INSTITUTO COLOMBIANO AGROPECUARIO - ICA
OFICINA CONTROL INTERNO
PROCEDIMIENTO EVALUACION Y SEGUIMIENTO
PLAN DE MEJORAMIENTO AUDITORIA OFICINA CONTROL INTERNO

Fecha de auditoria: 27/02/2026 al 30/06/2026

NÚMERO DE OBSERVACIÓN DENTRO DEL INFORME	NÚMERO ACCIÓN DE MEJORA	PROCESO / SUPROCESO / PROCEDIMIENTO	DESCRIPCION OBSERVACIÓN	DESCRIPCION RECOMENDACIÓN	AREA RESPONSABLE	DETERMINACIÓN DE LA CAUSA	ACCION DE MEJORAMIENTO	RESPONSABLES	FECHA INICIO	FECHA TERMINACIÓN	DESCRIPCION DEL AVANCE - AREA AUDITADA	EVIDENCIA - AREA AUDITADA	PORCENTAJE DE CUMPLIMIENTO - AREA AUDITADA	PORCENTAJE DE CUMPLIMIENTO OCI	ESTADO - OCI	OBSERVACIÓN - OCI	AREA AUDITADA	VIGENCIA
1	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Evidencia insuficiente sobre la formalización y trazabilidad de los roles operativos de seguridad de la información. Como resultado de la revisión del componente A2 —Roles y responsabilidades OTI—, se identificó que la Oficina de Tecnologías de la Información cuenta con funciones asociadas a la seguridad de la información, gestión de accesos, gestión de vulnerabilidades, copias de respaldo, gestión de incidentes, monitoreo, continuidad y supervisión contractual. Sin embargo, la evidencia aportada no permite verificar una matriz formal, vigente, integral y trazable que asigne responsabilidades específicas por control, actividad, dominio o componente del SGSI/MSPI. La información revisada evidencia una asignación funcional de responsabilidades por grupos o perfiles; no obstante, no se observa con suficiente claridad quién es responsable de ejecutar, aprobar, revisar, monitorear, escalar y reportar cada control relacionado con la Política GIT-PTI-POL-001 V.3. Tampoco se evidenciaron suplencias, periodicidad de seguimiento, autoridad asignada, mecanismo de rendición de cuentas, evidencia esperada por actividad ni relación directa entre los responsables definidos y los controles de la política. Esta situación limita la trazabilidad del gobierno de seguridad de la información, especialmente en componentes críticos como accesos, cuentas privilegiadas, vulnerabilidades, respaldos, logs, incidentes, continuidad, contratos y cumplimiento normativo. Desde el enfoque de auditoría basada en riesgos, un control puede existir documentalmente, pero su efectividad se dificulta cuando no se identifica de manera clara quién responde por su ejecución, seguimiento y mejora.	Formalizar una matriz integral de roles y responsabilidades de seguridad de la información, asociada a la Política GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información, el MSPI y a los controles aplicables de la NTC/ISO 27001. Esta matriz debería incluir, como mínimo: proceso o dominio de control, actividad, responsable funcional, responsable operativo, responsable de aprobación, suplente, periodicidad de ejecución, evidencia esperada, mecanismo de seguimiento, ruta de escalamiento y relación con los riesgos institucionales aplicables. Adicionalmente, se recomienda actualizar dicha matriz periódicamente y socializarla con los responsables asignados, de forma que exista trazabilidad entre el control definido, el responsable de ejecución, la evidencia generada y el seguimiento realizado.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	El capítulo de funciones, roles y responsabilidades se encuentra contenido en el Manual del Sistema de Gestion de Seguridad de la Información - SGSI. No obstante, no se contaba con un documento independiente que detallara y ampliara las funciones asociadas a cada uno de los roles.	Construir y formalizar la matriz de roles y responsabilidades, tomando como referencia la Declaración de Aplicabilidad y el documento de descripción de roles, con el fin de consolidar en un único instrumento institucional las funciones y responsabilidades asociadas al Sistema de Gestion de Seguridad de la Información - SGSI.	Equipo de Gestión Estratégica y Seguridad de Información TI.	1/09/2026	18/12/2026							Oficina de Tecnologías de Información	2026
