

	INFORME DE AUDITORIA	Auditoría no.		08-18
		Fecha del informe		
		Día	Mes	Año
		01	06	2018

Informe	<input type="checkbox"/>	Preliminar	<input checked="" type="checkbox"/>	Final
---------	--------------------------	------------	-------------------------------------	-------

1. INFORMACIÓN GENERAL

Tipo de Informe	<input checked="" type="checkbox"/>	Auditoría	<input type="checkbox"/>	Seguimiento
Procesos auditado /Evaluado	Gestión de la Tecnología de la Información y de las Comunicaciones			
Auditor líder	Marcela Pardo Beltrán	Equipo Auditor	Marcela Pardo Beltrán Sandra Martínez (Observador)	
Responsable del proceso, dependencia, área o actividad auditada /evaluada	Álvaro Iván Torres Gonzales			

2. OBJETIVO

Evaluar la gestión del proceso Gestión de Tecnología de la Información y de las comunicaciones conforme a los requisitos legales e institucionales.

3. ALCANCE

Verificar cumplimiento de los procedimientos, instructivos, políticas, riesgos y planes estratégicos definidos en el proceso de gestión TIC, correspondientes a la vigencia 2017 y 2018 a la fecha.

4. ACTIVIDADES DESARROLLADAS

- En cuanto a la caracterización, se verificó las entradas y salidas y secuencia del proceso, por tanto se solicitó información acerca de los productos descritos. Asimismo, se verificó los temas asociados al seguimiento. El resultado de esta verificación hace parte de las Conformidades, No Conformidades y Recomendaciones.
- Para la verificación del PETIC se consultó en la intranet la publicación del documento en la siguiente dirección:
<https://copnia.gov.co/sites/default/files/uploads/mapa-procesos/archivos/tecnologia/PETIC.pdf> el cual fue contrastado contra la guía:
http://www.mintic.gov.co/arquitecturati/630/articles-15031_recurso_pdf.pdf, la cual establece los criterios a tener en cuenta y orientaciones de los contenidos para desarrollar el PETIC en las entidades públicas. El resultado de esta actividad hace parte de las Conformidades con observación del presente informe.
- Para la Política de Seguridad de la Información se verificó la información publicada en la página web.

https://copnia.gov.co/sites/default/files/uploads/contenidos/politicas/normatividad/Politica_de_seguridad_de_la_informacion.pdf

Adicionalmente, se solicitó información relativa a la implementación de la Política asociada a:

- Guía de Seguridad de la Información
- Lineamientos para asegurar la información y los sistemas de información.
- Evidencia de capacitaciones sobre el usos adecuado de los sistemas de información.
- Planes establecidos para identificar los servicios y recursos esenciales frente a la ocurrencia de incidentes de seguridad de la información.
- Procedimientos desarrollados en el marco de la implementación del Sistema de Seguridad de la Información en el marco de la norma ISO 27001.

El resultado de esta actividad hace parte de las No Conformidades del informe.

4. Para verificar la Política de Protección de Datos Personales, se descargó la información publicada en la página web.

https://copnia.gov.co/sites/default/files/uploads/res_1197_2017_proteccion_datos_personales.pdf

Asimismo, se solicitó la información relativa a la implementación en el marco de la contratación y se verificó las cláusulas de confidencialidad y uso de las bases de datos del COPNIA. El resultado de esta actividad hace parte de las conformidades del presente informe.

5. En cuanto a la verificación del Comité de Seguridad de la Información, se revisó y analizó su creación y las respectivas actas. El resultado de la actividad hace parte de las recomendaciones del presente informe.
6. Para la verificación del inventario se solicitó los listados de inventario de equipos de cómputo y de software. De lo cual se remitió un archivo en Excel y un archivo en Word, cabe indicar que el archivo Word presentó dificultad para verificar la información, debido a que no todos los funcionarios se encuentran dentro del dominio. El resultado del informe hace parte de las recomendaciones.
7. Se verificó la trazabilidad de los tickets de servicios asociados a la mesa de ayuda, a través del reporte de base de datos de gestión ticket año 2017 y lo corrido de 2018. El resultado de esta actividad hace parte de las Conformidades, Observaciones y Recomendaciones del presente informe.
8. Fueron verificados los controles asociados a los riesgos de los procesos según lo dispuesto en la intranet, asimismo se efectuó encuesta a los funcionarios sobre el conocimiento de los mismos. El resultado de este análisis hace parte del análisis del riesgo y recomendaciones.

