Tipo de Informe	Preliminar		Definitivo	X	**Fecha de Emisión del Informe**	11	09	2020

1. INFORMACIÓN GENERAL	
Proceso (s) Auditado (s):	Gestión de Tecnologías de la Información
Actividad (es) auditada (s):	1) Procedimiento Gestión del desarrollo de software (P-TI-001) 2) Procedimiento Recibir información de IES para terminación de convocatorias (P-TI-004) 3) Procedimiento Gestión de cambios (P-TI-005) 4) Instructivo para la actualización o modificación de datos (I-TI-006) 5) Procedimiento Gestión de usuarios de TI (P-TI-006) 6) Procedimiento para la Prestación de servicios TI (P-TI-007) 7) Procedimiento Gestionar la plataforma de TI (P-TI-008) 8) Procedimiento Gestión de la capacidad de TI (P-TI-009) 9) Procedimiento Pruebas de rendimiento, carga y estrés para desarrollos (P-TI-010) y Protocolo para la ejecución de pruebas de seguridad para los desarrollos de software (PR-TI-003) 10) Requisitos de seguridad en el sistema de información SIMO 11) Mapa de riesgos aplicado al trabajo remoto 12) Plan Estratégico de Tecnologías de la Información – PETI vigencia 2019 – 2022 13) Manual de Gobierno Digital o el documento que se esté utilizando como marco de referencia 14) Plan de mejoramiento
Dependencia:	Oficina Asesora de Informática (OAI)
Líder del Proceso / Jefe(s) Dependencia(s):	Gustavo Adolfo Vélez Achury - Jefe Oficina Asesora de Informática
Objetivo de la Auditoría:	Verificar la aplicación de controles y su eficacia en el desarrollo de las actividades asociadas al proceso de Gestión de Tecnologías de la Información, así como la gestión sobre los riesgos para el logro de los objetivos organizacionales.
Objetivos Específicos:	1) Evaluar los registros y las evidencias asociadas a la aplicación de los procedimientos, el instructivo para la

	actualización o modificación de datos y el protocolo para la ejecución de pruebas de seguridad para los desarrollos de software. 2) Verificar la aplicación de controles en actividades regulares, así como en los riesgos asociados a la seguridad de la información. 3) Revisar elementos relacionados con el Plan Estratégico de Tecnologías de la Información – PETI.
Marco Normativo:	1) Decreto 1078 de 2015 - Título 9, Manual de Gobierno Digital - versión 7 o el documento que se esté utilizando como marco de referencia 2) Plan estratégico de tecnologías de la información - PETI 3) Matriz de riesgos institucional, versión 4.0 4) Caracterización del proceso 5) Procedimientos, instructivos y protocolos 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, protocolos y normas aplicables al proceso de Gestión de Tecnologías de la Información. **Periodo auditado**: 01 de julio de 2019 al 30 de junio de 2020

Fecha Reunión de Apertura			**Vigencia Auditada**	2019 – 2020
10	07	2020		

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

2. SITUACIONES DETECTADAS DURANTE EL PROCESO DE AUDITORÍA

2.1 Resumen de la auditoría

El pasado 10 de julio de 2020 inició la auditoría al proceso “Gestión de Tecnologías de la Información”, de conformidad con los lineamientos establecidos en el Procedimiento de Auditoría Interna (P-ES-001) de la CNSC y con el Programa Anual de Auditoría del año 2020, aprobado por el Comité Institucional de Coordinación de Control Interno de enero de 2020.

La reunión de apertura se realizó a través de la herramienta *Teams*, así como las demás reuniones efectuadas durante el proceso de auditoría, dado el distanciamiento social obligatorio y a las medidas decretadas por el Gobierno Nacional a causa de la pandemia presentada.

2.1.1 Planeación de la auditoría

Previo al inicio de la auditoría se realizó la planeación de esta, considerando los siguientes elementos:

1. Conocimiento de la entidad: se revisaron los procesos, la normatividad, el mapa de riesgos y los planes, asociados al alcance de la auditoría.

2. Identificación de los aspectos evaluables: se analizaron todos los procedimientos que hacen parte del proceso "Gestión de Tecnologías de la Información" y se decidió incluirlos todos en el alcance de la auditoría, pero a su vez identificando algunos aspectos que son susceptibles de ser evaluados y que pueden convertirse en puntos críticos en la ejecución del procedimiento. El detalle de este análisis se especificará más adelante en este informe.

   De igual manera, se analizaron todos los instructivos del proceso y se decidió incluir en el alcance el "Instructivo para la actualización o modificación de datos" (I-TI-006), debido a que es el que tiene mayor relación con las actividades misionales de la entidad.
   Adicionalmente, se incluyeron otros criterios de auditoría relacionados con planes y riesgos, para abarcar así los aspectos más críticos para la entidad, como lo es el sistema SIMO y el Plan Estratégico de Tecnologías de la Información – PETI

Durante la planeación se propuso efectuar dos (2) pruebas de recorrido, con fechas posteriores al plazo definido por la Alcaldía Mayor de Bogotá sobre la cuarentena, sin embargo, debido a los múltiples aplazamientos de esta (por la continuación de la cuarentena obligatoria), solamente se logró efectuar una prueba, realizándola con los responsables a través de escritorio compartido por Teams. Esto fue para la revisión de requisitos de seguridad en el sistema de información SIMO.

En esta etapa de planeación, producto del análisis de riesgos y objetivos de cada procedimiento, se identificaron puntos de control que de no realizarse pueden afectar el cumplimiento del objetivo del proceso, así como puntos de falla que pueden presentarse afectando igualmente su consecución. Se explica a continuación el análisis efectuado:

1) Procedimiento: *"Gestión del desarrollo de software (P-TI-001)"*: se evalúa el cumplimiento de la política de operación relacionada con la identificación de datos que ameritan protección específica y los casos en donde se deberían incluir controles de ingreso o de salida de dichos datos. El manejo de los datos es un aspecto crítico relacionado con la seguridad de la información, por lo cual es necesario verificar que se estén ejecutando los controles asociados.
2) *Procedimiento: "Recibir información de IES para terminación de convocatorias (P-TI-004":* las actividades 35 a 39 corresponden a aquellas donde el responsable principal es la Oficina Asesora de Informática y así mismo son las que cumplen con el objetivo principal del procedimiento que es la disposición final de la información recibida.
3) Procedimiento: "*Gestión de Cambios (P-TI-005)"*: se verifican los controles aplicados al proceso. En este punto es importante que para los cambios requeridos en los sistemas

de información se identifiquen los impactos que estos puedan generar, que se cuente con las aprobaciones para ejecutarlos y que se evalúen los resultados luego de su ejecución.

4) Documento: *"Instructivo para la actualización o modificación de datos (I-TI-006)"*: verificación de la ejecución de los controles realizados en la actualización o modificación, dado que corresponde a cambios en registros en las bases de datos de producción, las cuales son de misión crítica en la entidad.

5) Procedimiento: "*Gestión de usuarios de TI (P-TI-006*)": se identifican dos puntos de interacción importantes para evitar riesgos en la administración de usuarios, que son la actividad No. 1.2.3 "Verificar los requisitos aplicables", la cual corresponde al momento de la creación y las actividades 1.2.28 y 1.2.29 "Generar informe de cuentas sin uso" y "Reportar a jefe de dependencia" que están asociadas a la desactivación de usuarios que no es solicitada formalmente por un jefe inmediato.

6) Procedimiento: *"para la Prestación de servicios TI (P-TI-007)"*: se identifica que dentro de su objetivo se encuentra entregar los servicios con oportunidad, por lo cual se evalúa la aplicación de ANS en la atención y el aprovechamiento de una base de conocimiento a partir de la documentación de experiencias.

