	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

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

1. INFORMACIÓN GENERAL

Tipo de Informe	<input checked="" type="checkbox"/>	Auditoría	<input type="checkbox"/>	Seguimiento
Procesos auditados /Evaluado	Seguridad y Privacidad de la Información			
Auditor líder	Alberto Castiblanco Bedoya	Equipo Auditor	Raúl Alberto Ruiz García	
Responsable del proceso, dependencia, área o actividad auditada /evaluada	Rubén Darío Ochoa Arbeláez Iván Torres			

2. OBJETIVO

Evaluar la gestión del Proceso de Seguridad y Privacidad de la Información, conforme a los requisitos legales e institucionales tales como procedimientos, políticas, planes y demás lineamientos aplicables, así como la eficacia de las acciones de los planes de mejora y la de los controles frente a los riesgos.

3. ALCANCE

Verificar el nivel de cumplimiento de las actividades del Proceso de Seguridad y Privacidad de la información, en el marco de los procedimientos, instructivos, políticas, riesgos y planes estratégicos definidos, correspondiente al periodo comprendido entre Junio de 2023 a julio de 2024 e implica realizar una revisión de los sistemas, aplicaciones, gestiones, operaciones, el uso de datos y otros procesos relacionados con las tecnologías de la información en COPNIA, con el fin de verificar el acatamiento normativo, la efectividad de los controles definidos, identificar nuevos riesgos y formular recomendaciones para que el sistema logre las características de concordancia, integralidad e integridad y efectividad que promueven tanto las normas de calidad como las que regulan los sistema de información y tecnología del Estado Colombiano y el cumplimiento de las políticas definidas por el Copnia en su Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETIC.

4. ACTIVIDADES DESARROLLADAS

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

Dentro de la auditoría realizada al proceso de Tecnologías de la Información y las Comunicaciones se evaluaron criterios relacionados con la norma ISO 27001:2013 "Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", el Documento Maestro del Modelo de Seguridad de y Privacidad de la Información de MINTIC formalizado a través del Decreto 767 de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" y la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", el Decreto Único 1074 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo" y la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"

Las actividades efectuadas en el desarrollo de la auditoría y sus resultados correspondientes se presentan a continuación, divididas en la estructura de controles de la norma ISO 27001:

- **Control 5.1.1 Políticas para la seguridad de la información**

Se validan los documentos que sirven como evidencia:

Resolución 1027 2019 - Política de seguridad de la información.

Resolución 2068 de 2019 Política de seguridad digital.

Resolución 2069 de 2019 Política de gobierno digital.

Resolución 1197 de 2017 Política de Protección de Datos Personales.

SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN.

- **Control 5.1.2 Revisión de las políticas de seguridad de la información**

Se validan los siguientes documentos:

Resolución 1027 2019 - Política de seguridad de la información.

Resolución 2068 de 2019 Política de seguridad digital.

Resolución 1197 de 2017 Política de Protección de Datos Personales.

SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN.

Se recomienda en la próxima revisión realizar un actualización de la normatividad pues se encuentra alguna desactualizada.

- **Control A.6.1.1 Roles y responsabilidades de la seguridad de la información**

Se validan los documentos:

Resolución Nacional R2023053888 de 2023 - Actualiza el MIPG y reglamenta comités

Resolución Nacional R2024017396 de 2024 - Estructura orgánica COPNIA y funciones dependencias.

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

- **Control A.6.1.5 Seguridad de la información en la gestión de proyecto**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.12 implementación de proyectos tecnológicos donde se dictan los lineamientos necesarios para este control.

- **Control A.7.1.1 Selección**

Se validan los siguientes documentos:

GH-mf-01 MANUAL ESPECÍFICO DE FUNCIONES, REQUISITOS Y DE COMPETENCIAS LABORALES PARA LOS EMPLEOS DE LA PLANTA GLOBAL DE PERSONAL DEL COPNIA
GH-pr-01 SELECCIÓN Y VINCULACIÓN DE FUNCIONARIOS.

- **Control A.7.1.2 Términos y condiciones de la relación laboral**

Se validan los siguientes documentos:

GH-mf-01 MANUAL ESPECÍFICO DE FUNCIONES, REQUISITOS Y DE COMPETENCIAS LABORALES PARA LOS EMPLEOS DE LA PLANTA GLOBAL DE PERSONAL DEL COPNIA.

- **Control A.7.2.1 Responsabilidades de la dirección**

Se valida lo siguiente:

El personal contratista a través de contrato. Para el personal nombrado, esto se hace a través de acta de posesión.

- **Control A.7.2.2 Concientización, educación y formación en seguridad de la información**

Se valida lo siguiente:

Plan Institucional, programación de las sesiones. Listados de asistencia de las sesiones de capacitación y conscientización.

- **Control A.7.3.1 Responsabilidades en la desvinculación o cambio de empleo**

Se validan los siguientes documentos:

SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN. Dentro de estas actividades se realiza esto: 5.2.15 Backups o Copias de respaldo entrega de equipo y alistamiento de TI que hace parte del Novedad de retiro dentro del procedimiento TIC-PR-01 ATENCIÓN DE INCIDENCIAS Y REQUERIMIENTOS en el ANEXO 2 NOVEDADES DE PERSONAL COPNIA.

