UNIDAD DE RESTITUCIÓN DE TIERRAS

UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS

(UAEGRTD)

INFORME OCI-2026-19

AUDITORÍA INTERNA AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BAJO ESTÁNDARES DE LA NTC ISO 27001:2022

OFICINA DE CONTROL INTERNO

JUNIO DE 2026

DESTINATARIOS:

- **Rangel Giovani Yule Zape**, Director General.
- **Jaqueline Campos Rincón**, Secretaría General.
- **Aura Patricia Bolívar Jaime**, Subdirectora General.
- **Paula Andrea Villa Vélez**, Directora Jurídica y Directora Territorial Chocó (E).
- **Wilson Zapata**, Jefe Oficina Asesora de Planeación.
- **Carlos Alberto De la Ossa Hurtado**, Jefe Oficina de Tecnologías de la Información.

RESPONSABLE DEL INFORME:

- **Claudia Marcela Pinzón Martínez**, Jefe Oficina de Control Interno.

EQUIPO AUDITOR:

- **Carlos Alberto Quiñones Cárdenas,** Contratista, Líder de auditoría, Oficina de Control Interno.

OBJETIVO(S):

Evaluar de forma independiente el diseño y la eficacia operativa de los controles internos implementados en la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD), para gestionar los riesgos asociados al Modelo de Seguridad y Privacidad de la Información – MSPI.

ALCANCE:

El alcance establecido para la realización de este trabajo de auditoría comprende la evaluación de los controles internos y de gestión asociados a la adopción, implementación y actualización del Modelo de Seguridad y Privacidad de la Información (MSPI), en concordancia con los lineamientos actualizados por la Norma ISO/IEC 27001:2022.

En desarrollo de lo anterior, el alcance incluye la revisión y análisis de los siguientes componentes:

1. Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Se evaluó mediante la verificación de entregables definidos para cada una de las etapas del MSPI, específicamente:
   - Etapa de diagnóstico y planeación, incluyendo el diagnóstico del estado actual, la definición del alcance, roles y responsabilidades, y la identificación de riesgos.
   - Etapa de diseño, que contempla la definición de políticas, procedimientos, lineamientos y controles de seguridad y privacidad de la información.
   - Etapa de implementación, mediante la revisión de evidencias sobre la puesta en marcha de los controles definidos, así como su integración en los procesos institucionales.
   - Etapa de seguimiento y mejora, considerando los mecanismos de monitoreo, medición, revisión y mejora continua del MSPI. La evaluación de esta etapa se realizará con base

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

en los productos, documentos y registros formalmente establecidos como entregables en cada fase del modelo.

2. Controles del Anexo A de la Norma ISO/IEC 27001:2022. Respecto a los controles definidos en el Anexo A de la Norma ISO/IEC 27001 versión 2022, en el entendimiento realizado por parte de la Oficina de Control Interno, se elaboró un análisis comparativo y preliminar frente a los controles contenidos en la versión 2013 de la misma norma, con el fin de identificar:
   - Controles que han sido modificados.
   - Controles nuevos incorporados en la versión 2022.
   - Controles que se mantienen sin cambios sustanciales respecto a la versión 2013.

   Con base en dicho análisis, el alcance de la auditoría estableció que:

   - Se excluyeron de la verificación detallada aquellos controles que en la ISO27001 versión 2022, resultan nuevos o que presentan modificaciones frente a la versión 2013 de la Norma ISO/IEC 27001.
   - Se realizó la verificación mediante muestreo sobre una selección representativa de los controles que se mantienen equivalentes desde la versión 2013, con el propósito de evaluar su adecuada implementación dentro del MSPI.

Corte: abril de 2026.

Nota: El establecimiento de esta fecha de corte no limita la facultad de la Oficina de Control Interno para pronunciarse sobre hechos posteriores que, por su grado de materialidad deban ser revelados.

LIMITACIÓN: El proceso auditor no presentó limitaciones, dado que abordó todas las actividades previstas dentro del programa de auditoría.

CRITERIOS:

Relacione la normativdad tanto interna como externa que se tuvo en cuenta en la ejecución del proceso de auditoría.

Normatividad Externa:

- Decreto 767 de 2022 *"Por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital".*
- 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",* expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Resolución 2277 de 2025 *"Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia",* expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

- Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, versión 5 de 2025, expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Normatividad Interna:

- Documentación dispuesta en el Sistema Integrado de Planeación y Gestión (STRATEGOS), asociada al proceso de "Gestión de TI":
  - GT-CA-01 - Gestión de TI
  - GT-ES-02 - Compendio de políticas complementarias de MSPI
  - GT-ES-03 - Política de Gestión de Incidentes de Seguridad de la Información
  - GT-ES-04 - Política de Tratamiento de Datos Personales
  - GT-ES-09 - Manual de preparación TI para la continuidad del negocio
  - GT-ES-10 - Plan de preparación de TI para la continuidad del negocio
  - GT-ES-13 - Plan De Seguridad y Privacidad de la Información
  - GT-ES-14 - Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025
  - GT-ES-19 - Políticas de Infraestructura Tecnológica
  - GT-FO-38 - Control de Copias de Seguridad
  - GT-MA-06 - Arquitectura de Seguridad de la Información
  - GT-PR-14 - Gestión de Incidentes Red y Servidores
  - GT-PR-15 - Creación de Solicitudes o Incidentes
  - GT-PR-23 - Copias de Respaldo de Información en Servidores
  - GT-PR-24 - Continuidad de Negocio - Activar Contingencia Servicios Críticos
  - GT-PT-01 - Protocolo de Administración y Gestión para la Plataforma de Antivirus
  - GT-PT-02 - Protocolo Estándar de Configuración de Firewall Confidencial
  - GT-PT-03 - Protocolo Estándar de Cifrado o Descifrado
  - GT-PT-04 - Cifrado de Discos y Extraíbles
  - GT-PT-05 - Protocolo para la Configuración del Cliente VPN Forticlient
  - GT-PT-06 - Protocolo para el uso del Gestor de Contraseñas KEEPASS
  - GT-PT-07 - Protocolo para el Borrado Seguro de la Información sin Recuperación
  - GT-PT-10 - GT PT 10 Protocolo de configuración MFA

RIESGOS IDENTIFICADOS EN LA AUDITORÍA:

Tabla N° 1. Riesgos identificados en el marco del proceso auditor

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
Identificados en el Mapa de Riesgos de Gestión	
Posibilidad de pérdida reputacional debido a falta de disponibilidad y continuidad de los servicios de TI dada la inadecuada asignación de recursos y deficiencias en la gestión y monitoreo de la seguridad, plataforma y componentes de la infraestructura tecnológica y/o por eventos naturales que afectan los centros de datos y redes de comunicaciones.	Si
Identificados en el Mapa de Riesgos Fiscales y/o de Seguridad de la Información *(Si aplica)*	
Posibilidad de Pérdida de la Disponibilidad de los equipos de cómputo institucionales debido a eventos de intrusión, fallas, robo o pérdida a causa de errores en la aplicación de políticas seguridad, uso inapropiado y falta de conciencia en seguridad causando afectación económica y reputacional de la UAEGRTD.	Si

