RENOBO EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ

Informe de Auditoría

Proceso, Procedimiento o Proyecto auditado:	Plan Estratégico de Tecnologías de la Información (PETI) y el Sistema de Información Misional implementado.

1. INFORMACIÓN GENERAL

Trabajo de Auditoría No.		Fecha de reunión de inicio	10	08	2026	Fecha de reunión de cierre	12	11	2026
Auditor Líder:		Alberto Solano Jiménez (Contratista)							
Equipo Auditor:		José Edwin Lozano Gómez							

2. OBJETIVOS, ALCANCE, CRITERIOS Y RIESGOS DEL TRABAJO DE AUDITORÍA

2.1 OBJETIVOS

Objetivo General

Evaluar el grado de alineación, implementación y efectividad del Plan Estratégico de Tecnologías de Información (PETI) y del Sistema de Información Misional, verificando que su diseño, implementación, operación y controles contribuyan al cumplimiento de los objetivos institucionales y optimicen los procesos que se ejecutan.

Objetivos Específicos

- Evaluar la planeación, ejecución y seguimiento del PETI, verificando su alineación con las necesidades institucionales, la trazabilidad de los proyectos e iniciativas de TI y la confiabilidad de los mecanismos utilizados para medir su avance y cumplimiento.
- Evaluar el estado de implementación del Sistema de Información Misional y el funcionamiento de los componentes disponibles para evaluación, considerando su avance, funcionalidades, gestión de usuarios y perfiles, trazabilidad de cambios e integraciones con otros sistemas o servicios.
- Verificar la gestión y operación de la infraestructura tecnológica, los mecanismos de respaldo y recuperación, la administración de accesos, los activos de información, el soporte tecnológico y las actividades de mantenimiento preventivo y correctivo.
- Evaluar la implementación y operación de los controles relacionados con seguridad y privacidad de la información y gestión de riesgos de seguridad digital, considerando su diseño, aplicación y efectividad durante el período auditado.
- Verificar el cumplimiento de los procedimientos, manuales, políticas y demás lineamientos institucionales aplicables a la Gestión TIC, mediante la revisión selectiva de evidencias de su aplicación y operación.

2.2 ALCANCE

La auditoría comprendió la evaluación del proceso de Gestión TIC correspondiente al período comprendido entre enero de 2025 y la fecha de ejecución de la auditoría, incluyendo los siguientes aspectos:

- Planeación estratégica de TI.
- Seguimiento al PETI.
- Sistema de Información Misional.
- Gestión de infraestructura tecnológica.
- Gestión de respaldos.
- Administración de accesos.
- Gestión de activos de información.
- Seguridad y privacidad de la información.
- Soporte tecnológico.
- Mantenimiento preventivo y correctivo.
- Gestión de riesgos de seguridad digital.
- Cumplimiento de procedimientos, manuales y políticas institucionales.

2.3 CRITERIOS

- Ley 87 de 1993
- Ley 1712 de 2014
- Ley 1581 de 2012
- Decreto 1083 de 2015
- Decreto 1078 de 2015
- ISO 27000, 27001 y 27002
- Proceso, procedimientos y demás documentos SIG con relación a las TIC.

2.4 RIESGOS DEL TRABAJO DE AUDITORÍA

Riesgo	Causa	Consecuencia	Control	Observaciones
Manipulación u ocultamiento de información	Falta de ética o controles	Afectación reputacional y pérdida de credibilidad	Solicitud de evidencias por canales oficiales, verificación cruzada con fuentes primarias y aplicación del Código de Ética del auditor.	No se materializó; las evidencias se obtuvieron de fuentes institucionales y se validaron mediante pruebas.
Información incompleta o extemporánea	Debilidades en la gestión de información	Hallazgos por entes de control	Requerimientos formales con plazos definidos, seguimiento a las solicitudes y reiteración oportuna.	Se presentaron limitaciones en algunas evidencias (p. ej., reproducibilidad de indicadores), las cuales se documentaron en los resultados.
Deficiente planificación de la auditoría	Información insuficiente o no confiable	Bajo valor agregado de la auditoría	Programa de auditoría aprobado, análisis previo de criterios y riesgos, y revisión por la Jefatura de Control Interno.	El alcance y los criterios se definieron previamente y se ajustaron con base en la información obtenida.
Incumplimiento de cronograma	Factores internos o externos	Retrasos en entrega de resultados	Cronograma aprobado con seguimiento periódico al avance y comunicación oportuna de ajustes al auditado.	Se materializó por retrasos en el inicio de actividades del auditor líder, que se trasladaron sucesivamente a la entrega de evidencias por parte de TIC, su análisis y las etapas posteriores hasta el informe preliminar.

3. METODOLOGÍA

3.1 METODOLOGÍA APLICADA

La auditoría se desarrolló conforme a las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna y el procedimiento institucional de auditorías mediante:

- Revisión documental.
- Entrevistas con los responsables del proceso.
- Solicitud y análisis de evidencias.
- Pruebas de cumplimiento.
- Pruebas sustantivas.
- Verificación de controles.
- Validación del funcionamiento del Sistema de Información Misional.
- Muestreo de usuarios, accesos y respaldos.

4. RESULTADOS DEL TRABAJO DE AUDITORÍA

4.1 FORTALEZAS:

Como resultado de la revisión documental, el análisis de evidencias, la ejecución de pruebas de auditoría y las validaciones realizadas durante el período evaluado, se identificaron prácticas y capacidades institucionales que constituyen aspectos positivos de la Gestión TIC. Las principales fortalezas observadas son las siguientes:

Gestión y actualización de la planeación estratégica de TI

Durante la vigencia se actualizó el Plan Estratégico de Tecnologías de la Información, incluyendo la revisión y reorganización de iniciativas y su consolidación en macroproyectos. Los cambios relevantes fueron formalizados mediante la instancia institucional competente y se observaron decisiones de reorientación frente a cambios técnicos, institucionales y de prioridad, así como actuaciones materiales asociadas con la ejecución de la hoja de ruta tecnológica.

Participación de las áreas usuarias en la evolución del Sistema de Información Misional

Las áreas funcionales participaron en actividades de levantamiento y validación de requerimientos y en pruebas prácticas sobre funcionalidades parametrizadas del nuevo Sistema de Información Misional. Para casos seleccionados se comprobó la incorporación de observaciones formuladas durante las pruebas y la posterior verificación de ajustes, evidenciando un proceso iterativo de construcción de la solución orientado a las necesidades de los procesos institucionales.

Disponibilidad de una fuente institucional para la gestión del inventario tecnológico

La Empresa utiliza una fuente institucional para el registro de activos tecnológicos, cuyos identificadores permitieron efectuar cruces con otras evidencias operacionales. En particular, una proporción significativa de los registros de mantenimiento evaluados pudo ser relacionada con los activos registrados, proporcionando una base para su identificación, administración y seguimiento.

Operación de mecanismos de monitoreo y administración de infraestructura y seguridad tecnológica

Las pruebas mostraron el uso de herramientas para el monitoreo de infraestructura, conectividad y componentes tecnológicos, así como la ejecución de actividades de administración de seguridad perimetral, revisión de registros, segmentación de red, ajuste de configuraciones y verificaciones técnicas sobre componentes y servicios evaluados. Estas actividades acreditan la existencia de capacidades operativas de seguimiento y administración de la plataforma tecnológica.

Ejecución de mecanismos de respaldo y recuperación sobre componentes evaluados

La auditoría verificó la generación efectiva de copias de respaldo y la existencia de diferentes mecanismos de copia, réplica y automatización para componentes tecnológicos. Adicionalmente, para muestras específicas de infraestructura de almacenamiento y File Server se evidenció la recuperación satisfactoria de información previamente respaldada. Estos resultados acreditan capacidades técnicas de respaldo y recuperación para los componentes evaluados.

Uso operativo de GLPI para la gestión del soporte tecnológico

GLPI se utiliza de forma sostenida para registrar, asignar, gestionar, escalar y cerrar solicitudes de soporte tecnológico, conservando información sobre responsables, estados y tiempos de atención. Las pruebas permitieron verificar la operación de la mesa de servicio y la utilización de la herramienta como fuente transaccional para el seguimiento de los requerimientos tecnológicos.

Ejecución documentada de mantenimiento sobre equipos e infraestructura tecnológica

Los soportes examinados acreditan actividades efectivamente ejecutadas de mantenimiento preventivo, actualización, afinamiento y comprobación posterior de funcionamiento sobre equipos de usuario y componentes específicos de infraestructura y seguridad. Las evidencias permitieron establecer trazabilidad entre una proporción relevante de las intervenciones y los activos correspondientes, así como validar técnicamente algunas actualizaciones realizadas sobre componentes críticos.

Ejecución de análisis técnicos de vulnerabilidades

Existe evidencia de la realización de ejercicios técnicos de análisis de vulnerabilidades sobre sistemas institucionales mediante herramientas especializadas, con resultados que permitieron identificar, clasificar y priorizar exposiciones de seguridad. La ejecución de diferentes ciclos durante el período evaluado acredita la existencia de capacidades técnicas y la realización efectiva de actividades de identificación y análisis de vulnerabilidades.

Participación técnica de Gestión TIC en adquisiciones relevantes de infraestructura tecnológica

Para las adquisiciones seleccionadas relacionadas con seguridad perimetral y control de acceso a la red, se evidenció la participación técnica de Gestión TIC en la identificación y justificación de las necesidades, así como soportes posteriores asociados con la instalación, configuración y validación técnica de las soluciones adquiridas. Esta participación contribuye a que las inversiones en infraestructura respondan a necesidades técnicas sustentadas y a que las soluciones incorporadas sean verificadas antes de su operación.

4.2 DEBILIDADES:

Con base en los mismos procedimientos, se identificaron las siguientes debilidades principales en la Gestión TIC:

Confiabilidad y trazabilidad de la medición y seguimiento del PETI

En algunos de los indicadores y porcentajes utilizados para medir y reportar el avance del PETI se identificaron inconsistencias y limitaciones de reproducibilidad, así como diferencias entre metas establecidas en el instrumento aprobado y valores utilizados posteriormente en los informes de seguimiento. Adicionalmente, no quedó acreditado integralmente el cumplimiento de los mecanismos formales de autoevaluación de Estrategia y Gobierno de TI previstos en el PETI. Estas condiciones reducen la confiabilidad de la información utilizada para evaluar el cumplimiento de la planeación estratégica y soportar decisiones de seguimiento y priorización.

Trazabilidad y consistencia del seguimiento al proyecto de implementación del Sistema de Información Misional

La programación del proyecto presentó modificaciones materiales, diferencias entre líneas base y limitaciones para reconstruir integralmente la aprobación y transición entre las distintas programaciones. Asimismo, se identificaron actividades reportadas como completadas a una fecha de corte anterior a su fecha registrada de terminación y diferencias en la interpretación de los porcentajes de parametrización, pruebas y avance. La situación no desconoce los avances funcionales comprobados, pero limita la confiabilidad y comparabilidad de la información utilizada para gestionar y reportar el estado del proyecto.

Trazabilidad integral del ciclo de vida de los activos tecnológicos y su mantenimiento

Aunque la Empresa dispone de una fuente institucional de inventario y se comprobaron actividades efectivas de mantenimiento, no se evidenció una trazabilidad integral y homogénea que articule el estado operacional de los activos, mantenimiento programado, intervenciones realizadas, novedades identificadas, acciones posteriores y decisiones de continuidad, renovación o retiro. Esta condición puede limitar la capacidad para demostrar cobertura del mantenimiento y soportar oportunamente decisiones asociadas con obsolescencia y renovación tecnológica.

Cobertura, seguimiento y validación de los mecanismos de respaldo y recuperación tecnológica

La auditoría comprobó la ejecución efectiva de respaldos y restauraciones satisfactorias sobre determinados componentes; sin embargo, la capacidad de recuperación no se encuentra acreditada de manera homogénea para el conjunto de componentes evaluados. Se identificaron diferencias en cobertura, una prueba de recuperación de JSP7 que finalizó con resultado fallido sin evidencia suficiente de tratamiento, validación posterior y cierre de la excepción, así como limitaciones para comparar los resultados obtenidos con los objetivos de recuperación aplicables. En consecuencia, la debilidad no corresponde a una inexistencia de respaldos o de capacidades de recuperación, sino a la cobertura y validación integral de su efectividad.

Formalización y trazabilidad del ciclo de vida de los accesos, particularmente de cuentas privilegiadas

Las pruebas permitieron verificar la operación de mecanismos de solicitud y provisión de accesos; sin embargo, se identificaron limitaciones para reconstruir integralmente las autorizaciones, modificaciones, revisiones y retiros de privilegios durante el período auditado. En el Sistema de Información Misional se observaron además cuentas administrativas genéricas para las cuales no quedó suficientemente demostrada la custodia y atribución individual de las actuaciones, así como una dependencia del conocimiento del personal para traducir determinados perfiles funcionales en roles técnicos específicos. La auditoría no identificó accesos no autorizados, pero las condiciones observadas dificultan verificar de manera independiente la aplicación del principio de mínimo privilegio y la responsabilidad sobre actuaciones administrativas.

Seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información

Los resultados del autodiagnóstico MSPI y otros asuntos presentados ante las instancias de gobierno no evidenciaron de manera sistemática su transformación en acciones de mejora con responsables, fechas objetivo, seguimiento, validación de efectividad y cierre. Esta condición dificulta demostrar de manera integral que las brechas y necesidades de fortalecimiento identificadas mediante evaluaciones y ejercicios de seguimiento sean gestionadas hasta su tratamiento y cierre, limitando la trazabilidad del ciclo de mejora continua del SGSI.

Trazabilidad y reproducibilidad de la valoración y tratamiento de riesgos de seguridad digital

Existen limitaciones para reconstruir de manera homogénea la relación entre riesgos, controles, actividades de tratamiento, responsables, plazos, evidencias de ejecución, evaluación de efectividad y efecto sobre el riesgo residual. Estas condiciones reducen la capacidad para sustentar y reproducir de manera independiente las valoraciones realizadas y para demostrar que las reducciones registradas en el nivel de riesgo residual se encuentran soportadas en controles implementados y verificables.

Operación y trazabilidad del proceso de gestión de vulnerabilidades

Durante el período auditado se realizaron ejercicios técnicos de análisis de vulnerabilidades; sin embargo, la gestión no se encuentra soportada actualmente por un mecanismo periódico y suficientemente trazable que permita reconstruir de manera consistente el ciclo de identificación, priorización, tratamiento, remediación, reescaneo o revalidación y cierre. Para vulnerabilidades críticas o altas previamente identificadas no fue posible acreditar integralmente su tratamiento hasta la validación final. Esta condición incrementa el riesgo de permanencia de exposiciones conocidas sin que pueda demostrarse de manera suficiente su corrección efectiva.

4.3 RESULTADOS DE LAS EVIDENCIAS

4.3.1 ANÁLISIS DE RIESGOS - TEMAS OBJETO DE AUDITORÍA

El análisis efectuado sobre la Gestión TIC permitió identificar exposiciones asociadas con la planeación y seguimiento de las iniciativas tecnológicas, la implementación del Sistema de Información Misional, la continuidad y operación de la infraestructura, la administración de accesos, la seguridad y privacidad de la información, la gestión de riesgos de seguridad digital y el cumplimiento de los procedimientos institucionales.

De manera general, la auditoría evidenció que RenoBo dispone de mecanismos de control implementados y, en varios casos, operativos. Las principales exposiciones no se derivan de una ausencia generalizada de controles, sino de condiciones relacionadas con su trazabilidad, consistencia, cobertura y capacidad para demostrar de manera integral su operación y, cuando corresponde, su efectividad.

En materia de planeación estratégica y seguimiento al PETI, se verificaron mecanismos para actualizar, revisar y reorientar las iniciativas tecnológicas. La exposición principal se relaciona con la confiabilidad de la información utilizada para medir y comunicar su desempeño, debido a inconsistencias y limitaciones de reproducibilidad identificadas en algunos indicadores, metas y porcentajes de avance, así como a la acreditación incompleta de los mecanismos formales de autoevaluación establecidos en el propio Plan. Estas condiciones pueden afectar la capacidad para sustentar decisiones de seguimiento y priorización sobre información consistente y verificable.

Respecto del Sistema de Información Misional, se comprobaron avances efectivos de implementación, pruebas con usuarios y ajustes funcionales. La exposición se concentra principalmente en la consistencia y trazabilidad del seguimiento del proyecto, especialmente frente a modificaciones de programación, líneas base y porcentajes de avance. Dado que la nueva solución aún se encuentra en implementación, permanecen además riesgos propios de la transición tecnológica y de la futura puesta en producción, sin que ello constituya por sí mismo un incumplimiento.

En infraestructura tecnológica y mantenimiento, se verificó la existencia de inventarios, mecanismos de monitoreo y actividades efectivas de mantenimiento y renovación. La principal exposición se relaciona con la integración y trazabilidad de la información durante el ciclo de vida de los activos, particularmente para relacionar de manera homogénea su estado, mantenimiento, novedades, tratamiento y decisiones de continuidad, renovación o retiro. De forma complementaria, la ausencia de información histórica consolidada sobre indisponibilidades limita la capacidad para analizar tendencias y desempeño de los servicios tecnológicos.

En materia de respaldos y recuperación, se acreditaron mecanismos de copia de seguridad y restauraciones satisfactorias para componentes seleccionados. La evidencia no permitió demostrar de manera homogénea la recuperabilidad del conjunto de servicios evaluados ni contrastar integralmente los resultados de las pruebas con los objetivos de recuperación aplicables. La exposición se concentra, por tanto, en la posibilidad de que la capacidad real de recuperación de determinados servicios no haya sido validada bajo condiciones suficientemente trazables.

Respecto de la administración de accesos, se comprobó la operación del flujo básico de solicitud y provisión y la existencia de perfiles y permisos diferenciados. Permanecen exposiciones asociadas con la trazabilidad histórica de modificaciones y retiros de privilegios, la formalización de la correspondencia entre perfiles funcionales y roles técnicos y la atribución individual de actuaciones realizadas mediante cuentas administrativas genéricas. Estas condiciones dificultan demostrar de forma independiente la aplicación sostenida del mínimo privilegio y la responsabilidad individual sobre determinadas actuaciones administrativas, sin que la auditoría haya identificado accesos no autorizados.

En seguridad y privacidad de la información, RenoBo cuenta con políticas, instrumentos, mecanismos de monitoreo y controles implementados. La exposición propia de este ámbito se relaciona principalmente con la capacidad para transformar de manera sistemática los resultados de diagnósticos, evaluaciones y autodiagnósticos en acciones de mejora con responsables, plazos, seguimiento, validación de efectividad y cierre verificable. Esta condición limita la demostración integral del ciclo de seguimiento y mejora continua del SGSI, sin que ello implique una inefectividad general del sistema.

En la gestión de riesgos de seguridad digital, se verificó la existencia de matrices, controles y decisiones de tratamiento. Se identificaron limitaciones para relacionar de manera homogénea los riesgos con los controles implementados, las acciones de tratamiento, las evidencias de ejecución, la evaluación de efectividad de los controles y las reducciones aplicadas al riesgo residual. Esta condición limita la reproducibilidad independiente de las valoraciones y la capacidad para demostrar que las reducciones registradas en el nivel de riesgo residual se encuentran suficientemente sustentadas.

De manera diferenciada, la gestión de vulnerabilidades presenta una exposición específica. Aunque se comprobaron análisis técnicos realizados durante el período evaluado, se confirmó que actualmente no existe un mecanismo periódico soportado en herramienta, servicio o proveedor que asegure la ejecución sostenida del proceso. Adicionalmente, para determinados hallazgos previamente identificados no fue posible reconstruir integralmente la secuencia de tratamiento, remediación, revalidación y cierre técnico. Esta situación incrementa el riesgo de permanencia de exposiciones conocidas o de falta de identificación oportuna de nuevas vulnerabilidades.

En relación con la gestión de incidentes de seguridad, se verificó la existencia de un procedimiento institucional y de mecanismos de monitoreo; sin embargo, no se contó con una población verificable que permitiera seleccionar y recorrer incidentes reales de extremo a extremo. Esta situación constituye una limitación de aseguramiento y no evidencia de inoperancia del proceso.

Para la gestión de activos de información, los soportes disponibles permitieron comprobar la existencia de inventarios tecnológicos y actividades institucionales relacionadas con el análisis de activos, pero no verificar integralmente el Inventario y Clasificación de Activos de Información previsto institucionalmente. En consecuencia, permanece una limitación de verificación sobre la identificación, clasificación, actualización y formalización de dichos activos, sin evidencia suficiente para concluir incumplimiento.

Finalmente, en materia de cumplimiento de procedimientos, manuales y políticas institucionales, se observaron controles y procedimientos con aplicación efectiva, otros que requieren actualización frente a la operación tecnológica vigente y algunos cuya trazabilidad o aplicación no pudo demostrarse integralmente. El riesgo transversal se relaciona con la posibilidad de que existan diferencias entre el diseño documental y la operación real o que determinadas actuaciones no puedan ser reconstruidas posteriormente con suficiente evidencia.