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

- **Control A.8.1.1 Inventario de activos**

Se revisan los siguientes documentos:

REGISTRO DE ACTIVOS DE INFORMACIÓN PÚBLICA Versión 5 fecha de aprobación Enero de 2024.

En el documento SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN aparece la sección 5.2 Gestión de Activos dentro de la cual se encuentran la identificación de activos, al parecer en el COPNIA no se gestiona el inventario de activos de información de forma integrada sino que cada área lo hace de forma independiente, por un lado la información y por la otra los activos de TI (hardware, software, servicios, instalaciones, Infraestructura crítica cibernética nacional), no se informa quien realice la revisión de recurso humano que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.

Esta falta de integración no permite una gestión adecuada de los activos de información alineada a los riesgos de la Entidad.

- **Control A.8.1.2 Propiedad de los activos**

Presenta la misma situación descrita en el control A.8.1.1, pendiente revisión con Oficina de Tecnología de la Información y de las Comunicaciones.

- **Control A.8.1.3 Uso aceptable de los activos**

Presenta la misma situación descrita en el control A.8.1.1, pendiente revisión con Oficina de Tecnología de la Información y de las Comunicaciones.


- **Control A.8.1.4 Devolución de activos**

Se validan los siguientes documentos:

Documento Manual de la Seguridad de la Información, de código SPI-M-01, vigente a partir de Julio de 2019, 1era. Actualización, indica en su numeral 5.2.5 Disposición de los activos.

- **Control A.8.2.1 Clasificación de la información**

Existe la política dentro de SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN, Se informa que dentro de los documentos REGISTRO DE ACTIVOS DE INFORMACIÓN PÚBLICA Versión 5 con fecha de aprobación Enero de 2024 y el ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA Versión 5 con fecha de aprobación Enero de 2024.

	INFORME DE AUDITORIA	Auditoría no.	35 -24	
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

- **Control A.8.2.2 Etiquetado de la información**

Existe la política dentro de SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN en la sección 5.2.2 Clasificación y etiquetado de activos de información, aunque se identifica el uso de metadatos en los sistemas de información, no se identifica que esta política cumpla con otras buenas prácticas de la implementación del control que incluyen entre otras y dependiendo del medio (físico o digital): etiquetas físicas o visibles, marcas de agua.

- **Control A.8.2.3 Manejo de activos**

Existe la política dentro de SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN en la sección 5.2 Gestión de Activos que incluye la identificación, clasificación, etiquetado, devolución, disposición de activos así como los lineamientos para el uso de dispositivos móviles y portátiles, internet, correo electrónico, comunicaciones de texto, voz y video, redes sociales, recursos tecnológicos, escritorio y pantalla despejada, gestión de hardware, gestión de software, implementación de BitLocker para la encriptación de equipos de cómputo para usuarios finales, backups o copias de respaldo, objetivos de Punto de Recuperación (RPO) y Objetivos de Tiempo de Recuperación (RTO) de 24 horas para los sistemas de información.

- **Control A.8.3.1 Gestión de los medios removibles**

Existe la política dentro de SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN en la sección 5.2.6 Dispositivos móviles y portátiles.

- **Control A.8.3.3 Transferencia física de medios**

Existe la política dentro de SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN que establece que se realiza cifrado para equipos de cómputo para colaboradores.

- **Control A.9.1.1 Política de control de acceso**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política sección 5.3.1 Control de accesos con usuarios y contraseñas, donde se dictan los lineamientos necesarios para este control. También se evidencia que esta alineado con el procedimiento TIC-pr-01 ATENCIÓN DE INCIDENCIAS Y REQUERIMIENTOS en su ANEXO 2 NOVEDADES DE PERSONAL COPNIA.

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

Se realizó la verificación de la implementación del control con el proceso de Tecnologías de la Información y las Comunicaciones.

- **Control A.9.1.2 Accesos a las redes y a los servicios de la red**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política secciones 5.3 Control de Acceso define los capítulos de 5.3.1 Control de accesos con usuarios y contraseñas, 5.3.2 Suministro del control de acceso, 5.3.3 Gestión de contraseñas y 5.3.4 Perímetro de seguridad, donde se dictan los lineamientos necesarios para este control.

- **Control A.9.2.1 Registro y cancelación de registro de usuario**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política secciones 5.3 Control de Acceso define los capítulos de 5.3.1 Control de accesos con usuarios y contraseñas, 5.3.2 Suministro del control de acceso, 5.3.3 Gestión de contraseñas y 5.3.4 Perímetro de seguridad, donde se dictan los lineamientos necesarios para este control.

- **Control A.9.2.2 Control Asignación de acceso de usuario**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política secciones 5.3 Control de Acceso define los capítulos de 5.3.1 Control de accesos con usuarios y contraseñas, 5.3.2 Suministro del control de acceso, 5.3.3 Gestión de contraseñas y 5.3.4 Perímetro de seguridad, donde se dictan los lineamientos necesarios para este control.

Se verifica si la política de acceso a usuario está implementada desde el proceso de TIC.
Se evidencia que los sistemas de información lo hacen a través de las política de directorio activo.