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
Posibilidad de Pérdida de la Disponibilidad de los sistemas de información, aplicaciones, centro de datos on premise y en nube debido a cambios no planificados, autorizados ni controlados por falta de monitoreo a los accesos con credenciales de administrador causando incumplimiento en acuerdos de servicio y pérdida reputacional de la UAEGRTD.	Si
Posibilidad de Pérdida de la Integridad y confidencialidad de sistemas de información y aplicaciones en centros de datos y en nube debido a accesos no autorizados debido a activación y desactivación manual de credenciales lo puede ocasionar una fuga y alteración de información llevando a afectar negativamente la reputación de la UAEGRTD.	Si
Posibilidad de Pérdida de la Integridad y confidencialidad de los equipos de cómputo por la instalación de código o software malicioso debido a descarga no controlada de información, así como sistemas desprotegidos por acceso no autorizado, causando pérdida y/o fuga de información afectando negativamente la reputación de la UAEGRTD.	Si
Posibilidad de Pérdida de la Disponibilidad de equipos de cómputo personales utilizados en el trabajo en casa por acción de código o software malicioso debido al modelo de operación remota de la Entidad causando pérdida de información y afectando la reputación de la UAEGRTD.	Si
Posibilidad de Pérdida de la Integridad y confidencialidad de las contraseñas de administrador por fraude o fuga de información debido a falta de control en la custodia provocando pérdida de información y ocasionando deterioro en la reputación de la UAEGRTD.	Si
Posibilidad de Pérdida de la Disponibilidad e integridad de la información por inadecuada administración de las bases de datos alojadas en el centro de datos y en la nube debido a errores de configuración y definición de modelos de datos que pueden tener un efecto económico o reputacional desfavorable para la UAEGRTD.	Si
Posibilidad de Pérdida de la Confidencialidad y disponibilidad de la información fuera del centro de datos y en la nube debido a pobre definición de lineamientos para la gestión de interoperabilidad en la UAEGRTD (roles no identificados en el intercambio de información, arquitectura de interoperabilidad no definida, incumplimiento a la ley de datos personales y/o incumplimiento de acuerdos de confidencialidad), ocasionando deterioro en la reputación de la UAEGRTD.	Si
Identificados por la Oficina de Control Interno	
Posibilidad de afectación económica y reputacional, debido a la falta de una definición clara y formal de funciones y responsabilidades en seguridad de la información, así como a una clasificación insuficiente de la información institucional, permitiendo una materialización de incidentes de seguridad de la información que no sean identificados ni gestionados de manera oportuna y adecuada, ocasionando la divulgación no autorizada de información, afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información. (Organizacional)	Si
Posibilidad de afectación económica y reputacional, debido a la ausencia o debilidad en la definición y cumplimiento de los términos y condiciones de empleo en materia de seguridad de la información, así como a una gestión inadecuada de las responsabilidades de los colaboradores durante cambios de rol, terminación del vínculo laboral o modalidades de trabajo remoto, permitiendo el uso indebido, acceso no autorizado o divulgación no autorizada de la información institucional por parte de colaboradores o exempleados, generando afectaciones a la confidencialidad, integridad y disponibilidad de la información. (Personas)	Si
Posibilidad de afectación económica y reputacional, debido a deficiencias en la definición y aplicación de controles de seguridad física en las instalaciones de la entidad, así como a la falta de medidas adecuadas para la protección contra amenazas físicas y ambientales, mediante el acceso físico de personal no autorizado o la afectación de las instalaciones donde se encuentran los activos de información y la infraestructura tecnológica, generando pérdida, alteración o indisponibilidad de la información, interrupciones en la prestación de los servicios institucionales y afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información de la entidad. (Físico)	Si
Posibilidad de afectación económica y reputacional, debido a deficiencias en la protección de los sistemas de información frente a software malicioso, así como a la	Si

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
falta de prácticas de desarrollo seguro y de mecanismos de redundancia en las instalaciones de procesamiento de información, lo cual puede derivar en la materialización de incidentes de seguridad digital que comprometan los sistemas de información institucionales mediante la introducción de código malicioso, fallas en aplicaciones o interrupciones en la operación tecnológica, ocasionando pérdida o indisponibilidad de la información, afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información, interrupciones en la prestación de los servicios institucionales y el incumplimiento de los objetivos estratégicos de la entidad. (Tecnológicos)	

Fuente: Mapa de riesgos institucional.

RESULTADOS OBTENIDOS DEL PROCESO AUDITOR:

1. FORTALEZAS:

- La Entidad cuenta con una definición formal de roles y responsabilidades en materia de seguridad y privacidad de la información, a través de documentos como *"Roles y Responsabilidades 2026"* y el *"Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información (GT-ES-02)",* en los cuales se establecen los actores institucionales, sus funciones y responsabilidades dentro del Modelo de Seguridad y Privacidad de la Información (MSPI), incluyendo instancias de gobernanza, áreas operativas y actores externos, lo cual fortalece la gestión, implementación y control del sistema.
- La Entidad dispone de una metodología estructurada para la identificación, valoración y clasificación de activos de información, mediante el documento *"Metodología de Identificación, Valoración y Clasificación de Activos de Información (GT-GU-12)",* el cual establece lineamientos, criterios y herramientas para la gestión integral de los activos, incorporando principios de confidencialidad, integridad y disponibilidad, así como la asignación de responsables y el uso de instrumentos como la Matriz de Activos de Información, lo que contribuye a la adecuada gestión y protección de la información institucional.
- La Entidad dispone de un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información formalmente estructurado, en el cual se definen objetivos, actividades, responsables, metas, indicadores y recursos asociados a la mitigación de riesgos, evidenciando una planeación organizada y alineada con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital.
- La Entidad cuenta con un manual integral de políticas de seguridad de la información, materializado en el documento "*Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información (GT-ES-02)",* que consolida lineamientos, directrices y controles en diversos dominios de seguridad (accesos, activos, criptografía, incidentes, continuidad, entre otros), alineados con estándares internacionales como ISO 27001, lo cual fortalece el marco normativo interno para la protección de la información, la cual está en fase de actualización a la versión de la ISO 27001-2022.

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

2. HALLAZGOS:

A continuación se presenta un resumen ejecutivo de hallazgos elevados en el marco del proceso auditor, cuya información a detalle podrá ser consulta en los formatos de "Reporte de Hallazgo", los cuales forman parte integra del presente informe:

Hallazgo N° 1:

Tabla N° 2. Reporte de Hallazgo N° 1.

TÍTULO:	***Debilidad en los soportes que respaldan la adopción de las etapas del Documento Maestro del Modelo de Seguridad y Privacidad de la Información***

SITUACIÓN EVIDENCIADA:

El Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI), establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones, define el marco conceptual, metodológico y operativo para la gestión integral de la seguridad de la información en las entidades públicas, en armonía con estándares internacionales y las políticas de Gobierno Digital. Este documento se estructura en cinco (5) fases: diagnóstico, planificación, operación, evaluación del desempeño y mejoramiento continuo, las cuales orientan la implementación progresiva del modelo.

En el marco del objetivo de la auditoría, la presente verificación se enfocó en la revisión de los principales productos asociados a cada una de estas cinco (5) fases, a partir de una lista de chequeo compuesta por treinta y dos (32) numerales, mediante la cual se evaluó la existencia, completitud, consistencia, calidad y soporte documental de los productos definidos en el modelo, con el propósito de determinar el grado de implementación y madurez del MSPI en la entidad. Como resultado, se concluyó lo siguiente:

- Veintitrés (23) numerales (72%) cumplen con la información solicitada.
- Ocho (8) numerales (25%) tienen observaciones o debilidades en cuanto a los productos que soportan las etapas de adopción del modelo.
- Un (1) numeral (3%) no cumple con la información solicitada.

A continuación se detalla los resultados obtenidos frente a los numerales que presentaron observaciones o no cumplimiento:

Tabla No. 1. Resultado de la verificación de la información que soporta la sección de levantamiento de información del MSPI.