7) Procedimiento: *"Gestionar la plataforma de TI (P-TI-008)"*: uno de los puntos donde se pueden presentar fallas en cualquier área de TI es contar con copias de seguridad o backups, que al momento de restaurarse en una contingencia no funcionen, motivo por el cual se revisa la aplicación específica del procedimiento en este punto (actividad 1.3.1.11), así como la ejecución de verificaciones periódicas en el desempeño de las plataformas tecnológicas.

8) Procedimiento: *"Gestión de la capacidad de TI (P-TI-009)"*: este procedimiento se debe ejecutar previamente a los procesos de contratación de recursos de TI, por ello es necesario verificar que se haya ejecutado según lo estipulado para los procesos contractuales adelantados por la OAI.

9) Procedimiento: *"Pruebas de rendimiento, carga y estrés para desarrollos (P-TI-010)"* y Protocolo: *"para la ejecución de pruebas de seguridad para los desarrollos de software (PR-TI-003)"*: considerando la cantidad de usuarios a nivel nacional que hacen uso del SIMO, es necesario constatar que se están llevando a cabo las pruebas necesarias para garantizar la seguridad, disponibilidad y confiabilidad del aplicativo.

10) Requisitos de seguridad en el sistema de información SIMO: se considera que puede ser un punto de falla el otorgamiento de permisos inadecuados, por lo que se planea revisar mediante prueba de recorrido y constatar los permisos que tienen los usuarios.

11) Mapa de riesgos aplicado al trabajo remoto: se buscar verificar que en las condiciones de trabajo actual se mantienen los principios de confidencialidad, integridad y disponibilidad de la información.

12) Plan Estratégico de Tecnologías de la Información – PETI: como herramienta fundamental de planeación en un área de tecnología, se evalúa la medición al desarrollo de las estrategias propuestas y los proyectos formulados.

13) Manual de Gobierno Digital o el documento que se esté utilizando como marco de referencia: se buscar revisar el control sobre los recursos que se están utilizando en proyectos o iniciativas relacionadas con la Arquitectura Empresarial en la entidad, en principio, tomando como referencia los lineamientos de MINTIC o bajo cualquier otro marco de referencia que esté utilizando la OAI.
14) Plan de mejoramiento: seguimiento a la ejecución del mencionado plan, como uno de los elementos que permiten establecer la continuidad entre los procesos de auditoría.

2.1.2 Ejecución de la auditoría

Durante la reunión de apertura se solicitó el envío de información relacionada con los criterios y objetivos auditados, la cual fue remitida por la Oficina Asesora de Informática entre el 17 y el 24 de julio de 2020 a través de la herramienta OneDrive y posteriormente se solicitó complementar alguna información por medio del correo electrónico institucional.

Con la información recibida se utilizó la técnica de inspección, estudiando documentos y registros electrónicos, para comparar entre los criterios auditados y las evidencias verificables. También se realizaron consultas y entrevistas a los ingenieros Hugo Fernando Ramírez Ospina, Claudia Patricia Duarte Ramírez y Edgar Cuéllar, entre el 29 de julio y el 19 de agosto de 2020.

Con relación a los listados de información entregados para el ejercicio de auditoría, se tomaron muestras aleatorias para evaluar los datos consignados.

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

Información requerida: registros y evidencias de la identificación de los datos que ameritan protección específica y los casos en donde se deberían incluir controles de ingreso o de salida de dichos datos, para el periodo de alcance de la auditoría.

Información recibida: copia de requerimientos para los sistemas BNLE, Doctrina, EDL, PQR, SIAC y acceso por red a los requerimientos del SIMO.

La OAI informó que durante el periodo que comprende el alcance de la auditoría, no recibió requerimientos relacionados con sistemas de información o aplicaciones basadas en software, que especifique o incluya la necesidad de hacer una identificación detallada de los datos que ameritan protección específica, o casos en donde se deberían incluir controles de ingreso o de salida de dichos datos, sin embargo, se encontraron requerimientos reportados en GLPI como el 53780, 54145 y 54832, en los cuales se solicita crear campos nuevos en SIMO.

Para los tickets relacionados anteriormente, aunque es posible que se haya hecho la evaluación sobre el nivel de riesgo de estos datos y sus necesidades de protección, esto no se encuentra registrado en el formato F-TI-004 “Análisis de requerimientos funcionales”, ni se evidenció en ningún otro de los registros proporcionados para la auditoría.

2) Procedimiento Recibir información de IES para terminación de convocatorias (P-TI-004)

Información requerida: registros y evidencias de la ejecución de las actividades 35 a 39.

Información requerida: carta de aceptación de la oferta MC-06-2020 para el servicio de custodia de backups de la CNSC, listado de solicitudes de copia de información y bitácora diligenciada en el "Formato para la entrega de discos duros.

Para este procedimiento se planeó una evaluación en sitio de las actividades 35 a 39, las cuales corresponden a la copia de archivos, publicación y/o remisión de discos o cintas al servicio de custodia externa y la aplicación de tablas de retención documental. Esta verificación no fue posible hacerla en sitio; para esta auditoría se recibió el listado de solicitudes efectuadas por GLPI para la copia de información y una bitácora de manejo de discos duros, pero esto es insuficiente para verificar las actividades del procedimiento, por lo cual, se recomienda incluir este procedimiento en la siguiente auditoría presencial.

3) Procedimiento Gestión de Cambios (P-TI-005)

Información requerida: listado de controles de cambio.

Información recibida: 41 carpetas con formatos F-TI-001 de Solicitudes de cambio y formatos sin código de actividades de cambios tecnológicos presentadas a la mesa de trabajo.

Se verificaron los documentos de las mesas de trabajo del 16/10/2019, 06/11/2019, 11/12/2020, 28/01/2020, 18/03/2020, 08/04/2020, 15/04/2020 y 13/05/2020.

En la documentación entregada para la auditoría no se encontraban todos los soportes de las solicitudes de cambio, sin embargo, al consultar en GLPI se encontró que los requerimientos tenían adjunto el formato de solicitudes de cambio correspondiente.

Se destaca el cumplimiento de la OAI en la ejecución de las mesas de trabajo semanales y el seguimiento a la implementación de los cambios que se efectúa de manera posterior a su ejecución.

Hasta el mes de marzo de 2020 se encontraron los formatos de las mesas de trabajo firmados por sus integrantes, pero a partir del inicio del trabajo remoto no se encontró ninguna evidencia de la aprobación de estos documentos. Para cambios de emergencia como el 58133, 60843, 65113 y 65178 no aparece registro de su aprobación, aun cuando el procedimiento indica que todo cambio de emergencia debe ser aprobado explícitamente por el Jefe de la Oficina Asesora de Informática.

4) Instructivo para la actualización o modificación de datos (I-TI-006)

Información requerida: listado de solicitudes de datos actualizados o modificados durante el periodo de evaluación.

Información recibida: listado con 3.268 nombres de archivos, relacionados con cambios realizados en las bases de datos MARIADB, MS SQL SERVER y PostgreSQL.

Para la revisión se tomaron en cuenta principalmente las solicitudes que provenían de alguna entidad judicial o aquellas que implicaban modificar datos de aspirantes. Se revisaron en detalle los tickets 59910, 63775, 65007, 66318, 66328, 66809, 66826, 67211, 67230, 67628 y 68338.

En los tickets mencionados anteriormente, se encontró que diferentes usuarios realizan la solicitud de cambios en datos, luego el analista o técnico de la mesa de servicios atiende la solicitud y responde al usuario. No se encontraron validaciones frente a la autorización del usuario para pedir este tipo de cambios.

5) Procedimiento Gestión de usuarios de TI (P-TI-006)

Información requerida: listado de solicitudes atendidas durante el periodo de evaluación.

