PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

RESPONSABLE (S) DEL PROCESO O ACTIVIDAD AUDITADA	**Carlos Alberto de la Ossa Hurtado** – *Jefe de la Oficina de Tecnología de la Información*	**FECHA DEL REPORTE DEL HALLAZGO**	19/06/2026
COPIA DEL REPORTE DIRIGIDO A	**César Augusto Caro Amaya** - *Oficina de Tecnologías de la Información* **Silvia Juliana González Palomino** - *Oficina de Tecnologías de la Información*	**HALLAZGO RECURRENTE**	NO
AUDITOR(ES) RESPONSABLE(S)	**Carlos Alberto Quiñones Cárdenas -** *Contratista, rol Líder de Auditoría*		

OBJETIVO(S) DEL PAPEL DEL TRABAJO

1) Informar al(los) responsable(s) de la(s) unidad(es) auditada(s) acerca de los hallazgos identificados en el transcurso de la auditoría.
2) Recibir la retroalimentación por parte del(los) responsable(s) de la(s) unidad(es) auditada(s) frente a las situaciones evidenciadas para determinar si estas se mantienen en firme.

ESPACIO EXCLUSIVO PARA EL AUDITOR

TÍTULO DEL HALLAZGO

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

DESCRIPCIÓN DE LA 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.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

.

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**
P02	Acto administrativo con las funciones de seguridad y privacidad de la información	Se cuenta con un acto administrativo que define funciones relacionadas con la seguridad y privacidad de la información (Resolución 925 de 2016).	**Cumple**
P03	Adoptar la Política de seguridad y privacidad de la información mediante acto administrativo con el cual la entidad lo adopto colocar el número de resolución o acto administrativo	El documento *“Extracto Acta N.° 3 del Comité Institucional de Gestión y Desempeño”* evidencia la aprobación y actualización de la política del Subsistema de Seguridad de la Información en el marco del SIPG, aunque, no permite verificar la adopción de la Política de Seguridad y Privacidad de la Información mediante un acto administrativo, deja constancia de la aprobación del documento en instancia de comité.	**Cumple**
P4	Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información	El documento *“Roles y Responsabilidades 2026”* permite verificar la definición formal de roles y responsabilidades asociados a la seguridad y privacidad de la información, ya que define explícitamente los actores institucionales y sus funciones dentro del Modelo de Seguridad y Privacidad de la Información (MSPI). En este se establecen responsabilidades específicas para instancias como el Comité Institucional de Gestión y Desempeño, la Oficina de Tecnologías de la Información (incluyendo el rol de Oficial de Seguridad de la Información), la Oficina de Control Interno, la Oficina Jurídica, Talento Humano, áreas de contratación, servidores públicos, contratistas, proveedores y terceros, entre otros. Asimismo, se incluyen funciones relacionadas con la gestión de riesgos, implementación de controles, cumplimiento normativo, concientización, auditoría, manejo de activos de información y reporte de incidentes	**Cumple**

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

P5	Procedimiento de inventario y Clasificación de la Información e infraestructura crítica	El *documento "Metodología de Identificación, Valoración y Clasificación de Activos de Información (GT-GU-12)"* permite evidenciar la existencia de una metodología institucional para el inventario y clasificación de la información e infraestructura crítica, en tanto establece lineamientos, actividades y herramientas orientadas a la identificación, levantamiento, actualización, revisión y publicación del inventario de activos de información. Asimismo, describe de manera detallada la caracterización de activos (información, datos, software, hardware, redes, instalaciones, entre otros), la asignación de propietarios y custodios, y el uso de la Matriz de Activos de Información como instrumento de registro, junto con criterios de clasificación basados en confidencialidad, integridad y disponibilidad, así como aspectos de protección de datos y cumplimiento normativo. No obstante, si bien la metodología define de forma general la manera en que se debe realizar el levantamiento y gestión del inventario, no se evidencia la existencia de un procedimiento específico, formalmente documentado y detallado a nivel operativo, que estandarice paso a paso su ejecución dentro de la entidad.	**Cumple**
P6	Metodología de inventario y clasificación de la información e infraestructura crítica	El documento "*Metodología de Identificación, Valoración y Clasificación de Activos de Información (GT-GU-12)"* permite verificar la existencia de un procedimiento formal para el inventario y clasificación de la información e infraestructura crítica, en tanto establece lineamientos, actividades y herramientas para la identificación, levantamiento, actualización, revisión y publicación del inventario de activos de información. Asimismo, define un procedimiento estructurado que incluye la caracterización de activos (información, datos, software, hardware, redes, instalaciones, entre otros), la asignación de propietarios y custodios, y el uso de la Matriz de Activos de Información como instrumento de registro. Adicionalmente, incorpora criterios de clasificación de la información basados en confidencialidad, integridad y disponibilidad, así como aspectos de protección de datos personales, cumplimiento normativo y alineación con la Ley de Transparencia, lo que permite identificar activos críticos y priorizar su protección.	**Cumple**
P07	Política de Gestión de Riesgos de la entidad con los lineamientos para la gestión de riesgos de seguridad y privacidad de la información y demás documentación asociada que determinan dichos lineamientos para la administración y gestión del riesgo	El documento *"Política de Administración del Riesgo (MC-ES-04)"* permite verificar la existencia de una política institucional de gestión de riesgos, en la cual se establecen los lineamientos para la identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos, incluyendo de forma explícita los riesgos de seguridad y privacidad de la información. Asimismo, define el alcance sobre todos los procesos del SIPG, incorpora criterios metodológicos, niveles de aceptación, tratamiento y materialización del riesgo, y establece la articulación con documentación asociada, particularmente la Guía para la Administración del Riesgo (MC-GU-02), donde se desarrollan de manera detallada dichos lineamientos. De igual forma, adopta un enfoque integral contemplando riesgos de gestión, corrupción, fiscales y de seguridad de la información, lo que evidencia un marco estructurado para la administración y gestión del riesgo en la Entidad.	**Cumple**
P08	Plan de tratamiento de riesgos de seguridad de la información	El documento *"Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026 (GT-ES-14)"* permite verificar la existencia de un plan formal de tratamiento de riesgos de seguridad de la información, dado que establece el objetivo, alcance y contexto normativo para la gestión integral de estos riesgos, en concordancia con el MSPI y la Política de Gobierno Digital. Asimismo, incluye la identificación detallada de riesgos de seguridad de la información, así como la definición de actividades de tratamiento, responsables, entregables, recursos, metas e indicadores, lo que evidencia la planificación estructurada para su mitigación y control.	**Cumple**
P09	Declaración de aplicabilidad	Actualmente no se cuenta con el documento de Declaración de Aplicabilidad de los controles del MSPI	**No cumple**

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

P10	Manual de políticas de Seguridad de la Información	El documento *"Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información (GT-ES-02)"* permite verificar la existencia de un manual de políticas de seguridad de la información, dado que consolida en un solo instrumento institucional la política general y un conjunto amplio de lineamientos, directrices, controles y políticas específicas relacionadas con la gestión de la seguridad de la información. El documento establece objetivos, alcance, principios, roles y responsabilidades, así como políticas detalladas en múltiples dominios (gestión de activos, control de accesos, criptografía, seguridad física, operaciones, comunicaciones, gestión de incidentes, continuidad del negocio, entre otros), alineadas con el MSPI y estándares como ISO 27001. Si bien requiere la actualización con la versión 2022 de la ISO 27001, el compendio funciona como un marco normativo integral que orienta la protección de la confidencialidad, integridad y disponibilidad de la información, evidenciando claramente la existencia de un manual formal de políticas de seguridad de la información en la entidad.	**Cumple**
P11	Plan de Cambio, Cultura y Apropiación	El documento *"Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información 2026"* permite verificar la existencia de un Plan de Cambio, Cultura y Apropiación, ya que su contenido está orientado a fomentar la cultura organizacional en seguridad de la información y promover la adopción de buenas prácticas por parte de los funcionarios y contratistas. El plan define objetivos, alcance, actividades de sensibilización, capacitación y comunicación, así como estrategias de difusión, cronograma, roles, indicadores y mecanismos de seguimiento, enfocados en transformar comportamientos, fortalecer capacidades y generar apropiación institucional de la seguridad de la información.	**Cumple**
P12	Documentos obligatorios: Contexto de la entidad (Política de Planeación Institucional).	El documento *"Contexto Organizacional (PE-ES-04)"* permite verificar el contexto de la entidad en el marco de la Política de Planeación Institucional, en tanto desarrolla un análisis integral de la situación actual de la UAEGRTD, incluyendo la descripción institucional (misión, funciones, estructura organizacional), así como el análisis del entorno externo (político, económico, sociocultural, tecnológico, legal, de seguridad, entre otros) y del entorno interno, los procesos, el Sistema Integrado de Planeación y Gestión (SIPG), niveles de satisfacción y análisis DOFA.	**Cumple**
P13	Documentos obligatorios: Compendio de necesidades y expectativas de las partes interesada. (Política de Planeación Institucional). Análisis de partes interesadas en seguridad de la información.	Los documentos asociados al documento *"Contexto Organizacional"* (ANEXO 1 DOFA Contexto Organizacional, ANEXO 2 Matriz de Grupos de Valor y ANEXO 3 Contexto Direcciones Territoriales), permiten verificar las necesidades y expectativas de las partes interesadas, así como el análisis de partes interesadas en seguridad de la información, en tanto identifican y caracterizan los distintos grupos de valor (internos y externos), detallando sus necesidades, requisitos y expectativas, incluyendo aspectos relacionados con la protección, confidencialidad, disponibilidad e integridad de la información. De igual forma, estos anexos se articulan con el análisis DOFA y el contexto institucional y territorial, incorporando factores internos y externos, riesgos, debilidades, oportunidades y amenazas, entre ellos elementos específicos de seguridad digital, gestión de la información y riesgos asociados	**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**

