



INFORME DE AUDITORÍA DE GESTIÓN 20251400207773

PARA **Doctor FELIPE DURÁN CARRÓN**
 Superintendente de Servicios Públicos Domiciliarios

Ingeniera DEIZITH YADIRA DÍAZ BOHÓRQUEZ
 Jefe Oficina de Tecnologías de la Información y las Comunicaciones

DE Jefe Oficina de Control Interno

ASUNTO Informe Auditoría de Gestión “*Procedimiento Gestión de la Información e Inteligencia de Negocio - TI-P-003*”

Estimada Ingeniera Deizith:

La Oficina de Control Interno dando cumplimiento al Plan Anual de Auditoría para la vigencia 2025, con el fin de valorar en forma pertinente el desempeño de los procesos y la eficacia y efectividad de los controles, así como el Sistema de Control Interno, realizó la Auditoría Interna de Gestión al Procedimiento Gestión de la Información e Inteligencia de Negocio - TI-P-003, obteniendo como resultado el informe final de auditoría, que se remite para su conocimiento con el objetivo de fortalecer del proceso de toma de decisiones en la Entidad y la adopción de las medidas a que haya lugar.

Como resultado de la auditoría se generaron 3 observaciones respecto de las cuales deberán formularse las acciones correctivas, preventivas y/o correcciones, de acuerdo con el procedimiento MC-P-001 de la Superintendencia de Servicios Públicos Domiciliarios (SSPD) contenido en el Sistema Integrado de Gestión y Mejora (SIGME), en un plazo no mayor a 15 días hábiles, por parte de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) y con el acompañamiento de la Oficina Asesora de Planeación e Innovación Institucional.

La Oficina de Control Interno cumpliendo el ciclo de la presente auditoría, con Procedimiento Gestión de la Información e Inteligencia de Negocio continuará con su labor de seguimiento y asesoría permanente, propendiendo por el mejoramiento continuo de las unidades de gestión de la Entidad, lo que redundará en un desempeño institucional exitoso.

Cordialmente,

JUAN JOSE PEDRAZA VARGAS

Este documento está suscrito con firma mecánica autorizada mediante Resolución No. 20201000057315 de 09 de diciembre del 2020

Anexo: Informe de auditoría.

Copia: Omar Camilo López López – Superintendente Delegado de Energía y Gas
 Ana Melissa Almario Patarroyo – Superintendente Delegada de Acueducto, Alcantarillado y Aseo
 Andrea Paola Prieto Mosquera – Jefe Oficina Asesora de Planeación e Innovación Institucional
Proyectó: Daniel Alberto Nieto Clavijo – Profesional especializado OCI
 Ángelo Mauricio Díaz Rodríguez y Fabio Alexander Vargas Cárdenas – Contratistas OCI

DATOS GENERALES

Proceso o Actividad Auditada:	Procedimiento Gestión de la Información e Inteligencia de Negocio - TI-P-003
Líder de Proceso / Jefe(s) Dependencia(s):	Jefe Oficina de Tecnologías de la Información y las Comunicaciones
Objetivo General de la Auditoría:	Verificar con enfoque basado en riesgos, la gestión adelantada por la OTIC frente a las necesidades de soluciones de tecnologías de la información (TI) que las distintas dependencias de la SSPD requirieron durante la vigencia 2024 y primer trimestre de 2025.
Objetivos Específicos de la Auditoría:	<ol style="list-style-type: none"> 1. Verificar, mediante muestra aleatoria, la trazabilidad de la gestión de la OTIC frente a las necesidades expresadas por las distintas dependencias en cumplimiento de las operaciones del Procedimiento Gestión de la Información e Inteligencia de Negocio del Proceso de Gestión de Tecnologías de la Información de SIGME. 2. Verificar la satisfacción de los usuarios funcionales sobre la gestión adelantada por la OTIC, mediante aplicación de encuesta de medición de satisfacción frente a la necesidad y a la solución generada por OTIC. 3. Validar la gestión del riesgo y el diseño e implementación de controles en relación con el Procedimiento Gestión de la Información e Inteligencia de Negocio del Proceso de Gestión de Tecnologías de la Información.
Alcance de la Auditoría:	Verificar, a través de herramientas, metodologías y técnicas de auditoría, la aplicación del procedimiento establecido en el documento TI-P-003 V.3, que abarca desde la identificación y priorización de necesidades hasta la recepción, análisis, diseño, desarrollo, pruebas, aprobación y despliegue de soluciones de gestión de la información, como servicio de la OTIC.
Tipo de Auditoría:	Mixta (Remota, presencial)
Tipo de Informe:	Preliminar

Auditor Líder		Equipo Auditor	
Daniel Nieto Clavijo		Ángelo Mauricio Díaz Rodríguez Fabio Alexander Vargas Cárdenas	

Reunión de Apertura						Reunión de Cierre					
Día	22	Mes	10	Año	2025	Día	17	Mes	12	Año	2025

