectura de la aplicación, los documentos relacionados con seguridad de la información del Sistema de Información de Tierras en cuanto a: Control de accesos, seguridad perimetral, pruebas de vulnerabilidades efectuadas, planes de remediación, Auditorías Activas.</p>
<p>Manual de Gobierno Digital - Arquitectura y Diseño - La Entidad tiene definido y aplica una metodología de referencia para el desarrollo de sistemas de información - Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p>	<p>2. La Entidad mediante sus documentos alojados en el sistema integrado de gestión ha desarrollado diferentes métodos y procedimientos para el desarrollo de sistemas de información que entre los cuales se encuentra GINFO-Política002 LINEAMIENTOS PARA DESARROLLO DE PRODUCTOS DE SOFTWARE EN LA ANT, en esta política se determina los lineamientos generales para el desarrollo de software o sistemas de información que sean generados por la Agencia Nacional de Tierras, los lineamientos son los siguientes:</p> <ul style="list-style-type: none"> - <u>Lineamiento No. 1. Características básicas generales de las aplicaciones.</u> - <u>Lineamiento No. 2. Desarrollo de módulos genéricos, librerías y componentes.</u> - <u>Lineamiento No. 3. Buenas prácticas en el desarrollo de aplicaciones.</u> - <i>Lineamiento No. 4. Estándares para creación de apis rest e invocación</i> - <i>Lineamiento No. .5 Estándares para desarrollo de aplicativos móviles</i> - <i>Lineamiento No. 7. Estándares para desarrollo de escritorio</i>

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>desconectados de internet.</p> <p>- Lineamiento No 8. Control de versiones</p> <p>En la revisión del documento, se evidencia el cumplimiento de las buenas prácticas que se han tenido en cuenta para el desarrollo de los sistemas de información o de software, en cuanto a la revisión del sistema de información de tierras SIT, este cumple con el lineamientos de la Política donde se están aplicando los lineamientos Nos. 1,2 y 3, en general la aplicación está diseñada bajo los parámetros y políticas definidas por la Entidad, cumpliendo con las premisas descritas en los lineamientos, sin embargo es necesario incluir en el documento temas como:</p> <ul style="list-style-type: none"> - Metodologías de Desarrollo <p>Opciones de mejora:</p> <p>2.1 Corregir o incluir el Lineamiento No. 6, Se recomienda revisar en el documento <i>GINFO-Política002 LINEAMIENTOS PARA DESARROLLO DE PRODUCTOS DE SOFTWARE EN LA ANT</i>, el lineamiento No. 6 ya que no figura, lo cual puede haber ocurrido por omisión o por error en la transcripción del capítulo.</p> <p>2.2 Inclusión Temas: Se sugiere Incluir en el documento <i>GINFO-Política002 LINEAMIENTOS PARA DESARROLLO DE PRODUCTOS DE SOFTWARE EN LA ANT</i> temas relacionados con las metodologías de desarrollo que se vayan a implementar de acuerdo con las necesidades de la Entidad explicando cuales pueden ser las circunstancias para la implementación de la metodología, teniendo en cuenta la complejidad del desarrollo o cambios en el sistema que se presenten o soliciten los usuarios.</p>
<p>Manual de Gobierno Digital - Arquitectura y Diseño - Los sistemas de información de la entidad cuentan con funcionalidades de trazabilidad y auditoría de transacciones o acciones de creación, actualización, modificación o borrado de información para los sistemas que así lo requieran de acuerdo a su criticidad y relevancia para los procesos de la Entidad- Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p>	<p>3. De acuerdo con la documentación aportada por el auditado y en revisión por parte del equipo de auditoria de la Oficina de Control Interno, se evidencia que se describen temas de auditoria netamente informativos tanto en la base de datos como en el sistema de información de la siguiente manera:</p> <ul style="list-style-type: none"> - Servidor de Auditoria: Este servidor es el encargado de almacenar la auditoria de las transacciones del sistema de información, para este se seleccionó un motor en una base de datos NoSQL para almacenar las transacciones del sistema - Capa de Auditoria: La implementación de esta capa, permite registrar el uso de cualquier operación que se desee plasmar para una posterior revisión de auditoria en la cual se podrá gestionar tanto los parámetros de entrada como los resultados de cualquier operación del

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>sistema.</p> <ul style="list-style-type: none"> - Controlador Web API: El controlador Web API se encarga de encapsular los comportamientos de Seguridad y Auditoria por medio de Decoradores y este será capaz de exponer el API del servicio en RestFull utilizando los métodos (POST, PUT, GET y DELETE), adicional este controlador implementa las librerías de swagger para la generación de la documentación requerida. <p>De acuerdo con lo anteriormente expuesto y a las mesas de trabajo realizadas con el auditado se evidencia la existencia de la activación e implementación de auditorías tanto en la base de datos como en el sistema de información, sin embargo no se está realizando los tratamientos a la información que generan estas auditorías, estos datos son utilizados cuando se presenta algún tipo de incidencia que amerite la revisión de esta información, adicionalmente no se cuenta con la documentación que soporte las auditorias activadas tanto en el sistema de información como en la base de datos.</p> <p>Opciones de mejora:</p> <p>3.1 Elaboración de Documentación: Se recomienda la elaboración de un documento técnico donde se describa específicamente la siguiente información:</p> <ul style="list-style-type: none"> - Objetivo de la Auditoria tanto en la base de datos como el Sistema - Diseño (Como funciona) tanto en la base de datos como el Sistema - Tipo de Auditoria (Que hace) tanto en la base de datos como el Sistema - Proceso de Activación y Desactivación ´ (Sistema, base de datos) - Descripción de las trazas generadas - Rutas de Almacenamiento y respaldo de las trazas - Proceso de Tratamiento de la Información generada tanto en la base de datos como el Sistema.
<p>Manual de Gobierno Digital - Arquitectura y Diseño - La entidad tiene definido e implementado un esquema de soporte a los sistemas de información incluyendo si estos son mantenidos por terceros-</p> <p>Tiene establecido criterios de aceptación y Acuerdos de Nivel de Servicio (ANS) cuando se tenga contratado con terceros el mantenimiento de los sistemas de información</p>	<p>4. La Entidad mediante el procedimiento ADMBS-P-016 PROCEDIMIENTO GESTIÓN DE LOS SERVICIOS TECNOLÓGICOS, presenta las acciones que se llevan a cabo para la atención de los servicios tecnológicos a través de la mesa de ayuda, no se observa que específicamente se tengan definidos Acuerdo de Niveles de Servicio para la atención de los incidentes que se generen sobre el Sistema de Información de Tierras.</p> <p>Con base a lo anteriormente expuesto y teniendo en cuenta que el Sistema de Información de Tierras, es uno de los aplicativos COR de la Entidad, es necesario que se defina unos ANS para la atención de los incidentes que sean solicitados a través de la mesa de ayuda, garantizando que la atención de los casos sea oportuna de acuerdo</p>

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

<p>Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p>	<p>con la prioridad que se defina en los ANS.</p> <p>Opciones de Mejora:</p> <p>4.1 Elaboración Acuerdo de Niveles de Servicio: Se sugiere la elaboración de un documento donde se plasme los ANS para la atención de los incidentes que se generen en la mesa de ayuda con respecto al sistema de información de Tierras, teniendo en cuenta las buenas prácticas de ITIL con base a las necesidades de la Entidad y la criticidad de los casos reportados.</p>
<p>Modelo de Gestión IT4+ Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC .</p> <p><i>Orientación a una arquitectura basada en servicios. La entidad entrega servicios en línea que permiten la interoperabilidad con los mismos.</i></p>	<p>5. De acuerdo con la información suministrada por el auditado y las verificaciones efectuadas por el equipo de auditoria, la aplicación utiliza una tecnología denominada RESTFULL, la cual está orientada al consumo de servicios del backend y del frontend de la aplicación, garantizando la interoperabilidad e integridad de los datos.</p> <p>Adicionalmente se muestra el estilo basado en capas de la siguiente manera:</p> <ul style="list-style-type: none"> - Capa de Datos - Capa de Negocio - Capa de Servicios - Capa de Presentación <p>Si bien la integración de los servicios que presta la aplicación muestra que su arquitectura está orientada con el método SOA, hace falta la inclusión en la documentación de la arquitectura de la aplicación, los temas donde se indique la manera en que se ha implementado y orientando una Arquitectura basada en Servicios en la aplicación.</p> <p>Opciones de Mejora:</p> <p>5.1 Inclusión de Información: Se realiza la recomendación de incluir un capítulo en el documento DOCUMENTO DE ARQUITECTURA DE SOFTWARE, donde se indique específicamente que la arquitectura diseñada e implementada del Sistema de Información de Tierras – SIT está orientada a una Arquitectura orientada a servicios SOA.</p> <p>5.2 Elaboración de Documentación: Se recomienda la elaboración de un documento donde se describa la interoperabilidad que gestiona el SIT con los sistemas de información de la entidad, donde se explique en detalle cómo se realiza esta acción y a través de que herramientas, desde su proceso de implementación hasta la Disposición final de la información.</p>