Auditoría no.		08-18
Fecha del informe		
Día	Mes	Año
01	06	2018

9. Para la verificación de indicadores se solicitó a la Subdirección de Planeación, Control y Seguimiento soportes de esta actividad, asimismo se verificó la creación de indicadores asociados al PETIC y al trámite oportuno de los tickets. El resultado de esta actividad hace parte de las No Conformidades y Recomendaciones del presente informe.

5. HALLAZGOS

Para la presente auditoria fueron verificados 8 criterios de los cuales 5 son Conformidades y 3 No Conformidades.

5.1 REQUISITOS CON CUMPLIMIENTO – CONFORMIDADES CON OBSERVACION

Criterio	Evidencia
<p>Gobierno en Línea: Documentación de la estrategia de TI en el PETI. LI.ES.05</p> <p>Caracterización: Proceso de Tecnología de la Información y de las Comunicaciones.</p> <p>NTC-ISO 9001.2015 7.3.1 Infraestructura</p>	<p>A través de la Junta Nacional de Consejeros en el mes de diciembre de 2017 fue aprobado Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2018-2022. El cual se encuentra publicado en la intranet de la Entidad. Una vez verificados cada uno de los componentes del PETIC se generan observaciones y recomendaciones.</p> <p>Ver Recomendaciones.</p>
Criterio	Evidencia
<p>Política de Protección de Datos personales.</p> <p>El Consejo Profesional de Ingeniería-COPNIA desarrolla lineamientos y acciones orientadas a la protección y tratamiento de los datos personales recolectados para fines misionales, contractuales y administrativo, propendiendo por asegurar la confidencialidad, integridad, veracidad, transparencia y disponibilidad de la información y bases de datos relacionadas con sus consejeros, usuarios, proveedores, funcionarios y ex funcionarios, en cumplimiento de la normatividad vigente</p>	<p>Se verificaron cuatro (4) contratos con terceros asociados a entregas de base de datos, en las cuales se observó las cláusulas de confidencialidad de la información.</p>

colombiana que dicte disposiciones para el tratamiento de datos personales. Para tal efecto, el COPNIA se compromete a desarrollar medidas que contengan condiciones de seguridad adecuadas, y a brindar la infraestructura física y tecnológica requerida para evitar la adulteración, pérdida, consulta, uso o acceso fraudulento a la información.

Criterio	Evidencia
<p>Procedimiento Atención de Incidencias y Requerimientos. TIC-pr-01</p> <p>NTC-ISO 9001.2015 7.3.1 Infraestructura</p>	<p>Se verificó la trazabilidad de los tickets observando las actividades establecidas en el proceso. Sin embargo, no es posible identificar en 325 de 433 la satisfacción de usuario.</p> <p>Adicionalmente, se verificaron 21 tickets de novedades de personal observando que se tiene relacionado el formato de solicitud del área de talento humano.</p> <p>Ver recomendación.</p>
Criterio	Evidencia
<p>Resolución No 606 mayo de 2016. Por el cual se adopta el Modelo Integrado de Planeación y Gestión. Artículo 13. Subcomité de Seguridad de la Información se reunirá de manera ordinaria por lo menos tres veces por año. Asimismo se reunirá de manera extraordinaria, por solicitud del Presidente, cada vez que las necesidades lo exijan.</p> <p>NTC-ISO 9001.2015 7.3.1 Infraestructura</p>	<p>Se verificó las actas del Subcomité de Desarrollo Administrativo y se observó cuatro (4) reuniones en el año 2017 y uno (1) de 2018.</p> <p>Ver Recomendaciones.</p>

