Gobernación de Cundinamarca	**CULTURA ORGANIZACIONAL Y MEJORA CONTINUA**	**Código: E-COMC-FR-083**
		Versión: 05
	INFORME DE AUDITORIAS INTERNAS	**Fecha aprobación: 05/09/2025**

Proceso Auditado: Gestión de Seguridad de la Información, gestión de ingresos, Gestión de la Tecnología, contractual y de compra pública, Administrativa y de Recursos, Gestión estratégica del talento humano, Gestión Financiera, Gestión Documental.	Fecha			Total, de Solicitudes de Acción Correctiva o Preventiva: **N.A**
	AÑO	**MES**	**DÍA**	
	2026	08 09	31 2,3,4	

EQUIPO AUDITOR	Rodrigo Gutierrez Arias-Auditor Líder Martha Zornosa-Auditor
LÍDER DE PROCESO	Ricardo Hernández-Oficial de Seguridad de la Información

NORMAS AUDITADAS: ISO 9001 ☐ ISO 45001 ☐ DECRETO 1072 ☐ ISO/IEC 27001 ■

OBJETIVO DE LA AUDITORÍA

Determinar el grado de madurez que tiene el Sistema de Gestión de Seguridad de la Información de la Entidad en términos de mantenimiento y mejora.

ALCANCE DE LA AUDITORÍA:

El ejercicio de auditoría aplica para el alcance implementado: *"Seguridad de la información para la prestación de servicios del proceso de gestión de ingresos en la Dirección de Rentas y Gestión Tributaria en el recaudo de tributos y rentas monopólicas en favor del departamento de Cundinamarca".*

El ejercicio de auditoría fue verificado en los procesos de: *Gestión de Seguridad de la Información, gestión de ingresos, Gestión de la Tecnología, contractual y de compra pública, Administrativa y de Recursos, Gestión estratégica del talento humano, Gestión Financiera, Gestión Documental.*

Es importante indicar que el ejercicio de auditoría se realizó en dos fases. La primera fase se realizó mediante una verificación documental de algunos documentos. Entre estos documentos, se tomó la Declaración de Aplicabilidad para determinar el aseguramiento de la justificación y determinación de implementación de controles establecidos en el Anexo A. En la segunda fase (In Situ) se hizo verificación de los numerales de la Norma en los procesos auditados. Para los controles establecidos en la Declaración de Aplicabilidad se tomó una muestra para determinar el cumplimiento. En las listas de chequeo de auditoría se podrán observar las evidencias de verificación a numerales y controles determinados.

REQUISITOS APLICABLES AL PROCESO (NORMAS ISO 9001,ISO 45001, DECRETO 1072, ETC)

Numerales asociados a la Norma ISO/IEC 27001:2022 y al Anexo A de esta Norma

IMPORTANCIA DEL PROCESO

FORTALEZAS DEL PROCESO AUDITADO

- Las lecciones aprendidas asociadas a la gestión de incidentes determinan de forma clara la toma de acciones para sensibilizar a los funcionarios de la Entidad.
- El control de evidencias asociado a la gestión de incidentes permite hacer trazabilidad puntual y concreta a los eventos presentados.
- La gestión de amenazas es una fuente importante de información para blindar a la Organización ante amenazas y vulnerabilidades.
- Las actividades de etiquetado permiten asegurar un control apropiado de los documentos en términos de la triada de seguridad de la información
- Sus diferentes estrategias de comunicación, socialización y certificación han permitido que el SGSI sea asimilado e interiorizado por los usuarios internos y externos.
- Se encuentran certificados desde el año 2023 con la versión NTC/ISO 27001:2022; siendo tan reciente su actualización, fueron los primeros de las entidades públicas en certificarse, lo que les ha permitido ir adquiriendo un mayor nivel de madurez en el sistema.
- Se resalta el manejo de activos de información en su relación con el manejo de riesgos de acuerdo a su valoración.
- El monitoreo de plataformas es robusto y completo. Se cuenta con reportes, análisis, contingencia y continuidad de la operación por medio del contrato con el proveedor UT IDEAS 3 2026. La adecuada gestión del área técnica de la Secretaría de Transformación Digital en la dirección de infraestructura permite llevar control adecuado de actividades.
- Los avances en la integración documental entre los diferentes Procesos, mediante las actividades de implementación del etiquetado en las herramientas Condor e Isolución, han permitido aplicar transversalmente los procedimientos de gestión documental.