En conjunto, las principales exposiciones de la Gestión TIC se concentran en fortalecer la trazabilidad, consistencia, cobertura y demostrabilidad de los controles y mecanismos de gestión, de manera que la Entidad pueda medir de forma reproducible sus iniciativas tecnológicas, reconstruir el ciclo de vida de activos y privilegios, validar periódicamente su capacidad de recuperación, gestionar vulnerabilidades hasta su cierre técnico y demostrar que los riesgos y brechas identificados se traducen en tratamientos efectivos y verificables.

4.3.2 EVALUACIÓN DE LAS EVIDENCIAS

4.3.2.1 Planeación estratégica de TI

La evaluación de la planeación estratégica de TI se orientó a determinar si RenoBo contó durante el período auditado con un instrumento de planeación actualizado y alineado con las necesidades institucionales, así como a verificar la existencia de mecanismos para revisar y ajustar las iniciativas tecnológicas y el nivel de estructuración de los proyectos definidos para su ejecución.

Como criterio principal se utilizó el *Plan Estratégico de Tecnologías de la Información (PETI)*, particularmente las fases “Planear” y “Analizar” y el desarrollo de la “Situación objetivo”, en las cuales se establece la necesidad de articular la gestión de TI con los objetivos institucionales a partir de la identificación de la situación actual, las brechas, el portafolio de proyectos y la hoja de ruta. La actualización realizada durante 2025 reorganizó las iniciativas tecnológicas en cuatro macroproyectos: Fortalecimiento de Gobierno y estructura organizacional de TI, Sistemas de Información, Seguridad y Privacidad de la Información e Infraestructura y Operación de TI.

Para la evaluación se contrastaron, entre otros soportes, los archivos *PETI_2022-2025_29012025.pdf* y *PETI_2022-2025_09_2025_30092025.pdf*, el *FT-144_Acta_reuniones_proy_PETI(1).pdf*, correspondiente al Acta No. 1 de Proyectos PETI del 26 de agosto de 2025, y el acta del Comité Institucional de Gestión y Desempeño del 30 de septiembre de 2025. El control de versiones del PETI registra una versión 5.1 del 5 de junio de 2025 y una versión 6.0 del 30 de septiembre de 2025, esta última asociada con el análisis del alcance de Gestión TIC, el reajuste de proyectos y su aprobación por parte del Comité Institucional de Gestión y Desempeño.

El *FT-144_Acta_reuniones_proy_PETI(1).pdf* permitió evidenciar que el 26 de agosto de 2025 se efectuó una revisión del avance de los proyectos, del alcance del proceso Gestión TIC y de las iniciativas que integraban el PETI. Como resultado de este ejercicio se planteó la reorganización del portafolio en los cuatro macroproyectos mencionados, identificando para cada uno las principales actividades previstas. Esta evidencia permitió establecer que la planeación estratégica de TI fue objeto de revisión y reorientación durante la vigencia y que los cambios posteriormente fueron incorporados al PETI actualizado.

Con el propósito de evaluar el nivel de estructuración de dicha planeación, la auditoría analizó para cada macroproyecto seis atributos: actividades, productos o entregables, metas, responsables, recursos y fechas. El análisis permitió establecer que las actividades se encontraban definidas y que el PETI contenía una hoja de ruta para orientar su ejecución.

Por ejemplo, el macroproyecto de Sistemas de Información incorporó actividades relacionadas con interoperabilidad, análisis de procesos misionales, recolección de requerimientos, priorización de funcionalidades y BIM; Seguridad y Privacidad de la Información contempló, entre otros componentes, el fortalecimiento del SGSI, la implementación de NAC y la actualización de políticas; e Infraestructura y Operación de TI incluyó actividades relacionadas con el modelo de servicios, inventario, renovación de conectividad y fortalecimiento de la mesa de ayuda.

El análisis evidenció, a su vez, que los productos o entregables, metas, responsables específicos, recursos asociados y fechas de ejecución no se encontraban desarrollados con el mismo nivel de detalle para todas las actividades. En particular, los entregables, metas, responsables y fechas presentaban un desarrollo parcial, mientras que los recursos no se encontraban vinculados de manera homogénea a cada actividad. Ante la solicitud complementaria de auditoría sobre la existencia de un instrumento adicional que desarrollara estos elementos para los cuatro macroproyectos, Gestión TIC informó que no se había definido un documento adicional.

Esta condición limita la posibilidad de establecer posteriormente, con un criterio homogéneo, la correspondencia entre lo inicialmente planeado y lo efectivamente ejecutado para cada actividad, especialmente en términos de producto esperado, meta, responsable, recurso utilizado y plazo. La situación no desvirtúa la existencia del PETI ni de su hoja de ruta, ni permite concluir ausencia de planeación estratégica; corresponde a una oportunidad para fortalecer el nivel de formalización y trazabilidad de los elementos utilizados para gestionar los macroproyectos.

En conclusión, la planeación estratégica de TI se encontró formalizada, actualizada y en ejecución durante el período evaluado, con evidencia de revisión del portafolio, reorientación de iniciativas, consolidación de los cuatro macroproyectos y aprobación formal de los ajustes. Se destaca como elemento favorable la capacidad de Gestión TIC para revisar su planeación frente a cambios institucionales y tecnológicos. Como Oportunidad de Mejora, se identificó la necesidad de fortalecer la definición homogénea y trazable de productos o entregables, metas, responsables, recursos y plazos asociados a las actividades de los macroproyectos, sin que esta condición dé lugar a una No Conformidad independiente.

4.3.2.2 Seguimiento al PETI

La evaluación del seguimiento al *Plan Estratégico de Tecnologías de la Información (PETI)* se orientó a determinar si RenoBo contó con mecanismos para monitorear el avance de las iniciativas previstas, identificar desviaciones, adoptar decisiones de ajuste y medir los resultados alcanzados, así como a verificar la confiabilidad y reproducibilidad de los indicadores utilizados y el cumplimiento de los mecanismos formales de evaluación definidos por la propia Entidad.

Como criterio principal se utilizó el PETI vigente durante el período evaluado, particularmente su Plan de seguimiento, los indicadores definidos para medir la ejecución de TI y los Lineamientos de Gobierno. Entre los indicadores examinados se incluyeron el IND.GO.07, relacionado con la proporción de iniciativas ejecutadas satisfactoriamente frente a las planeadas; el IND.GO.11, asociado con proyectos que presentan dificultades por insuficiencia de recursos; y el IND.GO.05, correspondiente al entrenamiento del equipo de TI.

Adicionalmente, los Lineamientos de Gobierno establecen la realización de cuatro autoevaluaciones anuales de Estrategia y Gobierno de TI y la presentación de por lo menos un informe anual de Gestión y Gobierno de TI al Comité de Gestión de Desempeño.

Para verificar la operación de estos mecanismos se revisaron, entre otros soportes, *I2025001442 Informe Seg 2025(1).pdf*, correspondiente al seguimiento realizado por la Oficina de Control Interno al primer cuatrimestre de 2025; *FT-144_Acta_reuniones_proy_PETI(1).pdf*; *Informe cierre de brechas_TI_2025.pdf* y su versión complementaria; *Informe de Capacitaciones y Citaciones TIC 2025 Iván y Holman.pdf*; *I2025001229.pdf*; el *Informe de Gestión de Tecnología e Innovación (TIC) - RenoBo 2025* y la versión actualizada del PETI aprobada el 30 de septiembre de 2025.

El análisis permitió establecer que el seguimiento al PETI operó durante la vigencia. El informe *I2025001442 Informe Seg 2025(1).pdf* registró el estado de los proyectos durante el primer cuatrimestre de 2025 y señaló, entre otros aspectos, que seis de los 19 proyectos presentaban avance de 0 %, debido a que no tenían actividades programadas para ese período. Posteriormente, el Acta No. 1 del 26 de agosto de 2025 documentó decisiones de continuidad, modificación, eliminación y reorganización de proyectos, incluyendo el replanteamiento de la iniciativa de hiperconvergencia y la integración de diferentes iniciativas en los cuatro macroproyectos definidos posteriormente en el PETI actualizado.

Mediante la reconstrucción de la secuencia de seguimiento se contrastaron la actualización del PETI en enero de 2025, el seguimiento efectuado por la Oficina de Control Interno, los análisis técnicos realizados durante julio y agosto y la aprobación de la versión 6.0 en septiembre de 2025. Esta revisión permitió acreditar la existencia de seguimiento sustantivo y capacidad para ajustar la planeación frente a las condiciones identificadas.

No obstante, la información relacionada con desviaciones, retrasos, riesgos, acciones, responsables y estados se encontraba distribuida en diferentes documentos. Ante la solicitud de un instrumento consolidado que permitiera reconstruir estos elementos, Gestión TIC informó que no existía un documento con dichas características.

La auditoría evaluó igualmente la confiabilidad y reproducibilidad de la información utilizada para medir el avance del PETI. En este ejercicio se identificaron diferencias entre las metas contenidas en las distintas versiones del Plan. La versión aprobada en septiembre de 2025 estableció para el cierre de brechas una distribución del 63 % para 2025, 28 % para 2026 y 10 % para 2027, mientras que la versión de enero había previsto 65 %, 31 % y 4 %, respectivamente. La programación contenida en la versión actualizada suma 101 %, lo que evidencia una inconsistencia interna en la distribución porcentual.

A su vez, el *Informe cierre de brechas_TI_2025.pdf* reportó “Cierre de Brechas Total 2025: 60,2% de 65% programado para 2025”, utilizando como referente la meta del 65 % correspondiente a una versión anterior del PETI. La auditoría validó los resultados explícitamente presentados en dicho informe: Gobierno y Estrategia de TI, 35 %; Sistemas de Información, 8,4 %; e Infraestructura, 13,6 %. La suma de estos componentes corresponde a 57,0 %, sin que con la evidencia disponible fuera posible reconstruir el origen de los 3,2 puntos porcentuales adicionales necesarios para obtener el 60,2 % reportado.

También se revisaron los indicadores globales de ejecución del PETI y de dificultades por capacidad. El informe reportó un avance de 74 % para la ejecución y un 26 % para dificultades relacionadas con capacidad; no obstante, con la población y soportes disponibles no fue posible identificar de manera inequívoca los numeradores, denominadores y elementos clasificados que permitieran reproducir dichos porcentajes conforme a las definiciones establecidas en el PETI. La conclusión de auditoría no fue que los resultados fueran necesariamente incorrectos, sino que no pudieron reproducirse con suficiente evidencia.

En relación con el indicador de entrenamiento, el *Informe de Capacitaciones y Citaciones TIC 2025 Iván y Holman.pdf* registró información sobre horas acumuladas y participantes y presentó un resultado porcentual para el indicador. Al contrastar el cálculo reportado con la fórmula definida en el PETI, se identificaron diferencias en las variables utilizadas y en la aplicación de la operación correspondiente, configurándose una inconsistencia verificable en la medición del indicador.

La revisión de los mecanismos formales de evaluación de Estrategia y Gobierno de TI evidenció que su cumplimiento no quedó acreditado integralmente. En *I2025001229.pdf*, Gestión TIC indicó expresamente que no se habían realizado autoevaluaciones relacionadas con la Estrategia y el Gobierno de TI en 2024 y 2025. Posteriormente, la Oficina de Control Interno señaló que no se había realizado la primera autoevaluación correspondiente a 2025.

Aunque el *Informe cierre de brechas_TI_2025.pdf* reportó posteriormente cuatro sesiones de seguimiento y control como 100 % cumplidas y referenció cuatro actas de comité DATIC, estas actas no hicieron parte de las evidencias disponibles para comprobar que las sesiones hubieran desarrollado los componentes y objetivos establecidos para las autoevaluaciones previstas en el PETI.

Respecto del compromiso de presentación de un informe anual, se verificó la existencia del *Informe de Gestión de Tecnología e Innovación (TIC) - RenoBo 2025*, con corte a diciembre de 2025. Sin embargo, con las evidencias disponibles no quedó acreditada su presentación formal ante el Comité de Gestión de Desempeño en los términos establecidos en el PETI.

Como complemento, se evaluó el seguimiento a las iniciativas de SGSI, Plan de Recuperación ante Desastres (DRP), Plan de Continuidad del Negocio (BCP) y Network Access Control (NAC)/seguridad perimetral. Para ello se contrastaron los informes FUSS correspondientes a julio, agosto, septiembre, octubre, noviembre y diciembre de 2025, junto con el PETI actualizado, el seguimiento realizado durante 2025 y los productos institucionales formalizados posteriormente.

Esta revisión permitió distinguir entre actividad, producto y resultado. Los informes FUSS permitieron reconstruir razonablemente la evolución de las iniciativas y evidenciaron, entre otros elementos, continuidad entre la estructuración contractual del SGSI durante 2025 y la generación posterior de políticas, planes, procedimientos e instrumentos asociados. También se observó evolución en las actividades relacionadas con recuperación tecnológica y mecanismos de respaldo.

Para algunos compromisos la trazabilidad no pudo completarse. El documento denominado acta 02 BCP_DRP, referenciado como soporte del cambio de enfoque de continuidad y recuperación, no estuvo disponible dentro del expediente revisado, por lo que no fue posible establecer suficientemente si el compromiso BCP fue cerrado, sustituido, integrado con otro instrumento o reprogramado. De forma similar, para la iniciativa NAC se identificaron estudios de mercado, elaboración de anexos técnicos, gestión precontractual y adquisición, pero las evidencias revisadas no permitieron demostrar de manera integral la transición entre adquisición, instalación, configuración, operación y resultados del control.

En consecuencia, el seguimiento de las iniciativas estratégicas de TI no se encontró ausente. Se verificaron revisiones periódicas, informes, espacios de decisión, reprogramaciones, modificaciones de alcance y productos concretos derivados de la ejecución.

La principal debilidad se concentra en la consistencia, trazabilidad y reproducibilidad de la medición del PETI, debido a diferencias entre versiones, resultados que no pudieron ser reproducidos integralmente y una inconsistencia confirmada en la aplicación de uno de los indicadores. Adicionalmente, los mecanismos formales de autoevaluación de Estrategia y Gobierno de TI y de presentación del informe anual no quedaron acreditados integralmente conforme al diseño establecido por el propio Plan.

En conclusión, el seguimiento al PETI se encontró implementado y en operación, con evidencia de monitoreo, toma de decisiones, modificación de iniciativas y actualización de la planeación. No obstante, la capacidad del seguimiento para proporcionar información plenamente consistente, confiable y reproducible se encuentra limitada por las condiciones identificadas en algunos resultados de medición, por la dispersión de información necesaria para reconstruir determinadas decisiones y por la acreditación incompleta de los mecanismos formales de evaluación de Estrategia y Gobierno de TI.

Estas condiciones se consolidan en la No Conformidad relacionada con la confiabilidad, trazabilidad y reproducibilidad de la medición y seguimiento del PETI, sin que ello implique ausencia general de seguimiento o gestión sobre el Plan.

4.3.2.3 Sistema de Información Misional

La evaluación del Sistema de Información Misional (SIM) se orientó a determinar si la solución contaba con un alcance identificable, si su implementación respondía a requerimientos funcionales de las áreas usuarias, si existían evidencias de parametrización y pruebas, si el avance del proyecto era objeto de seguimiento y si se adelantaban actividades para gestionar cambios e interoperabilidad con otros sistemas institucionales.

Como criterio principal se utilizó el *Plan Estratégico de Tecnologías de la Información (PETI)*, en particular la “Política de Gestión de Portafolio y Proyectos”, que establece que la función de TI gestiona programas, proyectos y mejoras mediante actividades de evaluación, priorización, acompañamiento y seguimiento; el apartado “Desde el diseño hasta la entrega”, que contempla la gestión de requerimientos durante su ciclo de vida, el diseño y desarrollo de aplicaciones y la realización de pruebas; y el “Proyecto Sistemas de información”, que incorpora actividades de análisis de procesos, recolección y priorización de requerimientos, arquitectura de integración e interoperabilidad entre el SIM y otros sistemas institucionales.

Para la evaluación se revisaron, entre otros, los siguientes soportes:

- *Copia de ANÁLISIS CAMBIO DE HERRAMIENTA TECNOLÓGICA SIM.pdf*
- *Copia de Línea Base Cronograma V2.pdf*
- *Copia de Cronograma seguimiento 15-sep-26.pdf*
- *Copia de Cronograma de avance corte 30-sep-26.pdf*
- *Copia de PPT avance SIM.pdf*
- *Copia de 22. Acta prueba piloto 22.pdf*
- *Copia de 23. Acta prueba piloto 23.pdf*
- *Copia de 42. Acta prueba piloto 42.pdf*
- *Copia de Presentación Interoperabilidad CDE-Matriz .pdf*
- *presupuesto_inversion_equipoTIC.pdf*.

La revisión fue complementada con respuestas de Gestión TIC y demostraciones relacionadas con usuarios, roles y permisos de NocoBase.

El documento *Copia de ANÁLISIS CAMBIO DE HERRAMIENTA TECNOLÓGICA SIM.pdf*, elaborado en agosto de 2025, documentó el análisis efectuado para sustituir Oracle Primavera Unifier y evaluar alternativas para el nuevo SIM. En su página 24 relacionó 104 proyectos cargados en Oracle Primavera Unifier y señaló que la información fue descargada antes del vencimiento del licenciamiento, previsto para el 26 de agosto de 2025, y conservada en un repositorio institucional.

Esta evidencia permitió acreditar una acción concreta de preservación de información durante la transición tecnológica, aunque la auditoría no efectuó una prueba integral de completitud, restauración o posterior migración de la totalidad de la información descargada.

En relación con la nueva solución, Gestión TIC indicó expresamente que NocoBase “no está en producción” y que se encontraba en “fase de parametrización y pruebas del piloto”. Esta condición fue consistente con las actas examinadas.

En *Copia de 22. Acta prueba piloto 22.pdf*, del 16 de diciembre de 2025, se documentó la presentación del subproceso “Interés comercial y análisis de requerimiento”, parametrizado sobre la base de levantamientos realizados previamente con usuarios líderes de la Dirección Técnica Comercial. Posteriormente, *Copia de 23. Acta prueba piloto 23.pdf*, del 30 de diciembre de 2025, dejó constancia de que “se finalizaron satisfactoriamente las pruebas del piloto con la Dirección Técnica Comercial”, aunque el mismo documento estableció como pasos siguientes continuar las pruebas con otras áreas involucradas y avanzar en la formalización del proceso.

Mediante la verificación funcional del piloto “Propuestas Comerciales”, la auditoría contrastó actas, presentación de avance y cronogramas para los componentes de Interés Comercial y Análisis de Requerimientos, Elaboración de Propuesta y Consolidación Final. La evidencia confirmó una cadena suficientemente soportada para el primer componente y pruebas reales sobre la elaboración de propuestas comerciales.

En *Copia de 42. Acta prueba piloto 42.pdf*, del 26 de mayo de 2026, se documentaron actividades como creación de solicitudes, validación del comportamiento ante información faltante, actualización de estados e identificación de oportunidades de ajuste. Asimismo, se verificó que una solicitud formulada durante una prueba anterior (incorporar automáticamente la fecha de registro y el nombre de quien registra la solicitud) había sido implementada posteriormente. Estos elementos evidencian que la participación de los usuarios generó retroalimentación y ajustes concretos sobre la parametrización.

El contraste con *Copia de PPT avance SIM.pdf*, página 8, permitió además diferenciar entre el grado de parametrización y el grado de prueba funcional. La presentación registraba como parametrizados al 100 % los componentes “Interés comercial y análisis de requerimientos” y “Elaboración de Propuesta Comercial”, mientras que “Consolidación final”, “Seguimiento al cliente” y “Formalización y suscripción del contrato” figuraban al 95 %. En materia de pruebas con la Dirección Comercial, solamente los dos primeros aparecían al 100 %.

Gestión TIC hizo referencia a una grabación de pruebas finales que demostraría la validación de todos los submódulos; al no encontrarse disponible para revisión directa, la auditoría no la utilizó como evidencia para afirmar una aceptación funcional integral del piloto.

Para evaluar el seguimiento del proyecto, la auditoría contrastó el cronograma, el avance y la reprogramación del SIM, mediante la comparación de *Copia de Línea Base Cronograma V2.pdf*, *Copia de Cronograma seguimiento 15-sep-26.pdf* y *Copia de Cronograma de avance corte 30-sep-26.pdf*. La línea base programaba la actividad “PARAMETRIZACIÓN Y PRUEBAS FLUJOS DE TRABAJO EN EL SIM” entre el 19 de enero y el 22 de diciembre de 2026. El seguimiento del 15 de septiembre mantenía dicha fecha de terminación y registraba “Propuestas Comerciales” con avance del 98 %.