- **Control A.9.2.3 Gestión de derechos de acceso privilegiados**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.3.5 Política de Asignación y Uso de Derechos de Acceso Privilegiado. Se evidencia que está alineado con el procedimiento TIC-pr-01 ATENCIÓN DE INCIDENCIAS Y REQUERIMIENTOS y su ANEXO 2 NOVEDADES DE PERSONAL COPNIA

- **Control A.9.2.4 Gestión de información secreta de autenticación de usuarios**

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.3.5 Política de Asignación y Uso de Derechos de Acceso Privilegiado

Se evidencia que para la entrega de credenciales de autenticación se entregan a través de correo electrónico de contraseñas con obligatoriedad de cambio la primera vez de parte del usuario.

- **Control A.9.2.5 Revisión de los derechos de acceso de usuario**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.3.2 Política de Revisión y Mantenimiento de Matriz de Roles y Perfiles, los administradores de los sistemas de información generan una matriz con los derechos de acceso a los líderes funcionales de cada sistemas de información, quienes harán una revisión de los derechos de acceso actual. En caso tal que exista inconsistencia el líder pondrá un ticket para la actualización correspondiente.

- **Control A.9.2.6 Eliminación o ajuste de los derechos de acceso**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.3.2 Política de Revisión y Mantenimiento de Matriz de Roles y Perfiles, los administradores de los sistemas de información generan una matriz con los derechos de acceso a los líderes funcionales de cada sistemas de información, quienes harán una revisión de los derechos de acceso actual. En caso tal que exista inconsistencia el líder se genera un ticket para la actualización correspondiente.

- **Control A.9.3.1 Uso de información de autenticación secreta**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN la Política 5.3.7 Gestión de contraseñas. Se evidencia que está alineado con el procedimiento TIC-pr-01 ATENCIÓN DE INCIDENCIAS Y REQUERIMIENTOS y su ANEXO 2 NOVEDADES DE PERSONAL COPNIA en la sección PERFIL A ASIGNAR.

- **Control A.9.4.1 Restricción de acceso a la información**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN la Política 5.3.7 Gestión de contraseñas. Se evidencia que está alineado con el procedimiento TIC-pr-01 ATENCIÓN DE INCIDENCIAS Y REQUERIMIENTOS y su ANEXO 2 NOVEDADES DE PERSONAL COPNIA.

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

- **Control A.9.4.2 Procedimientos de inicio de sesión seguro**

Todos los sistemas de información están vinculados con directorio activo. Se tiene habilitado el doble factor de autenticación para los servicios de Office 365.

- **Control A.9.4.3 Sistema de gestión de contraseñas**

Se informa que todos los sistemas de información están vinculados con directorio activo y se tiene habilitado el doble factor de autenticación para los servicios de Office 365

- **Control A.9.4.4 Uso de programas utilitarios privilegiados**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN la Política 5.2.10 Recursos tecnológicos.

- **Control A.9.4.5 acceso al código fuente de los programas**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN la Política 5.2.10 Recursos tecnológicos, 5.2.6 Dispositivos móviles y portátiles.

- **Control A.10.1.1 Política sobre el uso de controles criptográficos**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.2.14 Política de Implementación de BitLocker para la Encriptación de Equipos de Cómputo para Usuarios Finales.

- **Control A.11.1.1 Perímetro de seguridad física**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.3.8 Perímetro de seguridad que incluye también la Política de acceso a las instalaciones o depósitos de archivo y En las instalaciones del centro de datos o de los centros de cableado no está permitido.

Se verifica si la política de Seguridad física y del ambiente se encuentra implementada dentro del proceso TIC, para lo cual se realiza lo siguiente: 1. Se solicita permiso de ingreso a través de correo electrónico para realizar el acompañamiento al menos 1 día antes, se programa el día de

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

la visita, se acompaña a la persona y se diligencia el formato de ingreso. Se evidencia el correo de solicitud.

- **Control A.11.1.2 Controles de acceso físico**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.3.8 Perímetro de seguridad que incluye también la Política de acceso a las instalaciones o depósitos de archivo y En las instalaciones del centro de datos o de los centros de cableado no está permitido.

- **Control A.11.1.3 Seguridad de oficinas, salas e instalaciones**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.3.8 Perímetro de seguridad que incluye también la Política de acceso a las instalaciones o depósitos de archivo y En las instalaciones del centro de datos o de los centros de cableado no está permitido.

- **Control A.11.1.5 Trabajo en áreas seguras**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.3.8 Perímetro de seguridad.


- **Control A.11.1.6 Áreas de entrega y carga**

Se informa que este control existe, pero se debe validar con el área administrativa.

- **Control A.11.2.1 Ubicación y protección del equipamiento**

Se informa que se cuenta con UPS para cada cuarto técnico, en el Plan Anual de Adquisiciones se validan los contratos de mantenimientos, se tiene acceso biométrico implementado, la sede principal cuenta con planta eléctrica de respaldo y hay servicio de mantenimiento de todos los equipos.

- **Control A.11.2.2 Elementos de soporte**

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

Se informa que se cuenta con UPS para cada cuarto técnico, en el Plan Anual de Adquisiciones se validan los contratos de mantenimientos, se tiene acceso biométrico implementado, la sede principal cuenta con planta eléctrica de respaldo y hay servicio de mantenimiento de todos los equipos.