2	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Soporte documental insuficiente para evidenciar la actualización de la Declaración de Aplicabilidad y del registro de excepciones en concordancia con el MSPI vigente. En el componente A3 —Registro de excepciones—, se aportó como evidencia la Declaración de Aplicabilidad 2023. No obstante, no se evidenció un registro consolidado de excepciones, exclusiones, dispensas o aceptaciones de riesgo frente a la Política GIT-PTI-POL-001 V.3 para el período evaluado 2022–2025. Tampoco se identificó evidencia suficiente de actualización de la declaración de aplicabilidad frente al marco vigente del MSPI actualizado por la Resolución 2277 de 2025 del MinTIC, ni frente a los controles aplicables de la NTC/ISO 27001 bajo la versión vigente aplicable al modelo. Esta condición es relevante porque la declaración de aplicabilidad debe permitir determinar qué controles son aplicables, cuáles no, cuál es la justificación de exclusión, quién aprueba dicha decisión, qué controles compensatorios existen y cómo se realiza el seguimiento. La existencia de una declaración de aplicabilidad correspondiente a 2023 constituye un insumo relevante; sin embargo, por sí sola no permite verificar que el SGSI/MSPI haya sido actualizado y ajustado frente al marco normativo vigente para 2025, ni que las excepciones o no aplicabilidades hayan sido formalmente justificadas, aprobadas y monitoreadas durante todo el período auditado.	Actualizar la declaración de aplicabilidad del SGSI/MSPI, incorporando la trazabilidad frente a la Política GIT-PTI-POL-001 V.3, el MSPI actualizado, la Resolución 2277 de 2025 y los controles aplicables de la NTC/ISO 27001. Esta actualización debería incluir: control, aplicabilidad, justificación, evidencia asociada, responsable, estado de implementación, exclusiones, controles compensatorios, aceptación de riesgos y aprobación correspondiente. De igual forma, se recomienda implementar y mantener un registro formal de excepciones, dispensas, exclusiones o aceptaciones de riesgo frente a la política y los controles de seguridad, indicando fecha, sistema o proceso afectado, justificación, riesgo asociado, vigencia, responsable, aprobador y controles compensatorios.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	No se habia presentado al Comité Institucional de Gestión y Desempeño la Declaración de Aplicabilidad del Gestión de Seguridad de la Información - SGSI / Modelo de Seguridad y Privacidad de la Información - MSPI, actualizada a la versión NTC/ISO 27001:2022, ni se contaba con un instrumento de seguimiento.	Presentar la Declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información - SGSI/ Modelo de Seguridad y Privacidad de la Información - MSPI, actualizada de conformidad con la versión NTC/ISO 27001:2022, para su aprobación por parte del Comité Institucional de Gestión y Desempeño, junto con la matriz de seguimiento de excepciones, exclusiones, dispensas y aceptaciones de riesgo.	Equipo de Gestión Estratégica y Seguridad de Información TI.	1/09/2026	18/12/2026							Oficina de Tecnologías de Información	2026
3	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	No se evidenció la actualización anual de la matriz de activos de información para las vigencias 2024 y 2025. Para el componente D1 —Matriz de activos de información—, se aportó una matriz correspondiente a la vigencia 2023. Adicionalmente, se recibieron inventarios tecnológicos, catálogos de sistemas, servicios y servidores. Estos soportes permiten evidenciar que la OTI cuenta con información base sobre activos, servicios y componentes tecnológicos; sin embargo, no se aportaron versiones actualizadas de la matriz de activos de información para las vigencias 2024 y 2025, ni una versión vigente que demuestre actualización anual. La Política GIT-PTI-POL-001 V.3 establece la necesidad de identificar y clasificar los activos de información, así como mantener actualizada la matriz correspondiente. En ese sentido, la matriz de activos debe permitir reconocer el activo, propietario, custodio, clasificación, criticidad, ubicación, sistema asociado, fecha de actualización y demás atributos requeridos para aplicar controles proporcionales al nivel de sensibilidad, criticidad y exposición de la información. La evidencia aportada permite verificar la existencia de una matriz 2023; sin embargo, no permite concluir que durante 2024 y 2025 se haya realizado actualización, revisión, clasificación, rotulado o validación de cambios de los activos de información. Esta condición limita la capacidad de la auditoría para verificar si los controles de confidencialidad, integridad, disponibilidad, retención, respaldo, acceso y tratamiento se aplican sobre una base de activos vigente.	