En contraste, el cronograma con corte al 30 de septiembre de 2026 registró la parametrización y pruebas del SIM con un avance del 50 %, una duración de 371,2 días y fecha final del 22 de junio de 2027. El mismo documento mostraba como completadas al 100 % actividades cuya fecha de terminación se encontraba registrada para el 1, 2 y 13 de octubre de 2026, es decir, fechas posteriores al corte informado.

La auditoría estableció que existe seguimiento periódico y ejecución real del proyecto; no obstante, la aprobación de la reprogramación, la transición entre líneas base y la metodología utilizada para recalcular el avance no pudieron reconstruirse integralmente con las evidencias disponibles. Esta condición sustenta la No Conformidad relacionada con las debilidades en la consistencia y trazabilidad del seguimiento al proyecto de implementación del Sistema de Información Misional.

No se determinó ausencia de responsables ni de recursos. Gestión TIC identificó como responsables del proyecto al Líder del Proyecto, Líder Funcional y Líder Técnico, y el archivo *presupuesto_inversion_equipoTIC.pdf* permitió comprobar la existencia de recursos contractuales asociados al Sistema de Información Misional, administración de aplicaciones, backend y actividades de análisis y documentación de arquitectura y funcionalidad. La limitación identificada se concentra, por tanto, en la trazabilidad consolidada de la planeación y sus modificaciones y no en la inexistencia de recursos o responsables.

En materia de cambios y mejoras, se revisaron casos orientados a establecer la trazabilidad entre su identificación, implementación y prueba. Los casos examinados demostraron que existen ajustes gestionados en la práctica y que algunos pueden reconstruirse desde su identificación hasta la implementación y validación. Gestión TIC manifestó que el cronograma actualizado periódicamente constituye el mecanismo utilizado para hacer seguimiento a los ajustes.

No obstante, la información se encontraba distribuida entre actas, análisis, cronogramas y otros soportes, sin un instrumento consolidado que permitiera reconstruir uniformemente para cada cambio la solicitud, fecha, responsable, aprobación, implementación, prueba y cierre. Esta condición constituye un aspecto susceptible de fortalecimiento dentro del proceso de implementación, sin configurar una Oportunidad de Mejora independiente en la clasificación de resultados.

Para evaluar la interoperabilidad se revisó *Copia de Presentación Interoperabilidad CDE-Matriz .pdf*. En su página 7 se documentó la identificación de mecanismos REST para Unifier y JSP7, utilización de SOAP por Tampus, definición del caso de uso JSP7 → Tampus como piloto e identificación de servicios que requerían análisis para su conversión hacia APIs. Estos soportes acreditan actividades concretas de análisis y diseño técnico.

Gestión TIC indicó que la interconexión productiva no podía ejecutarse todavía debido a que NocoBase no se encontraba en producción. En consecuencia, la auditoría acreditó avances de diseño de interoperabilidad, pero no la efectividad de integraciones productivas del nuevo SIM.

Desde la perspectiva de control de acceso de la aplicación, las pruebas efectuadas permitieron comprobar que NocoBase cuenta con capacidades para crear usuarios, definir roles y configurar permisos sobre operaciones y datos. Durante una demostración se observaron cuentas nominales y cuentas administrativas con privilegios elevados. Esta capacidad constituye un componente positivo del diseño de la solución; las limitaciones específicas relacionadas con custodia de cuentas genéricas y atribución individual de actuaciones privilegiadas se desarrollan en el aspecto Administración de accesos, para evitar duplicar resultados.

En conjunto, la evidencia permite concluir que la implementación del SIM sobre NocoBase corresponde a una iniciativa en ejecución efectiva, con actividades verificables de análisis, levantamiento de requerimientos, parametrización, participación de usuarios, pruebas funcionales, incorporación de ajustes, asignación de recursos y diseño de interoperabilidad. También se verificaron actuaciones dirigidas a preservar información de la plataforma anterior durante la transición tecnológica.

A la fecha de las pruebas, el sistema se encontraba aún en fase de parametrización y pruebas, por lo que no era posible evaluar la efectividad de una operación productiva integral, el uso sostenido por la población usuaria ni la efectividad de las integraciones de NocoBase en producción. La principal debilidad identificada corresponde a la consistencia y trazabilidad del seguimiento del proyecto, mientras que la consolidación de la gestión de cambios y el avance de la interoperabilidad corresponden a aspectos que continúan desarrollándose dentro del proceso de implementación.

En conclusión, el Sistema de Información Misional presenta avances materiales y verificables de implementación, soportados en requerimientos funcionales, parametrización, pruebas con usuarios y ajustes derivados de dichas pruebas. La participación de las áreas usuarias y la capacidad de incorporar cambios constituyen elementos favorables. La valoración integral del sistema permanece condicionada por su estado de implementación. La debilidad identificada en la consistencia y trazabilidad del seguimiento del proyecto sustenta una No Conformidad específica, sin que resulte procedente equiparar el estado actual del SIM con una solución plenamente implementada y operativa ni considerar como incumplimientos las funcionalidades o integraciones que todavía se encuentran dentro de la etapa prevista de construcción y puesta en funcionamiento.

4.3.2.4 Gestión de infraestructura tecnológica

La evaluación de la gestión de infraestructura tecnológica se orientó a determinar si RenoBo dispone de información suficiente y actualizada sobre sus componentes tecnológicos, si cuenta con mecanismos implementados para conocer su estado, disponibilidad y capacidad, si ejecuta actividades de renovación y fortalecimiento de infraestructura y si las adquisiciones relevantes cuentan con evaluación y validación técnica.

Como criterios principales se consideraron las disposiciones del *Plan Estratégico de Tecnologías de la Información (PETI)* relacionadas con “Activos y configuraciones”, monitoreo permanente, capacidad, disponibilidad y operación de servicios. El PETI establece la necesidad de mantener controlado el inventario de software y hardware para conocer la capacidad tecnológica disponible y determinar los momentos apropiados para mantener o renovar los activos. También dispone la utilización de mecanismos de monitoreo que permitan identificar indisponibilidades y apoyar la gestión de capacidad y niveles de servicio.

Desde la perspectiva estratégica, se revisaron *FT-144_Acta_reuniones_proy_PETI(1).pdf*, *I2025001442 Informe Seg 2025(1).pdf*, *Informe cierre de brechas_TI_2025.pdf* y soportes relacionados con renovación y conectividad.

Informe de Auditoría

El Acta No. 1 del 26 de agosto de 2025 documentó el análisis de la iniciativa de hiperconvergencia, respecto de la cual se concluyó que la arquitectura y las necesidades existentes no justificaban mantener el alcance originalmente previsto, orientándose recursos hacia la implementación de una solución NAC y la reposición de servidores por obsolescencia. También se documentaron actuaciones relacionadas con conectividad y adquisición de switches para fortalecer el control de la red LAN.

El *Informe cierre de brechas_TI_2025.pdf* registró, entre otras actuaciones, la recuperación y puesta en funcionamiento de cuatro servidores, el inicio de adquisición de un nuevo NAS, el replanteamiento de la iniciativa de hiperconvergencia, la adquisición de 12 switches y actividades de estabilización del canal MPLS. Estas evidencias permitieron acreditar actuaciones materiales de renovación y racionalización de infraestructura, aunque no para todos los componentes fue posible reconstruir de forma homogénea la cadena actividad planeada, producto, recepción, implementación.

Para evaluar el inventario tecnológico, se revisó *Hardware y software sep-26_fin.csv*, aportado como inventario oficial de Gestión TIC, así como información complementaria del módulo de Activos del ERP JSP7. La auditoría analizó la clasificación de activos, códigos, seriales, fechas asociadas a vida útil y registros correspondientes a infraestructura, y contrastó esta información con el *I2025001442 Informe Seg 2025(1).pdf*, cuyo apartado “4.3 Estado de la infraestructura de servidores de la Empresa” reportó 15 servidores, de los cuales 10 figuraban como encendidos y 5 como apagados.

El contraste permitió establecer que RenoBo dispone de una fuente institucional de inventario utilizada operacionalmente. Se observaron diferencias puntuales de clasificación, seriales y población entre las fuentes revisadas, incluyendo un componente registrado como servidor en un informe y clasificado como computador en el inventario. Estas diferencias no fueron interpretadas como ausencia del inventario ni como falta general de confiabilidad, sino como limitaciones de reconciliación y calidad de información que afectan la trazabilidad homogénea de determinados componentes.

La auditoría examinó igualmente los mecanismos de monitoreo y disponibilidad mediante el *Informe_CiberSeguridad_Disponibilidad Agosto.pdf* y evidencias asociadas con Zabbix, FortiGate, FortiAnalyzer y GLPI. Gestión TIC indicó que el seguimiento de disponibilidad y rendimiento se realiza directamente mediante estas herramientas. Los soportes revisados evidenciaron información sobre tráfico, conexiones VPN, canales y eventos técnicos, lo que permitió acreditar la existencia y utilización de mecanismos de monitoreo.

Como antecedente adicional, el *I2025001442 Informe Seg 2025(1).pdf* había señalado que, en las pruebas realizadas durante dicho seguimiento, los 20 servicios incluidos en el Catálogo de Servicios de TI se encontraban operativos. Esta evidencia fue considerada como una comprobación puntual de operación y no como demostración de disponibilidad continua durante todo el período auditado.

La solicitud complementaria buscó establecer si RenoBo disponía de una matriz, bitácora o reporte consolidado de indisponibilidades. Gestión TIC informó que “No se tiene un archivo que suministre una matriz, bitácora o reporte” que permita identificar de forma consolidada el componente afectado, fecha, duración exacta y análisis de causa. Por tanto, la auditoría distinguió entre la existencia y operación de mecanismos de monitoreo, que sí quedó acreditada, y la capacidad para reconstruir históricamente la disponibilidad de cada servicio, que presentó limitaciones.

Durante la revisión se observaron también períodos de tráfico en cero y otros eventos técnicos en determinadas gráficas. Estos elementos no fueron considerados evidencia suficiente de indisponibilidad, al no existir una correlación verificable con incidentes, afectación de servicios, duración o impacto. Las diferencias temporales detectadas entre algunos períodos declarados y las gráficas incorporadas en los informes fueron tratadas como inconsistencias de calidad del reporte y no como evidencia directa de fallas operacionales.

Desde la perspectiva de seguridad de infraestructura, se revisaron controles y soportes relacionados con seguridad perimetral, redundancia, registro y seguimiento de eventos. La validación del autodiagnóstico MSPI 2026 fue contrastada con *FUSS_noviembre2025.pdf*, documento que registró actividades relacionadas con segmentación de red, depuración de políticas de firewall, direcciones IP, VLAN y zonas sin uso, seguimiento mensual de registros en FortiAnalyzer, ajustes de almacenamiento para mejorar la retención de logs, validaciones de alta disponibilidad mediante FortiLink, conectividad MPLS, configuración de Veeam y mantenimiento de servidores de Directorio Activo.

Estas evidencias permitieron acreditar actividades operativas sobre determinados controles tecnológicos. Sin embargo, no se acreditó integralmente, mediante registros técnicos de las herramientas, la cobertura completa de fuentes de logs, los períodos efectivos de retención, las reglas de correlación, las alertas generadas, su tratamiento y escalamiento o la realización de pruebas integrales de conmutación para todos los servicios críticos. En consecuencia, la evidencia permite acreditar la operación de mecanismos específicos en los componentes revisados, sin extender esta conclusión a la efectividad integral de toda la infraestructura tecnológica.

La auditoría evaluó igualmente la aplicación del procedimiento *PD-50, Adquisición de Infraestructura Tecnológica V3*, mediante una muestra de los contratos 458-2025, Seguridad Perimetral y 522-2025, Solución NAC. Para el primero se revisó el anexo técnico y el acta de recibo, identificándose la justificación técnica de continuidad del licenciamiento y soporte de la solución Fortinet, así como evidencias posteriores de despliegue, configuración, puesta en marcha, entrega de documentación técnica, diagnóstico y transferencia de conocimiento.

Informe de Auditoría

Para el contrato 522-2025 se revisaron los documentos precontractuales y *Copia de ANEXO 1 CONTRATO No. 522-2025 SOLUCIÓN NAC - DATASEC SAS.pdf*. La documentación sustentó la necesidad de incorporar una solución NAC para control de acceso, autenticación, perfilamiento y aislamiento de dispositivos. Posteriormente se evidenció la instalación, configuración y parametrización de un FortiNAC 500F, contrastada además con *Mantenimiento FortiNAC 500 F 15 septiembre.pdf*, que identifica el equipo srvfnac.renobo.com.co, serial FN500FT225000308, y registra actividades realizadas sobre la plataforma el 15 de septiembre de 2026.

En la muestra seleccionada quedó razonablemente acreditada la existencia de una evaluación técnica previa y de actuaciones posteriores de recepción, instalación o validación. Se identificaron inconsistencias documentales puntuales en la denominación de algunos modelos de equipos y reservas sobre la formalización de determinados soportes de aceptación, condiciones que afectan la calidad de la trazabilidad documental pero no desvirtúan la evidencia técnica observada.

En conjunto, la auditoría comprobó que RenoBo cuenta con infraestructura tecnológica gestionada mediante inventarios, herramientas de monitoreo, actividades de renovación, mecanismos de seguridad perimetral y procesos técnicos de adquisición e implementación. Se acreditaron actuaciones reales sobre servidores, conectividad, switches, firewall, FortiAnalyzer, FortiNAC y otros componentes tecnológicos, así como decisiones de ajuste de la arquitectura frente a las necesidades institucionales.

La principal oportunidad de mejora se concentra en fortalecer la integración y trazabilidad de la información durante el ciclo de vida de los activos tecnológicos, de manera que pueda relacionarse homogéneamente el inventario, estado del activo, mantenimiento programado y ejecutado, novedades identificadas, acciones posteriores y decisiones de continuidad, renovación o retiro. De forma complementaria, disponer de información histórica consolidada sobre disponibilidad e interrupciones permitiría fortalecer el análisis del comportamiento de los servicios tecnológicos. La trazabilidad relacionada con mantenimiento se complementa con las pruebas desarrolladas en el apartado 10. Mantenimiento preventivo y correctivo.

Estas condiciones se mantienen como Oportunidad de Mejora, dado que la auditoría comprobó la existencia y operación de inventarios, mecanismos de monitoreo y actividades de gestión sobre la infraestructura, y no contó con evidencia suficiente para concluir una desviación general frente a un criterio institucional que exija un único mecanismo consolidado de trazabilidad del ciclo de vida o de disponibilidad histórica.

En conclusión, la gestión de infraestructura tecnológica se encuentra implementada y operativa en los componentes evaluados, con evidencia de inventario institucional, monitoreo, renovación tecnológica, seguridad perimetral y participación técnica en adquisiciones. Se identifica una Oportunidad de Mejora orientada a fortalecer la trazabilidad integral del ciclo de vida de los activos tecnológicos, complementada con el fortalecimiento de la información histórica sobre disponibilidad e interrupciones de los servicios, sin que estas condiciones den lugar a una No Conformidad independiente.

4.3.2.5 Gestión de respaldos

La evaluación de la gestión de respaldos se orientó a determinar si RenoBo cuenta con mecanismos implementados para proteger la información y los servicios tecnológicos mediante copias de seguridad, si dichos mecanismos se ejecutan efectivamente y, especialmente, si existe evidencia suficiente para demostrar la capacidad de recuperación de la información respaldada.

Como criterios se consideraron el *Plan Estratégico de Tecnologías de la Información (PETI)*, el procedimiento *PD-51, Copias de respaldo V3*, la *GI-27, Guía de Copias de Respaldo V1* y el *Plan de Recuperación Tecnológica ante Desastres*, versión 1, formalizado el 22 de junio de 2026. El PETI establece que la información crítica debe protegerse mediante mecanismos de respaldo y restauración y que, una vez realizada una recuperación, debe verificarse la integridad de los datos y el funcionamiento del componente recuperado. Por su parte, PD-51 establece la ejecución de las copias conforme a GI-27.

El *Plan de Recuperación Tecnológica ante Desastres*, en su numeral 8.4, Validación y pruebas, establece la realización de pruebas de restauración como mínimo semestrales para servicios críticos y anuales para servicios no críticos, o cuando se presenten eventos relevantes. El mismo apartado contempla la restauración controlada, verificación de integridad y validación funcional básica, así como la conservación de informes, registros de backup, bitácoras de restauración, resultados y acciones correctivas. Adicionalmente, el numeral 8.5, Relación con KPIs estratégicos define un indicador de pruebas exitosas de restauración con meta igual o superior al 90 %.

Para verificar la ejecución de respaldos se revisaron, entre otros soportes, Backup-2025-2026.pdf, Reporte_backup_Renobo_Julio_2026_SRV_NubeETB.pdf, prueba_restauracion_JSP7_agosto2026.pdf, prueba_restauracion_JSP7_agosto2026(1).pdf, Informe_Pruebas_Restauracion_NAS.pdf y reportes asociados con TAMPUS, hosting de georreferenciación, File Server, Proxmox y mecanismos de réplica alojados en infraestructura ETB. También se efectuaron validaciones sobre la recuperación de información del File Server.

El archivo *Backup-2025-2026.pdf* permitió identificar configuraciones de respaldo para diferentes máquinas virtuales alojadas sobre Proxmox, incluyendo VM 102, VMOCSINVENTORY, VM 104, Erunet, VM 100, VMDESARROLLO y VM 101, VMDESPLIEGUE, con mecanismos tipo Snapshot, almacenamiento local o de red y esquemas de compresión. También se revisaron evidencias de réplicas en infraestructura ETB, replicación entre unidades NAS y respaldos de configuración. Estas evidencias acreditaron la existencia de una arquitectura de respaldo, aunque la sola configuración no fue considerada evidencia suficiente para demostrar la ejecución histórica exitosa de todos los trabajos.

Para JSP7, *prueba_restauracion_JSP7_agosto2026.pdf* permitió verificar la existencia de múltiples objetos de respaldo correspondientes a agosto de 2026, con fecha, hora y tamaño registrados. La auditoría observó respaldos generados, entre otros, los días 17, 21, 24, 28 y 31 de agosto, lo que permitió establecer que el mecanismo no se encontraba únicamente configurado, sino que existían objetos efectivamente generados.

La misma evidencia documentó la ejecución #331 de Jenkins, realizada el 3 de septiembre de 2026. Las etapas “Declarative: Checkout SCM”, “Descarga de script”, “Agregando configuración” y “Descargando respaldo” finalizaron en estado SUCCESS; sin embargo, la etapa “Probando respaldo” terminó en estado FAILED, al igual que el resultado general de la ejecución. En los soportes examinados no se evidenció suficientemente el análisis de la causa, el tratamiento aplicado ni una validación posterior que permitiera acreditar el cierre de la excepción.

La revisión de soportes adicionales permitió observar que este resultado fallido no era suficiente para afirmar que el mecanismo de JSP7 nunca hubiese funcionado. En evidencias correspondientes a julio de 2026 se identificó una ejecución en la cual la fase “Probando respaldo” presentó resultado SUCCESS el 1 de julio de 2026. Esto evidencia que existe un mecanismo automatizado de respaldo y comprobación mediante Jenkins, pero también que la ejecución posterior de septiembre presentó una falla cuyo tratamiento, validación posterior y cierre no quedaron suficientemente acreditados.

Para infraestructura NAS, la auditoría revisó *Informe_Pruebas_Restauracion_NAS.pdf*, fechado el 30 de septiembre de 2026. El documento consolidó pruebas efectuadas entre el 21 y el 25 de septiembre mediante Dell PowerProtect Data Manager (PPDM) y registró dos respaldos manuales exitosos y dos restauraciones exitosas sobre el sistema de archivos evaluado, incluyendo recuperación al host original y a una ubicación alterna. La bitácora individualizó los respaldos con identificadores CA842525 y CEE1C1D7, y las restauraciones mediante DD793F5C y 620D1D56. Estas evidencias permitieron acreditar satisfactoriamente la cadena respaldo-restauración para la muestra examinada.

El mismo informe registró 59 trabajos en la consola, de los cuales cuatro figuraban como exitosos, 36 como fallidos y 19 como cancelados. La auditoría no interpretó estos valores como una tasa directa de fallas productivas, dado que correspondían a operaciones de diferente naturaleza. Adicionalmente, se observaron cuatro sistemas de archivos, de los cuales uno tenía una política de protección aplicada. Esta condición requiere considerar la función y criticidad de cada volumen antes de concluir que los restantes debían encontrarse necesariamente respaldados.

Las bitácoras NAS permitieron verificar fechas y horas de creación e inicio de los trabajos, pero no contenían de manera completa la hora final o duración efectiva de todas las restauraciones. En consecuencia, la auditoría pudo acreditar su resultado satisfactorio, pero no reconstruir suficientemente los tiempos de recuperación para contrastarlos de forma integral con los objetivos de recuperación aplicables.