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

<p>Modelo de Gestión IT4+ Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC .</p> <p><i>Funcionales - Su alcance está alineado con las necesidades propias de cada proceso y de la misión de la entidad</i></p>	<p>6. La Entidad mediante el documento DOCUMENTO ARQUITECTURA DE SOFTWARE presenta los procesos que el Sistema de Información de Tierras gestiona a través de los servicios funcionales que realiza con flujos de trabajo definidos de la siguiente manera:</p> <ul style="list-style-type: none"> - Consolidación de Insumos - Crear Análisis Predial Integrado - Gestión Análisis Predial Integrado - Validación - Gestión NUPRE - SIT – Desconectado - SIT – Solicitudes FISO - SIT – RESO – Valoración - SIT – Implementación POSPR - SIT – Procedimiento Único <p>Por la anteriormente expuesto se evidencia que la aplicación gestiona los procesos de la entidad a través de flujos de trabajo que están asociadas a las funcionalidades de la aplicación, adicionalmente la Dirección de Gestión del Ordenamiento Social de la Propiedad este año realizo un diagnóstico del estado actual del SIT, en donde su principal objetivo fue la identificación de oportunidades de mejora en los procesos que gestiona la aplicación o en su defecto determinar que procesos no han sido involucrados en el sistema, este ejercicio se efectuó con las dependencias que tienen injerencia directa en el COR del Entidad, donde finalmente se determinó la necesidad del planteamiento de un plan de trabajo donde se prioricen los temas detectados en este diagnóstico, identificando lo de mayor atención y prioridad, en sesiones que se realizaran en esta vigencia.</p>
<p>Modelo de Gestión IT4+ Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC</p> <p><i>Gestión del cambio - La gestión del cambio para la exitosa implantación de sistemas de información, es algo que se debe tener en cuenta durante todo el ciclo de diseño y desarrollo de sistemas de información, es decir, desde el levantamiento de necesidades hasta las actividades de entrenamiento y acompañamiento.</i></p>	<p>7. La Entidad mediante <i>la GINFO-Política002 LINEAMIENTOS PARA DESARROLLO DE PRODUCTOS DE SOFTWARE EN LA ANT</i> el cual se encuentra publicada en la Intranet de la Entidad en el siguiente Link :http://intranet.agenciadetierras.gov.co/index.php/gestion-de-la-informacion/, menciona en su lineamiento No. 8 el Control de las versiones de las aplicaciones o sistemas de Información.</p> <p>De acuerdo con los analisis y verificaciones efectuadas por el equipo auditor la Entidad realiza las acciones relacionadas con el control de versiones o actualizaciones del Sistema de Información de Tierras SIT a través de una Plataforma “Azure DevOps” donde se da cumplimiento al procedimiento, sin embargo se presentan acciones que no están avaladas por el Sistema Integrado de Gestión como lo es los requerimientos que se gestionan a través de un formato denominado FORMATO PARA SOLICITUD DE REQUERIMIENTOS DE SOFTWARE, adicionalmente se presenta que no existen lineamientos</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>de operatividad del comité de control de cambios, gestionando de manera informal las acciones de este comité.</p> <p>Opciones de Mejora:</p> <p>7.1 Normalización de Documentos: Se sugiere gestionar ante calidad la normalización de los documentos que no son controlados o avalados por el Sistema de Gestión de Calidad de la Entidad dentro del proceso de la gestión del cambio que se desarrolla para todas las aplicaciones de la ANT.</p> <p>7.2 Inclusión de Información : se sugiere la inclusión de información en el documento GINFO-I-015-INSTRUCTIVO-DE-BUENAS-PRÁCTICAS-EN-ITIL-PARA-LA-GESTIÓN-DE-LA-MESA-DE-SERVICIOS-DE-TI- en su capítulo 6.1 GESTIÓN DE CAMBIOS TECNOLÓGICOS temas relacionados como son:</p> <ul style="list-style-type: none"> - Integración del comité de Control de Cambios - Funciones del Comité - Responsabilidades del Comité - Documentos de Salida (actas, informes) <p>Adicionalmente se debe gestionar la consulta ante las dependencias responsables (Planeación o Jurídica) si se hace necesario la formalización o normalización del comité de control de cambios que se encuentra en producción en estos momentos.</p>
<p>Norma ISO 27001: 2013</p> <p>A.12.3 Copias de respaldo Objetivo: Proteger contra la pérdida de datos</p>	<p>8. De acuerdo con la información revisada en la ejecución de la auditoría en cuanto a respaldos de la información se valida el cumplimiento del proceso denominado GINFO-P-009-GENERACIÓN-COPIAS-DE-RESPALDO-DE-LA-INFORMACIÓN-CRITICA-DE-LA-ANT, sin embargo no se evidencia actividades previas donde las dependencias como responsables de la información informen las premisas de cumplimiento de los respaldos o backups que sean requeridos teniendo en cuenta su criticidad en las bases de datos así como también en los sistemas de información.</p> <p>Específicamente para el Sistema de Información de Tierras el respaldo de la información de las bases de datos es almacenado en el servidor con direccionamiento IP 172.23.90.133 unidad F:\MSSQLSERVER\DIARIO. Posteriormente la herramienta Veeam Backups los toma y los aloja en la NetApp, esta es una solución de almacenamiento exclusivo para los backups a disco que se utiliza en la Entidad.</p> <p>Para el tema del respaldo de la configuración, diseño y estructura del Sistema de Información de Tierras se ejecutan un backup de las máquinas virtuales donde está alojado el sistema, esto garantiza que</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>la recuperación del sistema tenga un alto grado de repuesta a cualquier incidencia que se pueda presentar a la negación de servicios para los usuarios.</p> <p>En relación con el criterio evaluado también se procedió a la revisión del cumplimiento del lineamiento que menciona el documento LINEAMIENTOS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN GINFO-Política-005, donde se indica específicamente los lineamientos que se deben realizar al respaldo, custodia y recuperación de la información de las bases de datos de los sistemas de información, y que de acuerdo con los análisis efectuados el método utilizado es un full backup, es decir se está tomando la totalidad de la información que conforma la base de datos, con una periodicidad diaria, donde se ejecuta un JOB que desarrolla las actividades concernientes a la maniobra en la hora y fechas programadas.</p> <p>En cuanto a temas de restauración de la información respaldada, el área de infraestructura está realizando pruebas aleatorias de todas las bases de datos incluyendo las SIT, esta información esta evidenciada de acuerdo a lo registrado en la forma NOVEDADES DE BACKUPS DE LA INFORMACIÓN CRÍTICA DE LA ANT, donde las restauraciones de las bases de datos asociadas al SIT tienen como resultado exitoso, sin embargo, es necesario que se incluya una actividad en el proceso, donde desde el ambiente pruebas del SIT se realice el direccionamiento donde se restauró la información con el objetivo de validar dentro de la aplicación que la información no ha sido corrupta o presentan fallas a la restauración.</p> <p>Adicionalmente se procedió a revisar la INTI-Política-001 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN en donde su Numeral 7.9 Respaldo de la Información indica todo lo relacionado con el respaldo de la Información, con sus obligaciones relacionadas con los sistemas de información, sin embargo, no se evidencio los documentos asociados a cada obligación de este criterio (formas, procedimientos).</p> <p>Opciones de Mejora:</p> <p>8.1 Inclusión de Información: Se sugiere incluir en el procedimiento GINFO-P-009-GENERACIÓN-COPIAS-DE-RESPALDO-DE-LA-INFORMACIÓN-CRÍTICA-DE-LA-ANT temas como:</p> <ul style="list-style-type: none"> - Análisis de la información a respaldar para su actualización, o inclusión de nuevas rutas teniendo en cuenta las observaciones que sean emitidas por las Dependencias responsables de la información del Sistema de Información de Tierras. <p>8.2 Elaboración de Procedimiento: Se sugiere elaborar un Proceso donde se describa el método y actividades que se debe implementar y ejecutar para los backup que se realizan a la configuración del SIT, incluyendo las acciones para</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>la puesta en producción de una copia de la configuración en caso de contingencia</p> <p>8.3 Respaldo a Cinta: Se recomienda realizar copias de respaldo de la información crítica de la entidad de las bases de datos y sistemas de información a cintas magnéticas a través de un robot de cintas (data protector).</p> <p>8.4 Elaboración de Procedimiento: Se sugiere la elaboración de un procedimiento donde la dependencia responsable del sistema de información SIT, realice las pruebas de consistencia de la información de las restauraciones de los backups que el área de infraestructura realiza, como actividad final ejecutándose en el ambiente de pruebas.</p> <p>8.5 Inclusión de Información: Se sugiere incluir en la INTI-Política-001 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN en el numeral 7.9 los documentos asociados al respaldo de la información que garantizan la ejecución de las actividades tanto en las bases de datos como en los sistemas de información de misión crítica.</p>
<p>Norma ISO 27001: 2013</p> <p>Seguridad de la Información</p> <p>A.13.1.1 - Controles de redes Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.</p>	<p>9. Se verifico el diseño de arquitectura de seguridad del SIT, donde a nivel de la WAN se evidencia varios puntos de control antes de llegar a los servidores donde esta alojada la aplicación, en cuanto a la red LAN de la Entidad, también se indica los puntos de control (seguridad) que se tienen entorno al Sistema de Información de Tierras, sin embargo, es necesario definir los documentos técnicos donde se describan la composición de la infraestructura de las redes WAN y LAN.</p> <p>Para el acceso a la aplicación de proveedores externos, la entidad a dispuesto de una red privada denominada GNAT donde se cuenta con los niveles de seguridad en donde solamente pueden acceder direccionamientos que hayan sido autorizados por la Entidad en cumplimiento de sus funciones, de esta manera se agregan los usuarios para poder ingresar a la aplicación de manera externa que no pertenezcan a la Entidad.</p> <p>Opciones de Mejora:</p> <p>9.1 Elaboración de Documentación: Se recomienda realizar la documentación soporte de los componentes que conforman las redes WAN y LAN de la Entidad.</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>9.2 Análisis de Seguridad Red LAN: Se recomienda realizar un análisis de seguridad de los puntos de red de la Entidad para determinar cuales están en uso, y en consecuencia realizar los apagados de puertos en los Switches perimetrales con el objetivo de mantener un control de seguridad para el acceso a la red, adicionalmente se sugiere implementar métodos de seguridad en los puertos de la red como por ejemplo autenticación mediante el protocolo 802.1. X.</p>
<p>Norma ISO 27001: 2013</p> <p>A.11.2 Gestión del acceso de usuarios.</p> <p>A.11 CONTROL DE ACCESO</p> <p>A.11.2.1 Registro de usuarios. Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.</p>	<p>10. Se realizo la revisión de los procedimientos asociados al criterio, los cuales están publicados en la intranet de la entidad en el siguiente link: http://intranet.agenciadetierras.gov.co/index.php/gestion-de-la-informacion/ donde se evidencia el cumplimiento de las acciones para la creación de los usuarios en el SIT, adicionalmente y teniendo en cuenta que el sistema maneja información sensible de la entidad, se están solicitando los acuerdos de confidencialidad y los documentos soporte que avalan la creación del usuario, sin embargo se detectó que no existe documentación, como base del conocimiento, donde se explique el paso a paso que se realiza desde que llega el caso al experto, hasta el reporte del cumplimiento y atención del requerimiento, esto determina un gran riesgo para la Entidad teniendo en cuenta que se depende de un recurso específico para la atención de la creación de los usuarios, o de las modificaciones respectivas.</p> <p>Adicionalmente se revisó las políticas mencionadas en el PETIC en su capa de seguridad, en el cual se menciona los accesos y el control de las sesiones del Sistema de Información de Tierras, en donde no se aportó la documentación que soporte la implementación de estas políticas dentro de la aplicación.</p> <p>Opciones de Mejora:</p> <p>10.1 Elaboración de Documentación: Se realiza la recomendación de elaborar una base de conocimiento de los procesos que se realizan para de la creación de los usuarios del SIT, teniendo en cuenta el flujo de datos que se debe aportar para la realización de la actividad, donde técnicamente se pueda realizar sin un conocimiento previo.</p> <p>10.2 Elaboración de Documentación: Se realiza la recomendación de elaborar los documentos técnicos y de configuración de las políticas que se mencionan en el PETIC en cuanto a la capa de seguridad del SIT.</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

<p>Norma ISO 27001: 2013</p> <p>A.11.2.2 Gestión de privilegios. Se debe restringir y controlar la asignación y uso de privilegios.</p>	<p>11. Se realizo la revisión de la matriz denominada ROLES A CONFIGURAR SIT donde se cuenta con la información base de roles describiendo una serie de caracterizaciones combinadas de acuerdo a las funciones que el usuario vaya a realizar dentro del SIT, en la aplicación esto se realiza a través de los flujos de trabajo, que están predeterminados en el sistema, pudiendo crear roles con diferentes caracterizaciones de acuerdo con la necesidad que se solicite por parte de las dependencias.</p> <p>Analizando la información de los privilegios de los roles de acceso que tiene la aplicación, se evidencia que aproximadamente se cuenta con 270 roles creados dentro del sistema, en algunos casos su categorización no es de fácil ubicación, si no se cuenta con el conocimiento previo de las características de cada rol, existiendo un riesgos alto en cuanto a que se hayan creado roles con iguales características presentándose duplicidad y un incremento en el número de roles que deberían estar activos en el sistema.</p> <p>No se evidencio seguimiento a los roles, que por sus características o antigüedad ya no están siendo utilizados o que por cambios en la aplicación ya no son funcionales.</p> <p>Opciones de Mejora:</p> <p>11.1 Revisión Matriz: Se sugiere la revisión de la matriz de roles que se tiene en la actualidad en producción, en donde se defina un método para su caracterización, esto con el fin de que su uso y administración sea de forma más ágil y no permita que se puedan repetir roles ya creados en la base principal de la aplicación.</p> <p>11.2 Elaboración Documentación: Se sugiere elaborar la documentación técnica necesaria sobre la creación de roles y perfiles en la aplicación, así como también la de su administración y mantenimiento respectivo.</p>
------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.2 REQUISITOS CON CUMPLIMIENTO – CONFORMIDADES – PLAN DE CONTINUIDAD DEL NEGOCIO

Teniendo en cuenta la importancia del cumplimiento de los objetivos de la Agencia Nacional de Tierras, es necesario preparar a la entidad frente a circunstancias de amenazas internas o externas que pueden desembocar en incidentes que afecten la continuidad de los servicios que la entidad proporciona en cumplimiento de las normativas, leyes y demás criterios por la cual fue creada, por tanto se debe establecer un plan de continuidad del negocio, el cual esta orientado a ser el mapa de ruta para responder de manera planeada, organizada y oportuna a situaciones que podrían interrumpir la operación de los procesos de la Entidad impactando en el cumplimiento de las metas y objetivos trazados por el Gobierno Nacional.