- **Control A.11.2.3 Seguridad en el cableado**

Se informa de parte del Profesional de Gestión Oficina de Seguridad y Privacidad de la Información que esta verificación se puede hacer directamente en los centros de cableado.

- **Control A.11.2.6 Seguridad del equipamiento y los activos fuera de las instalaciones**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.2.6 Dispositivos móviles y portátiles

- **Control A.11.2.7 Seguridad en la reutilización o descarte de equipos**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.2.10 Recursos tecnológicos.

- **Control A.11.2.8 Equipo de usuario desatendido**


Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.2.6 Dispositivos móviles y portátiles y 5.2.11 Escritorio y pantalla despejada.

Se verifica si la política se encuentra implementada dentro del proceso TIC, los equipos están configurados para bloqueo de pantalla los cinco (5) minutos.

- **Control A.11.2.9 Política de escritorio y pantalla limpios**

Se evidencia dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN: 5.2.11 Escritorio y pantalla despejada.

- **Control A.12.1.3 Gestión de la capacidad**

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

Se verifica si esta política esta implementada. Se informa que el análisis se realiza a través de los estudios previos y las fichas técnicas de los contratos, así como con los informes de supervisión mensual.

Se evidencia que no existe un análisis permanente a través de un plan de capacidad y disponibilidad que permita realizar una planeación de la capacidad de los sistemas de información e infraestructura a los largo del ciclo de vida. Esto se hace de manera contractual sin procedimientos técnicos definidos por el proceso.

- **Control A.13.2.1 Políticas y procedimientos de transferencia de información**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.4.4 Intercambio electrónico de información para soportar este control. Adicionalmente existe un proyecto con Agencia Nacional Digital para intercambio de información con MINITC y el Portal Gov.co utilizando la plataforma de intercambio de información XROAD que provee una capa de seguridad.

- **Control A.13.2.2 Acuerdos sobre transferencia de información**


Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.4.4 Intercambio electrónico de información para soportar este control. Adicionalmente existe un proyecto con Agencia Nacional Digital para intercambio de información con MINITC y el Portal Gov.co utilizando la plataforma de intercambio de información XROAD que provee una capa de seguridad, para esto se firmó un soporte de acta donde se determinaron los compromisos de cada Entidad en el intercambio de información.

- **Control A.13.2.3 Mensajería electrónica**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existen las políticas 5.2.8 Correo electrónico, comunicaciones de texto, voz y video; 5.2.9 Redes Sociales.

- **Control A.13.2.4 Acuerdos de confidencialidad o no divulgación**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existen la Política 5.6 Privacidad y Confidencialidad, adicionalmente existen contratos con cláusulas de

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

seguridad y privacidad de la información y se cuenta con el SPI-m-02 MANUAL PARA LA PROTECCIÓN DE DATOS PERSONALES.

- **Control A.14.1.1 Análisis y especificación de requisitos de seguridad de la información**

Se evidencia que dentro del Anexo Técnico "Anexo1. Fichas de especificaciones técnicas mínimas" aparecen los requisitos de seguridad para proyectos tecnológicos.

Nota: En este control revisar la Declaración de Aplicabilidad en el campo análisis pues se presta a confusión y no aclara bajo que alcance si es aplicable el control, es necesario revisar este mismo contexto los controles A.14.1.1, A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.8, A.14.2.9, A.14.3.1

- **Control A.14.2.2 Procedimientos de control de cambios del sistema**

Se verifica si los soportes de control de cambios existen en el proceso. Se informa que a través de los tickets de la mesa de ayuda se validan estos cambios, al líder área funcional y líder del proceso de seguridad y privacidad de la información.

Se evidencia existe soporte de la actividad.

- **Control A.15.1.1 Políticas de seguridad de la información para proveedores**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN cuenta con las políticas 5.3.5 Política de Asignación y Uso de Derechos de Acceso Privilegiado y 5.3.6 Contraseñas de plataformas tecnológicas administradas por terceros.

- **Control A.15.1.2 Gestión de los servicios prestados por proveedores**

Se encuentra que en el SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN se cuenta con las políticas 5.3.5 Política de Asignación y Uso de Derechos de Acceso Privilegiado y 5.3.6 Contraseñas de plataformas tecnológicas administradas por terceros.

- **Control A.15.1.3 Cadena de suministro de TIC**

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.2.8 Correo electrónico, comunicaciones de texto, voz y video; 5.4.4 Intercambio electrónico de información que soportan este control.

Adicionalmente Se realiza soporte y monitoreo a los sistemas de información, se realiza la documentación de los sistemas de información, se implementa en el proyecto de carpeta ciudadana se utiliza XROAD para incrementar la seguridad de la información.

- **Control A.15.2.1 Seguimiento y revisión de los servicios prestados por proveedores**

Se evidencia que dentro de las actividades administrativas del COPNIA se establecen controles a través del CT-pr-08 PROCEDIMIENTO DE SUPERVISIÓN DE CONTRATO.