DEBILIDADES DEL PROCESO AUDITADO / OPORTUNIDADES DE MEJORAMIENTO

Observaciones

- Asegurar que las salidas que se generen en las caracterizaciones se establezcan como entradas en los procesos del sistema. Al colocar "Todos los procesos" como salida en el ítem "parte interesada", determina la necesidad de incluirlas como entrada en los procesos que correspondan. Tener en cuenta este aspecto reduce la probabilidad de incumplimiento al numeral 4.4 de la Norma ISO/IEC 27001.
- Es importante mantener la misma valoración de activos de información de infraestructura crítica de la Gobernación (A-SGI-FR-002 versión 3 de 10 de septiembre de 2025) con la matriz de gestión de activos que se maneja por parte del tercero UT IDEAS 2026. Evidencia (Sistema de información portal web).
- Es importante asegurar una revisión en las hojas de vida de los funcionarios, permitiendo determinar si todos tienen acuerdos de confidencialidad firmados. Esta revisión permite reducir el riesgo de incumplimiento al control 6.6 Acuerdos de confidencialidad o no divulgación, de la norma ISO/IEC 27001.

Oportunidades de mejora

- Se sugiere incluir en los informes de seguimiento trimestral del proceso de Seguridad de la información el cumplimiento de los requisitos normativos asociados a SI.
- Establecer la posibilidad de ampliar la identificación de riesgos en otros procesos, enfocados a temas de seguridad de la información (ejemplo: riesgos enfocados al componente legal, objetivos de seguridad de la información).
- Asegurar que los hipervínculos que se encuentran en las caracterizaciones de Procesos estén asociados al aspecto que se determina en el título correspondiente.

- Asegurar que el documento de declaración de aplicabilidad incluya la palabra "debe" y no "debería" en la descripción de los controles.
- Se sugiere revisar la meta de aquellos indicadores que, por trazabilidad, han superado en varios periodos sus resultados. (Ejemplo: indicador de atención de los usuarios TIC)
- Es importante realizar un refuerzo de conocimientos asociado a temas como la gestión de riesgos, reporte de eventos y la Política de seguridad de la información a los funcionarios que están bajo el alcance certificado.
- En los requisitos de la caracterización de los procesos de gestión de ingresos, gestión contractual y de compra pública, gestión administrativa y de recursos y de gestión financiera, administración del recurso humano es importante determinar los numerales y controles aplicables de la Norma ISO/IEC 27001. Para los demás procesos establecidos en el sistema es importante indicar los controles del anexo aplicables.
- Es necesario realizar una revisión de los aspectos contemplados en el contexto organizacional para asegurar que corresponden en realidad a factores internos y externos
- Ajustar el manejo del formato de Control de datos y gestión de la información de la actividad del laboratorio de rentas y gestión tributaria, para que esté alineado a la guía de contraseñas seguras del SGSI, debido a que almacenan la secuencia de contraseñas en un archivo al cual tiene acceso todo el personal del laboratorio. (Hallazgo detectado en el proceso de gestión de ingresos)
- Evaluar los controles incluidos en la matriz de riesgos de seguridad de la información aplicados para reducir el riesgo residual, debido a que la valoración del riesgo inherente se mantiene. Por lo tanto, es importante incluir controles más efectivos que permitan llevar los riesgos al apetito de riesgo determinado por la Entidad. Este hallazgo fue detectado para las actividades de Riesgos de seguridad de la información
    - Nota: Tener en consideración los criterios establecidos por la guía DAFP
- Se recomienda desagregar y consolidar el detalle y el total de los recursos presupuestales de personal, infraestructura, componentes de seguridad de monitoreo, con el objetivo de tener identificado el presupuesto asignado para seguridad de la información, analizando si estos son suficientes para mantener y suplir las necesidades del SGSI.
- Es importante mejorar las evidencias en la revisión por la Dirección asociadas a la retroalimentación de partes interesadas

