REPÚBLICA DE COLOMBIA COPNIA Consejo Profesional Nacional de Ingeniería	**INFORME DE AUDITORIA**	**Auditoría No.**		**06-23**
		Fecha del informe		
		Día	**Mes**	**Año**
		18	**08**	**2023**

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			
Auditor líder	Alberto Castiblanco Bedoya	**Equipo Auditor**	Oscar Javier Zabala Merchán	
Responsable del proceso, dependencia, área o actividad auditada /evaluada	Profesional de Gestión – 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. 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.

Este modelo está basado en los lineamientos de la Norma ISO 27001:2013 e ISO 27002:2015 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.

Para la evaluación del Sistema de Seguridad de la Información del COPNIA, se ha referenciado como parámetro la norma ISO 27001, teniendo en cuenta que esta "*es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información*." (https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve)

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

1.- Se realizó firma del contrato PROCESO: CD – P – 23– 2023 del 4 de mayo de 2023 el cual tiene como OBJETO DEL CONTRATO: Prestación de servicios profesionales para apoyar a la oficina de Control Interno en la ejecución del programa anual de auditoría interna, especialmente en lo relacionado con realizar la auditoría interna al proceso de gestión de la tecnología de la información y las comunicaciones del Consejo Profesional Nacional de Ingeniera Copnia.

2.- Luego de protocolizar el contrato con sus respectivas pólizas el 2 de mayo de 2023, 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 9 de mayo de 2023 se generaron los accesos a los aplicativos por parte del profesional. Se realizaron acercamientos con el área de las TIC´s para los ingresos, procediendo a realizar las consultas sobre los documentos generales de la organización, lectura de los planes y proyectos publicados, proyección del plan de auditoría a aplicar en la auditoria, proyección preliminar de criterios de auditoría, entre otros y el día 25 de mayo de 2023 se realizó la reunión de apertura.

4- En el periodo comprendido entre 26 de mayo y el 10 de junio se definieron los criterios definitivos de la auditoria, considerando las observaciones y recomendaciones hechas por el Director del COPNIA, según consta en el acta de apertura.

5- Los días: junio 6, 13, 15, 23, 28 y julio 2, 6 y 11 de 2023 se realizaron actividades de manera remota usando la plataforma Microsoft Teams, el día 11 de julio de 2023 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 – Área de TIC´s.

Entre el 11 de julio y el 27 de julio de 2023 se procedió a elaborar la primera versión del informe preliminar y se presentó para revisión y observaciones del supervisor del contrato, para proceder a la entrega oficial de dicho preliminar ante el auditado.

El 31 de julio de 2023, el auditado remite mediante correo electrónico las observaciones al informe preliminar enviado y se procede en consecuencia a analizar cada una de ellas, dando como resultado final el informe preliminar que se describe en el presente documento con los ajustes del caso.

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, versión 7 con vigencia desde abril de 2019, se cuenta con un DOFA construido desde el Sistema de Gestión de Calidad. El objetivo del proceso es Mantener y gestionar la plataforma tecnológica existente, implementar nuevas soluciones tecnológicas que provean en forma oportuna, eficiente y transparente la información necesaria para el cumplimiento de los fines misionales del COPNIA y formular lineamientos relacionados con estándares y buenas practicas para el manejo de la información.

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

Las necesidades y expectativa de las partes interesadas están definidas dentro de la CARACTERIZACIÓN DEL PROCESO TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES de código TIC-cp-01, versión 7 con vigencia desde abril de 2019, y en la DOFA año 2022 con factores internos y externos.

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

No aplica ya que la organización NO tiene un Sistema de Gestión de Seguridad de la Información consolidado y se encuentra en la etapa temprana de construcción, con apoyo y asesoría del Mintic.

Aunque dentro de la caracterización del proceso se ha definido el alcance como: "*Incluye la identificación de necesidades TIC, la administración de la plataforma tecnológica, la formulación e implementación de los proyectos, la evaluación y seguimiento de los mismos y la definición de controles que faciliten la confidencialidad, integridad y disponibilidad de la información*."

