

EQUIPO AUDITOR:
Julie A. Rodríguez Torres
Laura C. Rueda Serrano

FECHA:
27 de agosto de 2025

OBJETIVOS DE LA AUDITORÍA

1. OBJETIVO DE LA AUDITORIA

Realizar la evaluación y seguimiento a las actividades que se realizan en el proceso de Sistemas e Informática, con el fin de revisar los procedimientos estandarizados del proceso, brindar recomendaciones, observaciones o no conformidades llegado el caso que permitan a la Empresa Municipal de Servicios Públicos Domiciliarios de Piedecuesta ESP Piedecuestana de Servicios Públicos implementar las oportunidades de mejora en los procesos asociados.

OBJETIVOS ESPECIFICOS

- Determinar la capacidad del proceso para asegurar el cumplimiento por la organización de los requisitos legales, reglamentarios y contractuales aplicables al alcance del sistema de gestión.
- Determinar la eficacia del proceso para asegurar razonablemente que la organización puede lograr sus objetivos especificados.
- Identificar oportunidades de mejora del proceso.

ALCANCE DE LA AUDITORÍA

Revisión de los Procesos que conforman el SG de la empresa, incluida su información documentada (procedimientos, registros, formatos e indicadores)

Verificar el cumplimiento de las actividades realizadas en el proceso de sistemas e informática.

PROCESOS AUDITADOS

Sistemas e informática.

ELEMENTOS DE LA NORMA INVOLUCRADOS: ISO 9001:2015, Acuerdo No.011 de 2023 Manual específico de funciones y competencias laborales, documentos que pertenecen al sistema de gestión.

LUGAR DONDE SE REALIZARON LAS ACTIVIDADES DE AUDITORÍA EN SITIO:
Instalaciones de la Empresa Piedecuestana de Servicios Públicos

ELABORÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
Profesional Universitario en Sistemas de Gestión	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025

INFORME DE AUDITORÍA

Código: GPI-SG.AI02-210.F03

Versión: 4.0

Página 2 de 7

PERSONAS ENTREVISTADAS:

Erik Jovanny Solano G. - Profesional Universitario Sistemas e informática.

CRITERIOS DE LA AUDITORÍA

1. Solicitud de documentación.
2. Lista de chequeo para comprobar la información.
3. Verificación ocular, verbal, escrita, documental y física.
4. Técnicas de Auditoría.
5. Desarrollo de la Auditoría.

HALLAZGOS Y/O OBSERVACIONES DE LA AUDITORÍA

CONSIDERACIONES INICIALES

La reunión de apertura de la auditoría interna del área de Sistemas e informática se llevó a cabo el 25 de abril de 2025, en la cual se presentaron los lineamientos generales y el objetivo de la auditoría.

Como punto de partida, se realizó una revisión preliminar de la documentación disponible en la página web institucional, incluyendo procedimientos, planes, resoluciones y políticas relacionadas con el área de Sistemas e informática.

Posteriormente, el área auditada remitió la información complementaria el 9 de mayo. Así mismo, se efectuó la revisión documental en los meses de mayo y junio, finalmente se realizaron visitas a las oficinas los días 16 y 29 de julio, con el propósito de verificar las evidencias correspondientes.

Con la información suministrada, se identificaron los siguientes hallazgos:

OBSERVACIÓN 1: Procedimiento de copias de seguridad desactualizado

- **Criterio:** Norma ISO 9001:2015, cláusula 7.5 — Información documentada.
- **Descripción:** Se evidenció que el procedimiento de copias de seguridad se encuentra desactualizado ya que existen actividades dentro del mismo que no se están realizando de la manera en la que se encuentran descritas.
- **Conclusión:** Se considera urgente la actualización del procedimiento, en el que se especifiquen las actividades que actualmente se están ejecutando para así mantener actualizada la documentación, definiendo responsables, tiempos y mecanismos de verificación, de ser necesario. Asimismo, se debe capacitar y sensibilizar al personal involucrado para que se garantice la ejecución efectiva y oportuna de los respaldos, minimizando riesgos operativos.

ELABORÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
Profesional Universitario en Sistemas de Gestión	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025

OBSERVACIÓN 2: Procedimiento de requisitos de software incompleto

- **Criterio:** Norma ISO 9001:2015, cláusula 7.5 — Información documentada.
- **Descripción:** El procedimiento actual no incluye de manera clara y estructurada los requisitos que deben cumplirse al momento de adquirir, contratar o desarrollar software. Esta omisión puede derivar en soluciones informáticas que no respondan adecuadamente a las necesidades institucionales, afectando la eficiencia, compatibilidad y seguridad de los sistemas.
- **Conclusión:** Se recomienda ampliar y formalizar el procedimiento para que contemple en su estructura la especificación detallada de requisitos previos a la implementación de nuevas plataformas o actualizaciones. Esta acción permitirá mejorar la calidad de las adquisiciones tecnológicas, evitar retrabajos y garantizar una mejor alineación entre las herramientas tecnológicas y los procesos institucionales. A su vez, se recomienda ampliar el procedimiento para que se especifiquen los: requisitos de software, los préstamos de equipos y las solicitudes de creación y actualización.