NO CONFORMIDADES DETECTADAS

Total No Conformidades detectadas: 3

- Al verificar el cumplimiento del procedimiento Visitas de inspección TIC para teletrabajadores A-GT-PR-029 versión de 11/09/2025 en el ítem 7 donde se determina la realización de informe de resultado de visita técnica formato E-GT-FR-113 V1, se observa que para la funcionaria Anyela Ortiz no se encontró evidencia de dicho informe. Lo anterior contraviene lo establecido en la norma ISO 27001:2022 numeral 8.1 Planificación y control operacional, en su párrafo "La información documentada debe estar disponible en lo posible para tener la confianza en que los procesos han venido siendo ejecutados según lo planeado."
- Al verificar la actividad 8 que determina la creación de un caso en la Herramienta Aranda para la creación de accesos de funcionarios determinado en el Procedimiento Gestión de accesos a sistemas TI A-GT-PR-039, versión 1, se evidencia que para la funcionaria Camila Ruiz no se evidenció dicho registro de creación en esta herramienta. Lo anterior contraviene lo establecido en la norma ISO 27001:2022 numeral 8.1 Planificación y control operacional, en su párrafo "La información documentada debe estar disponible en lo posible para tener la confianza en que los procesos han venido siendo ejecutados según lo planeado."
- Al verificar la información de contactos asociados a contingencias/continuidad de negocio determinados en los

documentos del Proceso de Tecnología, se pudo observar que algunos cargos que son críticos en la operación tecnológica no cuentan con un backup en caso de presentarse una eventualidad. Se verificaron los cargos de Administrador de Redes y seguridad perimetral, Administrador de base de datos, Supervisor de contrato de tecnología (Contrato de Collocation) para los cuales no fue posible establecer evidencia de tener un backup designado. Lo anterior contraviene lo establecido en el control del Anexo A "Preparación de las TIC para la continuidad de la actividad, el cual determina que "La preparación para las TIC debe planificarse, implementarse, mantenerse y probarse sobre la base de los objetivos de continuidad empresarial y los requisitos de continuidad de las TIC.

RESULTADOS DE SEGUIMIENTO NO CONFORMIDADES DE AUDITORIA ANTERIOR

Después de verificar las evidencias de acciones correctivas generadas de hallazgos de Auditoría Externa se pudo establecer:

- 1. NC: No se evidencia la medición de la eficacia de las capacitaciones, de acuerdo con el Plan de aprendizaje individual – PAI y Plan de Aprendizaje por Equipos - PAE correspondiente al periodo 2025.
- 1.1. Para este hallazgo no se pudo determinar la eficacia de la acción, ya que dos evidencias determinadas en la acción correctiva 5493 no tenían soportes de cumplimiento asociada a temas de seguridad de la información. Dichas evidencias son:

- 1.1.1. Se encuentra documento informe de Reinducción de 22 de julio de 2026 en donde no se evidenció planificación de actividades relacionadas con temas de seguridad de la información y/o eje temático número 4 "Transformación digital y cibercultura.

- 1.1.2. Se evidencia que en el documento Plan institucional de capacitación PIC 2026 de enero de 2026 no se establece en el capítulo 5 "presupuesto y cronograma" actividades que permitan establecer la ejecución de la formación sobre seguridad de la información y/o el eje temático 4 "Transformación digital y cibercultura.", tampoco se observa que en dicho documento en el capítulo 6 "Seguimiento y evaluación actividades" se determine un análisis puntual al cumplimiento de formaciones asociadas a seguridad de la información y/o eje temático "Transformación digital y cibercultura."
- 1.2. Al no poder evidenciar actividades asociadas a estos aspectos, el equipo de Auditoría no puede determinar la eficacia de la Acción. Se hace necesario asegurar el cumplimiento de actividades para poder determinar la eliminación de la causa raíz del hallazgo.