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

P15	Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.	La Resolución No. 544 de 2023, permite verificar la existencia de un acto administrativo que soporta la conformación del Comité Institucional de Gestión y Desempeño, en tanto establece formalmente su integración, funcionamiento, roles y responsabilidades dentro de la entidad. Asimismo, en el artículo 2 se definen sus funciones, dentro de las cuales se incluye explícitamente la responsabilidad de asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información, evidenciando la incorporación de funciones relacionadas con la seguridad y privacidad de la información.	**Cumple**
P16	Acto administrativo o acta de aprobación del Comité Institucional de Gestión y Desempeño con la adopción de la Política de seguridad y privacidad de la información	Si bien no hay un acto administrativo como tal, el documento *"Extracto Acta N.° 2 del Comité Institucional de Gestión y Desempeño"* permite verificar la existencia de un acta de aprobación en el marco del Comité, en la cual se somete a consideración y se aprueba por unanimidad el Compendio de Políticas Complementarias de Seguridad de la Información (GT-ES-02 V7), evidenciando la adopción y actualización de lineamientos asociados al MSPI durante la vigencia 2025, por lo que constituye evidencia de aprobación en instancia de gobernanza de adopción de la política.	**Cumple**
P17	• Roles y responsabilidades en seguridad de la información de las diferentes áreas o procesos de la entidad. • Definición del rol de: responsable de seguridad de la información, indicando sus funciones y responsabilidades	El documento *"Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información (GT-ES-02)"* permite verificar la definición de roles y responsabilidades en seguridad de la información para las diferentes áreas y procesos de la entidad, en tanto identifica actores institucionales como el Comité Institucional de Gestión y Desempeño, la Oficina de Tecnologías de la Información, Control Interno, Talento Humano, Gestión Documental, Contratación, Planeación, entre otros, asignándoles funciones específicas relacionadas con la implementación, seguimiento, control y cumplimiento del MSPI. Asimismo, el documento define explícitamente el rol de Oficial de Seguridad de la Información como responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones de seguridad, orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información, junto con otros roles técnicos de apoyo.	**Cumple**
P18	• Procedimiento de inventario y clasificación de activos de información del Modelo de Seguridad y Privacidad de la Información. • Documento metodológico de inventario y clasificación de la información. • Inventario de activos de información de cada proceso incluido en el alcance debidamente identificados, clasificados y valorados.	El documento *"Metodología de Identificación, Valoración y Clasificación de Activos de Información (GT-GU-12)"* permite verificar el cumplimiento de los requerimientos relacionados con la metodología para el levantamiento del inventario y clasificación de activos de información del MSPI, en tanto constituye un documento metodológico formal que define lineamientos, actividades, criterios y herramientas para la identificación, levantamiento, clasificación, valoración, actualización y publicación del inventario de activos. No obstante, se recomienda analizar la posibilidad o necesidad de generar en respectivo procedimiento, y de acuerdo con lo entregables establecidos remitir la Matriz de Activos de Información vigente, junto con el resultado de su actualización realizada a comienzos de la vigencia 2026.	**Cumple**

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA			
P19	• Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité institucional de gestión y desempeño. • Instrumento para la identificación y valoración de los riesgos de seguridad y privacidad de la información.	Los *documentos "Política de Administración del Riesgo (MC-ES-04)"* y *"Guía para la Administración del Riesgo (MC-GU-02)"* permiten verificar la existencia de un procedimiento y metodología institucional para la gestión de riesgos, en la medida en que establecen los lineamientos generales y desarrollan una metodología integral que abarca la identificación, análisis, valoración, tratamiento y monitoreo de riesgos, incluyendo de forma explícita los riesgos de seguridad y privacidad de la información dentro del alcance del Sistema Integrado de Planeación y Gestión. La guía incorpora un capítulo específico para la identificación y gestión de riesgos de seguridad de la información, articulado con el MSPI y basado en la identificación previa de activos, amenazas y vulnerabilidades, así como en los principios de confidencialidad, integridad y disponibilidad. Asimismo, se evidencia la existencia de instrumentos metodológicos para la identificación y valoración de riesgos, tales como matrices de riesgos, criterios de probabilidad e impacto, mapas de calor y formatos estructurados para la evaluación, lo que demuestra un enfoque técnico y estandarizado. Adicionalmente, la política de riesgos se encuentra formalmente definida y aprobada en instancia institucional (CICCI), lo que asegura su validez dentro del marco de gobernanza.	**Cumple**
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**
P21	• Incluir dentro de los proyectos de inversión de la entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido. • Actualización del PETI de acuerdo con los recursos necesarios para realizar la gestión adecuada de los riesgos de seguridad de la información identificados y el plan de seguridad y privacidad de la información.	El documento *"Plan Estratégico de Tecnologías de la Información – PETI 2024–2026 (GT-ES-08)"* permite verificar la inclusión de proyectos de inversión y componentes tecnológicos alineados con la adopción del MSPI, en tanto define un portafolio de proyectos de TI, una hoja de ruta, asignación de recursos financieros y humanos, y la participación activa de la Oficina de TI en la planeación y ejecución de iniciativas institucionales, incorporando explícitamente lineamientos del Modelo de Seguridad y Privacidad de la Información dentro de la gestión tecnológica. Asimismo, el PETI evidencia su actualización y alineación estratégica con la Política de Gobierno Digital, Seguridad Digital y el PEI, integrando la gestión de riesgos, la seguridad de la información, la interoperabilidad, y el fortalecimiento de capacidades institucionales y de infraestructura tecnológica.	**Cumple**

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

P22	Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC. Plan de comunicaciones del modelo de seguridad y privacidad de la información.	El Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información 2025, el Plan de Comunicaciones de Seguridad de la Información 2025 (y su respectivo reporte de ejecución), junto con el Plan Institucional de Capacitación – PIC 2025, permiten verificar la existencia de un plan de cambio, cultura, apropiación, capacitación y sensibilización en seguridad de la información y seguridad digital, en tanto articulan acciones orientadas a fortalecer la cultura organizacional, el uso y apropiación de buenas prácticas, y la prevención de riesgos asociados a la seguridad de la información. Estos documentos incluyen objetivos, alcance, cronograma, actividades de capacitación (presenciales, virtuales y asincrónicas), campañas de comunicación, piezas gráficas, roles, indicadores y mecanismos de seguimiento, así como resultados de ejecución que evidencian su implementación efectiva. Asimismo, el plan se encuentra articulado con el PESI y con el PIC, integrando la formación del talento humano y los procesos de comunicación institucional como parte de la estrategia de apropiación del MSPI.	**Cumple**
P23	• Políticas, manuales, procesos procedimientos guías, entre otros. • Inventario de activos, matriz de riesgos, planes de tratamiento, declaración de aplicabilidad, proceso de gestión de eventos, vulnerabilidades.	Dentro de la lista de documentos en el SPG del procesos de Gestión de TI, se encuentran entre otros, los siguientes relacionados con seguridad de la información, y vale la pena mencionar que la OTI planea realizar ajustes a los documentos de acuerdo con la actualización de las políticas de seguridad: compendio de políticas complementarias de MSPI, política de gestión de incidentes de seguridad de la información, política de tratamiento de datos personales, plan estratégico de seguridad de la información, plan de tratamiento de riesgos de seguridad y privacidad de la información 2026, manual de preparación ti para la continuidad del negocio, plan de preparación de ti para la continuidad del negocio, arquitectura de seguridad de la información, matriz de activos de información (MAI), metodología de identificación valoración y clasificación de los activos de información, copias de seguridad y recuperación de información en servidores, copias de respaldo de información en servidores, gestión de incidentes red y servidores, protocolo de administración y gestión para la plataforma de antivirus, protocolo estándar de configuración de firewall, protocolo estándar de cifrado o descifrado, cifrado de discos y extraíbles, protocolo para el uso del gestor de contraseñas KEEPASS, protocolo para el borrado seguro de la información sin recuperación, protocolo de configuración MFA, control de copias de seguridad, solicitud de recuperación de información servidores.	**Cumple**
	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**
O02	• Matriz de riesgos de seguridad de la información. • Planes de tratamiento de los riesgos de seguridad de la información.	El documento permite evidenciar la existencia de una base de gestión de riesgos de seguridad de la información, ya que presenta un listado estructurado de riesgos identificados con sus descripciones, lo que demuestra el ejercicio institucional de identificación y análisis; adicionalmente, incorpora un plan de tratamiento al definir actividades, responsables, fases, tiempos y entregables orientados a la mitigación, seguimiento y mejora continua de dichos riesgos, aunque enfocado principalmente en la planeación y gestión de las acciones. Para futuros seguimientos, se recomienda incorporar dentro de la evidencia las matrices de riesgos de seguridad de información con sus resultados de valoración.	**Cumple**

