REPÚBLICA DE COLOMBIA COPNIA Consejo Profesional Nacional de Ingeniería	**INFORME DE AUDITORIA**	**Auditoría no.**		**09-21**
		Fecha del informe		
		Día	**Mes**	**Año**
		28	**07**	**2021**

Informe	☐	**Preliminar**	☒	**Final**

1. INFORMACIÓN GENERAL

Tipo de Informe	☒ **Auditoría**	☐	**Seguimiento**
Procesos auditados /Evaluado	Proceso de Gestión de la Tecnología de la Información y de las Comunicaciones		
Jefe OCI	Alberto Castiblanco Bedoya	**Auditor**	Oscar Javier Zabala Merchán
Responsable del proceso, dependencia, área o actividad auditada /evaluada	Profesional de Gestión – Área de TIC´s Profesional Universitario – Área de TIC´s		

2. OBJETIVO

Evaluar la gestión del Proceso de Gestión de la Tecnología de la Información y de las Comunicaciones conforme a los requisitos legales e institucionales tales como procedimientos, políticas, planes y demás lineamientos aplicables.

3. ALCANCE

Verificar el nivel de cumplimiento de las actividades del Proceso de Gestión de la Tecnología de la Información y de las Comunicaciones en el marco de los procedimientos, instructivos, políticas, riesgos y planes estratégicos definidos.

4. ACTIVIDADES DESARROLLADAS

En el marco del proceso de auditoria llevado a cabo, se tomaron como criterios los requisitos establecidos en el modelo de gestión sobre el que se construyó la Estrategia TI para Colombia que es IT4+®. Éste es un modelo resultado de la experiencia, de las mejores prácticas y lecciones aprendidas durante la implementación de la estrategia de gestión TIC en los últimos 10 años. IT4+® es un modelo integral que está alineado con la estrategia empresarial u organizacional y permite desarrollar una gestión de TI que genere valor estratégico para la organización y sus clientes.

Este modelo está basado en los lineamientos de la Norma ISO 27001:2013, así como las políticas, lineamientos, procesos y procedimientos institucionales y las normas legales establecidas en el Normograma de la institución, con el fin de determinar el grado de eficacia del proceso.

Las actividades efectuadas en el desarrollo de la auditoría fueron las siguientes:

1.- Se realizó firma del contrato PROCESO: CD – P – 36– 2021 del 24 de mayo de 2021 el cual tiene como OBJETO DEL CONTRATO: Prestación de servicios profesionales como auditor de

Tecnologías de la Información y las Comunicaciones TICS, a la oficina de Control Interno, con el fin de apoyar el Programa Anual de Auditoria Interna del Consejo Profesional Nacional de Ingeniera Copnia.

2.- Luego de protocolizar el contrato con sus respectivas pólizas el 25 de mayo y 26 de mayo se nombra al Supervisor del contrato al Doctor Alberto Castiblanco quien realizó las solicitudes de accesos a las diferentes plataformas de la entidad.

3.- El 27 de mayo de 2021 se generaron los accesos a los aplicativos por parte del profesional Universitario. Se realizaron acercamientos con el área de las TIC´s para los ingresos y el día 8 de junio de 2021 se realizó la reunión de apertura.

4.- Los días: junio 8, 9, 18, 21, 25 y julio 2 y 8 de 2021 se realizaron actividades de manera remota usando la plataforma Microsoft Teams, el día 25 de junio de 2021 se realiza visita presencial a las instalaciones de la sede nacional en la calle 78. En todas las actividades participaron activamente el Profesional de Gestión – Área de TIC´s y el Profesional Universitario – Área de TIC´s

Los resultados obtenidos en el desarrollo de las actividades se describen a continuación:

4. CONTEXTO DE LA ORGANIZACIÓN

4.1 Comprensión de la organización y de su contexto:

Dentro de la CARACTERIZACIÓN DEL PROCESO TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONESde código TIC-CP-01, se cuenta con un DOFA manejado en calidad. Desde 1936 el COPNIA tiene registros de profesionales desde el mismo grado, conservan mucha información de muchos tipos y en diferentes repositorios, desde el 2019 se estructuró el PETIC basado en TOGAF, con un estudio de arquitectura empresarial AS -IS y TO-BE, generando el PETIC, Mintic IT4+ y Análisis de Infraestructura TI, con las conclusiones de adquirir un BPM y un Gestor Documental, migraron el directorio activo a Azure, Karspesky en la nube, office 365.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas.