La evaluación fue complementada con una validación realizada sobre el File Server. Durante la sesión, Gestión TIC mostró la configuración de respaldo del almacenamiento institucional, que contemplaba una copia sintética diaria con retención de 15 días y una copia mensual con conservación de un mes. También se presentó la recuperación de carpetas previamente respaldadas, lo que permitió comprobar materialmente la recuperabilidad de información para la muestra seleccionada.

Los responsables de Tecnología indicaron que los respaldos administrados directamente por RenoBo se concentran principalmente en información alojada en el File Server, mientras que para aplicaciones prestadas bajo modalidad SaaS, como algunos sistemas institucionales, la operación de respaldo es gestionada total o parcialmente por sus proveedores.

Esta diferencia de arquitectura implica que la evaluación integral de la capacidad de recuperación debe considerar el alcance y las responsabilidades aplicables a cada servicio.

Desde la perspectiva documental, la auditoría identificó una diferencia entre la operación tecnológica actual y la *GI-27, Guía de Copias de Respaldo V1*, expedida originalmente el 27 de diciembre de 2019. La guía mantiene referencias a tecnologías y plataformas históricas, incluyendo ERUDITA, ERUNET, Kaspersky y Apoteosys, además de instrucciones específicas para respaldos de cuentas institucionales. La arquitectura observada durante 2026 incorpora nuevos servicios, infraestructura y esquemas SaaS que no se encuentran reflejados integralmente en dicho instrumento.

En consecuencia, la evidencia permite concluir que RenoBo cuenta con mecanismos de respaldo implementados y operativos y que existen pruebas satisfactorias de recuperación sobre componentes específicos, particularmente NAS y File Server. Para JSP7 también se acreditó la generación de respaldos y la existencia de un mecanismo automatizado de prueba; sin embargo, una ejecución examinada terminó fallida y no quedó suficientemente acreditado su tratamiento, validación posterior y cierre.

La principal debilidad no corresponde a una ausencia general de respaldos, sino a la cobertura y validación homogénea de la capacidad de recuperación tecnológica. Las pruebas realizadas no permiten extrapolar automáticamente los resultados favorables de NAS y File Server al conjunto de sistemas y servicios, ni demostrar integralmente la recuperación funcional o el cumplimiento de los objetivos de recuperación para el universo aplicable. Esta condición sustenta la No Conformidad relacionada con la cobertura y validación de la capacidad de recuperación tecnológica.

En conclusión, la gestión de respaldos se encuentra implementada y operativamente acreditada para las muestras examinadas, con evidencia de generación de copias, automatización y restauraciones exitosas. No obstante, la capacidad para demostrar de forma homogénea y periódica la recuperabilidad del conjunto de servicios presenta una debilidad que da lugar a una No Conformidad, particularmente frente al tratamiento y cierre de excepciones, la validación sobre el universo aplicable y el contraste de los resultados con los objetivos de recuperación definidos.

De manera complementaria, la actualización de la GI-27 frente a la arquitectura tecnológica vigente se mantiene como Oportunidad de Mejora. La evidencia disponible no permite afirmar que los servicios sean irrecuperables ni que los respaldos sean inefectivos de manera general.

4.3.2.6 Administración de accesos

La evaluación de la administración de accesos se orientó a determinar si RenoBo cuenta con mecanismos para gestionar de manera controlada el ciclo de vida de los accesos lógicos, incluyendo su solicitud, aprobación, creación, modificación, revisión y retiro, así como la administración de cuentas privilegiadas, técnicas, de servicio, de terceros y accesos asociados con plataformas institucionales.

Como criterio principal se utilizó el procedimiento *PD-71, Administración de Acceso Lógico*, considerando la versión aplicable al período evaluado. La versión 6, contenida en P_SGSI-PROC-SUP-071-v06.docx, establece controles para gestionar de manera segura, oportuna y trazable las novedades de acceso y contempla validación de solicitudes, aprobación funcional, aplicación del principio de mínimo privilegio, tratamiento de cuentas especiales, revisión periódica y conservación de evidencia. Para cuentas temporales, privilegiadas, de servicio o de terceros, el procedimiento incorpora controles adicionales y vigencias definidas.

En relación con el Sistema de Información Misional, NocoBase, se revisó el archivo *Usuarios en Nocobase.pdf* y posteriormente se efectuó una demostración en vivo sobre la administración de usuarios, roles y permisos. El documento relacionó siete usuarios y permitió observar perfiles diferenciados, entre ellos Super Usuario, Administrador, Miembro y Proceso de Interés comercial. También identificó las cuentas *nocobase* / admin@*nocobase*.com y administrador / administrador@*nocobase*.com, ambas con privilegios elevados.

El archivo describe que los perfiles administrativos pueden configurar la interfaz, instalar, activar y desactivar plugins y administrar fuentes de datos, y señala que “el Super Usuario es el único que puede borrar la caché y reiniciar la aplicación”. Para los usuarios funcionales revisados se observaron restricciones acordes con los flujos asignados, y el contraste con las actas de prueba permitió establecer correspondencia razonable entre determinadas funciones conocidas y los permisos observados.

Durante la validación realizada sobre NocoBase se verificó adicionalmente que la plataforma permite crear usuarios y roles y definir permisos sobre acciones como crear, consultar, editar, eliminar, importar y exportar registros, incluyendo el alcance de los datos sobre los cuales puede operar cada rol. Esta capacidad constituye un control de autorización implementado dentro de la aplicación.

La principal limitación identificada en este componente correspondió a las cuentas privilegiadas genéricas *nocobase* y *administrator*. Durante la demostración, los responsables de Tecnología informaron que la primera corresponde a la cuenta con mayores privilegios y que la segunda fue creada como cuenta administrativa de respaldo. También señalaron que su responsabilidad operativa recae actualmente sobre integrantes del equipo de desarrollo y pruebas; sin embargo, durante la sesión no se evidenció un registro formal de asignación de custodia.

La auditoría revisó igualmente la funcionalidad de logs de NocoBase. Se observaron archivos JSON y registros técnicos asociados con solicitudes, eventos de sistema y operaciones, con información como timestamps, endpoints y métodos. No obstante, con la configuración y los mecanismos demostrados durante la sesión no fue posible reconstruir de forma uniforme la secuencia usuario individual, acción, objeto afectado, fecha/hora, resultado para actuaciones realizadas mediante cuentas genéricas privilegiadas.

Esta condición debe interpretarse en sus términos exactos: la auditoría no comprobó que las cuentas fueran utilizadas por personas no autorizadas, que hubieran sido objeto de uso indebido ni que se hubiera materializado un incidente de seguridad. La situación identificada corresponde a una limitación de custodia formal y atribución individual de las actuaciones administrativas cuando se utilizan identidades genéricas.

Para evaluar los accesos de infraestructura se revisaron *Accesos y Privilegios Active Directory.pdf*, *Reporte_Usuarios_AD.csv*, *Usuarios AD (estado).xlsx* e *Informe de cuentas de usuario de Active Directory.pdf*. El primer reporte identificó 608 cuentas, de las cuales 31 presentaban privilegios administrativos elevados y 577 correspondían a cuentas estándar u operativas. Un reporte posterior, con corte a octubre de 2026, identificó 620 cuentas listadas y 155 deshabilitadas, evidenciando que las fuentes corresponden a momentos diferentes del ciclo de administración.

El cruce realizado entre las 31 cuentas privilegiadas inicialmente reportadas y el archivo posterior de estado produjo 17 coincidencias exactas. Para las demás no fue posible establecer una correspondencia inequívoca únicamente a partir de los identificadores disponibles. Esta situación no fue interpretada como evidencia de eliminación, permanencia indebida o acceso no autorizado, sino como una limitación para reconstruir los movimientos realizados entre las diferentes fuentes de información.

También se revisaron evidencias de cuentas administrativas en FortiGate, FortiAnalyzer y FortiNAC, confirmándose la existencia de perfiles diferenciados y usuarios con privilegios elevados. En determinadas evidencias de FortiGate se observaron cuentas administrativas para las cuales el segundo factor de autenticación aparecía deshabilitado. La auditoría mantuvo esta condición como factor de exposición y contexto de control, sin formular un incumplimiento autónomo, dado que en esta prueba no se acreditó un requisito institucional específico que exigiera MFA para la totalidad de dichas cuentas durante el período evaluado.

Respecto de accesos VPN, Gestión TIC informó, con base en *Reporte_Usuarios_AD.csv*, que 561 usuarios presentaban membresía en uno o varios grupos relacionados con acceso remoto, entre ellos Int_VPN, VPN 13, VPN 14, VPN 17, VPN 30, VPN_Admon y VPN_TERCEROS. La auditoría consideró que esta información demuestra pertenencia a grupos de Active Directory, pero no permite equiparar automáticamente dicha población con 561 accesos VPN efectivamente habilitados, utilizados o vigentes en la solución perimetral.

Uno de los elementos relevantes para la trazabilidad histórica surgió de la solicitud de una relación de altas, modificaciones y retiros de accesos durante el período auditado. Gestión TIC respondió expresamente: “No se cuenta con una bitácora sobre las modificaciones”, indicando que *Usuarios AD (estado).xlsx* permite conocer el estado activo o inactivo de las cuentas y su última conexión. La auditoría consideró que esta información permite conocer una situación actual, pero no sustituye la trazabilidad histórica necesaria para reconstruir de manera consistente las novedades de acceso y privilegios durante el período evaluado.

El ciclo de accesos fue complementado mediante una validación en la que se recorrieron solicitudes desde su generación hasta la configuración técnica. Para los casos seleccionados se confirmó el funcionamiento del flujo básico.

En uno de ellos, correspondiente a Karin Yulieth Bonilla Hernández, el formulario de novedad registraba el perfil general “*USUARIO ESTÁNDAR*”, mientras que en el sistema se encontraba asignado el rol técnico *CONSULTA_PREDIO*. Al consultar sobre la correspondencia entre ambos elementos, Gestión TIC manifestó que dicha determinación se realiza con base en el conocimiento y experiencia del equipo y que actualmente no se dispone de un mecanismo formal

que relacione de manera homogénea los perfiles funcionales solicitados con los roles técnicos configurados.

Esta prueba permitió acreditar que el flujo de solicitud y aprovisionamiento funciona, pero también evidenció la necesidad de fortalecer la formalización del vínculo entre la necesidad funcional autorizada y el permiso técnico asignado. Esta condición dificulta que un tercero pueda reconstruir de manera independiente la correspondencia entre el acceso solicitado, su autorización y los roles o privilegios finalmente configurados.

En materia de retiro de accesos, se revisaron *usuarios bloqueados.pdf*, *Informe de cuentas de usuario de Active Directory.pdf* y casos correspondientes a usuarios retirados. Para los casos de Claudia Patricia Silva Yepes y Alexander Rodríguez Gómez se observaron cuentas bloqueadas o deshabilitadas y respaldos relacionados, por lo que quedó acreditado su estado final. No obstante, los soportes no permitieron reconstruir con precisión la fecha técnica en la que se produjo cada revocación y, por tanto, no fue posible determinar independientemente su oportunidad frente a la fecha de retiro. Esta condición se mantuvo como limitación de trazabilidad y no como evidencia de revocación tardía.

También se revisaron cuentas privilegiadas y de terceros como *nvillalop* e *itsoluciones*. Para la primera se identificaron obligaciones contractuales relacionadas con administración tecnológica, aunque dichas obligaciones no constituyen por sí solas una autorización específica para cada grupo privilegiado asignado. Para *itsoluciones*, Gestión TIC informó que el acceso VPN se habilita temporalmente por demanda. Estos casos evidencian la existencia de mecanismos de administración, pero también la necesidad de conservar trazabilidad suficiente sobre la justificación, vigencia, autorización y privilegios efectivamente otorgados.

Desde la perspectiva del procedimiento PD-71 y de la evaluación de seguridad, la evidencia permitió identificar una población de cuentas y privilegios y comprobar mecanismos operativos de administración; sin embargo, para la totalidad de la muestra no fue posible reconstruir integralmente la secuencia solicitud, autorización, configuración, revisión, modificación, vigencia, retiro, ni demostrar de manera homogénea la aplicación del principio de mínimo privilegio y de los controles aplicables sobre las cuentas especiales evaluadas.

En conjunto, la auditoría acreditó que RenoBo dispone de mecanismos operativos para administrar usuarios y privilegios, que existen perfiles diferenciados en Active Directory, NocoBase y plataformas de infraestructura y que el flujo básico de solicitud y aprovisionamiento funciona para los casos examinados. Tampoco se obtuvieron evidencias que permitan concluir de manera general la existencia de accesos no autorizados.

Las principales debilidades se concentran en cuatro elementos relacionados entre sí: trazabilidad histórica de altas, modificaciones y retiros; formalización de la correspondencia entre perfiles funcionales y roles técnicos; custodia y atribución individual de cuentas genéricas privilegiadas; y evidencia suficiente para demostrar de manera reproducible la vigencia, justificación y autorización de determinados privilegios. Estas condiciones convergen en la No Conformidad relacionada con la formalización y trazabilidad del ciclo de vida de accesos y privilegios, evitando formular hallazgos independientes por cada plataforma o excepción identificada.

En conclusión, la administración de accesos se encuentra implementada y operativa en los flujos evaluados, con mecanismos para solicitar, aprobar y configurar accesos y con perfiles y permisos diferenciados en las plataformas examinadas. No obstante, las debilidades identificadas en la trazabilidad histórica del ciclo de vida de determinados privilegios, la formalización de su correspondencia con las necesidades funcionales y la atribución individual de actuaciones mediante cuentas administrativas genéricas sustentan una No Conformidad específica.

Esta conclusión no implica que se hayan comprobado accesos indebidos, uso no autorizado de cuentas o revocaciones tardías; se refiere específicamente a la trazabilidad, formalización y demostrabilidad del control.

4.3.2.7 Gestión de activos de información

La evaluación de la gestión de activos de información se orientó a determinar si RenoBo cuenta con mecanismos para identificar, clasificar, valorar, actualizar y formalizar los activos de información utilizados por los procesos institucionales, de manera que puedan relacionarse con sus responsables, criticidad, necesidades de protección y riesgos asociados.

Como criterio principal se consideró la *GI-61, Gestión de Activos de Información*, la cual establece la necesidad de mantener un Inventario y Clasificación de Activos de Información, utilizando el formato institucional correspondiente y contemplando su valoración, clasificación y proceso de formalización y revisión. También se consideraron las disposiciones de la *Política General de Seguridad y Privacidad de la Información* y del *Plan de Seguridad y Privacidad de la Información* relacionadas con identificación, clasificación, criticidad y protección de activos.

Desde la evaluación del Sistema de Gestión de Seguridad de la Información se verificaron además actividades institucionales orientadas al diagnóstico y revisión de activos. En particular, el Acta No. 9 del Comité Institucional de Gestión y Desempeño del 30 de septiembre de 2025 incluyó dentro de su orden del día el diagnóstico de activos de información de los procesos y dependencias de RenoBo. Posteriormente, *FUSS_octubre2025.pdf* registró actividades de “Revisión y Análisis de Activos Críticos”, orientadas a identificar aplicaciones, sistemas y datos críticos migrados o por migrar a servicios en nube, así como actuaciones relacionadas con activos no críticos alojados localmente.

Estas evidencias permitieron establecer que la gestión de activos de información fue objeto de actividades concretas de revisión y seguimiento durante el período auditado y no permaneció limitada únicamente a la existencia de políticas o lineamientos. Para evaluar el instrumento vigente y su contenido específico se requirió evidencia adicional que permitiera efectuar una verificación independiente sobre la población de activos.

En respuesta a la solicitud complementaria se recibieron, entre otros soportes, los archivos *Hardware y Software_dic_2025.xls*, *2026-10 Inventario (1).xlsx*, *SERVIDORES.pdf* y el *Informe de cierre de inventarios 2026*. El archivo *2026-10 Inventario (1).xlsx* contenía información relacionada con activo, descripción, serial, equipo, ubicación, familia contable y tipo de dispositivo, mientras que *SERVIDORES.pdf* incluía relaciones de servidores, virtualizadores, máquinas virtuales y servicios.

La auditoría contrastó estos soportes con el instrumento requerido por GI-61. El análisis permitió establecer que los archivos aportados corresponden principalmente a inventarios físicos y tecnológicos, útiles para la administración de infraestructura, pero materialmente diferentes del Inventario y Clasificación de Activos de Información, que debe permitir identificar y clasificar activos de información con atributos asociados a valoración y protección.

En particular, con las evidencias recibidas no fue posible seleccionar una muestra del Inventario y Clasificación de Activos de Información y verificar de manera independiente atributos como identificador, responsable o propietario, clasificación de confidencialidad, integridad y disponibilidad, criticidad, ubicación o modalidad de alojamiento, fecha de actualización y relación con riesgos. Por esta razón, la auditoría no pudo evaluar integralmente la calidad, integridad y actualización del instrumento vigente.

Durante la solicitud de evidencias, Gestión TIC indicó que la carpeta correspondiente a GI-61 contenía versiones de diciembre de 2025 y octubre de 2026 del Inventario y Clasificación de Activos de Información. Sin embargo, los archivos efectivamente disponibles para revisión no correspondían materialmente al instrumento descrito, sino a inventarios tecnológicos y físicos. En consecuencia, no fue posible comprobar la versión vigente del Inventario y Clasificación de Activos de Información ni su proceso de formalización institucional.

Esta situación debe diferenciarse de la gestión de activos tecnológicos evaluada en el aspecto de infraestructura. La auditoría sí verificó la existencia y utilización de inventarios de hardware, software, servidores y otros componentes tecnológicos. La limitación aquí identificada se refiere específicamente al instrumento de activos de información previsto por GI-61 y a la imposibilidad de verificar sus atributos, actualización y formalización con la evidencia disponible.

En este sentido, las actividades de diagnóstico documentadas en el Comité Institucional de Gestión y Desempeño y en los informes FUSS constituyen evidencia favorable de que RenoBo ha adelantado ejercicios relacionados con la identificación y análisis de activos. No obstante, dichos soportes no sustituyen la disponibilidad del inventario vigente para efectuar una prueba sobre su población y verificar los atributos definidos institucionalmente.

La condición observada constituye una limitación de verificación relevante. La evidencia disponible no permite afirmar que RenoBo carezca de un Inventario y Clasificación de Activos de Información, pero tampoco permite acreditar que dicho instrumento se encuentre actualizado, completo y formalizado de acuerdo con GI-61. En consecuencia, no resulta procedente convertir la falta de disponibilidad del soporte específico en un incumplimiento material confirmado.

En conclusión, se verificaron actividades institucionales de diagnóstico y revisión de activos, así como la existencia de inventarios tecnológicos utilizados para administrar infraestructura. No obstante, no fue posible comprobar integralmente el Inventario y Clasificación de Activos de Información requerido por GI-61 ni verificar mediante muestreo sus atributos, actualización y formalización vigente. Esta condición se mantiene como limitación de verificación y, para efectos de la clasificación de resultados de la auditoría, se presenta como Oportunidad de Mejora orientada a fortalecer la disponibilidad, formalización y trazabilidad del instrumento, sin que constituya una No Conformidad confirmada.

4.3.2.8 Seguridad y privacidad de la información

La evaluación de seguridad y privacidad de la información se orientó a determinar si RenoBo dispone de un marco institucional formalizado para la gestión de la seguridad de la información, si existen controles y mecanismos implementados para su operación y si los resultados de evaluaciones, diagnósticos y actividades de seguimiento se traducen en acciones de mejora trazables hasta su tratamiento y cierre.

Como criterios se consideraron la *Política General de Seguridad y Privacidad de la Información*, PL-16, el *Plan de Seguridad y Privacidad de la Información* (PSPI) 2026-2030, los procedimientos e instrumentos asociados al Sistema de Gestión de Seguridad de la Información (SGSI), el Modelo de Seguridad y Privacidad de la Información (MSPI) y los demás documentos institucionales relacionados con gestión de riesgos, vulnerabilidades, incidentes y controles de seguridad.

La revisión documental permitió verificar que RenoBo cuenta con un marco formal para la gestión de seguridad y privacidad de la información. Durante el período evaluado se evidenció la actualización y formalización de políticas, planes, procedimientos e instrumentos relacionados con el SGSI, así como actividades de implementación y seguimiento desarrolladas por Gestión TIC.

Entre los soportes revisados se encontraron la *Política General de Seguridad y Privacidad de la Información*, el PSPI 2026-2030, el Plan de Tratamiento de Riesgos, procedimientos asociados con gestión de incidentes y vulnerabilidades, matrices de riesgos, ejercicios de autodiagnóstico MSPI, informes FUSS y actas de instancias institucionales de gestión y desempeño.

El contraste de estas evidencias permitió establecer que el SGSI no se encuentra limitado a una estructura documental. Se observaron actividades concretas relacionadas con seguridad perimetral, segmentación de red, revisión de registros, actualización de configuraciones, gestión de accesos, análisis de vulnerabilidades, respaldos, evaluación de riesgos y fortalecimiento de controles tecnológicos. En consecuencia, existe evidencia de implementación y operación de mecanismos específicos de seguridad en diferentes componentes evaluados.