Información recibida: listado de usuarios creados entre el 01 de julio de 2019 y el 30 de junio de 2020.

Se efectuó la verificación del cumplimiento de las actividades del procedimiento 1.2.3: Verificar los requisitos aplicables, 1.2.28: Reportar a jefe de dependencia y 1.2.29: Generar informe de cuentas sin uso.

Para la actividad 1.2.3 se recibió un documento donde se indican los pasos que sigue el ingeniero de soporte que recibe la solicitud, para verificar la existencia de algún tipo contrato válido y vigente.

Con respecto a las actividades 1.2.28 y 1.2.29, no se encontraron evidencias de su ejecución para el periodo de alcance de la auditoría.

6) Procedimiento para la Prestación de servicios TI (P-TI-007)

Información requerida:
- Catálogo de acuerdos de prestación de los servicios.
- Listado de solicitudes atendidas durante el periodo de evaluación.
- Documentación de la solución de casos recurrentes.

Información recibida:
- Listado de categorías de servicios en GLPI.
- Listado de tickets abiertos durante el periodo del alcance de la auditoría.
- Enlace a la base de conocimiento de la herramienta GLPI (http://mesadeservicios.cnsc.gov.co/front/knowbaseitem.php)

Dentro de la documentación aportada para la auditoría no se encontraron registros de los acuerdos de niveles de servicio o un catálogo estructurado de los servicios que presta la OAI. Únicamente se tienen 23 ítems configurados en la herramienta GLPI (ver imagen *Service*

levels) los cuales no reflejan los servicios que efectivamente reciben los usuarios internos de la entidad.

Nombre
(TA 30 TS 1440) Actividades Especiales T2 AET2 R (2)
(TA 30 TS 480) Actividades Especiales T1 AET1 R (3)
(TA 30 TS 4800) Actividades Especiales T3 AET3 R (4)
(TA 30 TS 1440) Adquisiciones T1 AT1 R (6)
(TA 30 TS 1440) Hardware T1 HT1 R (11)
(TA 30 TS 1440) Redes T2 RT2 R (10)
(TA 30 TS 1440) Redes T3 RT3 I (16)
(TA 30 TS 1440) Software T8 ST8 R (25)
(TA 30 TS 1920) Software T6 ST6 R (23)
(TA 30 TS 2400) Hardware T2 HT2 R (12)
(TA 30 TS 2400) Redes T1 RT1 I (14)
(TA 30 TS 2400) Software T5 ST5 R (22)
(TA 30 TS 28800) Software T3 ST3 R (19) (20)
(TA 30 TS 480) Adquisiciones T2 AT2 R (7)
(TA 30 TS 480) Redes T1 RT1 R (9)
(TA 30 TS 480) Software T4 ST4 R (21)
(TA 30 TS 4800) Adquisiciones T3 AT3 R (8)
(TA 30 TS 4800) Software T7 ST7 R (24)
(TA 30 TS 960) Hardware T1 HT1 I (17)
(TA 30 TS 960) Redes T2 RT2 I (15)
(TA 30 TS 960) Software T1 ST1 I (18)
(TA 30 TS 960) Software T1 ST1 R (13)
(TA 30 TS 9600) Software T2 ST2 R (19)

Imagen: Service levels

Aunque la OAI informó que la herramienta GLPI cuenta con una base de conocimiento donde reposan los casos que más comúnmente se repiten, se verificó directamente en la herramienta uno a uno los elementos de la lista de la base de conocimiento (ver imagen Artículos recientes) y no se encontró tal.

Imagen: Artículos recientes en GLPI

El primer elemento de la lista corresponde a un registro creado el 16 de julio de 2020, el segundo es del 15 de marzo de 2019 y los demás son del año 2018, 2017 y 2016. Al verificar el detalle de los elementos se pudo verificar que 8 de 10 no contienen información que constituyan una base de conocimiento, puesto que ni siquiera mencionan pasos mínimos para dar respuesta al caso que enuncian y los 2 restantes tienen datos insuficientes sobre la solución.

Adicionalmente, se encontraron los tickets 68054, 68196, 68232 y 68259, en los cuales se está solicitando información personal de aspirantes como el teléfono, dirección y correo electrónico. Es claro que en la entidad requiere esta información para su gestión interna, sin embargo, se sugiere revisar los controles que se están aplicando para entregar dichos datos, puesto que es bien sabido que a los aspirantes luego de inscribirse a una convocatoria comienzan a recibir publicidad de empresas que no tienen relación con la CNSC.

7) Procedimiento Gestionar la plataforma de TI (P-TI-008)

Información requerida: registros y evidencias de la ejecución de las actividades 1.2.11: Evaluar desempeño de recursos y 1.3.1.11: Validar copias de seguridad.

Información recibida: documento con imágenes de las herramientas Zabbix, HP Insight Remote Support, Integrated Lights Out, VMware, Storage Advisor Embedded, Hitachi.
Inventarios de backups a cintas con la herramienta Data Protector y backups con la herramienta Veeam.

Se encontró que la OAI cuenta con herramientas de control y monitoreo sobre la plataforma tecnológica de la entidad.

Con respecto a las bitácoras de los backups ejecutados, se recomienda revisar el de la herramienta Veeam Backup & Replication infrastructure, puesto que muestra fecha expiración de la licencia el 11/07/2020 para el servidor MUISKA.

Para los backups a cinta ejecutados por la herramienta Data Protector, se recomienda revisar la configuración del elemento JBOSS, debido a que el 21% de los registros en abril de 2020, el 88% para mayo de 2020 y el 100% para junio de 2020, presentan algún tipo de falla o error. De igual manera el elemento SYSTEM_STATE_LINUX durante todo el periodo auditado presentó errores o fallas en la ejecución del backup programado.

Con relación a la actividad 1.3.1.11: Validar copias de seguridad, si bien el procedimiento indica que se debe efectuar una revisión periódica de la calidad y completitud de las tareas de respaldo de la información mediante actividades de restauración de las copias de seguridad, y se establece como actividad de control la ejecución mensual de una restauración aleatoria de una copia de seguridad efectuada en el periodo que culmina, se encontró que solamente se restauran copias de seguridad por petición explícita de algún usuario, pero no se está realizando la tarea de verificar los backups que se están guardando en las herramientas dispuestas para ello.

8) Procedimiento Gestión de la capacidad de TI (P-TI-009)

Información requerida: registros y evidencias para procesos de contratación como hiperconvergencia, escritorios virtuales, entre otros.

Información recibida: documentos de estudios previos y anexos técnicos de las siguientes contrataciones:

- Adquisición de balanceadores y equipos para la ampliación de la plataforma de hiperconvergencia de la CNSC.
- Adquirir una solución tecnológica que integre componentes de procesamiento, almacenamiento, comunicaciones y virtualización que soporte servicios informáticos de la Comisión Nacional del Servicio Civil.
- Contratar la adquisición, instalación y puesta en funcionamiento de una solución de telefonía IP con funciones de Contac Center.
- Adquisición, implementación, soporte y mantenimiento de una plataforma de escritorios y aplicaciones virtuales para la CNSC.

Se encontró que, por medio de los estudios previos y los anexos técnicos de los diferentes procesos de contratación, se está llevando a cabo el registro de los requisitos de recursos adicionales de TI, pero no se encontraron evidencias de la trazabilidad entre el estado actual y el estado futuro esperado.

Aunque el procedimiento no indica que se deba utilizar un formato específico para reportar las mediciones de capacidad realizadas a los elementos de TI, sí indica que se deben registrar dichas mediciones para llevar un control adecuado. La falta de dichos registros puede generar interrogantes frente a las adquisiciones tales como:

- Por qué el controlador de Wireless requerido en el proceso de contratación debe soportar hasta 2000 usuarios concurrentes, si los usuarios de la CNSC son aproximadamente 500.
- Cómo se estimó que los servidores de aplicación para virtualización deben tener en cada nodo 9 discos SSD de 1,92TB.