A la fecha de la presente auditoria, se evidencia que la entidad cuenta con Manual de seguridad de la información, Política de Gobierno Digital, Matriz de riesgos digitales, Política de Seguridad digital, Comité de seguridad de la información y Riesgos del proceso de TIC

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

Para la vigencia 2023, se tiene un Manual de Seguridad de la Información de código TIC-m-01, Vigente a partir de mayo de 2023 2ª Actualización, firmado por el Director General.

Durante la vigencia 2022, se evidencia el liderazgo de compromiso de la alta dirección, mediante la formulación de la política y la expedición de un MANUAL DE SEGURIDAD DE LA INFORMACIÓN, de código TIC-m_01 vigencia a partir de julio de 2019, 1 era. Actualización, firmado por la Directora Encargada. y el seguimiento periódico de la gestión del proceso TIC.

Igualmente se evidencia el apoyo de la alta dirección con el impulso mediante la creación de la oficina para la SIG que lidere la estructuración e implementación del Sistema de Seguridad de la Información.

5.2 POLÍTICA

Existe un PETIC - PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES 2023-2026, firmado por el director general y documentación de alineación estratégica con la organización. Este plan busca ser la guía tecnológica del desarrollo e innovación de la entidad, asegurando que tanto los funcionarios como los ciudadanos cuenten con una entidad sólida, eficaz, eficiente, segura y transparente en materia TIC, fortaleciendo así la gestión institucional y su alineación a las políticas nacionales e institucionales.

Se evidencia la resolución 2068 del 24 de diciembre de 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. La resolución 1027 del 05/07/2019 por medio de la cual se actualiza y modifica la Política de Seguridad y Privacidad de la Información del Consejo Profesional de Ingeniería - COPNIA

5.3 Roles, responsabilidades y autoridades de la organización.

Se creo la oficina de Seguridad de la Información, se evidencia el Manual de funciones y de competencias laborales que en el numeral 6.2 define la Oficina de Seguridad y Privacidad de la Información con la descripción de las funciones esenciales en su numeral IV

6 Planificación.

6.1 Acciones para abordar los riesgos y las oportunidades.

Se evidencia la matriz de riesgos en MAPA DE RIESGOS DE SEGURIDAD DIGITAL, versión 1 vigente a partir de diciembre de 2020 alineada a la metodología de Mintic 4+ con causa consecuencia, riesgo inherente, aunque define el Responsable del Riesgo no describe el Propietario del Riesgo y la aceptación del plan de tratamiento y de los riesgos residuales.

6.1.2 Evaluación de riesgo de la seguridad de la información

Se evidencia el Formato de Mapa de Riesgos del Proceso de Tecnologías de la Información y de las Comunicaciones con fecha de revisión de diciembre de 2022, versión 9 con 6 riesgos para el área, contiene Identificación del riesgo, análisis del riesgo Inherente, evaluación del riesgo – Valoración de los controles, nivel de riesgo residual y plan de acción, con sus respectivas firmas electrónicas del Profesional de Gestión TIC y el Director General.

6.1.3 Tratamiento de riesgo de la seguridad de la información

Se evidencia el Formato de Mapa de Riesgos del Proceso de Tecnologías de la Información y de las Comunicaciones con fecha de revisión de diciembre de 2022, versión 9 adaptado del curso de riesgo operativo Universidad del Rosario por la Dirección de Gestión de Desempeño Institucional de Función Pública, 2020 y ajustado en su versión 9 a la metodología definida en el Procedimiento Administración de Riesgos Versión 7.

6.2 Objetivos de seguridad de la información y planificación para lograrlos

Se evidencia alineación del PETIC con los objetivos específicos como:

- Alinear el plan estratégico de tecnologías de la información y las comunicaciones, al objetivo estratégico de "Consolidar el modelo de gestión de la entidad para mejorar la prestación de los servicios misionales"
- Innovar, mediante nuevas tecnologías estables, la parte operacional y misional del COPNIA.
- Garantizar la consolidación de las tecnologías de la información y comunicaciones garantizando la confiabilidad, utilidad y oportunidad de los datos de la entidad.
- Mejorar los servicios tecnológicos que tiene el COPNIA, garantizando la integridad, disponibilidad y seguridad de la información.
- Implementar estratégicamente soluciones tecnológicas que puedan beneficiar a la entidad.
- Establecer un portafolio de proyectos 2023 a 2026 que permita acciones articuladas para brindar un mejor servicio TI dirigido a la ciudadanía y a los funcionarios, para dar cumplimiento con las exigencias nacionales (Gobierno en línea - GEL), con los procesos misionales y las necesidades propias de la entidad.