ID	PRODUCTOS	CONCLUSIONES DE LA VERIFICACIÓN	RESULTADO
	1. Diagnóstico		
D01	Documento de la herramienta de autodiagnóstico diligenciada, identificando las brechas en la implementación del MSPI en toda la entidad, y sus acciones de mejora.	El instrumento de autodiagnóstico del MSPI de la UAEGRTD, presenta un cumplimiento del 92%, con una alta cantidad de dominios en niveles "gestionado" u "optimizado", políticas formalizadas, gestión de riesgos estructurada, controles técnicos y administrativos implementados, programas de capacitación activos y procesos de auditoría y seguimiento. No obstante, el diligenciamiento del archivo también evidencia debilidades y oportunidades de mejora, tales como enlaces incorrectos, ausencia de documentos clave (inventarios, declaración de aplicabilidad, planes de seguimiento y control), falta de evidencias de aprobación por la alta dirección, y vacíos en la implementación de componentes críticos como continuidad del negocio, gestión de proyectos con enfoque de seguridad, indicadores del MSPI y seguimiento a planes e indicadores. Asimismo, se destacan oportunidades de mejora en la actualización normativa, y la documentación de resultados de auditoría y gestión de riesgos. Se recomienda subsanar estas situaciones para el diligenciamiento de la autoevaluación de la vigencia 2026.	Observaciones
	2. Planificación		
P01	Alcance MSPI	Los documentos analizados corresponden a herramientas de planeación, ejecución y seguimiento de la seguridad de la información, ya que contienen actividades, cronogramas, responsables y avances del MSPI; sin embargo, no definen el alcance del modelo, dado que no establecen de manera explícita los límites, procesos, activos, áreas organizacionales ni la cobertura del sistema de seguridad de la información, elementos que son necesarios para considerar formalmente definido el alcance del MSPI.	Observaciones

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

P09	Declaración de aplicabilidad	Actualmente no se cuenta con el documento de Declaración de Aplicabilidad de los controles del MSPI	**No cumple**
P14	Alcance MSPI (Este alcance puede estar integrado al Manual del Sistema Integrado de Gestión, o en el documento del Modelo de Planeación y Gestión)	El documento *"Política y Objetivos del Sistema Integrado de Planeación y Gestión – SIPG (MC-ES-05)"* permite verificar de manera parcial el alcance del MSPI, en tanto establece lineamientos institucionales que integran la seguridad y privacidad de la información como parte del SIPG, definiendo su aplicación en todos los procesos misionales y de apoyo, así como la protección de la confidencialidad, integridad y disponibilidad de la información y la gestión de riesgos asociados. Sin embargo, aunque el documento evidencia la incorporación del MSPI dentro del sistema de gestión y su orientación estratégica, no define de forma explícita y delimitada un apartado específico de alcance del MSPI (por ejemplo, en términos de cobertura organizacional, activos, sedes o exclusiones), por lo que el alcance se infiere de manera general dentro de la política y no como un elemento claramente estructurado.	**Observaciones**
P20	• Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia). • La aceptación de los riesgos residuales e indicación en que parte se deben aceptar. • Declaración de aplicabilidad, aceptada y aprobadas en el comité institucional de gestión y desempeño.	Los documentos aportados al equipo auditor, permiten verificar de manera parcial el cumplimiento de los requisitos evaluados. Por un lado, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 (GT-ES-14) constituye evidencia formal de la existencia del instrumento, el cual define objetivos, alcance, actividades, responsables, indicadores y fecha de aprobación (01/11/2024), en concordancia con lo exigido por el Decreto 612 de 2018 respecto a su integración dentro de los planes institucionales. Asimismo, el extracto del acta evidencia que dicho plan es socializado en el Comité Institucional de Gestión y Desempeño en el marco de la planeación institucional. No obstante, no se evidencia el documento de Declaración de Aplicabilidad aprobado por el comité.	**Observaciones**
3. Operación			
O01	• Plan de seguridad y privacidad de la información que defina la implementación de controles de seguridad y privacidad de la información y contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. • Evidencia de la implementación de los controles de seguridad y privacidad de la información.	El Plan Estratégico de Seguridad de la Información - PESI 2025 y 2026 define las líneas de acción, controles, actividades, cronogramas, entregables, recursos y presupuesto general, así como la implementación de medidas técnicas y organizacionales para proteger la información; adicionalmente, para 2026 se observa un avance en la trazabilidad al incluir cronogramas más detallados, fechas de ejecución y la asignación de dependencias responsables. No obstante, en ambas vigencias persisten debilidades que limitan la verificación integral del cumplimiento, tales como la ausencia de un desglose específico de responsables por actividad y de presupuesto por control, así como la falta de evidencias concretas de implementación, ya que estas se presentan principalmente como informes y entregables esperados, sin soportes verificables de ejecución efectiva de los controles.	**Observaciones**
O03	Indicadores de gestión de seguridad de la información	Se evidencia la existencia de indicadores de gestión de seguridad de la información, en la medida en que el documento define indicadores asociados al MSPI, como el porcentaje de avance del Plan de Seguridad y Privacidad de la Información (PESI) y del Plan de Tratamiento de Riesgos (PTRSI), incorporando variables como metas, ejecución, porcentaje de cumplimiento, periodicidad mensual, responsables y rangos de medición. No obstante, su alcance resulta limitado, ya que estos indicadores se enfocan principalmente en el seguimiento al avance de planes (gestión y cumplimiento) y no permiten una evaluación integral del modelo. En este sentido, los indicadores del MSPI deberían diseñarse para medir de manera completa la implementación, madurez y efectividad del sistema, incluyendo aspectos como la gestión de riesgos, la atención de incidentes, la gestión de vulnerabilidades, los controles de acceso y la eficacia de los controles. Esto implica incorporar métricas como el porcentaje de riesgos tratados, tiempos de respuesta a incidentes, nivel de cumplimiento en capacitación, grado de inventario y clasificación de activos, efectividad de controles y cierre de hallazgos de auditoría, de modo que los indicadores sean medibles, periódicos y sirvan como insumo para el seguimiento, la evaluación del desempeño y la mejora continua del modelo.	**Observaciones**
4. Evaluación de desempeño			

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

E01	• Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el Decreto 612 de 2018. • Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.	De acuerdo con el Decreto 612 de 2018, los indicadores que deben incluirse en el tablero de control del Plan de Acción son aquellos que permiten hacer seguimiento al cumplimiento de los planes institucionales y estratégicos, entre los cuales se encuentran el Plan de Seguridad y Privacidad de la Información (PESI) y el Plan de Tratamiento de Riesgos. En este sentido, el archivo de indicadores evidencia la existencia de estos indicadores de gestión asociados al MSPI, al contemplar elementos como metas, ejecución, responsables, periodicidad y variables de medición. No obstante, para efectos de futuras verificaciones, se recomienda complementar la documentación mediante la inclusión explícita de una hoja de vida completa e individualizada por cada indicador, que detalle su definición técnica, fórmula, línea base y análisis. Por otro lado, el Informe de Autodiagnóstico 2025 constituye evidencia de la evaluación y medición de la efectividad de los controles, al presentar resultados cuantitativos (con un promedio del 92%), análisis por dominios de la ISO 27001 y evaluación del avance del modelo mediante enfoques como PHVA y NIST, lo que permite evidenciar el desempeño general de los controles implementados; sin embargo, este análisis se realiza a nivel global del modelo y no se encuentra plenamente articulado con la verificación específica de la ejecución de los controles definidos en el plan de tratamiento de riesgos mediante evidencias puntuales por cada acción de mitigación. Adicionalmente, el documento se encuentra en estado de borrador, toda vez que no presenta fecha formal de aprobación, lo cual limita su estado como soporte definitivo.	**Observaciones**
E03	• Revisión a la implementación. • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección.	El documento *"Informe de Rendición de Cuentas"* permite verificar que, en el marco de la rendición de cuentas de 2025, se realizó una Revisión por la Dirección del Subsistema de Gestión de Seguridad de la Información, en la cual se analizó el desempeño, la eficacia, la adecuación y los resultados del modelo, incluyendo planes, riesgos, indicadores y oportunidades de mejora. Asimismo, se indica que los avances y productos del subsistema son presentados al Subcomité de Gobierno y Transformación Digital y posteriormente al Comité Institucional de Gestión y Desempeño, lo que permite inferir un flujo de seguimiento y aprobación institucional de los temas estratégicos. No obstante, el documento no aporta evidencia explícita de actas de aprobación formal de la política y el manual de seguridad, ni de los actos administrativos que los adopten, tampoco se identifican de manera detallada los compromisos derivados de la revisión por la dirección, o la periodicidad de estas revisiones, lo que limita la verificación integral del requisito en cuanto a aprobación formal, trazabilidad de decisiones y evidencia documentada de la revisión periódica del MSPI por parte de la alta dirección.	**Observaciones**
5. Mejoramiento continuo			

Fuente: Construcción del equipo auditor a partir de la información suministrada por la Oficina de Tecnologías de la Información – OTI.