TABLA DE CONTENIDO

1.	METODOLOGÍA.....	4
2.	DESARROLLO DE LA AUDITORÍA.....	4
2.1.	PROCEDIMIENTO GESTIÓN DE LA INFORMACIÓN E INTELIGENCIA DE NEGOCIO..	4
2.1.1.	Dependencias encuestadas.....	5
2.1.2.	Tipo de requerimiento o solución.....	6
2.1.3.	Parte del procedimiento que presentó dificultades.....	6
2.1.4.	Parte del procedimiento que funcionó mejor.....	7
2.1.5.	Sugerencias al proceso.....	7
2.2.	PRUEBA DE AUDITORÍA.....	8
2.2.1.	Recibo de la solicitud de información, Numeral 3.....	9
2.2.2.	Prueba de la solución de información, Numeral 7.....	10
2.2.3.	Aprobación del paso a producción, Numeral 8.....	10
2.2.4.	Despliegue de la solución de información, Numeral 9.....	10
2.3.	RIESGOS.....	12
3.	CONCLUSIONES.....	13
4.	RECOMENDACIONES E INVITACIÓN A LA MEJORA.....	14

1. METODOLOGÍA

Para la realización de esta auditoría, la OCI tuvo en cuenta diversos requerimientos de información y técnicas de auditoría como la observación, entrevistas con la unidad auditada mediante prueba de recorrido, verificación aleatoria documental de expedientes en la Herramienta de Servicios Tecnológicos de TI - Aplicativo ARANDA y contraste de información aportada con la contenida en los sistemas institucionales de información.

En el alcance de la presente auditoría el cual abarca el cumplimiento de las operaciones 3,7,8 y 9 del Procedimiento Gestión de la Información e Inteligencia de Negocio del Proceso de Gestión de Tecnologías de la Información de la vigencia 2024, hasta el primer trimestre de la vigencia 2025. el equipo auditor tuvo en cuenta los lineamientos institucionales y normas concordantes con el procedimiento a la luz de los lineamientos impartidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), en lo que tiene que ver específicamente con los modelos de arquitectura empresarial, gobierno y gestión de Tecnologías e Información.

Así mismo la OCI, teniendo en cuenta el referente estratégico institucional, realizó una verificación de los productos y actividades del Plan de Acción de la OTIC en el Sistema para la Formulación y Seguimiento a la Planeación Institucional (SISGESTION) durante el período auditado, donde se tuvieron en cuenta aspectos clave como la formulación de indicadores, riesgos del proceso y del procedimiento con sus respectivos controles.

2. DESARROLLO DE LA AUDITORÍA

2.1 PROCEDIMIENTO GESTIÓN DE LA INFORMACIÓN E INTELIGENCIA DE NEGOCIO

El Procedimiento Gestión de La Información e Inteligencia De Negocio - TI-P-003, en su versión 3 vigente desde 2024, se encuentra asociado al Proceso de Gestión de Tecnologías de la Información y su objetivo es: “*Gestionar las solicitudes de inteligencia de negocio priorizadas y las consultas de información, con el propósito de apoyar la capacidad de análisis y la toma de decisiones al interior de las dependencias*”.

Imagen 1 – Inteligencia de Negocio



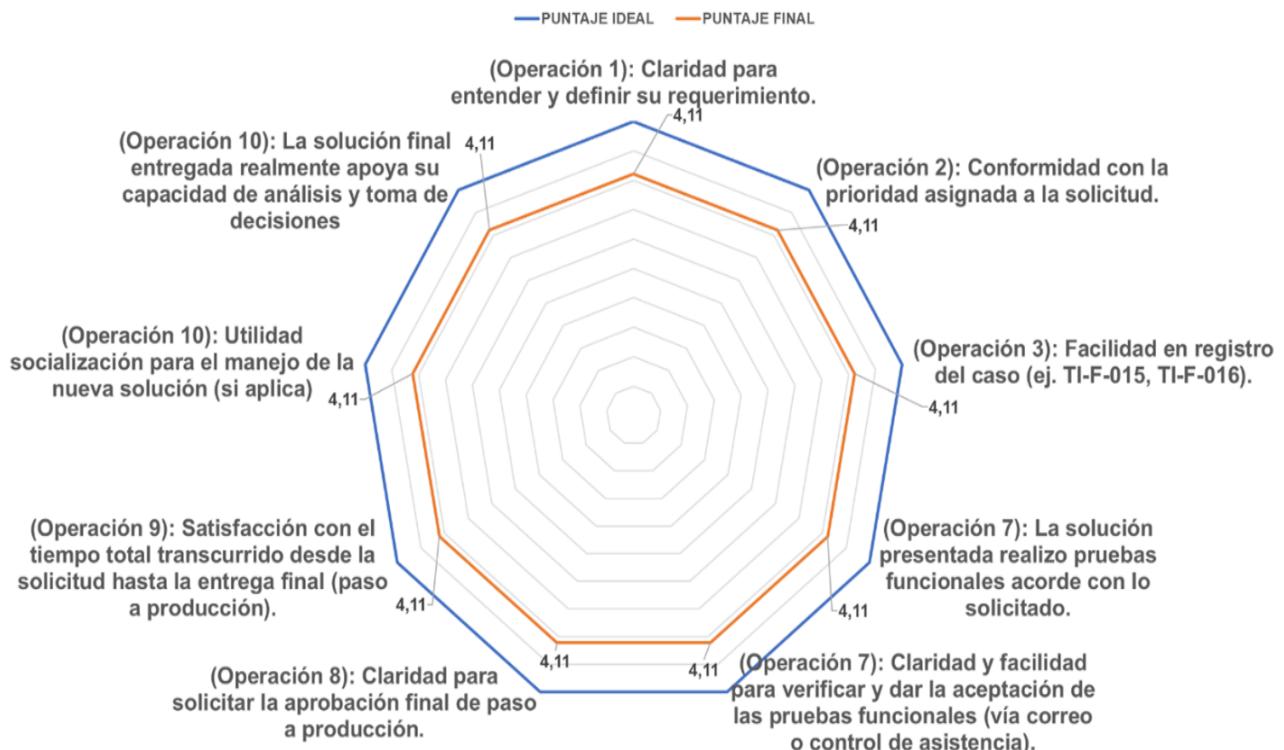
Fuente: <https://upress.mx/secciones/vida-universitaria/11228-1-de-octubre-dia-de-la-inteligencia-de-negocios>