7. APOYO

7.1 Recursos El Copnia es una entidad de origen público y manejan su propio presupuesto, se Evidencia el presupuesto anual para el año 2022 de: $22.989 millones.

7.2 Competencias En los procesos de Gestión Humana Manual de funciones versión 18/08/2021, se evidencia el Manual de funciones y de competencias laborales, que en su numeral 6.2 describe la Oficina de Seguridad y Privacidad de la Información con:

- Nivel: Profesional
- Denominación del empleo: Profesional de Gestión
- Código 2165
- Grado: 22
- Numero de cargos: 1
- Dependencia: Donde se ubique el cargo
- Empleo del Jefe Inmediato: Quien ejerza la supervisión directa
- Personal a cargo: sí.

El propósito principal es implementar las políticas institucionales, dirigir y ejecutar los planes, programas y proyectos encaminados al logro y cumplimiento del Sistema de Seguridad y privacidad de la Información, garantizando que los bienes y las tecnologías de la información están siendo adecuadamante protegidos.

7.3 Conocimiento Nivel alto de asistencia en las capacitaciones del Seguridad de la Información. Tienen ERP Seven y Cactus de Digital Ware, tiene con ETB un IAS, y los servidores de Azure. En el Gestor del Concomiento se Evidencia n temas de Seguridad de la Información.

7.4 Comunicación La organización cuenta con los medios adecuados para las comuniciones internas y externas, se evidencia 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 evidencia el listado maestro de documentos externos y el proceso Control de documentos DE-pr-01 Vigente a partir de nov de 2019.

8. OPERACIÓN

8.1 Planificación y control operacional. Los riegos evidenciados en el Mapa de Riesgos del Proceso de Tecnologías de la Información y de las Comunicaciones con fecha de revisión de diciembre de 2022, versión 9 con 6 riesgos para el área. Se evidencia 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 evidencia el Mapa de Riesgos del Proceso de Tecnologías de la Información y de las Comunicaciones con fecha de revisión de diciembre de 2022, versión 9.

8.3 Tratamiento de riesgo de la seguridad de la información. El análisis de riesgos contempla un plan de tratamiento del riesgo de la seguridad de la información y planes de acción.

9 Evaluación de desempeño

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN. Se evidencia ANÁLISIS INDICADOR PETIC con indicadores de: Medición sobre el portafolio de proyectos de TI, planteado en el ROADMAP del PETIC, Medición del proceso de tecnología, donde se evidencia la eficiencia y la eficacia del ciclo de vida del servicio.

9.2 Auditoría Interna: Se evidencia en el proceso "Auditorías 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 segunda auditoría realizada al SGSI (TIC´s) en el período 2021-2023.

9.3 Revisión por la dirección: El PETIC se somete a revisión y aprobación del Comité Institucional de Gestión y Desempeño en enero de 2023.

10. MEJORA

10.1 No conformidades y acciones correctivas. Se evidencian planes de Mejoramiento a partir de la auditoría interna del año 2021, con sus planes de acción, análisis de causa y seguimientos.

10.2 Mejora continua. Se evidencian planes de Mejoramiento del Sistema de Gestión Seguridad de la Información

5. HALLAZGOS

Es importante recalcar que la organización no tiene implementado un Sistema de Gestión Seguridad de la Información, cuya construcción se encuentra en etapa temprana con la asesoría y acompañamiento del Mintic, por lo tanto, existen ciertos numerales y/o controles que no se cumplen o no aplican de acuerdo con sus requerimientos.