5.2 REQUISITO DE NO CUMPLIMIENTO – NO CONFORMIDADES

Código NC	Descripción de la No Conformidad	
	Criterio	No Conformidad
	<p>Resolución 1332 del 4 de septiembre de 2014 Sistema de Gestión de Seguridad de la Información</p> <p>NTC-ISO 9001:2015 7.1.3 Infraestructura</p>	<p>Falta de implementación de los objetivos y alcance del Sistema de Seguridad de la Información</p>
	Descripción de Criterio	Evidencia
01-0818	<p>Resolución 1332. Objetivos de Seguridad de la Información.</p> <ul style="list-style-type: none"> • Establecer Guía de Seguridad de la Información. • Lineamientos para asegurar la información y los sistemas de información. • Concientizar a los funcionarios sobre el uso adecuado de los sistemas de información. • Asegurar la continuidad del negocio • Brindar elementos de trazabilidad <p>Alcance. El Sistema de Seguridad de la Información se encuentra basado en el marco de la norma ISO 27001:2013</p> <p>Infraestructura. La organización debe determinar, proporcionar y mantener la infraestructura necesaria para la operación de sus procesos y lograr la conformidad de sus</p>	<p>A partir de la verificación de la implementación de planes, verificación de procesos y capacitaciones del Sistema de Gestión de Calidad no se observó el desarrollo de procedimientos, concientización y desarrollo de actividad en el marco de la implementación del Sistema de Seguridad de la Información.</p> <p>Ver Recomendaciones.</p>

	productos y servicios.	
	Criterio	No Conformidad
	<p>Caracterización del Proceso.</p> <p>Gobierno en Línea: Documentación de la estrategia de TI en el PETI. LI.ES.05 2.8.3.1</p> <p>NTC-ISO 9001:2015 9.1.3 Análisis y evaluación; 9.3.2 Entradas de la revisión por la dirección</p>	Falta de identificación de Indicadores de Seguimiento del PETIC y diferencias en el indicador de seguimiento.
	Descripción de Criterio	Evidencia
02-0818	<p>Caracterización del Proceso: Evaluación del proceso. Realizar seguimiento al PETI.</p> <p>2.8.3.1 Definición de indicadores. Para cada uno de los seis (6) dominios del plan maestro se deben definir indicadores de logro y resultado, incluyendo: tipo Indicador (proceso o logro), nombre, descripción, metas para los siguientes años, meta (valor esperado).</p>	<p>Una vez se verificó la batería de indicadores asociada al área de Tecnología de la Información y de las Comunicaciones no se observó indicadores de seguimiento al PETIC.</p> <p>Asimismo, se replicó el indicador de tercer y cuarto trimestre denominados "Cumplimiento en el tiempo para la atención de incidentes y requerimientos de TIC" y se observó diferencia en el cálculo.</p> <p>Ver anexo 1. Indicadores</p> <p>Ver Recomendaciones.</p>
	Criterio	No Conformidad
03-0818	<p>Procedimiento Atención de Incidencias y Requerimientos. TIC-pr-01.</p> <p>5.7...Tiempo de atención y solución...</p> <p>NTC-ISO 9001.2015 7.3.1 Infraestructura</p>	Incumplimiento en los tiempos establecidos para el trámite de tickets

	Descripción de Criterio	Evidencia
	<p>5.7 De acuerdo al nivel de impacto el tiempo de atención y solución de incidencias se efectuará bajo el siguiente esquema de servicio...</p>	<p>De los 433 tickets analizados, se observó que 73 no cumplieron los tiempos establecidos.</p> <p>Anexo 2. Trazabilidad tickets</p>

6. EVALUACIÓN DEL RIESGO

Riesgo identificado / Posible riesgo	Observación	Responsable del análisis del riesgo
<p>Pérdida o indisponibilidad de la información</p>	<p>Para el riesgo se observan controles asociados a: Hardenig de RED Hardenig de SERVIDORES y Hardenig de equipos de COMPUTO. La Oficina de Control Interno recomienda una desagregación del riesgo conforme a la metodología aplicables en materia de identificación de riesgos TIC, con el fin de efectuar controles que permitan un monitoreo efectivo en el cual se garantice trazabilidad, frecuencia y documentación del mismo.</p> <p>Asimismo, efectuar una valoración de los controles de tal manera que permita abordar el riesgo residual, toda vez que se identifica que la calificación del riesgo antes y después de controles permanece constante.</p>	<p>Profesional de Gestión del Área TIC</p>

7. CONCLUSIONES Y RECOMENDACIONES

Del análisis de criterio efectuado al área de Tecnología de la Información y de las Comunicaciones se obtuvo una calificación de 63% de cumplimiento.