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Para la puesta en producción de este tipo de planes, es necesario contar con la disposición de recursos humanos, técnicos, financieros y tecnológicos que deben ser identificados a la realización de la construcción del documento con base a las necesidades de la Entidad para realizar una continuidad del negocio.

Criterio	Observación
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>COMPONENTE – PLANIFICACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</p> <p>Objetivos, alcance y límites para la preparación de las TIC para la continuidad del negocio (IRBC)</p>	<p>1. La Entidad cuenta con un documento denominado ANT-Plan de Continuidad del Negocio - Nov 2019 Versión 4, el cual no se encuentra publicado. por ser considerado un documento de naturaleza confidencial, este plan contiene elementos que se ajustan al criterio de la Guía para la preparación de las TIC para la continuidad del negocio teniendo en cuenta lo siguientes objetivos definidos en el documento de la siguiente manera:</p> <ul style="list-style-type: none"> - Definir las actividades preventivas, detectives y correctivas para reaccionar de manera eficiente ante una eventualidad que comprometa el desarrollo de las actividades cotidianas, la seguridad del personal o la prestación del servicio SIT. - Producir y mantener un conjunto de planes de continuidad del servicio de TI en adelante BCP que soporten los planes generales de continuidad del negocio. - Generar los lineamientos para completar ejercicios regulares del BIA para asegurar que todos los planes de continuidad se mantienen alineados con los cambiantes requerimientos e impactos del negocio de la ANT. - Establecer las guías para las evaluaciones de riesgo regulares y ejercicios de análisis de riesgo con el fin de gestionar los servicios de TI dentro de un nivel de riesgo acordado en conjunto con la entidad y la gestión de disponibilidad. - Proveer gua y directrices a todas las demás áreas del negocio y TI sobre todos los temas relacionados a continuidad y recuperación. <p>En cuanto a los alcances se define lo siguiente:</p> <p>"El presente BCP (Sus Siglas en Ingles) tiene como alcance los siguientes parámetros en los cuales su descripción se detalla a continuación:</p> <p><i>El plan de continuidad del negocio - BCP inicia con la identificación y socialización de los elementos críticos para el que puedan definirse como incidente o desastre que impidan continuar la operación y finaliza con el análisis y acciones de mejora identificadas de la reacción ante la situación presentada mínimo una vez al año (simulacro o realidad)</i></p> <p><i>se enfoca en aquellos eventos que el negocio considera suficientemente significativos para ser tratados como un "desastre".</i></p> <p><i>Soporta los requerimientos específicos de servicios de TI y técnicos. Para recuperarse de un desastre.</i></p> <p><i>Se apoya principalmente en los activos de TI y las configuraciones que soportan los</i></p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p><i>procesos de negocio críticos definidos en el DRP.</i></p> <p><i>No cubre directamente riesgos de largo plazo, incluso si estos afectan considerablemente los servicios del SIT."</i></p> <p>Por lo anteriormente expuesto se determina }el cumplimiento del criterio teniendo en cuenta que en el documento del Plan de Continuidad del Negocio se definen los objetivos y los alcances correspondientes.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>COMPONENTE – PLANIFICACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</p> <p><i>Política para la preparación de las TIC para la continuidad del negocio (IRBC)</i></p>	<p>2. De acuerdo con los análisis de los documento asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, se observó que la dependencia desarrolló el documento del Plan de Continuidad del Negocio, en este plan hace falta la referencia a la Política para la preparación de las TIC para la continuidad del negocio (IRBC), del mismo modo en dicho documento hace falta gestionar por parte del auditado un plan de trabajo donde se programe la elaboración del producto que menciona el criterio que para este caso es la política para la preparación de las TIC para la continuidad del negocio (IRBC).</p> <p>Opciones de mejora:</p> <p>2.1 Elaborar Documento, se recomienda documentar y socializar una Política para la preparación de las TIC para la continuidad del negocio (IRBC) que defina los lineamientos a seguir, antes, durante y después de una interrupción en los servicios de la Agencia oportunamente o cuando su normal funcionamiento sea afectado por cualquier evento, buscando el mínimo impacto para clientes internos y externos.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</p> <p><i>Asignación de recurso humano competente y capacitado, comunicación de roles y responsabilidades para la preparación de las TIC para la continuidad del negocio (IRBC)</i></p>	<p>3. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, se observa que existe la definición del oficial de seguridad en la entidad que es desempeñado por el Subdirector de Sistemas de Información de Tierras y adicionalmente existe un profesional – contratista que desempeña tareas de seguridad de la Información, sin embargo hace falta definir más roles con la totalidad del recurso humano de que trata el criterio para el cumplimiento de y definir una propuesta sobre el grupo de trabajo de seguridad planeada o programada en cumplimiento del criterio para ser implementada a posteriori.</p> <p>Opciones de mejora:</p> <p>3.1 Asignación de Recurso: Se recomienda realizar la asignación de recurso humano que cumpla las capacidades, academia y experiencia en el dominio de la Seguridad de la Información, el cual tendrá a cargo las funciones de Oficial de Seguridad, comunicando sus respectivos roles y responsabilidades para la preparación de las TIC para la continuidad del negocio.</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.

COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Definición de un plan de requerimientos, categorizando las actividades para la continuidad definiendo el nivel con el cual cada actividad crítica necesita para su reanudación, estas actividades deberán contar con un tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO) para el objetivo mínimo de continuidad del negocio (MBCO) por producto, servicio o actividad.

Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.

COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO

Para cada servicio TIC crítico los acuerdos actuales de preparación de TIC – tales como prevención, monitoreo, detección, respuesta y recuperación – deben ser comparados con los requerimientos de continuidad del negocio y cualquier “brecha” debe ser documentada e informada a la alta dirección.

- De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, Si bien la Entidad cuenta con el documento del plan de continuidad del negocio, hace falta incluir el plan de requerimientos como lo menciona el criterio, sin embargo, en la mesa de trabajo con la dependencia se indago sobre el particular, concluyendo que se han efectuado acciones preliminares en la recolección de la información como avance en el mencionado plan.

Opciones de Mejora:

- 4.1 Elaboración Documento:** Se sugiere la elaboración de un plan de requerimientos, donde se categoricen las actividades para la continuidad, se definan los niveles con los que cada actividad crítica necesita reanudar. Debe contar con un tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO) para el objetivo mínimo de continuidad del negocio (MBCO) por producto, servicio o actividad.

- De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, se evidencia documentación de misión crítica como son **GINFO-P-010-ADMINISTRACIÓN Y MANTENIMIENTO DE BASES DE DATOS** publicado en: <http://intranet.agenciadetierras.gov.co/wp-content/uploads/2020/10/GINFO-P-010-ADMINISTRACION%20Y-MANTENIMIENTO-DE-BASES-DE-DATOS.pdf> el cual tiene por objetivo: "Gestionar eficientemente las bases de datos de propiedad de la Agencia Nacional de Tierras para garantizar la disponibilidad, seguridad y oportunidad de la información almacenada en los diferentes sistemas de gestión." y alcance: "Aplica para las bases de datos productivas administradas por la Subdirección de Sistemas de Información y el Equipo de Infraestructura y Soporte Tecnológico, y se incluyen los ambientes de pruebas y desarrollo Únicamente para la configuración de servidores e instalación de bases de datos.

El alcance va desde la creación de una base de datos o instancia, configuración y cambios de estructuras de base de datos hasta la generación y restauración de backups".

En virtud de los anterior, se presenta un documento de misión crítica el cual puede ser parte del plan de continuidad del negocio, pero hace falta definir los demás documentos técnicos donde se exponga la infraestructura de misión crítica como son:

- Arquitectura Sistemas de Información



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<ul style="list-style-type: none"> - Infraestructura Tecnológica vigente - Programas o Software Activos <p>Opciones de Mejora:</p> <p>5.1 Analisis de la Información: Se realiza la recomendación de elaborar los documentos de misión crítica de la entidad donde se incluya temas de Software y Hardware definiendo indicadores de gestión que permitan evaluar los comportamientos, usabilidad y necesidades para una operación alterna.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</p> <p><i>Definir la estrategia de IRBC, la aproximación para implementar la resiliencia requerida de tal manera que los principios de prevención de incidentes, detección, respuesta, recuperación y restauración se pongan en marcha, se deberán contemplar aspectos tales como: habilidades y conocimiento del personal, instalaciones, tecnología, datos, procesos y proveedores, estas deberán ser aprobadas por la alta dirección y sensibilizadas al interior de la Entidad.</i></p>	<p>6. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, se encontraron referencias al equipo de estrategia de la siguiente manera:</p> <ul style="list-style-type: none"> - Medidas requeridas de reducción de riesgo - Opciones requeridas de recuperación" <p>Teniendo en cuenta lo anteriormente expuesto, es necesaria la definición de la estrategia IRBC de manera concisa, solamente a manera informativa se definen lineamientos que no están alineados con el criterio.</p> <p>Opciones de Mejora:</p> <p>6.1 Fortalecer la definición de estrategia de IRBC en el Plan de Continuidad del Negocio, de modo que los principios de prevención de incidentes, detección, respuesta, recuperación y restauración sean incluidos, contemplando además los aspectos recomendados por la guía tales como: habilidades y conocimiento del personal, instalaciones, tecnología, datos, procesos y proveedores, aprobadas por la alta dirección y sensibilizadas al interior de la Entidad.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</p> <p><i>Concientización, habilidades y conocimiento general de la preparación de los elementos de servicios de TIC personas, infraestructura, tecnología, datos, procesos y proveedores, así</i></p>	<p>7. De acuerdo con las revisiones efectuadas a la documentación soporte del criterio y a las mesas trabajo realizadas, hace falta incluir en el documento del Plan de Continuidad del Negocio o como documento anexo las acciones o lecturas que estén enfocadas al cumplimiento del lineamiento, el cual está orientado al conocimiento de las Tecnologías de la Información y las Comunicaciones en su entorno general que son utilizados por la Entidad para su operación.</p> <p>Opciones de Mejora:</p> <p>7.1 Elaboración Documentación : Se sugiere documentar aspectos como son: lecciones aprendidas, planes de trabajo, planes de acción y demás elementos, conformando una base de conocimiento que sistematice la experiencia de trabajo, habilidades y conocimiento general de la preparación de los elementos de servicios de</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

<p>como sus componentes críticos</p>	<p>Tecnologías de la Información y las Comunicaciones así como también otros aspectos como son : recursos humanos, infraestructura, tecnología, datos, procesos, proveedores y sus componentes críticos.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</p> <p><i>La infraestructura de los sistemas de recuperación de TIC y la información crítica deben, en lo posible, ser físicamente separada del sitio operacional para prevenir que sea afectada por el mismo incidente.</i></p>	<p>8. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, se mencionan de manera informativa temas asociados a la normativa como son:</p> <p><i>"Una amplia estrategia de recuperación y respaldo, incluyendo almacenamiento fuera del sitio."</i></p> <p>Teniendo en cuenta lo anteriormente expuesto y con base a los analisis efectuados por el equipo auditor, se observó que hace falta documentar avances sobre el criterio y planes de trabajo donde se proyecte su atención al cumplimiento de la normativa.</p> <p>Opciones de Mejora:</p> <p>8.1 Inclusión de Información : Se sugiere incluir las posibles estrategias y opciones que se tienen contempladas para la implementación o tercerización de un sitio alternativo que cumpla los requisitos tecnológicos para replicar los servicios de misión crítica que la entidad defina en sus analisis respectivos, adicionalmente se hace necesario realizar las proyecciones de implementación de este requerimiento en los planes de gestión de las siguientes vigencias como objetivo estratégico siendo este requerimiento esencial en cumplimiento del plan de continuidad del negocio y de recuperación ante desastres.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</p> <p>Las estructuras tecnológicas de TIC deben ser implementadas, incluyendo el tipo de implementación y acuerdo, como, por ejemplo:</p> <p>Documento con la estrategia de</p>	<p>9. De acuerdo con los análisis de los documentos dispuestos por la dependencia y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, únicamente se presenta documentación asociada al lineamiento con un plan de recuperación ante desastres, se indica por parte de la dependencia auditada que no se tiene documentos adicionales anexos al Plan de Continuidad del Negocio.</p> <p>Opciones de Mejora:</p> <p>9.1 Elaboración Documentación : Se sugiere elaborar o construir el documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección así como los documentos que contengan los planes para el manejo de interrupciones potenciales, para la habilitación de los servicios TIC y la recuperación de los servicios críticos y que contemplen el propósito y alcance, roles y responsabilidades, activación del plan y la</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