Las normas ISO, orientadas a la seguridad de la información establecen un conjunto de buenas prácticas que ayudan a las organizaciones en la protección y gestión de sus sistemas de información frente a riesgos y amenazas, tanto intencionados como accidentales, por lo que para el presente ejercicio se aplicó un total de ciento cuarenta (140) criterios de auditoría entre las exigencias los numerales de la norma ISO 27001:2013 (26) y los 114 controles del Anexo A o ISO 27002:2013, de los cuales, nueve (09) son Observaciones, que le permitirán a la entidad identificar aquellos puntos en los que se requiere tomar acciones de mejora de carácter preventivo, en especial para reforzar los puntos de control sobre la seguridad de la información mientras se consolida el sistema que está en construcción, como se detalla a continuación:

5.1 REQUISITOS DE NUMERALES DE OBLIGATORIO CUMPLIMIENTO CON OBSERVACIONES

Criterios	**Observación**
6.1.3 Tratamiento de riesgo de la seguridad de la información	Frente al numeral 6.1.3 sobre el tratamiento del riesgo de la seguridad de la información, literales b y f, no se observa la aceptación del plan de tratamiento de los riesgos y de los riesgos residuales por parte de los propietarios de los riesgos. Tampoco define el propietario del riesgo y los controles del Anexo A usados, el auditado informa que este componente esta está en etapa de construcción con apoyo del MINTIC.
Descripción de Criterio	**Evidencia**
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	Se evidencia el Formato de Mapa de Riesgos del Proceso de Tecnologías de la Información y de las Comunicaciones con fecha de revisión de diciembre de 2022, versión 9 con 6 riesgos para el área, contiene Identificación del riesgo, análisis del riesgo Inherente, evaluación del riesgo – Valoración de los controles, nivel de riesgo residual y plan de acción, con sus respectivas firmas electrónicas del Profesional de Gestión TIC y el Director General. Dentro de la CARACTERIZACIÓN DEL PROCESO TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES de código TIC-CP-01, se cuenta con un DOFA manejado en calidad. Desde 1936 el COPNIA tiene registros de profesionales desde el mismo grado,

controles que son necesarios 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	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. En cuanto a los riesgos de seguridad de la información, no se evidencia la aceptación del plan de tratamiento de los riesgos residuales por parte de los propietarios de los riesgos. Tampoco define el propietario del riesgo y los controles, del Anexo A, conforme se puede evidenciar en las casillas vacías del mapa de riesgos publicado en página WEB (https://www.copnia.gov.co/sites/default/files/uploads/mapa-procesos/archivos/tecnologia/Riesgos_TIC.pdf) El auditado informa que que este componente de la norma se encuentra en etapa de estructuración y formulación según plan de trabajo concertado con el MINTIC, por lo que mientras se surte el proceso anunciado, se debe revisar esta situación para controlar de manera EFICAZ los riesgos de seguridad de la información.

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

Código	**Descripción de la observación**	
01-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, control A.15.1.3 Cadena de suministro de la tecnología de información y comunicación	No se cumplen los parámetros de seguridad en la cadena de suministro de la tecnología, en el sentido que se debe subir a una nube segura el On Premise, Firewall, Servidores que está alojados localmente y que pueden contener información sensible, o establecer los controles necesarios para que la información sensible de la organización no este expuesta a intrusiones. Lo que está pendiente es el Call Manager de Cisco, que se debe llevar a telefonía IP en la nube y los controles Biométricos.
	Descripción de Criterio	**Evidencia**
	Los acuerdos con los proveedores deberían incluir	Las prácticas de administración de riesgos de

	los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones. Se aconseja a las organizaciones a trabajar con los proveedores para comprender la cadena de suministro de la tecnología de información y comunicación y cualquier otro asunto que tenga un impacto importante en los productos y servicios que se proporcionan. Las organizaciones pueden influenciar las prácticas de seguridad de información de la cadena de suministro de la tecnología de información y comunicación aclarando en los acuerdos con sus proveedores los asuntos que deberían abordar proveedores en la cadena de suministro de tecnología de información y comunicación.	la cadena de suministro de la tecnología de información y comunicación específicas se desarrollan sobre la seguridad de la información general, la calidad, la administración de proyectos y las prácticas de ingeniería del sistema, pero no las reemplazan.
Código	**Descripción de la observación**	