OBSERVACIÓN 3: Plan de tratamiento de riesgos, seguridad y privacidad de la información desactualizado

- **Descripción:** El plan de tratamiento de riesgos actualmente en uso no ha sido actualizado con base en la nueva matriz de riesgos vigente. Esta desactualización implica que las medidas adoptadas pueden estar respondiendo a amenazas o vulnerabilidades ya superadas, o no contemplar nuevos riesgos emergentes, reduciendo así la efectividad del plan de acción ante eventos de seguridad de la información.
- **Conclusión:** Es fundamental revisar y ajustar el plan de tratamiento de riesgos conforme al análisis más reciente realizado en el Mapa de Riesgos Institucionales. Esta actualización debe permitir la identificación precisa de amenazas actuales, la asignación de responsables, el seguimiento a las medidas implementadas y la mejora de la postura institucional frente a posibles incidentes relacionados con la seguridad de la información. Se deben remitir las políticas asociadas a datos personales, derechos de autor y términos y condiciones del sitio web al comité de gestión y desempeño para su aprobación.

OBSERVACIÓN 4: Falta de evidencia en el seguimiento de las políticas del área de sistemas e informática

- **Descripción:** Durante la auditoría no se encontró evidencia documental o registros que respalden el cumplimiento efectivo de las políticas establecidas dentro del Plan de Seguridad y Privacidad de la Información y las políticas que en las que tiene

ELABORÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
Profesional Universitario en Sistemas de Gestión	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025

INFORME DE AUDITORÍA

Código: GPI-SG.AI02-210.F03

Versión: 4.0

Página 4 de 7

incidencia el área. Aunque se reconoce que no todas las políticas son competencia exclusiva del proceso de sistemas, sí se constató que dicho proceso tiene incidencia directa o indirecta en la mayoría de ellas.

Las políticas que se encuentran asociadas al área son:

- Política de tratamiento de la información de datos personales.
- Política general de seguridad y privacidad de la información.
- Política de escritorio y pantalla limpia.
- Política de dispositivos móviles.
- Política de copias de seguridad (backups).

A su vez, Plan de Seguridad y Privacidad de la Información contiene las siguientes políticas:

- Política para la identificación, clasificación y control de activos de información.
- Política de acceso a Redes y recursos de Red.
- Política de Administración de acceso a usuarios.
- Política de control de acceso a sistemas de información y aplicativos.
- Política de control de acceso y seguridad física.
- Política de seguridad para los equipos de cómputo.
- Política de uso adecuado del internet.
- Política de tratamiento y protección de datos personales.
- Política de continuidad, contingencia y recuperación de la información.

La ausencia de evidencia y la cantidad de políticas establecidas dificulta verificar la implementación de controles, la gestión de riesgos asociados y la articulación entre áreas responsables, lo cual podría afectar la protección integral de la información institucional.

- **Conclusión:** Se concluye que existe una debilidad en el seguimiento del cumplimiento de las políticas del Plan de Seguridad y Privacidad de la Información y las políticas asociadas al proceso. Es necesario fortalecer los mecanismos de coordinación institucional, así como consolidar evidencias que demuestren el nivel de implementación y efectividad de cada una de las políticas, asegurando así una gestión responsable y segura de la información en todos los niveles organizacionales.

Desde la oficina de control interno es importante que prioricen las políticas del área de sistemas e información, debido a que se encuentran cinco políticas en la página web y nueve políticas en el plan de seguridad y privacidad de la información, se deben institucionalizar las más importantes para el área y las que requiera la entidad.

ELABORÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
Profesional Universitario en Sistemas de Gestión	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025

OBSERVACIÓN 5: Ausencia de avance en la implementación de la tecnología IPv6

- **Descripción:** Se evidenció que no existe documentación, registros o informes que demuestren avances significativos en la implementación de la tecnología IPv6 dentro de la infraestructura tecnológica de la entidad. Esta situación se atribuye, en parte, a que se trata de una tecnología emergente que requiere la renovación de equipos de red, computadores y otros dispositivos que actualmente no son compatibles. Adicionalmente, no se ha realizado un diagnóstico técnico que permita establecer el estado actual de la infraestructura ni se ha gestionado con terceros especializados la elaboración de un plan de migración progresiva. Esta falta de avance también está relacionada con la necesidad de recursos presupuestales que aún no han sido asignados.
- **Conclusión:** Se concluye que la entidad no ha iniciado de manera formal el proceso de migración hacia IPv6, lo cual representa una desventaja frente a los estándares tecnológicos actuales y puede generar limitaciones a futuro en la interoperabilidad y el acceso a servicios modernos. Se recomienda realizar un diagnóstico técnico con apoyo de expertos externos, elaborar un plan de acción con cronograma definido y gestionar los recursos necesarios para su ejecución gradual y eficiente.