9) Procedimiento Pruebas de rendimiento, carga y estrés para desarrollos (P-TI-010) y Protocolo para la ejecución de pruebas de seguridad para los desarrollos de software (PR-TI-003)

Información requerida: registros y evidencias de la aplicación a un (1) desarrollo de software y registros de la aplicación al sistema SIMO.

Información recibida: se informó a la auditoría que desde el periodo de vigencia de los documentos (mayo de 2020) y hasta la fecha de alcance de la auditoría (30 de junio de 2020) no se han entregado desarrollos de software, por lo cual no se cuentan con registros de la aplicación.

Con relación a SIMO se recibió el documento "*VALORACIÓN DE LOS HALLAZGOS DE VULNERABILIDAD DE SIMO*", el cual no tiene fecha de emisión, y se recibió además un documento de solución para estos hallazgos.

Se informó también a la auditoría que las pruebas a SIMO estaban programadas para la segunda mitad del mes de julio de 2020.

10) Requisitos de seguridad en el sistema de información SIMO

Información requerida: listado de roles, usuarios y permisos del SIMO.

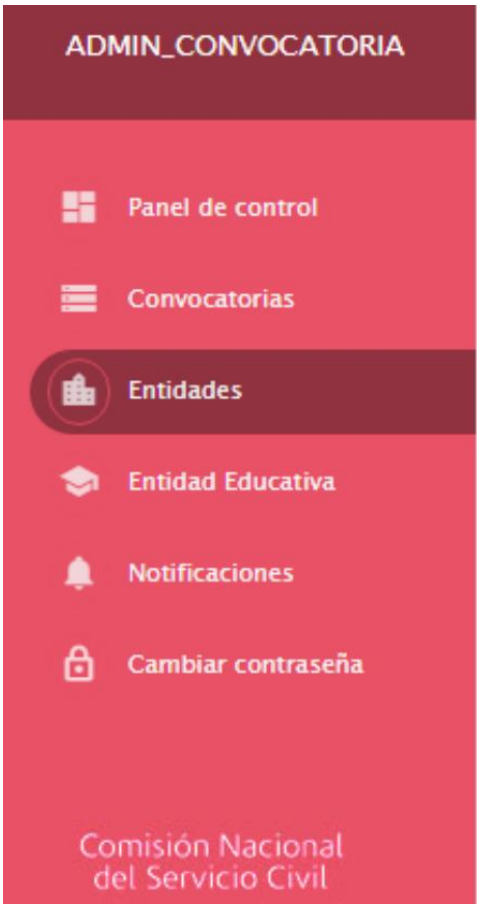
Información recibida: listado de roles con su descripción y listado de usuarios de la CNSC.

Frente al listado de usuarios recibido, se encuentran 216 personas de la entidad con algún tipo de rol dentro de SIMO, de los cuales 82 no están registrados con el correo electrónico institucional, sino con correos personales.

Se tuvo acceso a los siguientes manuales a través de la Wiki (http://gestion.cnsc.net/cnscwiki/doku.php):

- MANUAL DE USUARIO ANALISTA LISTA DE ELEGIBLES
- MANUAL DE USUARIO CARGADOR NUEVO REGISTRO OPEC
- MANUAL DE USUARIO CIUDADANO - SIMO
- MANUAL DE USUARIO ESTRUCTURA
- manual_gerente
- MANUAL DE USUARIO ADMINISTRADOR INSTITUCIÓN DE EDUCACIÓN SUPERIOR
- MANUAL DE USUARIO ANALISTA IES
- MANUAL DE USUARIO AUDITOR IES
- MANUAL DE USUARIO SUPERVISOR IES
- MANUAL DE USUARIO ADMINISTRADOR ENTIDAD
- MANUAL DE ROL APOYO CORPORATIVO
- MANUAL DE USUARIO CARGADOR
- MANUAL DE USUARIO Cargue,aprobación y Publicación de Resultado de Pruebas
- MANUAL DE USUARIO OPEC
- MANUAL DE USUARIO RECLAMACIONES
- MANUAL DE USUARIO REPRESENTANTE LEGAL- SIMO
- MANUAL DE USUARIO REQUISITOS MÍNIMOS
- MANUAL DE USUARIO VALORACIÓN DE ANTECEDENTES
- MANUAL DE USUARIO ADMINISTRADOR ENTIDAD
- MANUAL DE USUARIO ADMINISTRADOR DE EMPLEOS
- manual_opec_g
- MANUAL DE USUARIO MÓDULO CIUDADANO

En el MANUAL DE USUARIO OPEC se encontró que el rol ADMIN_CONVOCATORIA tiene 6 opciones en el menú, tal y como se observa en la siguiente imagen:



Imágenes tomadas de:
http://gestion.cnsc.net/cnscwiki/doku.php?id=simo:documentos:manual_opec_g
y del ambiente piapoco1:8080 durante prueba de recorrido

En las entrevistas realizadas con la ingeniera Claudia Patricia Duarte se observó el mismo rol, sin embargo, el menú de opciones es diferente, según se puede apreciar en la imagen:

Por otra parte, en la WIKI no se encontró el manual de "*Administrador Modulo OPEC*" y el manual para el rol "*Consulta Apoyo*".

11) Mapa de riesgos aplicado al trabajo remoto

Información requerida: detalle de medidas y controles tomados frente a los riesgos durante el primer semestre de 2020.

Información recibida: matriz de análisis de riesgos, listas de verificación para construcción de ítems y otros.

La OAI elaboró una matriz de riesgos con fecha 06 de abril de 2020 para 3 aspectos:

- Trabajo remoto para los colaboradores de la CNSC en general

- Trabajo remoto para los colaboradores de la OAI
- Trabajo remoto para los operadores de convocatorias en curso (IES)

Se observa que, aunque se identificaron claramente los riesgos y se efectuó su valoración, no se definieron controles y/o planes de tratamiento para dichos riesgos, aún cuando hay 4 riesgos en valoración "*Alto*".

En la Intranet de la entidad se encuentra publicado el archivo "*2020_mapa-de-riesgos_v1*" el cual tiene fecha de publicación del 29 de abril de 2020, donde se incluyen 17 riesgos para el proceso "*Gestión de Tecnologías de la Información*", sin embargo, en este mapa no se encuentran incluidos los riesgos que identificó la OAI para el trabajo remoto.

De los 17 riesgos solamente el "*R-TI-012 Daño en equipos informáticos asignados a los funcionarios en los puestos de trabajo"*, tiene una valoración residual de exposición en nivel ALTO; esto significa que es el único riesgo que tiene establecido un plan de tratamiento con acciones de mitigación, pero es claro que este riesgo ya no es relevante cuando la mayor parte del trabajo de la entidad se realiza en forma remota. La no actualización del plan de tratamiento eventualmente implicará un incumplimiento a lo establecido y un hallazgo para la OAI.

Con relación a los otros 16 riesgos identificados en el mapa publicado, se evaluaron los controles en 7 de estos, dado que en algunos casos son riesgos que están relacionados con los criterios de auditoría y en otros casos porque fue posible verificar directamente el riesgo con pruebas de escritorio. Las observaciones de esta evaluación se presentan en la siguiente tabla.