Código	**Descripción de la Observación**	
02-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, control	No todos los funcionarios aplican el

	A.9.4.3 Sistema de gestión de contraseñas	requerimiento de claves seguras.
	Descripción de Criterio	**Evidencia**
	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	Se evidencia que, dentro de las políticas del directorio activo, se debe establecer que todos los usuarios cuenten con doble factor de autenticación, control de acceso con usuarios y contraseñas, incluir mayor tamaño de las claves y caracteres especiales. Las contraseñas deben ser de 8 caracteres alfanuméricos, con una vigencia de 40 días, no todos los usuarios tienen 2FA.

Código	**Descripción de la Observación**	
03-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, control A.9.2.5 Revisión de los derechos de acceso de usuario	No se evidencia que los propietarios de activos revisen los derechos de acceso de los usuarios de manera periódica.
	Descripción de Criterio	**Evidencia**
	Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica.	Se evidencia que en el Manual de Seguridad de la Información de código TIC-m-01, vigente a partir de mayo de 2023 2ª Actualización, numeral 5.1, define que los líderes funcionales son los encargados de revisar los usuarios.

Código	**Descripción de la Observación**

04-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, control A.9.2.3 Gestión de derechos de acceso privilegiados	El Manual de la Seguridad de la Información, de código TIC-m-01 no hace referencia a los usuarios privilegiados. Se evidencia que no se restringe y controla la asignación y uso de los derechos de acceso privilegiado de manera adecuada.
	Descripción de Criterio	**Evidencia**
	Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado	Usuarios Privilegiados: En One Drive se maneja una carpeta PASS con los usuarios privilegiados.

Código	**Descripción de la Observación**	
05-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, controles A.12.1.2 Gestión de cambios, A.14.2.2 Procedimientos de control de cambios del sistema y A.15.2.2 Gestión de cambios a los servicios del proveedor	Dentro de la información revisada No existe control de cambios
	Descripción de Criterio	**Evidencia**
	• Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de	No existe control de cambios

	información y los sistemas que afecten la seguridad de la información. • Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios. • Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos.	

Código	Descripción de la Observación

06-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, controles A.12.3.1 Respaldo de la información	No se hacen restauraciones aleatorias de las copias de seguridad.
	Descripción de Criterio	**Evidencia**
	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 observa la evidencia de la realización periódica de copias de seguridad, sin embargo, no ha restauraciones aleatorias.

Código	**Descripción de la Observación**	
07-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, control A.12.6.1 Gestión de las vulnerabilidades técnicas	No se evidencia una adecuada y oportuna gestión de las vulnerabilidades técnicas.
	Descripción de Criterio	**Evidencia**
	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	No se evidencia Escaneo de vulnerabilidad por un ente/profesional certificado, con alcance de los sistemas críticos de la Entidad. Se deberían tomar medidas adecuadas y oportunas en respuesta a la identificación de las posibles vulnerabilidades técnicas. Se deberían seguir los próximos puntos de orientación para establecer un proceso de administración eficaz para las vulnerabilidades técnicas

	riesgo asociado. a) la organización debería definir y establecer los roles y las responsabilidades asociadas a la administración de vulnerabilidades técnicas, incluido el monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidad, los parches, el seguimiento de activos y cualquier tipo de responsabilidades de coordinación necesarias; b) se deberían identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otras tecnologías (en base a la lista de inventario de activos, ver 8.1.1); estos recursos de información se deberían actualizar en base a los cambios en el inventario o cuando se encuentran nuevos recursos útiles; c) se debería definir una línea de tiempo para reaccionar frente a las notificaciones de vulnerabilidades técnicas	