OBSERVACIÓN 6: No se evidencian condiciones seguras

No se evidencian condiciones óptimas para mantener la seguridad de la información y la seguridad de los equipos en custodia de manera adecuada.

- **Descripción:** Durante la auditoría se verificó que no se evidencian mecanismos que velen por la seguridad de la información y la seguridad de los equipos que contiene el área de sistemas e informática, no se evidencia adecuado tratamiento ni almacenamiento temporal de los RAES existentes in situ, los equipos que se trasladan al área para realizar el mantenimiento reposan en el piso y en superficies en las cuales pueden materializarse riesgos.

Así mismo se observó que el espacio físico usado por el profesional a cargo no garantiza las condiciones de seguridad y salud en el trabajo adecuadas.

- **Conclusión:**
Se debe realizar un ajuste en la distribución de los espacios de almacenamiento de equipos, a su vez, el cuarto donde se almacenan los sistemas de información debe contener señalización y un instructivo para el manejo de la misma.

Así mismo el área de sistemas debe solicitar al área de Seguridad y Salud en el Trabajo la revisión del espacio de trabajo del Profesional Universitario de Sistemas e Informática y si es preciso realizar las mejoras del espacio físico en las condiciones adecuadas para el desempeño de las tareas.

ELABORÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
Profesional Universitario en Sistemas de Gestión	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025

OPORTUNIDADES DE MEJORA.

- Realizar las actividades estipuladas en el cronograma para el segundo semestre del año en vigencia, con el fin de efectuar los planes institucionales, específicamente las capacitaciones del plan de tratamiento de riesgos de seguridad y privacidad de la información y el plan de preservación digital.
- Ajustar y socializar el procedimiento de copias de seguridad, incluyendo cronograma y responsables.
- Ampliar el procedimiento de requisitos de software, detallando requerimientos técnicos y funcionales.
- Revisar y actualizar el inventario de equipos, asegurando consistencia con fechas y registros.
- Actualizar las fechas del catálogo que dice 2021, por requisito de FURAG, gobierno digital o MRI.
- Actualizar el plan de tratamiento de riesgos de seguridad, alineado con la nueva matriz institucional.
- Fortalecer la evidencia documental relacionada con cada procedimiento (actas, cronogramas, formatos actualizados).
- Realizar el cambio de logo institucional en todos los documentos que pertenecen al sistema de gestión.

CONCLUSIONES DE LA AUDITORÍA

- Aunque el área cuenta con prácticas implementadas en mantenimiento y control de servicios tecnológicos, se requieren mejoras en la documentación, socialización y actualización de algunos procedimientos clave. Las oportunidades identificadas permitirán fortalecer el sistema de gestión, la seguridad de la información y el soporte tecnológico de la entidad.
- Existen fortalezas en la gestión de mantenimiento de servicios tecnológicos y en la contratación de hosting.
- Se detectaron oportunidades de mejora en la documentación de procedimientos clave como copias de seguridad, requisitos de software y tratamiento de riesgos.
- Es necesario actualizar y fortalecer algunos procedimientos para asegurar el cumplimiento efectivo del SIG.

RECOMENDACIONES PARA LA SIGUIENTE AUDITORÍA

1. Actualizar los procedimientos de copias de seguridad y requisitos de software incluyendo cronogramas y criterios técnicos específicos.
2. Revisar y actualizar el inventario de herramientas y equipos informáticos con fechas verificables.
3. Socializar y documentar de manera formal los planes y políticas con los responsables del área.

ELABORÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
Profesional Universitario en Sistemas de Gestión	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025

INFORME DE AUDITORÍA

Código: GPI-SG.AI02-210.F03

Versión: 4.0

Página 7 de 7

4. Actualizar el plan de tratamiento de riesgos alineado con la última matriz de riesgos institucional.

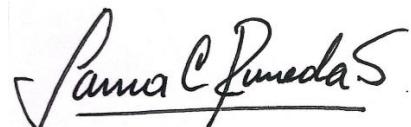
ASPECTOS POSITIVOS (Incluyendo los obstáculos encontrados y las oportunidades de mejora).

- Contratación formalizada y vigente del servicio de hosting (Contrato 113-2025).
- Existencia de indicadores de mantenimiento correctivo, lo cual permite seguimiento técnico adecuado.
- Participación del comité de inventarios y bajas, fortaleciendo la trazabilidad de equipos. El proceso de sistemas e informática emite el concepto técnico para verificar las razones por las cuales el bien se considera objeto de baja.
- Documentación de planes de mantenimiento, soportada con contratos y cronogramas.
- En los mantenimientos de los computadores se está realizando la revisión de la aplicabilidad de la política de escritorio y pantalla limpia.

FIRMA AUDITOR LÍDER:



FIRMA AUDITOR Y/O ACOMPAÑANTE:



FECHA: 27 de agosto de 2025

ELABORÓ	FECHA	REVISÓ	FECHA	APROBÓ	FECHA
Profesional Universitario en Sistemas de Gestión	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025	Jefe Oficina de Planeación Institucional	11/03/2025