El análisis del autodiagnóstico MSPI permitió identificar además un ejercicio institucional de valoración del nivel de implementación de controles y capacidades de seguridad. Para una muestra de componentes revisados se observaron registros de valoración y recomendaciones asociadas. No obstante, en varios casos los campos destinados a documentar brechas y recomendaciones se encontraban sin diligenciar, lo que limitó la posibilidad de reconstruir la relación entre el resultado obtenido, la brecha identificada y la acción definida para su tratamiento.

La auditoría examinó igualmente la forma en que los resultados de evaluaciones, diagnósticos y asuntos de seguridad son llevados a instancias de gobierno. Se evidenciaron presentaciones y discusiones en el Comité Institucional de Gestión y Desempeño, incluyendo temas relacionados con seguridad de la información, activos y avances del SGSI. Por tanto, no se concluyó ausencia de mecanismos institucionales de gobierno o de espacios para tratar asuntos de seguridad.

Dentro de la estructura prevista para el SGSI se identificó también la referencia a una Mesa de Seguridad y Privacidad de la Información. Durante las validaciones se informó que esta instancia específica no se había implementado y que los temas correspondientes estaban siendo tratados mediante el Comité Institucional de Gestión y Desempeño. Esta situación fue considerada como un elemento de contexto sobre el modelo de gobernanza utilizado durante el período y no como fundamento autónomo de incumplimiento.

La principal debilidad se identificó al evaluar la trazabilidad del ciclo de mejora continua. Para los asuntos seleccionados no fue posible reconstruir de manera sistemática la secuencia evaluación o diagnóstico, brecha, acción de mejora, responsable, fecha objetivo, seguimiento, validación de efectividad, cierre.

En particular, los resultados del autodiagnóstico MSPI y otros asuntos identificados mediante actividades del SGSI no presentaron de manera homogénea evidencia suficiente que permitiera determinar qué acciones específicas fueron definidas frente a cada brecha, quién asumió su ejecución, cuál fue el plazo establecido, qué seguimiento se realizó y bajo qué criterio se consideró tratada o cerrada.

Esta condición no permite concluir que la Entidad no haya adelantado acciones de mejora. Durante la auditoría se observaron actuaciones concretas de fortalecimiento de seguridad. La debilidad corresponde a la capacidad para demostrar de manera sistemática y reproducible que los resultados obtenidos mediante los distintos mecanismos de evaluación del SGSI alimentan un ciclo formal de tratamiento, seguimiento y cierre.

Respecto de la gestión de incidentes de seguridad, se verificó la existencia de un procedimiento institucional y de mecanismos tecnológicos que pueden generar información relacionada con eventos de seguridad. No obstante, durante la auditoría no se dispuso de una población consolidada y verificable de incidentes ocurridos en el período que permitiera seleccionar una muestra y reconstruir casos reales desde su identificación y clasificación hasta la contención, tratamiento, recuperación y cierre.

Por esta razón, la auditoría no contó con evidencia suficiente para emitir una conclusión integral sobre la efectividad operacional del proceso de gestión de incidentes durante el período evaluado. Esta situación se considera una limitación de aseguramiento y no evidencia de que el proceso sea inexistente o inoperante.

En materia de vulnerabilidades se comprobó la realización de ejercicios técnicos sobre sistemas institucionales, lo que acredita capacidades de identificación y análisis. Las condiciones relacionadas con periodicidad, remediación, revalidación y cierre técnico fueron evaluadas específicamente en el aspecto de Gestión de riesgos de seguridad digital y gestión de vulnerabilidades, por lo que no se duplican como resultado independiente dentro de este apartado.

De manera similar, la valoración y tratamiento de riesgos de seguridad digital cuenta con instrumentos y controles formalizados. Las limitaciones específicas identificadas en la relación entre riesgos, controles, evidencias, efectividad y riesgo residual se desarrollan en el apartado correspondiente a Gestión de riesgos de seguridad digital.

En conjunto, las evidencias permiten acreditar que RenoBo cuenta con un SGSI formalizado y con actividades materiales de implementación sobre diferentes componentes tecnológicos y organizacionales. Se observaron políticas, planes, procedimientos, matrices, mecanismos de monitoreo y controles con evidencia concreta de operación. Estos elementos sustentan una Conformidad respecto de la formalización e implementación de mecanismos del Sistema de Gestión de Seguridad de la Información.

No obstante, la evidencia disponible no permitió acreditar de manera homogénea un ciclo sistemático mediante el cual las brechas y oportunidades identificadas en autodiagnósticos, evaluaciones y ejercicios de seguimiento sean transformadas en acciones con responsables, plazos, seguimiento, validación de efectividad y cierre verificable. Esta condición sustenta la No Conformidad relacionada con el seguimiento y mejora continua del SGSI.

En conclusión, RenoBo presenta avances materiales en la formalización e implementación de su Sistema de Gestión de Seguridad de la Información y dispone de controles y mecanismos operativos sobre diferentes componentes evaluados. La debilidad identificada no corresponde a una ausencia general del SGSI ni permite concluir su inefectividad integral; se concentra específicamente en la trazabilidad y demostrabilidad del ciclo de seguimiento y mejora continua. La evaluación de incidentes estuvo limitada por la ausencia de una población verificable para muestreo, mientras que las condiciones específicas de riesgos y vulnerabilidades se desarrollan en los apartados correspondientes.

4.3.2.9 Soporte tecnológico

La evaluación del soporte tecnológico se orientó a determinar si RenoBo cuenta con una mesa de servicio implementada, si las solicitudes e incidentes tecnológicos son registrados, asignados, gestionados, escalados y cerrados, y si la información generada permite realizar seguimiento sobre volumen, estado y tiempos de atención.

Como criterio principal se consideró el procedimiento *PD-70, Soporte técnico y mantenimiento correctivo de dispositivos TI V3*, que establece actividades relacionadas con registro, clasificación, diagnóstico, asignación, gestión, escalamiento, solución y cierre de solicitudes. También se consideraron las disposiciones del *Plan Estratégico de Tecnologías de la Información (PETI)*, que prevén el registro de requerimientos en la herramienta de gestión, el seguimiento de incidentes, peticiones y requerimientos y la disponibilidad de “Estadísticas de atención, reportes de ANS, con histórico consultable”.

Para evaluar la operación general de la mesa de servicio se revisaron *Informe Técnico glpi 2025.pdf*, *glpi 2025.csv*, la exportación *GLPI 2026 - HASTA 5 OCT* e *Informe Técnico glpi 2026.pdf*. El informe correspondiente a 2025 señala que la Dirección Administrativa de TIC implementó formalmente GLPI 10.0.18 en abril de 2025, a partir de lo cual se estructuró el registro de solicitudes y la medición de tiempos de atención. Para el período cubierto de 2025 se reportaron 2.764 solicitudes y una tasa de cierre del 100 %.

Respecto de los meses de enero a marzo de 2025, Gestión TIC informó que antes de la implementación formal de GLPI no se disponía de un sistema centralizado ni de una base consolidada para la gestión de la mesa de ayuda. Esta condición se consideró una limitación

temporal de información asociada al momento de implementación de la herramienta y no una falla atribuible retrospectivamente a GLPI.

Para 2026 se revisó la exportación de tickets correspondiente al período comprendido entre el 1 de enero y el 5 de octubre, así como el *Informe Técnico glpi 2026.pdf*. Gestión TIC reportó 4.293 tickets, una tasa de cierre de 99,8 % y una mediana de solución de 26,57 horas. La auditoría validó la información recibida y logró reproducir el universo de 4.293 registros y los principales indicadores generales de cierre, proporcionando evidencia favorable sobre la consistencia aritmética de la información reportada.

La revisión identificó oportunidades de mejora en la calidad y completitud de los registros. En la población de 2026 se encontraron 396 tickets sin categoría, equivalentes al 9,2 % del universo, de los cuales 270 se concentraron en julio. El propio *Informe Técnico glpi 2026.pdf* calificó esta situación como un “punto de atención para la calidad y consistencia del registro de solicitudes”. Asimismo, se identificaron registros sin técnico asignado y algunos casos en los cuales la información temporal no permitía reconstruir de manera consistente la secuencia de atención.

También se revisó la metodología utilizada para calcular indicadores de tiempo. El informe emplea como duración la diferencia entre la Fecha de Apertura y la Última actualización para los tickets en estado final. La auditoría pudo reproducir los valores calculados mediante esta metodología; sin embargo, determinó que dicha medida no equivale necesariamente al tiempo efectivo de solución y no permite, por sí sola, concluir cumplimiento o incumplimiento de acuerdos de nivel de servicio, debido a que no incorpora de manera suficiente elementos como pausas, horarios de servicio, tiempos atribuibles a terceros o estados intermedios.

La evaluación general fue complementada con una muestra dirigida de casos revisada frente al procedimiento PD-70. Se analizaron los tickets #7105 “Solicitud de préstamo equipo portátil”, #4059 “Novedad Acceso Lógico”, #7184 “Inconveniente acceso DRIVE”, #6814 “Fiducias Álvaro García Terminación” y #4017 “Solicitud de restablecimiento del internet”, seleccionados para observar diferentes características de atención, incluyendo soporte de primer y segundo nivel, comportamiento frente a tiempos configurados y escalamiento a terceros.

El ticket #7105 permitió observar apertura, asignación y solución dentro del mismo día. Por su parte, el ticket #6814 presentó en GLPI una marcación asociada con el tiempo de solución configurado, evidenciando que la herramienta conserva información que permite identificar el comportamiento del caso frente a los parámetros registrados. Esta marcación fue considerada como un dato operacional de la herramienta y no, por sí sola, como evidencia suficiente para concluir incumplimiento de un acuerdo formal de nivel de servicio.

El ticket #4017, relacionado con una caída del canal, permitió reconstruir el escalamiento hacia ETB, acreditándose que la herramienta soporta también la gestión de casos que requieren intervención de terceros.

La muestra confirmó que GLPI se encuentra operativa para registrar, asignar, gestionar y cerrar solicitudes y para conservar información temporal asociada con su atención. También se acreditó la existencia de mecanismos de escalamiento a proveedores cuando la solución requiere intervención externa.

En los casos examinados se identificaron algunas diferencias de clasificación y documentación. El ticket correspondiente al préstamo de un portátil fue registrado como “Incidencia”, aunque por su naturaleza correspondía a una solicitud de servicio. En otro de los casos presentado como ejemplo de Nivel 2 no fue posible comprobar inequívocamente en los registros la transición o clasificación hacia dicho nivel. Adicionalmente, algunas soluciones contenían descripciones generales que dificultaban reconstruir con detalle la actuación técnica realizada.

Estas excepciones deben interpretarse en el contexto del funcionamiento general de la mesa de servicio. No se obtuvo evidencia de pérdida generalizada de solicitudes, ausencia de atención o incapacidad para registrar y cerrar casos. Su efecto se concentra principalmente en la calidad de las estadísticas, el análisis de tendencias, la medición de niveles de atención y la capacidad de reconstruir de manera uniforme las actuaciones técnicas efectuadas.

En conjunto, la auditoría acreditó una operación sostenida de GLPI y la capacidad de Gestión TIC para administrar un volumen significativo de solicitudes y requerimientos. Los universos y principales indicadores generales pudieron ser reproducidos, se observaron porcentajes elevados de cierre y las pruebas de casos permitieron comprobar registro, asignación, resolución y escalamiento.

Las oportunidades de mejora se concentran en la clasificación y completitud de determinados campos, asignación de responsables, documentación de las soluciones, trazabilidad entre niveles de atención y metodología utilizada para algunos indicadores de tiempo. Estas condiciones no fueron consideradas evidencia de una falla general de la mesa de servicio, sino oportunidades para fortalecer la calidad de la información utilizada en la gestión y evaluación del soporte.

En conclusión, el soporte tecnológico mediante GLPI se encuentra operativamente acreditado, con evidencia suficiente de registro, atención, cierre y escalamiento de solicitudes en las muestras examinadas. La herramienta constituye un mecanismo operativo para la gestión de la mesa de servicio; no obstante, requiere fortalecer la calidad y consistencia de sus registros para mejorar la confiabilidad de las estadísticas, la medición de niveles de servicio y la trazabilidad detallada de la atención. Las situaciones identificadas se mantienen como Oportunidad de Mejora y no dieron lugar a una No Conformidad independiente.

4.3.2.10 Mantenimiento preventivo y correctivo

La evaluación del mantenimiento preventivo y correctivo se orientó a determinar si RenoBo cuenta con mecanismos para planificar, ejecutar y documentar las actividades de mantenimiento sobre equipos de usuario final e infraestructura tecnológica, y si las novedades identificadas durante las intervenciones pueden ser objeto de seguimiento hasta su tratamiento y cierre.

Como criterios principales se consideraron el numeral 6.4.2.4.1.4 “Mantenimiento” del *Plan Estratégico de Tecnologías de la Información (PETI)*, que establece la necesidad de contar con un plan de mantenimiento basado en el inventario de infraestructura física y organizado de acuerdo con el tipo de componente y su periodicidad, así como el procedimiento *PD-52, Mantenimiento de equipos de TI V3*, que contempla programación, ejecución y validación posterior de las actividades realizadas.

Para el componente correctivo se revisó también *PD-70, Soporte técnico y mantenimiento correctivo de dispositivos TI V4*, de fecha 4 de junio de 2026. Este procedimiento establece, entre otros elementos, el registro de la solicitud en GLPI, clasificación y diagnóstico, escalamiento cuando corresponda, documentación de la intervención, validación funcional, actualización del inventario y cierre del registro. Considerando su fecha de expedición, fue utilizado como criterio únicamente para el período en que se encontraba vigente y no como requisito aplicable de forma retroactiva a intervenciones anteriores.

Para verificar el mantenimiento preventivo sobre equipos de usuario final se revisaron los archivos *PC PISO 16 MTO.pdf*, *PC PISO 22 MTO.pdf*, *PC PISO 23 MTO.pdf* y *PC PISO 24 MTO.pdf*. Las fichas correspondían a órdenes de servicio asociadas al Contrato 438-2023 y registraban, entre otros campos, fecha de servicio, identificación del activo, características técnicas, trabajo realizado, estado del equipo y observaciones. En los casos examinados se evidenció la marcación “Mantenimiento Preventivo X” y campos destinados a clasificar los equipos como operativos, inoperativos, pendientes de reemplazo o requeridos de mantenimiento correctivo, suministros o repuestos.

La auditoría revisó el conjunto de fichas y determinó 174 registros efectivos de mantenimiento correspondientes a 169 activos únicos. De las 174 fichas examinadas, 172 pudieron reconciliarse con el inventario institucional mediante código o placa, evidenciándose una relación significativa entre los soportes de mantenimiento y la información de activos.

Como ejercicio exploratorio se contrastaron las fichas con el inventario vigente de computadores, equipos All-in-One y portátiles, obteniéndose una cobertura observable aproximada del 81,6 %. Este porcentaje no fue utilizado como indicador formal de cumplimiento del plan de mantenimiento, debido a que el inventario empleado como denominador correspondía a una fecha posterior y no necesariamente representaba con exactitud la población programada para la fecha de ejecución de los mantenimientos.

Para evaluar las actividades sobre infraestructura tecnológica se revisaron *PLAN_DE_TRABAJO_MANTENIMIENTO-RENOBO-30012026.pdf*, *Mantenimientos Programados 2026.pdf* e *Informe actualización de firmware PPDM.pdf*. Los soportes permitieron verificar actividades realizadas sobre distintos componentes, aunque no fue posible reconstruir con el mismo nivel de evidencia, para todos los elementos incluidos en la programación, una secuencia individual completa de programación, ejecución, resultado y cierre.

El *Informe actualización de firmware PPDM.pdf* presentó un nivel de trazabilidad particularmente completo. La auditoría verificó la actualización de Dell PowerProtect Data Manager (PPDM) desde la versión 5.19.1.0-196 a la 5.20.1.0-306, incluyendo programación, ejecución, seguimiento y validación del estado posterior. El informe registró que los health checks finalizaron sin fallas y que Dell confirmó satisfactoriamente la culminación de la actividad. Este caso constituye evidencia favorable de un ciclo de mantenimiento documentado desde la intervención hasta la comprobación posterior del funcionamiento.

La evaluación fue complementada con soportes correspondientes a infraestructura Fortinet, entre ellos mantenimientos del FortiGate 400F realizados durante 2026, *Mantenimiento FortiNAC 500 F 15 septiembre.pdf* y *Mantenimiento preventivo fortiswitch 16 Octubre.pdf*. Para FortiGate se observaron actualizaciones y verificaciones posteriores sobre conectividad, VPN, alta

disponibilidad y otros servicios. En el caso de FortiNAC, el informe documentó la intervención realizada el 15 de septiembre de 2026, identificando el equipo, hostname, serial y actividades de revisión y configuración efectuadas.

El soporte correspondiente a FortiSwitch contenía un plan de trabajo que incluía actividades previstas, respaldo de configuraciones, actualización, pruebas y mecanismos de rollback. En este caso, la auditoría consideró que el documento acreditaba la planeación del mantenimiento, pero no constituía por sí solo evidencia suficiente de la ejecución y finalización de todas las actividades previstas.

Para evaluar la relación entre mantenimiento preventivo y tratamiento correctivo se revisaron las observaciones consignadas en las fichas de los equipos y se contrastaron con los registros GLPI disponibles. La auditoría identificó 27 activos con novedades materiales susceptibles de requerir seguimiento posterior, entre ellas ausencia de FortiClient, problemas de sistema operativo, periféricos faltantes, fallas de pantalla, problemas de identificación física y situaciones relacionadas con garantía.

El cruce permitió reconstruir directamente la relación con tickets GLPI únicamente para una parte de los casos. Esta situación no fue considerada evidencia de que las demás novedades no hubieran sido atendidas, dado que su seguimiento pudo haberse registrado bajo títulos, descripciones o mecanismos que no permitían una coincidencia directa con la exportación examinada. La condición comprobada corresponde a una limitación para reconstruir de manera sistemática la secuencia novedad preventiva, actuación correctiva, solución, cierre.

Durante la auditoría se había previsto adicionalmente una validación destinada a recorrer una novedad de mantenimiento desde su identificación hasta el ticket correctivo, solución y cierre. Esta prueba no fue ejecutada, por lo cual no se obtuvieron elementos adicionales de aseguramiento sobre la trazabilidad integral del ciclo correctivo.

En conjunto, las evidencias permitieron acreditar actividades efectivamente ejecutadas de mantenimiento preventivo y correctivo sobre equipos de usuario final y componentes de infraestructura tecnológica. Se observaron soportes de intervención, reconciliación con inventarios, actualizaciones técnicas, validaciones posteriores de funcionamiento y casos con trazabilidad completa, como la actualización de PPDM.

La principal limitación se concentra en la trazabilidad integral del ciclo de mantenimiento. No se dispuso de un mecanismo consolidado que permitiera contrastar de forma uniforme la población programada frente a la totalidad de mantenimientos ejecutados, pendientes y sus resultados, ni reconstruir sistemáticamente el tratamiento posterior de todas las novedades identificadas durante las actividades preventivas.

Esta condición se encuentra directamente relacionada con la gestión del ciclo de vida de los activos tecnológicos y, por tanto, no se presenta como una Oportunidad de Mejora ni como una No Conformidad independiente dentro de este aspecto. Las evidencias obtenidas complementan la Oportunidad de Mejora desarrollada en el apartado 4. Gestión de infraestructura tecnológica, relacionada con la integración y trazabilidad entre inventario, estado del activo, mantenimiento programado y ejecutado, novedades, acciones posteriores y decisiones de continuidad, renovación o retiro.

En conclusión, se acreditaron actividades de mantenimiento preventivo y correctivo efectivamente ejecutadas en las muestras examinadas, tanto sobre equipos de usuario final como sobre componentes de infraestructura tecnológica, incluyendo casos con validación posterior de funcionamiento. La principal oportunidad de fortalecimiento corresponde a la trazabilidad consolidada entre activo, programación, mantenimiento ejecutado, resultado, novedad identificada, acción correctiva y cierre. Esta condición se integra a la Oportunidad de Mejora asociada con el ciclo de vida de los activos tecnológicos y no da lugar a un resultado independiente.

4.3.2.11 Gestión de riesgos de seguridad digital

La evaluación de la gestión de riesgos de seguridad digital se orientó a determinar si RenoBo cuenta con mecanismos para identificar, valorar, tratar y hacer seguimiento a los riesgos asociados con la seguridad de la información y los componentes tecnológicos, y si las valoraciones residuales pueden ser sustentadas y reproducidas razonablemente a partir de los controles, tratamientos y evidencias disponibles. Como componente relacionado, se evaluó la gestión de vulnerabilidades técnicas, considerando su identificación periódica, tratamiento, remediación, revalidación y cierre.