Actualizar y formalizar la matriz de activos de información para las vigencias 2024, 2025 y la vigencia actual, incorporando como mínimo: nombre del activo, descripción, propietario, custodio, clasificación, criticidad, ubicación, repositorio o sistema asociado, tratamiento de datos personales si aplica, controles asignados, fecha de última actualización y responsable de validación. Se recomienda establecer un procedimiento o cronograma de actualización periódica que permita evidenciar revisión anual, cambios en activos, nuevas adquisiciones, retiro de activos, reclasificaciones y validación por los propietarios de la información.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	No se establecieron mecanismos formales de seguimiento y control que garantizaran la revisión, validación y actualización periódica de la matriz de activos de información despues de la vigencia 2023, situación que generó la falta de actualización de este instrumento en las vigencias posteriores.	Actualizar y formalizar anualmente la matriz de activos de información de la entidad.	Equipo de Gestión Estratégica y Seguridad de Información TI.	1/09/2026	31/07/2027							Oficina de Tecnologías de Información	2026
4	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Evidencia insuficiente de gestión integral de accesos e identidades. En el componente de gestión de accesos se aportaron solicitudes VPN y documentación asociada a cuentas privilegiadas, incluyendo procedimiento y formatos institucionales. Estos soportes permiten verificar algunos casos de acceso remoto y la existencia de un procedimiento específico para cuentas privilegiadas. Sin embargo, no se aportó evidencia suficiente para el componente E2 —Gestión de accesos—, relacionado con el ciclo completo de altas, bajas, modificaciones, autorizaciones, implementación, cierre y revisión periódica de accesos. La evidencia de solicitudes VPN no permite concluir por sí sola sobre la gestión integral de accesos a sistemas, servicios digitales, infraestructura, bases de datos, plataformas críticas o ambientes productivos. Tampoco se aportó muestra suficiente de casos completos que permitan seguir la trazabilidad desde la solicitud hasta la aprobación, creación o modificación del acceso, notificación, uso autorizado, revisión periódica y retiro cuando el acceso deja de ser necesario. Adicionalmente, no se evidenció recertificación o revisión periódica de accesos para el período evaluado. Esta verificación es necesaria para confirmar que los usuarios mantienen únicamente los privilegios requeridos, que los accesos de funcionarios, contratistas o terceros se retiran oportunamente y que no permanecen cuentas activas sin justificación vigente.	Consolidar e implementar evidencia integral de gestión de accesos, incluyendo procedimiento, matriz de perfiles, solicitudes, aprobaciones, creación, modificación, suspensión, retiro, revisión periódica y cierre de accesos. La evidencia debería permitir verificar, para cada caso, usuario, sistema, perfil, justificación, aprobador, fecha de autorización, fecha de implementación, responsable técnico y estado del acceso. Se recomienda realizar recertificaciones periódicas de accesos a sistemas críticos, cuentas privilegiadas, cuentas de servicio, VPN y accesos de terceros, dejando evidencia de revisión, ajustes, revocaciones y responsables.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	No se contaba con un mecanismo de gestión integral de accesos a sistemas, servicios digitales, Infraestructura, bases de datos, plataformas críticas o ambientes productivos.	Diseñar, implementar y adoptar una matriz institucional de gestión de accesos que consolide todo el ciclo de vida de las cuentas y los privilegios, incluyendo altas, bajas, modificaciones, autorizaciones, recertificaciones y cierres. La matriz contendrá el usuario, el sistema, el perfil asignado, la justificación, el aprobador, la fecha de autorización, la fecha de implementación, el responsable técnico y el estado del acceso.	Equipo de Gestión Estratégica y Seguridad de Información TI.	1/09/2026	31/07/2027							Oficina de Tecnologías de Información	2026
