Tipo de Informe	Preliminar		Definitivo	X	**Fecha de Emisión del Informe**	20	09	2021

1. INFORMACIÓN GENERAL	
Proceso (s) Auditado (s):	Gestión de Tecnologías de la Información
Actividad (es) auditada (s):	1) Caracterización Gestión de Tecnologías de la Información - C-TI-001, Versión: 3.0, fecha: 23/10/2019 2) Procedimiento Gestión del desarrollo de software - P-TI-001, versión 4.0, fecha 23/04/2020 3) Guía estándares y lineamientos para desarrollo de software - GU-TI-001, Versión 2.0, fecha 13/11/2020 4) Procedimiento Gestión de cambios - P-TI-005, versión 1.0, fecha 29/08/2018 5) Procedimiento para la prestación de servicios TI – P-TI-007, versión 3.0, fecha 23/10/2019 6) Procedimiento gestión de la capacidad de TI - P-TI-009, versión 1.0, fecha 06/11/2019 7) Procedimiento Pruebas de rendimiento, carga y estrés para desarrollos de software - P-TI-010, versión 2.0, fecha 07/05/2020 8) Protocolo para la ejecución de pruebas de seguridad para los desarrollos de software - PR-TI-003, versión 1.0, fecha 14/05/2020 9) Mapa de riesgos 10) Plan de mejoramiento
Dependencia:	Oficina Asesora de Informática (OAI)
Líder del Proceso / Jefe(s) Dependencia(s):	Hernán Darío Gutiérrez Casas – Jefe Oficina Asesora de Informática
Objetivo de la Auditoría:	Evaluar las actividades y soportes del proceso Gestión de Tecnologías de la Información, así como el diseño y efectividad de los controles asociados a este y a los riesgos identificados en el proceso.
Objetivos Específicos:	1) Evaluar los registros y las evidencias asociadas con la ejecución de los procedimientos, instructivos, políticas, protocolos y demás documentación relacionada con el proceso. 2) Verificar la aplicación de controles en actividades regulares, así como en los riesgos asociados a la seguridad de la información. 3) Efectuar el seguimiento y verificación de la efectividad de los Planes de mejoramiento.
Marco Normativo:	1) Caracterización del proceso

	2) Plan estratégico de tecnologías de la información - PETI 3) Matriz de riesgos institucional 4) Política de Gobierno Digital 5) Procedimientos, instructivos, políticas, protocolos y formatos del proceso 6) Plan de mejoramiento
Alcance:	Comprende la evaluación de la ejecución de actividades, controles y seguimientos, según lo establecido en la caracterización, procedimientos, instructivos y protocolos definidos en el plan de auditoría, así como las normas aplicables al proceso de Gestión de Tecnologías de la Información. **Periodo auditado**: 01 de julio de 2020 al 30 de junio de 2021

Fecha Reunión de Apertura			**Vigencia Auditada**	2020 – 2021
16	06	2021		

Auditor Líder	**Auditor (es) de Apoyo**
Yaneth Montoya García	-

2. SITUACIONES DETECTADAS DURANTE EL PROCESO DE AUDITORÍA

2.1 Resumen de la auditoría

El 24 de febrero de 2021 fue aprobado en Comité Institucional de Coordinación de Control Interno el Plan de Auditorías para la vigencia 2021 y dentro de este se encuentra el proceso Gestión de Tecnologías de la Información. Por lo anterior, se da inicio a esta auditoría el día 16 de junio de 2021 con la ejecución de la reunión de apertura y la participación del líder del proceso, el ingeniero Hernán Darío Gutiérrez Casas, Jefe de la Oficina Asesora de Informática, en la cual se solicitaron los documentos y las evidencias a la Oficina Asesora de Informática, de acuerdo con las actividades auditadas y el alcance descrito en este documento.

La información para el desarrollo de la auditoría fue compartida por el ingeniero Hugo Ramírez a través de OneDrive y las evidencias adicionales fueron recopiladas en las mesas de trabajo y pruebas de recorrido llevadas a cabo en las siguientes fechas:

- 22 de julio: prueba de recorrido virtual del Procedimiento Gestión del desarrollo de software - P-TI-001 en el aplicativo BNLE – Banco Nacional de Listas de Elegibles, realizada con los ingenieros Leonardo Chaves Chaves y Hugo Fernando Ramírez Ospina

- 23 de julio: prueba de recorrido presencial del Procedimiento Gestión del desarrollo de software - P-TI-001 en el aplicativo SIMO – Sistema de apoyo para la Igualdad, el Mérito y la Oportunidad, realizada con el ingeniero Jeison Hernan Candamil Mahecha y en forma virtual el ingeniero Hugo Fernando Ramírez Ospina y de forma parcial la ingeniera Claudia Ardila
- 27 de julio: mesa de trabajo virtual con la ingeniera Lorena Moreno, para observar el método de seguimiento a los planes de trabajo.
- 09 de agosto: prueba de recorrido virtual del Procedimiento Gestión de la capacidad de TI - P-TI-009 – primera parte, con los ingenieros Milton Andrés Tovar Bonilla y Hugo Fernando Ramírez Ospina.
- 12 de agosto: prueba de recorrido virtual del Procedimiento Gestión de la capacidad de TI - P-TI-009 – segunda parte, con los ingenieros Milton Andrés Tovar Bonilla y Hugo Fernando Ramírez Ospina.
- 13 de agosto: mesa de trabajo virtual para aclaración de fichas de indicadores con el ingeniero Hugo Fernando Ramírez Ospina.

Nota: es importante mencionar que la auditoría estuvo suspendida entre el 30 de junio y el 20 de julio de 2021, debido a la finalización de los contratos de prestación de servicios, de algunas personas que iban a ser auditadas.

1) CARACTERIZACIÓN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Código: C-TI-001 Versión: 3.0 Fecha: 23/10/2019

Sobre este documento se revisaron las entradas, recursos, proveedores y salidas de los procedimientos que hacen parte del alcance de la auditoría, de los cuales se tienen observaciones que se describirán en los capítulos correspondientes a cada procedimiento.

Adicionalmente, se observó dentro del numeral 7 el procedimiento “Gestionar la Continuidad de los servicios de TI” el cual tiene como entradas:

a. Instituto de Ingenieros Eléctricos y Electrónicos – IEEE.
b. Organización Internacional de Estándares – ISO
c. Proceso de Infraestructura
d. Proceso de Planeación Institucional y programación presupuestal.

De otra parte, tiene como proveedores:

Norma técnica TIA-942 – Centros de cómputo. (a)
Norma técnica ISO 22301:2012 (b)
Suscripción con las Empresas de Servicios públicos (ESP) – energía eléctrica. (d)
Direccionamientos y recurso Humano para continuidad (d)

Se puede ver que la información se encuentra intercambiada entre las columnas, por lo cual se debe corregir para mantener la consistencia con el resto del documento.

Dentro de la caracterización se encuentra también el enlace al Normograma de la entidad, que al consultarlo lleva a dos procesos:

- Gestión de Recursos Tecnológicos
- Gestión de Tecnologías de la Información

Es necesario recordar que el proceso "Gestión de Recursos Tecnológicos" fue eliminado del mapa de procesos y por esta razón no debería hacer parte del Normograma, pero también está relacionado en la caracterización en el numeral 4 "Gestionar la prestación de los Servicios de TI".

Finalmente, se encontró que las últimas resoluciones y leyes incluidas en el Normograma corresponden a la vigencia 2019, por tanto, no se encuentran las posteriores como:

- Ley 2052 de 2020, relacionada con la racionalización de trámites, digitalización, automatización, trámites en línea, revisión, compilación y formularios únicos, servicios ciudadanos digitales, estampillas electrónicas, entre otros.
- Resolución 1519 de 2020, por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos.
- Resolución 2893 de 2020, por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano.
- Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
- Ley 2080 de 2021 en lo relacionado con Procedimientos Administrativos Electrónicos.