Con el fin de verificar la satisfacción de los usuarios funcionales sobre la gestión adelantada por la por la OTIC, la OCI diseñó una encuesta, con preguntas en escala Likert, que es una herramienta de encuesta para evaluar las opiniones, actitudes y percepciones de los usuarios que requirieron de la

solución tecnológica dispuesta en el procedimiento, en los siguientes niveles: muy insatisfecho = 1, insatisfecho = 2, neutral = 3, satisfecho = 4, muy satisfecho = 5.

Como resultado, se obtuvieron nueve (9) respuestas que hacen referencia a los casos registrados a través del aplicativo ARANDA como se observa en la siguiente gráfica:

Gráfica 1 - Percepción usuarios funcionales



Fuente: Creación propia de la OCI respuestas formulario Google

Como se puede ver, en general los usuarios se encuentran satisfechos con las soluciones ofrecidas en el procedimiento con un resultado uniforme en 4,11. Sin embargo, se evidencia una pequeña brecha respecto del puntaje ideal de 5, por lo que se puede inferir que existen oportunidades de mejora en cuanto a las operaciones analizadas y que hacen parte de cada componente del procedimiento.

2.1.1 Dependencias encuestadas:

Gráfica 2 - Dependencias encuestadas



Se pudo establecer que los mayores usuarios de las soluciones ofrecidas en el procedimiento son las Superintendencias Delegadas de Energía y Gas Combustible (SDEGC) y la de Acueducto, Alcantarillado y Aseo (SDAAA), dado que seis (6) respuestas fueron suministradas por el Grupo SUI de la SDEGC y 3 respuestas fueron suministradas por la SDAAA.

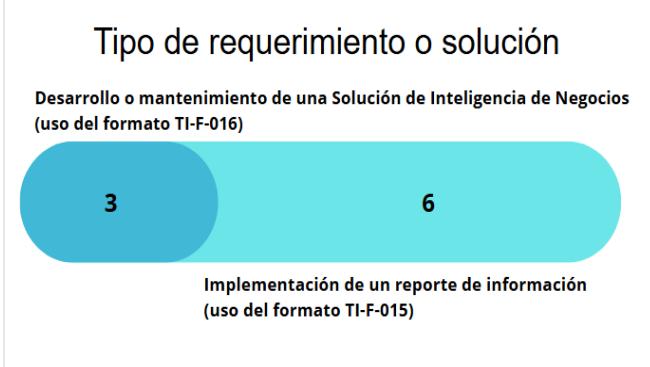
Fuente: Creación propia de la OCI respuestas formulario Google

En tal contexto, la OCI **recomienda** divulgar el Procedimiento Gestión de la Información e Inteligencia de Negocio - TI-P-003, con el propósito de que las soluciones no se centren únicamente en los procesos misionales toda vez que las soluciones ofrecidas sirven para apoyar la toma de decisiones en todos los procesos a cargo de las distintas dependencias de la entidad, como son los procesos estratégicos, de apoyo y de evaluación.