- **Control A.15.2.2 Gestión de los cambios en los servicios de proveedores**

Se evidencia que dentro de las actividades administrativas del COPNIA se establecen controles a través del TIC-pr-02 PROCEDIMIENTO CONTROL DE CAMBIOS.

- **Control A.16.1.1 Responsabilidades y procedimientos**

Para implementar este control se cuenta con lo siguiente:

- PROCEDIMIENTO TIC-pr-01 ATENCIÓN DE INCIDENCIAS Y REQUERIMIENTOS dentro del cual se atienden los incidentes de Tecnología, aunque este no estipula específicamente el tipo de incidente "seguridad de la información" este si se valida dentro del sistema de información.
- El proceso de Seguridad y Privacidad de la Información cuenta con el indicador 38 "Tratamiento de eventos relacionados en el marco de seguridad y privacidad de la información, del cual se evidencia medición para los dos primeros trimestres de 2024.
- En cuanto a uso y apropiación se evidencia las presentaciones de las charlas de seguridad de la información que hacen parte del Plan Institucional de Capacitación donde se realizan las capacitaciones pertinentes a reporte de información.
- Se evidencia que dentro de las actividades administrativas del COPNIA se establecen controles a través del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política donde existe la Política Gestión de Incidentes de Seguridad de la Información.
- Para el reporte ante el CSIRT se envía un formato por correo a CSIRT, desde 2022 no ha habido eventos que reportar. Se recomienda que este formato y los contactos del CSIRT (teléfonos de contacto, correo electrónico y formato) estén disponibles permanentemente no solo para el Oficial de Seguridad de la Información sino también para una copia de seguridad en caso de ausencia del primero.

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

- **Control A.16.1.2 Informe de eventos de seguridad de la información**

Para implementar este control se cuenta con lo siguiente:

El proceso de Seguridad y Privacidad de la Información cuenta con el indicador 38 "Tratamiento de eventos relacionados en el marco de seguridad y privacidad de la información, del cual se evidencia medición para los dos primeros trimestres de 2024 y la herramienta de gestión de tickets de mesa de ayuda. A partir de ello se realizan informes relacionados de seguridad y privacidad de la información donde se realizan los análisis, para este caso se evidencia el documento "Informe de proyecto de monitoreo de amenazas de COPNIA".

- **Control A.16.1.3 Informe de las debilidades de seguridad de la información**

El proceso de Seguridad y Privacidad de la Información cuenta con el indicador 38 "Tratamiento de eventos relacionados en el marco de seguridad y privacidad de la información, del cual se evidencia medición para los dos primeros trimestres de 2024 y la herramienta de gestión de tickets de mesa de ayuda. A partir de ello se realizan informe relacionados de seguridad y privacidad de la información donde se realizan los análisis, para este caso se evidencia el documento "Informe de proyecto de monitoreo de amenazas de COPNIA".

- **Control A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información**

Para implementar este control se cuenta con el PROCEDIMIENTO TIC-pr-01 ATENCIÓN DE INCIDENCIAS Y REQUERIMIENTOS donde se toman decisiones para la solución a través del escalamiento requerido por cada incidente.

- **Control A.16.1.5 Respuesta ante incidentes de seguridad de la información**

Se evidencia que el proceso de Seguridad y Privacidad de la Información cuenta con el indicador 38 "Tratamiento de eventos relacionados en el marco de seguridad y privacidad de la información, del cual se evidencia medición para los dos primeros trimestres de 2024 y la herramienta de gestión de tickets de mesa de ayuda.

Se evidencia a que en el SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política donde existe la Política 5.10 Gestión de Incidentes de Seguridad de la Información

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

También que en la "RESOLUCIÓN NACIONAL R2023053888 de 2023 - Actualiza el MIPG y reglamentan comités en el ARTÍCULO DÉCIMO SEXTO. Créase el Subcomité de Seguridad de la Información del Consejo Profesional Nacional de Ingeniería"

- **Control A.16.1.6 Aprendizaje de los incidentes de seguridad de la información**

El proceso de Seguridad y Privacidad de la Información cuenta con el indicador 38 "Tratamiento de eventos relacionados en el marco de seguridad y privacidad de la información, del cual se evidencia medición para los dos primeros trimestres de 2024 y la herramienta de gestión de tickets de mesa de ayuda. A partir de ello se realizan informe relacionados de seguridad y privacidad de la información donde se realizan los análisis, para este caso se evidencia el documento "Informe de proyecto de monitoreo de amenazas de COPNIA".

- **Control A.16.1.7 Recolección de evidencia**

Se informa que no existe como tal un procedimiento de recolección de evidencia, de los incidentes de seguridad y privacidad de la información adicional, en este se almacena la información enviada por el usuario que pone el ticket en el sistema de información de gestión de tickets, la evidencia se recolecta solo en los casos en que se reporte a CSIRT pues es obligación en este caso.

- **Control A.17.2.1 Disponibilidad de las instalaciones de procesamiento de la información**


Los sistemas de información se encuentran en la plataforma Azure que garantiza la redundancia y existe procedimientos de backup y pruebas de restauración dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN en la Política 5.2.15 Backups o Copias de respaldo y el ANEXO 2-PROGRAMACION DE REVISION DE BACKUPS

- **Control A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales**

Se evidencia el documento Normograma SPI de septiembre de 2024.