Como criterios principales se consideraron la *Política General de Seguridad y Privacidad de la Información*, particularmente sus numerales 9.7.2, Gestión del riesgo y mejora continua y 9.8.1, Gestión del riesgo y controles, así como el *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026-2030*. Estos instrumentos establecen la necesidad de articular la identificación y valoración de los riesgos con controles, acciones de tratamiento, responsables, seguimiento, indicadores y evidencia de ejecución.

Valoración y tratamiento de riesgos de seguridad digital

Para evaluar la valoración y tratamiento de riesgos de seguridad digital, la auditoría revisó el archivo *Gestión_Riesgos.xlsx*, específicamente la hoja *03_Gestion_Riesgos*, que contenía una población de 21 riesgos identificados desde R-001 hasta R-021. Mediante muestreo dirigido se seleccionaron cinco riesgos: R-015, Gestión Ambiental; R-004, Gestión Urbana; R-018, Gestión TIC; R-014, Gestión del Talento Humano; y R-012, Gestión Contractual. La selección consideró características como nivel de valoración, relación con información institucional y vinculación con infraestructura y sistemas tecnológicos.

Para los cinco casos seleccionados se reconstruyeron los elementos utilizados en la valoración, incluyendo probabilidad, impacto, riesgo inherente, controles y riesgo residual. El ejercicio no identificó errores aritméticos aparentes al reproducir los coeficientes implícitos de los resultados almacenados, por lo que la auditoría no concluyó que las valoraciones fueran matemáticamente incorrectas.

Las fórmulas del archivo contenían referencias a un libro externo denominado *[1]10_Reglas_Riesgo*, que no hacía parte de la copia disponible para la prueba. Esta situación limitó la reproducción independiente de la totalidad de las reglas, parámetros y umbrales incorporados en el instrumento. Esta condición se consideró un elemento complementario de reproducibilidad y no constituye, por sí misma, el fundamento de la No Conformidad.

La auditoría observó que los 21 riesgos contenidos en *Gestión_Riesgos.xlsx* registraban como decisión de tratamiento “Reducir” y como estado “En tratamiento”. Aunque la matriz relacionaba riesgos, controles y decisiones de tratamiento, la evidencia disponible no permitía reconstruir de manera completa y homogénea la secuencia entre riesgo identificado, control aplicado, acción específica de tratamiento, responsable, fecha objetivo, evidencia de ejecución, evaluación de efectividad y cierre.

En diferentes casos se observaron disminuciones entre la valoración inherente y la residual. Sin embargo, no fue posible establecer de manera suficientemente trazable cómo la ejecución y evaluación de los controles sustentaban las reducciones registradas en la probabilidad o el nivel residual. Esta condición no permite concluir que las reducciones sean incorrectas ni que los controles sean inefectivos; limita la capacidad para demostrar de manera independiente el efecto atribuido a los controles y tratamientos sobre el nivel de riesgo.

De forma complementaria se revisó *Mapa_de_Riesgos_SGSI_2026_V1.0(1).xlsx*, que contenía una población de 45 riesgos. Ambos instrumentos fueron evaluados separadamente y no se asumió correspondencia automática entre sus identificadores, debido a que presentan poblaciones, estructuras y numeraciones diferentes.

Sobre el Mapa de Riesgos SGSI se seleccionaron seis riesgos asociados con Gestión TIC, identificados con los números 33 y 41 a 45, y se examinaron 25 registros de controles. Las pruebas permitieron reproducir determinadas operaciones individuales de reducción; sin embargo, se observaron limitaciones en la documentación y soportes utilizados para demostrar la implementación y efecto de los controles considerados dentro de las valoraciones.

De los 25 registros examinados, 12 controles figuraban como “*Sin Documentar*” y 11 como “*Sin Registro*”. Estas denominaciones constituyen evidencia de insuficiencia de soporte dentro del propio instrumento, pero no permiten afirmar que los controles sean inexistentes, que no hayan operado o que resulten inefectivos. Su efecto para la auditoría se concentra en la capacidad de demostrar de manera independiente su diseño, aplicación y contribución a la valoración residual.

Las solicitudes complementarias hicieron referencia a informes mensuales de seguimiento del Plan de Acción y a un Plan de Mejora Continua como posibles fuentes adicionales para reconstruir la evolución de los tratamientos. Estos documentos no estuvieron disponibles dentro del período de revisión y, por tanto, las conclusiones se fundamentaron en las matrices y demás evidencias efectivamente examinadas.

En consecuencia, la debilidad identificada no corresponde a la inexistencia de una metodología de riesgos ni a errores generalizados de cálculo. RenoBo dispone de matrices, riesgos identificados, controles y decisiones de tratamiento. La condición se concentra en la trazabilidad necesaria para relacionar de forma reproducible los controles y acciones ejecutadas con sus evidencias, evaluación de efectividad y efecto sobre el nivel de riesgo residual.

Esta condición sustenta la No Conformidad relacionada con la trazabilidad y reproducibilidad de la valoración y tratamiento de riesgos de seguridad digital.

Gestión de vulnerabilidades

Como componente operacional de la gestión del riesgo digital, se evaluó la gestión de vulnerabilidades. El procedimiento institucional define un ciclo que comprende identificación, priorización, tratamiento, remediación y revalidación y establece como mínimo la realización de análisis anuales sobre los activos comprendidos dentro de su alcance, además de revisiones asociadas con eventos que puedan modificar su exposición.

El *Plan de Seguridad y Privacidad de la Información* (PSPI) 2026 establece adicionalmente una gestión trimestral de vulnerabilidades para el portal web, sede electrónica y servicios expuestos, acompañada de informes y plan de remediación. En consecuencia, para estos componentes se consideró la periodicidad específica definida en dicho instrumento.

La revisión documental permitió identificar ejercicios técnicos efectivamente realizados durante 2026 mediante herramientas especializadas. Se examinaron informes correspondientes a ciclos desarrollados entre febrero y marzo y durante julio de 2026 sobre diferentes sistemas institucionales. Estas evidencias acreditan que RenoBo cuenta con capacidades técnicas y que durante el período auditado se realizaron actividades de identificación y análisis de vulnerabilidades.

La existencia de estos ejercicios no permitió, sin embargo, acreditar una ejecución periódica y sostenida durante todo el período aplicable ni reconstruir suficientemente el ciclo posterior de tratamiento para determinados hallazgos relevantes. Por esta razón, la auditoría realizó una verificación de trazabilidad orientada a recorrer la secuencia identificador, severidad, activo, responsable, tratamiento, fecha objetivo, remediación, revalidación, estado final.

Para efectos de esta prueba, el registro de una vulnerabilidad como “solucionada” no fue considerado por sí solo evidencia suficiente de cierre cuando no estaba acompañado de reescaneo, revalidación técnica u otro mecanismo equivalente que permitiera comprobar que la condición identificada había dejado de presentarse.

Durante la sesión en vivo, los responsables de Tecnología indicaron que actualmente no cuentan con un proceso operativo periódico soportado en una herramienta, servicio o proveedor mediante el cual se ejecuten de forma sostenida los análisis de vulnerabilidades. Esta manifestación permitió diferenciar la condición de una simple ausencia documental: aunque durante el período existieron ejercicios técnicos de análisis, no se encontraba operando de manera periódica un mecanismo que asegurara su continuidad conforme a las frecuencias previstas.

Respecto de hallazgos de severidad relevante incluidos en análisis anteriores, tampoco fue posible reconstruir de manera completa y homogénea su tratamiento hasta una remediación y posterior revalidación técnica. Para vulnerabilidades asociadas con el portal institucional se informó que el responsable actual no contaba con la trazabilidad histórica completa de determinadas remediaciones. Para un hallazgo relacionado con la intranet tampoco se evidenció un registro suficiente de la corrección acompañado de una validación técnica posterior que permitiera acreditar su cierre.

El cambio de responsables constituye un elemento contextual, pero no modifica la necesidad institucional de conservar la evidencia del tratamiento y cierre de las vulnerabilidades. De igual forma, la identificación de categorías técnicas similares en diferentes ejercicios fue considerada un elemento de contexto y no evidencia suficiente para concluir que se tratara necesariamente de las mismas vulnerabilidades que hubiesen permanecido sin remediación.

La debilidad identificada tampoco se refiere a la ausencia de una herramienta comercial determinada. El análisis periódico puede ejecutarse mediante capacidades internas, herramientas propias, servicios especializados o proveedores. La condición relevante es que exista un mecanismo periódico acorde con los criterios institucionales y que los hallazgos puedan ser trazados desde su identificación hasta su remediación y cierre técnico verificable.

En consecuencia, la auditoría comprobó la existencia de diseño formal y antecedentes de ejecución efectiva de análisis de vulnerabilidades, pero confirmó una debilidad en la operación periódica actual y en la trazabilidad del tratamiento y cierre técnico de determinados hallazgos. Esta condición incrementa el riesgo de que nuevas exposiciones no sean identificadas oportunamente o que vulnerabilidades previamente reportadas permanezcan sin un cierre técnicamente demostrable.

Esta condición sustenta una No Conformidad específica relacionada con la periodicidad, tratamiento y cierre técnico de la gestión de vulnerabilidades.

En conclusión, RenoBo dispone de instrumentos estructurados para la identificación, valoración y tratamiento de riesgos de seguridad digital, y las muestras revisadas no evidenciaron errores aritméticos generalizados en las valoraciones. No obstante, se identificaron limitaciones para demostrar de manera reproducible la relación entre controles, acciones de tratamiento, evidencias de ejecución, evaluación de efectividad y reducción del riesgo residual, condición que sustenta una No Conformidad.

De manera diferenciada, se verificó la realización de ejercicios técnicos de análisis de vulnerabilidades durante el período evaluado, pero se confirmó que actualmente no existe un mecanismo periódico de ejecución y que para determinados hallazgos no fue posible reconstruir integralmente la remediación, revalidación y cierre técnico. Esta condición sustenta una segunda No Conformidad, independiente de la relacionada con la valoración y tratamiento de riesgos.

4.3.2.12 Cumplimiento de procedimientos, manuales y políticas institucionales

La evaluación del cumplimiento de procedimientos, manuales y políticas institucionales se desarrolló de manera transversal sobre los diferentes componentes del proceso Gestión TIC, con el propósito de determinar si los lineamientos formalmente establecidos por RenoBo se encontraban reflejados en la operación observada durante el período auditado.

Conforme al Plan de Trabajo de Auditoría, se utilizaron como criterios los procesos, procedimientos, políticas, guías, planes y demás documentos del Sistema Integrado de Gestión relacionados con Gestión TIC, complementados con las disposiciones contenidas en el PETI y en los instrumentos institucionales específicos aplicables a cada uno de los aspectos evaluados.

La evaluación distinguió entre existencia documental, diseño del control, implementación, operación y efectividad, y consideró la fecha de aprobación o entrada en vigencia de cada instrumento. En consecuencia, los requisitos formalizados o actualizados durante 2026 fueron aplicados únicamente al período en que resultaban exigibles y no de manera retroactiva a actuaciones realizadas con anterioridad. Este criterio fue particularmente relevante para los procedimientos relacionados con seguridad de la información, acceso lógico, soporte y mantenimiento.

Gobierno y seguimiento de TI

En materia de Gobierno y seguimiento de TI se evaluaron los mecanismos previstos en el PETI para realizar autoevaluaciones de Estrategia y Gobierno de TI y presentar el informe anual correspondiente ante la instancia institucional definida.

La evidencia examinada mostró actividades efectivas de seguimiento, revisión, decisión y actualización del PETI. No obstante, no quedó acreditado integralmente el cumplimiento de los mecanismos formales de autoevaluación previstos en el Plan ni la presentación del informe anual ante la instancia establecida.

Esta condición no implica ausencia general de seguimiento al PETI, puesto que se comprobaron otros mecanismos de revisión y decisión durante el período. Las condiciones específicas relacionadas con confiabilidad, trazabilidad y reproducibilidad de la medición y con los mecanismos formales de evaluación se desarrollan en el apartado 2. Seguimiento al PETI y sustentan la No Conformidad correspondiente.

Administración de accesos

Para administración de accesos se utilizó el procedimiento *PD-71, Administración de Acceso Lógico*, considerando la versión aplicable durante cada período. Las pruebas documentales y en vivo permitieron comprobar la operación del flujo básico de solicitud, aprobación y configuración de accesos en los casos examinados, así como la existencia de cuentas deshabilitadas para usuarios retirados y perfiles diferenciados en Active Directory, NocoBase y otras plataformas.

La aplicación integral del procedimiento no pudo reconstruirse con el mismo nivel de trazabilidad para todo el ciclo de vida de los accesos. Se identificaron limitaciones en la trazabilidad histórica de modificaciones y retiros de privilegios, en la formalización de la correspondencia entre perfiles funcionales y roles técnicos y en la atribución individual de actuaciones realizadas mediante determinadas cuentas administrativas genéricas.

Estas condiciones corresponden a debilidades de formalización y trazabilidad y no constituyen evidencia de accesos indebidos. Su tratamiento como No Conformidad se desarrolla en el apartado 6. Administración de accesos.

Copias de respaldo y recuperación

En materia de copias de respaldo se contrastaron el procedimiento *PD-51, Copias de respaldo V3*, la *GI-27, Guía de Copias de Respaldo V1*, el PETI y el *Plan de Recuperación Tecnológica ante Desastres* con la operación observada.

La auditoría comprobó la ejecución de respaldos y restauraciones satisfactorias en componentes seleccionados, particularmente NAS y File Server, así como mecanismos automatizados de comprobación para JSP7. En consecuencia, la gestión de respaldos no se encontró limitada a la existencia formal de procedimientos.

La principal diferencia documental se identificó en la GI-27, cuya versión original corresponde al 27 de diciembre de 2019 y conserva referencias a tecnologías y plataformas históricas que no reflejan integralmente la arquitectura tecnológica observada durante 2026. La operación encontrada presenta una evolución superior a la reflejada en el instrumento documental, por lo que su actualización se mantiene como Oportunidad de Mejora.

Las condiciones relacionadas con cobertura y validación homogénea de la capacidad de recuperación tecnológica se desarrollan separadamente en el apartado 5. Gestión de respaldos y sustentan la No Conformidad correspondiente.

Soporte tecnológico

Para soporte tecnológico se evaluó la aplicación del procedimiento PD-70, Soporte técnico y mantenimiento correctivo de dispositivos TI, considerando la versión vigente durante cada período, mediante el análisis de registros GLPI y de una muestra dirigida de casos.

Las pruebas permitieron acreditar registro, asignación, atención, cierre y escalamiento de solicitudes, incluyendo casos que requirieron intervención de terceros. Por tanto, la operación básica prevista en el procedimiento se encontró implementada.

Se identificaron oportunidades para fortalecer la clasificación de tickets, completitud de registros, asignación de responsables, documentación de soluciones, trazabilidad entre niveles de atención y metodología utilizada para determinados indicadores de tiempo. Estas condiciones afectan principalmente la calidad y reproducibilidad de la información utilizada para gestionar y evaluar el servicio, pero no permiten concluir que el procedimiento de soporte sea inoperante. Su tratamiento se desarrolla en el apartado 9. Soporte tecnológico.

Mantenimiento preventivo y correctivo

Para mantenimiento preventivo y correctivo se consideraron el procedimiento *PD-52, Mantenimiento de equipos de TI V3*, los lineamientos del PETI y los componentes aplicables de PD-70.

La auditoría verificó actividades de mantenimiento efectivamente ejecutadas sobre equipos de usuario final e infraestructura tecnológica, incluyendo intervenciones sobre FortiGate, FortiNAC y PPDM. Para algunos componentes se obtuvo evidencia de programación, ejecución y validación posterior del funcionamiento.

La principal limitación correspondió a la trazabilidad uniforme entre activo, mantenimiento programado, intervención ejecutada, novedad identificada, actuación correctiva y cierre para la totalidad de la población. Esta condición no se presenta como resultado independiente, sino que complementa la Oportunidad de Mejora desarrollada en el apartado 4. Gestión de infraestructura tecnológica, relacionada con la trazabilidad del ciclo de vida de los activos tecnológicos y su mantenimiento.

Adquisición de infraestructura tecnológica

Para el procedimiento *PD-50, Adquisición de Infraestructura Tecnológica V3* se evaluó una muestra correspondiente a los contratos 458-2025, Seguridad Perimetral y 522-2025, Solución NAC.

La documentación precontractual y los soportes posteriores permitieron acreditar la participación de Gestión TIC en la evaluación técnica de las necesidades y en actividades posteriores de recepción, instalación, configuración o validación de las soluciones adquiridas.

Se observaron inconsistencias documentales puntuales en la denominación de algunos equipos y limitaciones sobre determinados soportes de aceptación. Estas situaciones afectan la calidad de la trazabilidad documental, pero no desvirtúan la evidencia técnica de aplicación del procedimiento obtenida en la muestra seleccionada.

Gestión de activos de información

En relación con *GI-61, Gestión de Activos de Información*, la auditoría solicitó el Inventario y Clasificación de Activos de Información vigente y recibió soportes correspondientes principalmente a inventarios físicos y tecnológicos.

Estos documentos permitieron acreditar mecanismos de inventario utilizados para la administración de infraestructura, pero no verificar integralmente el instrumento específico de clasificación de activos de información previsto en GI-61, ni efectuar pruebas suficientes sobre sus atributos, actualización y formalización.

En consecuencia, esta condición se mantuvo como limitación de verificación. La evidencia disponible no permite afirmar que RenoBo carezca del instrumento, pero tampoco acreditar integralmente su estado actual. Su tratamiento como Oportunidad de Mejora se desarrolla en el apartado 7. Gestión de activos de información.

Seguridad y privacidad de la información

En materia de seguridad y privacidad se contrastaron la *Política General de Seguridad y Privacidad de la Información*, el *Plan de Seguridad y Privacidad de la Información*, los procedimientos de accesos, vulnerabilidades e incidentes, el *Plan de Recuperación Tecnológica ante Desastres* y demás instrumentos del SGSI con las evidencias operacionales disponibles.

Las pruebas permitieron comprobar actuaciones concretas de implementación, entre ellas monitoreo de seguridad, administración de accesos, análisis técnicos de vulnerabilidades, mecanismos de respaldo y recuperación, gestión de riesgos y presentación de asuntos de seguridad ante instancias institucionales. En consecuencia, el marco de seguridad no se encontró limitado exclusivamente a su diseño documental.

En gestión de vulnerabilidades se verificó que el procedimiento institucional contempla etapas de identificación, priorización, tratamiento, remediación y revalidación. También se acreditaron ejercicios técnicos de análisis efectuados durante el período evaluado.

No obstante, las pruebas permitieron confirmar que actualmente no se encuentra operando de manera sostenida un mecanismo periódico de análisis conforme a las frecuencias institucionalmente definidas y que, para determinados hallazgos, no fue posible reconstruir integralmente su tratamiento hasta la remediación, revalidación y cierre técnico.