2.1.2 Tipo de requerimiento o solución:

Gráfica 3 - Tipo de requerimiento o solución

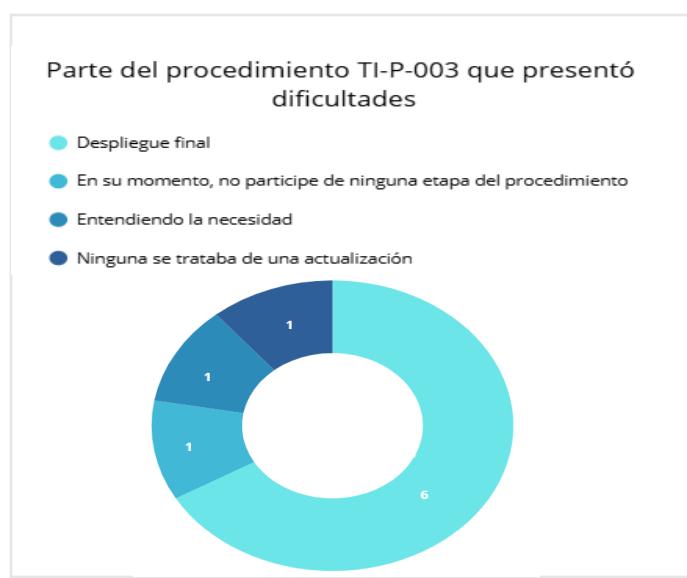
Se evidenció que, durante el período auditado, se requirieron 3 desarrollos de una solución de inteligencia de negocios o mantenimiento que surgieron luego de haberse priorizado y diagnosticado por la OTIC mediante formato TI-F-016. Por otra parte, se evidenció que se solicitaron 6 reportes de información mediante Formato TI-F-015, encontrando así, que este último fue el que generó un mayor número de requerimientos.



Fuente: Creación propia de la OCI respuestas formulario Google

2.1.3 Operaciones con Dificultades:

Gráfica 4 - Operaciones con dificultades



formulario Google

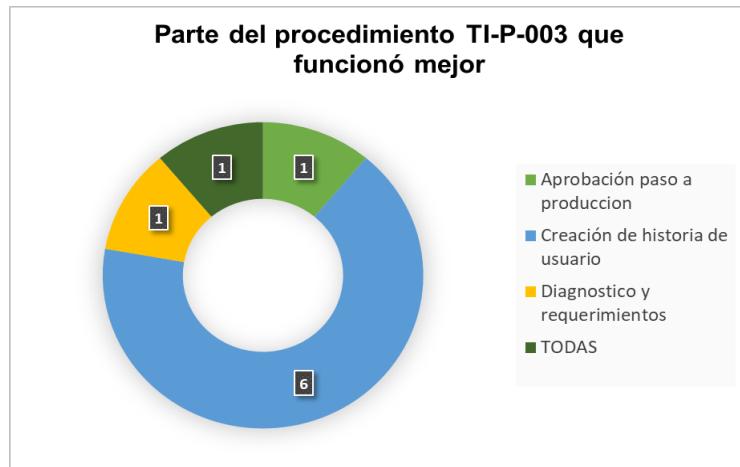
De la tabulación de la encuesta, se evidenció que seis (6) de los nueve (9) usuarios funcionales encuestados manifestaron haber tenido algunas dificultades en el desarrollo de las soluciones ofrecidas en procedimiento, específicamente en lo que tiene que ver con las operaciones 9 y 10 del procedimiento, las cuales están relacionadas con el despliegue, paso a producción, uso y apropiación de la solución, evidenciando una oportunidad de mejora frente a la finalización del procedimiento en cuanto a los despliegues de las soluciones ofrecidas.

Fuente: Creación propia de la OCI respuestas

2.1.4 Operaciones Destacadas

Gráfica 5 - Operaciones que funcionaron mejor

Es de resaltar, respecto a lo evidenciado, que en cada una de las etapas de recolección de datos y en los instrumentos utilizados para el levantamiento de información, por parte de los profesionales de la OTIC y la líder de la dependencia, que el proceso y repositorio de la información es coherente y ordenado, lo que permite encontrar de una manera ágil y fidedigna cualquier tipo de información respecto a las soluciones ofrecidas en el procedimiento.



Fuente: Creación propia de la OCI respuestas formulario Google

En la encuesta, los usuarios funcionales resaltaron precisamente que la creación de los historiales de usuario y diagnóstico de las necesidades, funciona bien y debería mantenerse de esta manera, encontrando fortalezas especialmente en la Política de Gestión de Datos e Información GIC-M-002 Versión 03 en el numeral 7.1.2 Lineamiento de calidad de datos “*criterios adicionales de calidad...*” literales a, b, d, h, k y m.

2.1.5 Sugerencias al proceso

Gráfica 6 Sugerencias



En la encuesta, los usuarios funcionales recomiendan agilizar las operaciones 8 y 9 en lo que tiene que ver con la aprobación y despliegue de las soluciones, pues la percepción es que el tiempo transcurrido entre la finalización de las pruebas funcionales y el paso a producción o despliegue es amplio y en algunos casos ambiguo, pues al no contar con un Acuerdo de Nivel de Servicio (ANS) claro y establecido desde el inicio, los usuarios perciben demoras y retrasos en la puesta en marcha de las soluciones ofrecidas a través del procedimiento.