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA			
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			
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**
E02	• Resultados de las auditorías internas. • No conformidades, hallazgos u oportunidades de mejora de las auditorías internas. • Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de Coordinación de Control Interno.	Si bien en la vigencia 2025 no se ejecutaron auditorías específicas al MSPI, sí se desarrollaron auditorías y ejercicios de seguimiento relacionados con este ámbito, como la auditoría especial al Sistema de Registro – SRTDAF, el seguimiento a la implementación de la estrategia de Gobierno Digital y el monitoreo de indicadores, incluyendo aquellos asociados a riesgos de seguridad de la información, de los cuales se derivaron hallazgos y la formulación de planes de mejoramiento. Esta situación resulta relevante, considerando que dentro de las entradas del lineamiento se contemplan, además de las auditorias, los documentos derivados de las fases del MSPI, los informes de evaluaciones independientes, seguimientos y auditorías. Vale la pena resaltar que para la vigencia 2026, se incluyó de manera formal una auditoría al MSPI dentro del programa de auditoría interna.	**Cumple**

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

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			
M01	• Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar, oportunidades de mejora, no conformidades y demás desviaciones identificadas en la gestión de los diferentes procesos de seguridad y privacidad de la información que componen el SGSI. • Plan estratégico de seguridad y privacidad de la información actualizado.	El Plan Estratégico de Seguridad de la Información (PESI) 2025 y 2026, permite evidenciar de manera articulada la gestión de la seguridad y privacidad de la información en la entidad, en tanto ambos documentos identifican acciones orientadas a la mejora continua del MSPI y del SGSI, mediante la definición de líneas de acción, fases del modelo (diagnóstico, planificación, operación, evaluación y mejoramiento continuo) y actividades específicas. Asimismo, se consolidan como planes estratégicos actualizados, alineados con el PETI y la normatividad vigente, incorporando la implementación de controles, tratamiento de riesgos, y la gestión de hallazgos derivados de auditorías y diagnósticos. Adicionalmente, evidencian mecanismos de seguimiento, evaluación y análisis, a través de indicadores, reportes periódicos, informes de seguimiento y monitoreo mensual, así como resultados de autodiagnóstico, evaluación de controles y medición del avance del ciclo PHVA, incluyendo la identificación de brechas y niveles de madurez. De igual forma, se observa la referencia a auditorías internas y externas y la gestión de sus resultados mediante planes de mejoramiento, lo cual refleja un enfoque sistemático de evaluación y fortalecimiento continuo del SGSI.	**Cumple**
M02	• Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar • Plan estratégico de seguridad y privacidad de la información actualizado. • Planes de acción para la remediación de las no conformidades	El PESI 2025 y 2026, evidencian una gestión integral de seguridad de la información, con enfoque en mejora continua del MSPI y SGSI, alineación normativa, implementación de controles, gestión de riesgos y seguimiento mediante indicadores, auditorías y planes de mejoramiento, no obstante, el documento no presenta de manera explícita un plan anual consolidado de mejora del MSPI que integre en un solo instrumento todas las oportunidades de mejora, no conformidades y desviaciones del SGSI, ni desarrolla detalladamente resultados históricos de auditorías o de ejecución del plan.	**Cumple**

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

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

CRITERIOS ASOCIADOS *(FUNDAMENTO LEGAL, NORMATIVO, PROCEDIMENTAL, ETC)*

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.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

RIESGOS ASOCIADOS

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.

CAUSA(S) PROBABLE(S)	**POSIBLES IMPACTOS**
▪ Desconocimiento del modelo, sus etapas y productos requeridos. ▪ Falta de una definición e identificación de los productos esperados por cada etapa del modelo. ▪ Ausencia de seguimiento sistemático al avance y cumplimiento de actividades asociadas para generar o actualizar los productos que soportan la adopción del marco de trabajo establecido en el modelo.	▪ Incumplimiento de lineamientos del MSPI, políticas de Gobierno Digital y normativa aplicable. ▪ Dificultad para avanzar en el nivel de implementación y madurez de la implementación del Modelo de Seguridad y Privacidad de la Información.

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.

ESPACIO EXCLUSIVO PARA EL RESPONSABLE DEL PROCESO O ACTIVIDAD AUDITADA

RESPUESTA DEL PROCESO O ACTIVIDAD AUDITADA:

D01 Documento de la herramienta de autodiagnóstico.

1. Enlace Incorrecto
Con respecto al hallazgo del Autodiagnóstico 2025, se aclara que la omisión de algunas rutas de enlace en la columna de observaciones constituyó un evento netamente formal y de digitación que no generó impacto ni incidencia en la evaluación final. Lo anterior se sustenta en que el documento soporte se encontraba plenamente identificado en la columna "Nombre del Documento Entregado", demostrando que las evidencias existían y fueron consideradas correctamente para el cálculo del resultado.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

2. Ausencia de documentos claves
Si bien existió una ausencia de documentos de inventario señalados en el hallazgo, se aclara no obstante que estas necesidades fueron tipificadas oportunamente como brechas de control, se infiere que las mismas se incorporaron dentro de la planeación estratégica de la vigencia 2026. Actualmente, su desarrollo se encuentra programado y en gestión como parte de los compromisos del Plan de Trabajo de Seguridad y Privacidad de la Información (PESI) de este año.

3. Formalización de la Declaración de Aplicabilidad (Aprobación de la alta Dirección)
Con relación a la falta de aprobación formal de la Declaración de Aplicabilidad por parte de la Alta Dirección, se aclara que esta situación obedeció al proceso estratégico de transición y actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) de la norma ISO/IEC 27001:2013 a la nueva estructura de controles de la versión 2022; cambio normativo y metodológico que requirió una fase técnica previa de alineación y diagnóstico, razón por la cual el documento actualizado se encuentra actualmente proyectado y en circuito de revisión para su correspondiente aprobación formal en la presente vigencia.

4. Implementación de Componentes Críticos

a. Continuidad de Negocio
Con respecto a la observación formulada, se aclara que durante la vigencia 2025 la Oficina de Tecnologías de la Información diseñó y estructuró de manera integral el Plan de Continuidad de TI. Este instrumento articuló de forma transversal todos los subdominios tecnológicos bajo el liderazgo de Seguridad de la Información, garantizando así la protección operativa de la infraestructura. Por lo tanto, se evidencia que el componente no presenta un vacío de implementación, por el contrario, se encuentra plenamente documentado y operativo conforme a las necesidades de la Entidad.

b. Gestión de Proyectos
Sobre este particular, se informa que desde el subdominio de Estrategia y Gobierno de TI se lideró la actualización técnica de la Guía para la Gestión de Proyectos de TI (GT-GU-14) durante la vigencia 2025, integrando la Seguridad de la Información. Actualmente, dicho documento fue presentado ante la Oficina Asesora de Planeación para su respectivo trámite.

c. Indicadores del MSPI y Seguimiento a Planes e Indicadores
Se precisa que la entidad cuenta con un esquema activo de medición, por lo cual los indicadores del MSPI son reportados y gestionados de manera regular a través de la plataforma institucional STRATEGOS (ruta: ESTRATEGIA/INDICADORES/REPORTES/REPORTE INDICADORES/ SEGURIDAD), desvirtuando la existencia de un vacío en esta materia. No obstante, en un esfuerzo de alineación normativa y mejora continua bajo el marco de la Resolución 2277 de 2025, proceso de implementación de la resolución que viene adoptando nuevos indicadores conforme lo dispone Gobierno Digital.

P01 Alcance MSPI
En cuanto el Alcance del MPSI, se debe mirar en todo el contexto del MSPI, donde se observa el alcance definido del (PESI- GT-ES-13), "El Plan Estratégico de Seguridad de la Información" busca consolidar la implementación del Subsistema de Gestión de Seguridad de la Información de la UAEGRTD, con impacto en el alcance de la Política General de Seguridad de la Información, en todos los procesos de la entidad". Por tanto, el alcance se encuentra definido en el numeral 2.2 Alcance del COMPENDIO DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (GT-ES-02). En cuanto a los procesos los activos y las dependencias se encuentran definidos en el mismo instrumento.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

Igualmente, el documento que se suministró como evidencia, fue producto de la misma definición de la fase de planeación que refiere que en el desarrollo se debe utilizar los resultados de la fase anterior para proceder el plan de seguridad.