CIRTERIOS ASOCIADOS:	**NORMATIVIDAD EXTERNA:** ▪ 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"*, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, en su artículo 4 establece: ***"ARTÍCULO 4o. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL.*** *Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia*.
RIESGOS ASOCIADOS:	▪ GT-RG-9 Posibilidad de pérdida reputacional debido a falta de disponibilidad y continuidad de los servicios de TI dada la inadecuada asignación de recursos y deficiencias en la gestión y monitoreo de la seguridad, plataforma y componentes de la infraestructura tecnológica y/o por eventos naturales que afectan los centros de datos y redes de comunicaciones. ▪ GT-RSI-1 Posibilidad de Pérdida de la Disponibilidad de los equipos de cómputo institucionales debido a eventos de intrusión, fallas, robo o pérdida a causa de errores en la aplicación de políticas seguridad, uso inapropiado y falta de conciencia en seguridad causando afectación económica y reputacional de la UAEGRTD. ▪ GT-RSI-2 Posibilidad de Pérdida de la Disponibilidad de los sistemas de información, aplicaciones, centro de datos on premise y en nube debido a cambios no planificados, autorizados ni controlados por falta de monitoreo a los accesos con credenciales de

	administrador causando incumplimiento en acuerdos de servicio y pérdida reputacional de la UAEGRTD. ▪ GT-RSI-3 Posibilidad de Pérdida de la Integridad y confidencialidad de sistemas de información y aplicaciones en centros de datos y en nube debido a accesos no autorizados debido a activación y desactivación manual de credenciales lo puede ocasionar una fuga y alteración de información llevando a afectar negativamente la reputación de la UAEGRTD. ▪ GT-RSI-4 Posibilidad de Pérdida de la Integridad y confidencialidad de los equipos de cómputo por la instalación de código o software malicioso debido a descarga no controlada de información, así como sistemas desprotegidos por acceso no autorizado, causando pérdida y/o fuga de información afectando negativamente la reputación de la UAEGRTD. ▪ GT-RSI-5 Posibilidad de Pérdida de la Disponibilidad de equipos de cómputo personales utilizados en el trabajo en casa por acción de código o software malicioso debido al modelo de operación remota de la Entidad causando pérdida de información y afectando la reputación de la UAEGRTD. ▪ GT-RSI-6 Posibilidad de Pérdida de la Integridad y confidencialidad de las contraseñas de administrador por fraude o fuga de información debido a falta de control en la custodia provocando pérdida de información y ocasionando deterioro en la reputación de la UAEGRTD. ▪ GT-RSI-7 Posibilidad de Pérdida de la Disponibilidad e integridad de la información por inadecuada administración de las bases de datos alojadas en el centro de datos y en la nube debido a errores de configuración y definición de modelos de datos que pueden tener un efecto económico o reputacional desfavorable para la UAEGRTD.
RECOMENDACIONES	▪ Garantizar que los productos asociados a las etapas del Documento Maestro del MSPI se encuentren generados, organizados, y actualizados. Para ello, es importante la existencia de controles documentados de monitoreo y/o seguimiento que permitan mejorías en su cumplimiento y conservación de soportes documentales correspondiente. ▪ Fortalecer el conocimiento del marco conceptual establecido en el Documento Maestro del MSPI, asegurando una adecuada comprensión del alcance de cada etapa para poder fortalecer la ejecución metodológica de la adopción de estos lineamientos del Ministerio de Tecnología y las Comunicaciones.

Fuente: Construcción propia del equipo auditor, a partir de los resultados de las pruebas de auditoría.

Hallazgo N° 2:

Tabla N° 3. Reporte de Hallazgo N° 2.

TÍTULO:	***Debilidad en los soportes que respaldan la sección de levantamiento de información del instrumento de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información***

SITUACIÓN EVIDENCIADA:

El instrumento de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones, contempla el diligenciamiento de información relacionada con el contexto institucional requerido para la gestión del marco de seguridad de la información, así como con los controles definidos en la norma ISO 27001. Al respecto, la verificación realizada por la Oficina de Control Interno se enfocó exclusivamente en la totalidad de los requisitos de la sección *"Levantamiento de información"*, la cual está compuesta por cuarenta y dos (42) numerales, respecto de los cuales se validó la completitud, consistencia, actualización y existencia de los soportes de la información reportada, teniendo en cuenta que la sección de controles fue evaluada de manera independiente. Como resultado, se concluyó lo siguiente:

- Veintitrés (23) numerales (54.8%) cumplen con la información solicitada.
- Nueve (9) numerales (21.4%) tienen observaciones o debilidades, ya sea de diseño, implementación o efectividad operativa.
- Nueve (9) numerales (21.4%) no cumplen con la información solicitada.
- Un (1) numeral (2.4%) no fue corroborado debido a que el documento indica ser reservado y no fue remitido para su verificación.
-

A continuación se detalla los resultados obtenidos frente a los numerales que presentaron observaciones o no cumplimiento:

Tabla No. 1. Resultado de la verificación de la información que soporta la sección de levantamiento de información del MSPI.

No.	Información requerida	Resultado	Observaciones de la OCI
4	Mapa de Procesos	Observaciones	Para el numeral 4, se incluyó un enlace que redirige a la sección de misión, visión y propósito de la URT, en lugar de dirigir al mapa de procesos de la Entidad.

10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	**No cumple**	Para el numeral 10, se solicita el documento que contenga el resultado de la estratificación de la Entidad, debidamente aceptado y aprobado por la alta dirección; sin embargo, no se evidencia enlace ni referencia que permita acceder a dicho documento como soporte.
21	Inventario de áreas de procesamiento de información y telecomunicaciones	**No cumple**	Para el numeral 21, no existe el documento Inventario de áreas de procesamiento de información y telecomunicaciones.
22	Diagrama de red de alto nivel o arquitectura de TI	**No verificado**	Documento reservado. No se verificó.
23	Inclusión de la seguridad de la información en la gestión de proyectos	**Observaciones**	Para el numeral 23, si bien se cuenta con una guía de gestión de proyectos de TI de agosto de 2023, no se observó que esta incorpore la seguridad de la información como un componente transversal durante la ejecución, alineado con buenas prácticas internacionales y con el Sistema de Gestión de Seguridad de la Información institucional. En este sentido, se recomienda articular la definición de roles y responsabilidades en seguridad, la gestión de riesgos asociados a la confidencialidad, integridad y disponibilidad de la información, así como la clasificación y adecuado manejo de la información del proyecto. Igualmente, incluir controles de acceso bajo el principio de mínimo privilegio, la gestión segura de cambios, la protección de datos personales conforme a la normativa vigente y la segregación y aseguramiento de los distintos ambientes (desarrollo, pruebas y producción). De igual forma, es necesario que estas guías establezcan mecanismos para la gestión de incidentes de seguridad, políticas de respaldo y continuidad de la información, así como controles sobre terceros y proveedores. También garantizar la trazabilidad de las actividades y la generación de evidencias para auditoría, junto con acciones de sensibilización del equipo del proyecto en buenas prácticas de seguridad. En conjunto, estos elementos permiten asegurar que la seguridad de la información se gestione de manera integral durante la ejecución del proyecto, basada en riesgos, con controles claros y verificables.
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad	**No cumple**	Para el numeral 24, Si bien se aportó como soporte un registro en formato Excel que contiene la lista de entidades con las cuales se comparte información, se evidencian debilidades relacionadas con su formalización dentro del Sistema Integrado de Planeación y Gestión (SIPG). En particular, dicho registro no se encuentra incorporado como documento controlado dentro de los instrumentos oficiales de la Entidad, lo que impide determinar su reconocimiento formal como inventario/registro institucional. Asimismo, no se evidencia la existencia de un procedimiento, instructivo o lineamiento que regule su diligenciamiento, actualización y control, lo cual limita garantizar la completitud, consistencia y actualización periódica de la información contenida en el mismo.
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden	**No cumple**	Para el numeral 26, no existe el documento Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden.
28	Plan de continuidad de la Entidad aprobado	**Observaciones**	Para el numeral 28, se cuenta con el plan de preparación de TI para la continuidad del negocio, desde octubre de 2020, el cual cumple parcialmente con los elementos que debe contar un plan de continuidad de negocios, ya que define el contexto, alcance, objetivos y justificación, y se encuentra alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO 27001, e incorpora un enfoque metodológico basado en un ciclo de mejora continua (planeación, implementación, gestión y mejora), contempla de forma conceptual la realización del análisis de impacto al negocio (BIA), la identificación de servicios críticos, la definición de estrategias de continuidad y la necesidad de realizar pruebas y seguimiento, lo cual evidencia una base metodológica coherente con buenas prácticas. No obstante, el documento presenta debilidades importantes que impiden considerarlo