Fuente: Creación propia de la OCI respuestas formulario Google

2.2 PRUEBA DE AUDITORÍA

La OCI solicitó a la OTIC la remisión de los casos de inteligencia de negocios solicitados por las diferentes dependencias, para el período de tiempo comprendido entre el año 2024 y primer trimestre de 2025, reportándose nueve (9) casos, así:

Tabla 1 - Relación de Despliegues Inteligencia de Negocio

Caso Aranda	Nombre Informe	Plataforma Publicación	Link	Fecha Publicación
241510	GRTG1 Gestión del Riesgo	PBI-Reporte Interno	https://wa-reportsui.azurewebsites.net/home/report/10f820a8-37ca-435b-9ea6-a5b90101a806	19/06/2024
236979	Informe General de Auditoría de Gestión y Resultados	PBI-Reporte Interno	https://wa-reportsui.azurewebsites.net/home/report/903f107d-336d-4a1a-957c-eb7c984d88c5	16/04/2024
236981	Indicadores de Riesgo de prestadores por Auditores	PBI-Reporte Interno	https://wa-reportsui.azurewebsites.net/home/report/903f107d-336d-4a1a-957c-eb7c984d88c5	16/04/2024
239057	NUECA - Registro de estaciones de clasificación y aprovechamiento	PBI-Reporte Externo	https://wa-reportsui.azurewebsites.net/home/report/b466540a-b687-43ea-a63d-d544705a113b	17/05/2024
240350	SUI_Calidad_Estratificación	Cubo-Bodega	http://bi.superservicios.gov.co/o3web/viewdesktop.jsp?cmnd=open&source=SUI_CALIDAD_ESTRATIFICACION	04/06/2024
244734	SUI_Rups_Oficial	Cubo-Bodega	http://bi.superservicios.gov.co/o3web/viewdesktop.jsp?cmnd=open&source=SUI_RUPS_OFICIAL	12/08/2024
246174	Consolidado de Información Comercial - ZNI	PBI-Reporte Interno	https://wa-reportsui.azurewebsites.net/home/report/ec1b7a82-123e-4d7d-a7db-99bbfec7429	02/09/2024
247224	SUI_Componentes_Tarifarios	Cubo-Bodega	http://bi.superservicios.gov.co/o3web/viewdesktop.jsp?cmnd=open&source=SUI_COMPONENTES_TARIFARIOS_GAS_RED	17/09/2024
251632	Contratos Suministro	PBI-Reporte Interno	https://wa-reportsui.azurewebsites.net/home/report/8f4e54b7-d7ae-44da-9998-83d4132407d6	26/11/2024

Fuente: Información suministrada por la OTIC

En la prueba de auditoría, se encontraron dos (2) casos adicionales, que no fueron reportados por la OTIC, en respuesta al requerimiento de información realizado por la OCI, por lo que se presentó un error por omisión de identificación y suministro de la información solicitada a la dependencia. Estos corresponden a los casos 250810 y 256856 identificados en la herramienta Aranda, en el período evaluado y dado el alcance de la auditoría, los cuales fueron igualmente analizados y evaluados.

De acuerdo con revisión técnica de los nueve (9) casos suministrados por la OTIC, en el Aplicativo ARANDA, a través de un usuario especialista creado y asignado para el desarrollo de la auditoría se obtuvieron los siguientes resultados:

2.2.1 Recibo de la solicitud de información, Numeral 3

De acuerdo con el Procedimiento TI-P-003 su numeral 3, se reciben los documentos con los siguientes formatos: TI-F-032, TI-F-016 y TI-F-015 en los siguientes casos; consulta de información específica, solución de inteligencia de negocios e implementación de un reporte de información.

El Formato TI-F-032 no se emplea en ninguno de los casos enlistados. Se presenta, en la mayoría de los casos el Formato TI-F-016, en 8 de 9 y el Formato TI-F-015 en 4 de 9. Los dos formatos son utilizados en 5 de los 9 casos.

La OCI, en su Rol de Enfoque Hacia la Prevención, **recomienda** la revisión de la funcionalidad de la inclusión del Formato TI-F-032 en el procedimiento, ya que, al ser diligenciado por el usuario, requiere cierto conocimiento y dominio técnico.

De igual manera, se **sugiere** actualizar el Formato TI-F-016 en el cual se menciona el uso del Sistema de Gestión Documental (SGD ORFEO), el cual no es sistema que utiliza actualmente la Entidad.