<p>planificación y control operacional, revisado y aprobado por la alta Dirección.</p> <p>Documentos con los planes para el manejo de interrupciones potenciales, para la habilitación de los servicios TIC y la recuperación de los servicios críticos este debe contemplar el propósito y alcance, roles y responsabilidades, activación del plan y la documentación del plan de respuesta y recuperación de TI propietario y mantenimiento.</p> <p>Documentación del plan de respuesta de TIC y plan de recuperación.</p> <p>Documento con los registros de concientización, competencia y programa Definido</p> <p>a. Espera en caliente, donde la infraestructura TIC es replicada a través de dos sitios.</p> <p>b. Espera en tibio, donde la recuperación toma lugar en un sitio secundario donde la infraestructura TIC está parcialmente preparada.</p> <p>c. Espera en frío, donde la infraestructura es construida o configurada a partir de cero en una ubicación alterna.</p> <p>d. Banco de acuerdos, sobre los cuales los proveedores de servicios externos puedan proveer hardware.</p> <p>e. Acuerdos compuestos de las estrategias precedentes: con un enfoque de “escoger y mezclar”.</p>	<p>documentación del plan de respuesta y recuperación de TI propietario y mantenimiento. además de la documentación del plan de respuesta de TIC y plan de recuperación. Finalmente, el documento con los registros de concientización, competencia y programa definido.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p><i>COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</i></p>	<p>10. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, se observa la definición del plan de continuidad del negocio, la cual si bien define elementos de gran importancia en cuanto a la respuesta de la entidad ante un incidente que requiera de la recuperación de los sistemas, hace falta definir la disponibilidad de los datos y requerimientos, sin embargo el Auditado ha manifestado a esta dependencia, que está en proceso de aprobación, es importante mencionar que no se remitieron</p>

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

<p><i>Los acuerdos para la disponibilidad de los datos deben estar alineados con los requerimientos de la estrategia.</i></p>	<p>los documentos soporte para el análisis correspondiente.</p> <p>Opciones de Mejora:</p> <p>10.1 Elaboración Documentación: Se sugiere construir el plan y el árbol de comunicaciones en caso de contingencia, con el objetivo de cumplir con los acuerdos para la disponibilidad de los datos y que estos se organicen con los requerimientos de la estrategia.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p><i>COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</i></p> <p><i>La Entidad debe asegurar que los proveedores críticos están en capacidad de soportar los servicios de la estrategia, conforme a los requerimientos de la Entidad.</i></p>	<p>11. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, en el plan de continuidad del negocio se hace referencia a asegurar que los proveedores críticos están en capacidad de soportar los servicios de la estrategia, conforme a los requerimientos de la Entidad.</p> <p>En el numeral 1.24 del plan de continuidad del negocio, se menciona Información para un plan integral de soporte de un BCP, sin embargo, hace falta mencionar los lineamientos que deberían cumplir los proveedores para soportar los servicios de la estrategia, que en esta información es el resultado de una evaluación de la criticidad de los servicios de la Entidad.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p><i>COMPONENTE – IMPLEMENTACIÓN PARA LA PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO</i></p> <p>Implementar el plan de respuesta de incidentes que permita confirmar la naturaleza y grado del incidente, tomar control de la situación, contener el incidente y comunicar a las partes interesadas.</p>	<p>12. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, en el plan de continuidad del negocio indica en su numeral 1.19. que se deben integrar los siguientes planes:</p> <ul style="list-style-type: none"> - Plan de respuesta a emergencias. - Plan de evaluación de daños. - Plan de salvamento. - Plan de registros vitales. - Plan de relaciones públicas y gestión de crisis. - Plan de servicios y alojamiento. - Plan de seguridad. - Plan de personal. <p>Teniendo en cuenta lo anteriormente expuesto se observó que se tiene contemplado la elaboración de los planes correspondientes a la atención de los incidentes en plan de continuidad del negocio los cuales pueden estar abocados a la respuesta donde su naturaleza debe definir su criticidad y las acciones que se deben realizar para su mitigación, sin embargo no es posible validar los avances que se han ejecutado en cuanto a la construcción de estos documentos o en su defecto los planes de trabajo gestionados por la dependencia donde se defina la planeación para su elaboración.</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>Opciones de Mejora:</p> <p>12.1 Elaboración Planes de Trabajo: Se sugiere elaborar o construir los planes de trabajo donde se programe la elaboración de los documentos anexos al plan de continuidad del negocio, así como también garantizar la integridad de la información plasmada en cada plan.</p>
<p>Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>ANALISIS DEL IMPACTO DEL NEGOCIO</p> <p><i>Métodos para la obtención de información</i></p>	<p>13. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, en el plan de continuidad del negocio se mencionan los métodos para la obtención de la información de la siguiente manera:</p> <ul style="list-style-type: none"> - Se realizaron entrevistas a las áreas de TI y obtener las actividades y procesos de cada una de ellas. - Se determinaron las dependencias de TI de cada una de las actividades. - Se determinaron las necesidades temporales (RTO) y limitaciones de pérdida de datos (RPO) para cada proceso o actividad, desde el punto de vista del negocio. -Se determinaron las capacidades de los sistemas en cuanto al tiempo de recuperación (RTO) y la política de copias (RPO). -Con esta información, fue posible determinar las actividades y recursos TIC más críticos, así como determinar en qué casos hay que aplicar medidas para cumplir con los requerimientos de negocio los cuales fueron expresados en los escenarios posibles de fallas dentro del anexo Formato Manual DRP - Nov 2019." <p>Por lo anteriormente expuesto existe conformidad en cuanto al cumplimiento del criterio, toda vez que se han utilizado métodos para la obtención de la información los cuales pueden ser evaluados en su utilización.</p>
<p>Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>ANALISIS DEL IMPACTO DEL NEGOCIO</p> <p><i>Requerimientos de tiempos de recuperación</i></p>	<p>14. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, en el plan de continuidad del negocio se mencionan temas relacionados con el criterio de la siguiente manera:</p> <ul style="list-style-type: none"> - Se determinaron las necesidades temporales (RTO) y limitaciones de pérdida de datos (RPO) para cada proceso o actividad, desde el punto de vista del negocio. -Se determinaron las capacidades de los sistemas en cuanto al tiempo de recuperación (RTO) y la política de copias (RPO). <p>Teniendo en cuenta lo anteriormente expuesto, si bien se menciona las necesidades de los RTO y RPO, hace falta documentar la ejecución del levantamiento de información para determinar los tiempos de recuperación óptimos para de los servicios críticos de la Entidad, adicionalmente incluir los planes de trabajo donde se programe o planee la elaboración y levantamiento de la información necesaria para la definición de los RTO y los RPO.</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>Opciones de Mejora:</p> <p>14.1 Definición de Requerimientos: Se sugiere realizar la construcción de los requerimientos iniciales para la definición de los RTO y RPO del plan de continuidad del negocio.</p>
<p>Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>ANALISIS DEL IMPACTO DEL NEGOCIO</p> <p>Metodología del Análisis de impacto del negocio</p>	<p>15. De acuerdo con los análisis de los documentos asociados y las mesas de trabajo realizadas en cumplimiento del criterio evaluado, se evidencian ejemplos de una matriz para el Análisis de impacto del negocio BIA (Sus siglas en Inglés), sin embargo hace falta determinar una metodología en donde se describa específicamente cuales son las actividades que se deben ejecutar para el levantamiento de la información que determine la afectación que podría incurrir la entidad como resultado de un incidente o desastre en la prestación de los servicios.</p> <p>Opciones de Mejora:</p> <p>15.1 Definición de Metodología BIA: Se sugiere elaborar un documento anexo al plan de continuidad del negocio en donde se describa la metodología que se va a desarrollar para el levantamiento de información con el objetivo de definir los impactos del negocio.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>ANALISIS DEL IMPACTO DEL NEGOCIO</p> <p>“Gestión del riesgo”</p>	<p>16. De acuerdo al análisis realizado a la documentación aportada por la dependencia, así como a lo expuesto en las mesas de trabajo, se observó que la entidad tiene un alto nivel de dependencia con los sistemas de información para su gestión operativa, se evidenció, que el plan de continuidad del negocio está alineado con la metodología de riesgos que la entidad ha implementado, articulándose de este modo al mapa de riesgos institucional. Adicionalmente se tienen en cuenta un conjunto de medidas de reducción de riesgo que apalancan su administración y seguimiento.</p>
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p>ANALISIS DEL IMPACTO DEL NEGOCIO</p> <p>“Clasificación de escenarios de riesgo”</p>	<p>17. De acuerdo a los documentos aportados por la dependencia, así como la información recolectada en las mesas de trabajo en el marco del presente ejercicio, se observó la inclusión y clasificación de diferentes escenarios de riesgo consignadas en el Mapa de Riesgos de Seguridad de la Entidad de la siguiente manera:</p> <ul style="list-style-type: none"> - Pérdida de la integridad, confidencialidad y disponibilidad de la información física manejada por los procesos de la ANT. - Pérdida de la integridad, confidencialidad y disponibilidad de la información y equipos de cómputo debido a la falta de controles de acceso físico para el ingreso a las sedes de la ANT. - Incumplimiento por parte de los funcionarios y contratistas de las políticas general y específicas de seguridad de la información



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>definidas por la ANT.</p> <ul style="list-style-type: none"> - Pérdida de la confidencialidad, integridad y disponibilidad de la información almacenada y procesada por la infraestructura tecnológica de la ANT, ocasionada por la explotación de las vulnerabilidades técnicas existentes. - Incumplimiento de las responsabilidades de seguridad de la información definidas por la ANT, por parte de los funcionarios y Contratistas. - Pérdida de la integridad, confidencialidad y disponibilidad de la información procesada en el correo electrónico, aplicaciones, equipos de cómputo y sistemas de información, debido a la gestión inadecuada de los usuarios y contraseñas. - Pérdida de la cultura organizacional en materia de seguridad de la información, debido a la baja participación de los funcionarios y Contratistas en actividades de sensibilización y capacitación en esta temática. - Pérdida de la confidencialidad, integridad o disponibilidad de la información de los proyectos de todo tipo ejecutados en la ANT, debido a la falta de integración de la seguridad de la información con la gestión de proyectos y contratación. - Pérdida de la confidencialidad de la información de la ANT almacenada en medios removibles. - Pérdida de la confidencialidad de la información provocada por un acceso no autorizado a la red de la ANT. - Pérdida de la disponibilidad de la información de la ANT, debido a la falta de redundancias de las instalaciones de procesamiento de información. - Pérdida de la disponibilidad de la información, sistemas de información y servicios almacenados y procesados en el hardware (servidores, dispositivos de red y seguridad) ubicados en el datacenter debido a fallas técnicas.
<p>NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001</p> <p>Anexo A, A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</p> <p>“Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio”</p>	<p>18. De acuerdo con los soportes dispuestos por el auditado, se observó que la dependencia definió en su plan de continuidad del negocio objetivos relacionados a la seguridad de la información de la siguiente manera:</p> <ul style="list-style-type: none"> - Definir las actividades preventivas, detectives y correctivas para reaccionar de manera eficiente ante una eventualidad que comprometa el desarrollo de las actividades cotidianas, la seguridad del personal o la prestación del servicio SIT. - Producir y mantener un conjunto de planes de continuidad del servicio de TI en adelante BCP que soporten los planes generales de continuidad del negocio. - Generar los lineamientos para completar ejercicios regulares del BIA