Dentro de la CARACTERIZACIÓN DEL PROCESO TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES de código TIC-CP-01 y en la DOFA año 2020 con factores internos y externos

4.3 Determinación del alcance del sistema de gestión de la calidad.

Se tomaron como criterios los requisitos establecidos en el modelo de gestión sobre el que se construyó la Estrategia TI para Colombia que es IT4+® y en el caso especificó del COPNIA, el Manual de seguridad de la información. Éste es un modelo resultado de la experiencia, de las mejores prácticas y lecciones aprendidas durante la implementación de la estrategia de gestión TIC en los últimos 10 años. IT4+® es un modelo integral que está alineado con la estrategia

empresarial u organizacional y permite desarrollar una gestión de TI que genere valor estratégico para la organización y sus clientes.

.

4.4 SISTEMA DE GESTIÓN DE LA CALIDAD Y SUS PROCESOS.

La organización ha definido procesos/procedimientos que puede mejorar para la conveniencia del SGSI.

5. LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO

El liderazgo y el compromiso de la dirección, se evidencia en la formulación de la política, la expedición del documento denominado Manual de Seguridad de la Información, la formulación y adopción del PETIC y el seguimiento de indicadores y acciones o compromisos de mejora que realiza trimestralmente el Comité de Gestión y Desempeño.

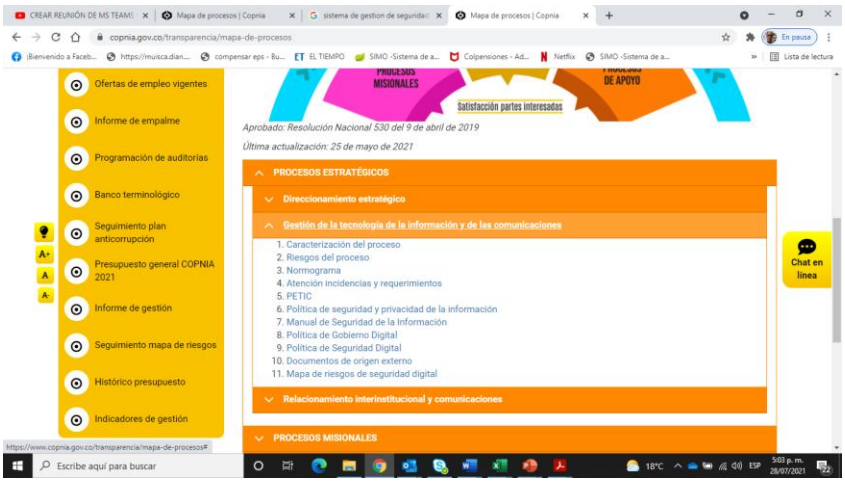
5.2 POLÍTICA

Existe un PETIC PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES 2018 -2022 firmado por el director general y documentación de alineación estratégica con la organización. Existe la resolución 2068 del 24/12/2019 por medio de la cual se adopta la política de Gestión y Desempeño de Seguridad Digital para Copnia, por otro lado, existe la resolución 2069 del 24/12/2019 por medio de la cual se adopta la política de Gestión y Desempeño de Gobierno Digital para Copnia.