Es importante hacer un seguimiento continuo a la expedición de toda la normatividad relacionada con el proceso, para no solo actualizar el Normograma sino también para llevar a cabo los ajustes en los procesos, procedimientos, sistemas de información y demás temas internos en la entidad que se vean involucrados.

Como conclusión se evidencia que la Caracterización del proceso y el Normograma no se encuentran actualizados.

1) Procedimiento Gestión del desarrollo de software (P-TI-001)

Información requerida:

- Lista de personas que intervienen en el procedimiento identificando sus respectivos roles.

- Catálogo de sistemas de información.
- Diagramas en BPMN del procedimiento.
- Listado de solicitudes de desarrollo recibidas en el periodo auditado indicando la metodología utilizada (tradicional o ágil).
- Historias de usuario o casos de uso relacionados con las solicitudes atendidas.
- Documentación de artefactos o registros que soportan el procedimiento o acceso al repositorio donde se encuentren en modo de solo lectura.
- Registros en DNDA.

Dentro del procedimiento se indica lo siguiente: Toda la documentación (requerimientos, levantamientos de información, documentos técnicos, documentos de gestión de los proyectos y documentos para los usuarios finales) asociada a las actividades del procedimiento se manejará al interior de la OAI en los repositorios físicos y lógicos dispuestos para este propósito. La **estructura general de documentación** que se puede asociar a un proyecto de desarrollo corresponde a:

Nombre del Proyecto
0_Requerimientos
1_Planificacion
2_Analisis
3_Diseño
4_Implementacion
5_Pruebas
6_InstalacionDespliegue
7_MantenimientoYSoporte

Con este criterio se revisó la información dispuesta en el *file server* de la entidad (\\fileserver\SISTEMAS\SistemasDeInformacion), según se indica a continuación.

APLICATIVO BNLE – Banco Nacional de Listas de Elegibles

Carpeta: \\fileserver\SISTEMAS\SistemasDeInformacion\BNLE
Nota: la carpeta tiene la estructura descrita en el procedimiento, sin embargo, contiene información de requerimientos sólo hasta junio de 2020, tal y como se muestra en la imagen 1 tomada de dicho repositorio:

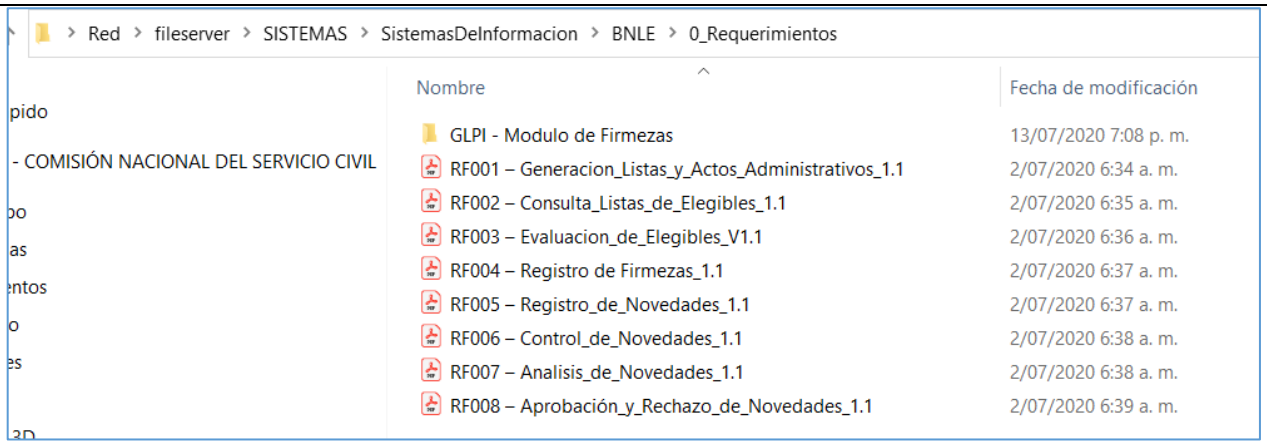

Imagen 1

Es necesario aclarar que los requerimientos RF001 a RF008 son de fecha 12 de junio de 2020.

Según la información proporcionada para la auditoría, la cual se observa en la imagen 2, existen 3 requerimientos adicionales para BNLE (aparecen en formato Word), los cuales al revisar en detalle el archivo corresponden a documentos elaborados entre el 11 de diciembre de 2020 y el 08 de marzo de 2021.

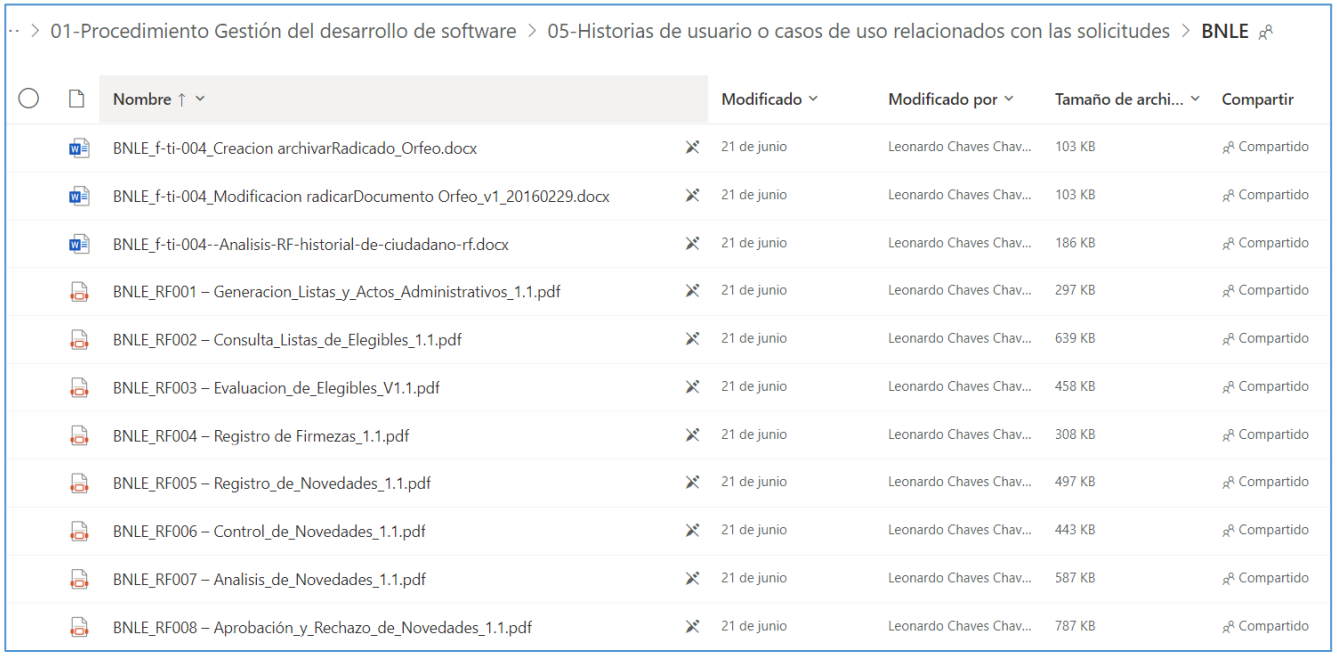

Imagen 2

Lo anterior muestra que el repositorio definido en file server no se encuentra actualizado. De otra parte, durante la prueba de recorrido llevada a cabo el 22 de julio para el aplicativo BNLE, el líder informó que todos los proyectos relacionados con SIMO 4.0 están usando GitLab, lo cual incluye BNLE, pero en la estructura presentada en GitLab durante la prueba no se observó que la información se esté organizando según lo descrito en el procedimiento. Por tanto, aunque se cambió el tipo de repositorio que se está llevando para los soportes documentales

bajo los cuales se ejecutan los requerimientos, en este caso GitLab, no se actualizó el procedimiento indicando las nuevas condiciones bajo las cuales se está operando.