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

	<p>para asegurar que todos los planes de continuidad se mantienen alineados con los cambiantes requerimientos e impactos del negocio de la ANT.</p> <ul style="list-style-type: none"> - Establecer las guías para las evaluaciones de riesgo regulares y ejercicios de análisis de riesgo con el fin de gestionar los servicios de TI dentro de un nivel de riesgo acordado en conjunto con la entidad y la gestión de disponibilidad. - Proveer guía y directrices a todas las demás áreas del negocio y TI sobre todos los temas relacionados a continuidad y recuperación. <p>Así mismo en los documentos asociados a la gestión de riesgos se observó la inclusión de elementos de seguridad de información, sobre lo cual también se define en los objetivos del plan de continuidad del negocio.</p>
<p>NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001</p> <p>Anexo A, A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</p> <p>“continuidad del negocio y evaluación de riesgos”</p>	<p>19. Se observó, de acuerdo al análisis de la documentación dispuesta por la dependencia un alto nivel de dependencia de la operación que mantiene con los sistemas de información para su gestión misional, articulándose con la metodología de riesgos de la entidad, incluyendo estos temas en el mapa de riesgos institucional, mediante el desarrollo del mapa de riesgos de seguridad.</p> <p>De igual manera se valida las medidas de reducción de riesgo las cuales son dispuestas en el plan continuidad de la siguiente manera:</p> <ul style="list-style-type: none"> - Instalación de fuentes de poder interrumpibles y respaldo de energía a los equipos de cómputo y servidores. - Sistemas tolerantes a fallas para las aplicaciones críticas donde aún la más mínima inactividad es inaceptable. - Arreglos RAID y discos espejos para servidores LAN para prevenir en contra de pérdida de datos y asegurar disponibilidad continuada de datos. - Equipos/componentes de repuesto para ser usados en el evento de falla de un equipo o componente – por ejemplo, un servidor LAN de repuesto preconfigurado con la configuración estándar y disponible para reemplazar un servidor defectuoso con el menor tiempo de configuración y construcción. - Eliminación de puntos únicos de falla, tales como puntos únicos de acceso a la red o suministros únicos de energía dentro de un edificio. - Sistemas de TI y redes resistentes. - Servicios tercerizados con más de un proveedor. - Mayores controles de seguridad tanto físicos como basados en TI. - Mejores controles para detectar interrupciones de servicio, tales como sistema de detección de incendios, acompañados con sistemas de supresión. - Una amplia estrategia de recuperación y respaldo, incluyendo almacenamiento fuera del sitio.
<p>NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001</p>	<p>20. De acuerdo con el análisis de la documentación aportada por la dependencia, se observó la definición de un conjunto de actividades</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

<p>Anexo A, A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</p> <p>“Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información”</p>	<p>que buscan mantener el funcionamiento óptimo de las actividades misionales de la entidad en su sistema de información, para lo que establecen enfoques de la siguiente manera:</p> <p>Preventivo: Dentro de este aspecto se involucran los recursos humanos tanto funcionarios, contratistas o terceros de la ANT, quienes deben estar preparados en caso de presentarse un evento inesperado, y las acciones anticipadas que se puedan coordinar y prever en el marco de la gestión de la entidad en los diferentes procesos misionales que sean afectados por la interrupción del servicio del SIT.</p> <p>Reactivo: Este aspecto va dirigido a fortalecer las políticas internas de la ANT y comunicarlas oportunamente para ponerlas en marcha una vez detectada y convocada la contingencia y el DRP.</p> <p>Recuperación: Este aspecto está enfocado en las actividades a desarrollar en el momento de atender una contingencia, una vez se haya cumplido con el protocolo de invocación del DRP. La descripción consecutiva de las actividades en los diferentes momentos estará definida en el documento denominado “Formato Manual DRP - Nov 2019” anexo a este documento.</p>
<p>NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001</p> <p>Anexo A, A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</p> <p>“Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio”</p>	<p>21. De acuerdo a la documentación aportada por la dependencia, se observó que el plan de continuidad del negocio contempla la necesidad de establecer una política de pruebas con una periodicidad mínima de un año. Sin embargo, hace falta desarrollar dicha política.</p> <p>Opciones de Mejora:</p> <p>21.1Elaboración Documentación: Se sugiere elaborar, documentar y comunicar la política de pruebas en la entidad. Esta debe incluir además de las pruebas los elementos de mantenimiento y reevaluación del plan de continuidad del negocio evidenciado las oportunidades de mejora de acuerdo con los resultados de las pruebas efectuadas en la ejecución del Plan de Continuidad del Negocio.</p>

3.3 REQUISITOS CON CUMPLIMIENTO – CONFORMIDADES – GESTION DOCUMENTAL

La gestión documental tiene una gran connotación en las entidades públicas, teniendo en cuenta la importancia de los documentos que se reciben y producen en la Agencia Nacional de Tierras, la normatividad archivística establece la obligación de generar mecanismos y herramientas que permitan asegurar la información institucional desde su uso, origen hasta su destino final, con el objeto de facilitar su uso, conservación y preservación. Las entidades públicas deben velar por la eficiente gestión de documentos, contemplando el uso de nuevas tecnologías y soportes, en cuya aplicación deberán observarse los principios y procesos archivística.

Es así como el SIT debe tener en cuenta que, para la gestión misional, es necesario contar con la parametrización de los diferentes instrumentos archivísticos dentro de su funcionalidad.



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Criterio	Observación
<p>Decreto 1080 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura” Presidencia de la Republica</p> <p>ARTÍCULO 2.8.2.5.9. PROCESOS DE LA GESTIÓN DOCUMENTAL. LA GESTIÓN DOCUMENTAL EN LAS DIFERENTES ENTIDADES PÚBLICAS EN SUS DIFERENTES NIVELES, DEBE COMPRENDER COMO MÍNIMO LOS SIGUIENTES PROCESOS. (...)</p>	<p>1. De acuerdo a la documentación aportada por la dependencia y a las mesas de trabajo efectuadas se observó que en la validación de los tipos documentales generados por el SIT contra los tipos documentales pertenecientes a series y subseries del cuadro de actualización de las Tablas de Retención Documental se observó que algunos de ellos no coinciden.</p> <p>Opciones de Mejora:</p> <p>1.1 Actualización tipos documentales TRD: Se sugiere actualizar la totalidad de tipos documentales pertenecientes a series y subseries producidos y tramitados en el SIT teniendo en cuenta que los siguientes no guardan relación:</p> <ul style="list-style-type: none"> • Autos (Apertura y Cierre) • Solicitud FISO • Solicitud de información • Colillas (Firma FISO)
<p>Decreto 1080 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura” Presidencia de la Republica</p> <p>DECRETO 1080 DE 2015 “POR MEDIO DEL CUAL SE EXPIDE EL DECRETO ÚNICO REGLAMENTARIO DEL SECTOR CULTURA” PRESIDENCIA DE LA REPUBLICA</p> <p>Artículo 2.8.2.6.1. Generalidades del sistema de gestión documental. Las entidades públicas deben contar con un sistema de gestión documental que permita. (...)</p>	<p>2. De acuerdo a la información aportada por la dependencia, así como una revisión a expedientes del SIT y ORFEO se evidencio la disposición de series, subseries y tipos documental, así como el establecimiento de plazos de conservación y eliminación, en donde debido a el proceso de actualización de las TRD convalidadas se concluye que, por su reciente convalidación, no se han realizado transferencias documentales.</p> <p>Así mismo la agrupación de la documentación en Series y subseries facilita la integridad de los documentos y favorece el acceso y disponibilidad a la información.</p> <p>La interoperabilidad de los documentos del SIT se realiza mediante integración al sistema documental ORFEO, sin embargo, en este no se encuentran parametrizadas las TRD convalidadas ni en proceso de actualización. Del mismo modo y de acuerdo a la información reportada en mesa de trabajo, la entidad se encuentra definiendo y planificando la puesta en marcha del Sistema de Gestión de Documentos Electrónicos de Archivo - SGDEA por lo cual los documentos del SIT se integran con ORFEO pero no tienen definidos esquemas de metadatos que garanticen la integridad de los mismos</p>
<p>Decreto 1080 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura” Presidencia de la Republica</p> <p>ARTÍCULO 2.8.2.7.1. Aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.</p>	<p>3. De acuerdo a la información reportada en mesa de trabajo, la entidad no cuenta con definición de tipo de expediente (mixtos (híbridos), digitales y electrónicos) dado que no se cuenta con un SGDEA implementado. Dicha implementación es responsabilidad de Secretaria General, quien se encuentra llevando a cabo gestiones para su desarrollo.</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

<p>Es responsabilidad de las Entidades Públicas cumplir con los elementos esenciales tales como: autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad y conservación, que garanticen que los documentos electrónicos mantienen su valor de evidencia a lo largo del ciclo de vida, incluyendo los expedientes mixtos (híbridos), digitales y electrónicos.</p>	
<p>Acuerdo 004 de 2019 Por el cual se reglamenta el procedimiento para la elaboración, aprobación, evaluación y convalidación, implementación, publicación e inscripción en el Registro único de Series Documentales – RUSD de las Tablas de Retención Documental – TRD y Tablas de Valoración Documental – TVD Archivo General de la Nación</p> <p>TÍTULO 4</p> <p>IMPLEMENTACION, PUBLICACIÓN E INSCRIPCIÓN EN EL RUSD DE LAS TABLAS DE RETENCIÓN DOCUMENTAL -TRD Y TABLAS DE VALORACIÓN DOCUMENTAL TVD</p> <p>TÍTULO 5</p> <p>ACTUALIZACION Y MODIFICACIÓN DE LAS TABLAS DE RETENCIÓN DOCUMENTAL – TRD</p> <p>ANEXO 1.1</p> <p>INSTRUCTIVO DE DIGILIGENCIAMIENTO DEL FORMATO DE TABLA DE RETENCIÓN DOCUMENTAL</p> <p>Artículo 17. Implementación.</p> <p>Artículo 22. Eliminación de Documentos.</p>	<p>4. De acuerdo a la Información aportada por la dependencia se encuentra que cuenta con TRD convalidadas, y cuadro de caracterización diligenciado en el marco de las mesas de trabajo con el equipo de Gestión Documental donde se encuentra la traza de la actualización de las series, subseries y tipos documentales.</p> <p>Dicha actualización la está tramitando Secretaría General frente al Archivo General de la Nación - AGN</p>

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Artículo 23. Actualización.	
-----------------------------	--

Como resultado de la presentación de los resultados del Informe Preliminar de la Auditoría de la Gestión de la Información efectuado por el equipo Auditor de la Oficina de Control Interno el día 12 de noviembre al área auditada, se recibió contestación por medio de correo electrónico de la Subdirección de Sistemas de Información el día 13 de noviembre de 2020 el cual indico lo siguiente:

“Luego de revisar el informe preliminar la Subdirección de Sistemas de Información de Tierras SSIT, en cabeza del Subdirector manifiesta no tener observaciones sobre el informe, tal y como se expresó en la reunión de cierre de la auditoría la SSIT acepta las recomendaciones o mejoras y los 2 hallazgos que fueron identificados producto de la auditoría al Sistema de Integrado de Tierras y al Plan de Continuidad del Negocio”.