No.	Riesgo	Controles	Observación
R-TI-001	Disminución de la oportunidad, eficiencia y efectividad en la prestación de los servicios TIC.	1. Realizar revisión periódica de Plan Estratégico de Sistemas - PETI (antes PETIC). 2. Realizar identificación de las necesidades TIC por parte de los procesos para la siguiente vigencia, mediante comunicación interna.	No se encontraron evidencias de que se esté realizando la revisión periódica al PETI, entendiendo que es un plan en ejecución permanente y no se debe realizar seguimiento únicamente una vez al año.
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).	Se utilizan dos tipos de formato para el levantamiento de requerimientos y en ambos casos no incluyen todos los campos necesarios para registro de información según lo indicado en el Procedimiento Gestión del desarrollo de software (P-TI-001).
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 instalar en el equipo de cómputo de la entidad un software no autorizado (Balsamiq), lo cual indica que no se han aplicado controles efectivos a este riesgo.

R-TI-014	Inadecuada gestión de las contraseñas.	Documentar políticas generales de operación del directorio activo (GPO), para la administración de usuarios.	Se evidenció que aún no se han aplicado políticas de contraseñas y que el proceso de cambio de contraseña no se puede realizar de forma independiente por parte de los usuarios, sino que requiere de la intervención del personal de la mesa de ayuda, lo cual dificulta el proceso.
R-TI-015	Descarga de aplicaciones, datos, imágenes o en general contenidos de internet sin control.	1. Documentar políticas generales de operación del directorio activo (GPO), para la administración de usuarios. 2. Realizar campañas de divulgación	Se realizó una prueba de escritorio en la que se pudo descargar e instalar el sofwtare µTorrent, el cual favorece la descarga indiscriminada de información. Esto evidencia que no se han aplicado controles efectivos, aun cuando se hayan realizado campañas de divulgación. Por otra parte, se recomienda revisar la valoración de este riesgo, dado que su impacto está calificado en “Moderado”.
R-TI-016	Uso de programas utilitarios o herramientas especializadas que cambien los controles establecidos.	1. Documentar políticas generales de operación del directorio activo (GPO), restringir la instalación de programas. 2. Aplicar procedimiento para la prestación de servicios TI (P-TI-007).	Se repite la observación efectuada al riesgo R-TI-010 y al R-TI-015.
R-TI-017	Eventos o incidentes sin solución definitiva.	Gestionar herramienta de Gestión de los Servicios de TI por la Mesa de Servicios.	No se encontró que se esté aplicando el control en la herramienta de la Mesa de Servicios, dado que tal y como se evidenció en el numeral 6) de este informe, el Procedimiento para la Prestación de servicios TI (P-TI-007) indica que se deben tener Acuerdos de Niveles de Servicios, pero estos están definidos ni parametrizados en la herramienta.

12) Plan Estratégico de Tecnologías de la Información – PETI

Información requerida: registros de los seguimientos efectuados mensualmente en la herramienta destinada para ello.

Información recibida: listados de asistencia, bitácora de reuniones, acceso a Open Project y cronogramas en Microsoft Project.

Para la auditoría se otorgó acceso a la herramienta Open Project (http://openproject.cnsc.net/projects/), sin embargo, la OAI informó que en esta herramienta sólo se encuentran los proyectos hasta 2019 y que para 2020 se comenzó a utilizar la herramienta Project Professional.

Dentro de las evidencias de seguimiento de 2020 se recibieron 3 archivos en Project con cronogramas construidos bajo diferentes estructuras. El archivo más reciente recibido se

denomina "*Cronograma-SIMO4-v1_04082020.mpp*", sobre el cual se realizó una revisión detallada, encontrando varias inconsistencias en su elaboración, tal y como las que se señalan más adelante, de conformidad con la siguiente imagen:

	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos	% comple
1		**Definir Los Lineamientos de Desarrollo Ágil SIMO 4**	**37 días**	**lun 20/01/20**	**mié 11/03/20**			**86%**
2		Propuesta Lineamientos y Procedimiento Desarrollo Ágil	15 días	lun 20/01/20	vie 7/02/20		Jeison;Leonardo;Sandra	100%
3		Aprobación Arquitectura TI Lineamientos y Procedimiento Desarrollo Ágil	17 días	lun 10/02/20	mar 3/03/20	2	Arquitectura TI	100%
4		Oficialización Lineamientos y Procedimiento Desarrollo Ágil	5 días	mié 4/03/20	mar 10/03/20	3	Hugo Ramírez	0%
5		Procedimiento Desarrollo Agil Aprobado	0 días	mié 11/03/20	mié 11/03/20	4	OAI	0%
6		**Definir las Tecnologías SIMO 4**	**25 días**	**mié 5/02/20**	**mié 11/03/20**			**10%**
7		Propuesta Tecnologías SIMO 4	3 días	mié 5/02/20	vie 7/02/20		Santiago;Jaime	80%
8		Aprobación Arquitectura TI Tecnologías SIMO 4	15 días	lun 10/02/20	vie 28/02/20	7	Arquitectura TI	0%
9		Oficialización Lineamientos Tecnológicos	5 días	mié 4/03/20	mar 10/03/20	8	Hugo Ramírez	0%
10		Lineamientos Tecnológicos Aprobados	0 días	mié 11/03/20	mié 11/03/20	9	OAI	0%
11		**Hitos Integración**	**229 días?**	**jue 16/01/20**	**mar 1/12/20**			**24%**
12		Version 1 Modelo de Datos Unificado	152 días	sáb 1/02/20	lun 31/08/20		Javier A.	28%
13		**Usuario Integrados**	**228 días?**	**jue 16/01/20**	**lun 30/11/20**			**8%**
19		DIVIPOLA centralizada	1 día?	lun 14/09/20	lun 14/09/20	148;192;239		0%
20		Personas Centralizadas	1 día?	lun 9/11/20	lun 9/11/20	255;208;163;288		0%
21		Entidades Centralizadas	1 día?	lun 9/11/20	lun 9/11/20	154;130;201		0%
22		Empleos y cargos Centralizados	1 día?	lun 9/11/20	lun 9/11/20	217;262;170;290		0%
23		Menus Depurados	1 día?	mié 30/09/20	mié 30/09/20	125;177;224;269		0%
24		Interoperabilidad entre Sistemas Alcanzada	1 día?	lun 9/11/20	lun 9/11/20	178;225;270;275;		0%
25		Pruebas Funcionales Superadas	1 día?	lun 9/11/20	lun 9/11/20	128;137;179;226;		0%

- Las tareas no se encuentran redactadas con verbos en infinitivo, lo cual en líneas como la 7 "*Propuesta Tecnologías SIMO 4*" no permite identificar si la acción que se ejecutará es elaborar, desarrollar, analizar u otra similar, dificultando el seguimiento al plan.
- Tareas como la 8 y la 9 no tienen registro de avance, aunque las fechas de ejecución se establecieron para el mes de marzo de 2020.
- Las tareas se encuentran programadas en modo manual, haciendo que las predecesoras identificadas no tengan ningún valor para la planeación.
- Las tareas de la 19 a la 25 tienen una duración estimada (esto se representa con el interrogante junto a la palabra "*día*") lo que indica que no se ha hecho efectivamente la planeación.
- En la imagen las tareas de la 19 a la 25 no tienen recursos asignados y esta situación se repite en el 18% de las actividades del cronograma, pero adicionalmente hay recursos nombrados como "*Infraestructura*" o "*Equipo SIMO*", donde no se identifica realmente al responsable de la acción.
- No se tienen identificados los días no hábiles, lo cual puede generar errores como reportar tareas con una duración mayor a la real.
- A lo largo del cronograma hay tareas que no tienen identificada una fecha de inicio, una fecha final o ambas.
- Varias semanas del año (como por ejemplo 3 semanas de mayo, 4 de junio y 3 de octubre) no tienen nada programado.

Se recibió también un archivo en Excel llamado "*Bitacora ReunionesSeguimientoProyecto*" el cual solamente contiene un listado de tareas relacionadas a múltiples temas, pero no se observa continuidad entre ellas o relación directa con alguno de los proyectos del PETI.