En el Link https://www.copnia.gov.co/transparencia/mapa-de-procesos, se evidencia la existencia de los componentes básicos del Sistema de Seguridad de la Información que ha implementado el COPNIA, a saber:

1. Caracterización del proceso
2. Riesgos del proceso
3. Normograma
4. Atención incidencias y requerimientos
5. PETIC
6. Política de seguridad y privacidad de la información
7. Manual de Seguridad de la Información
8. Política de Gobierno Digital
9. Política de Seguridad Digital
10. Documentos de origen externo
11. Mapa de riesgos de seguridad digital

Grafico: Pantallazo Mapa de procesos – Gestion de las TICS



5.3 Roles, responsabilidades y autoridades de la organización.

En los procesos de Gestión Humana Manual de funciones versión 18/08/2021, se valida el perfil de un profesional universitario código 2044 y el de profesional de gestión código 2165 (Iván) profesional especializado (2028) (Isaac Pereira), son 3 2044.

6 Planificación.

6.1 Acciones para abordar los riesgos y las oportunidades. Se valida la matriz de riesgos en MAPA DE RIESGOS DE SEGURIDAD DIGITAL, versión 1 de diciembre de 2020 alineada a 4+ con causa consecuencia, riesgo inherente, Se uso la metodología de Mintic en la versión 4+ para la Gestión de los Riesgos.

6.1.2 Evaluación de riesgo de la seguridad de la información

Se valida la matriz de riesgos en MAPA DE RIESGOS DE SEGURIDAD DIGITAL, versión 1 de diciembre de 2020 alineada a 4+ con causa consecuencia, riesgo inherente, figurando como responsables Profesional de gestión del área TIC, y en el cual se evidencia la identificación, valoración y administración del riesgo residual, asociado al riego de seguridad de la información, cuando hay ocurrencia no autorizada de: Sustracción de información Eliminación de Información Modificación de la información Pérdida de información. Indisponibilidad de información. Divulgación de información sensible.

6.1.3 Tratamiento de riesgo de la seguridad de la información

Se valida la matriz de riesgos en MAPA DE RIESGOS DE SEGURIDAD DIGITAL, versión 1 de diciembre de 2020 alineada a 4+ con causa consecuencia y riesgo residual.

Sin embargo, no se evidencia un documento que soporte la "Declaración de aplicabilidad (SoA por sus siglas en inglés Stament off Aplicabillity))", que permita asegurar el compromiso y la aceptación explícita de los funcionarios y contratistas con el cumplimiento de la política, objetivos, metas y acciones de control para el tratamiento del riesgo inherente y residual.

Adicionalmente, se evidencia que la primera acción de control para eliminar el riesgo residual de seguridad de la información, se describe como "Implementar el SGSI en el COPNIA con los lineamientos de seguridad de la información para generar acciones preventivas y correctivas en la entidad", lo que hace entender que el proceso de implementación del sistema de seguridad de la información es posterior a las acciones de control del riesgo inherente, generándose una contradicción conceptual del mismo.

6.2 Objetivos de seguridad de la información y planificación para lograrlos

Existe un PETIC-PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES - 2018 -2022, firmado por el director general y documentación de alineación estratégica con la organización. Existe la resolución 2068 del 24/12/2019 por medio de la cual se adopta la política de Gestión y Desempeño de Seguridad Digital para Copnia, por otro lado, existe la resolución 2069 del 24/12/2019 por medio de la cual se adopta la política de Gestión y Desempeño de Gobierno Digital para Copnia.

El PETIC se ha formulado, en alineación a la estrategia institucional "Contar con una arquitectura tecnológica, que incluya lineamientos, estándares y mejores prácticas, para el soporte y el manejo apropiado de los datos y la información, en términos de autenticidad, integridad, fiabilidad y disponibilidad" la cual está dentro del marco del segundo objetivo estratégico institucional descrito como "Fortalecer y articular el modelo de gestión de la entidad para mejorar la prestación de los servicios misionales", como se puede evidenciar en el artículo octavo, de la resolución 1703 del 30 de noviembre de 2018 del COPNIA y en coherencia con el primer objetivo especifico del PETIC 2018 – 2022, en su segunda versión vigente a partir del mes de enero de 2020.