5	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	No se aportó evidencia para verificar la gestión de parches y protección contra malware. Para el componente H4 —Parches y protección Malware—, no se allegaron soportes documentales o técnicos. En consecuencia, no fue posible verificar la existencia de reportes de cumplimiento de parches, actualización de servidores y estaciones, cobertura de antimalware o EDR, tratamiento de excepciones, vulnerabilidades pendientes, responsables de remediación, fechas de cierre o seguimiento periódico. La Política GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información contempla controles orientados a la protección contra código malicioso y a la aplicación de actualizaciones de seguridad. Estos controles son esenciales para reducir la exposición a vulnerabilidades conocidas, ataques automatizados, malware, explotación de sistemas desactualizados, accesos no autorizados y afectación de la disponibilidad de servicios tecnológicos. La ausencia de evidencia no permite afirmar que el control sea inexistente; sin embargo, desde la perspectiva de auditoría, un control que no cuenta con soporte documental, reportes de ejecución, cobertura, periodicidad y seguimiento no puede considerarse demostrado. Esta situación impide evaluar la efectividad del control durante el período auditado.	Aportar, consolidar o implementar reportes periódicos de gestión de parches y protección contra malware, diferenciando servidores, estaciones de trabajo, sistemas críticos, dispositivos tecnológicos y componentes administrados por terceros. Estos reportes deberían incluir cobertura, estado de actualización, fecha del último parche, criticidad, excepciones, vulnerabilidades asociadas, responsable de remediación y fecha de cierre. Se recomienda definir una periodicidad formal de revisión, establecer indicadores de cumplimiento, documentar excepciones y relacionar la gestión de parches con los resultados de análisis de vulnerabilidades.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	No se disponia de un procedimiento formalizado ni de mecanismos de seguimiento que permitieran consolidar, verificar y conservar, de manera periódica, la evidencia relacionada con la instalación de parches y actualizaciones de seguridad.	Diseñar e implementar un procedimiento de gestión y seguimiento para los controles de actualización de seguridad y protección contra malware de los activos tecnológicos administrados por la OTI, incluyendo reportes periódicos de actualización, con indicadores de cumplimiento verificables.	Equipo de Gestión Estratégica y Seguridad de Información TI.	1/09/2026	31/07/2027							Oficina de Tecnologías de Información	2026
6	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Gestión de logs y trazabilidad sin un esquema consolidado de control y con evidencia técnica parcial. Para el componente H6 —Gestión de logs y trazabilidad—, la OTI aportó archivos de logs técnicos, evidencia de configuración de tiempo AD/NTP y documentos relacionados con monitoreo, disponibilidad y respaldo. Estos soportes evidencian la existencia de registros técnicos en algunos sistemas o componentes. Sin embargo, no se evidenció un documento consolidado que defina el esquema institucional de gestión de logs. No se identificó una matriz o procedimiento que precise, para los sistemas críticos: qué eventos se registran, dónde se almacenan, por cuánto tiempo se conservan, quién puede acceder a ellos, cómo se protege su integridad, cómo se revisan, qué eventos generan alerta, quién analiza las alertas y cómo se documentan las acciones derivadas. La existencia de archivos de logs es un elemento positivo, pero no demuestra por sí sola un control integral de trazabilidad. Para que el control sea verificable, se requiere conocer alcance, responsables, retención, protección contra alteración, acceso autorizado, revisión periódica y tratamiento de eventos. Sin esta formalización, se dificulta reconstruir incidentes, verificar acciones administrativas, soportar investigaciones internas y demostrar integridad de la evidencia técnica.	Formalizar un procedimiento o matriz de gestión de logs y trazabilidad que incluya fuentes de registro, sistemas cubiertos, eventos mínimos, ubicación de almacenamiento, responsables, retención, controles de acceso, mecanismos de protección contra alteración, sincronización horaria, revisión periódica, alertas, escalamiento y tratamiento de eventos relevantes. Se recomienda priorizar sistemas críticos, servicios digitales, infraestructura de seguridad, bases de datos, cuentas privilegiadas y componentes expuestos, y vincular esta gestión con incidentes, monitoreo, auditoría técnica y análisis forense cuando aplique.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	No se contaba con un manual de procedimientos formalizado para la gestión de logs y la trazabilidad de los sistemas de información de la entidad.	Diseñar, aprobar y divulgar el procedimiento institucional para la gestión de registros de eventos (logs), estableciendo los lineamientos aplicables a los sistemas y servicios definidos por la OTI.	OTI	1/09/2026	31/07/2027							Oficina de Tecnologías de Información	2026