P05 Procedimiento de inventario y Clasificación de la Información e infraestructura crítica
Inexistencia de un procedimiento (MAI)
Con respecto a la observación sobre la ausencia de un procedimiento formal, se aclara que la Oficina de Tecnologías de la Información actualizó el instrumento codificado Matriz de Activos de Información (GT-FO-45), incorporando de manera integral un instructivo técnico detallado que define los parámetros de presentación, identificación, clasificación, índice, datos personales y baja de activos, bajo los lineamientos vigentes de MinTIC. Esta herramienta actualizada por Seguridad de la Información, para su correcta adopción, fue socializada oficialmente a la entidad mediante una campaña de actualización documental; por lo tanto, considerando que el instructivo integrado detalla exhaustivamente los criterios operativos para la gestión del inventario, la creación de un procedimiento adicional resultara redundante para el control.

P09 Declaración de Aplicabilidad
La Declaración de Aplicabilidad correspondiente al periodo 2025 no fue presentada al Comité de Gestión y Desempeño debido al proceso de migración y transición hacia los controles de la norma ISO/IEC 27001:2022. Por lo tanto, el instrumento se gestionó como un documento técnico de trabajo interno de la OTI para evaluar los impactos del cambio normativo. Sin embargo, para la presente vigencia se viene trabajando un borrador de la declaración el cual está supeditado a la definición de los controles a implementar.

P14 Alcance MSPI
El alcance definido en el PESI y en el Compendio de Políticas Complementarias es claro, al dar cubrimiento a todos los procesos de la entidad donde se maneja información que deba ser resguardada.

P20 Declaración de Aplicabilidad
Formalización de la Declaración de Aplicabilidad (Aprobación de la alta Dirección)
Con relación a la falta de aprobación formal de la Declaración de Aplicabilidad por parte de la Alta Dirección, se aclara que esta situación obedeció al proceso estratégico de transición y actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) de la norma ISO/IEC 27001:2013 a la nueva estructura de controles de la versión 2022; cambio normativo y metodológico que requirió una fase técnica previa de alineación y diagnóstico, razón por la cual el documento actualizado se encuentra actualmente proyectado y en circuito de revisión para su correspondiente aprobación formal en la presente vigencia.

O01 PESI
El dominio de Seguridad de la Información dentro de la OTI apenas cuenta con dos colaboradores, en quienes recae la responsabilidad de la gestión del PESI, los entregables esperados corroboran la ejecución del plan de manera anual y el manejo del presupuesto de la OTI está en cabeza de la Jefatura de esta oficina, saliendo de la órbita de Seguridad de la Información.

O03 Indicadores de Gestión
Se precisa que la entidad cuenta con un esquema activo de medición, por lo cual los indicadores del MSPI son reportados y gestionados regularmente a través de la plataforma institucional STRATEGOS (ruta: ESTRATEGIA/INDICADORES/REPORTES/REPORTE INDICADORES/ SEGURIDAD), lo que desvirtúa la existencia de un vacío en la materia; no obstante, en el marco del proceso de implementación de la Resolución 2277 de 2025 y como parte de un esfuerzo de mejora continua, actualmente se está contemplando la adopción y actualización de nuevas métricas conforme a las directrices vigentes de la Política de Gobierno Digital.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

E01 Hoja de Vida Indicadores
Se precisa que la entidad cuenta con un esquema activo de medición, por lo cual los indicadores del MSPI son reportados y gestionados regularmente a través de la plataforma institucional STRATEGOS (ruta: ESTRATEGIA/INDICADORES/REPORTES/REPORTE INDICADORES/ SEGURIDAD), lo que desvirtúa la existencia de un vacío en la materia; no obstante, en el marco del proceso de implementación de la Resolución 2277 de 2025 y como parte de un esfuerzo de mejora continua, actualmente se está contemplando la adopción y actualización de nuevas métricas conforme a las directrices vigentes de la Política de Gobierno Digital.

E**03 Revisión a la Implementación**
Referente a su observación consideramos que el informe por su carácter gerencial no necesitaba los soportes a los que Uds. hace referencia de igual manera las referencias que se hacen en el mismo pueden ser verificadas en los archivos documentales de la entidad. Por tanto, dichos aspectos no le quitan la veracidad y objeto al informe de Rendición de cuentas.

M02 Plan Anual de Mejoras MSPI
Referente a su observación en necesario señalar que precisamente el MSPI incluye PESI, PTRSI, Plan de Capacitaciones, los cuales integran en sus componentes la mejora y el ajuste a las debilidades evidenciadas en vigencias anteriores, por tanto, el contexto del mismo no necesita un plan consolidado de mejoras ya que su propósito y alcance es precisamente la mejora continua.

CONCEPTO DE LA OFICINA DE CONTROL INTERNO	NO DESVIRTUADO

Al realizar la revisión de la respuesta emitida por la Oficina de Tecnologías de la Información (OTI) frente a lo dispuesto en el presente documento, la Oficina de Control Interno (OCI) efectuó ajustes en la calificación de aquellos numerales cuya información fue debidamente soportada. No obstante, considerando que aún persisten ocho (8) numerales con debilidades u observaciones, así como uno (1) que no cumple con el hito establecido, dentro del total de treinta y dos (32) numerales verificados en la prueba, se concluye que las situaciones evidenciadas no han sido subsanadas en su totalidad. En consecuencia, si bien se reconocen avances puntuales, de manera general el hallazgo se mantiene.

El detalle de la revisión a la respuesta emitida por la OTI, y la conclusión para cada uno de los numerales se encuentra a continuación:

- **D01 Documento de la herramienta de autodiagnóstico.**

  La Oficina de Control Interno (OCI) realizó la revisión y análisis de las respuestas remitidas por la Oficina de Tecnologías de la Información (OTI) frente a las situaciones evidenciadas, precisando que, si bien se presentan aclaraciones y precisiones por parte de la OTI, estas no desvirtúan las situaciones identificadas para el corte evaluado, por lo cual la calificación se mantiene, conforme se expone a continuación:

  - Enlace incorrecto: La OTI confirma la existencia de omisiones o errores en el diligenciamiento de algunas rutas de enlace asociadas a las evidencias, indicando que estas obedecieron a errores de digitación. Esta situación resulta consistente con lo evidenciado por la OCI, por lo que la observación se mantiene.
  - Ausencia de documentos clave: La OTI confirma la ausencia de los documentos señalados en la observación, indicando que dicha situación fue identificada internamente como brechas de cumplimiento e incorporada en la planeación estratégica de la vigencia 2026 y en el Plan de Seguridad y Privacidad de la Información (PESI).
  - Formalización de la Declaración de Aplicabilidad: La OTI manifiesta que la ausencia del documento obedece al proceso de transición hacia la norma ISO/IEC 27001:2022, precisando que actualmente se encuentra en elaboración un borrador para su posterior aprobación, hecho que ratifica lo evidenciado por la OCI.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

- **Implementación de componentes críticos:**

  a. Continuidad del negocio:

  La OTI indica que durante la vigencia 2025 se estructuró el Plan de Continuidad de TI y que este se encuentra operativo. No obstante, la OCI evidenció que el documento aportado corresponde al *"Plan de Preparación de TI para la Continuidad del Negocio"* de la vigencia 2020 y no el del 2025. El documento aportado presenta debilidades o ausencia en talas clave como procedimientos detallados de respuesta y recuperación, el plan de recuperación de desastres (DRP), resultados documentados del análisis de impacto al negocio (BIA), definición de roles, plan de comunicaciones, escenarios de contingencia e inventarios de recursos críticos. Adicionalmente, varias actividades clave del plan se encuentran en estado "no iniciadas" de acuerdo con lo descrito en los soportes aportados, lo cual dificulta verificar su operatividad.

  b. Gestión de proyectos:

  La OTI informa que la guía de gestión de proyectos fue actualizada incorporando aspectos de seguridad de la información; sin embargo, al encontrarse en trámite de aprobación, no se evidencia su implementación efectiva al momento de la auditoría, razón por la cual la observación se mantiene.

  c. Indicadores del MSPI y seguimiento:

  La OTI señala que cuenta con indicadores gestionados a través de la herramienta STRATEGOS y que estos se encuentran en proceso de actualización conforme a la Resolución 2277 de 2025. No obstante, la OCI generó la observación enfocada en que los indicadores actuales no permiten evaluar de manera integral la efectividad del Sistema de Gestión de Seguridad de la Información, debido a que están orientados principalmente al seguimiento de planes. En este sentido, se mantiene la observación relacionada con la necesidad de fortalecer su alcance, incorporando métricas operativas asociadas a la gestión de riesgos, incidentes, vulnerabilidades, controles de acceso y eficacia de los controles de la norma.