			un plan de continuidad operativo, ya que no referencia los procedimientos detallados de respuesta y recuperación ante incidentes, el plan de recuperación de desastres (DRP) ni resultados documentados del BIA, y no define claramente roles operativos, plan de comunicaciones, escenarios de contingencia ni inventarios de recursos críticos. Adicionalmente, actividades clave (como el plan de requerimientos, implementación y pruebas) se encuentran en estado "no iniciada", lo cual no permite evidencia la madurez en cuanto a su implementación.
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	**Observaciones**	Para el numeral 29, se hace referencia al normograma institucional disponible en el portal web; sin embargo, al verificar la inclusión de los requisitos legales relacionados con la seguridad de la información, no se evidenció la incorporación de, al menos, las siguientes disposiciones, las cuales constituyen criterios relevantes para el objetivo de la auditoría al MSPI: la Resolución 0500 de 2021 del MinTIC, mediante la cual se establecen los lineamientos y estándares para la adopción del Modelo de Seguridad y Privacidad de la Información, así como la Resolución 02277 de 2025 del MinTIC, por medio de la cual se actualiza el Anexo 1 de la Resolución 0500 de 2021 y se adopta la transición de la norma ISO/IEC 27001 de la versión 2013 a la versión 2022.
30	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad	**Observaciones**	Para el numeral 30, se recomienda enlistar los informes de auditoría de seguimiento realizadas a la Estrategia de Gobierno Digital que incluyan el seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información realizadas en las vigencias 2025 y anteriores, y la auditoría de aseguramiento al Modelo de Seguridad y Privacidad de la información de la en ejecución de la actual vigencia 2026
32	Indicadores y métricas de seguridad de la información definidos.	**Observaciones**	Para el numeral 32, el soporte remite a STRATEGOS, en donde se encuentran entre otros, los indicadores *"GT-2-2026- Porcentaje de avance del plan de seguridad y privacidad de la información. PESI"*, y *"GT-3-2026- Porcentaje de avance del plan de tratamiento de riesgos de seguridad y privacidad de la información. PTRSI"*. No obstante, los indicadores y métricas del MSPI deben permitir evaluar de manera integral la eficacia del sistema, abarcando aspectos como la gestión de riesgos, la atención de incidentes de seguridad, la identificación y corrección de vulnerabilidades, el control de accesos y el cumplimiento normativo. En este sentido, es fundamental medir variables como el porcentaje de riesgos tratados, el número y tiempo de respuesta a incidentes, el nivel de remediación de vulnerabilidades, el control de accesos no autorizados y el grado de cumplimiento frente a políticas, normas y auditorías, la continuidad del negocio, la gestión de respaldos, la protección de datos personales, la gestión de activos de información, el desempeño de proveedores y la cultura de seguridad en la Entidad. Y respecto a la ISO/IEC 27001:2022 la norma, en su cláusula 9.1 exige que la organización defina métricas e indicadores para monitorear, medir, analizar y evaluar el desempeño y la eficacia del SGSI, determinando qué medir, cómo, cuándo y quién lo hace. De acuerdo con esto, los indicadores deben alinearse con los objetivos de seguridad y cubrir tanto la efectividad de los controles como el desempeño del sistema. En la práctica, los principales indicadores suelen agruparse en categorías clave: gestión de riesgos (ej. % de riesgos tratados), incidentes de seguridad (número de incidentes, tiempo de detección y respuesta – MTTD/MTTR), vulnerabilidades y controles técnicos (nivel de parchado, vulnerabilidades críticas abiertas), control de accesos (accesos no autorizados, revisiones periódicas), cumplimiento y auditoría (hallazgos y cierre de no conformidades), conciencia y capacitación (porcentaje de personal capacitado, resultados de phishing), y efectividad del SGSI (grado de cumplimiento de objetivos de seguridad, desempeño de controles)
33	Declaración de aplicabilidad	**No cumple**	Para el numeral 33, no existe el documento Declaración de aplicabilidad
Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN			

35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	**No cumple**	Para el numeral 35, no existe el Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección
36	Avance en la ejecución del plan de tratamiento de riesgos	**Observaciones**	Para el numeral 36, se observó que se cuenta con la definición del indicador *"GT-3-2025 - Porcentaje de avance del plan de tratamiento de riesgos de seguridad y privacidad de la información (PTRSI)";* sin embargo, al verificar los Indicadores en el módulo de "Estrategia", opción "Indicadores" de STRATEGOS, no se observan registros de los avances correspondientes a la vigencia 2025. En consecuencia, no es posible evidenciar el progreso reportado en dicho indicador
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	**Observaciones**	Para el numeral 37, se observó que se cuenta con la definición del *indicador "GT-2-2025- Porcentaje de avance del plan de seguridad y privacidad de la información. PESI";* sin embargo, al verificar el módulo de "Estrategia", opción "Indicadores" de STRATEGOS, no se observan registros de los avances correspondientes a la vigencia 2025. En consecuencia, no es posible evidenciar el progreso reportado en dicho indicador.
Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO			
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	**No cumple**	Para el numeral 38, no existe el Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	**No cumple**	Para el numeral 40, como evidencia, se remitió el documento "GT-ES-14_V5 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025"; no obstante, este corresponde únicamente al plan formulado y no al resultado del seguimiento, la evaluación y el análisis de su ejecución, debidamente revisado y aprobado por la Alta Dirección
Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA			
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	**No cumple**	Para el numeral 41, no existe el documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.	**Observaciones**	Para el numeral 42, en el documento referenciado es el Plan Estratégico de Seguridad de la Información (PESI), pero este no contiene el consolidado de las auditorías realizadas, los hallazgos u oportunidades de mejora, ni los planes de mejoramiento establecidos para su subsanación

Fuente: Construcción del equipo auditor a partir de la información suministrada por la Oficina de Tecnologías de la Información – OTI.