Por otra parte, se consultó sobre el avance físico y financiero de los proyectos y este fue el reporte recibido:

PROYECTO	EJECUCIÓN FÍSICA	EJECUCIÓN FINANCIERA*
Estructuración de la arquitectura empresarial	50%	$ 456.768.000
Definición del modelo de interoperabilidad de sistemas de información	10%	$ 259.584.000
Mejoramiento del Centro de Datos de la CNSC	100 % en el año 2019	$ 161.070.923
Renovación del esquema de seguridad perimetral	100 % en 2019 En el 2020 en operación y mantenimiento sin presupuesto	$ 1.792.107.061
Plan de Recuperación de Desastres de TI	62 % 2019 34 % 2020 de un proyectado a 31 de julio de 2020 de 66,7%	$ -
Sistema de provisión de empleo	39%	$ 257.088.000
Mejoras funcionales EDL	56%	$ 266.656.000
Solución de Carpeta Ciudadana	0% Proyecto no se inicia por falta de direccionamiento de MinTIC	$ -
Implementación de la estrategia Gobierno Digital	0%	$ -
Operación y mejora de la inteligencia de negocios de la CNSC	10%	$ 404.160.000
Sistema de Gestión Documental	Sin datos	$ 1.543.952.000

* Nota: aunque en el reporte se indica este valor como ejecución financiera, posteriormente se indicó que correspondía a presupuesto planeado.

Se revisó el Plan Estratégico de Tecnologías de la Información con fecha de actualización enero de 2020, en particular el capítulo 7.1 Resultados de la vigencia 2019, y se comparó con los registros aportados a la auditoría.

A continuación, se registran las observaciones a los proyectos del PETI.

PROYECTO	PROYECCIÓN 2020 DEL PETI	OBSERVACIÓN AUDITORÍA
Estructuración de la arquitectura empresarial	- Ejecución de la AE para la nueva cada de valor de la administración y vigilancia de la carrera administrativa.	No se encontró dentro de los planes de trabajo las tareas o actividades específicas, encaminadas a dar cumplimiento a este proyecto.
	- Aplicación de la AE en los proyectos de transformación digital como son:	
	a) SIMO 4.0	
	b) Sistema de Gestión Documental Electrónica y de Archivo - SGDEA	
	c) Gestión del Conocimiento	
	d) Servicios al ciudadano	
	e) Planificación de Recursos Empresariales - ERP	
	- Integración SIMO 4.0 con SGDEA	

Definición del modelo de interoperabilidad de sistemas de información	- Integración ERP con SIMO 4.0 - Integración ERP con SIIF - Integración solución de software de CallCenter con SIMO 4.0	Dentro del cronograma SIMO 4.0 no se logró identificar si alguna de las integraciones relacionadas allí pertenece a este proyecto. En cuanto a la ejecución física reportada (10%) es un valor bajo, respecto al tiempo transcurrido de la vigencia.
Mejoramiento del Centro de Datos de la CNSC	- Adquisición de sistema UPS para el Datacenter - Adecuación para independizar el cuarto eléctrico en el Datacenter, creación de puesta a punto.	No se encontró un plan de trabajo para este proyecto. Aun cuando en el avance se informa cumplido en el 2019, en el PETI 2020 se establecen las metas aquí señaladas.
Renovación del esquema de seguridad perimetral	Adquisición Licencia Antivirus. Contratar Servicios Especializados de Ethical Hacking, Análisis de Vulnerabilidades y Pruebas de Ingeniería Social para la Comisión Nacional del Servicio Civil.	En el reporte de ejecución se informó que este proyecto no tiene presupuesto, sin embargo, en el documento de PETI publicado en enero de 2020, se incluyeron proyectos por $140.000.000.
Plan de Recuperación de Desastres de TI	Formalizar documento del DRP. La ejecución del DRP queda sujeta a disponibilidad presupuestal para la vigencia 2020.	No se encontró un plan de trabajo para este proyecto, sin embargo, se reporta un avance del 34% frente a un 66,7% planeado.
Sistema de provisión de empleo	Incluido dentro del proyecto de SIMO 4.0 como una funcionalidad propia de un sistema único de administración y vigilancia de la carrera administrativa	Dentro del cronograma SIMO 4.0 no se logró identificar este proyecto o los paquetes de trabajo que le aporten a su cumplimiento.
Mejoras funcionales EDL	La evaluación del desempeño laboral fue incluida dentro del proyecto de SIMO 4.0 como una funcionalidad más del sistema único de administración y vigilancia de la carrera administrativa, se realizará unificación de base de datos e interfaz de usuario.	El plan de trabajo de SIMO 4.0 para la integración con EDL, incluye tareas que tienen registrado un 0% de avance, aun cuando su fecha de inicio corresponde al primer semestre de 2020 y la fecha de actualización del archivo es el 04 de agosto de 2020.
Solución de Carpeta Ciudadana	La CNSC está a la espera de los lineamientos del MinTIC y del DAFP para identificar puntos de intercambio de información que permita la interoperabilidad que pretende la política de gobierno digital el estado colombiano.	Dado que el Gobierno Nacional emitió el Decreto 620 del 2 de mayo de 2020, se recomienda actualizar la planeación conforme a lo estipulado en el decreto.
Implementación de la estrategia Gobierno Digital	**OBJETIVOS** a. Identificar el grado de cumplimiento de los requisitos de la Estrategia de Gobierno Digital. b. Definir la hoja de ruta para dar cabal cumplimiento a los requisitos de la Estrategia de Gobierno Digital. **ENTREGABLES** 1. Diagnóstico de cumplimiento de las indicaciones para Gobierno Digital.	No se encontró dentro de los documentos aportados a la auditoría, la hoja de ruta o plan de acción para este proyecto; ni avance sobre los entregables enunciados.

	2. Identificación de brechas y oportunidades de mejoramiento de los servicios de la Entidad. 3. Plan de acción para atender los requerimientos sobre Gobierno Digital. Dentro del proceso de transformación digital que viene adelantando la CNSC se identificó que se puede aplicar la utilización de tecnologías emergentes en varios servicios dentro de la cadena de valor de la administración y vigilancia de la carrera administrativa como son: Recomendador de Empleos, OPEC inteligente, Verificación de Requisitos mínimos y Valoración de antecedentes. Estos servicios se consideraron implementar dentro del proyecto SIMO 4.0	
Operación y mejora de la inteligencia de negocios de la CNSC	Se potencializará el uso de la herramienta Qlik por parte de las áreas líderes funcionales, se migrarán los tableros actuales y se crearán unos nuevos según las necesidades.	No se encontró un plan de trabajo para este proyecto.
Implementación de un Contact Center para PQR.	Se realizará la implementación de la solución de Contact Center.	No se encontró un plan de trabajo para este proyecto.
Sistema de Gestión Documental	Implementar un sistema de Gestión Documental Electrónico y de Archivo – SGDEA en la CNSC. **OBJETIVOS** - Reemplazar el sistema de información actual de gestión documental Orfeo - Cumplir con los requerimientos establecidos por el Archivo General de la Nación en lo referente al manejo de los documentos que gestione la CNSC. - Que el SGDEA sea el repositorio único y central de toda la documentación de la Entidad.	No se encontró un plan de trabajo para este proyecto y su fecha estimada de inicio era junio de 2020.

Es necesario recordar que el PETI 2019 – 2022 establece que, como mecanismo de medición y seguimiento a las estrategias propuestas y los proyectos formulados en este plan, cada responsable de ejecución "*registrará sus avances y novedades mensualmente a más tardar el quinto día hábil del siguiente mes*". Además, "*para efectos de control de la ejecución se harán revisiones detalladas de estos registros bimestralmente por parte del Arquitecto de TI conjuntamente con el Jefe de la Oficina Asesora de Informática y la colaboración del grupo funcional de apoyo a la gestión*".