7. APOYO

7.1 Recursos Son una entidad de origen público y manejan su propio presupuesto, se valida el presupuesto anual en TI para el año 2021 es de: $2.121.100.000

7.2 Competencias En los procesos de Gestión Humana Manual de funciones versión 18/08/2021, se valida el perfil de un profesional universitario código 2044 y el de profesional de gestión codigo 2165 (Iván) profesional especializado (2028) (Isaac Pereira)

7.3 Conocimiento Las personas que trabajen en el COPNIA tienen conocimiento de la política de seguridad de la información; los resultados del seguimiento y evaluación frente al cumplimiento de los indicadores de gestión y de seguridad en la información que analiza el

Comité de Gestión y Desarrollo y de las implicaciones disciplinarias por no cumplir con los requisitos del SGSI.

Como evidencia, se observa la realización de jornadas de capacitación, socialización y sensibilización que se hace periódicamente, a través de comunicados, capsulas informativas y NotiCopnia. La última medición evidencia que el nivel de asistencia a jornadas de capacitación fue del 94% en las capacitaciones del SGSI-Tienen ERP Seven y Cactus de Digital Ware, tiene con ETB un IAS, y los servidores del IVESTDoc (Corte Ingles).

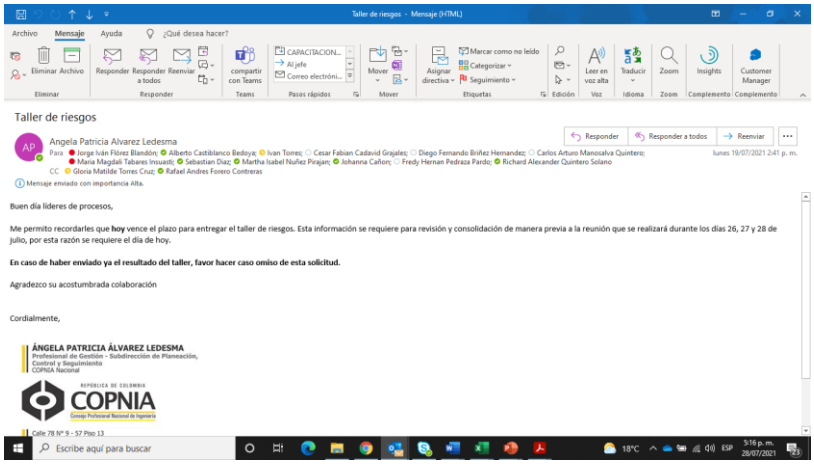
7.4 Comunicación La organización cuenta con los medios adecuados para las comuniciones internas y externas, se valida el documento de código CI-m-02 MANUAL DE COMUNICACIONES.

7.5 Información documentada Se verifica la página: https://gestordocumental.copnia.gov.co/sites/docs/ Se valida el listado maestro de documentos externos y el proceso Control de documentos DE-pr-01 de nov de 2019

8. OPERACIÓN

8.1 Planificación y control operacional. Los riegos validados en el mapa de riesgos versión 7 están alineados con el Sistema de Gestión de Calidad. Se valida el Mapa de riesgos de Seguridad Digital versión 1 vigente a partir de diciembre de 2020 cuenta con 3 riesgo asociados a la pérdida de Confidencialidad, Integridad y Disponibilidad.

8.2 Evaluación de riesgo de la seguridad de la información. Se valida el mapa de riesgos versión 7 con fecha de revisión de enero de 2019, la norma habla de intervalos planificados y han pasado 2 años y medio desde la última revisión de acuerdo con este documento; sin embargo, de manera trimestral se realizan talleres de revisión del mapa de riesgos, a través de los cuales cada líder de proceso debe actualizar o ratificar los riesgos identificados y su tratamiento, como se puede observar en el pantallazo de invitación de correo electrónico, en el que solicita dicha actualización:



Por lo anterior, es recomendable actualizar la fecha del documento oficial publicado, para que la misma corresponda a la fecha de la última revisión y ajuste.