CIRTERIOS ASOCIADOS:	**NORMATIVIDAD EXTERNA:** ▪ Resolución N° 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"*, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, en su anexo 2 "Modelo de Seguridad y Privacidad de la Información", numeral 6 establece: "*06. Diagnóstico: La fase de diagnóstico permite a los sujetos obligados establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación."*
RIESGOS ASOCIADOS:	▪ OCI-1: Posibilidad de afectación económica y reputacional, debido a la falta de una definición clara y formal de funciones y responsabilidades en seguridad de la información, así como a una clasificación insuficiente de la información institucional, permitiendo una materialización de incidentes de seguridad de la información que no sean identificados ni gestionados de manera oportuna y adecuada, ocasionando la divulgación no autorizada

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

	de información, afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información. (Organizacional). ▪ OCI-2: Posibilidad de afectación económica y reputacional, debido a la ausencia o debilidad en la definición y cumplimiento de los términos y condiciones de empleo en materia de seguridad de la información, así como a una gestión inadecuada de las responsabilidades de los colaboradores durante cambios de rol, terminación del vínculo laboral o modalidades de trabajo remoto, permitiendo el uso indebido, acceso no autorizado o divulgación no autorizada de la información institucional por parte de colaboradores o exempleados, generando afectaciones a la confidencialidad, integridad y disponibilidad de la información. (Personas). ▪ OCI-3: Posibilidad de afectación económica y reputacional, debido a deficiencias en la definición y aplicación de controles de seguridad física en las instalaciones de la Entidad, así como a la falta de medidas adecuadas para la protección contra amenazas físicas y ambientales, mediante el acceso físico de personal no autorizado o la afectación de las instalaciones donde se encuentran los activos de información y la infraestructura tecnológica, generando pérdida, alteración o indisponibilidad de la información, interrupciones en la prestación de los servicios institucionales y afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad. (Físico). ▪ OCI-4: Posibilidad de afectación económica y reputacional, debido a deficiencias en la protección de los sistemas de información frente a software malicioso, así como a la falta de prácticas de desarrollo seguro y de mecanismos de redundancia en las instalaciones de procesamiento de información, lo cual puede derivar en la materialización de incidentes de seguridad digital que comprometan los sistemas de información institucionales mediante la introducción de código malicioso, fallas en aplicaciones o interrupciones en la operación tecnológica, ocasionando pérdida o indisponibilidad de la información, afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información, interrupciones en la prestación de los servicios institucionales y el incumplimiento de los objetivos estratégicos de la Entidad. (Tecnológicos).
RECOMENDACIONES	▪ Establecer controles que permitan garantizar que todos los numerales del instrumento de autodiagnóstico cuenten con soportes completos, organizados, actualizados y verificables. ▪ Establecer revisiones internas para validar la consistencia, integridad y pertinencia de la información reportada antes de su consolidación. ▪ Formular e implementar un plan de acción para los numerales que presentan incumplimiento u observaciones, con responsables y tiempos definidos. ▪ Fortalecer el conocimiento del MSPI y de los requisitos de la norma ISO/IEC 27001:2022, asegurando una adecuada comprensión del alcance de cada numeral

Fuente: Construcción propia del equipo auditor, a partir de los resultados de las pruebas de auditoría.

Hallazgo N° 3:

Tabla N° 6. Reporte de Hallazgo N° 3.

TÍTULO:	***Debilidad en el diseño y efectividad de los controles establecidos en el Anexo A de la norma ISO 27001-2022 en el marco del Modelo de Seguridad y Privacidad de la Información***
SITUACIÓN EVIDENCIADA:	
En el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), la norma ISO/IEC 27001:2022 constituye el referente internacional para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en las entidades del Estado. Esta norma define un conjunto de noventa y tres (93) controles orientados a la gestión de riesgos de seguridad de la información, los cuales son adoptados y contextualizados a través del MSPI. De acuerdo con la estructura de la norma ISO/IEC 27001:2022, los noventa y tres (93) controles se organizan en cuatro (4) grupos principales, los cuales permiten abordar de manera integral la gestión de la seguridad de la información. 1. El primer grupo corresponde a treinta y siete (37) controles organizacionales, enfocados en la definición de políticas, roles, responsabilidades, gestión de riesgos y gobierno de la seguridad de la información. 2. El segundo grupo reúne ocho (8) controles de personas, orientados a la gestión del talento humano, incluyendo aspectos como concienciación, formación y responsabilidades del personal frente a la seguridad. 3. El tercer grupo comprende catorce (14) controles físicos, relacionados con la protección de las instalaciones, equipos y activos frente a accesos no autorizados o daños físicos. 4. Finalmente, el cuarto grupo corresponde a treinta y cuatro (34) controles tecnológicos, los cuales abordan la protección de sistemas, redes, aplicaciones y datos mediante la implementación de medidas técnicas de seguridad.	

Estos grupos, en conjunto, permiten a las entidades fortalecer su Sistema de Gestión de Seguridad de la Información en alineación con los lineamientos del MSPI.

En este sentido, la presente validación se enfocó en los controles de la ISO/IEC 27001:2022, con el propósito de verificar su implementación, adecuación y evidencia de cumplimiento dentro de la Entidad, en concordancia con los lineamientos definidos por el modelo y las buenas prácticas internacionales en materia de seguridad de la información.

Considerando que la norma ISO/IEC 27001 fue actualizada en el año 2022, introduciendo cambios en su estructura y en el conjunto de controles aplicables, y que el Ministerio de Tecnologías de la Información y las Comunicaciones, mediante la Resolución 2277 de 2025, dispuso la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) alineándolo con dicha versión, se generó la necesidad de evaluar el grado de adopción de los controles en la Entidad. No obstante, debido a la complejidad, extensión y alcance de la norma, la auditoría se enfocó en la revisión de una muestra representativa de controles, con el fin de verificar su implementación, adecuación y evidencia de cumplimiento en el marco del Sistema de Gestión de Seguridad de la Información.

Para ello, se realizó un análisis comparativo de los controles de la norma ISO/IEC 27001, considerando los ciento catorce (114) controles establecidos en la versión 2013, frente a los noventa y tres (93) controles definidos en la versión 2022. A partir de este ejercicio, se identificó que treinta y siete (37) controles presentaron modificaciones o que fueron incorporados en la nueva versión, conllevando a excluirlos del universo de verificación. De esta manera, se definió la procedencia de validar cincuenta y siete (57) controles sobre los cuales, se seleccionó una muestra de veintitrés (23) controles, distribuidos de la siguiente forma: siete (7) controles organizacionales, tres (3) controles de personas, siete (7) controles físicos, y seis (6) controles tecnológicos. Lo cual corresponde al 40% del universo verificable (Excluyendo los controles nuevos o modificados en la actualización de la norma).

En consecuencia, tras la revisión realizada a los veinte tres (23) controles de la norma ISO/IEC 27001:2022, se obtuvo el siguiente resultado:

- 4 controles (17%) efectivos.
- 14 controles (61%) tienen observaciones o debilidades.
- 5 controles (22%) no efectivos.

A continuación se detalla los resultados obtenidos frente a los controles que presentaron observaciones o que no lograron mostrar efectividad:

Tabla No. 7. Resultado de la verificación efectividad de la muestra de veinte tres (23) controles de la norma ISO/IEC 27001:2022.

No.	Anexo A Tipo de control	Identificador del Anexo A de ISO/IEC 27001:2022	Nombre del Control	Descripción del objetivo del control	Resultado
2	Controles organizacionales	Anexo A 5.3	Segregación de deberes	Establecer y mantener mecanismos adecuados para segregación de deberes con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
4		Anexo A 5.16	Gestión de identidad	Establecer y mantener mecanismos adecuados para gestión de identidad con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
5		Anexo A 5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Establecer y mantener mecanismos adecuados para planificación y preparación de la gestión de incidentes de seguridad de la información con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
6		Anexo A 5.27	Aprender de los incidentes de seguridad de la información	Establecer y mantener mecanismos adecuados para aprender de los incidentes de seguridad de la información con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	No efectivo