- **P01 / P14 Alcance MSPI**

  En cuanto el Alcance del MPSI, la información inicialmente aportada durante la fase de ejecución de la auditoría fueron documentos con actividades, cronogramas, responsables y avances del MSPI; los cuales no definen el alcance del modelo, por lo cual se solicita que la información solicitada sea remitida en los tiempos establecidos para ser evaluados correctamente. Ahora bien, analizando el alcance establecido en el Compendio de Políticas Complementarias, este incorpora de manera adecuada varios elementos fundamentales para la definición del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) en el marco del MSPI, al incluir la cobertura de todos los procesos institucionales (estratégicos, misionales, de apoyo y de evaluación), así como las dependencias de la entidad. Igualmente, contempla la participación de terceros y proveedores, abarca la información en todos sus formatos, medios y ubicaciones, y extiende su aplicabilidad a usuarios internos y externos. En este sentido, el enfoque adoptado se encuentra alineado con el principio de cobertura integral del SGSI/MSPI, al reconocer la seguridad de la información como un elemento transversal a toda la organización.

  No obstante, el alcance presenta debilidades que limitan su completitud según las buenas prácticas de MinTIC e ISO 27001. En particular, no define de manera explícita los límites del sistema, es decir, qué está incluido y qué eventualmente podría estar excluido, ni establece exclusiones justificadas; lo anterior teniendo en cuenta que el alcance documentado hace referencia a la declaración de aplicabilidad, pero a la fecha este documento no se encuentra formalizado en la UAEGRTD. Asimismo, no identifica los activos, procesos, sistemas o servicios críticos del negocio que deben ser priorizados dentro del SGSI. Tampoco delimita con precisión las fronteras tecnológicas y físicas (infraestructura específica, ambientes o sedes), ni actualiza la referencia normativa a ISO 27001:2022, lo cual constituye una observación a ser atendida en la actualización que está realizando la OTI a esta documentación. Por lo anterior, la OCI procede a ajustar la calificación de este numeral, el cual pasa de "No cumple", a "Observaciones".

PROCESO O ACTIVIDAD AUDITADA	Modelo de Seguridad y Privacidad de la Información - MSPI	NÚMERO HALLAZGO	01

- **P05 Procedimiento de inventario y Clasificación de la Información e infraestructura crítica**

  La Oficina de Control Interno (OCI), en la evaluación inicial, informó que la Entidad cuenta con una metodología y un formato para la gestión de activos de información, específicamente la Matriz de Activos de Información (MAI), identificando como observación la ausencia de un procedimiento formal, planteada a manera de recomendación para analizar la conveniencia de fortalecer la operatividad del diligenciamiento del instrumento. Lo anterior, considerando que las buenas prácticas del MSPI e ISO 27001 establecen la necesidad de asegurar la adecuada interpretación, uso y consistencia de la información documentada mediante lineamientos claros. No obstante, teniendo en cuenta la respuesta de la Oficina de Tecnologías de la Información (OTI), se reevaluó que el instrumento MAI (GT-FO-45) fue actualizado e incorpora un instructivo técnico que define los criterios para su diligenciamiento, el cual fue socializado a los enlaces de los procesos de la entidad. En este sentido, y bajo el entendido de que tanto la metodología como el formato resultan claros, y que su diligenciamiento se realiza con el acompañamiento permanente de la OTI conforme a la periodicidad definida para su actualización, se considera que la ausencia de un procedimiento independiente puede ser razonablemente subsanada. En consecuencia, la observación se acoge y se ajusta la calificación del requisito de “Observaciones” a “Cumple”.

- **P09 / P20 Declaración de Aplicabilidad**

  Se confirma que el documento proyectado de la Declaración de Aplicabilidad no ha sido presentado al Comité de Gestión y Desempeño, por lo cual la calificación presentada se mantiene.

- **O01 PESI**

  La Oficina de Control Interno (OCI) analizó la respuesta emitida por la Oficina de Tecnologías de la Información (OTI) frente a la observación formulada, concluyendo que, si bien se reitera la estructura y contenido del Plan Estratégico de Seguridad de la Información (PESI) para las vigencias 2025 y 2026, no se aportan elementos adicionales que permitan aclarar que en particular, no se aportaron evidencian del desglose específico de responsables por actividad del PESI, la asignación detallada de presupuesto, ni la incorporación de soportes que den cuenta de la ejecución efectiva de los controles definidos. En consecuencia, la respuesta no desvirtúa la situación evidenciada en la auditoría, por lo que la observación se mantiene.

- **O03 Indicadores de Gestión**

  La OTI señala que cuenta con indicadores gestionados a través de la herramienta STRATEGOS y que estos se encuentran en proceso de actualización conforme a la Resolución 2277 de 2025. No obstante, la OCI generó la observación enfocada en que los indicadores actuales no permiten evaluar de manera integral la efectividad del Sistema de Gestión de Seguridad de la Información, debido a que están orientados principalmente al seguimiento de planes. En este sentido, se mantiene la observación relacionada con la necesidad de fortalecer su alcance, incorporando métricas operativas asociadas a la gestión de riesgos, incidentes, vulnerabilidades, controles de acceso y eficacia de los controles de la norma.

- **E01 Hoja de Vida Indicadores**

  En el concepto emitido por la Oficina de Control Interno (OCI) se formuló una observación relacionada con el “Informe de Autodiagnóstico 2025” del Modelo de Seguridad y Privacidad de la Información, aportado como soporte, el cual se encuentra en estado de borrador, al no evidenciarse una fecha formal de aprobación. En consecuencia, no se acredita la formalización del hito requerido para este numeral, correspondiente al “Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos”. Dicha situación no fue subsanada en la respuesta final emitida por el proceso auditado, razón por la cual la observación se mantiene.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**01**

- **E03 Revisión a la Implementación**

  Se aclara que, el informe aportado avala una Revisión por la Dirección, en el cual se presenta un análisis estructurado del contexto, liderazgo, planificación, operación y seguimiento del subsistema de seguridad de información, y que este incorpora la evaluación del desempeño mediante el análisis de planes (PESI y PTRSI), riesgos identificados, indicadores de gestión y resultados alcanzados durante el periodo evaluado. Lo que no evidencia el documento de manera explícita es, la definición, seguimiento ni ejecución de compromisos derivados de la Revisión por la Dirección. En particular, no se identifican decisiones formales adoptadas por la alta dirección, acciones concretas con responsables y plazos definidos, ni mecanismos de trazabilidad que permitan verificar el cumplimiento de compromisos establecidos. Esta observación se mantiene debido a que el hito de este numeral solicita evidencia de “Compromisos de la Revisión por la Dirección”. Por lo anterior la calificación se mantiene.

- **M02 Plan Anual de Mejoras MSPI**

  La observación inicial se fundamentó en los soportes suministrados por la OTI a través del repositorio de SharePoint, en los cuales se evidenciaban el Plan Estratégico de Seguridad de la Información (PESI) correspondiente a la vigencia 2025 y la proyección general del plan de trabajo asociada al PESI y al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para esa misma vigencia. No obstante, una vez analizada la respuesta de la OTI y verificada la actualización del PESI para la vigencia 2026, se evidencia que este incorpora de manera general elementos orientados a la mejora del SGSI, incluyendo la gestión de hallazgos derivados de auditorías internas y externas, así como la consideración de observaciones y recomendaciones como insumo para planes de mejoramiento, y la definición de actividades para el cierre de brechas identificadas en el autodiagnóstico y el análisis de riesgos. En este sentido, al evidenciarse el cumplimiento del hito asociado al numeral evaluado, correspondiente a la definición de un plan que contemple estos aspectos, se procede a ajustar la calificación de “Observaciones” a “Cumple”.

En virtud de lo expuesto, las respuestas emitidas por el proceso auditado no aportan elementos suficientes que permitan desvirtuar las situaciones evidenciadas durante la auditoría, razón por la cual el hallazgo se ratifica, en procura de establecer acciones que den cobertura a la totalidad de situaciones identificadas y susceptibles de mejora.

De acuerdo con lo anterior, y conforme los lineamientos establecidos en la Guía para formulación y seguimiento de planes de mejoramiento (MC-GU-05), el líder del proceso deberá adelantar la formulación del plan de mejoramiento en un plazo máximo de diez (10) días hábiles. Es importante indicar, que el proceso, además de determinar las acciones preventivas que permitan atacar la causa raíz de la situación evidenciada, podrá determinar dentro del alcance del plan, las correcciones, cuando estas procedan.