“Por otro lado los temas relacionados con la infraestructura tecnológica fueron analizados por el Equipo de Infraestructura de la ANT y ellos sí tuvieron observaciones sobre algunos puntos los cuales están referenciados en el documento adjunto (Informe Auditoría Preliminar 09112020 BG.doc), de igual manera se adjuntan las evidencias suministradas por el Equipo de Infraestructura sobre los temas observados”.

De acuerdo con las observaciones emitidas por el Grupo de Infraestructura y Soporte Tecnológico efectuados en el mismo informe mediante comentarios al documento la Oficina de Control Interno emite las siguientes apreciaciones:

DISEÑO Y ARQUITECTURA DEL SISTEMA DE INFORMACIÓN

Página del informe No 6 a la opción de mejora 1.1. que indica:

1.1 Seguridad de la Información: *Se sugiere incluir dentro de la carpeta donde están alojados los documentos de arquitectura de la aplicación, los documentos relacionados con seguridad de la información del Sistema de Información de Tierras en cuanto a: control de accesos, seguridad perimetral, pruebas de vulnerabilidades efectuadas, planes de remediación, Auditorías Activas.*

Observación No. 1 Equipo de Infraestructura señala lo siguiente:

“Es solo incorporar los diseños y las pruebas entregadas por EIST. La remediación depende de su plan de trabajo”.

Apreciaciones de la Oficina de Control Interno a la observación recibida

Se reitera la explicación efectuada en la reunión de cierre de la Auditoría, especio en el cual se ilustro al área, de la necesidad de incorporar al repositorio dispuesto para tal fin, la información que esté relacionada con seguridad de la

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

información del Sistema de Información de Tierras, lo que indica el equipo de infraestructura hace parte de la información que se debe analizar por los responsables, en cuanto si debe o no incluirse en el repositorio.

Página del informe No 9 Numeral 4 indica:

4. La Entidad mediante el procedimiento **ADMBS-P-016 PROCEDIMIENTO GESTIÓN DE LOS SERVICIOS TECNOLÓGICOS**, presenta las acciones que se llevan a cabo para la atención de los servicios tecnológicos a través de la mesa de servicio, no se observa que específicamente se tengan definidos Acuerdo de Niveles de Servicio para la atención de los incidentes que se generen sobre el Sistema de Información de Tierras.

Con base a lo anteriormente expuesto y teniendo en cuenta que el Sistema de Información de Tierras, es uno de los aplicativos COR de la Entidad, es necesario que se defina unos ANS para la atención de los incidentes que sean solicitados a través de la mesa de ayuda, garantizando que la atención de los casos sea oportuna de acuerdo con la prioridad que se defina en los ANS.

Observación No. 2 Equipo de Infraestructura señala lo siguiente:

“Esto es ambiguo... Si se debe ampliar el catálogo para los servicios relacionados con el SIT se puede hacer, deben especificar cual serán requisitos y cuales incidentes, para estos últimos, se deberá definir la criticidad de los mismo para asociar el SLA. Adicionalmente, no sé si Basco lo quiera llevar a una falla que presente indisponibilidad total en los servicios y como se va a manejar”.

Apreciaciones de la Oficina de Control Interno a la observación recibida

Teniendo en cuenta la observación, se clarifica que el propósito de la misma corresponde a las mencionadas en el numeral 4 y la opción de mejora 4.1, ahí se indica la necesidad de incluir unos Acuerdo de Niveles de Servicios enfocados a la requerimientos, incidentes o problemáticas que se puedan estar presentando en el Sistema de información de Tierras, la forma como se implemente estas características deben ser definidas entre el administrador de la aplicación o la persona responsable de la atención de los casos con el acompañamiento del equipo de infraestructura, determinando las mejores opciones y la mediciones que dieran a lugar.

Página del informe No 11 Opción de mejora No. 7.2 el cual indica:

7.2 Elaboración de Documentos: Se recomienda la elaboración de un documento donde se incluyan las siguientes características de la operatividad del comité de control de cambios de la Entidad donde se indiquen las siguientes características:

- Integración del comité de Control de Cambios,
- Gobernabilidad del Comité
- Funciones del Comité
- Responsabilidades del Comité
- Periodicidad del Comité
- Documentos de Salida (actas, informes)

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Adicionalmente se debe gestionar ante la Dirección General el documento interno donde se autoriza la creación del comité de control de cambios para la Entidad.

Observación No. 3 Equipo de Infraestructura señala lo siguiente:

- “Esto ya lo tenemos nosotros que pusimos en marcha el comité de cambios y respondemos por él, si lo necesitan se los compartimos.
- Hasta donde sé esto no es un tema de dirección general, esto es algo que se define a nivel nosotros para controlar las actividades que ejecutamos a nivel tecnológico. Nosotros lo podemos socializar, pero no que se requiera autorización de la dirección”.

Apreciaciones de la Oficina de Control Interno a la observación recibida

De acuerdo con la información enviada por el equipo de infraestructura mediante correo electrónico de fecha 17 de noviembre en donde se adjunta dos (2) documentos denominados de la siguiente manera:

- Cambios CI.pptx – Tipo de Archivo Presentación
- GINFO-I-015-INSTRUCTIVO-DE-BUENAS-PRÁCTICAS-EN-ITIL-PARA-LA-GESTIÓN-DE-LA-MESA-DE-SERVICIOS-DE-TI- Tipo de Archivo Documento PDF

Se observa en la documentación suministrada que existe el proceso de control de cambios como uno de los apartes de las buenas practicas en ITIL para la gestión de la mesa de servicios de TI, sin embargo, es necesario complementar la información descrita en donde se incluyan temas como:

- **Integración del comité de Control de Cambios**, lo que se pretende en este aparte es el de incluir cuales son los roles dentro de la entidad que conformarían el comité indicando las funciones y responsabilidades que deberán asumir en este comité.
- **Documentos de Salida**, de acuerdo con la información enviada, se evidencia un repositorio para las actas de los comités de control de cambios, sin embargo, solo dos (2) de las cuatro subcarpetas tiene información de las actas gestionadas, (actas 3 y 4), adicionalmente es necesario que estos documentos estén acompañados con sus respectivos anexos complementarios como son: planes de trabajo e informes de ejecución.

En cuanto a la observación para la normalización del comité de control de cambios, si bien el equipo de infraestructura definió el comité, este debe ser formalizado ante las dependencias encargadas de gestionar la inclusión de estas mesas técnicas, donde se definirán los requisitos que se deben cumplir para su legalización, puesta en producción y socialización ante toda la Entidad.

Teniendo en cuenta lo anteriormente mencionado se procederá al cambio en la redacción de la opción de mejora 7.2 en este informe final, teniendo en cuenta que se allegaron documentos relacionados con esta observación y que hacen parte integral de la auditoria.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Página del informe No 11 Numeral No. 8 el cual indica:

De acuerdo con la información revisada en la ejecución de la auditoría en cuanto a respaldos de la información se valida el cumplimiento del proceso denominado **GINFO-P-009-GENERACIÓN-COPIAS-DE-RESPALDO-DE-LA-INFORMACIÓN-CRITICA-DE-LA-ANT**, sin embargo no se evidencia actividades previas donde las dependencias como responsables de la información informen las premisas de cumplimiento de los respaldos o backups que sean requeridos teniendo en cuenta su criticidad en las bases de datos así como también en los sistemas de información.

Observación No. 4 Equipo de Infraestructura señala lo siguiente:

“Esto lo hablamos en una reunión con el Ing. Duberly, hasta donde corresponde lo estamos haciendo bien, si quieren ir más allá de hacer pruebas de la data con la operación en ambientes controlados queda a su criterio”.

Apreciaciones de la Oficina de Control Interno a la observación recibida

En vista de que la responsabilidad de la opción de mejora indicada en la observación está a cargo de la Subdirección de Sistema de Información de Tierras, y que de acuerdo con su respuesta al informe preliminar no fue objeto de observación, esta oportunidad de mejora se mantiene, teniendo en cuenta la importancia de cerrar el ciclo de las pruebas de restauración de los backups, en donde es necesario probar la data respaldada funcional en el Sistema de Información de Tierras SIT.

Página del informe No 12 Numeral No. 8 el cual indica:

Estos respaldos de la información se están realizando tanto a los ambientes de producción como al de pruebas, en cuanto a las custodia de los backups esta actividad está a cargo del área de infraestructura, sin embargo, no se evidencia las bitácoras donde se registre la información que se encuentra en custodia. (el subrayado es nuestro)

Observación No. 5 Equipo de Infraestructura señala lo siguiente:

Que se cuenta con toda la información.

Apreciaciones de la Oficina de Control Interno a la observación recibida

De acuerdo con la información enviada por el equipo de infraestructura mediante correo electrónico de fecha 17 de noviembre en donde se adjuntan dos (2) documentos denominados de la siguiente manera:

- Jobs de Tareas de Backups
- Jobs de Tareas de Backups

Adicionalmente se adjunta pantallazos de la ubicación y direccionamiento donde se guardan los backups (custodia).

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

La Oficina de Control Interno procedió a la validación de la información, donde se evidencia las tareas programadas de los backups que respaldan la información, adicionalmente en las imágenes enviadas se puede validar las rutas donde se custodia o almacena la data.

Teniendo en cuenta lo anteriormente mencionado se procederá a la eliminación de la observación indicada en este informe de la versión final, así como también la opción de mejora mencionada en cuanto a la bitácora de custodia de información.

Página del informe No 12 Numeral No. 8 el cual indica:

*En cuanto a temas de restauración de la información respaldada, el área de infraestructura está realizando pruebas aleatorias de todas las bases de datos incluyendo las SIT, esta información esta evidenciada de acuerdo a lo registrado en la forma **NOVEDADES DE BACKUPS DE LA INFORMACIÓN CRÍTICA DE LA ANT**, donde las restauraciones de las bases de datos asociadas al SIT tienen como resultado exitoso, sin embargo, es necesario que se incluya una actividad en el proceso, donde desde el ambiente pruebas del SIT se realice el direccionamiento donde se restauró la información con el objetivo de validar dentro de la aplicación que la información no ha sido corrupta o presentan fallas a la restauración.*

Observación No. 6 Equipo de Infraestructura señala lo siguiente:

“Bajo su consideración por las implicaciones”.

Apreciaciones de la Oficina de Control Interno a la observación recibida

En virtud que la responsabilidad de la observación indicada en el numeral está a cargo de la Subdirección de Sistema de Información de Tierras, y de acuerdo con la respuesta al informe preliminar no fue objeto de observación, esta revisión se mantiene, esto teniendo en cuenta la importancia de cerrar el ciclo de las pruebas de restauración de los backups, en donde es necesario probar la data respaldada funcional en el Sistema de Información de Tierras SIT.

Página del informe No 13 Numeral No. 8 el cual indica:

*Adicionalmente se procedió a revisar la **INTI-Política-001 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** en donde su Numeral 7.9 Respaldo de la Información indica todo lo relacionado con el respaldo de la Información, con sus obligaciones relacionadas con los sistemas de información, sin embargo no se evidencio los documentos asociados a cada obligación de este criterio (formas, procedimientos) y más aún no se suministró documentación que valide el proceso que se está realizando específicamente a las copias de las máquinas virtuales donde funciona y opera el SIT.*

Observación No. 7 Equipo de Infraestructura señala lo siguiente:

La información fue entregada.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Apreciaciones de la Oficina de Control Interno a la observación recibida

Como se indicó en la reunión de cierre y en las mesas de trabajo realizadas con el área responsable, la observación está enfocada a que se debe relacionar en la política todos los documentos que estén asociados al respaldo de la información de los sistemas de información.

En cuanto a la documentación que valide el proceso que se está realizando específicamente a las copias de las maquinas virtuales, la Oficina de Control Interno reviso la documentación suministrada evidenciando la ejecución del proceso, por lo tanto, se procederá a el cambio en la redacción en la observación efectuada en cuanto a este tema.