	posiblemente relevantes; d) una vez que se ha identificado una vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las medidas que se deberían tomar, dichas medidas podrían involucrar la aplicación de parches a los sistemas vulnerables o la aplicación de otros controles; e) en función de la urgencia con la que se deba abordar una vulnerabilidad técnica, la medida tomada se debería realizar de acuerdo a los controles relacionados con la administración de cambios (ver 12.1.2) o siguiendo los procedimientos de respuesta ante incidentes de seguridad (ver 16.1.5); f) si existe un parche disponible de una fuente legítima, se deberían evaluar los riesgos asociados a la instalación del parche (los riesgos que impone la vulnerabilidad se deberían comparar con el riesgo de instalar el parche); g) los parches se pueden evaluar y probar antes	

	de su instalación para garantizar que son eficaces y no involucran efectos colaterales que no se pueden tolerar; si no existen parches disponibles se deberían considerar otros controles como: 1) desactivar todos los servicios o capacidades relacionadas a la vulnerabilidad; 2) adaptar o agregar controles de acceso, es decir, firewalls, en las fronteras de la red (ver 13.1); 3) mayor monitoreo para detectar ataques reales; 4) concientizar sobre la vulnerabilidad; h) se debería mantener un registro de auditoría para todos los procedimientos que se realizan; i) el proceso de vulnerabilidad técnica se debería monitorear y evaluar regularmente para poder garantizar su efectividad y eficiencia; j) se deberían abordar primero los sistemas en alto riesgo; k) se debería alinear un proceso de administración de vulnerabilidades técnicas	

	eficaz con actividades de administración de incidentes para comunicar los datos sobre vulnerabilidades con la función de respuesta ante incidentes y proporcionar los procedimientos técnicos en caso de que ocurra un incidente; l) definir un procedimiento para abordar la situación donde se ha identificado una vulnerabilidad, pero donde no existe una contramedida. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las medidas defectivas y correctivas adecuadas.	

Código	**Descripción de la Observación**	
08-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, control A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio	El Plan de Continuidad del negocio está en construcción a mediano plazo, lo que incide en un eventual incremento de la probabilidad de materialización de riesgos durante el periodo en que no se tenga plenamente desarrollado.
	Descripción de Criterio	**Evidencia**
	Los controles de Planificación de la continuidad de la seguridad de la información,	El tema del Plan de Continuidad del negocio está en construcción

	Implementación de la continuidad de la seguridad de la información, Verificación, revisión y evaluación de la continuidad de la seguridad de la información, así como las redundancias con Disponibilidad de las instalaciones de procesamiento de la información. Una organización debería determinar si la continuidad de la seguridad de la información se incluye dentro del proceso de administración de continuidad del negocio o dentro del proceso de administración de recuperación ante desastres. Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad comercial y la recuperación ante desastres. En la ausencia de una continuidad comercial formal y una planificación de recuperación ante desastres, la administración de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos ante situaciones adversas, en comparación	

	con las condiciones operacionales normales. De manera alternativa, una organización puede desarrollar un análisis de impacto comercial para los aspectos de seguridad de la información y determinar los requisitos de seguridad de la información que se aplican a situaciones adversas.	

Código	**Descripción de la Observación**	
09-0623	**Criterio**	**Observación**
	La norma ISO 27001:2013 en su anexo A, control A.18.1.3 Protección de los registros	Se observan casos de alteración de Registros en el aplicativo BPM.
	Descripción de Criterio	**Evidencia**
	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio	• Modificación de un dato de registro profesional señor GEAN CARLOS SALCEDO BENITEZ, con CC 1006558638, casos el ticket 4335. Anexo correo asunto *"Ticket pendiente de solución vencimiento".* • Registro de presuntos documentos en blanco en trámites de creación automática que forzaron el timer (estipulado a 10 días) para la creación automática para ajuste de requisitos, el cual se parametrizó en este tiempo para que de manera automática el sistema alerte a los 10 días hábiles el no cargue de documentos. Casos reportados o