SUSCRIPCIÓN			
OFICINA DE CONTROL INTERNO		**PROCESO O ACTIVIDAD AUDITADA**	
Socializado o comunicado por		**Respondido por**	
Nombre(s) y Apellido(s):	**Carlos Alberto Quiñones Cárdenas**	**Nombre(s) y Apellido(s):**	**Cesar Augusto Caro Amaya**
Cargo y/o Rol:	Líder de auditoría, Oficina de Control Interno	**Cargo y/o Rol:**	Oficial de Seguridad de la Información / OTI
Fecha:	26-jun-2026	**Fecha:**	24-jun-2026

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

RESPONSABLE (S) DEL PROCESO O ACTIVIDAD AUDITADA	**Carlos Alberto de la Ossa Hurtado** – *Jefe de la Oficina de Tecnología de la Información*	**FECHA DEL REPORTE DEL HALLAZGO**	26/06/2026
COPIA DEL REPORTE DIRIGIDO A	**César Augusto Caro Amaya** - *Oficina de Tecnologías de la Información* **Silvia Juliana González Palomino** - *Oficina de Tecnologías de la Información*	**HALLAZGO RECURRENTE**	NO
AUDITOR(ES) RESPONSABLE(S)	**Carlos Alberto Quiñones Cárdenas -** *Contratista, rol Líder de Auditoría*		

OBJETIVO(S) DEL PAPEL DEL TRABAJO

1) Informar al(los) responsable(s) de la(s) unidad(es) auditada(s) acerca de los hallazgos identificados en el transcurso de la auditoría.
2) Recibir la retroalimentación por parte del(los) responsable(s) de la(s) unidad(es) auditada(s) frente a las situaciones evidenciadas para determinar si estas se mantienen en firme.

ESPACIO EXCLUSIVO PARA EL AUDITOR

TÍTULO DEL HALLAZGO

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.

DESCRIPCIÓN DE LA 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.

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
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)	**Cumple**	Ninguna
2	Misión	**Cumple**	Ninguna

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.	**Cumple**	Ninguna
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.
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	**Cumple**	Ninguna
6	Políticas de seguridad de la información formalizada y firmada	**Cumple**	Ninguna
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	**Cumple**	Ninguna
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección	**Cumple**	Ninguna
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	**Cumple**	Ninguna
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.
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	**Cumple**	Ninguna
12	Procedimientos de control documental del MSPI	**Cumple**	Ninguna
13	Metodología de Gestión de riesgos	**Cumple**	Ninguna
14	Riesgos identificados y valorados de acuerdo con la metodología	**Cumple**	Ninguna
15	Planes de tratamiento de los riesgos	**Cumple**	Ninguna
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	**Cumple**	Ninguna

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad	**Cumple**	Ninguna
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	**Cumple**	Ninguna
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información	**Cumple**	Ninguna
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección	**Cumple**	Ninguna
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.
25	Formato de acuerdo de transferencia de información	**Cumple**	Ninguna

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA			
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.
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	**Cumple**	Ninguna
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
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.	**Cumple**	Ninguna

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA			
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
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	**Cumple**	Ninguna
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			

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

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
39	Documento con el plan de auditorías internas y resultados, de acuerdo con lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	**Cumple**	Ninguna
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.

CRITERIOS ASOCIADOS *(FUNDAMENTO LEGAL, NORMATIVO, PROCEDIMENTAL, ETC)*

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."*

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

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 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).

CAUSA(S) PROBABLE(S)	**POSIBLES IMPACTOS**
▪ Ausencia de criterios estandarizados que definan qué constituye un soporte válido y suficiente para cada numeral del instrumento. ▪ Inadecuada organización, actualización o disponibilidad de los documentos que respaldan la información reportada. ▪ Debilidad en procesos de revisión previa que garanticen la calidad, consistencia y completitud de la información que soporta los numerales del instrumento.	▪ La información incompleta o no soportada puede afectar la confiabilidad del autodiagnóstico, limitando la toma de decisiones estratégicas en seguridad de la información. ▪ La ausencia o debilidad de evidencias puede generar sobreestimación o subestimación del nivel real de implementación del modelo. ▪ Posibles desviaciones frente a los requisitos establecidos por MinTIC y el MSPI.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

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.

ESPACIO EXCLUSIVO PARA EL RESPONSABLE DEL PROCESO O ACTIVIDAD AUDITADA

RESPUESTA DEL PROCESO O ACTIVIDAD AUDITADA:

4. Mapa de Procesos
Con respecto a la observación formulada del Autodiagnóstico 2025, se aclara que la omisión de algunas rutas de enlace en la columna de observaciones correspondió un evento casual de mecanografía que no generó impacto ni incidencia en la evaluación final. Lo anterior se sustenta en que el documento soporte se encontraba plenamente identificado en la columna "Nombre del Documento Entregado", demostrando que las evidencias existen y fueron consideradas correctamente para el cálculo del resultado. (Evidencia Prueba 6)

10. Estratificación
Con respecto al hallazgo, se aclara que se cuenta con la Estratificación vigente. (Evidencia Prueba 6)

21. Inventario Áreas de Procesamiento
Con respecto al hallazgo, se aclara que fue identificado en la realización del autodiagnóstico 2025, lo cual fue solicitado al subdominio de Servicios.

23. Seguridad de la Información en Gestión de Proyectos
El dominio de Estrategia y Gobierno de TI lideró la actualización técnica de la Guía para la Gestión de Proyectos de TI (GT-GU-14) durante la vigencia 2025, integrando la Seguridad de la Información. Actualmente, dicho documento está en trámite ante la Oficina Asesora de Planeación para su formalización/publicación respectiva.
24. Inventario de Externos a los Que se Transfiere Información
Se cuenta con un inventario de partes externas o terceros a los que se transfiere información, Acuerdos_Convenio_OTI, ANEXO TECNICO1524_URT_UARIV, Lista de partes externas.

26. Inventario de Proveedores con Acceso a activos de Información
El inventario solicitado se encuentra en una base de proveedores con acceso a Activos de Información y fue suministrado como parte de la información requerida.

28. Plan de Continuidad

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

Durante la vigencia 2025 la Oficina de Tecnologías de la Información diseñó y estructuró de manera integral el Plan de Continuidad de TI. Este instrumento articuló de forma transversal todos los subdominios tecnológicos bajo el liderazgo de Seguridad de la Información, garantizando así la protección operativa de la infraestructura. Por lo tanto, se evidencia que el componente no presenta un vacío de implementación, por el contrario, se encuentra plenamente documentado y operativo conforme a las necesidades de la Entidad.

29. Inventario Obligaciones Legales
En el normograma publicado en Strategos se incluye la resolución 500 de 2021, la resolución 2277 de 2025 está en proceso de actualización la cual se está articulando con la Dirección Jurídica.

30. Auditoría Relacionadas a Seguridad de la Información
Los seguimientos de Gobierno Digital del periodo 2025 fueron consolidados y publicados formalmente. Dichos informes se encuentran disponibles para su consulta y verificación.

32. Indicadores y Métricas de Seguridad de Información
La entidad cuenta con un esquema activo de medición, por lo cual los indicadores del MSPI son reportados y gestionados de manera regular a través de la plataforma institucional STRATEGOS (ruta: ESTRATEGIA/INDICADORES/REPORTES/REPORTE INDICADORES/ SEGURIDAD), desvirtuando la existencia de un vacío en esta materia. No obstante, en un esfuerzo de alineación normativa y mejora continua bajo el marco de la Resolución 2277 de 2025, en el proceso de implementación de la resolución se vienen adoptando nuevos indicadores conforme lo dispone Gobierno Digital.

33. Declaración de Aplicabilidad
Con relación a la falta de aprobación formal de la Declaración de Aplicabilidad por parte de la Alta Dirección, se aclara que esta situación obedeció al proceso estratégico de transición y actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) de la norma ISO/IEC 27001:2013 a la nueva estructura de controles de la versión 2022; cambio normativo y metodológico que requirió una fase técnica previa de alineación y diagnóstico, razón por la cual el documento actualizado se encuentra actualmente proyectado y en circuito de revisión para su correspondiente aprobación formal en la presente vigencia.

35. Planificación y Control Operacional
La entidad cuenta con el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), el cual fue formalmente presentado y aprobado por el Comité Interinstitucional.

36. Ejecución Plan de Tratamiento de Riesgos
La entidad cuenta con un esquema activo de medición, por lo cual los indicadores del MSPI son reportados y gestionados de manera regular a través de la plataforma institucional STRATEGOS (ruta: ESTRATEGIA/INDICADORES/REPORTES/REPORTE INDICADORES/ SEGURIDAD), no hay un vacío en esta materia. No obstante, en un esfuerzo de alineación normativa y mejora continua bajo el marco de la Resolución 2277 de 2025, en el proceso de implementación de la resolución se vienen adoptando nuevos indicadores conforme lo dispone Gobierno Digital.