Respecto a la caracterización del proceso se recomienda determinar otros clientes internos y externos dentro de las etapas del proceso TIC, así como los productos asociados al PETIC que pueden considerarse salidas y entradas dentro del proceso.

En cuanto al Plan Estratégico de Tecnología de la Información y de las Comunicaciones 2018-2022, se generan las siguientes recomendaciones acorde a los ítems que lo componen:

	INFORME DE AUDITORIA	Auditoría no.		08-18
		Fecha del informe		
		Día	Mes	Año
		01	06	2018

Tabla 1. Actualización PETIC-Recomendaciones

Ítem	Guía	Observación
Uso y Apropiación de la Tecnología	2.5.2	Desarrollar la valoración de uso y apropiación de los sistemas misionales.
Sistemas de Información	2.5.3	Incluir los campos de líder funcional y líder técnico, módulos de los sistemas, contrato activo, grado de aceptación, controles, Incluir esfuerzos, logros, problemáticas y recomendaciones.
Gestión de Información	2.5.5	Reorganizar cuadro con diagnóstico y solución.
Gobierno TI	2.5.6	Incluir función principal, cantidad de funcionarios y contexto del organigrama, así como los perfiles de los funcionarios.
Necesidades de información	2.6.2	Incorporar los flujos de información para atención al ciudadano, gestión documental, gestión financiera, gestión del talento humano, gestión de contratación. Falta categorías de la información, Gestión de actividad litigiosa, entes de control, entre otras.
Alineación de la estrategia de TIC con la estrategia de la institución pública	2.7.1.3	Fortalecer el contexto y descripción en la cual se desarrolla el ítem.
Gobierno TI	2.7.2	Fortalecer el contexto y descripción en la cual se desarrolla el ítem.
Cadena de Valor	2.7.2.1	Fortalecer el contexto y descripción en la cual se desarrolla el ítem.
Plan de Implementación de procesos	2.7.2.3	Desarrollar el ítem conforme al plan de procesos con los mínimos establecidos para el área TIC.
Estructura organizacional TI	2.7.2.4	A partir del análisis de la estructura organizacional existente en el área de TI realizado en el numeral 2.5.4 se debe estructurar o mantener una estructura de funciones y roles que permita cumplir con los objetivos estratégicos de TI. Incluir función principal, cantidad de funcionarios y contexto del organigrama, así como perfiles de los funcionarios.

Herramientas de análisis	2.7.3.1	Desarrollar el componente teniendo en cuenta las herramientas de análisis, iniciativa a largo plazo para la parte misional, convenios interinstitucionales, valoración cruzada de listados, creación de bodegas de datos y desarrollo de BI, modelamiento de datos para la toma de decisiones, las herramientas de información para análisis (grupo de inteligencia de negocios) empoderar a los usuarios funcionales del análisis. Asimismo Biodata kactus, evaluación del desempeño través de Kactus.
Arquitectura de Información	2.7.3.2	Fortalecer el análisis con los sistemas de apoyo de la entidad.
Arquitectura de sistemas de información	2.7.4.1	Fortalecer el análisis con los sistemas de apoyo de la entidad y determinar un contexto al gráfico.
Implementación de sistemas de información	2.7.4.2	Desarrollar el ítem a partir de la Identificación de arquitectura, definición del alcance y análisis de requerimientos, construcción del sistema, puesta en producción y pruebas, uso de la solución, mesas de trabajo, pruebas y finalidad.
Servicios de soporte técnico	2.7.4.3	Proceso de soporte técnico mesa de ayuda en el contexto futuro.
Modelo de gestión de servicios tecnológicos	2.7.5.1	Incorporar los criterios de calidad. Ejemplos de criterios de calidad son: alta disponibilidad, recuperación ante desastres, capacidad para responder de manera rápida y controlada a las demandas de crecimiento de los servicios (escalabilidad), uso de mejores prácticas como ITIL e ISO 20000. Asimismo, Criterios de calidad y gestión tic, Infraestructura, Conectividad, Servicio de operación, Mesas de servicios y Procedimientos de gestión.
Infraestructura	2.7.5.2	No se observa el desarrollo del Ítem Observación: Desarrollar el ítem conforme a la guía.
Conectividad	2.7.5.3	No se observa el desarrollo del Ítem Observación: Desarrollar el ítem conforme a la guía.
Servicios de operación.	2.7.5.4	No se observa el desarrollo del Ítem Observación: Desarrollar el ítem conforme a la guía.
Mesa de servicios	2.7.5.5	No se observa el desarrollo del Ítem Observación: Desarrollar el ítem conforme a la guía.