Observación 1 – Falta de Formato Requerido para Gestión de la Solicitud

No.	Descripción de la observación o situación encontrada (Condición)	Criterios	Posibles causas identificadas por la OCI	Posibles Riesgos (Efectos o impactos)
1.	Se encuentra el caso 256856 que no fue reportado por la OTIC y no cuenta con el Formato TI-F-016, previsto en el procedimiento auditado. Lo mismo ocurre con el caso 246174, que no cuenta con este formato, de acuerdo con el diagnóstico realizado por la OTIC. Cabe anotar que este formato debe usarse también en caso de solicitarse un mantenimiento.	Procedimiento TI-P-003, descripción numeral 3: “A partir de un caso registrado en la Herramienta de Servicios Tecnológicos de TI, se revisa la solicitud de información, la cual puede ser: una consulta de información específica, un desarrollo o mantenimiento de una solución de inteligencia de negocios o la implementación de un reporte de información”.	Descuido por parte de la OTIC en la identificación de los casos archivados en aplicativo ARANDA como GESTIÓN DE LA INFORMACIÓN e INTELIGENCIA DE NEGOCIO. Al tratarse de un mantenimiento de un desarrollo previamente realizado, se obvió el uso de los formatos, por una posible agilidad en la entrega del ajuste en el producto ya existente. Sin embargo, el procedimiento lo tiene contemplado en su descripción.	Posibilidad de afectación reputacional al no cumplir el procedimiento, lo que conlleva a la perdida de trazabilidad en el producto final entregado por la dependencia.

2.2.2 Prueba de la solución de información, Numeral 7

De acuerdo con el Procedimiento TI-P-003 su numeral 3, se realizan las pruebas funcionales a una solución de inteligencia de negocios o a la implementación de un reporte de información y el resultado se registra en el Formato TI-F-049.

En las pruebas realizadas, se evidencia que este formato está presente en 3 de los 9 casos, lo que representa un 33,33% de registro en los casos auditados y se encuentra ausente en el 66,66% de los mismos. Se recomienda llevar siempre este registro para contar con la trazabilidad en el resultado de las pruebas.

2.2.3 Aprobación del paso a producción, Numeral 8

De acuerdo al Procedimiento TI-P-003, una vez se tiene la aceptación de las pruebas, el Delegado/ Director/ Coordinador/ Jefe de la dependencia o a quien se designe a través de reunión o correo electrónico, envía la aprobación para la publicación o despliegue de la solución de información. La OCI evidencia que el correo de aprobación fue enviado en 3 de los 9 casos objeto de auditoría, y mediante reunión evidenciado por el formato GD-F-063 se presentó en 7 de los 9 casos, lo que demuestra un mayor número de aprobaciones por este último medio.

2.2.4 Despliegue solución de información (paso ambiente de producción), Numeral 9

De acuerdo al procedimiento TI-P-003, el despliegue se realiza a través del Formato TI-F-033 y el Formato TI-F-013 al tratarse de una inteligencia de negocios. Se evidencia el uso de este último formato en 3 de los casos reportados por OTIC y utilizados en mantenimiento de diferentes cubos.

Posterior a la verificación de las operaciones contenidas en los numerales del alcance de la auditoria del procedimiento T-P-003 a evaluar en la prueba de auditoría, el equipo auditor realizó una revisión en la información publicada como producto final, encontrando algunos datos de prueba en el ambiente de producción. En el Sistema O3 se permite la grabación de vistas o consultas en primera instancia al usuario funcional, pero a su vez al usuario externo sin ningún tipo de registro o autenticación, lo cual supone un riesgo en la seguridad digital de la SSPD, en caso de infiltrarse un sistema de automatización robótica de procesos (RPA) y realizar la creación de varias vistas y reglas de forma indiscriminada, lo cual podría constituir un riesgo de seguridad no gestionado.

Imagen 2 - Publicación de cubos de información en herramienta O3 de la SSPS

The screenshot shows the Business Intelligence Enterprise Portal interface. At the top, there is a logo for 'Business Intelligence' and a link to 'Cerrar sesión'. Below the header, there are two main navigation links: 'Enterprise Portal' and 'O3bi AdHoc'. The 'O3bi AdHoc' section is currently active, displaying a list of cube definitions. On the left, a scrollable list includes entries like 'Mercado Gas y electricidad (Rol User)', 'Mercado Gas y electricidad -VATIA (Privada)', and 'prueba_f@nc1On4l (Pública)'. On the right, another scrollable list titled 'Reglas' lists various entities such as 'AAA', 'AGUADELOSANDES', 'AquaDeLosAndes', 'ASOCIACION AMBIENTAL DE RECICLADORES UNION BTA', and 'ASOCIACION ECOLOGICA PUNTO VERDE'. The interface has a clean, modern design with a white background and grey accents.

Fuente: <http://bi.superservicios.gov.co/o3web/index.jsp>

Observación 2 - Debilidades en la Seguridad Digital.