8.3 Tratamiento de riesgo de la seguridad de la información. En el Mapa de Riesgos se evidencia que se identifica cómo "Riesgo de seguridad de la información: cuando hay ocurrencia no autorizada de: Sustracción de información Eliminación de Información Modificación de la información Pérdida de información. Indisponibilidad de información. Divulgación de información sensible."

Igualmente se evidencia que, frente al riesgo identificado, se han descrito las acciones de control existente, así:

*Subcomité de seguridad de la información, que vela por el cumplimiento de las políticas de seguridad de la información de la entidad, en cuyas funciones toma decisiones que generan lineamientos y reportes a entes de control en caso de ser necesario consignándose en actas.

*Especificaciones técnicas exclusivas para el tema de seguridad de la información en los contratos de proyectos tecnológicos, contratos de soporte y mantenimiento.

*Reporte en bitácora de seguimiento de tickets en caso de encontrar un evento que atente a la seguridad, integridad o disponibilidad de la información.

*Alertas a través de informes proactivos

Y para el tratamiento del riesgo residual, se han identificado acciones de control, así:

* Para eliminar las causas del riesgo: Implementar el SGSI en el COPNIA con los lineamientos de seguridad de la información para generar acciones preventivas y correctivas en la entidad

*Para reducir y evitar el riesgo: Generar especificaciones técnicas detalladas de seguridad de la información en los contratos donde se detalla acciones proactivas y reactivas

*Contingencia: Restaurar backups enmarcados en los RPO y RTO pactados contractualmente

Se reitera la anotación hecha en el numeral 6.1.3 del presente informe

9. Evaluación de desempeño

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN. Se valida ANÁLISIS INDICADOR PETIC 2020 con una Frecuencia trimestral y una meta particular para cada vigencia del 100%, en el proyecto de seguridad de la información el resultado es del 83%, los otros 5 ítems tienen un resultado del 100%.

En este punto, se recomienda, elaborar y oficializar un documento que de soporte al Plan Estratégico de Seguridad de la Información – PESI o Plan de Seguridad Informática – PSI o el Modelo de Seguridad y Privacidad de la Información (MSPI – ver https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/), en el que se identifique:

1. Alertas y acciones ante el riesgo de ciberataques
2. Prever cambios en el sistema informático, que respondan a las necesidades y requerimientos de hardware y software, según las necesidades cambiantes de los procesos
3. Identificación de nuevas vulnerabilidades de seguridad
4. Revisión periódica de las políticas y procedimientos de seguridad informática

El documento sugerido, debería contemplar aspectos básicos, tales como

La identificación y registro de los activos de información (Programas informáticos, servidores, servicios externos como alojamiento Web, bases de datos o registros)

Frente a cada activo, identificar los riesgos y su daño potencial en caso de materializarse los mismos (virus informáticos, hackers, daños físicos, errores humanos)

Evaluación de cada uno de los daños potenciales, para priorizar la protección de los activos con mayor impacto en la entidad.

Identificación de las acciones o medidas de precaución para la protección de los activos (restricciones de acceso, instalación de firewall, plan de recuperación ante fallos o desastres, plan de contingencia, entre otros)

Definición e implementación de las estrategias de socialización y sensibilización de funcionarios y contratistas frente al PESI, incluyendo la firma de la carta de compromiso o declaración de aplicabilidad.

Mantenimiento del plan de seguridad Informática, con monitoreo de indicadores que permitan medir la eficacia y la efectividad de las acciones y controles implementados.