Se recomienda realizar actualización periódica de la normatividad de tal forma que el cumplimiento de las leyes, decretos, resoluciones, etc. Se realizan de manera más efectiva

- **Control A.18.1.2 Propiedad intelectual**

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

Se evidencia en el SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN la Política 5.2.1 Identificación de activos en el subtítulo Propiedad intelectual.

Las licencias de uso de cada sistema de información se encuentran en las áreas de Tecnología y Administrativa.

- **Control A.18.1.3 Protección de los registros**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.4 No repudio, 5.4.1 Trazabilidad, 5.4.2 Retención, 5.4.3 Auditoría" donde se dictan los lineamientos para este control.

- **Control A.18.1.4 Privacidad y protección de los datos personales**

Se evidencia el documento SPI-m-02 MANUAL PARA LA PROTECCIÓN DE DATOS PERSONALES que establece los procedimientos internos que adopta el COPNIA para la implementación de la Política de Protección y Tratamiento de Datos Personales en concordancia con las disposiciones legales vigentes.

- **Control A.18.1.5 Regulación de los controles criptográficos**

Se evidencia que dentro del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN existe la Política 5.2.14 Política de Implementación de BitLocker para la Encriptación de Equipos de Cómputo para Usuarios Finales.

- **Control A.18.2.1 Revisión independiente de la seguridad de la información**

La revisión a través de auditoría interna ha sido incorporada dentro del plan Anual de Auditorías del COPNIA.

No se identifican revisiones independientes a través de auditorías externas

- **Control A.18.2.2 Cumplimiento con las políticas y normas de seguridad**

	INFORME DE AUDITORIA	Auditoría no.	35 -24	
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

Se informa que este es un proceso que tiene algo más de un año de formalizado por lo que en el momento no existen procedimientos de seguridad de la información, las actividades se monitorean a través del indicador 37 Disponibilidad de los servicios de gobierno en línea que presta la entidad (por ataques informáticos a la entidad), el indicador 38 Tratamiento de eventos relacionados en el marco de seguridad y privacidad de la información y el reporte de Cumplimiento a la declaración de aplicabilidad (DDA) para seguridad de la información.

- **Control A.18.2.3 Verificación del cumplimiento técnico**

Se verifica si los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización.

No se presenta evidencia del soporte de la revisión de los permisos para los sistemas de información, pues se informa que hasta agosto salió la política.

- **Lineamiento Decreto Único 1074 de 2015 capítulo 26, Ley 1581 de 2012 art. 25 Registro Nacional de Bases de Datos**

Se valida si se ha realizado el Registro Nacional de Bases de Datos, para los sistemas de información BPM (BPM COPNIA) y Gestor documental.

Se evidencia a través de consulta del Registro Nacional de Bases de Dato RNBD de la Superintendencia de Industria y Comercio que las Bases de Datos inscritas por la Entidad son: COPNIA, SEVEN, KACTUS e INVESDOC, la finalidad registrada es la siguiente:

- COPNIA: la Base de datos en la que se registran datos relacionados a la asignación de la matrícula profesional del COPNIA (datos sensibles)
- SEVEN: Base de datos ERP procesos administrativos y financieros
- KACTUS: Base de datos de funcionarios COPNIA (Planta de Personal)
- INVESDOC: Es la Base de datos de los egresados reportados por las Instituciones de Educación Superior, (es una sola base de datos para controlar, revisar, evidenciar comprobar y garantizar lo establecido en la Ley 842 para el procedimiento de Matrículas. Garantizando la idoneidad que exige a un profesional de la Ingeniería, sus Profesiones Afines, Auxiliares y Maestros de Obra, La Constitución Nacional en su Artículo 26, con el fin único de Conjurar el riesgo que implica un eventual antiética o incorrecta practica de su ejercicio. Lo dice Además de la Ley y la pluralidad abundante de sentencia de la Honorable Corte Constitucional (C 606 de 1992 C-177 de 1993 C-226 de 1994 C-570 de 2004 entre otras), procesos disciplinarios, permisos temporales y PQR.

No se evidencia la inscripción de la base de datos de Gestor documental en el Registro Nacional de Bases de Datos.

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

5. HALLAZGOS

Para el desarrollo de la auditoria se aplicó un total de setenta y seis (77) criterios, de los cuales, (4) son no conformidad y (2) son conformidad con observación; dando como resultado del ejercicio auditor un cumplimiento del 94.8% frente a los criterios de auditoría evaluados.

5.1. REQUISITOS CON CUMPLIMIENTO – CONFORMIDADES CON OBSERVACION

Criterio	Evidencia
ISO 27001:2013 Control 5.1.2 Revisión de las políticas para seguridad de la información. Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	Se evidencia que en la Resolución 2068 de 2019 'Política de Gestión y Desempeño de seguridad Digital para el Copnia' se hace referencia al Decreto 1008 de 2015, norma actualizada por el Decreto 767 de 2022, y no se evidencia referencia a la Resolución 500 de 2021 'Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital', adicionalmente no se identifica dentro del texto de la Resolución 2068 de 2019 la periodicidad de revisión a intervalos planificados. Esto ocasiona debilidades en el cumplimiento del control 5.1.2.
MSPI sección 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información. Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión.	Se evidencia que en la Declaración de Aplicabilidad, los controles A.14.1.1, A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.8, A.14.2.9 presentan inconsistencias en cuanto al alcance y aplicabilidad de los controles de seguridad de la información agregando una doble fila para la columna APLICABLE PARA LA ENTIDAD donde se identifica contradicción en la respuesta (Si y NO en dos columnas diferentes), lo que puede generar interpretaciones erróneas sobre la aplicabilidad de ciertos controles y debilidades en el seguimiento y control.