Con relación a la **actividad 1.1.7.2** "Identificar necesidades" del procedimiento, se revisó en detalle la documentación de los siguientes requerimientos entregados en formato Word:

- Nombre del requerimiento: Creación del servicio web archivar Radicado

  Id. Requerimiento: RF001
  Fecha solicitud: 08 Mar 2021
  Formato utilizado para la documentación: FORMATO ANÁLISIS DE REQUERIMIENTOS FUNCIONALES, Código: F-TI-004 Versión: 1.0 Fecha: 29/02/2016

- Nombre del requerimiento: Módulo de historial del ciudadano

  Id. Requerimiento: RF001
  Fecha de la Solicitud: 16/12/2020
  Formato utilizado para la documentación: ANÁLISIS DE REQUERIMIENTOS FUNCIONALES, Código: F-TI-004 Versión: 2.0 Fecha: 12/01/2021

De los anteriores requerimientos se puede observar:

- Ninguno utilizó la versión del formato aprobada o que estaba vigente en la fecha en que se recogió la solicitud.
- Ambos requerimientos tienen el identificador RF001, aun cuando el campo ID debe corresponder con un número en consecutivo.
- En ninguno de los documentos se deja constancia certera de la aprobación del mismo, solamente se marca con una "x" en una casilla indicando si la persona aprobó o no y en algunos casos no hay ninguna marca.

La actividad 1.1.7.4 "Presentar requerimiento a la OAI" indica que, posterior al análisis, el documento de Requerimientos Funcionales se debe presentar formalmente a la Oficina Asesora de Informática. Esta solicitud puede realizarse mediante la remisión de un correo electrónico emitido desde el buzón del Líder de Proceso Institucional, o a través de una radicación de la solicitud en la herramienta de apoyo de la mesa de servicios de TI.

Para los 3 requerimientos entregados en formato Word y asociados al BNLE, no se encontró evidencia de la presentación de ninguno de ellos por correo ni por GLPI.

APLICATIVO EDL – Evaluación del Desempeño Laboral

Carpeta: \\fileserver\SISTEMAS\SistemasDeInformacion\EDL
Nota: contiene información de requerimientos hasta mayo de 2020, como se observa en la imagen 3.

Imagen 3

APLICATIVO MVP – Módulo de Pruebas Virtuales

Carpeta: \\fileserver\SISTEMAS\SistemasDeInformacion\Pruebas Informatizadas SIMO 4.0\1.Requerimientos
Nota: no se encontraron requerimientos, por lo cual se consultan en OneDrive los archivos proporcionados a la auditoría.

Carpeta en OneDrive:

- Archivo: Análisis Psicométrico de Ítems.docx

  Id. Requerimiento: RF001X
  Nombre requerimiento: Creación de
  Fecha solicitud: 08/01/2020

- Archivo: Construcción de Items.docx

  Id. Requerimiento: RF001X
  Nombre requerimiento: Creación de
  Fecha solicitud: (no definida)

- Archivo: Evaluación de Item Taller V 3.docx

  Id. Requerimiento: RF001X
  Nombre requerimiento: Creación de
  Fecha solicitud: (no definida)

- Archivo: Reclamaciones.docx

  Id. Requerimiento: RF001X
  Nombre requerimiento: Creación de
  Fecha solicitud: (no definida)

De los 4 documentos revisados se observa:

- Todos los archivos se encontraron en el formato Código: F-RT-001 ANÁLISIS DE REQUERIMIENTOS FUNCIONALES Versión: 1.0 Fecha: 29/02/2016, es decir, en un formato que no se encuentra vigente.
- Los documentos no contienen el consecutivo del requerimiento.
- Los campos no están completamente diligenciados.
- En 3 de los 4 no se encontró la fecha de la solicitud.
- No se encontró evidencia de la presentación de ninguno de los 4 requerimientos a la OAI, por correo ni en GLPI.

APLICATIVO RECOMENDADOR

Carpeta: \\fileserver\SISTEMAS\SistemasDeInformacion\Recomendador
Nota: la ubicación solamente contiene un requerimiento en 3 versiones, relacionado con: F-TI-004 - Recomendador de Empleo

Se consultó la carpeta en OneDrive encontrando el archivo:

- F-TI-004 - Recomendador de Empleo V21-DACA.docx

  Código: F-RT-001 ANÁLISIS DE REQUERIMIENTOS FUNCIONALES Versión: 1.0 Fecha: 29/02/2016
  Id. Requerimiento: RF001X
  Nombre requerimiento: Creación del recomendador de empleos a través de SIMO
  Fecha solicitud: 03-02-2021

Frente a este documento se repiten las observaciones hechas a los del aplicativo MPV, a excepción de la presentación del requerimiento a la OAI, dado que se encontró en GLPI el ticket 75464 con el trámite correspondiente.

APLICATIVO RPCA – Registro Público de Carrera Administrativa

Se revisaron los siguientes archivos en la carpeta de OneDrive:

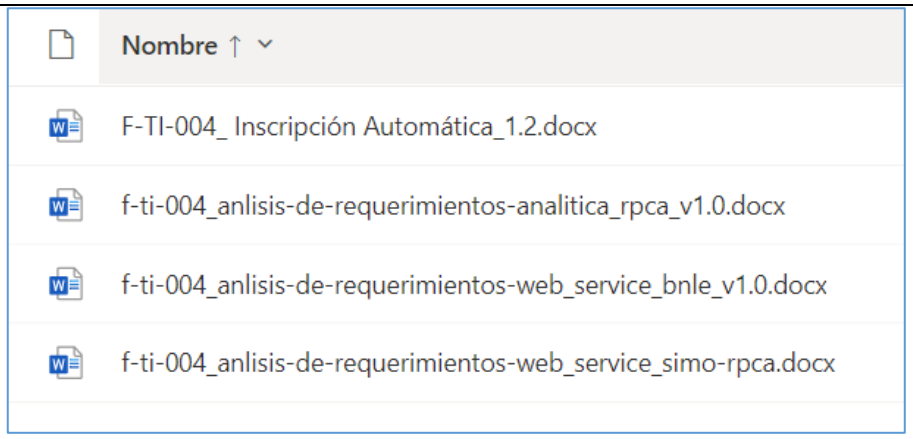

Imagen 4

Del análisis de los 4 documentos se observa:

- Ninguno de los 4 archivos contiene el ID del requerimiento
- No es claro cómo se está llevando a cabo la aprobación de los requerimientos. Hay varios roles descritos en los formatos, pero el procedimiento señala que hay una validación inicial realizada por el Jefe de la OAI y en ninguno de los formatos se indica que hubo alguna revisión, validación o aprobación por parte de dicho rol.
- No se encontró evidencia de la presentación de ninguno de los 4 requerimientos por correo ni en GLPI.

APLICATIVO SIMO – Sistema de apoyo para la Igualdad, el Mérito y la Oportunidad

Carpeta: \\fileserver\SISTEMAS\SistemasDeInformacion\SIMO
Nota: se revisaron los archivos listados a continuación.

- Decreto 2365 de 2019 Ingreso jovenes V1 2021_ glpi75856.docx

  Formato empleado: Código: F-RT-001, Versión: 1.0, Fecha: 29/02/2016
  Nombre requerimiento: Ceración de nuevo campo – Módulo Búsqueda de ofertas de empleo en SIMO.
  Id. Requerimiento: RF001X
  Fecha solicitud: 20-01-2021

- Requerimiento - Excepciones V6_glpi79500.docx

  Formato empleado: Código: F-RT-001, Versión: 1.0, Fecha: 29/02/2016
  Nombre requerimiento: Adición de funcionalidades SIMO para la Dirección de Administración de Carrera Administrativa y gerentes de convocatoria
  Id. Requerimiento: RF001X
  Fecha solicitud: 19-04-2021

Nuevamente se observa que, de acuerdo con la fecha de solicitud, se están utilizando formatos desactualizados, además, no se está usando adecuadamente el campo de ID. En este caso sí se encontraron en la herramienta de mesa de servicios GLPI los tickets 75856 y 79500.