9.2 Auditoría Interna: Se valida el proceso "Auditorias Internas" de código EG-pr-01 que determina los lineamientos para evaluar el grado de cumplimiento de la Entidad frente a la normatividad legal vigente, las disposiciones internas planificadas, los modelos de gestión y/o cualquier otro lineamiento adoptado. Esta es la primer auditoria realizada al SGSI (TIC´s)

9.3 Revisión por la dirección: Se valida los temas de Revisión por la Dirección a nivel del Sistema de Gestión de calidad que incluye los procesos de Tecnologías de la Información y las Comunicaciones TICS; sin embargo, no se evidencia una evaluación integral del Sistema de Gestión de Seguridad de la Información.

10. MEJORA

10.1 No conformidades y acciones correctivas. No aplica ya que no tienen acciones de mejora asociada a hallazgos o inconformidades de auditorías anteriores.

10.2 Mejora continua. No aplica ya que no tienen acciones de mejora asociada a hallazgos o inconformidades de auditorías anteriores.

5. HALLAZGOS

En cumplimiento de los lineamientos señalados en la guía de auditorías, "Guía de auditoría interna basada en riesgos para entidades públicas", versión 4, de julio de 2020, en especial lo señalado en su numeral 2.4.3, expedido por el DAFP, se procede a revisar y evaluar las evidencias aportadas por el auditado, encontrando que el COPNIA soporta su Sistema de Seguridad de la Información en el MANUAL DE SEGURIDAD DE LA INFORMACIÓN TIC-m-01 Vigente a partir de Julio de 2019 1era. Actualización.

Para la evaluación contenida en el objeto de la presente auditoria, se consideraron 26 criterios, de obligatorio cumplimiento, evidenciando que no se encontraron hallazgos asociados a incumplimiento de la Ley y que se evidencio el incumplimiento de un criterio, asociado a la inexistencia de un documento que sustente la declaración de aplicabilidad, como tampoco que permita evidenciar la aceptación para el tratamiento de los riesgos residuales por parte de funcionarios y contratista (Ver numeral 5.1 del presente informe).

Igualmente se procedió a revisar los criterios de control que sugiere el modelo de gestión sobre el que se construyó la Estrategia TI para Colombia IT4+®, cuyo fundamento son los lineamientos de la Norma ISO 27001:2013; en consecuencia se evaluaron 112 criterios asociados a los controles que propone dicha norma técnica, con el propósito de identificar la posible brecha que existe entre los controles aplicados según el Manual de Seguridad de la entidad, frente a los sugeridos por la norma técnica, para plantear a par de ello posibles acciones de mejora, por parte del auditado. 8Ver numeral 5.2 del presente informe

5.1 REQUISITOS MINIMOS EXIGIDOS CON INCUMPLIMIENTO

Criterio	Evidencia
6.1.3 Tratamiento de riesgo de la seguridad de la información La organización debe definir y aplicar un proceso de tratamiento de riesgo de la seguridad de la información para: a) seleccionar las opciones apropiadas de tratamiento de riesgo de la seguridad de la información, tomando en consideración los resultados de la evaluación de riesgo; b) determinar todos los controles que son necesarios	No existe un documento denominado "Declaración de Aplicabilidad o SoA (por sus siglas en inglés Statement off Applicability) y no se evidencia la aceptación del plan de tratamiento de los riesgos y de los riesgos residuales por parte de los propietarios de los riesgos.

para implementar las opciones de tratamiento de riesgo de la seguridad de la información escogida; NOTA Las organizaciones pueden diseñar controles, según sea necesario, o identificarlos desde cualquier fuente. c) comparar los controles definidos en 6.1.3 b) más arriba con aquellos en Anexo A y verificar que ningún control necesario fue omitido; NOTA 1 Anexo A contiene una completa lista de objetivos de control y controles. Los usuarios de esta norma son dirigidos al Anexo A para asegurar que ningún control necesario se pasó por alto. NOTA 2 Los objetivos de control se incluyen de manera implícita en los controles escogidos. Los objetivos de control y los controles enumerados en Anexo A no son exhaustivos, por lo que se podrían necesitar objetivos de control y controles adicionales. d) generar una Declaración de Aplicabilidad que contenga los controles necesarios [consultar 6.1.3 b) y c)], y además la justificación de inclusiones, sean estas implementadas o no y la justificación para exclusiones de controles de Anexo A; e) formular un plan de tratamiento del riesgo de seguridad de la información; y f) obtener la aprobación del propietario del riesgo del plan de tratamiento del riesgo de la seguridad de la información y la aceptación de los riesgos de la seguridad de la información residual. La organización debe conservar la información documentada acerca del proceso de tratamiento del riesgo de la seguridad de la información.	