7	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Estrategia DRP y continuidad tecnológica en estado preliminar, sin evidencia suficiente de implementación y pruebas periódicas. Para el componente J2 —Continuidad DRP—, se aportó una Estrategia DRP – ICA Preliminar. Adicionalmente, en el componente H2 se aportaron evidencias de restauraciones y respaldos sobre algunos sistemas. Estos soportes permiten identificar avances en actividades de recuperación y respaldo. No obstante, no se evidenciaron planes DRP finales, aprobados y vigentes por servicios o sistemas de alto impacto. Tampoco se identificaron resultados de pruebas periódicas de continuidad o recuperación durante el período 2022–2025, actas de ejercicios, evaluación de resultados, lecciones aprendidas, responsables, tiempos objetivo de recuperación, puntos objetivo de recuperación, dependencias críticas ni planes de acción derivados. La evidencia de restauraciones puntuales es relevante, pero no equivale por sí sola a un plan de recuperación ante desastres formal, probado y mantenido. Un DRP debe permitir recuperar servicios críticos ante eventos	Formalizar, aprobar e implementar planes DRP para los servicios y sistemas críticos de la entidad, priorizando aquellos con alto impacto en la operación institucional. Los planes deberían incluir escenarios de desastre, responsables, contactos, dependencias, infraestructura requerida, RTO, RPO, procedimientos de recuperación, criterios de activación, retorno a la normalidad, pruebas periódicas, resultados, lecciones aprendidas y acciones de mejora. Se recomienda ejecutar pruebas periódicas documentadas de continuidad y recuperación, conservar actas de resultados, registrar desviaciones y hacer seguimiento a los planes de acción derivados.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	No se contaba con un proceso formalmente definido y aprobado para la elaboración, implementación, mantenimiento y ejecución de pruebas periódicas de los Planes de Recuperación ante Desastres (DRP) asociados a los servicios y sistemas críticos de la entidad.	Finalizar la elaboración del documento de la estrategia de Plan de Recuperación ante Desastres - DRP para el ICA, tramitar su correspondiente formalización con las areas misionales y de apoyo, el cual contiene la priorización de los servicios y sistemas críticos, incluyendo escenarios, contactos, dependencias, Recovery Time Objective u Objetivo de Tiempo de Recuperación - RTO, Objetivo de Punto de Recuperación - RPO, criterios de activación, recuperación y retorno a la normalidad.	OTI	1/09/2026	31/07/2027							Oficina de Tecnologías de Información	2026
7	2	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Estrategia DRP y continuidad tecnológica en estado preliminar, sin evidencia suficiente de implementación y pruebas periódicas. Para el componente J2 —Continuidad DRP—, se aportó una Estrategia DRP – ICA Preliminar. Adicionalmente, en el componente H2 se aportaron evidencias de restauraciones y respaldos sobre algunos sistemas. Estos soportes permiten identificar avances en actividades de recuperación y respaldo. No obstante, no se evidenciaron planes DRP finales, aprobados y vigentes por servicios o sistemas de alto impacto. Tampoco se identificaron resultados de pruebas periódicas de continuidad o recuperación durante el período 2022–2025, actas de ejercicios, evaluación de resultados, lecciones aprendidas, responsables, tiempos objetivo de recuperación, puntos objetivo de recuperación, dependencias críticas ni planes de acción derivados. La evidencia de restauraciones puntuales es relevante, pero no equivale por sí sola a un plan de recuperación ante desastres formal, probado	Formalizar, aprobar e implementar planes DRP para los servicios y sistemas críticos de la entidad, priorizando aquellos con alto impacto en la operación institucional. Los planes deberían incluir escenarios de desastre, responsables, contactos, dependencias, infraestructura requerida, RTO, RPO, procedimientos de recuperación, criterios de activación, retorno a la normalidad, pruebas periódicas, resultados, lecciones aprendidas y acciones de mejora. Se recomienda ejecutar pruebas periódicas documentadas de continuidad y recuperación, conservar actas de resultados, registrar desviaciones y hacer seguimiento a los planes de acción derivados.