		detectados en marzo y abril de 2023. • Bloqueo de 284 trámites por comunicados de solicitudes de certificación de egresados dirigido a las IES por más de un mes (abril mayo 2023) por BPM que bloquearon y/o retrasaron la gestión en las solicitudes de certificación, pues por falla en tag quedaron en la actividad *Generar radicados de salida*. De estos se produjeron 2 tutelas. • 130 resoluciones seccionales que después de firmadas por el Secretario y que debieron pasar de manera automática a la bandeja de la dirección general, no pasó, pues se devolvieron en el flujo a la segunda revisión lo que pudo incurrir en una doble firma de resoluciones, estos casos fueron retirados del flujo 1 semana por parte del proveedor. • Retiro de 214 resoluciones seccionales de Cundinamarca por fallas en los tag de los epígrafes que duraron 1 mes a la espera de solución. • Aprobación de una matrícula de Maestro de Obra caso 5393128 sin el cumplimiento de requisitos, faltaban 2.3 años por completar experiencia. • Modificación de un dato de registro profesional señor GEAN CARLOS SALCEDO BENÍTEZ, con CC 1006558638, casos el ticket 4335. Anexo correo asunto "*Ticket pendiente*

		de solución vencimiento". • Casos de profesionales de 3 de la Universidad el Bosque con otorgamiento de matrículas sin el cumplimiento de requisitos, la Universidad del Bosque cargó los listados en diciembre 2022. Los egresados iniciaron el trámite y se les concedió matrícula, luego la Universidad solicitó eliminar los 3 usuarios por no acreditar el total de materias, indicando que no se graduaron. Anexo radicado asunto "Egresado con anulación grado".

7. CONCLUSIONES Y RECOMENDACIONES

Como resultado del ejercicio auditor, se obtuvo un cumplimiento del 95% frente a los criterios de auditoría evaluados en los numerales y de los cuales los soportes se encuentran en la tabla denominada "Anexo 7.3 Análisis de criterios objeto de auditoría evaluación V4", se describen las conclusiones y recomendaciones.

1. Norma IEC/ISO 27001:2013

1. La organización ha implementado planes de acción a partir del ejercicio de Auditoría Interna anterior.
2. Es importante destacar el nombramiento del Oficial de Seguridad de la Información.
3. 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.
4. 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.
5. Teniendo en cuenta que la entidad no ha adoptado oficialmente la Norma Técnica ISO 27001: 2013 y su Anexo y según información aportada por el auditado, se

encuentra en proceso de diseño del sistema de Seguridad de la Información, esta auditoria insiste en la necesidad de que, si bien es cierto no se constituyen No Conformidades, si se hacen varias observaciones para que estas sean tenidas en cuenta en la formulación de los planes de mejoramiento de los procesos de TIC y en el Sistema de Seguridad de la Información.

8. SEGUIMIENTO A PLANES DE MEJORAMIENTO

Revisadas las evidencias, se observa que de la auditoría 09-21 realizada el año 2021 se generó una acción de mejoramiento por la NO conformidad reportada y que hacía referencia a que "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."
La acción de mejora fue definida por el auditado, como que "Se debe realizar la construcción del documento SOA, en donde se especifique: Identificar qué controles ha elegido una empresa para hacer frente a los riesgos que ha identificado, Explique por qué la organización ha seleccionado estos controles. Indique si la empresa ha implementado los controles Explicar por qué la organización ha decidido omitir ciertos controles. Enlace a la documentación relevante sobre la implementación de cada control que la empresa ha implementado; cada control debe tener su propia entrada. Adicional se debe coordinar con el área de planeación la aceptación del plan de tratamiento de riesgos por cada líder de proceso.

Igualmente, en dicho plan de mejora se identificó como causa raíz de la no conformidad, por parte del auditado La generación de documentación de apoyo a la aceptación de riesgos no estaba inmersa dentro de la construcción de las matrices de riesgo.

Durante la ejecución de la presente auditoria, se evidencio la existencia de un documento en borrador y no oficializado denominado **DOCUMENTO SOA (Statement off Applicability) COPNIA,** que fue entregado por el auditado como evidencia de avance la acción de mejora; sin embargo, cabe destacar que esta acción figura con plazo de vencimiento el 31 de diciembre de 2022 y en consecuencia en el seguimiento a junio de 2023 figura como incumplida y No eficaz.

9. ANEXOS NO CONFORMIDADES

Proyectado: Oscar Javier Zabala Merchán – Auditor Externo

Revisado por: Lina Luz Ramos Santos – Jefe Oficina de Control Interno (E).