5.2. REQUISITO DE NO CUMPLIMIENTO – NO CONFORMIDADES

Código NC	Descripción de la No conformidad	
	Criterio	No Conformidad
1-3524	Norma ISO 27001: 2013 controles A.8.1.1 y A.8.1.2, Modelo de seguridad de la información	Incumplimiento de los controles A.8.1.1 y A.8.1.2 del Norma ISO

		27001: 2013
	Descripción del criterio	Evidencia
	<p>A.8.1.1 Inventario de activos. Control: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.</p> <p>A.8.1.2 Propiedad de los activos Control: Los activos mantenidos en el inventario deben tener un propietario.</p>	<p>Se evidencia una ausencia de clasificación unificada de activos de información relacionados con seguridad y privacidad de la información que integre todos los tipos de activos: información, infraestructura, recursos humanos críticos, junto con la falta de responsables claros para su revisión, y que identifique la propiedad de estos ocasionada por una fragmentación en el proceso de gestión de activos, una ausencia de requisitos claros para los activos de información tipo hardware, software, servicios, recurso humano e instalaciones, lo que puede derivar en riesgos de seguridad y operación, así como una deficiente gestión del riesgo.</p>
	Criterio	No Conformidad
	Norma ISO 27001: 2013 control A.8.2.2	Incumplimiento del control A8.2.2 de la norma ISO 27001:2013
	Descripción del criterio	Evidencia
2-3524	Etiquetado de la información. Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	<p>No se evidencia de parte del proceso la implementación del etiquetado de la información, al no contar con etiquetas o marcas de agua en documentos físicos o etiquetas digitales, lo que ocasiona debilidades en el cumplimiento del control A.8.2.2. La ausencia de un esquema formal de etiquetado es causada por la omisión de estos elementos en las políticas actuales, lo que puede generar confusión en la clasificación de la información y un riesgo de exposición no controlada.</p>
	Criterio	No Conformidad
3-3524	Modelo de Seguridad y Privacidad de la Información, Resolución 500 de 2021 y controles A.8.3.1, A.8.3.2, A.9.4.2, A.11.1.5, A.12.1.1, A.12.5.1, A.13.2.1, A.15.2.2,	Incumplimiento de los requisitos del Modelo de Seguridad y Privacidad de la Información, la Resolución 500 de

<p>A.16.1.1, A.16.1.5, A.16.1.7, A.17.1.2, A.18.1.2, A.18.2.1, A.18.2.2 (ISO 27001)</p>	<p>2021 y los controles A.8.3.1, A.8.3.2, A.9.4.2, A.11.1.5, A.12.1.1, A.12.5.1, A.13.2.1, A.15.2.2, A.16.1.1, A.16.1.5, A.16.1.7, A.17.1.2, A.18.1.2, A.18.2.1, A.18.2.2 (ISO 27001)</p>
<p>Descripción del criterio</p>	<p>Evidencia</p>
<p>Modelo de Seguridad y Privacidad de la Información 04. Propósitos: Establecer procedimientos de seguridad que permita a las entidades apropiar el habilitador de seguridad en la política de Gobierno Digital. Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de las entidades.</p> <p>Para el desarrollo de esta fase se deben utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI. Los documentos que se deben generar en esta fase son: Procedimiento de inventario y Clasificación de la Información e infraestructura crítica Procedimiento de gestión de riesgos de seguridad de la información</p> <p>Resolución 500 de 2021</p> <p>ARTÍCULO 1o. OBJETO. La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.</p> <p>ARTÍCULO 3o. LINEAMIENTOS GENERALES. Los sujetos obligados deben adoptar medidas</p>	<p>La ausencia de procedimientos documentados y formalizados en el proceso de Seguridad y Privacidad de la información debilita el cumplimiento de los requisitos del Modelo de Seguridad y Privacidad de la Información, la Resolución 500 de 2021 y los controles de la norma ISO 27001:2013.</p>

técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.

ISO 27001:2013

A.8.2.3 Manejo de activos Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización

A.8.3.1 Gestión de medios removibles Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.

A.8.3.2 Disposición de los medios Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.

A.9.4.2 Procedimiento de ingreso seguro Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.

A.11.1.5 Trabajo en áreas seguras Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras

A.12.1.1 Procedimientos de operación documentados Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.

A.12.5.1 Instalación de software en sistemas operativos Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos

A.13.2.1 Políticas y procedimientos de

transferencia de información Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.

A.15.2.2 Gestión de cambios en los servicios de proveedores Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.

A.16.1.1 Responsabilidad y procedimientos Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.