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

7		Anexo A 5.28	Recolección de evidencia	Establecer y mantener mecanismos adecuados para recolección de evidencia con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	No efectivo
8		Anexo A 6.1	Selección de Personal	Establecer y mantener mecanismos adecuados para examen en línea. con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
10		Anexo A 6.3	Concientización, educación y capacitación en seguridad de la información	Establecer y mantener mecanismos adecuados para concientización, educación y capacitación sobre seguridad de la información con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
11	Controles físicos	Anexo A 7.1	Perímetros físicos de seguridad	Establecer y mantener mecanismos adecuados para perímetros de seguridad física con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
12		Anexo A 7.5	Protección contra amenazas físicas y ambientales.	Establecer y mantener mecanismos adecuados para protección contra amenazas físicas y ambientales con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	No efectivo
13		Anexo A 7.7	Escritorio despejado y pantalla despejada	Establecer y mantener mecanismos adecuados para limpiar escritorio y limpiar pantalla con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
14		Anexo A 7.9	Seguridad de los activos fuera de las instalaciones	Establecer y mantener mecanismos adecuados para seguridad de los activos fuera de las instalaciones con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	No efectivo
15		Anexo A 7.12	seguridad del cableado	Establecer y mantener mecanismos adecuados para seguridad del cableado con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
16		Anexo A 7.13	Mantenimiento de equipo	Establecer y mantener mecanismos adecuados para mantenimiento de equipo con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
17		Anexo A 7.14	Eliminación segura o reutilización de equipos	Establecer y mantener mecanismos adecuados para eliminación segura o reutilización del equipo con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	No efectivo
18		Anexo A 8.6	Gestión de capacidad	Establecer y mantener mecanismos adecuados para gestión de capacidad con el fin de proteger	Debilidades

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

	Controles Tecnológicos			la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	
19		Anexo A 8.7	Protección contra malware	Establecer y mantener mecanismos adecuados para protección contra malware con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
20		Anexo A 8.17	Sincronización de reloj	Establecer y mantener mecanismos adecuados para sincronización de reloj con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
22		Anexo A 8.21	Seguridad de los servicios de red.	Establecer y mantener mecanismos adecuados para seguridad de los servicios de red con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades
23		Anexo A 8.22	Segregación de redes	Establecer y mantener mecanismos adecuados para segregación de redes con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, reducir riesgos de seguridad y asegurar el cumplimiento de los requisitos del SGSI.	Debilidades

Fuente: Construcción del equipo auditor a partir de la información suministrada por la Oficina de Tecnologías de la Información – OTI.

Nota: El detalle de la verificación realizada se encuentra en los papeles de trabajo que reposan en el repositorio de la Oficina de Control Interno, disponible para consulta previa solicitud formal.

Estos resultados reflejan debilidades y oportunidades de mejora en el diseño y efectividad de los controles del anexo A de la ISO 27001:2022 asociados al Modelo de Seguridad y Privacidad de la Información.

CIRTERIOS ASOCIADOS:	**NORMATIVIDAD EXTERNA:** ▪ 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"*, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, y la Resolución 2277 de 2025 *"Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021",* las cuales establecen la adopción de los controles del Anexo A de la norma ISO/IEC 27001, los cuales se adoptaron al interior de la UAEGRTD en los siguientes criterios de la normatividad interna. **NORMATIVIDAD INTERNA** ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, específicamente en el Capítulo 6 *"Organización de la Seguridad de la Información"*, numeral 6.1.1. En este se definen los lineamientos para la asignación clara y documentada de roles y responsabilidades en seguridad de la información, contemplando su alineación con la estructura organizacional y con los procesos del SGSI. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, específicamente en el Capítulo 6 *"Organización de la Seguridad de la Información"*, numeral 6.1.2, en el cual se establecen lineamientos para la adecuada segregación de funciones como principio de control organizacional. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 8 *"Gestión de Activos"*, numeral 8.2.1, así como en la GT-GU-12 *"Metodología de identificación, valoración y clasificación de los activos de información"*, los cuales definen los lineamientos para la clasificación de la información en la Entidad. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo *9 "Control de Acceso",* numeral 9.2.1, así como en el GT-IN-04 *"Instructivo de Administración de Usuarios en el Directorio Activo"*, los cuales establecen lineamientos para la gestión de identidades en la Entidad. ▪ GT-ES-03 *"Política de Gestión de Incidentes de Seguridad de la Información"* y en el *"Compendio de Políticas Complementarias del MSPI"* (Capítulo 16, numeral 16.1.1), donde se establecen lineamientos para la preparación y respuesta ante incidentes.

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

	▪ GT-ES-03 *"Política de Gestión de Incidentes de Seguridad de la Información"*, el GT-PR-15 *"Creación de Solicitudes o Incidentes y el Compendio de Políticas Complementarias del MSPI"* (Capítulo 16, numeral 16.1.6), en donde se establecen lineamientos generales para el análisis posterior de los incidentes y la generación de mejoras al SGSI. ▪ GT-ES-03 *"Política de Gestión de Incidentes de Seguridad de la Información"*, el GT-PR-15 *"Creación de Solicitudes o Incidentes y el Compendio de Políticas del MSPI"* (Capítulo 16, numeral 16.1.7 – Recolección de evidencia), donde se establecen lineamientos generales para la gestión de la evidencia en el contexto de incidentes de seguridad. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, específicamente en el Capítulo 7 *"Seguridad de los Recursos Humanos",* numeral 7.1.1, en el cual se definen lineamientos generales para la incorporación de criterios de seguridad de la información en el proceso de selección de personal. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI",* específicamente en el Capítulo 7 *"Seguridad de los Recursos Humanos",* donde se definen lineamientos para la formalización de compromisos de seguridad de la información como parte del proceso de vinculación. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 7 *"Seguridad de los Recursos Humanos"*, numeral 7.2.2, en el cual se establecen lineamientos para la implementación de programas de concientización y capacitación en seguridad de la información. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 11 *"Seguridad Física y del Entorno"*, numeral 11.1.1 *"Perímetros de Seguridad Física",* el cual establece los lineamientos para la protección de áreas seguras dentro de la entidad. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 11 *"Seguridad Física y del Entorno",* específicamente en el numeral 11.1.4 *"Protección contra las amenazas externas y ambientales".* ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo *11 "Seguridad Física y del Entorno",* numeral 11.2.9 *"Política de Escritorio y Pantalla Limpia".* En este documento se establecen lineamientos orientados a minimizar el riesgo de exposición de información en los puestos de trabajo, incluyendo, escritorio despejado, y cultura y sensibilización. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 11, numeral 11.2.6, en el cual se establecen lineamientos generales para la protección de activos fuera de las instalaciones. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 11 *"Seguridad Física y del Entorno"*, numeral 11.2.3 *"Seguridad de Cableado",* donde se establecen lineamientos orientados a proteger la infraestructura de cableado de la entidad. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 11, numeral 11.2.4, el cual establece lineamientos para la gestión del mantenimiento de los equipos tecnológicos. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI",* Capítulo 11, numeral 11.2.7, así como en el GT-PT-07 *"Protocolo para el borrado seguro de la información sin recuperación"*, en donde se establecen lineamientos para la disposición segura de equipos y medios de almacenamiento. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 12, numeral 12.1.3, así como en documentos complementarios como el *"Modelo de Arquitectura y Gestión de Infraestructura TI"*, el *"Documento de Gestión de Capacidades TI"* y el *"Plan de Capacidad Tecnológica para ambientes en Azure y on-premise"*. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 12, numeral 12.2.1, así como en el GT-PT-01 *"Protocolo de administración y gestión para la plataforma de antivirus",* los cuales establecen lineamientos para la protección contra software malicioso. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 12, numeral 12.4.4, donde se establecen lineamientos para la sincronización de la hora en los sistemas institucionales. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 13 *"Seguridad de las Comunicaciones",* numeral 13.1.1, donde se establecen lineamientos para la gestión de la seguridad en redes. ▪ GT-ES-02 *"Compendio de Políticas Complementarias del MSPI"*, Capítulo 13 "*Seguridad de las Comunicaciones",* numeral 13.1.2, en el cual se establecen lineamientos para la seguridad de los servicios de red. ▪ GT-ES-02 Compendio de Políticas Complementarias del MSPI, Capítulo *13 "Seguridad de las Comunicaciones",* numeral 13.1.3, el cual establece lineamientos para la segregación de la infraestructura de red.
RIESGOS ASOCIADOS:	▪ OCI-1: Posibilidad de afectación económica y reputacional, debido a la falta de una definición clara y formal de funciones y responsabilidades en seguridad de la información, así como a una clasificación insuficiente de la información institucional, permitiendo una materialización de incidentes de seguridad de la información que no sean identificados ni gestionados de manera oportuna y adecuada, ocasionando la divulgación no autorizada