13) Manual de Gobierno Digital o el documento que se esté utilizando como marco de referencia

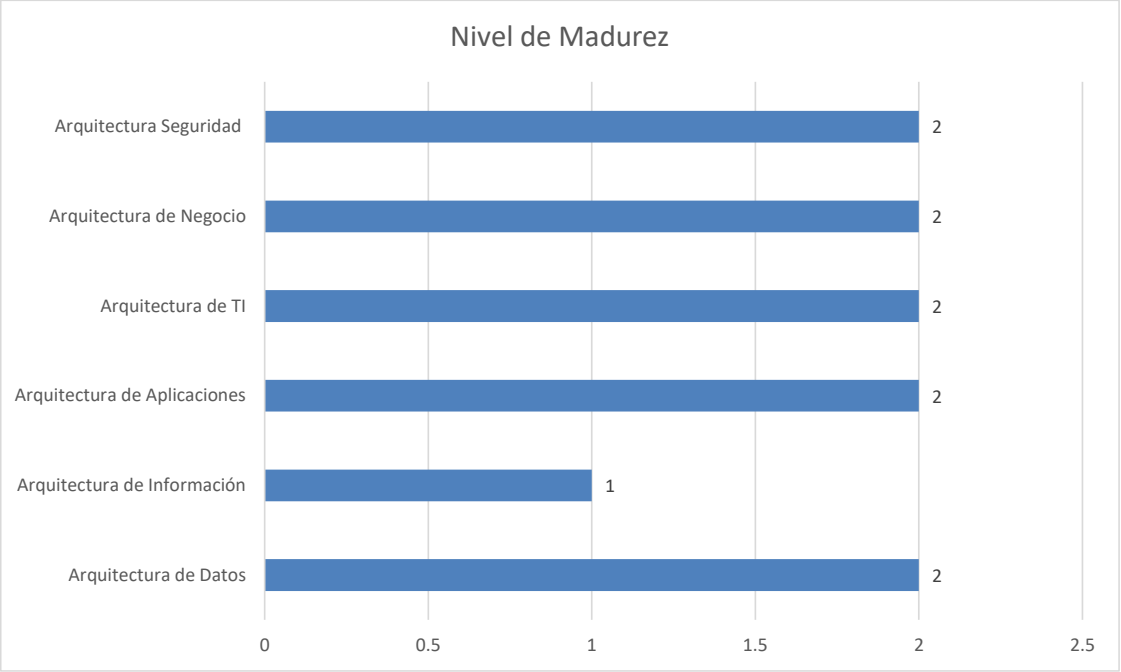
Información requerida: autoevaluación de los indicadores de cumplimiento a nivel de Arquitectura para la presente vigencia y resultados de la vigencia anterior.

Información recibida: Diagnóstico Arquitectura 2017, Arquitectura de Datos 2020, propuesta de Arquitectura de junio 2020 y anexos, Inventario de Sistemas de Información, entre otros.

En reunión de apertura de esta auditoría el ingeniero Gustavo Vélez informó que no se está utilizando como marco de referencia de Arquitectura Empresarial el modelo de MINTIC, dado que, por el carácter de la entidad, no tiene la obligación de utilizar dicho documento.

Por otra parte, la OAI vinculó en el mes de mayo de 2020 al ingeniero Edgar Cuéllar, quien informó que se está utilizando parcialmente el modelo de MINTIC y parcialmente el marco de referencia TOGAF.

El ingeniero Cuéllar efectuó una medición del nivel de madurez de la Arquitectura Empresarial encontrando lo siguiente:



Como conclusión obtiene un consolidado en Nivel 2 (en desarrollo), e indica que es "*un proceso de arquitectura en desarrollo donde interviene la definición de una arquitectura objetivo, adopción de estándares y mayor alineación con los componentes estratégicos*".

Se recibió durante la auditoría un documento llamado "*Evaluación Arquitectura de Datos CNSC*" elaborado por Javier Andrés Arias Sanabria, en el cual se formulan una serie de preguntas y se evalúan en una escala de 1 a 5. Al final se obtuvo un puntaje de 1,88 / 5, pero no se indica la fecha de corte del documento, el alcance de la medición, ni las acciones derivadas.

Adicionalmente, de acuerdo con los documentos aportados a la auditoría, se están construyendo indicadores por cada dominio de arquitectura (los dominios consignados en la imagen), para realizar seguimiento a la implementación de la Arquitectura Empresarial. Informaron que se cuenta además con una propuesta de trabajo en los diferentes dominios.

Aunque el inventario de sistemas de información contiene 29 aplicativos, no se encontraron planes de trabajo para todos aquellos que se encuentran en desarrollo, en particular, para el aplicativo de "*Contratos*" del cual se indica que aún no se cuenta con versión definitiva entregada a producción. Tampoco se encontró un plan de trabajo global donde se pueda evidenciar las fases o Arquitecturas de transición que se tendrán en las integraciones y desarrollos hacia SIMO 4.0.

14) Plan de mejoramiento

Información requerida: plan de mejoramiento de la auditoría anterior y registros de seguimiento.

Información recibida: correos de solicitudes a la Oficina de Planeación, procedimientos actualizados, políticas de backup, entre otros.

Se encontraron dos planes de mejoramiento correspondientes a la auditoría de la vigencia 01 de junio de 2018 al 30 de junio de 2019, el primero para el proceso "*Gestión de Tecnologías de la Información*" con 24 actividades y el segundo para el proceso "*Gestión de Recursos Tecnológicos*" con 13 actividades, el cual ya no se encuentra vigente debido a su unificación con el primero.

De conformidad con las evidencias aportadas a la auditoría, se confirma la ejecución y cumplimiento de todas las actividades establecidas en los planes, sin embargo, no se tienen evidencias frente a la eficacia de las siguientes actividades:

- Solicitar al proceso de Gestión de Comunicaciones que se realice una campaña de sensibilización para toda la Entidad en donde se resalte la obligación de calificar los servicios de TI prestados por la Mesa de Servicios.

- Solicitar al proceso de Gestión de Comunicaciones que se realice una campaña de sensibilización para toda la Entidad en la cual se explique la importancia del SGSI y las responsabilidades que todos los colaboradores tienen con este subsistema.

2.2 Hallazgos y/o No Conformidades

RECOMENDACIÓN 1:

Se recomienda tomar acciones sobre la identificación de datos que requieren ser protegidos, lo cual se alinea con regulaciones de privacidad y confidencialidad, e incluye también a los acuerdos contractuales y requerimientos del servicio. Esto dado que, aun cuando se informó a la auditoría que en el desarrollo del **Procedimiento Gestión del desarrollo de software (P-TI-001)** las necesidades sobre los datos no fueron definidas por parte del solicitante o del líder del proceso, es necesario recordar que la custodia de los datos y la responsabilidad sobre la información recae en la OAI, lo cual incluye la seguridad de los datos.

Se recomienda también reemplazar en la Intranet el documento P-TI-001, toda vez que no es legible la imagen del procedimiento en BPMN.

RECOMENDACIÓN 2:

Se recomienda unificar y actualizar el formato llamado **Análisis de requerimientos funcionales** con respecto al procedimiento P-TI-001 "*Gestión del Desarrollo de Software*", en el cual no se menciona el formato F-TI-004 y se hace referencia en cambio a "*Historias de usuario*". Esto debido a que se identificó que los requerimientos se están documentando en dicho formato, pero este aparece con dos códigos y plantillas diferentes, el F-TI-004 y el F-RT-001. Por ejemplo, el requerimiento 64971 del 25/03/2020 está documentado en el F-TI-004 y el requerimiento 67280 del 26/05/2020 en el F-RT-001. Es preciso aclarar que ambos formatos aparecen con fecha de vigencia 29/02/2016 y con el mismo nombre.