Procedimientos de gestión	2.7.5.6	Los procedimientos que deben ser incluidos como mínimo: mesa de Estructura del Plan Estratégico de TI Guía Técnica servicios, gestión de incidentes, gestión de problemas, gestión de eventos, gestión de cambios, gestión de seguridad, gestión de la configuración, gestión de la entrega, gestión de niveles de servicio, gestión de disponibilidad, gestión de capacidad y gestión de continuidad. No se observa en el marco del ítem cuales procedimientos se van a desarrollar si no cuales se tienen en este momento.
Uso y apropiación	2.7.6	Desarrollar los ítems de acuerdo a los proyectos de evaluación y apropiación de los nuevos sistemas de información y el rezago de los antiguos.
Lineamientos y/o principios que rigen el plan estratégico de TIC	2.8.1	Establecer lineamientos de tecnología a futuro como por ejemplo: La toma de decisiones de la entidad a partir de las herramientas tecnológicas, Procesos misionales se fundamenten a partir de análisis BI, Indicadores de gestión a partir de estadísticas, entre otras.
Estructura de actividades estratégicas	2.8.2	Enfocar el desarrollo del ítem sobre Iniciativas consolidadas en el documento y detallar las etapas para llegar al objetivo. Por ejemplo: La semaforización de los procesos, Análisis de Kactus, Análisis de Seven, Análisis de los misionales y diseñarla sobre la estructura del plan de acción, con los valores por año para cada Roadmap de inversión.
Plan maestro mapa de ruta	2.8.3	Fortalecer el Roadmap a través de un cuadro de plan de inversión (dominios - proyecto) + producto esperado por proyecto
Definición de indicadores.	2.8.3.1	Para cada uno de los seis (6) dominios del plan maestro se deben definir indicadores de logro y resultado, incluyendo: tipo Indicador (proceso o logro), nombre, descripción, metas para los siguientes años, meta (valor esperado). No se observa el desarrollo de los indicadores.
Proyección de presupuesto área de TI	2.8.4	Establecer el seguimiento mensual al presupuesto.
Plan de intervención sistemas de información	2.8.5	Establecer el Plan de intervención del Invesflow para cambiarlo al nuevo modelo.

Plan de comunicaciones del PETI	2.9	Desarrollar el plan de comunicaciones del PETIC.
---------------------------------	-----	--

Fuente: Control Interno

Como se observa en la tabla anterior, algunos de los ítems no se han desarrollado y otros es necesario fortalecer y/o anexas los instrumentos al PETIC ya desarrollado, por lo cual se recomienda actualizar el documento PETIC conforme a las observaciones realizadas, asimismo implementar los mecanismos e instrumentos de seguimiento y control de la información y las actividades planteadas.

En cuanto a la verificación del inventario de equipos, efectuar la actualización de aquellos que se encontraban en arrendamiento, dada la adquisición de nuevos equipos.

Con relación a la Política de Seguridad de la Información y a través de los instrumentos del PETIC establecer el plan de implementación de procesos, que permitan dar respuesta al nuevo esquema incorporado del modelo tecnológico para el COPNIA a la par de la implementación del Sistema, el cual representa un reto para la modernización de la gestión de la Entidad.

En cuanto a la trazabilidad de los tickets de servicio se verificó lo correspondiente a los periodos julio 2017 a diciembre 2017 y enero 2018 a abril 2018. De un total de 5001 registros de solicitudes, se observó una recepción mensual promedio de 500 tickets.