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	No se contaba con un proceso formalmente definido y aprobado para la elaboración, implementación, mantenimiento y prueba periódica de los Planes de Recuperación ante Desastres (DRP) asociados a los servicios y sistemas críticos de la entidad.	Programar y ejecutar, al menos, una prueba documentada para cada elemento del alcance priorizado, registrando los resultados, las lecciones aprendidas y el respectivo plan de mejora.	OTI	1/09/2026	15/12/2027							Oficina de Tecnologías de Información	2026

8	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Seguimiento contractual de controles de seguridad y ANS/SLA no evidenciado de forma integral. En los componentes I1 —Proveedores y contratos—, I2 —Soportes contractuales— y K1 —Cumplimiento políticas—, se aportaron contratos, actas de inicio, estudios previos, acuerdos de confidencialidad y soportes contractuales relacionados con servicios tecnológicos, infraestructura, SOC y obersaeguridad. Estos documentos evidencian la existencia de soportes contractuales relevantes. Sin embargo, no se evidenció una matriz consolidada que relacione los contratos TI/seguridad del periodo 2022–2025 con los servicios asociados, acceso a información o infraestructura, requisitos de seguridad, acuerdos de nivel de servicio, obligaciones de confidencialidad, tratamiento de datos, entregables, informes de supervisión, incidentes asociados, no conformidades, controles pactados y evidencia de cumplimiento. La política exige que los riesgos de seguridad se identifiquen desde la etapa precontractual y que los contratos con proveedores incluyan requisitos de seguridad, confidencialidad, protección de datos, continuidad y niveles de servicio cuando aplique. Igualmente, se requiere seguimiento durante la ejecución contractual. La falta de consolidación	Consolidar una matriz de seguimiento contractual para contratos TI/seguridad del período evaluado y vigencias posteriores, que incluya número de contrato, objeto, proveedor, supervisor, vigencia, servicio asociado, acceso a información o infraestructura, requisitos de seguridad, obligaciones de confidencialidad, tratamiento de datos, SLA/ANS, entregables, informes de supervisión, incidentes, no conformidades y estado de cumplimiento. Se recomienda que los supervisores contractuales incorporen dentro de sus informes evidencia específica sobre cumplimiento de obligaciones de seguridad de la información, niveles de servicio, continuidad, confidencialidad y gestión de incidentes cuando aplique.	Jefatura de la Oficina de Tecnologías de la Información —OTI—, supervisores contractuales y Equipo de Gestión Estratégica y Seguridad de Información TI.	Inexistencia de un mecanismo institucional formal que integrara la identificación, documentación, seguimiento, control y actualización periódica de los requisitos legales, contractuales y de privacidad aplicables a la OTI.	Diseñar la matriz consolidada de seguimiento de los contratos de TI y seguridad, por vigencia, con su respectiva actualización anual, asignación de responsables, seguimiento al cumplimiento y conservación de las evidencias correspondientes.	OTI	1/09/2026	31/07/2027							Oficina de Tecnologías de Información	2026
9	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Gestión de incidentes documentada mediante soportes por caso, sin un registro consolidado suficiente para el período evaluado. En el componente J1 —Gestión de incidentes—, se aportaron documentos relacionados con eventos o incidentes específicos, entre ellos situaciones asociadas a la página web institucional, Google Search Console, DNS y posible vulneración o hackeo de cuenta institucional de YouTube. También se allegaron formatos de incidentes de seguridad. Estos soportes permiten evidenciar que algunos eventos fueron documentados y atendidos mediante comunicaciones, revisiones técnicas o registros específicos. Sin embargo, no se evidenció un registro consolidado de incidentes de seguridad para el periodo 2022–2025 que permita identificar, por cada evento: fecha, hora, sistema afectado, tipo de incidente, severidad, impacto, responsable, acciones de contención, acciones correctivas, fecha de cierre, lecciones aprendidas y controles ajustados. La gestión por caso aporta trazabilidad puntual, pero no permite evaluar integralmente la gestión de incidentes. Sin un registro consolidado, se limita el análisis de recurrencia.	