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

	de información, afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información. (Organizacional). ▪ OCI-2: Posibilidad de afectación económica y reputacional, debido a la ausencia o debilidad en la definición y cumplimiento de los términos y condiciones de empleo en materia de seguridad de la información, así como a una gestión inadecuada de las responsabilidades de los colaboradores durante cambios de rol, terminación del vínculo laboral o modalidades de trabajo remoto, permitiendo el uso indebido, acceso no autorizado o divulgación no autorizada de la información institucional por parte de colaboradores o exempleados, generando afectaciones a la confidencialidad, integridad y disponibilidad de la información. (Personas). ▪ OCI-3: Posibilidad de afectación económica y reputacional, debido a deficiencias en la definición y aplicación de controles de seguridad física en las instalaciones de la Entidad, así como a la falta de medidas adecuadas para la protección contra amenazas físicas y ambientales, mediante el acceso físico de personal no autorizado o la afectación de las instalaciones donde se encuentran los activos de información y la infraestructura tecnológica, generando pérdida, alteración o indisponibilidad de la información, interrupciones en la prestación de los servicios institucionales y afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad. (Físico). ▪ OCI-4: Posibilidad de afectación económica y reputacional, debido a deficiencias en la protección de los sistemas de información frente a software malicioso, así como a la falta de prácticas de desarrollo seguro y de mecanismos de redundancia en las instalaciones de procesamiento de información, lo cual puede derivar en la materialización de incidentes de seguridad digital que comprometan los sistemas de información institucionales mediante la introducción de código malicioso, fallas en aplicaciones o interrupciones en la operación tecnológica, ocasionando pérdida o indisponibilidad de la información, afectaciones a la confidencialidad, integridad y disponibilidad de los activos de información, interrupciones en la prestación de los servicios institucionales y el incumplimiento de los objetivos estratégicos de la Entidad. (Tecnológicos). ▪ GT-RG-9 Posibilidad de pérdida reputacional debido a falta de disponibilidad y continuidad de los servicios de TI dada la inadecuada asignación de recursos y deficiencias en la gestión y monitoreo de la seguridad, plataforma y componentes de la infraestructura tecnológica y/o por eventos naturales que afectan los centros de datos y redes de comunicaciones. ▪ GT-RSI-1 Posibilidad de Pérdida de la Disponibilidad de los equipos de cómputo institucionales debido a eventos de intrusión, fallas, robo o pérdida a causa de errores en la aplicación de políticas seguridad, uso inapropiado y falta de conciencia en seguridad causando afectación económica y reputacional de la UAEGRTD. ▪ GT-RSI-2 Posibilidad de Pérdida de la Disponibilidad de los sistemas de información, aplicaciones, centro de datos on premise y en nube debido a cambios no planificados, autorizados ni controlados por falta de monitoreo a los accesos con credenciales de administrador causando incumplimiento en acuerdos de servicio y pérdida reputacional de la UAEGRTD. ▪ GT-RSI-3 Posibilidad de Pérdida de la Integridad y confidencialidad de sistemas de información y aplicaciones en centros de datos y en nube debido a accesos no autorizados debido a activación y desactivación manual de credenciales lo puede ocasionar una fuga y alteración de información llevando a afectar negativamente la reputación de la UAEGRTD. ▪ GT-RSI-4 Posibilidad de Pérdida de la Integridad y confidencialidad de los equipos de cómputo por la instalación de código o software malicioso debido a descarga no controlada de información, así como sistemas desprotegidos por acceso no autorizado, causando pérdida y/o fuga de información afectando negativamente la reputación de la UAEGRTD. ▪ GT-RSI-5 Posibilidad de Pérdida de la Disponibilidad de equipos de cómputo personales utilizados en el trabajo en casa por acción de código o software malicioso debido al modelo de operación remota de la Entidad causando pérdida de información y afectando la reputación de la UAEGRTD. ▪ GT-RSI-6 Posibilidad de Pérdida de la Integridad y confidencialidad de las contraseñas de administrador por fraude o fuga de información debido a falta de control en la custodia provocando pérdida de información y ocasionando deterioro en la reputación de la UAEGRTD. ▪ GT-RSI-7 Posibilidad de Pérdida de la Disponibilidad e integridad de la información por inadecuada administración de las bases de datos alojadas en el centro de datos y en la nube debido a errores de configuración y definición de modelos de datos que pueden tener un efecto económico o reputacional desfavorable para la UAEGRTD.
RECOMENDACIONES	▪ Fortalecer la formalización documental y operativa de los controles, asegurando que todos cuenten con procedimientos, metodologías, formatos y evidencias trazables. ▪ Implementar un enfoque integral de gestión, que articule diseño, implementación, monitoreo y mejora continua de los controles del SGSI.

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos

	▪ Estandarizar la implementación de controles a nivel nacional, garantizando consistencia entre nivel central y direcciones territoriales. ▪ Definir y aplicar mecanismos de monitoreo, medición y seguimiento a todos los controles por parte del líder del Subsistema de Gestión y Seguridad de la Información. ▪ Fortalecer la gestión de incidentes, incluyendo preparación, respuesta, análisis posterior, lecciones aprendidas y manejo de evidencia. ▪ Establecer e implementar planes de acción para cierre de brechas, priorizando controles clasificados como no efectivos.

Fuente: Construcción propia del equipo auditor, a partir de los resultados de las pruebas de auditoría.

Notas:

- La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Plan Anual de Auditoría, se encuentra limitada por restricciones de tiempo y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.
- La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por los responsables de atender el proceso auditor, a través de solicitudes y consultas realizadas por la Oficina de Control Interno. Nuestro alcance no pretende corroborar la precisión de la información y su origen.
- Es discrecional de Entidad determinar si se acogen las recomendaciones elevadas por la Oficina de Control Interno ante las situaciones observadas, no obstante, se invita a que las mismas sean consideradas en el establecimiento de los planes de mejoramiento a que haya lugar.

CLAUDIA MARCELA PINZON MARTINEZ

Firmado digitalmente por CLAUDIA MARCELA PINZON MARTINEZ
DN: T=JEFE DE OFICINA ASESORA, SN=PINZON MARTINEZ, STREET=CR 13 A 29 24 P 5 A L 13, S=BOGOTA D.C., OU=TOKEN VIRTUAL, SERIALNUMBER=2368203, OID.1.3.6.1.4.1.23267.2.3=9004988799, OID.1.3.6.1.4.1.23267.2.2=53077880, OID.1.3.6.1.4.1.23267.2.1=364, O=UNIDAD DE RESTITUCION DE TIERRAS, L=BOGOTA D.C., G=CLAUDIA MARCELA, C=CO, CN=CLAUDIA MARCELA PINZON MARTINEZ
Razón: Yo soy el autor de este documento
Ubicación:
Fecha: 30/06/2026 17:03:30 -05'00'

CLAUDIA MARCELA PINZÓN MARTÍNEZ
Jefe Oficina de Control Interno

Anexos*: Consolidado reportes de hallazgos - (formato CI-FO-34) con los tres (3) hallazgos*

Elaboró: *Carlos Alberto Quiñones Cárdenas, Contratista Oficina de Control Interno*

Revisó: *Maicol Stiven Zipamocha Murcia, Contratista Oficina de Control Interno*

Si usted copia o imprime este documento, la UAEGRTD lo considerará como No Controlado y no se hace responsable por su consulta o uso. Si desea consultar la versión vigente y controlada, consulte el Sistema de Información Strategos