No.	Descripción de la observación o situación encontrada (Condición)	Criterios	Possibles causas identificadas por la OCI	Possibles Riesgos (Efectos o impactos)
2	<p>Al revisar el resultado de los despliegues, se encuentra que los casos 240350, 247224, 244734 correspondientes a los cubos de inteligencia de negocios, alojados en la plataforma O3, se evidencian que cualquier usuario puede crear cualquier tipo vista en cualquier combinación de datos, lo que puede constituirse en una debilidad en la seguridad digital.</p> <p>http://bi.superservicio s.gov.co/o3web/index .jsp</p>	<p>Numeral 2 Lineamientos Modelo de Gestión y Gobierno TI Gestión de Sistemas de información (MGGTI.G.SI) - Guía de Dominio de Gestión de Sistemas de información.</p> <p>Subnumeral 4: Ambientes independientes en el ciclo de vida de los Sistemas de información.</p> <p>La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar y mantener ambientes independientes (desarrollo, pruebas, producción) durante el ciclo de vida de los sistemas de información.</p> <p>Ley de protección de datos personales 1581 de 2012</p>	<p>Possible desconocimiento de los lineamientos y protocolos establecidos para el uso de ambientes de pruebas.</p> <p>Falta de mantenimiento en los ambientes de producción para depurar datos de prueba de los usuarios.</p> <p>Bajas restricciones para la creación de vistas de cubos sin previo registro o autenticación del usuario cliente.</p>	<p>Posibilidad de afectación a la seguridad digital institucional, por la vulnerabilidad en la falta de control y el uso inadecuado de las consultas que ofrece el aplicativo O3.</p> <p>Posibilidad de afectación reputacional por la fiabilidad de la información publicada de la entidad, generando confusiones en la calidad de su contenido, dado que de cara al ciudadano se evidencia ambientes de pruebas.</p>

En consecuencia y en su Rol de Enfoque Hacia la Prevención, la OCI invita a que se analice y se cree un riesgo específico para el procedimiento TI-P-003 para evitar o mitigar la materialización e impacto de las vulnerabilidades de la gestión en materia de riesgos de seguridad digital de la SSPD.

2.3 RIESGOS

Se revisaron las versiones 2 y 3 del Procedimiento de Gestión de la Información e Inteligencia de Negocio (TI-P-003), con el fin de analizar su alcance y si los puntos de control resultaban suficientes para gestionar la incertidumbre y lograr los productos esperados, ejecutando las actividades descritas. Como resultado de este ejercicio se evidenció que no se describen puntos de control en ninguna de las versiones del procedimiento auditado.

La OCI, en su requerimiento de información, solicitó a la dependencia que informara si existe un riesgo relacionado con el procedimiento, a lo que respondieron que se ha identificado el riesgo de seguridad de la información, descrito así: *"Possible afectación a la disponibilidad de los sistemas de información por inadecuadas estrategias de respaldo y restauración debido a realización de copias de seguridad sin control"*. Al respecto, la OCI considera que este riesgo es indirecto y no corresponde con la gestión de potenciales vulnerabilidades dentro del procedimiento auditado.

Por otra parte, se revisó la gestión realizada en el período auditado acerca del Servicio de Inteligencia de Negocios que presta la OTIC, y se encontró relación con las actividades 86635, 86631 y 86929 del plan de acción en SISGESTION, en la cuales se evidenciaron 10 contratos relacionados directamente con el servicio, los cuales se enfocan en servicios profesionales para la OTIC, principalmente en tres líneas: (i) desarrollo de requerimientos en los sistemas de información según la gestión de la demanda; (ii) actualización y desarrollo de interacciones de usuario en los portales web institucionales; y (ii) apoyo al ciclo de vida del software con énfasis en la especificación de historias de usuario.

En conjunto, se observa que todos los contratos están orientados a fortalecer el desarrollo, mantenimiento y actualización de las soluciones tecnológicas de la Entidad. Dichos contratos son los números 054, 062, 076, 077, 112, 114, 134, 135, 157 y 156 de 2024, financiados con recursos de inversión del proyecto de “*Fortalecimiento de la Gobernanza de las Tecnologías de la Información en el Cumplimiento de la Misionalidad de la Superservicios a Nivel Nacional*”.

Observación 3 - Debilidades en la Gestión del Riesgo

No.	Descripción de la observación o situación encontrada (Condición)	Criterios	Possibles causas identificadas por la OCI	Possibles Riesgos (Efectos o impactos)
3	No se evidencia riesgos asociados al Procedimiento de Gestión de la Información e Inteligencia de Negocio (TI-P-003), en sus versiones 2 y 3, ni controles operativos en el mismo, aunado a que se evidencia una brecha de insatisfacción por parte de algunos usuarios funcionales.	Según los artículos 2, 3 y 9 de la Ley 87 de 1993 , El Decreto 1083 de 2015 , modificado por el Decreto 648 de 2017 , y el Decreto 1499 de 2017 (MECI) , establecen que la gestión del riesgo es componente obligatorio del Sistema de Control Interno y que la Oficina de Control Interno debe verificar su implementación. Finalmente, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFF versión 7 (2025) indica que todos los procesos deben contar con identificación, valoración y tratamiento de riesgos.	Falta de articulación del proceso con la metodología institucional de administración de riesgos establecida en el Instructivo DE-I-004, y ausencia de seguimiento por parte de los responsables del proceso para incorporar la gestión de riesgos en la planeación, ejecución y control de las actividades.	Posibilidad de afectación reputacional y económica, debido a la potencial utilización de recursos humanos, técnicos y financieros de la entidad en el desarrollo de soluciones tecnológicas sin que exista certeza sobre su viabilidad, funcionalidad o adopción final. Esta situación incrementa la probabilidad de errores operativos, incidentes de seguridad de la información y observaciones por parte de entes de control, afectando la eficiencia y transparencia institucional.