Formalizar y mantener actualizado un registro consolidado de incidentes de seguridad de la información para cada vigencia, incluyendo fecha y hora, sistema o servicio afectado, tipo de incidente, severidad, impacto, responsable, línea de tiempo, acciones de contención, análisis de causa, acciones correctivas, cierre, lecciones aprendidas y controles ajustados. Se recomienda establecer reportes periódicos de incidentes para análisis de tendencias, seguimiento de recurrencias y toma de decisiones sobre controles preventivos, detectivos y correctivos.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	Ausencia de una herramienta unificada para el seguimiento y control que consolide los eventos e incidentes de seguridad.	Diseñar e implementar una herramienta para el registro consolidado de incidentes de seguridad de la información, definiendo su alcance, responsables, periodicidad de actualización y mecanismos de seguimiento, con el fin de garantizar la consolidación, trazabilidad y consulta de los incidentes gestionados por la entidad.	OTI	1/09/2026	31/07/2027							Oficina de Tecnologías de Información	2026
10	1	Gestión de Servicios TIC / Sistema de Gestión de Seguridad de la Información —Controles Informáticos— / Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	Matriz de requisitos legales, contractuales y de privacidad no evidenciada de forma integral. Para el componente K1 —Cumplimiento políticas—, se aportaron soportes contractuales específicos, tales como estudio previo, contrato, acuerdo de confidencialidad y acta de inicio. Estos documentos son útiles para verificar obligaciones contractuales particulares relacionadas con seguridad y confidencialidad. Sin embargo, no se evidenció una matriz integral de requisitos legales, contractuales y de privacidad aplicables a la OTI, al SGSI/MSPI y a los servicios tecnológicos bajo su gestión. Tampoco se evidenció una relación consolidada de sistemas, servicios o bases de datos que tratan datos personales, con sus responsables, obligaciones aplicables, controles técnicos, evidencias de cumplimiento y periodicidad de revisión. La Política GIT-PTI-POL-001 V.3 contempla el cumplimiento de requisitos legales y contractuales, así como privacidad y protección de datos personales. En ese sentido, la entidad debe contar con mecanismos que permitan identificar qué obligaciones aplican, a qué sistemas o contratos corresponden, quién es responsable de su cumplimiento y qué evidencia se conserva para demostrarlo. La falta de una matriz consolidada puede afectar la capacidad de la OTI para demostrar cumplimiento normativo de manera sistemática y trazable. También dificulta la identificación de obligaciones asociadas a proveedores, sistemas, servicios digitales, tratamiento de datos personales, confidencialidad, conservación de información y seguridad contractual.	Elaborar, actualizar y mantener una matriz integral de requisitos legales, contractuales y de privacidad aplicables a la OTI, al SGSI/MSPI y a los servicios tecnológicos bajo su gestión. Esta matriz debería incluir norma u obligación, descripción del requisito, sistema o proceso asociado, responsable, evidencia de cumplimiento, periodicidad de revisión, estado, fecha de actualización y acciones pendientes. Se recomienda articular esta matriz con el inventario de activos de información, catálogo de sistemas y servicios, contratos tecnológicos, tratamiento de datos personales, acuerdos de confidencialidad, declaración de aplicabilidad y seguimiento al MSPI.	Oficina de Tecnologías de la Información —OTI— / Equipo de Gestión Estratégica y Seguridad de Información TI.	Inexistencia de un mecanismo institucional formal que integrara la identificación, documentación, seguimiento, control y actualización periódica de los requisitos legales, contractuales y de privacidad aplicables a la OTI.	Adoptar e implementar un mecanismo integral para la gestión de los requisitos legales, contractuales y de privacidad aplicables a la OTI.	OTI	1/09/2026	31/07/2027							Oficina de Tecnologías de Información	2026
																FORMA: 4-610 VERSIÓN 5		