Resumen de Hallazgos de Auditoría

TIPO	CRITERIO ESPECÍFICO EVALUADO	DESCRIPCIÓN
C	Planeación estratégica de TI. *Plan Estratégico de Tecnologías de la Información* (PETI), fases "Planear" y "Analizar" y desarrollo de la "Situación objetivo".	Se verificó la actualización, revisión y aprobación del PETI durante el período evaluado, así como la reorganización de las iniciativas en cuatro macroproyectos y la adopción de decisiones de reorientación frente a necesidades institucionales y tecnológicas.
OM	Planeación estratégica de TI. PETI actualizado y estructuración de los cuatro macroproyectos.	Se identificó oportunidad para fortalecer la definición homogénea y trazable de productos o entregables, metas, responsables, recursos y fechas para las actividades que integran los macroproyectos del PETI. La situación no desvirtúa la existencia de planeación ni configura una desviación independiente.
NC	Ley 87 de 1993. Literales d) y e) del artículo 2. Seguimiento al PETI. *Plan Estratégico de Tecnologías de la Información* (PETI): IND.GO.07 "Indicador ejecución PETI"; IND.GO.11 "Dificultades por capacidad en proyectos de TI"; IND.GO.05 "Indicador de entrenamiento relacionado con regulación y políticas de TI"; y Lineamientos de Gobierno relativos a cuatro autoevaluaciones anuales de Estrategia y Gobierno de TI y a la presentación de un informe anual de Gestión y Gobierno de TI.	Se evidenciaron inconsistencias y limitaciones para reproducir determinados resultados utilizados en el seguimiento al PETI. La versión actualizada distribuye el cierre de brechas en 63 % para 2025, 28 % para 2026 y 10 % para 2027, totalizando 101 %. El informe de cierre reportó 60,2 %, mientras que los componentes cuantificados explícitamente suman 57,0 %, sin soporte suficiente para reconstruir los 3,2 puntos porcentuales restantes. Los resultados globales de IND.GO.07 e IND.GO.11 tampoco pudieron reproducirse integralmente a partir de los numeradores, denominadores y soportes disponibles. Para IND.GO.05 se identificó una inconsistencia verificable en la aplicación de la fórmula, y no quedó acreditada integralmente la ejecución de las cuatro autoevaluaciones ni la presentación formal del informe anual ante la instancia definida. La condición constituye una desviación frente a las definiciones, fórmulas y mecanismos formales de seguimiento establecidos en el PETI para los indicadores IND.GO.07, IND.GO.11 e IND.GO.05 y para los mecanismos de evaluación de Estrategia y Gobierno de TI. En esa medida, se están incumpliendo los literales d) y e) del artículo 2 de la Ley 87 de 1993. Esta condición genera el riesgo de que la Alta Dirección y las instancias de gobierno utilicen información sobre avance y

TIPO	CRITERIO ESPECÍFICO EVALUADO	DESCRIPCIÓN
		desempeño cuya línea base, metodología o resultado no pueda verificarse independientemente, afectando la confiabilidad de las decisiones de priorización, seguimiento y asignación de recursos. De acuerdo con lo anterior, se recomienda fortalecer el seguimiento al PETI mediante la definición y aplicación uniforme de fuentes, variables, fórmulas, líneas base, responsables, periodicidades y controles de validación, y conservar evidencia suficiente de las autoevaluaciones y de la presentación del informe anual ante la instancia correspondiente.
C	Sistema de Información Misional. PETI, *Política de Gestión de Portafolio y Proyectos*, componente "Desde el diseño hasta la entrega" y proyecto Sistemas de Información.	Se comprobaron avances materiales en la implementación del nuevo SIM, incluyendo levantamiento de requerimientos, parametrización, pruebas con usuarios y ajustes derivados de la retroalimentación de las áreas funcionales.
NC	Ley 87 de 1993. Literales d) y e) del artículo 2. Sistema de Información Misional. PETI, *Política de Gestión de Portafolio y Proyectos* y componente "Desde el diseño hasta la entrega", que contemplan evaluación, priorización, acompañamiento, seguimiento, gestión de requerimientos, pruebas, despliegues y puesta en producción.	Se evidenciaron diferencias materiales entre la línea base y los cronogramas de seguimiento del proyecto SIM. La línea base y el seguimiento del 15 de septiembre de 2026 mantenían la finalización al 22 de diciembre de 2026, mientras que el cronograma con corte al 30 de septiembre registró 50 % de avance y nueva finalización al 22 de junio de 2027. En ese mismo corte se observaron actividades reportadas al 100 % con fechas de terminación posteriores al 30 de septiembre. No fue posible reconstruir integralmente la aprobación y justificación de la reprogramación, la transición entre programaciones ni la metodología utilizada para determinar determinados porcentajes de avance. La condición constituye una desviación frente a los lineamientos del PETI sobre gestión y seguimiento de programas, proyectos y mejoras, al no permitir reconstruir de manera consistente y trazable la programación vigente, sus modificaciones, la justificación de las reprogramaciones y el estado real del proyecto. En esa medida, se están incumpliendo los literales d) y e) del artículo 2 de la Ley 87 de 1993. Esto genera riesgo de que el estado comunicado no refleje de manera suficientemente confiable la programación vigente y el avance real, dificultando la identificación de desviaciones, la evaluación de impactos y la toma de decisiones sobre reprogramaciones.

TIPO	CRITERIO ESPECÍFICO EVALUADO	DESCRIPCIÓN
		De acuerdo con lo anterior, se recomienda fortalecer el mecanismo de seguimiento del proyecto SIM para conservar la trazabilidad de la programación de referencia, reprogramaciones, justificación y aprobación, fechas de corte, hitos y reglas de cálculo del avance, incorporando controles de consistencia antes de reportar la información.
C	Gestión de infraestructura tecnológica. PETI, disposiciones sobre "Activos y configuraciones", monitoreo, capacidad y disponibilidad; y PD-50, *Adquisición de Infraestructura Tecnológica*, para las adquisiciones evaluadas.	Se verificó la existencia de una fuente institucional de inventario, herramientas de monitoreo en operación, actuaciones de renovación y fortalecimiento de infraestructura y participación técnica de Gestión TIC en adquisiciones relevantes evaluadas.
OM	Gestión de infraestructura tecnológica y mantenimiento. PETI, lineamientos sobre activos, configuraciones, mantenimiento, monitoreo y disponibilidad.	Se identificó la necesidad de fortalecer la integración y trazabilidad entre inventario, estado del activo, mantenimiento programado, intervenciones realizadas, novedades, acciones posteriores y decisiones de continuidad, renovación o retiro. De forma complementaria, constituye una oportunidad de mejora disponer de información histórica consolidada sobre disponibilidad e interrupciones de los servicios tecnológicos.
C	Gestión de respaldos. PETI; PD-51, *Copias de respaldo*; GI-27, *Guía de Copias de Respaldo*; y *Plan de Recuperación Tecnológica ante Desastres*.	Se acreditó la existencia y operación de mecanismos de respaldo y se comprobaron restauraciones satisfactorias para componentes seleccionados, particularmente NAS y *File Server*, así como mecanismos automatizados de validación para otros servicios.
NC	Ley 87 de 1993. Literal b) del artículo 2. Gestión de respaldos y recuperación. PETI; PD-51, *Copias de respaldo*; GI-27, *Guía de Copias de Respaldo*; y *Plan de Recuperación Tecnológica ante Desastres*, numeral 8.4 "Validación y pruebas" y numeral 8.5 "Relación con KPIs estratégicos". El Plan establece pruebas de restauración como mínimo semestrales para servicios críticos y anuales para servicios no críticos, verificación de integridad y validación funcional, conservación de	Se evidenció que la capacidad de recuperación no se encuentra validada y documentada de manera homogénea para el conjunto de componentes evaluados. Aunque NAS y *File Server* presentaron restauraciones satisfactorias y JSP7 contó con una ejecución satisfactoria previa, la ejecución #331 de Jenkins del 3 de septiembre de 2026 terminó en estado *FAILED* en la etapa "Probando respaldo" sin evidencia suficiente del análisis de la causa, tratamiento aplicado y validación posterior de cierre. Para NAS, las bitácoras no permitieron reconstruir integralmente la duración efectiva de todas las restauraciones para contrastarlas con los objetivos de recuperación. La condición constituye una desviación frente a los numerales 8.4 y 8.5 del *Plan de Recuperación Tecnológica ante Desastres*, en cuanto a la ejecución y documentación de pruebas de restauración, validación de integridad y

TIPO	CRITERIO ESPECÍFICO EVALUADO	DESCRIPCIÓN
	evidencias y una meta de pruebas exitosas de restauración igual o superior al 90 %.	funcionamiento, conservación de evidencias y seguimiento de los resultados frente a los objetivos de recuperación. En esa medida, se está incumpliendo el literal b) del artículo 2 de la Ley 87 de 1993. Esto genera el riesgo de que, ante una pérdida de información o interrupción tecnológica, la Entidad no cuente con evidencia suficiente y actualizada para determinar anticipadamente la recuperabilidad de todos los servicios bajo las condiciones y objetivos definidos, y de que excepciones identificadas permanezcan sin tratamiento y cierre verificable. De acuerdo con lo anterior, se recomienda fortalecer el esquema de pruebas de recuperación, identificando el universo aplicable, criticidad, responsables, periodicidad y objetivos de recuperación, y documentar para cada prueba sus resultados, excepciones, tratamiento, nueva validación y cierre, incluyendo los servicios administrados por terceros o bajo modalidad SaaS.
NC	Ley 87 de 1993. Literales b) y e) del artículo 2. Administración de accesos. PD-71, *Administración de Acceso Lógico*, versión aplicable durante el período evaluado: validación de solicitudes, aprobación funcional, principio de mínimo privilegio, creación y modificación de accesos, revisión periódica, retiro de permisos, conservación de evidencia y controles adicionales para cuentas temporales, privilegiadas, técnicas, de servicio o de terceros.	Se evidenciaron limitaciones para reconstruir de manera suficiente y homogénea determinados componentes del ciclo de vida de accesos y privilegios. Gestión TIC informó que no cuenta con una bitácora sobre las modificaciones de accesos; para usuarios retirados se comprobó el estado final bloqueado o deshabilitado, pero no fue posible determinar con precisión la fecha técnica de revocación; no se evidenció un mecanismo formalizado que relacione perfiles funcionales autorizados con roles técnicos configurados; y en NocoBase se observaron cuentas administrativas genéricas sin evidencia suficiente de asignación formal de custodia y atribución individual uniforme de actuaciones. Estas condiciones constituyen una desviación frente al PD-71, *Administración de Acceso Lógico*, al limitar la trazabilidad de modificaciones, revisiones, vigencia y retiro de privilegios, la correspondencia entre la necesidad funcional autorizada y el rol técnico configurado, y la custodia y atribución individual de determinadas cuentas privilegiadas. En esa medida, se está incumpliendo los literales b) y e) del artículo 2 de la Ley 87 de 1993. Como efecto, se dificulta demostrar que los privilegios se mantienen alineados con las necesidades autorizadas y que las modificaciones y retiros son oportunos; además, el uso de cuentas genéricas sin atribución suficiente incrementa el riesgo de que actuaciones privilegiadas no puedan asociarse

TIPO	CRITERIO ESPECÍFICO EVALUADO	DESCRIPCIÓN
		posteriormente con una persona específica, afectando la responsabilidad individual y la capacidad de investigación o reconstrucción. De acuerdo con lo anterior, se recomienda fortalecer la gestión del ciclo de vida de accesos y privilegios, formalizar la correspondencia entre perfiles funcionales y roles técnicos y establecer controles de custodia y atribución individual para las cuentas administrativas genéricas cuya utilización resulte necesaria.
OM	Gestión de activos de información. GI-61, *Gestión de Activos de Información*, e instrumento institucional de *Inventario y Clasificación de Activos de Información*.	Los soportes aportados permitieron comprobar inventarios tecnológicos y físicos, pero no verificar integralmente el instrumento específico previsto en GI-61. La condición constituye una limitación de verificación y se presenta como oportunidad de mejora orientada a fortalecer la disponibilidad, formalización y trazabilidad del instrumento. No constituye un incumplimiento confirmado.
C	Seguridad y privacidad de la información. *Política General de Seguridad y Privacidad de la Información* (PL-16), *Plan de Seguridad y Privacidad de la Información* (PSPI) e instrumentos asociados al SGSI.	Se verificó la existencia de política, plan de seguridad, procedimientos, instrumentos de riesgos, autodiagnóstico MSPI, mecanismos de monitoreo y controles con evidencia concreta de operación. El SGSI presenta avances materiales de formalización e implementación.
NC	Ley 87 de 1993. Literales b) y e) del artículo 2. Seguridad y privacidad de la información. *Política General de Seguridad y Privacidad de la Información*, PL-16-V1, numeral 9.7.1 “Dirección y gobernanza” y numeral 9.7.2 “Gestión del riesgo y mejora continua”; *Plan de Seguridad y Privacidad de la Información* y demás instrumentos del SGSI que contemplan evaluación, seguimiento, autodiagnóstico y mejora.	Se evidenció que, aunque RenoBo cuenta con elementos formales y operativos del SGSI y presenta asuntos de seguridad ante el Comité Institucional de Gestión y Desempeño, los resultados de evaluaciones y diagnósticos no permitieron reconstruir sistemáticamente una secuencia entre brecha o resultado identificado, acción de mejora o tratamiento, responsable, fecha objetivo, seguimiento, evidencia de implementación, validación de efectividad y cierre. En una muestra de seis controles del *Autodiagnóstico MSPI 2026*, los campos “Brecha” y “Recomendación” se encontraban sin diligenciar, aun cuando para varios controles se identificaron diferencias o insuficiencia de evidencia. La condición constituye una desviación frente a los numerales 9.7.1, Dirección y gobernanza, y 9.7.2, Gestión del riesgo y mejora continua, de la PL-16-V1 y frente a los mecanismos de evaluación, seguimiento y mejora previstos en los instrumentos del SGSI. En esa medida, se está incumpliendo los literales b) y e) del artículo 2 de la Ley 87 de 1993.

TIPO	CRITERIO ESPECÍFICO EVALUADO	DESCRIPCIÓN
		Esto genera el riesgo de que brechas, desviaciones o necesidades de fortalecimiento no sean priorizadas o tratadas oportunamente, o que su tratamiento no pueda demostrarse posteriormente, limitando la capacidad institucional para evaluar la efectividad de las acciones adoptadas y evidenciar la mejora continua del SGSI. De acuerdo con lo anterior, se recomienda fortalecer el mecanismo de seguimiento y mejora continua del SGSI para relacionar cada brecha o necesidad identificada con la acción definida, responsable, prioridad, fecha objetivo, seguimiento, evidencia de implementación, validación del resultado y cierre, definiendo además la instancia responsable de efectuar dicho seguimiento.
C	Soporte tecnológico. PD-70, *Soporte técnico y mantenimiento correctivo de dispositivos TI*, y PETI, lineamientos de gestión de soporte y seguimiento de solicitudes.	Se comprobó la operación sostenida de GLPI para registrar, asignar, atender, escalar y cerrar solicitudes tecnológicas, así como la posibilidad de reproducir los principales indicadores generales de gestión revisados.
OM	Soporte tecnológico. PD-70, *Soporte técnico y mantenimiento correctivo de dispositivos TI*, y PETI, disposiciones sobre estadísticas de atención, reportes e histórico consultable.	Se identificaron oportunidades para fortalecer la categorización, completitud, asignación de responsables, documentación de las soluciones, trazabilidad entre niveles de atención y metodología utilizada para determinados indicadores de tiempo. Estas condiciones afectan principalmente la calidad y reproducibilidad de la información y no evidencian inoperancia general de la mesa de servicio.
C	Mantenimiento preventivo y correctivo. PETI, numeral 6.4.2.4.1.4 “Mantenimiento”; PD-52, *Mantenimiento de equipos de TI*; y, para el período de vigencia aplicable, PD-70.	Se verificaron actividades efectivamente ejecutadas sobre equipos de usuario final e infraestructura tecnológica, incluyendo intervenciones con validaciones posteriores de funcionamiento. Las limitaciones de trazabilidad identificadas se integran a la oportunidad de mejora relacionada con el ciclo de vida de los activos tecnológicos.
NC	Ley 87 de 1993. Literales b) e) y f) del artículo 2. Gestión de riesgos de seguridad digital. *Política General de Seguridad y Privacidad de la Información* (PL-16), numeral 9.7.2 “Gestión del riesgo y mejora continua” y numeral	Se evidenciaron limitaciones para reconstruir de manera completa y homogénea la relación entre riesgos, controles aplicados, acciones de tratamiento, evidencias de ejecución, evaluación de efectividad y reducciones reflejadas en el riesgo residual. En *Gestión_Riesgos.xlsx*, los 21 riesgos figuraban con decisión “Reducir” y estado “En tratamiento”, pero para la muestra

TIPO	CRITERIO ESPECÍFICO EVALUADO	DESCRIPCIÓN
	9.8.1 “Gestión del riesgo y controles”; y *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026-2030*.	examinada no fue posible reconstruir uniformemente la secuencia acción, responsable, fecha objetivo, evidencia de ejecución, evaluación de efectividad y cierre. En el *Mapa de Riesgos SGSI 2026*, de 25 controles revisados, 12 figuraban como “Sin Documentar” y 11 como “Sin Registro”. La condición constituye una desviación frente a los numerales 9.7.2, Gestión del riesgo y mejora continua, y 9.8.1, Gestión del riesgo y controles, de la PL-16 y frente al *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026-2030*, al no permitir demostrar de forma suficientemente trazable la relación entre controles, acciones de tratamiento, evidencias, evaluación de efectividad y nivel de riesgo residual. En esa medida, se está incumpliendo los literales b) e) y f) del artículo 2 de la Ley 87 de 1993. Esto genera el riesgo de que los niveles de riesgo residual reportados no puedan ser sustentados o reproducidos independientemente, limitando la capacidad de las instancias responsables para evaluar la evolución de los riesgos, priorizar tratamientos adicionales y decidir sobre la aceptación o permanencia del riesgo residual. De acuerdo con lo anterior, se recomienda fortalecer los instrumentos de gestión de riesgos para relacionar, para cada riesgo, la valoración inherente, controles, evidencias de ejecución, evaluación de efectividad, acciones de tratamiento, responsables, fechas objetivo, seguimiento, cierre y efecto considerado en la valoración residual, asegurando además la reproducibilidad de las reglas y parámetros utilizados.
NC	Ley 87 de 1993. Literales b) e) y f) del artículo 2. Gestión de vulnerabilidades. Procedimiento P_SGSI-PROC-OPS-VUL-v01, que establece el ciclo de preparación, análisis, identificación, priorización, tratamiento, remediación y revalidación, con un análisis mínimo anual sobre los activos tecnológicos dentro del alcance aplicable del SGSI; y *Plan de Seguridad y Privacidad de la Información* (PSPI) 2026, que establece gestión trimestral de	Se evidenció que RenoBo realizó ejercicios técnicos de análisis de vulnerabilidades durante 2026; sin embargo, los responsables confirmaron que actualmente no cuentan con un mecanismo operativo periódico, soportado en herramienta, servicio o proveedor, que asegure la ejecución sostenida de los análisis. Para determinados hallazgos de severidad relevante no fue posible reconstruir integralmente la secuencia entre hallazgo, activo, responsable, tratamiento, remediación, revalidación y estado final; en un caso de intranet tampoco se evidenció soporte suficiente de corrección acompañado de reescaneo o revalidación técnica. La condición constituye una desviación frente al procedimiento P_SGSI-PROC-OPS-VUL-v01 y al PSPI 2026, respecto de las periodicidades definidas para los análisis y de la trazabilidad

TIPO	CRITERIO ESPECÍFICO EVALUADO	DESCRIPCIÓN
	vulnerabilidades para portal web, sede electrónica y servicios expuestos, acompañada de informes y acciones de remediación.	del ciclo de tratamiento, remediación, reescaneo o revalidación y cierre técnico de los hallazgos. En esa medida, se está incumpliendo los literales b) e) y f) del artículo 2 de la Ley 87 de 1993. Esto genera el riesgo de que nuevas vulnerabilidades no sean identificadas oportunamente o que exposiciones conocidas permanezcan sin cierre técnicamente demostrable, incrementando la exposición de los sistemas y servicios institucionales y dificultando determinar la efectividad de las acciones de remediación. De acuerdo con lo anterior, se recomienda fortalecer la operación de la gestión de vulnerabilidades mediante un mecanismo periódico y sostenible que cumpla las frecuencias establecidas y conserve la trazabilidad de cada hallazgo desde su identificación y priorización hasta la remediación, reescaneo o revalidación y cierre técnico, preservando institucionalmente la evidencia de tratamiento y cierre.
OM	Cumplimiento de procedimientos, manuales y políticas institucionales. Documentos SIG aplicables a Gestión TIC, particularmente GI-27, *Guía de Copias de Respaldo*, y demás procedimientos revisados durante la auditoría.	Se identificaron instrumentos cuya actualización puede fortalecerse para reflejar la operación tecnológica vigente, particularmente la GI-27 de copias de respaldo, así como oportunidades puntuales de mejora en el control documental de otros procedimientos. No se evidenció un incumplimiento generalizado del marco documental de Gestión TIC.

Convenciones:

- **C:** Conformidad.
- **NC:** No Conformidad.
- **OM:** Oportunidad de Mejora.

5. CONCLUSIONES DEL TRABAJO DE AUDITORIA

Como resultado de la auditoría se concluye que RenoBo cuenta con un marco de planeación, gestión y operación de tecnologías de la información implementado, soportado en el Plan Estratégico de Tecnologías de la Información (PETI), procedimientos institucionales, herramientas tecnológicas y mecanismos de seguimiento y control. Durante el período evaluado se evidenciaron actuaciones concretas relacionadas con planeación estratégica, implementación del Sistema de Información Misional, administración de infraestructura, respaldos y recuperación, gestión de accesos, activos de información, seguridad y privacidad, soporte tecnológico, mantenimiento y gestión de riesgos de seguridad digital.

En relación con la planeación estratégica de TI, se verificó que el PETI fue objeto de revisión, actualización y reorientación durante el período evaluado, incluyendo la reorganización de las iniciativas en cuatro macroproyectos y la aprobación institucional de sus ajustes. La planeación estratégica se encontró implementada y constituye un elemento favorable de la gestión. Como Oportunidad de Mejora, se identificó la necesidad de fortalecer la definición homogénea y trazable de productos o entregables, metas, responsables, recursos y plazos asociados con las actividades de los macroproyectos.