En conclusión, se encontraron fallas en el uso del formato F-TI-004 Análisis de requerimientos funcionales, versión 2.0, fecha: 12/01/2021, dado que en algunos casos se está empleando una versión obsoleta del mismo y en otros casos no se diligencia la información completamente, no se diferencian entre sí los requerimientos por medio del campo de consecutivo (ID) diseñado para tal fin y no se cuenta con evidencias de la aprobación por parte de los involucrados. Lo anterior genera debilidad en la documentación de los requerimientos desde su levantamiento, muestra falta de control en la documentación, impide tener trazabilidad en el tiempo sobre lo establecido por los involucrados y puede generar cambios no controlados.

De otra parte, en la prueba de recorrido de este aplicativo, el líder informó que en la herramienta GitLab se manejan todas las solicitudes de desarrollo y/o requerimientos, incluyendo los documentos de pruebas de los requerimientos del sistema, de manera que en esta herramienta se maneja el repositorio de código fuente, el control de versiones y los archivos asociados al desarrollo, por lo cual se recomienda establecer estándares para organizar la información y garantizar los criterios de calidad de la misma.

En cuanto a la **actividad 1.1.7.10 "Estimar esfuerzo de desarrollo"** del procedimiento, se indica que se llevará a cabo el cálculo del esfuerzo (tiempo y cantidad de horas de trabajo) que pueden ser necesarios para poder atender el requerimiento presentado. En las observaciones de la ejecución del procedimiento se encontró que se utiliza Excel para hacer estos cálculos, siendo esta una estimación subjetiva según el criterio de quien la hace y en otros casos se asignan las tareas a través de los tableros en GitLab, sin embargo, esta última herramienta no permite conocer los porcentajes de avance, balancear cargas de trabajo o conocer cuánto trabajo tiene asignado una persona.

Se evidencia entonces debilidad en el control que se debe realizar sobre la asignación de cargas laborales a las personas del equipo de trabajo, lo que genera dificultad para determinar fechas de finalización de los desarrollos con alto grado de certeza, impactando el cumplimiento de los objetivos institucionales.

La actividad **1.1.7.14 "Definir metodología de desarrollo"** aparece dentro del procedimiento después de levantar los requerimientos, pero en la auditoría se pudo observar que este paso se lleva a cabo antes del levantamiento.

Dentro de la actividad **1.1.7.21 "Remitir a pruebas de QA (Funcionales, REC y Vulnerabilidades)"** se confirmó a través de las evidencias aportadas a la auditoría, que se están ejecutando diferentes tipos de pruebas, sin embargo, no se encontró que se estén realizando pruebas específicas sobre usabilidad y accesibilidad, aun teniendo en cuenta que la mayoría de los aplicativos desarrollados por la OAI serán utilizados por la ciudadanía y que existe normativa nacional relacionada con el tema que se debe cumplir en el corto plazo.

Se encontró que las pruebas funcionales se ejecutan completamente de forma manual por parte de un grupo de personas asignadas específicamente a esta labor y que hay una iniciativa para desarrollar pruebas automatizadas que no se ha concretado.

En el procedimiento la actividad **1.1.7.27 "Ir a procedimiento gestión de pruebas"** indica que es "un llamado al procedimiento vigente de gestión de pruebas de calidad del software que abarca desde el momento en que el líder de un grupo desarrollo de software hace entrega formal del conjunto de objetos y artefactos que comprenden la solución del requerimiento aprobado, hasta que el grupo de aseguramiento de calidad de software entrega el visto bueno de aceptación de la solución". En las pruebas de recorrido y en la revisión documental no se encontró dicho procedimiento, ni evidencias de su ejecución.

Por lo anterior, se está incumpliendo la actividad 1.1.7.27 del procedimiento, dado que no se realizan pruebas de calidad de software por parte del equipo de trabajo, ni verificaciones que permitan minimizar los riesgos de aparición de fallas en la operación, o aspectos implementados para mejorar la confianza de las partes interesadas.

En la actividad **1.2.1.2 "Validar conformidad legal"** se señala como participante al asesor legal de la OAI (interno o designado desde el proceso de representación judicial y extrajudicial), pero en las personas relacionadas con la ejecución del procedimiento no se encontró alguien desempeñando dicho rol.

En las actividades **2.1.1.19 "Realizar seguimiento de avances"** y **2.1.1.24 "Cronograma detallado"** se señala que se hace uso de cronogramas de trabajo y de las herramientas Openproject o Microsoft Project, con propósito de lograr una mayor efectividad al realizar seguimiento. La periodicidad de este se programa desde el inicio del proyecto y se debe realizar al menos una vez al mes o en eventos críticos. Este es un punto de control importante, dado que se compara lo planeado contra lo entregado, sin embargo, se observó el repositorio relacionado en el procedimiento y ubicado en la ruta (http://openproject.cnsc.gov.co/) y se encontró que desde 2019 no se actualiza esta herramienta, situación que se evidenció también en la auditoría anterior y sobre la cual se generó un plan de mejoramiento. Sobre esta situación se hará mención más adelante en el capítulo señalado como seguimiento al plan.

En la mesa de trabajo del 27 de julio con la ingeniera Lorena Moreno, se observó que se utilizan diferentes herramientas dentro de los equipos de trabajo para hacer seguimiento, tales como matrices en Excel, listados en SharePoint e incluso en Project de forma centralizada porque no se tienen suficientes licencias para que todos los involucrados hagan a través de esta herramienta el seguimiento. De otra parte, los proyectos que usan metodología ágil no elaboran cronogramas, usan GitLab básico que no tiene funcionalidades para conocer los porcentajes de avance y no hay un estándar para programar y hacer seguimiento al trabajo.

De acuerdo con todo lo expuesto anteriormente, se evidencia desactualización en el procedimiento Gestión del desarrollo de software, puesto que lo descrito en el documento P-TI-001 no corresponde con las condiciones bajo las cuales se está desarrollando actualmente el mismo.

2) Guía estándares y lineamientos para desarrollo de software - GU-TI-001, Versión 2.0, fecha 13/11/2020

Dentro del contenido de este documento se hace referencia a la "Guía de Roles y Responsabilidades del Proceso Gestión de TI", sin embargo, esta guía no se encontró dentro del Sistema de Gestión de Calidad de la entidad y para la auditoría fueron entregadas solamente matrices RACI de los aplicativos, las cuales, aunque contienen los roles, no contienen el detalle de las responsabilidades.

Con relación a los lineamientos de desarrollo, se revisaron secciones de código proporcionadas en las imágenes entregadas como evidencia para esta auditoría, en particular para BNLE y SIMO, de las cuales se halló lo siguiente:

- Se está utilizando el IDE Visual Studio Code, el cual no está relacionado en las plataformas estándar.
- En el documento la descripción de la notación Camel y la notación Pascal es la misma.
- No se está cumpliendo la estructura del nombre que debe manejarse en los repositorios de versionamiento, de acuerdo con el numeral 5.5 del documento.
- En las imágenes de métodos Java, las variables que se usan en los catch es una letra "e" y no cumpliría con ninguna de las notaciones mencionadas en el documento de estándares. El documento solo da permiso para usar variables locales de un carácter en ciclos FOR, pero no menciona que se incluya en el manejo de excepciones.

Por otra parte, en la actividad **5.11. "Accesibilidad y Usabilidad"** se mencionan los "Lineamientos y metodologías de Usabilidad para Gobierno en línea", pero esta información se encuentra desactualizada, dado que con el Decreto 1008 de 2018 se subrogó la Estrategia de Gobierno en Línea y se habilitó la Política de Gobierno Digital. En otros apartados del documento sí se hace referencia a Gobierno Digital.

Dado lo anterior, se evidencia incumplimiento a lo establecido en la Guía estándares y lineamientos para desarrollo de software - GU-TI-001, así como desactualización en la normatividad relacionada.