Tabla 2. Promedio Tickets

mes	cantidad
julio	550
agosto	676
septiembre	521
octubre	383
noviembre	409
diciembre	397
enero	735
febrero	454
marzo	396
abril	480

Fuente: Área TIC

	INFORME DE AUDITORIA	Auditoría no.		08-18
		Fecha del informe		
		Día	Mes	Año
		01	06	2018

Para cada año, se pueden visualizar en la siguiente tabla las solicitudes agrupadas por tipo de soporte:

Tabla 3. Tipología de Tickets

Tipología	No Tickets 2017	No Tickets 2018
Administración de Usuarios	102	49
Invesdoc Gallery Suite	2020	1321
Networking - Redes y Comunicación	158	109
Página Web	28	12
SEVEN ERP	120	206
Sistema KACTUS	55	44
Software Consulta de Matriculado	15	24
Solicitud Resolución Nacional	173	0
Soporte Equipos De Computo	265	300
Total	2936	2065

Fuente: Área TIC

Para realizar la verificación y de acuerdo a lo establecido en la tabla, la tipología en la que se encuentran los porcentajes más altos de solicitudes es en "INVEDOC GALLERY SUITE" para 2017 el 69% del total.

En cuanto a la revisión de los requerimientos de novedades de personal, se observó que el ticket 19376 en el formato tiene la firma de Subdirector Administrativo y Financiero (E), sin embargo, no tiene la firma del Profesional de Gestión del área de Gestión Humana, el ticket 19580 tiene la firma de un abogado del Seccional Cundinamarca, no obstante, no tiene la firma del Profesional de Gestión del área de Gestión Humana y el ticket 19590 es un formato en Excel que no contiene firmas. Por lo cual se recomienda que los formatos este firmados por el profesional de Gestión Humana o quien haga sus veces con el visto bueno del jefe inmediato.

Adicionalmente, determinar un mecanismo para evaluar la satisfacción del usuario sobre la solución de los tickets.

En cuanto al modelo de riesgos, la auditoria identificó documentos en los cuales se encuentran plasmados riesgos no contemplados en la matriz de riesgos del COPNIA, razón por la cual se considera pertinente analizar la implementación de lo mismos en la matriz general de la Entidad, así como la actualización de controles en los cuales se considere la implementación de bitácoras, rutinas de monitoreo a campos específicos de las bases, verificación de consecutivos y monitoreo de matrices de roles y privilegio.

Por otra parte, es pertinente fortalecer las herramientas del Sistema de Gestión de Calidad y de Control Interno en cuanto al conocimiento de riesgos del procesos y controles, asimismo la socialización y conocimiento de los resultados de la auditoria, como también orientar a los funcionarios sobre el enfoque

	INFORME DE AUDITORIA	Auditoría no.		08-18
		Fecha del informe		
		Día	Mes	Año
		01	06	2018

estratégico del área y su impacto en la organización; esto basado en la encuesta de autocontrol realizada al equipo de trabajo.

Por último, es importante resaltar que para los funcionarios y contratistas del área se ha observado la mejora del proceso con relación a mesa de ayuda y dinámica general del área.

8. SEGUIMIENTO A PLANES DE MEJORAMIENTO

Código NC	Estado	Observaciones
02-1717	Cerrada	Incumplimiento en la atención de la incidencia reportada por el Seccional Santander en cuanto al funcionamiento de la telefonía CISCO e impresora Xerox. Se efectuó comunicación con el seccional para confirmar la efectividad de la acción, a lo cual se respondió que las líneas telefónicas funcionan correctamente.
09-0318	Abierta	Asignación y activación de usuario en la plataforma SEVEN y portal bancario no asociados a la funciones del cargo. Esta para cierre en el segundo corte de seguimiento a planes de mejoramiento.

9. ANEXOS NO CONFORMIDADES

Anexo 1. Indicadores

Anexo 2. Trazabilidad tickets

Elaborado por: Viviana Marcela Pardo Beltrán

Revisado por: Viviana Marcela Pardo Beltrán