Página del informe No 13 Numeral No. 8 Opción de Mejora No. 8.1 el cual indica:

8.1 Inclusión de Información: *Se sugiere incluir en el procedimiento **GINFO-P-009-GENERACIÓN-COPIAS-DE-RESPALDO-DE-LA-INFORMACIÓN-CRITICA-DE-LA-ANT** temas como:*

Análisis de la información a respaldar para su actualización, o inclusión de nuevas rutas teniendo en cuenta las observaciones que sean emitidas por las Dependencias responsables de la información del Sistema de Información de Tierras.

Observación No. 8 Equipo de Infraestructura

“No entiendo el contexto”.

Apreciaciones de la Oficina de Control Interno a la observación recibida

Como se indicó en la reunión de cierre y en las mesas de trabajo realizadas con el área responsable, la observación está enfocada a que es necesario que dentro del procedimiento **GINFO-P-009-GENERACIÓN-COPIAS-DE-RESPALDO-DE-LA-INFORMACIÓN-CRITICA-DE-LA-ANT**, se incluya una actividad previa donde se valide con las dependencias que la información que se está respaldando no haya cambiado las rutas o se necesite algunas adicionales.

Página del informe No 13 Numeral No. 8 Opción de Mejora No. 8.2 el cual indica:

8.2 Elaboración de Procedimiento: *Se sugiere elaborar un Proceso donde se describa el método y actividades que se debe implementar y ejecutar para los backup que se realizan a la configuración del SIT, incluyendo las acciones para la puesta en producción de una copia de la configuración en caso de contingencia.*

Observación No. 9 Equipo de Infraestructura señala.

“Ya existe en el procedimiento de backup. Lo último, se remite a un DRP que se mirará en 2021 porque tiene una serie de implicaciones muy importantes”.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Apreciaciones de la Oficina de Control Interno a la observación recibida

Si bien existe un procedimiento de backup general, se hace necesario realizar un proceso específico para el entorno general del SIT en cuanto a temas de backups, teniendo en cuenta que es uno de los sistemas de información de misión crítica de la entidad, en cuanto a las acciones de puesta en producción de una contingencia del SIT, es necesario definir las acciones que puedan determinar el funcionamiento y operatividad del sistema en caso de una emergencia de manera preventiva.

Página del informe No 13 Numeral No. 8 Opción de Mejora No. 8.4 el cual indica:

8.4 Respaldo a Cinta: *Se recomienda realizar copias de respaldo de la información crítica de la entidad de las bases de datos y sistemas de información a cintas magnéticas a través de un robot de cintas (dataprotector).*

Observación No. 10 Equipo de Infraestructura señala lo siguiente:

“Lo vamos a implementar, no con dataprotector que requiere licencia e incrementaría los costos. Con Veeam lo vamos hacer, los full de fin de año van en disco y a cinta. Solo tenemos un robot con un drive”.

Apreciaciones de la Oficina de Control Interno a la observación recibida

Con fundamento en la opción de mejora descrita, la pretensión de la recomendación efectuada por la Oficina de Control Interno es que se pueda proyectar la implementación de backups a través de cintas magnéticas como un respaldo adicional en un medio extraíble, la forma como se realice esta disposición del área de infraestructura de acuerdo con sus recursos tecnológicos actuales.

Página del informe No 13 Numeral No. 8 Opción de Mejora No. 8.5 el cual indica:

8.5 Elaboración de Procedimiento: *Se sugiere la elaboración de un procedimiento donde la dependencia responsable del sistema de información SIT, realice las pruebas de consistencia de la información de las restauraciones de los backups que el área de infraestructura realiza, como actividad final ejecutándose en el ambiente de pruebas.*

Observación No. 11 Equipo de Infraestructura señala lo siguiente:

“A su criterio”.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Apreciaciones de la Oficina de Control Interno a la observación recibida

En vista de que la responsabilidad de la observación indicada en el numeral está a cargo de la Subdirección de Sistema de Información de Tierras, y que de acuerdo con su respuesta al informe preliminar no fue objeto de anotación, esta observación se mantiene, esto teniendo en cuenta la importancia de cerrar el ciclo de las pruebas de restauración de los backups, en donde es necesario probar la data respaldada funcional en el Sistema de Información de Tierras SIT.

Página del informe No 14 Numeral No.9 el cual indica:

Se verifico el diseño de arquitectura de seguridad del SIT donde a nivel de la WAN se evidencia varios puntos de control antes de llegar a los servidores donde esta alojada la aplicación, en cuanto a la red LAN de la Entidad, solamente se cuenta como punto de seguridad el SW CORE para restringir y tener un control sobre la información que entra y sale de la Entidad, es necesario establecer puntos de control adicionales, que garanticen una barrera antes de ingresar a la red LAN permitiendo establecer un perímetro de seguridad en las comunicaciones para evitar accesos no autorizados y ataques.

Observación No. 12 Equipo de Infraestructura señala lo siguiente:

“Esto está mal, el tráfico está protegido pues de entrada como de salida está protegido por el FW. Cuando ingresa el tráfico tenemos varios equipos de perímetro”.

Apreciaciones de la Oficina de Control Interno a la observación recibida

La Oficina de Control Interno manifiesta no estar de acuerdo con a la observación efectuada, esto teniendo en cuenta la mesa de trabajo realizada con el equipo de infraestructura y la SSIT, ahí se mostró el diseño de la red LAN en donde solamente el punto de control que se evidencio para el sistema de información de tierras era el SW COR, y de lo cual se manifestó en los resultados expuestos en el cierre de la auditoria.

El equipo de infraestructura mediante correo electrónico enviado el día miércoles 18 de noviembre manifiesta a la observación lo siguiente:

1. *“La petición realizada al Registro Tipo A a sit.agenciadetierras.gov.co (201.217.200.211) desde Internet, pasa por el DDoS, luego va al Firewall, quien envía el paquete al WAF, de ahí va al servidor”.*
2. *“Cuando la petición sale directamente desde las estaciones de trabajo al Registro DNS sit.agenciadetierras.gov.co (172.23.90.45), sale del equipo, pasa por los switch de borde, baja por backbone, llegue al CORE, pasa por el Firewall que levanta la CAPA 3 del segmento de servidores, regresa al CORE y sale directamente al ENCLOSURE a través de un port channel”.*

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Apreciaciones de la Oficina de Control Interno a la observación recibida

Para la aclaración No.1, la explicación es valida teniendo en cuenta el diseño indicado en las mesas de trabajo, sin embargo, es necesario realizar la documentación técnica pertinente que soporte lo mencionado teniendo en cuenta la infraestructura de la red WAN.

Para la aclaración No. 2 la explicación técnica efectuada procede, sin embargo, es necesario que este tipo de explicaciones técnicas estén soportadas mediante un documento donde se indique de manera específica la estructura de la red LAN y los puntos de control (seguridad) que están implementados en la Entidad.

Por lo anteriormente expuesto se procede al cambio en la redacción de la Observación y de las opciones de mejora indicadas en el Numeral.

Página del informe No 14 Numeral No.9 Opción de Mejora 9.2 el cual indica:

Análisis de Seguridad Red LAN: *Se recomienda realizar un análisis de seguridad de los puntos de red de la Entidad para determinar cuales están en uso, y en consecuencia realizar los apagados de puertos en los Switches perimetrales con el objetivo de mantener un control de seguridad para el acceso a la red, adicionalmente se sugiere implementar métodos de seguridad en los puertos de la red como por ejemplo autenticación mediante el protocolo 802.1. X.*

Observación No. 13 Equipo de Infraestructura

Si bien es cierto que esto es una oportunidad de mejora que ya evidenciamos, no tiene nada que ver con el SIT, esto aplica para toda la infraestructura.

Apreciaciones de la Oficina de Control Interno a la observación recibida

La Oficina de Control Interno manifiesta su inconformidad a la observación efectuada, pues técnicamente el SIT funciona a través de toda la infraestructura tecnológica de la Entidad y mas aun en la red LAN de la entidad, donde todos los funcionarios o contratistas que por injerencia deben acceder al SIT desde un punto de red que pertenece a la red LAN, existiendo la posibilidad de intrusiones no autorizadas por falta de controles en los puntos finales como bien lo mencionamos en la opción de mejora.

PLAN DE CONTINUIDAD DEL NEGOCIO

Página del informe No 27 Numeral No.19 el cual indica:

Se observó, de acuerdo al análisis de la documentación dispuesta por la dependencia un alto nivel de dependencia de la operación que mantiene con los sistemas de información para su gestión misional, articulándose con la metodología de riesgos de la entidad, incluyendo estos temas en el mapa de riesgos institucional, mediante el desarrollo del mapa de riesgos de seguridad.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

De igual manera se valida las medidas de reducción de riesgo las cuales son dispuestas en el plan continuidad de la siguiente manera:

- Instalación de fuentes de poder interrumpibles y respaldo de energía a los equipos de cómputo y servidores.
- Sistemas tolerantes a fallas para las aplicaciones críticas donde aún la más mínima inactividad es inaceptable.
- Arreglos RAID y discos espejos para servidores LAN para prevenir en contra de pérdida de datos y asegurar disponibilidad continuada de datos.
- Equipos/componentes de repuesto para ser usados en el evento de falla de un equipo o componente – por ejemplo, un servidor LAN de repuesto preconfigurado con la configuración estándar y disponible para reemplazar un servidor defectuoso con el menor tiempo de configuración y construcción.
- Eliminación de puntos únicos de falla, tales como puntos únicos de acceso a la red o suministros únicos de energía dentro de un edificio.
- Sistemas de TI y redes resistentes.
- Servicios tercerizados con más de un proveedor.
- Mayores controles de seguridad tanto físicos como basados en TI.
- Mejores controles para detectar interrupciones de servicio, tales como sistema de detección de incendios, acompañados con sistemas de supresión.
- Una amplia estrategia de recuperación y respaldo, incluyendo almacenamiento fuera del sitio.

Observaciones No. 14 Equipo de Infraestructura señala lo siguiente:

- *Si, se debe organizar la parte eléctrica y tener un UPS independiente para Datacenter y los Equipos de Computo.*
- *Esto no se define de esta forma...*
- *Todos los almacenamientos están en esas condiciones.*
- *Esto funciona así en ambientes virtualizados.*

Apreciaciones de la Oficina de Control Interno a la observación recibida

Por parte de la Oficina de Control Interno se deja la claridad que de acuerdo a lo expuesto en las mesas de trabajo y la explicación de los resultados preliminares de la Auditoría efectuados a los interesados en los tiempos indicados de acuerdo al plan de auditoría, las observaciones efectuadas por el equipo de Infraestructura no son procedentes, pues lo que se indica en la observación efectuada, es que existe el cumplimiento del criterio con base a la Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC sobre el plan de continuidad del negocio elaborado por la Entidad.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