3) Procedimiento Gestión de cambios - P-TI-005, versión 1.0, fecha 29/08/2018

En la caracterización del proceso, en la sección de entradas a este procedimiento, se relaciona "Cronograma de aprovisionamiento de Infraestructura y despliegue de aplicativos", sin embargo, durante la auditoría no se encontraron dichos cronogramas y en especial, lo relacionado con aprovisionamiento en las fechas que se va a tener gran concurrencia de usuarios, como lo son las fechas límites de inscripción para las convocatorias de la entidad.

Con respecto al procedimiento se encontró:

- El documento tiene 3 años de haberse elaborado.
- La normatividad incluida en el capítulo 4 se encuentra desactualizada, como lo es el Decreto 1078 de 2015 y la NTC-ISO 20000, o en otros casos no tiene relación directa con el procedimiento, como es la Ley 909 de 2004.
- El nombre del archivo en PDF es "INTERRELACIÓN OBJETIVOS ESTRATÉGICOS DEL EJÉRCITO NACIONAL Vs".
- En las políticas de operación se informa que la mesa de trabajo de gestión de cambios debe reunirse de manera ordinaria todos los días miércoles de cada semana a las 09:00 (nueve de la mañana) o el siguiente día hábil. En la auditoría se determinó que ese horario no se cumple y, en este sentido, aun cuando la estandarización de día y hora de las reuniones es buena para organizar el tiempo, no se recomienda incluirla en los procedimientos.
- No se está ejerciendo control sobre la fecha en que se ejecutarán los cambios, dado que no hay una programación o una planeación general, sino que se llevan a la mesa de cambios a aprobación los requerimientos que van resultando. Por ejemplo, en el documento "Plan Despliegues SIMO" se encuentran los cambios realizados hasta el 18 de junio, pero no hay registro de los que continúan.
- No se encontró documentación actualizada sobre los cambios emergentes que se realizan semanalmente.
- Aun cuando se observó un listado en Excel con la relación de los tickets de servicio en GLPI asociados con los controles de cambio, se sugiere revisar si puede ser más eficiente la gestión de las solicitudes de cambio diligenciándose directamente en GLPI por el módulo de "Cambios".

En conclusión, se evidencia falta de planeación en la gestión de cambios y desactualización en el procedimiento.

4) Procedimiento para la prestación de servicios TI – P-TI-007, versión 3.0, fecha 23/10/2019

Tal y como se indicó en el Plan de auditoría, la información requerida para este punto tiene como objetivo el seguimiento a la eficacia del plan de mejoramiento de la auditoría 2020.

Para este caso se revisaron los tiempos de atención definidos en el CATÁLOGO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Código: PR-TI-005 Versión: 1.0 Fecha: 28/02/2021.

Se tomó como referencia el numeral 6.2.4.5. Servicio: *Permiso a usuarios*, el cual tiene como tiempo de asignación normal 30 minutos y tiempo de solución normal 3 horas. Se realizó un

filtro en GLPI de los tickets en la categoría "PERMISOS A USUARIOS", obteniendo los siguientes resultados:

ID	*Título*	*Fecha de Apertura*	*Fecha de solución*	***Conclusión**: Tiempo en dar solución*
82 374	Configuracion VPN Dispositivo Movil (82374)	29/06/2021 7:52	29/06/2021 9:55	2 horas 3 min
81 925	creacion usuario nukak (81925)	18/06/2021 6:50	21/06/2021 10:14	11,5 horas 46 min
82 303	Solicitud apoyo en actualización listado correos personal de planta (82303)	28/06/2021 10:23	28/06/2021 15:12	4 horas 49 min
82 126	SOLICITUD PERMISOS ACCESOS A EQUIPOS (82126)	23/06/2021 12:36	24/06/2021 12:10	11 horas 34 min
81 470	Solicitud Acceso Via VPN (81470)	3/06/2021 12:20	16/06/2021 20:27	74,5 horas 7 min
81 246	Asignación Permisos Ing. Ronald Pérez Sánchez (81246)	28/05/2021 15:02	29/05/2021 8:49	3 horas 51 min
81 264	Asignación Permisos Ing. Ronald Pérez Sánchez - Gitlab (81264)	29/05/2021 8:20	31/05/2021 7:57	27 min
80 900	Solicitud permiso a usuarios externos para consulta de carpeta en ONE DRIVE (80900)	21/05/2021 10:52	21/05/2021 19:42	8 horas 50 min

De los 8 tickets obtenidos en la consulta se pudo observar que:

- Las solicitudes en esta categoría son de diferentes tipos, incluyendo grados de dificultad diferentes.
- El ticket 82303 está mal categorizado, pues no corresponde a un permiso como tal.
- El ticket 81470 correspondía a un permiso y a una instalación de software, por lo cual el tiempo de atención se extendió.
- Sólo en el ticket 81264 se cumplió con el tiempo previsto de atención. No se tiene en cuenta el 81264 por ser una continuación del 81246.

En conclusión, aun cuando la Oficina Asesora de Informática elaboró el catálogo de servicios de TI y configuró los tiempos de atención en la herramienta GLPI, se advierten oportunidades de ajuste y mejora, tanto en las categorías como en los tiempos de atención, así como se refleja una posible falta de conocimiento de los usuarios finales al seleccionar el tipo de requerimiento en el momento de su apertura.

Adicionalmente, se observó que la herramienta GLPI posee módulos para gestionar Problemas, Cambios, Incidencias recurrentes, entre otros, y dichos módulos no contienen ninguna información. Esto indica que se está subutilizando una herramienta para diseñada para gestionar servicios de TI desde diferentes ámbitos.

5) Procedimiento gestión de la capacidad de TI - P-TI-009, versión 1.0, fecha 06/11/2019

Para la evaluación de este procedimiento se efectuó prueba de recorrido los días 9 y 12 de agosto con el ingeniero Milton Tovar. Se realizó la auditoría teniendo en cuenta lo descrito en el procedimiento, además de su función y utilidad, y la definición de **gestión de la capacidad** de ITIL, donde se indica que es un proceso utilizado para gestionar

las tecnologías de la información asegurando que la capacidad de los sistemas de TI cumplen los requisitos actuales y futuros de la organización con unos costes asumibles. Las distintas versiones de ITIL consideran que la gestión de la capacidad engloba tres subprocesos: gestión de la capacidad de negocio (en este caso las necesidades de la entidad pública), gestión de la capacidad del servicio (servicios de TI que soportan las necesidades de la entidad) y gestión de la capacidad de los componentes.

Con respecto a la actividad **1.2.2 "Validar requisitos de capacidad y desempeño",** en la prueba de recorrido se pudo determinar que se hace seguimiento a la plataforma de hiperconvergencia con la herramienta ZABIX, en cuanto a uso de memoria, disco, CPU y disponibilidad. Los umbrales bajo los cuales se hace este seguimiento están definidos en plantillas con valores estándar para la industria y no se han modificado según las necesidades de la entidad. Esto último indica que no se está dando cumplimiento a la actividad donde se menciona que "el líder de infraestructura de TI debe revisar detalladamente los requisitos de la Comisión respecto a las capacidades que deben tenerse de los recursos tecnológicos, y a las expectativas de funcionamiento de dichos recursos que se hayan ofrecido a las partes interesadas".

Para la adquisición de la plataforma actual de hiperconvergencia se informó a la auditoría que hubo una estimación de crecimiento de un 25% anual, pero estos cálculos no quedaron documentados.

Se preguntó por cómo se gestiona la capacidad en fechas donde hay picos de usuarios como aquellas que representan hitos importantes dentro de las convocatorias, para asignar recursos suficientes y evitar caídas de la plataforma, pero se informó a la auditoría que no se recibe dicha información de parte de los gerentes de las convocatorias, por lo cual no se conoce con antelación.