37. Indicadores de Gestión MSPI
Se precisa que la entidad cuenta con un esquema activo de medición, por lo cual los indicadores del MSPI son reportados y gestionados de manera regular a través de la plataforma institucional STRATEGOS (ruta: ESTRATEGIA/INDICADORES/REPORTES/REPORTE INDICADORES/ SEGURIDAD), desvirtuando la existencia de un vacío en esta materia. No obstante, en un esfuerzo de alineación normativa y mejora continua bajo el marco de la Resolución 2277 de 2025, en el proceso de implementación de la resolución se vienen adoptando nuevos indicadores conforme lo dispone Gobierno Digital.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

38. Plan de Seguimiento MSPI
La entidad cuenta con un esquema activo de medición, por lo cual los indicadores del MSPI son reportados y gestionados de manera regular a través de la plataforma institucional STRATEGOS (ruta: ESTRATEGIA/INDICADORES/REPORTES/REPORTE INDICADORES/ SEGURIDAD). Se adelantan además seguimientos periódicos en el marco de Gobierno y Transformación Digital al interior de la OTI.

40. Resultado del Seguimiento al Plan de Tratamiento De Riesgos
Se cuenta con el consolidado de reporte de auditorías anteriores que se encuentra publicado en la herramienta de Strategos.

41. Plan de Seguimiento MSPI
La entidad cuenta con el autodiagnóstico que brinda un grado de avance exacto en la implementación de los lineamientos y controles exigidos por el Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.

42. Consolidado de Auditorías Realizadas
Se cuenta con el consolidado de reporte de auditorías anteriores que se encuentra publicado en la herramienta de Strategos.

CONCEPTO DE LA OFICINA DE CONTROL INTERNO	NO DESVIRTUADO

La Oficina de Control Interno precisa que la evaluación efectuada, de conformidad con el alcance del proceso auditor, corresponde a la información diligenciada por la Oficina de Tecnologías de la Información en la herramienta de Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), con corte al 31 de diciembre de 2025. En este sentido, el autodiagnóstico correspondiente a la vigencia 2026 no fue objeto de evaluación por parte de la Oficina de Control Interno (OCI), debido a que, a la fecha, dicho instrumento no ha sido aportado por la OTI, toda vez que su diligenciamiento y evaluación se realizarán una vez finalice la presente vigencia.

En consecuencia, tras la revisión de la respuesta emitida por la OTI frente a lo observado y descrito en el presente documento, la Oficina de Control Interno mantiene la calificación inicial, dado que esta se fundamenta en la información evaluada con corte a la vigencia 2025. Por lo tanto, los soportes o gestiones adicionales señalados por la OTI podrán ser considerados en el diligenciamiento del instrumento correspondiente al corte 31 de diciembre de 2026, momento en el cual se evaluará la subsanación de las situaciones evidenciadas.

El detalle de la revisión a la respuesta emitida por la Oficina de Tecnologías de la Información (OTI), y la conclusión para cada uno de los numerales se encuentra a continuación:

4. Mapa de Procesos
La OTI confirma que la omisión de algunas rutas de enlace en la columna de observaciones correspondió un evento de error mecanográfico en el diligenciamiento del instrumento con corte a 31 de diciembre de 2025, por lo anterior, se recomienda adoptar medidas de prevención para su debido diligenciamiento en el proceso de autoevaluación que realice la OTI en el instrumento, con corte de la vigencia 2026.

10. Estratificación
La OTI informa que se cuenta con la Estratificación vigente, sin embargo, esto no fue diligenciado y el soporte no fue referenciado en el instrumento para el corte a 31 de diciembre de 2025. Por lo anterior, se recomienda su debido diligenciamiento para la autoevaluación que realice la OTI en el instrumento para el corte de la vigencia 2026.

PROCESO O ACTIVIDAD AUDITADA	Modelo de Seguridad y Privacidad de la Información - MSPI	NÚMERO HALLAZGO	02

21. Inventario Áreas de Procesamiento
La OTI confirma esta situación, indicando que esta información ha sido solicitada al subdominio de Servicios para su generación para 2026.

23. Seguridad de la Información en Gestión de Proyectos
La OTI informa que para la Guía para la Gestión de Proyectos de TI (GT-GU-14) se han proyectado actualizaciones desde la vigencia 2025, y que actualmente, dicho documento está en trámite de actualización ante la Oficina Asesora de Planeación para su formalización; por lo anterior, la OCI reitera la recomienda para que en dicha actualización se fortalezca 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. Lo anterior para 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 Externos a los Que se Transfiere Información
En la verificación inicial no se aportó soporte a este numeral. Si bien en la respuesta reporte preliminar 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. Adicionalmente, se reitera que la calificación obedece al diligenciamiento realizado por la OTI en el instrumento de evaluación del corte a 31 de diciembre de 2025. Por lo anterior, se recomienda su debido diligenciamiento para la autoevaluación que realice la OTI en el instrumento para el corte de la vigencia 2026.

26. Inventario de Proveedores con Acceso a activos de Información
En la verificación inicial no se aportó soporte a este numeral. Si bien en la respuesta del hallazgo se aportó como soporte un registro con la relación de tres (3) proveedores que indican tener acceso a Activos de Información, 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. Adicionalmente, se reitera que la calificación obedece al diligenciamiento realizado por la OTI en el instrumento de evaluación del corte a 31 de diciembre de 2025, por lo anterior, se recomienda su debido diligenciamiento para la autoevaluación que realice la OTI en el instrumento para el corte de la vigencia 2026.

28. Plan de Continuidad
Para este numeral, la OCI confirma que se verificó el Plan que formalmente se encuentra establecido, no obstante, la calificación obedece a que el documento presenta debilidades 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 del análisis de impacto al negocio (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 Obligaciones Legales
La OTI confirma que el normograma requiere actualización, la cual se está articulando con la Dirección Jurídica.

30. Auditoría Relacionadas a Seguridad de la Información
La calificación de este numeral hace referencia a que, en el instrumento de autodiagnóstico del MSPI con corte al 31 de diciembre de 2025, se debieron enlistar las auditorías que incluyeron evaluación al modelo de seguridad y privacidad de la información. En este sentido, se generó una observación orientada a que en la evaluación de la vigencia 2026 se incorporen las auditorías realizadas en el marco de la Estrategia de Gobierno Digital realizadas en vigencias anteriores, así como la auditoría al SRTDAF – Sistema de Registro de Tierras Despojadas y Abandonadas Forzosamente realizada en el 2025. Por lo anterior, se recomienda a la OTI subsanar esta situación en el diligenciamiento del instrumento correspondiente a la evaluación que deberá efectuarse para el corte de diciembre de 2026.

32. Indicadores y Métricas de Seguridad de Información
Respecto a este numeral, se aclara que en la evaluación se reconoce que si existen en STRATEGOS indicadores orientados al seguimiento del avance del PESI y del Plan de Tratamiento de Riesgos, pero, la observación se fundamenta en que estos se deben fortalecer toda vez que no permiten evaluar de manera integral la efectividad de los controles ni el desempeño del Sistema de Gestión de Seguridad de la Información (SGSI), al centrarse principalmente en el cumplimiento de planes y no en la medición de aspectos clave como riesgos, incidentes, vulnerabilidades, acceso y eficacia de los controles. Lo cual está alineado con la respuesta de la OTI, en la cual indica que bajo el marco de la Resolución 2277 de 2025, la OTI está proyectando adoptar nuevos indicadores conforme lo dispone Gobierno Digital.

33. Declaración de Aplicabilidad
La OTI confirma que, a la fecha, está pendiente la aprobación formal de la Declaración de Aplicabilidad por parte de la Alta Dirección.

35. Planificación y Control Operacional
Para este numeral no fue referenciado el soporte en el instrumento diligenciado del corte a 31 de diciembre de 2025. Por lo anterior, se recomienda su debido diligenciamiento para la autoevaluación que realice la OTI en el instrumento para el corte de la vigencia 2026.

36. Ejecución Plan de Tratamiento de Riesgos
Para este numeral, la OCI confirmó que si bien 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)";* 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 MSPI
Para este numeral, la OCI confirmó que si bien se cuenta con la definición del *indicador "GT-2-2025- Porcentaje de avance del plan de seguridad y privacidad de la información. PESI";* 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.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**02**

38. Plan de Seguimiento MSPI
Para este numeral no fue referenciado el soporte en el instrumento diligenciado del corte a 31 de diciembre de 2025, por lo anterior, se recomienda su debido diligenciamiento para la autoevaluación que realice la OTI en el instrumento para el corte de la vigencia 2026.

40. Resultado del Seguimiento al Plan de Tratamiento De Riesgos
Para este numeral se requiere la presentación del resultado del seguimiento, la evaluación y el análisis de su ejecución, debidamente revisado y aprobado por la Alta Dirección. La calificación otorgada obedece a que, como evidencia, se remitió el *documento "GT-ES-14_V5 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025";* sin embargo, este corresponde únicamente a la formulación del plan y no contiene los resultados de seguimiento, evaluación ni análisis de su ejecución, conforme a lo exigido.