5.2 REQUISITOS DE CONTROLES DEL ANEXO CON INCUMPLIMIENTO

CONTROL	Evidencia
A.8.2.2 Etiquetado de la información Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo	Si bien es cierto que la entidad cuenta con un procedimiento específico para el manejo de bienes, identificado como AB-pr-02, vigente a partir de Noviembre de 2020, no se evidencia que exista un procedimiento

con el esquema de clasificación de información adoptado por la organización.	detallado para el etiquetado del inventario de activos de la información.
A.8.2.3 Manejo de activos Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No existe procedimiento, sólo hay una referencia en El documento Manual de la Seguridad de la Información, de código TIC-m-01, vigente a partir de Julio de 2019, 1era. Actualización, indica en su numeral en 5.2.5 Disposición de los activos
A.8.3.2 Eliminación de los medios Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales	El numeral 5.2.4 Gestión de medios removibles del Manual TIC-m-01 no determina la eliminación de los medios, se valida ejemplo de extracción de un firewall de las instalaciones de COPNIA sin borrado seguro.
A.8.3.3 Transferencia física de medios Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte.	El Manual de la Seguridad de la Información, de código TIC-m-01 no determina la Transferencia física de medios
A.10.1.1 Política sobre el uso de controles criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No existe política sobre el uso de controles criptográficos
A.10.1.2 Gestión de claves Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.	No se establecen los controles sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.
A.11.1.4 Protección contra amenazas externas y del ambiente Se debe diseñar y aplicar la protección física contra daños por desastre natural, ataque malicioso o accidentes.	No se observan sensores ni CCTV que garanticen la protección por desastres a ataques maliciosos.
A.11.1.5 Trabajo en áreas seguras Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.	No existe procedimiento para trabajar en áreas seguras

A.11.1.6 Áreas de entrega y carga Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones, y si es posible, aislarlas de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.	No están definidos los controles sobre las áreas de carga
A.12.1.3 Gestión de la capacidad Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Para la gestión de la capacidad, en el numeral 3.12 de Implementación de Proyectos tecnológicos, en el Manual de Seguridad de la Información de código TIC-m-01, pero no especifica la Gestión de la Capacidad
A.12.3.1 Respaldo de la información Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.	Se valida el Manual de Seguridad de la Información de código TIC-m-01 numeral 3.2.5 Disposición de activos, enfocados hacia Azure, One Drive, respaldo de las BD cada 24 horas. No hay pruebas de restauración periódicas ni políticas.
A.12.4.3 Registros del administrador y el operador Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.	No se valida la revisión periódica de los registros de los administradores y/o usuarios privilegiados.
A.12.6.1 Gestión de las vulnerabilidades técnicas Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado.	Se tiene el procedimiento de ATENCIÓN DE INCIDENCIAS Y REQUERIMIENTOS de código TIC-pr-01, se valida el contrato de la página web en el contrato 84-2016 v1.0 con las definiciones de seguridad, sin embargo, no se valida un contrato de un Hacking Ético periódicamente.
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	La organización dentro de su objeto