Por lo anterior, se establecen deficiencias en la gestión de la capacidad, dado que no se evidenció planificación de la demanda de servicios de TI y su impacto en la infraestructura de la entidad, en especial en fechas con alta concurrencia de usuarios. Esto representa debilidad en la futura justificación de las inversiones, riesgos de caídas de los servicios y falta de eficiencia en el manejo de los recursos.

6) Procedimiento Pruebas de rendimiento, carga y estrés para desarrollos de software - P-TI-010, versión 2.0, fecha 07/05/2020

Información recibida:
Como registros de las pruebas REC se recibieron documentos de pruebas en los aplicativos:

- Escuela virtual
- MPV
- Nuevo portal y Observatorio CNSC
- RPCA

Se observó que se está utilizando la herramienta JMETER para analizar la **carga** y ver con una determinada cantidad de usuarios si el software es capaz de soportarlo, en un lapso de tiempo determinado.

No se encontraron pruebas de **estrés** donde se esté saturando la solución de software, hasta un punto de quiebre donde aparezcan posibles defectos, potencialmente peligrosos y verificar si los mismos pueden se pueden recuperar de forma autónoma sin requerir la intervención humana.

Tampoco se encontraron pruebas de **rendimiento**, para determinar lo rápido que realiza una tarea un sistema en condiciones particulares de trabajo, que son definidas tomando como base los requerimientos expresados por el usuario final.

De esta manera, no se pudo evidenciar la completitud en la ejecución de las actividades del Procedimiento P-TI-010.

7) Protocolo para la ejecución de pruebas de seguridad para los desarrollos de software - PR-TI-003, versión 1.0, fecha 14/05/2020

Información recibida:
Como registros de las pruebas de seguridad se recibieron documentos de pruebas en los aplicativos:

- Portal unificado
- RPCA
- Nuevo portal web

Teniendo en cuenta que se han efectuado desarrollos para los aplicativos MPV y Escuela virtual, de acuerdo con las evidencias recibidas, no se ejecutaron pruebas de seguridad para estos sistemas.

Dado que los aplicativos que está desarrollando la entidad son de uso público, se recomienda que las pruebas de seguridad no se realicen por demanda, sino que se extiendan al 100% de los desarrollos.

8) Mapa de riesgos, versión 1.0, fecha 29/04/2021

Información requerida:
- Evidencias de la aplicación de los controles a cada uno de los riesgos del mapa (del 01 de enero de 2021 al 31 de mayo de 2021).

Para esta evaluación se tuvo en cuenta el Mapa de Riesgos de 2021 que publicó la Oficina Asesora de Planeación en la Intranet el pasado 05 de agosto de 2021, indicando como fecha de su actualización el 29 de abril de 2021.

No.	Riesgo	Controles	Observación
R-TI-001	Disminución de la oportunidad, eficiencia y efectividad en la prestación de los servicios TIC.	1. Revisión periódica de Plan Estratégico de Tecnologías de la Información - PETI, recibiendo reportes de avance y evidencias de las actividades ejecutadas en el periodo, para validar el cumplimiento de metas y proyectos. 2. Indicadores de efectividad sobre los proyectos clave del PETI.	El 29 de enero de 2021 se publicó la actualización al PETI vigencia 2019-2022. El documento indica que es versión 1, sin embargo, es la versión 3. No se encontraron los indicadores de efectividad mencionados en el segundo control.
R-TI-002	Indisponibilidad de las aplicaciones misión crítica de la entidad.	1. Monitoreo interno y externo al portal y a los servicios alojados, que permita evidenciar posibles interrupciones y adoptar medidas de contención y restauración. 2. Inventario de aplicaciones (sistemas de información) actualizado anualmente. 3. Mantener firewall para seguridad perimetral y Software de antivirus institucional.	Se encontraron los reportes de monitoreo. Se observan 3 caídas de casi una hora cada una en el portal web. No es claro cuáles medidas correctivas y preventivas se han tomado. Se recomienda hacer gestión con el catálogo de sistemas de información para optimizar temas como el uso de infraestructura.
R-TI-003	Errores no detectados en la construcción de las aplicaciones de software.	1. Asignación de un colaborador de cada grupo de desarrollo por parte de su líder, para la realización de pruebas funcionales, que debe registrar sus resultados en el formato vigente para tal fin (F-TI-002 - Formato de Pruebas Funcionales) y consignarlo en el repositorio de código fuente. 2. Tomando como base la información centralizada del repositorio de código fuente, generación de reportes por cada sistema relacionados con: requerimientos solicitados, pruebas realizadas y pruebas aprobadas.	Con respecto al control 1 se recomienda implementar pruebas automatizadas. No se encontraron evidencias sobre el control No. 2.
R-TI-004	Caída del portal web y los servicios desplegados a través de dicho portal.	1. Aplicar las actividades del instructivo para gestionar vulnerabilidades TI. 2. Mantener control de los contratos de servicios de telecomunicaciones (informes de gestión de los proveedores) 3. Incluir los servicios del portal web en el ambiente de contingencia.	No se encontraron registros que indiquen que el portal web se encuentra en ambiente de contingencia.
R-TI-005	Funcionalidad de las aplicaciones que no corresponde a lo esperado por el usuario.	1. Levantamiento de requerimientos con el usuario final. 2. Formato análisis de requerimientos funcionales (F-TI-004).	Como se indicó en el capítulo 1 de este documento, no se está utilizando correctamente el formato F-TI-004, por tanto, esta deficiencia en la documentación

R-TI-006	Documentación de usuario diferente a las funcionalidades de las aplicaciones.	1. Gestionar el código fuente y la documentación en GitLab y demás repositorios acordados por el arquitecto de sistemas de información. 2. Mantener una documentación de usuario y técnica actualizada y completa.	de los requerimientos puede llevar a que se materialice el riesgo. Dado que este tema se repite en el riesgo R-TI-006, se recomienda revisar los controles.
R-TI-007	Uso de datos de producción para propósitos de prueba.	1. Aplicar documento de gestión de pruebas funcionales para desarrollos de software (DOCUMENTO EN CONSTRUCCIÓN) en donde se especifica el uso del formato de pruebas funcionales (F-TI-002). 2. Asignación de un colaborador de cada grupo de desarrollo por parte de su líder, para la realización de pruebas funcionales, que debe registrar sus resultados en el formato vigente para tal fin (F-TI-002 - Formato de Pruebas Funcionales) y consignarlo en el repositorio de código fuente.	El control No. 1 se encuentra desactualizado. El control No. 2 se recomienda complementarlo incluyendo en los contratos de los ingenieros acuerdos de confidencialidad para el manejo de los datos.
R-TI-008	Inadecuada aplicación de los parches de software en la plataforma tecnológica de la Entidad.	1. Aplicar las actividades del instructivo para gestionar vulnerabilidades TI.	No se encontraron evidencias de la ejecución del control. Se solicita tomarlas para el próximo seguimiento de riesgos.
R-TI-009	Fallas temporales en los sistemas de comunicación de la CNSC con los usuarios.	1. Uso del formato "Informe complementario de supervisión periódico o final de los contratos - F-TI-006" 2. Mantener vigentes los contratos de servicios de telecomunicaciones.	Desde el día 05 de abril hasta el 08 de abril de 2021 se materializó el riesgo de fallas en los servicios, lo cual dificultó la inscripción de los aspirantes al proceso “Entidades del Orden Nacional Nación 3”. Según lo informado por el ingeniero Hernán Gutiérrez (jefe de la OAI) en sesión de sala del 08 de abril, esto se debió al cambio de proveedor del servicio de internet. Se solicita reportar lo sucedido en el formato disponible y administrado por la Oficina de Planeación, evaluar los controles y tomar las medidas necesarias para evitar nuevamente su ocurrencia.
R-TI-010	Instalación de software no autorizado o uso no autorizado de software valido por parte de cualquier colaborador de la Comisión.	1. Verificar en forma permanente que el software instalado esté debidamente licenciado. 2. Desplegar políticas de seguridad de la información.	Se realizó una prueba de escritorio en la cual se pudo descargar el ejecutable de una aplicación no autorizada, pero al momento de tratar de instalarla