41. Plan de Seguimiento MSPI
Para este numeral no fue referenciado el soporte en el instrumento diligenciado del corte a 31 de diciembre de 2025, por lo anterior, se recomienda su debido diligenciamiento para la autoevaluación que realice la OTI en el instrumento para el corte de la vigencia 2026.

42. Consolidado de Auditorías Realizadas
Este numeral requería el diligenciamiento de un consolidado que incluyera las auditorías realizadas, los hallazgos u oportunidades de mejora identificadas y los respectivos planes de mejoramiento definidos para su tratamiento. No obstante, como soporte se referenció el Plan Estratégico de Seguridad de la Información (PESI), el cual no contiene ni detalla la información solicitada, por lo que no permite evidenciar el cumplimiento del requisito.

En virtud de lo expuesto, las respuestas emitidas por el proceso auditado no aportan elementos suficientes que permitan desvirtuar las situaciones evidenciadas durante la auditoría, razón por la cual el hallazgo se ratifica, en procura de establecer acciones que den cobertura a la totalidad de situaciones identificadas y susceptibles de mejora.

De acuerdo con lo anterior, y conforme los lineamientos establecidos en la Guía para formulación y seguimiento de planes de mejoramiento (MC-GU-05), el líder del proceso deberá adelantar la formulación del plan de mejoramiento en un plazo máximo de diez (10) días hábiles. Es importante indicar, que el proceso, además de determinar las acciones preventivas que permitan atacar la causa raíz de la situación evidenciada, podrá determinar dentro del alcance del plan, las correcciones, cuando estas procedan.

SUSCRIPCIÓN			
OFICINA DE CONTROL INTERNO		**PROCESO O ACTIVIDAD AUDITADA**	
Socializado o comunicado por		**Respondido por**	
Nombre(s) y Apellido(s):	**Carlos Alberto Quiñones Cárdenas**	**Nombre(s) y Apellido(s):**	**Cesar Augusto Caro Amaya**
Cargo y/o Rol:	Líder de auditoría, Oficina de Control Interno	**Cargo y/o Rol:**	Oficial de Seguridad de la Información / OTI
Fecha:	26-jun-2026	**Fecha:**	24-jun-2026

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

RESPONSABLE (S) DEL PROCESO O ACTIVIDAD AUDITADA	**Carlos Alberto de la Ossa Hurtado** – *Jefe de la Oficina de Tecnología de la Información*	**FECHA DEL REPORTE DEL HALLAZGO**	26/06/2026
COPIA DEL REPORTE DIRIGIDO A	**César Augusto Caro Amaya** - *Oficina de Tecnologías de la Información* **Silvia Juliana González Palomino** - *Oficina de Tecnologías de la Información*	**HALLAZGO RECURRENTE**	NO
AUDITOR(ES) RESPONSABLE(S)	**Carlos Alberto Quiñones Cárdenas -** *Contratista, rol Líder de Auditoría*		

OBJETIVO(S) DEL PAPEL DEL TRABAJO

1) Informar al(los) responsable(s) de la(s) unidad(es) auditada(s) acerca de los hallazgos identificados en el transcurso de la auditoría.
2) Recibir la retroalimentación por parte del(los) responsable(s) de la(s) unidad(es) auditada(s) frente a las situaciones evidenciadas para determinar si estas se mantienen en firme.

ESPACIO EXCLUSIVO PARA EL AUDITOR

TÍTULO DEL HALLAZGO

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.

DESCRIPCIÓN DE LA 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.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

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.

Resumen del resultado obtenido:

Tabla No. 1. 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

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

1	Controles organizacionales	Anexo A 5.2	Roles y responsabilidades de seguridad de la información	Establecer y mantener mecanismos adecuados para funciones y responsabilidades 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.	Efectivo
2		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
3		Anexo A 5.12	Clasificación de la información	Establecer y mantener mecanismos adecuados para clasificación 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.	Efectivo
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
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	Controles de personas	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
9		Anexo A 6.2	Términos y condiciones de empleo	Establecer y mantener mecanismos adecuados para términos y condiciones de empleo 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.	Efectivo
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

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

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	Controles Tecnológicos	Anexo A 8.6	Gestión de capacidad	Establecer y mantener mecanismos adecuados para gestión de capacidad 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
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
21		Anexo A 8.20	Seguridad en redes	Establecer y mantener mecanismos adecuados para seguridad 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.	Efectivo
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

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

DESCRIPCIÓN DE LA SITUACIÓN EVIDENCIADA

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.

CRITERIOS ASOCIADOS *(FUNDAMENTO LEGAL, NORMATIVO, PROCEDIMENTAL, ETC)*

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.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

CRITERIOS ASOCIADOS *(FUNDAMENTO LEGAL, NORMATIVO, PROCEDIMENTAL, ETC)*

- 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 de 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.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

CRITERIOS ASOCIADOS *(FUNDAMENTO LEGAL, NORMATIVO, PROCEDIMENTAL, ETC)*

- 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 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.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

RIESGOS ASOCIADOS
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.

CAUSA(S) PROBABLE(S)	**POSIBLES IMPACTOS**
▪ Enfoque predominante normativo/documental con debilidades en el desarrollo operativo de los controles. ▪ Falta de procedimientos detallados, metodologías y lineamientos técnicos específicos. ▪ Debilidades en la gestión documental y trazabilidad de evidencias. ▪ Insuficiencia de mecanismos de monitoreo, seguimiento y control continuo. ▪ Falta de estandarización institucional en la implementación de controles. ▪ Debilidades en la cultura organizacional de seguridad de la información.	▪ Afectación a la disponibilidad y continuidad de los servicios tecnológicos, por problemas de capacidad, infraestructura o incidentes. ▪ Debilidad en la capacidad de respuesta ante incidentes, así como en su análisis y aprendizaje organizacional. ▪ Incumplimiento de lineamientos del MSPI y de la ISO 27001:2022, con posibles impactos en evaluaciones externas. ▪ Limitaciones en la toma de decisiones, por falta de información confiable sobre el estado del SGSI.

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

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.
- 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.

ESPACIO EXCLUSIVO PARA EL RESPONSABLE DEL PROCESO O ACTIVIDAD AUDITADA

RESPUESTA DEL PROCESO O ACTIVIDAD AUDITADA:

No se recibieron observaciones dentro del plazo establecido.

CONCEPTO DE LA OFICINA DE CONTROL INTERNO	NO DESVIRTUADO

En atención al proceso auditor adelantado por la Oficina de Control Interno (OCI), el hallazgo denominado *"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",* fue comunicado a la Oficina de Tecnologías de la Información (OTI) en su versión preliminar el 22 de junio de 2026, para que fuera objeto de análisis y presentación de respuesta que pudiera desvirtuar lo observado, no obstante, cumplido el plazo otorgado para ello no hubo pronunciamiento por parte de la OTI, por lo cual, el hallazgo se mantiene en firme y será incorporado en el informe final de auditoría, junto con los resultados obtenidos respecto a la implementación, adecuación y efectividad de los controles evaluados, en virtud de lo establecido en el procedimiento CI-PR-07 "Ejecución de Trabajos de Aseguramiento y Comunicación de Resultados", versión 1, que en su actividad 14, establece:

"Nota: En caso de no recibir respuesta al hallazgo por parte del(los) responsables del proceso o actividad auditada dentro del plazo establecido, se considera en firme el mencionado hallazgo y, por tanto, el mismo debe ser objeto de tratamiento mediante la suscripción de un Plan de Mejoramiento que debe ser formulado en virtud de lo dispuesto en la "MC-GU-05 Guía para Formulación y Seguimiento de Planes de Mejoramiento"".

PROCESO O ACTIVIDAD AUDITADA	**Modelo de Seguridad y Privacidad de la Información - MSPI**	**NÚMERO HALLAZGO**	**03**

De acuerdo con lo anterior, y conforme los lineamientos establecidos en la Guía para formulación y seguimiento de planes de mejoramiento (MC-GU-05), el líder del proceso deberá adelantar la formulación del plan de mejoramiento en un plazo máximo de diez (10) días hábiles. Es importante indicar, que el proceso, además de determinar las acciones preventivas que permitan atacar la causa raíz de la situación evidenciada, podrá determinar dentro del alcance del plan, las correcciones, cuando estas procedan.

SUSCRIPCIÓN			
OFICINA DE CONTROL INTERNO		**PROCESO O ACTIVIDAD AUDITADA**	
Socializado o comunicado por		**Respondido por**	
Nombre(s) y Apellido(s):	**Carlos Alberto Quiñones Cárdenas**	**Nombre(s) y Apellido(s):**	No Aplica
Cargo y/o Rol:	Líder de auditoría, Oficina de Control Interno	**Cargo y/o Rol:**	No Aplica
Fecha:	26-jun-2026	**Fecha:**	No Aplica