- 2. NC: No se etiquetan la información de acuerdo con los niveles de clasificación establecidos.
- 2.1. Se verifica el plan de acción 5494 encontrando la implementación de todas las actividades propuestas, con su respectiva evidencia de implementación. Teniendo en cuenta lo anterior, el equipo de auditoría determina el cierre eficaz de la acción.

- 3. NC: No se evidencian que los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información.
- 3.1. Se verifica el plan de acción 5495 encontrando la implementación de todas las actividades propuestas, con su respectiva evidencia de implementación. Teniendo en cuenta lo anterior el equipo de auditoría determina el cierre eficaz de la acción.

- 4. NC: No se cumple con los lineamientos de seguridad de contraseñas de acuerdo a política de acceso lógico de la Entidad, en específico en la longitud de la contraseña (8 caracteres) y la complejidad de las contraseñas
- 4.1. Se verifica el plan de acción 5496 encontrando la implementación de todas las actividades propuestas, con su respectiva evidencia de implementación. Teniendo en cuenta lo anterior, el equipo de auditoría determina el cierre eficaz de la acción.

CAMBIOS QUE AFECTEN AL PROCESO/ORGANIZACIÓN

- No se detectó en este ejercicio de Auditoría algún cambio que pueda afectar a los Procesos/Organización

CONCLUSIÓN GENERAL

1. Grado en el que se han cumplido los criterios de la auditoría

Durante el ejercicio de Auditoría ejecutado y teniendo en cuenta las evidencias obtenidas, se pudo establecer que existe un SGSI implementado, mantenido y con tendencia a la mejora continua.

Aunque se determinaron hallazgos asociados a oportunidades de mejora, observaciones y no conformidades, las mismas no tienen una afectación sobre la integridad del SGSI.

Se observa un grado de cumplimiento adecuado asociado a los lineamientos de la Norma ISO/IEC 27001:2022.

Asociado al objetivo de Auditoría establecido, se determina el cumplimiento del mismo y la determinación de un sistema maduro acorde a los requerimientos de la Entidad.

2. Buenas prácticas identificadas

Para este punto y en la tendencia de mejora continua que se ha determinado por la Entidad, se resalta:

2.1. El Proyecto Collocation, establece una serie de medidas y controles que permiten trabajar en pro de mantener la confidencialidad, disponibilidad e integridad de la información de las partes interesadas. Para este mismo Proyecto, se observa la determinación de recursos por parte de la Entidad para mantener una robusta infraestructura tecnológica.

2.2. Las diferentes herramientas de seguimiento asociadas al sistema permiten mantener una trazabilidad adecuada sobre diversos temas establecidos en el sistema; esto también permite, en donde aplique, la toma de acciones de mejora.

En el ítem "Fortalezas" se comparten otras buenas prácticas encontradas durante el ejercicio de Auditoría

RIESGOS Y OPORTUNIDADES

Incluir los comentarios sobre los riesgos y oportunidades asociados al logro de los resultados deseados y al mantenimiento del sistema de gestión.

1. LIMITACIONES IDENTIFICADAS EN EL PROCESO DE AUDITORÍA

- Sin limitaciones identificadas.

2. DEBILIDADES VERIFICABLES DEL SISTEMA DE GESTIÓN AUDITADO, O DEL PROCESO DE AUDITORÍA.

N/A

Auditores	Líder de Proceso
Rodrigo Gutierrez Arias-Auditor Líder Rodrigo Gutierrez Martha Zornosa-Auditor Martha P Zornosa G	Ingrid Johanna Cubides Puentes