			el sistema puso en cuarentena el archivo.
R-TI-011	Ataques informáticos.	1. Mantener consola de Antivirus actualizada. 2. Aplicar instructivo de uso adecuado de los recursos tecnológicos de la CNSC (I-TI-002).	No se recibieron evidencias sobre la ejecución de estos controles. Esta misma observación se hizo en el seguimiento a riesgos del primer cuatrimestre, por lo cual se reitera que es necesario documentar lo necesario.
R-TI-012	Daño en equipos informáticos asignados a los funcionarios en los puestos de trabajo.	1. Aplicar Instructivo de uso adecuado de los recursos tecnológicos de la CNSC (I-TI-002). 2. Realizar campañas de sensibilización sobre el uso de los equipos. 3. Mantener pólizas de seguros para los equipos actualizadas.	Se evidenció mediante los tickets en GLPI los mantenimientos a los equipos. Se recibió información sobre campaña en seguridad en los puestos de trabajo. Falta la evidencia del control No. 3.
R-TI-013	Presencia de Malware (Virus informáticos, Ransomware, Troyanos, Gusanos).	1. Mantener consola de Antivirus actualizada. 2. Aplicar instructivo de uso adecuado de los recursos tecnológicos de la CNSC (I-TI-002). 3. Aplicar instructivo Protección de la información digital - Herramienta de cifrado (I-TI-003).	No se evidenció la materialización del riesgo.
R-TI-014	Inadecuada gestión de las contraseñas.	Políticas generales de operación del directorio activo (GPO), para la administración de usuarios.	Se reitera la observación sobre la no aplicación de la política de contraseñas, en particular la que señala: “Cambie las contraseñas periódicamente. De forma obligatoria debe hacerlo cada treinta (30) días, siga este ciclo para aquellas aplicaciones que no le obliguen a realizar cambios periódicamente”. La política configurada está en 45 días.
R-TI-015	Descarga de aplicaciones, datos, imágenes o en general contenidos de internet sin control.	1. Políticas generales de operación del directorio activo (GPO), para la administración de usuarios. 2. Verificar en forma permanente que el software instalado esté debidamente licenciado.	No hay control eficiente sobre la descarga de aplicaciones u otros datos sin control, dado que es posible obtener desde internet archivos que pueden ser potencialmente perjudiciales. Se recomienda identificar controles que logren el bloqueo completo de este tipo de acciones.
R-TI-016	Uso de programas utilitarios o herramientas especializadas que cambien los controles establecidos.	1. Políticas generales de operación del directorio activo (GPO), para la administración de usuarios. 2. Verificar en forma permanente que el software instalado esté debidamente licenciado.	No se evidenció la materialización del riesgo, sin embargo, no se tienen evidencias de los controles aplicados.
R-TI-017	Eventos o incidentes sin solución definitiva.	Gestionar herramienta de Gestión de los Servicios de TI por la Mesa de Servicios.	En el reporte de mayo de 2021 hay 1.223 casos registrados, de los cuales había

			aproximadamente 135 sin resolver. Se solicita incluir para el próximo seguimiento la evidencia de la gestión efectiva sobre este tipo de situaciones.

9) Plan de mejoramiento correspondiente a la auditoría efectuada en la vigencia 2020

Información requerida:
Evidencias de las acciones adelantadas del plan de mejoramiento de las auditorías anteriores y registros de seguimiento.

En la auditoría se estableció el hallazgo 5 que indica: No se evidenciaron cronogramas de trabajo que permitan realizar un monitoreo y control sobre el desarrollo de cada uno de los proyectos del PETI; incumpliendo los "Mecanismos de Medición y Seguimiento" establecidos en el PETI Cuatrienio 2019 - 2022, generando riesgos en la ejecución y en el logro de las metas, por debilidad en los procesos de seguimiento.

Para dicho hallazgo se estableció un plan de mejoramiento, que luego de su verificación por parte de la Oficina de Control Interno se encontró que no había sido efectivo. Por lo anterior, la OAI generó un nuevo plan que contenía las siguientes actividades:

ACTIVIDAD	FECHA
1. Reorganizar los proyectos a cargo de la OAI con sus respectiva información general y específica.	11/05/2021
2. Clasificar los proyectos según los planes y metas institucionales.	13/05/2021
3. Revisar los cronogramas individuales de los proyectos.	14/05/2021
4. Comparar las actividades de los cronogramas individuales contra las actividades de los archivos de consolidación.	20/05/2021
5. Validar la completitud de las evidencias de avance aportadas hasta la fecha de corte.	20/05/2021
6. Actualizar las fechas reales de inicio y finalización de las actividades y de los proyectos individuales.	21/05/2021
7. Unificar las fuentes de información y los mecanismos de reporte de avance y seguimiento de actividades.	26/05/2021
8. Unificar los repositorios y estructuras de almacenamiento de las evidencias de avance presentadas por los proyectos.	26/05/2021
9. Validar la consistencia de alineación de los proyectos con respecto a los planes institucionales (PETI – POA – PAA)	28/05/2021
10. Presentar el estado final de la revisión y unificación del control de proyectos a los líderes funcionales, para su entendimiento y aceptación de responsabilidades frente al reporte oportuno de novedades y avances.	31/05/2021
11. Adoptar la herramienta de SEGUIMIENTO de proyectos	31/05/2021
12. Mantener actualizados los cronogramas y herramientas de control de la gestión de los proyectos.	05-05-2021 a 05-01-2022
13. Realizar el seguimiento y validación de cada uno de los proyectos.	Semanal
14. Presentar el estado general (avances y novedades) de los proyectos al Jefe de la OAI	Mensual

Con respecto a dicho plan se revisaron las evidencias aportadas por la oficina, en especial lo relacionado con la actividad No. 12 y de acuerdo con los cronogramas de trabajo de la ruta: \\fileserver\sistemas\ProyectosTI\Cnsc\2021\Consolidado Proyectos PETI -POA 2021\Cronogramas

Se encontró que el cronograma del proyecto "Nuevo Portal" para el mes de junio de 2021 indicaba un avance del 99% y una fecha de terminación el 28 de junio de 2021. El mismo proyecto para el mes de agosto tenía un cronograma con los mismos datos y el proyecto no había concluido.

Se revisó también el cronograma del proyecto "BNLE" el cual para junio mostraba avance del 95% y fecha de fin el 16 de julio de 2021. Para el mes de agosto el avance era del 91% y la fecha de finalización el 09 de agosto de 2021. A la fecha de revisión de esta información (el 27 de agosto de 2021) el proyecto no había concluido.

Lo anterior indica que, aun cuando se ha mejorado en la estrategia de seguimiento y organización de la información, todavía no se lleva un control con datos actualizados de los proyectos de la OAI. En el caso del portal se evidencia un atraso de 2 meses sobre la fecha establecida inicialmente por lo que se concluyen deficiencias en la planeación.

Se continuará haciendo el seguimiento a este plan de mejoramiento, en especial a la actividad No. 12 que tiene fecha de vencimiento en enero de 2022 y las actividades 13 y 14 que son de carácter permanente.

2.2 Hallazgos y/o No Conformidades

RECOMENDACIÓN 1:

Teniendo en cuenta el volumen de desarrollos ejecutados en la entidad y las necesidades de contar con aplicativos que cumplan con las expectativas de los usuarios, se recomienda implementar un proceso de pruebas automatizadas que permita disminuir los tiempos y ampliar los controles de calidad al software.

RECOMENDACIÓN 2:

Se recomienda ejecutar pruebas específicas sobre usabilidad y accesibilidad, teniendo en cuenta que la mayoría de los aplicativos desarrollados por la OAI serán utilizados por la ciudadanía y que existe normativa nacional relacionada con el tema que se debe cumplir en el corto plazo.