A.16.1.5 Respuesta a incidentes de seguridad de la información Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

A.16.1.7 Recolección de evidencia Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.


A.17.1.2 Implementación de la continuidad de la seguridad de la información Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

A.18.1.2 Derechos de propiedad intelectual Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

A.18.2.1 Revisión independiente de la seguridad

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

	<p>de la información Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.</p> <p>A.18.2.2 Cumplimiento con las políticas y normas de seguridad Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.</p>	
4-3524	Criterio	No Conformidad
	Decreto Único 1074 de 2015 Artículo 2.2.2.26.1.3, Ley 1581 de 2012 Artículo 25	Incumplimiento del Decreto Único 1074 de 2015 Artículo 2.2.2.26.1.3, Ley 1581 de 2012 Artículo 25
	Descripción del criterio	Evidencia
	<p>Decreto Único 1074 de 2015 Artículo 2.2.2.26.1.3. Deber de inscribir las bases de datos. El Responsable del Tratamiento debe inscribir en el Registro Nacional de Bases de Datos, de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a Tratamiento.</p> <p>Ley 1581 de 2012 Artículo 25. Definición. Reglamentado por el Decreto Nacional 886 de 2014 El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos. Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán</p>	<p>No se evidencia la inscripción de la base de datos de Gestor Documental en el Registro Nacional de Bases de Datos, lo cual incumple con la normatividad.</p>

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

	ser inferiores a los deberes contenidos en la presente ley. Parágrafo. El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.	
--	---	--

6. EVALUACIÓN DEL RIESGO DEL PROCESO


De acuerdo con el MAPA DE RIESGOS DE SEGURIDAD DIGITAL versión 2 de febrero de 2024 del proceso, se establecen 7 riesgos a saber:

- PÉRDIDA DE CONFIDENCIALIDAD para el tipo de activo servicios
- PÉRDIDA DE CONFIDENCIALIDAD para el tipo de activo componentes de red
- PÉRDIDA DE CONFIDENCIALIDAD para el tipo de activo hardware
- PÉRDIDA DE integridad para el tipo de activo servicios
- PÉRDIDA DE integridad para el tipo de activo componentes de red
- PÉRDIDA DE DISPONIBILIDAD para el tipo de activo servicios
- PÉRDIDA DE DISPONIBILIDAD para el tipo de activo componentes de red

Riesgo Identificado/posible riesgo	Observación
Pérdida de integridad Tipo de activo servicios: Activo: bpm; micrositio; gestor documental; pqrs; office 365; página web; catedra de ética; seven; kactus; plataforma de pagos; invsedoc	Control asociado: Generación de plan de backup y contratos de mantenimiento y soporte sobre las plataformas tecnológicas Cláusula de confidencialidad de la información, funciones del personal, restricción de acceso a terceros según manual de seguridad Observación: Se evidencia la falta de oportunidad en la vigencia del contrato de mantenimiento para el sistema de información BPM. Esto incrementa el riesgo de interrupciones en la disponibilidad del sistema de información. así como en las actividades misionales de la Entidad.

7. CONCLUSIONES Y RECOMENDACIONES

Se evidencia que el proceso, a poco tiempo de crearse, logra un cumplimiento de los criterios de evaluación de esta auditoría de 94.8, cifra significativa para el poco tiempo de creado y con una sola persona trabajando en el proceso.

	INFORME DE AUDITORIA	Auditoría no.		35 -24
		Fecha del informe		
		Día	Mes	Año
		11	15	2024

La implementación de un Sistema de Gestión de Seguridad de la Información debe lograr comprometer a toda la Entidad en el cumplimiento de las Políticas de seguridad de la Entidad y permitir alinear los diversos procesos y normatividad aplicable al Copnia.

Luego la realización del proceso auditor es importante tener presente las siguientes recomendaciones:

- Desarrollar el inventario de activos de información de acuerdo con las buenas prácticas establecidas.
- Realizar seguimiento a la implementación del SPI-M-01 MANUAL DE SEGURIDAD DE LA INFORMACIÓN de parte de los responsables.
- Se recomienda establecer un proceso claro de etiquetado para mejorar el control de los activos de información.
- Se sugiere planear e implementar un calendario de revisiones semestrales de la normatividad y buenas prácticas para garantizar el cumplimiento continuo.
- Se recomienda revisar y clarificar el documento Declaración de Aplicabilidad para evitar confusión y garantizar que se cumplan adecuadamente los requisitos de seguridad.
- Se recomienda establecer procedimientos claros para planear, ejecutar y monitorear el cumplimiento en todas las áreas relevantes.
- Finalmente, considerar la adopción de la norma ISO 27001:2022 para alinearse con la actualización de buenas prácticas.
- Realizar la inscripción de la base de datos de Gestor Documental en el RNBD para asegurar el cumplimiento de la normatividad.

8. SEGUIMIENTO A PLANES DE MEJORAMIENTO

A la fecha de esta auditoría no se tiene un Plan de Mejoramiento asignado al proceso de Seguridad y Privacidad de la información.

9. ANEXOS NO CONFORMIDADES

Elaborado por: Raúl Alberto Ruiz García – Contratista Oficina de Control Interno

Revisado por: Alberto Castiblanco Bedoya – Jefe Oficina de Control Interno