RECOMENDACIÓN 3:

Se recomienda revisar opciones que no impliquen la impresión de los formatos para consignar las firmas de aprobación.

En el caso de los formatos de **Análisis de requerimientos funcionales** (F-TI-004 / F-RT-001), estos no se encuentran completamente diligenciados, siendo repetitiva la falta del registro de las aprobaciones correspondientes por parte de los usuarios involucrados (Usuario avanzado, Desarrollador y/o Arquitecto, Líder de equipo de desarrollo).

El formato de **Solicitud de cambio** (F-TI-001) contiene espacios para identificar la autorización, fecha, responsable y comentarios, pero en ninguno de los documentos revisados se encontró diligenciada dicha información.

RECOMENDACIÓN 4:

Se recomienda registrar las mediciones de capacidad que se establecen en el **Procedimiento Gestión de la capacidad de TI (P-TI-009)** y proporcionarlas como puntos de referencia en los procesos de contratación futuros.

No se encontraron registros que demuestren trazabilidad de los requerimientos, al aplicar el procedimiento para los procesos de contratación actuales de la OAI.

RECOMENDACIÓN 5:

Se recomienda informar sobre la ejecución de las pruebas que se tenían previstas para el mes de julio de 2020 a la Oficina de Control Interno, para constatar la ejecución de las actividades según lo indicado, dado que no se pudo evidenciar la ejecución del **Procedimiento Pruebas de rendimiento, carga y estrés para desarrollos (P-TI-010)** y el **Protocolo para la ejecución de pruebas de seguridad para los desarrollos de software (PR-TI-003)**.

RECOMENDACIÓN 6:

Se recomienda revisar las versiones y estado de la actualización de los **manuales de SIMO.** Dicha documentación se consultó y se encontraron versiones diferentes en la WIKI y durante la prueba de recorrido. Es necesario que lo que se encuentre en la WIKI sea coherente con las versiones publicadas dentro del software en producción.

RECOMENDACIÓN 7:

Dado que uno de los objetivos de esta auditoría era revisar el avance en la implementación de las iniciativas relacionadas con **Arquitectura Empresarial**, se recomienda informar a la Oficina de Control Interno una vez se cuente con los planes detallados e indicadores que según las entrevistas están en construcción.

Se recomienda de igual manera, indicar de forma clara cuál es el marco de referencia que se está utilizando para la implementación de la Arquitectura, o en caso de que se utilicen varios marcos indicar cuál es el alcance en cada uno de ellos, y, en particular, informar cuál se utilizará como modelo para el seguimiento y la evaluación con los respectivos indicadores de cumplimiento, que permitan contar periódicamente con una medición puntual del avance.

RECOMENDACIÓN 8:

Se recomienda realizar la medición de la eficacia de las campañas de sensibilización incluidas en el plan de mejoramiento de la auditoría anterior e informar los resultados a la Oficina de Control Interno.

HALLAZGO 1:

Criterio de auditoría: 4) Instructivo para la actualización o modificación de datos (I-TI-006), versión: 1.0, fecha: 27/07/2018.

De acuerdo con el **Instructivo para la actualización o modificación de datos (I-TI-006)** las solicitudes deben ser radicadas por el Jefe de Dependencia, Coordinador de Proceso o Colaborador autorizado, sin embargo, en los tickets revisados, la solicitud no provenía de alguno de estos cargos y no se pudo evidenciar si los colaboradores solicitantes estaban autorizados, dado que no se encontró trazabilidad o evidencia de la autorización que tienen las personas que radican las solicitudes, incumpliendo lo establecido en el instructivo.

HALLAZGO 2:

Criterio de auditoría: 5) Procedimiento Gestión de usuarios de TI (P-TI-006), actividades 1.2.28 y 1.2.29, versión: 1.0, fecha: 23/10/2019.

No se encontraron registros que permitan evidenciar la ejecución de las actividades 1.2.28: Reportar al jefe de dependencia y 1.2.29: Generar informe de cuentas sin uso del **Procedimiento Gestión de usuarios de TI (P-TI-006)**. Esto representa un incumplimiento al procedimiento en las actividades mencionadas, una debilidad para el proceso y un riesgo en seguridad de la información, puesto que no se están deshabilitando los usuarios que ya no tienen un contrato vigente con la entidad.

HALLAZGO 3:

Criterio de auditoría: 6) Procedimiento para la Prestación de servicios TI (P-TI-007), versión: 3.0, fecha: 23/10/2019.

En los registros del **Procedimiento para la Prestación de servicios TI (P-TI-007)**, no se encontró el registro de los acuerdos de prestación de los servicios. De igual manera, no se encontró documentación para la solución de casos recurrentes y para construir una base de datos de conocimientos que a futuro sirvan como herramientas de autogestión o soluciones rápidas. Esto indica un incumplimiento a lo establecido en las políticas de operación del procedimiento.

Lo anterior se constituye en una debilidad para el proceso, puesto que no es posible medir la eficacia del procedimiento ni tomar acciones para la mejora continua del mismo, al no existir indicadores que verifiquen su cumplimiento.

HALLAZGO 4:

Criterio de auditoría: 7) Procedimiento Gestionar la plataforma de TI (P-TI-008), versión: 2.0, fecha: 06/11/2019.

No se encontraron registros o evidencias que permitan verificar que se está realizando la actividad 1.3.1.11 “Validar copias de seguridad” del **Procedimiento Gestionar la plataforma de TI (P-TI-008)**. Esto implica un incumplimiento a la actividad mencionada del procedimiento y un riesgo para la entidad, al no efectuar los debidos controles sobre la ejecución de los backups.

HALLAZGO 5:

Criterio de auditoría: 12) Plan Estratégico de Tecnologías de la Información – PETI Cuatrienio 2019 - 2022, versión 30 de enero de 2019 y actualización versión 1: enero 2020.

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.

HALLAZGO 6:

Criterio de auditoría: 11) Mapa de riesgos, versión: 4.0, fecha de publicación: 29/04/2020

Se evidenció que en al menos 6 de los 17 riesgos del proceso "*Gestión de Tecnologías de la Información*", identificados en el Mapa de riesgos de la entidad, no se están aplicando controles efectivos. De igual forma se encontró que los riesgos no están actualizados de conformidad con la situación actual de la entidad.

3. CONCLUSIONES DE LA AUDITORÍA

3.1. La Oficina Asesora de Informática cuenta con procedimientos actualizados, acordes a las necesidades actuales de la entidad.

3.2. La participación y buena disposición de los auditados, permitió a la auditoría verificar la aplicación de los controles definidos en el alcance; no obstante, es necesario que la OAI efectúe revisiones periódicas para validar la aplicación efectiva de todos los controles establecidos.

3.3. Para garantizar la implementación del Plan Estratégico de Tecnologías de la Información – PETI, es necesario que se haga un seguimiento riguroso al desarrollo de estrategias y proyectos.

3.4. Es necesario que se documente el marco de Arquitectura Empresarial bajo el cual se implementarán los proyectos e iniciativas asociadas a tal, así como los modelos de medición y seguimiento que se llevarán a cabo para garantizar el uso eficiente de los recursos asignados.

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\Auditorias\2020\6. Tecnologías de la Información

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

ORIGINAL FIRMADO	ORIGINAL FIRMADO
GUSTAVO ADOLFO VELEZ ACHURY Jefe oficina Asesora de Informática Auditado	**HUGO FERNANDO RAMIREZ OSPINA** Oficina Asesora de Informática Auditado