3.2 REQUISITOS CON INCUMPLIMIENTO – NO CONFORMIDADES

	Observación
<p>Guía para la preparación de las TIC para la continuidad del negocio – Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.</p> <p><i>Descripción Detallada de la Preparación de las TIC para la continuidad del negocio y el modelo de operación de Seguridad y Privacidad de la Información</i></p> <p><i>Ciclo de funcionamiento del modelo de operación de continuidad del negocio y su funcionamiento dentro del modelo de operación seguridad y privacidad de la información y la descripción detallada de cada una de las fases</i></p> <ul style="list-style-type: none"> - Planificación - Implementación - Gestión - Mejora Continua 	<p>No. conformidad 1. Debilidades en la gestión en la ejecución de las fases para el cumplimiento de la preparación de las TIC para la Continuidad del Negocio de la Entidad.</p> <p>De acuerdo con la información suministrada se evidenciaron debilidades en la falta de Gestión y Planeación para el avance de la implementación de la preparación de las TIC para continuidad del negocio, lo anterior en virtud de las revisiones efectuadas en cada componente que menciona la Guía, solamente se ha logrado avanzar en algunos aspectos técnicos que conforman el Plan de Continuidad del Negocio en su etapa de planificación.</p>
<p>Modelo de Gestión IT4+ Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC .</p> <p><i>Mantenibles - Los sistemas deben ser operativamente gestionados tanto en la parte técnica como financiera</i></p>	<p>No. conformidad 2. Debilidades en la gestión para realizar acciones que garanticen que en el Sistema de Información SIT y sus componentes, se ejecuten actividades periódicas de mantenimiento.</p> <p>De acuerdo con las revisiones efectuadas a la documentación soporte del criterio y a las mesas de trabajo realizadas con el auditado, no se evidencian implementación de procesos o actividades en producción que se estén llevando a cabo para una gestión de mantenimiento de la aplicación SIT en su entorno técnico como son:</p> <ul style="list-style-type: none"> - Mantenimiento preventivo - Mantenimiento predictivo - Mantenimiento correctivo - Mantenimiento adaptativo - Mantenimiento evolutivo



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

4. GESTION DEL RIESGO

A continuación, se registra el cumplimiento de los controles a los riesgos identificados en el mapa de riesgos de la Agencia con relación al proceso de Gestión de Información:

No.	NOMBRE DE RIESGO	ACCION DE CONTROL	CUMPLIMIENTO CONTROLES
R35	Perdida de información	<p>Generar copias de seguridad de base de datos, ambientes web y aplicativos.</p> <p>Ejecutar plan de pruebas de los sistemas de información de la entidad.</p> <p>Pruebas automáticas de integridad a las copias de seguridad.</p> <p>Modulo auditoria del SIT</p>	<p>Se observó que se está realizando los respaldos de información sobre el Sistema de Información de Tierras, tanto en capa de aplicación como en las bases de datos con un Fullbackup con una periodicidad diaria, es decir de la totalidad de los datos alojados en la base de datos como también del servidor donde esta alojada la aplicación</p> <p>Es necesario incluir en el protocolo de pruebas de recuperación o restauración de los datos respaldados la validación y consistencia de los datos en el Sistema de Información de Tierras.</p> <p>Se observo que se tiene habilitadas auditorias en las bases de datos relacionadas con el SIT, así como también en la aplicación, pero es necesario definir el tratamiento de la información que genera las auditoria determinando las acciones de control y seguimiento que se deben efectuar.</p>
R38	Inconsistencias de la información.	Generar copias de respaldo y respaldo de información	Se observó que se está realizando los respaldos de información de las bases de datos que están relacionadas con el sistema de información de Tierras, sin embargo, es necesario incluir temas de actualización de la información a respaldar donde se involucren las dependencias de la Entidad.
R40	Perdida de disponibilidad de sistemas de información y servicios TIC	<p>Copias de respaldo de los sistemas de información</p> <p>Atención y corrección de incidencias sobre los sistemas de información.</p>	<p>Se observó que se está realizando los respaldos de información sobre el Sistema de Información de Tierras, tanto en capa de aplicación como en las bases de datos con un Fullbackup con una periodicidad diaria, es decir de la totalidad de los datos alojados en la base de datos como también del servidor donde esta alojada la aplicación.</p> <p>Es necesario incluir en el protocolo de pruebas de</p>



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

			<p>recuperación o restauración de los datos respaldados la validación y consistencia de los datos en el Sistema de Información de Tierras.</p> <p>Se observo que se tiene habilitadas auditorias en las bases de datos relacionadas con el SIT, así como también en la aplicación, pero es necesario definir el tratamiento de la información que genera las auditoria determinando las acciones de control y seguimiento que se deben efectuar.</p> <p>Adicionalmente es necesario que se defina los Acuerdo de Niveles de Servicio para la atención de los casos o incidentes que se generen en la mesa de ayuda para el Sistema de Información de Tierras.</p>
--	--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5. CONCLUSIONES

5.1 DISEÑO Y ARQUITECTURA DEL SISTEMA DE INFORMACIÓN

- Al realizar la evaluación de la documentación y de más evidencias que soportan la Gestión de la información se concluye que el Sistema de Información de Tierras ha sido desarrollado teniendo en cuenta las buenas prácticas y demás normativas asociadas el desarrollo de aplicaciones, también se evidencia que su administración, uso y demás características están siendo gestionadas de manera adecuada.
- En cuanto al diseño y arquitectura que se han implementado en el Sistema de información de Tierras, se evidencia que se han tenido en cuenta las buenas prácticas, incluyendo las capas de gestión que un sistema necesita y requiere para un óptimo funcionamiento.
- Se evidencia temas de seguridad de la información que han sido implementados por medio de auditorias activas tanto en el Sistema de Información, como en la base de datos, sin embargo, el tratamiento de la información que se genera por parte de estas auditorias no se le está realizando los tratamientos frecuentes con el propósito de emitir alertas tempranas en los cambios de la información que se realicen por medio de la aplicación y la base de datos.
- Es importante realizar los ajustes sugeridos a la documentación asociada a los procesos que involucran el Sistema de Información de Tierras teniendo en cuenta su entorno general (bases de datos, aplicación, accesos, red, seguridad)
- Elaborar la documentación sugerida a los procesos auditados teniendo en cuenta los criterios de auditoria evaluados por la Oficina de Control Interno en la ejecución del ejercicio de la auditoria.
- Se evidencia la falta de documentación en cuanto a procesos de mantenimiento y administración tanto para las bases, como también en el Sistema de información, teniendo un alto grado de criticidad a las fallas o situaciones que se pueden detectar de manera oportuna para una atención prioritaria.



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

5.2 PLAN DE CONTINUIDAD DEL NEGOCIO

A partir de la observación del cumplimiento de requisitos y de la información dispuesta por la Subdirección de Sistemas de Información de Tierras, adicionalmente teniendo en cuenta los parámetros definidos en la Guía para la preparación de las TIC para la continuidad del negocio y el Anexo A, A.14 Gestión de la Continuidad del Negocio de la Norma Técnica NTC-ISO/IEC Colombiana 27001, se presentan las siguientes conclusiones:

- Se evidencia que la Entidad ha desarrollado las primeras etapas de continuidad del negocio en su fase de planeación, sin embargo, existen requisitos de cumplimiento que no han sido abordados los cuales son importantes para cerrar actividades dentro de las fases que se proponen.
- No se evidencia una planeación respectiva al cumplimiento de implementación de las fases a corto, mediano y largo plazo.
- La dependencia responsable ha desarrollado el documento: **"ANT-Plan de Continuidad del Negocio - Nov 2019"**, en donde se consignan las actividades de prevención, detección y corrección a llevar a cabo ante una eventualidad que comprometa la prestación de servicios incluyendo los sistemas de información de Misión Crítica.
- El documento "ANT-Plan de Continuidad del Negocio - Nov 2019" define entre otros aspectos los objetivos y alcance en la preparación de las TIC para continuidad del Negocio.
- De acuerdo a la evaluación efectuada el nivel de madurez del Plan de Continuidad del Negocio se determina que este se encuentra en una fase de preparación y ajustes al documento, es decir un nivel de madurez es inicial en la fase de planeación, está pendiente el desarrollo o ejecución de algunos criterios y anexos de información que son requeridos como son :
 - Política para la preparación de las TIC para la continuidad del negocio (IRBC)
 - Asignación de recurso humano competente y capacitado, comunicación de roles y responsabilidades para la preparación de las TIC para la continuidad del negocio (IRBC)
 - Definición de un plan de requerimientos
 - Documentación y comunicación de las rutinas de mantenimiento, prevención y copias de seguridad
 - Desarrollo de la política de pruebas de la entidad
 - Desarrollo del Analisis de Impacto del Negocio BIA (sus siglas en ingles)

5.3 GESTION DCOUMENTAL

Por otro lado, de acuerdo a los criterios de gestión documental definidos en el presente ejercicio se encontraron los siguientes resultados:

- La dependencia tuvo en cuenta para la mayoría de salidas del sistema, la definición de series, subseries y tipos documentales consignadas en el ejercicio de actualización de TRD liderado por el equipo de gestión documental de la Secretaría General.
- Existe una relación coherente entre las agrupaciones documentales del SIT y los expedientes relacionados que se administran en el Sistema Documental ORFEO, desarrollado en la Entidad.

	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

Por lo anteriormente expuesto el grupo auditor evidencio Dos (2) No Conformidades y treinta y cuatro (34) Opciones de Mejora en cumplimiento del objetivo de la Auditoria.

6. RECOMENDACIONES

6.1 DISEÑO Y ARQUITECTURA DEL SISTEMA DE INFORMACIÓN

Es necesario precisar que las “Recomendaciones” propuestas corresponden a las planteadas por la Oficina de Control Interno, que en ningún caso son de obligatoria ejecución por parte de la Entidad, sin embargo, se hace un llamado a ser consideradas en los planes de acción a que haya lugar en las vigencias futuras.

1. Actualizar la documentación de acuerdo a las recomendaciones o sugerencias descritas en las oportunidades de mejora, con el objetivo de fortalecer las acciones y mitigar la falta de conocimiento de la información.
2. Elaborar la documentación sugerida descritas en las oportunidades de mejora asociadas a los procesos evaluados.
3. Formalizar los procesos que se están ejecutando de manera informal en cumplimiento de los objetivos propuestos.
4. Evaluar la pertinencia a los cambios propuestos en el entorno donde opera el Sistema de Información de Tierras.

6.2 PLAN DE CONTINUIDAD DEL NEGOCIO

1. Elaborar los documentos pertinentes de planeación (cronograma, plan de proyecto) donde se defina como se va a realizar los temas pendientes y prioritarios para el desarrollo de la continuidad del negocio en la Entidad a corto, mediano y largo plazo de acuerdo con las proyecciones que se puedan tener para su cumplimiento.
2. Documentar y socializar una Política para la preparación de las TIC para la continuidad del negocio (IRBC)
3. Definir el plan de requerimientos de acuerdo a la Guía para la preparación de las TIC para la continuidad del negocio.
4. Asignar el recurso humano competente y capacitado, comunicando sus respectivos roles y responsabilidades para la preparación de las TIC para la continuidad del negocio.
5. Documentar y comunicar las rutinas de mantenimiento, prevención y copias de seguridad.
6. Fortalecer la definición de estrategia de IRBC.
7. Documentar aspectos clave como lecciones aprendidas, planes de trabajo, planes de acción y demás elementos, conformando así una base de conocimiento que sistematice la experiencia de trabajo, habilidades y conocimiento general.



	FORMA	INFORME DE AUDITORÍA	CÓDIGO	SEYM-F-007
	ACTIVIDAD	EVALUACIÓN INDEPENDIENTE	VERSIÓN	1
	PROCESO	SEGUIMIENTO, EVALUACIÓN Y MEJORA	FECHA	22-06-2017

8. Garantizar que la infraestructura de los sistemas de recuperación de TIC y la información crítica estén separadas del sitio operacional
9. Construir y comunicar el documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
10. Gestionar la aprobación del plan y el árbol de comunicaciones en caso de contingencia.
11. Documentar y comunicar la Política de pruebas en la entidad.

6.3 GESTION DOCUMENTAL

12. Relacionar la totalidad de salidas del sistema con los tipos documentales de acuerdo a la normatividad documental de la entidad.
13. Mantener la coherencia entre los expedientes del SIT y los gestionados en el aplicativo ORFEO.

Aprobó,

LILIBETH AGUILERA PUA

Auditor Líder

(Documento Original Firmado)

Elaboró,

BASCO GERMAN RICAURTE GUERRA

Auditor

(Documento Original Firmado)

SERGIO ALEJANDRO MATIZ PARRA

Auditor

(Documento Original Firmado)

Bogotá, 19 de noviembre de 2020.