En cuanto al porcentaje de avance del PETI, el PETI 2026-2029 registra como línea base para 2025 una ejecución del 74 %. Sin embargo, la auditoría no pudo reproducir de manera independiente este porcentaje con las evidencias disponibles, debido a que no fue posible identificar de forma inequívoca la población utilizada, las iniciativas incluidas como ejecutadas ni la regla aplicada para clasificar proyectos parciales, sustituidos o reprogramados. De manera complementaria, para el cierre de brechas se reportó un avance de 60,2 %, mientras que los componentes cuantificados y verificables examinados por la auditoría sumaron 57,0 %. En consecuencia, no se cuenta con un porcentaje único de avance del PETI a la fecha que haya podido ser validado integralmente por la auditoría.

Respecto de los recursos requeridos para la ejecución del PETI, se evidenciaron restricciones de capacidad y el propio PETI registra un indicador de dificultades por capacidad del 26 %. La auditoría identificó evidencia relacionada con limitaciones de personal; sin embargo, dicho porcentaje tampoco pudo reproducirse conforme a la metodología definida y no se obtuvo evidencia suficiente para concluir que las desviaciones o reprogramaciones de los macroproyectos obedecieran específicamente a insuficiencia de recursos presupuestales provenientes de proyectos de inversión. Adicionalmente, los recursos no se encontraban vinculados de manera homogénea a las actividades de cada macroproyecto, lo cual limita establecer con precisión la relación entre los recursos previstos, los efectivamente disponibles y el nivel de ejecución alcanzado.

Respecto del seguimiento al PETI, se comprobó la existencia de mecanismos de revisión, seguimiento y toma de decisiones. Se identificaron debilidades en la confiabilidad, consistencia, trazabilidad y reproducibilidad de determinados indicadores y porcentajes de avance, así como en la acreditación de los mecanismos formales de autoevaluación y reporte previstos en el propio Plan. Estas condiciones dieron lugar a una No Conformidad relacionada con la calidad y verificabilidad de la información utilizada para medir y comunicar el desempeño del PETI.

En cuanto al Sistema de Información Misional, se evidenciaron avances materiales en su implementación sobre NocoBase, incluyendo levantamiento de requerimientos, parametrización, participación de usuarios, pruebas funcionales y ajustes derivados de dichas pruebas. El cronograma suministrado con corte al 30 de septiembre de 2026 reportaba un avance del 50 % para la parametrización y pruebas del SIM y una fecha de terminación reprogramada al 22 de junio de 2027. Este porcentaje corresponde al avance reportado por el proyecto, dado que la auditoría no pudo reconstruir integralmente la metodología utilizada para determinarlo ni la transición entre las diferentes programaciones utilizadas para su seguimiento.

A la fecha de evaluación, la nueva solución continuaba en fase de implementación y pruebas, por lo que no resultaba procedente efectuar una valoración de su efectividad como sistema plenamente productivo. La principal debilidad se relacionó con la consistencia y trazabilidad del seguimiento del proyecto, particularmente frente a programaciones, reprogramaciones, fechas de corte y metodología utilizada para determinar los porcentajes de avance. Esta condición dio lugar a una No Conformidad.

En relación con los proyectos de inversión asociados con iniciativas TIC, con las evidencias examinadas no fue posible establecer un porcentaje consolidado de avance físico y financiero que permitiera determinar su estado global a la fecha de corte. La documentación revisada permite identificar iniciativas tecnológicas y su articulación con el PETI, pero no proporcionó una medición consolidada que relacionara, para los proyectos de inversión aplicables, presupuesto programado, presupuesto ejecutado, metas físicas y porcentaje de avance. En consecuencia, la auditoría no asigna un porcentaje global de ejecución a estos proyectos.

La gestión de infraestructura tecnológica, soporte y mantenimiento presentó evidencia material de operación. RenoBo dispone de fuentes institucionales de inventario tecnológico, mecanismos de monitoreo, actuaciones de renovación y fortalecimiento de infraestructura, una mesa de servicio operada mediante GLPI y actividades de mantenimiento preventivo y correctivo efectivamente ejecutadas en las muestras examinadas. Las oportunidades de mejora se concentran en fortalecer la trazabilidad integral del ciclo de vida de los activos, disponer de información histórica consolidada sobre disponibilidad e interrupciones y mejorar la calidad, completitud y trazabilidad de determinados registros de soporte.

En materia de respaldos y recuperación tecnológica, se comprobó la existencia y operación de mecanismos de respaldo y se evidenciaron restauraciones satisfactorias para componentes seleccionados. La debilidad identificada no corresponde a ausencia de respaldos, sino a la capacidad para demostrar de manera homogénea y periódica la recuperabilidad del universo aplicable, gestionar hasta su cierre las excepciones identificadas durante las pruebas y contrastar suficientemente sus resultados con los objetivos de recuperación definidos. Esta condición dio lugar a una No Conformidad.

Respecto de la administración de accesos, se acreditó la operación del flujo básico de solicitud, aprobación y configuración y la existencia de perfiles y permisos diferenciados. Se identificaron debilidades relacionadas con la trazabilidad histórica de modificaciones y retiros, la formalización de la correspondencia entre necesidades funcionales y roles técnicos y la custodia y atribución individual de determinadas actuaciones realizadas mediante cuentas administrativas genéricas. La auditoría no obtuvo evidencia que permita concluir la existencia generalizada de accesos no autorizados, utilización indebida de cuentas o revocaciones tardías.

En la gestión de activos de información, los soportes disponibles permitieron comprobar la existencia de inventarios tecnológicos y actividades institucionales relacionadas con la identificación y revisión de activos. Sin embargo, no fue posible verificar integralmente el Inventario y Clasificación de Activos de Información previsto en la guía institucional ni efectuar pruebas suficientes sobre sus atributos, actualización y formalización. Esta condición se mantuvo como limitación de verificación y Oportunidad de Mejora, sin evidencia suficiente para concluir que RenoBo carezca del instrumento.

En materia de seguridad y privacidad de la información, se verificaron avances materiales en la formalización e implementación del SGSI, incluyendo política, plan de seguridad, procedimientos, instrumentos de riesgos, autodiagnóstico MSPI, mecanismos de monitoreo y controles cuya implementación y operación fue acreditada en diferentes componentes evaluados. La principal debilidad se relacionó con la capacidad para demostrar de manera sistemática que los resultados de evaluaciones, diagnósticos y revisiones se transforman en acciones de mejora con responsables, plazos, seguimiento, validación de resultados y cierre. Esta condición dio lugar a una No Conformidad relacionada específicamente con el seguimiento y mejora continua del SGSI, sin que ello permita concluir una inefectividad general del sistema.

En relación con la gestión de incidentes de seguridad, se verificó la existencia de un procedimiento institucional y de mecanismos técnicos de monitoreo. Sin embargo, no se dispuso de una población verificable de incidentes que permitiera seleccionar una muestra y recorrer casos reales de extremo a extremo. Esta circunstancia constituyó una limitación de verificación y no evidencia de inoperancia del proceso.

Respecto de la gestión de riesgos de seguridad digital, RenoBo dispone de matrices, controles y decisiones de tratamiento, y las pruebas realizadas no evidenciaron errores aritméticos generalizados en las muestras examinadas. La debilidad se concentró en la trazabilidad necesaria para relacionar de manera verificable los controles y acciones de tratamiento con sus evidencias de ejecución, evaluación de efectividad y efecto sobre el riesgo residual. Esta condición dio lugar a una No Conformidad.

De manera diferenciada, en la gestión de vulnerabilidades se acreditaron ejercicios técnicos de análisis realizados durante el período evaluado. Se confirmó que actualmente no se encuentra operando de manera sostenida un mecanismo periódico que asegure la ejecución de los análisis conforme a las frecuencias institucionales y que, para determinados hallazgos, no fue posible reconstruir integralmente la remediación, revalidación y cierre técnico. Esta condición dio lugar a una No Conformidad independiente.

La evaluación transversal del cumplimiento de procedimientos, manuales y políticas institucionales mostró resultados diferenciados. Se acreditó la aplicación de diversos procedimientos y controles, mientras otros requieren actualización, mayor formalización o fortalecimiento de su trazabilidad. En determinados componentes la evidencia disponible generó limitaciones de verificación que no constituyen, por sí mismas, evidencia de incumplimiento. En consecuencia, no se identificó un incumplimiento generalizado del marco documental de Gestión TIC. Se estableció como Oportunidad de Mejora fortalecer la actualización y el control documental de los instrumentos aplicables, particularmente cuando la operación tecnológica ha evolucionado frente a lo reflejado en los documentos vigentes.

Informe de Auditoría

En términos generales, la auditoría concluye que la Gestión TIC de RenoBo presenta un nivel material de implementación y operación, con capacidades institucionales establecidas y controles cuya aplicación pudo ser acreditada en diferentes componentes evaluados. Las principales necesidades de fortalecimiento se concentran en la confiabilidad, trazabilidad, consistencia, cobertura y demostrabilidad de determinados mecanismos de seguimiento y control, más que en una ausencia generalizada de procesos o capacidades tecnológicas.

Como resultado de la evaluación se consolidaron siete (7) Conformidades, siete (7) No Conformidades y cinco (5) Oportunidades de Mejora. Las No Conformidades se concentran en seguimiento y medición del PETI, seguimiento del proyecto de implementación del SIM, cobertura y validación de la capacidad de recuperación tecnológica, ciclo de vida de accesos y privilegios, valoración y tratamiento de riesgos de seguridad digital, operación periódica y cierre técnico de la gestión de vulnerabilidades, y seguimiento y mejora continua del SGSI.

Los resultados obtenidos no permiten concluir una inefectividad general de la Gestión TIC, del PETI o del SGSI. El principal reto identificado consiste en fortalecer la capacidad institucional para demostrar, mediante evidencia suficiente, consistente y reproducible, el nivel real de avance de las iniciativas, la relación entre los recursos asignados y los resultados obtenidos, la ejecución de los mecanismos definidos, la gestión de excepciones y desviaciones hasta su cierre y el efecto de los controles y acciones implementados sobre los resultados considerados dentro de los procesos de seguimiento, valoración y toma de decisiones.

6. RECOMENDACIONES

Con fundamento en los resultados de la auditoría, se formulan las siguientes recomendaciones orientadas al tratamiento de las siete No Conformidades identificadas y al fortalecimiento de las cinco Oportunidades de Mejora resultantes de la evaluación.

Las acciones específicas, responsables, recursos y plazos para atender estas recomendaciones deberán ser definidos por los responsables de los procesos en el marco del Plan de Mejoramiento institucional.

6.1 RECOMENDACIONES ASOCIADAS CON LAS NO CONFORMIDADES

Fortalecer el seguimiento y medición del PETI

Se recomienda fortalecer el mecanismo de seguimiento al PETI, de manera que permita identificar y aplicar consistentemente, para cada indicador, meta e iniciativa, las fuentes de información, variables, fórmulas, líneas base, responsables, periodicidades, fechas de corte y evidencias utilizadas para determinar los resultados.

Asimismo, se recomienda incorporar controles de validación y consistencia previos a la utilización o presentación de la información y conservar trazabilidad sobre las modificaciones efectuadas a metas, indicadores y programaciones.

De igual forma, fortalecer la evidencia que permita demostrar la realización de las autoevaluaciones de Estrategia y Gobierno de TI y la presentación de los informes previstos en el PETI ante las instancias correspondientes.

Fortalecer el seguimiento y control del proyecto de implementación del Sistema de Información Misional

Se recomienda fortalecer el mecanismo de seguimiento del proyecto SIM, de manera que permita identificar de forma trazable la programación utilizada como referencia, las modificaciones y reprogramaciones efectuadas, su justificación y aprobación, las fechas de corte, hitos, dependencias y las reglas utilizadas para determinar el avance.

Asimismo, establecer controles de consistencia sobre la información utilizada para reportar el estado del proyecto, de forma que exista correspondencia verificable entre fechas de corte, fechas de inicio y terminación, estado de las actividades y porcentajes de avance.

Fortalecer la validación de la capacidad de recuperación tecnológica

Se recomienda fortalecer el esquema de pruebas de recuperación tecnológica, considerando el universo de servicios y componentes aplicables, su criticidad, mecanismos de respaldo, responsables, periodicidades y objetivos de recuperación definidos.

Para las pruebas realizadas, conservar evidencia suficiente que permita verificar el resultado de la restauración, integridad y funcionamiento de la información o servicio recuperado y, cuando corresponda, contrastar los tiempos obtenidos con los objetivos de recuperación aplicables.

Cuando se presenten pruebas fallidas o excepciones, mantener trazabilidad sobre su análisis, tratamiento, revalidación posterior y cierre.

Asimismo, considerar dentro del esquema los servicios administrados por terceros o bajo modalidades SaaS, de acuerdo con las responsabilidades de recuperación que correspondan a RenoBo y a sus proveedores.

Fortalecer la formalización y trazabilidad del ciclo de vida de accesos y privilegios

Se recomienda fortalecer los mecanismos utilizados para conservar trazabilidad sobre las solicitudes, autorizaciones, altas, modificaciones, revisiones de vigencia y retiros de accesos y privilegios, especialmente para cuentas privilegiadas, técnicas, de servicio y de terceros.

Asimismo, formalizar la correspondencia entre las necesidades o perfiles funcionales autorizados y los roles o privilegios técnicos configurados, mediante el mecanismo que la Entidad determine, de forma que dicha asignación pueda ser reproducida y verificada independientemente.

Para las cuentas administrativas genéricas cuya utilización resulte necesaria, establecer controles de custodia y mecanismos que permitan atribuir individualmente las actuaciones administrativas relevantes.

Fortalecer la trazabilidad y reproducibilidad de la valoración y tratamiento de riesgos de seguridad digital

Se recomienda fortalecer los instrumentos de gestión de riesgos de seguridad digital para que permitan relacionar de manera trazable la valoración inherente, los controles asociados, las evidencias de su ejecución, la evaluación de su efectividad, las acciones de tratamiento, responsables, fechas objetivo, seguimiento y estado de cierre, así como el efecto considerado para determinar el riesgo residual.

Asimismo, procurar que las reglas, parámetros y fuentes utilizadas para efectuar las valoraciones puedan identificarse y reproducirse a partir de la documentación disponible, manteniendo trazabilidad entre las diferentes versiones e instrumentos utilizados.

Fortalecer la operación periódica y el cierre técnico de la gestión de vulnerabilidades

Se recomienda establecer y mantener un mecanismo periódico y sostenible de gestión de vulnerabilidades que permita cumplir las frecuencias definidas institucionalmente para los diferentes activos y servicios.

El mecanismo deberá permitir conservar trazabilidad sobre los hallazgos desde su identificación y priorización hasta la asignación, tratamiento, remediación, reescaneo o revalidación y cierre técnico.

Asimismo, fortalecer la conservación institucional de la evidencia de tratamiento y cierre, especialmente para hallazgos de mayor severidad, de manera que su estado pueda ser verificado independientemente y no dependa exclusivamente del conocimiento de los responsables que participaron en su atención.

Fortalecer el seguimiento y mejora continua del SGSI

Se recomienda fortalecer el mecanismo de seguimiento y mejora continua del SGSI, de manera que los resultados provenientes de autodiagnósticos, evaluaciones, revisiones, indicadores y demás ejercicios de seguimiento puedan relacionarse de forma trazable con las acciones de tratamiento o mejora definidas.

Para las situaciones que requieran intervención, conservar información suficiente sobre la brecha o necesidad identificada, acción definida, responsable, prioridad, fecha objetivo, estado, evidencia de implementación, seguimiento, validación del resultado y cierre.

Asimismo, definir claramente la instancia o mecanismo responsable del seguimiento periódico y conservar evidencia de las decisiones y compromisos adoptados, independientemente de la estructura de gobernanza que RenoBo determine para ejercer esta función.

6.2 RECOMENDACIONES ASOCIADAS CON LAS OPORTUNIDADES DE MEJORA

Fortalecer la estructuración de los macroproyectos del PETI

Se recomienda complementar la estructuración de los cuatro macroproyectos mediante una definición más homogénea y trazable de los productos o entregables, metas, responsables, recursos y plazos asociados con sus principales actividades.

Este fortalecimiento permitirá mejorar la correspondencia entre lo planeado y lo ejecutado y facilitar posteriormente la medición del avance y los resultados de cada iniciativa.

Fortalecer la trazabilidad del ciclo de vida de los activos tecnológicos y su mantenimiento

Se recomienda fortalecer la integración y trazabilidad entre la información del inventario tecnológico, estado del activo, mantenimientos programados y ejecutados, novedades identificadas, intervenciones correctivas y decisiones de continuidad, renovación o retiro.

Asimismo, procurar que las novedades identificadas durante actividades de mantenimiento puedan relacionarse con su tratamiento y cierre cuando requieran acciones posteriores.

De manera complementaria, evaluar la conveniencia de disponer de información histórica consolidada sobre disponibilidad e interrupciones de los servicios tecnológicos que permita analizar su comportamiento, duración, causas e impacto cuando resulte necesario.

Fortalecer la disponibilidad y verificabilidad del Inventario y Clasificación de Activos de Información

Se recomienda fortalecer la disponibilidad, actualización, formalización y trazabilidad del Inventario y Clasificación de Activos de Información previsto en la GI-61, manteniéndolo claramente diferenciado de los inventarios físicos y tecnológicos.

El instrumento debería permitir verificar de manera consistente los atributos establecidos institucionalmente y su relación con las necesidades de protección y gestión de riesgos aplicables.

Fortalecer la calidad y trazabilidad de los registros de soporte tecnológico

Se recomienda fortalecer la calidad de la información registrada en GLPI, particularmente en aspectos relacionados con categorización, asignación de responsables, documentación de las soluciones, escalamiento entre niveles de atención y consistencia de los registros temporales.

Asimismo, revisar la metodología utilizada para los indicadores de tiempo, de forma que las métricas reportadas correspondan claramente con los eventos que pretenden medir y puedan ser reproducidas a partir de la información registrada en la herramienta.

Fortalecer la actualización y el control documental de los instrumentos de Gestión TIC

Se recomienda revisar y actualizar los procedimientos, guías y demás instrumentos que presenten diferencias frente a la operación tecnológica vigente, particularmente la GI-27, Guía de Copias de Respaldo, considerando la evolución de la infraestructura, los servicios administrados por terceros y las soluciones bajo modalidad SaaS.

Asimismo, fortalecer los controles documentales relacionados con fechas, denominaciones, versiones, objeto de los documentos e historial de cambios, de manera que exista consistencia entre el contenido vigente, su identificación formal y las modificaciones realizadas.

Estas acciones deberán orientarse a mantener la correspondencia entre el marco documental y la operación institucional, sin duplicar controles o registros que ya se encuentren gestionados mediante otros mecanismos.

7. PLAN DE MEJORAMIENTO

La Subgerencia de Gestión Corporativa y la Dirección Administrativa y de TICs, como responsables del proceso Gestión TIC para efectos del presente trabajo de auditoría, deberán elaborar un Plan de Mejoramiento que contenga las acciones correctivas para subsanar las causas de las No Conformidades detectadas, de acuerdo con el procedimiento PD-17 Plan de Mejoramiento.

El tiempo estimado para la formulación de dicho plan será de un plazo no mayor a diez (10) días hábiles contados desde la fecha de radicación de informe del trabajo de auditoría definitivo. La entrega del Plan de Mejoramiento deberá surtirse ante la Oficina Asesora de Planeación para lo de su competencia.

Informe de Auditoría

8. DECLARACIÓN DE CUMPLIMIENTO

El trabajo de auditoría se realizó con base en un muestreo aleatorio que no implica la detección de la totalidad de las situaciones de Conformidad, No Conformidad u Observaciones.

CRITERIOS DE CUMPLIMIENTO DEL TRABAJO DE AUDITORÍA	SI	NO	JUSTIFICACIÓN
1. ¿El trabajo de auditoría cumplió con todos los estándares y requisitos generalmente aceptados?	X		
2. ¿Durante el trabajo de auditoría, con la entrega del informe preliminar de auditoría, días hábiles para observaciones y en la reunión de cierre, se aseguró el derecho del auditado a explicar, justificar, defender o contradecir los resultados?	X		
3. ¿Se presentaron impedimentos o conflictos de intereses que afectaran la independencia y objetividad del trabajo de auditoría?		X	
4. ¿Se materializaron los riesgos del trabajo de auditoría?	X		
5. ¿Se presentaron impedimentos legales o de otras regulaciones que afectaran el acceso a la información o el cumplimiento las partes del trabajo de auditoría?		X	
6. ¿Se cumplieron los criterios del código de ética del auditor y del estatuto de auditoría?	X		
7. ¿La información insumo para el trabajo de auditoría fue dispuesta de manera oportuna y completa?	X		
8. ¿El trabajo de auditoría requiere de la declaración de alguna salvaguarda?		X	

9. EQUIPO AUDITOR	
NOMBRE	**CALIDAD DEL AUDITOR**
Alberto Mario Solano Jiménez	Auditor Líder
José Edwin Lozano Gómez	Auditor Acompañante

10. APROBACIÓN	
NOMBRE	**CARGO**
Dik Martínez Velásquez	**JEFE OFICINA DE CONTROL INTERNO**