En consecuencia y en su Rol de Enfoque Hacia la Prevención, la OCI invita a la OTIC a establecer los puntos de control en el procedimiento y diseñar los controles operativos necesarios para gestionar de una manera adecuada y preventiva los riesgos asociados al procedimiento auditado.

3 CONCLUSIONES

La OCI, con el fin de mejorar la gestión de las soluciones tecnológicas y asegurar que los recursos institucionales se utilicen de manera eficiente y controlada, plantea las siguientes conclusiones orientadas a corregir las debilidades identificadas en la forma en que se gestionan los desarrollos de inteligencia de negocios, reportes de SUI y aplicaciones dentro de la Entidad. Estas acciones buscan aportar claridad, trazabilidad y control sobre los procesos que posiblemente presentan vacíos en su planificación, seguimiento y medición.

- La herramienta de publicación de datos en el sistema O3 cumple con la funcionalidad de presentar bases de datos e información de interés a los usuarios de la SSPD, sin embargo, se evidencia que algunos usuarios han hecho uso de la misma sin aplicar nombres adecuados a las vistas y reglas, los cuales no se han depurado. Se sabe que esto no afecta la estructura y contenido de las bases de datos, pero puede inducir al error al hacer la consulta de estas vistas y se satura el sistema por la presentación inadecuada de los nombres de estas.
- Se presentan debilidades en la aplicación de la gestión del riesgo, gestión de la información y ambientes de prueba y producción o despliegue dentro del Procedimiento de Gestión de la Información e Inteligencia de Negocio (TI-P-003). Estas falencias afectan la integridad del proceso, la protección de los activos de información y la adecuada administración de los recursos institucionales.
- El procedimiento auditado no tiene identificados y gestionados riesgos específicos de acuerdo con sus vulnerabilidades, así como puntos de control que permitan su manejo.
- La OTIC no cuenta con controles que le permitan realizar un monitoreo al uso adecuado de los desarrollos y consultas creadas a través del sistema O3.

4 RECOMENDACIONES E INVITACIÓN A LA MEJORA

En consecuencia y en su Rol de Enfoque Hacia la Prevención, la OCI invita a que se tengan en cuenta las siguientes recomendaciones, con el fin de propender a la mejora continua y a la optimización de los recursos con los que cuenta la SSPD, las cuales de describen a continuación:

- Hacer una mayor divulgación del procedimiento para cumplir el objetivo y promover la pluralidad de usuarios funcionales de las distintas dependencias de la SSPD, no solo los misionales, haciendo publicaciones por los medios de comunicación institucionales, protectores de pantalla, comunicados en el Boletín Infórmate y comunicaciones internas.
- Establecer los acuerdos de nivel de servicio (ANS), según la metodología de gestión de proyectos adoptada por la OTIC.
- Usar un marco de trabajo ágil como (Scrum) en la gestión de soluciones de inteligencia de negocios o desarrollo de aplicaciones. Esto permitirá gestionar proyectos donde no hay certeza sobre el tiempo o los recursos requeridos, pues asegura entregables claros en términos de calidad y promueve la adaptación continua del alcance en intervalos de tiempo fijos (Spirnt).
- Configurar la plataforma O3 para exigir la autenticación (registro de usuario y contraseña) a cualquier usuario, interno o externo, que desee crear, guardar o modificar vistas y reglas, con el fin de mitigar el riesgo de saturación del sistema y la creación indiscriminada de vistas por mecanismos automatizados (RPA) o usuarios no autorizados.
- Implementar un proceso de mantenimiento programado (ej: trimestral) liderado por la OTIC, cuyo objetivo sea revisar y depurar aquellas vistas y reglas que contengan datos de prueba, que no hayan sido utilizadas en un período de tiempo definido. Esta medida contribuirá directamente a la fiabilidad de la información publicada y a la seguridad de la plataforma, respondiendo a la debilidad sobre la calidad de los datos y el posible riesgo reputacional.
- Evaluar el servicio de inteligencia de negocio y desarrollo por fuera del Aplicativo ARANDA, pues obedece a otras necesidades y sus resultados no reflejan la satisfacción del producto entregado en desarrollo del procedimiento (se califica mucho antes de iniciar con la gestión de la solución), con

20251400207773

una encuesta de satisfacción que se envía al usuario radicador de la necesidad en el aplicativo ARANDA y el que a la postre puede que no sea quien reciba el desarrollo o la solución a satisfacción.

- Revisar y remitir de manera completa y precisa la información requerida por la oficina de control interno o entes de control, para evitar la pérdida de confianza en la misma y posteriores aclaraciones y suspicacias, sobre los asuntos relacionados con el procedimiento auditado.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	Cargo	Firma
Juan José Pedraza Vargas	Jefe Oficina Control Interno	