A.14.1.2 Aseguramiento de servicios de aplicación en redes públicas. A.14.1.3 Protección de las transacciones de servicios de aplicación A.14.2.1 Política de desarrollo seguro A.14.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación A.14.2.4 Restricciones en los cambios a los paquetes de software. A.14.2.5 Principios de ingeniería de sistema seguro A.14.2.6 Entorno de desarrollo seguro A.14.2.8 Prueba de seguridad del sistema A.14.2.9 Prueba de aprobación del sistema A.14.3.1 Protección de datos de prueba	contractual NO está el desarrollo de software, por lo tanto, no aplica estos controles. Se excluye este criterio en la calificación.
A.17.1.1 Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	El Manual de la Seguridad de la Información, de código TIC-m-01 en el numeral 5. 5.8 Disponibilidad del Servicio e Información, indica que el área de TIC´s implementará la continuidad, no se determinan los requerimientos en situaciones adversas.
A.17.1.2 Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.	El Manual de la Seguridad de la Información, de código TIC-m-01 en el numeral 5. 5.8 Disponibilidad del Servicio e Información, indica que el área de TIC´s implementará la continuidad, no se determinan procesos, procedimientos y controles para asegurar el nivel necesario de continuidad
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas.	El Manual de la Seguridad de la Información, de código TIC-m-01 en el numeral 5. 5.8 Disponibilidad del Servicio e Información, indica que el área de TIC´s implementará la continuidad, no se verifica de forma periódica la continuidad.

A.18.2.2 Cumplimiento con las políticas y normas de seguridad. Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.	No se evidencia validación de los procesos/procedimiento, asociados a los controles de la seguridad de la información, por parte de los lideres de los procesos de la entidad, estos son realizados por el área de sistemas mediante un autodiagnóstico.

7. CONCLUSIONES Y RECOMENDACIONES

El resultado del ejercicio auditor obtuvo un cumplimiento del 92% frente a los 26 criterios mínimos de auditoría evaluados y de los cuales los soportes se encuentran en la tabla denominada *"Anexo 7.3 Análisis de criterios objeto de auditoria evaluación"* en la página *"Análisis"*.

Respecto al cumplimiento de los controles asociados a la norma técnica, establecidos en el Anexo A de la misma, se encuentra un nivel de cumplimiento del 78% de los 101 controles sugeridos (Excluyendo los que no aplican), los soportes de esta revisión se encuentran en el documento *"Anexo 7.3 Análisis de criterios objeto de auditoria evaluación"* en la página *"Controles"*. A continuación, se describen las conclusiones y recomendaciones.

1. Norma IEC/ISO 27001:2013

1. El Sistema de Gestión de Seguridad de la Información, está documentado a través del Manual de Seguridad de la Información, el cual se ha elaborado a partir del modelo propuesto por MINTIC IT4+, que es una buena práctica basada en la ISO 27001:2013

2. Se resalta la infraestructura física y las inversiones realizadas por la entidad para adquirir los productos y servicios de Nube Azure, Office 365, BPM y otros productos que han permitido mantener las prácticas actuales de trabajo en casa.

3. El anexo A de la norma ISO 27001:2013 es un código de buenas practicas que permite la exclusión de ciertos controles que no están articulados al objeto social de el COPNIA, como por ejemplo los controles relacionados con Desarrollo de Software. Así mismo, se evidencia una oportunidad de mejora, estableciendo nuevos controles, conforme lo sugiere el anexo de la norma técnica, sin que ello implique la adopción oficial de la misma.

4. A partir de la evaluación, tanto de los criterios mínimos, como de los controles sugeridos en la norma técnica, se presenta una oportunidad de mejora, para

fortalecer el Sistema de Seguridad de la Información, en especial elaborando y oficializando un documento que de soporte al Plan Estratégico de Seguridad de la Información – PESI o Plan de Seguridad Informática – PSI o el Modelo de Seguridad y Privacidad de la Información (MSPI – ver https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/).

8. SEGUIMIENTO A PLANES DE MEJORAMIENTO

No aplica ya que es la primera actividad de Auditoria Interna

9. ANEXOS NO CONFORMIDADES

Proyectado: Oscar Javier Zabala Merchán – Auditor Externo
Revisado por: Alberto Castiblanco Bedoya – Jefe Oficina de Control Interno.