RECOMENDACIÓN 3:

Teniendo en cuenta que la herramienta GLPI contiene módulos relacionados con Problemas, Cambios, Incidencias recurrentes, entre otros, y que actualmente dichos módulos no contienen

ninguna información, se recomienda aprovechar dichas funcionalidades para automatizar procedimientos como el de Gestión de Cambios e implementar mejoras al proceso en general.

RECOMENDACIÓN 4:

Dado que los aplicativos que está desarrollando la entidad son de uso público, se recomienda que las pruebas de seguridad no se realicen por demanda, sino que se extiendan al 100% de los desarrollos.

RECOMENDACIÓN 5:

Teniendo en cuenta lo observado en el seguimiento al mapa de riesgos, se recomienda realizar análisis de los controles aplicados actualmente para fortalecer la gestión de riesgos y tomar los correctivos necesarios con las situaciones evidenciadas en el seguimiento.

RECOMENDACIÓN 6:

Se recomienda mantener toda la documentación del sistema de gestión de calidad actualizada, con los cambios que sean pertinentes para mantener una gestión de TI controlada y con resultados de valor para los usuarios finales y en particular a la ciudadanía.

HALLAZGO 1:

Criterio de auditoría: Caracterización del proceso GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Código: C-TI-001 Versión: 3.0 Fecha: 23/10/2019 y Normograma relacionado.

En la revisión documental se encontró que la caracterización del proceso y el normograma hacen mención del subproceso “Gestión de Recursos Tecnológicos” el cual fue eliminado en el año 2019 del sistema de gestión de calidad. De igual manera, el Normograma contiene resoluciones y leyes hasta 2019, por lo cual ambos documentos están desactualizados.

HALLAZGO 2:

Criterio de auditoría: procedimiento P-TI-001 “*Gestión del Desarrollo de Software*”.

Se encontraron fallas en el uso del formato F-TI-004 Análisis de requerimientos funcionales Versión: 2.0 Fecha: 12/01/2021, dado que en algunos casos se está empleando una versión obsoleta del mismo y en otros casos no se diligencia la información según los campos del formato. Además, no se cuenta con evidencias concretas de la aprobación del requerimiento por parte de los involucrados. Lo anterior genera debilidad en la documentación de los requerimientos desde su levantamiento, muestra falta de control en la documentación, impide tener trazabilidad en el tiempo sobre lo definido por los involucrados y puede generar cambios no controlados.

HALLAZGO 3:

Criterio de auditoría: procedimiento P-TI-001 "*Gestión del Desarrollo de Software*", actividad 1.1.7.10 "*Estimar esfuerzo de desarrollo*"

De acuerdo con los registros de la actividad, se evidencia debilidad en el control que se debe realizar sobre la asignación de cargas laborales a las personas del equipo de trabajo, lo cual genera dificultad para determinar fechas de finalización de los desarrollos con alto grado de certeza, impactando el cumplimiento de los objetivos institucionales.

HALLAZGO 4:

Criterio de auditoría: procedimiento P-TI-001 "*Gestión del Desarrollo de Software*", actividad 1.1.7.27 "*Ir a procedimiento gestión de pruebas*".

No se encontró información sobre el procedimiento "gestión de pruebas" ni evidencias sobre su ejecución, incumpliendo la actividad 1.1.7.27 del procedimiento P-TI-001. De la misma manera, no se encontraron registros de la ejecución de pruebas de calidad de software, ni verificaciones que permitan minimizar los riesgos de aparición de fallas en la operación, o aspectos implementados para mejorar la confianza de las partes interesadas.

HALLAZGO 5:

Criterio de auditoría: procedimiento P-TI-001 "*Gestión del Desarrollo de Software*".

De acuerdo con el trabajo desarrollado en la auditoría y lo referenciado en el primer capítulo de este informe, se evidencia desactualización en el procedimiento P-TI-001, puesto que lo descrito en el documento no corresponde con las condiciones bajo las cuales se está desarrollando actualmente el mismo.

HALLAZGO 6:

Criterio de auditoría: Guía estándares y lineamientos para desarrollo de software - GU-TI-001

En la revisión de las imágenes parciales del código fuente proporcionado para la auditoría, se observó que no se están cumpliendo los estándares y lineamientos de la guía, lo cual puede generar dificultades en el mantenimiento de los aplicativos, errores que no sean fácilmente rastreables e impedimentos para asegurar la calidad del software.

HALLAZGO 7:

Criterio de auditoría: Procedimiento Gestión de cambios - P-TI-005, versión 1.0, fecha 29/08/2018

No se encontró programación o cronogramas que indiquen que se está realizando la fase de planeación del procedimiento Gestión de cambios - P-TI-005. De otra parte, se encontró que la normatividad relacionada en el documento está desactualizada. Lo anterior evidencia falta de planeación, lo cual puede generar que los cambios se realicen de emergencia y de forma no controlada, elevando los niveles de riesgo de impactos negativos en otros componentes de TI de la entidad.

HALLAZGO 8:

Criterio de auditoría: Procedimiento gestión de la capacidad de TI - P-TI-009, versión 1.0, fecha 06/11/2019

Se encontraron deficiencias en la gestión de la capacidad, dado que no se evidenció planificación de la demanda de servicios de TI y su impacto en la infraestructura de la entidad, en especial en fechas con alta concurrencia de usuarios. Esto representa debilidad en la futura justificación de las inversiones, riesgos de caídas de los servicios y falta de eficiencia en el manejo de los recursos.

HALLAZGO 9:

Criterio de auditoría: Procedimiento Pruebas de rendimiento, carga y estrés para desarrollos de software - P-TI-010, versión 2.0, fecha 07/05/2020

No se pudo evidenciar la completitud en la ejecución de las actividades del Procedimiento de Pruebas de rendimiento, carga y estrés, dado que no se encontraron registros que muestren el ciclo completo de las pruebas, el cumplimiento del alcance de cada una de ellas y la toma de acciones frente a sus resultados. Lo anterior representa riesgos en la gestión, al disponer aplicativos a los usuarios que no tengan el rendimiento esperado.

3. CONCLUSIONES DE LA AUDITORÍA

3.1. La Oficina Asesora de Informática cuenta con documentación dentro del sistema de gestión de calidad que ha quedado desactualizada, bien sea por el tiempo que tiene de expedición o por los cambios que se han implementado en el área.

3.2. Se deben continuar fortaleciendo los controles e implementando mejores prácticas, para generar software de calidad a los usuarios, teniendo además en cuenta la normatividad nacional y la Política de Gobierno Digital.

3.3. Como fortaleza se han implementado herramientas como GitLab y Jmeter en búsqueda de mejoras para el proceso, pero es posible continuar con la búsqueda de otras herramientas que permitan automatizar mayor número de pasos en los procedimientos y así aumentar la capacidad del equipo y disminuir la probabilidad de error.

3.4. Es importante resaltar la participación y buena disposición de los auditados, lo cual permitió realizar las verificaciones requeridas según el alcance definido.

3.5. Se mantiene abierto el hallazgo No. 05 de la auditoría efectuada en la vigencia 2020, dado que aún no se encontraron los resultados esperados con el plan de mejoramiento.

4. PLAN DE MEJORAMIENTO

Como mecanismo de control la Oficina Asesora de Informática deberá elaborar un plan de mejoramiento, tendiente a generar acciones correctivas frente a las no conformidades y las acciones requeridas frente a las observaciones. Este plan deberá ser presentado a la Oficina de Control Interno máximo cinco (5) días hábiles después de la fecha de entrega del informe final de la auditoría.

5. ANEXOS

Los documentos soporte de la auditoría se encuentran en: \\fileserver\CONTROL_INTERNO\1. PAPELES DE TRABAJO (PAA- PA OCI)\1. AUDITORIAS\2021\6. Gestión de Tecnologías de la Información

Elaboró	Aprobó
ORIGINAL FIRMADO	ORIGINAL FIRMADO
MYRIAM NELLY BORDA TORRES Jefe Oficina de Control Interno	**YANETH MONTOYA GARCÍA** Auditor