

M E M O R A N D O



20262000080403

No. 20262000080403
Bogotá, 18 agosto 2026

Para: **Ludmila Del Carmen Vergara Rosales - Superintendente**

De: Jefe De Oficina - Oficina De Control Interno

Asunto: Remisión del informe de verificación al proceso gestión de comunicaciones

Cordial saludo,

En cumplimiento de las funciones asignadas a la Oficina de Control Interno y de conformidad con el Plan Anual de Auditoría 2026, aprobado por el Comité Institucional de Coordinación de Control Interno (CICCI) en sesión No. 1 del 27 de marzo de 2026 y sus modificaciones, se remite para su conocimiento el Informe de Verificación al Grupo Interno de Trabajo de Comunicaciones, cuyo objetivo estuvo orientado a evaluar el cumplimiento de los lineamientos relacionados con la seguridad de la información, gestión de información reservada y confidencial, administración de redes sociales institucionales, custodia de los equipos asignados al Grupo Interno de Trabajo de Comunicaciones y gestión de los riesgos asociados al proceso.

Como resultado de la verificación, se identificaron situaciones que requieren fortalecimiento relacionadas, entre otros aspectos, con la formalización y documentación de controles, manejo de información sensible y confidencial, custodia y administración de activos, administración de activos digitales y redes sociales, gestión de riesgos y trazabilidad de los controles implementados.

En atención a las recomendaciones formuladas en el informe, La Oficina de Control Interno sugiere suscribir el correspondiente Plan de Mejoramiento dentro de los quince (15) días hábiles siguientes a la recepción del presente memorando, estableciendo para cada recomendación la acción de mejora, el responsable de su ejecución, la fecha o plazo de cumplimiento y los soportes que permitan acreditar su implementación.

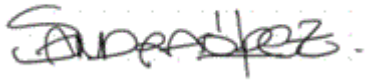
Asimismo, en cumplimiento de lo dispuesto en el parágrafo 1.º del artículo 2.2.21.4.7 del Decreto 1083 de 2015, se remite al representante legal con copia del presente informe a los integrantes del Comité Institucional de Coordinación de Control Interno (CICCI), para su conocimiento, de

Página | 1

conformidad con las disposiciones aplicables sobre los destinatarios de los informes de auditoría, seguimientos y evaluaciones.

Agradecemos su oportuna gestión, orientada a la implementación de las acciones de mejora y al fortalecimiento continuo del Sistema de Control Interno de la Entidad.

Atentamente,



Sandra Lucia Lopez Pedreros
Jefe De Oficina
OFICINA DE CONTROL INTERNO
Superintendencia de Transporte

Anexos:

- AJUSTADO INFORME_VERIFICACION_COMUNICACIONES.pdf
- 20262000080403.pdf

	Nombre del funcionario	Documento Firmado Digitalmente
Proyectó y elaboró	Edy Johana Melgarejo Pinto	edymelgarejo [18/agosto/2026 09:40:36 a. m.]
Aprobó	Sandra Lucia Lopez Pedreros	sandrallopez [18/agosto/2026 10:19:58 a. m.]

Evaluación: _____ Seguimiento: _____ Auditoría Interna: _____ Otro: (X)
Verificación

FECHA DE EMISIÓN DEL INFORME: 18 de agosto de 2026

NOMBRE DEL INFORME:

Verificación proceso Gestión de Comunicaciones.

1. OBJETIVO GENERAL

Evaluar la gestión del proceso de comunicaciones responsabilidad del GIT de Comunicaciones, mediante la verificación del cumplimiento de los lineamientos de seguridad de la información y reserva, así como de los controles asociados al manejo de información confidencial y a la custodia, uso y protección de los equipos asignados, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información institucional y de los recursos tecnológicos de la Entidad y asignados al GIT.

2. ALCANCE

La verificación comprendió la revisión de la información remitida mediante correo electrónico por el Grupo de Comunicaciones de la Secretaría General, el 22 de abril de 2026, correspondiente al periodo del 1 de enero al 31 de marzo de 2026.

El ejercicio de verificación estuvo orientado a evaluar los controles relacionados con la Seguridad de la información y reserva: Incluye: Manejo de información confidencial en el GIT de Comunicaciones; Manejo de información confidencial dado que el GIT de comunicaciones por ser personal cercano al Superintendente de Transporte, siempre maneja información confidencial de la Entidad. Custodia de equipos: elementos de trabajo como cámaras, micrófonos, trípodes, memorias, cables, dron, teléfonos celulares, etc. Información contenida en los computadores, celulares y cámaras de la Entidad. Se puede presentar el riesgo de pérdida de información ya sea por extravío de equipos o por descuidos en el manejo de esta. Comunicaciones institucionales y riesgo reputacional. Incluye: Información publicada en redes sociales para revisar campañas vigentes; requerimientos permanentes del Ministerio de Transporte y Presidencia de la República en materia de comunicaciones y sinergias gubernamentales. (Secretaría General)

2.1 LIMITACIONES AL ALCANCE

La presente verificación se realizó bajo un enfoque de aseguramiento independiente, orientado a probar la existencia y operación de los controles del proceso y a evidencias su ausencia cuando corresponda, y no bajo un enfoque de asesoría sobre los

documentos que a la fecha se encuentran en construcción por el proceso en coordinación con la Oficina Asesora de Planeación (OAP) y la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC). En consecuencia, la Oficina de Control Interno se abstiene de participar en el diseño de dichos controles, con el fin de preservar su independencia frente a una eventual auditoría posterior de los mismos.

Se identifican las siguientes limitaciones al alcance de la verificación, conforme a las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna 2210 y 2220:

- (i) La evidencia considerada en esta verificación se circunscribe a la información y soportes remitidos por el proceso auditado mediante correo electrónico del 22 de abril de 2026, en respuesta al memorando de apertura No. 20262000032303 del 13 de abril de 2026. En consecuencia, las conclusiones se formulan sobre la base de la documentación efectivamente suministrada y de los procedimientos de verificación independientes realizados por la Oficina de Control Interno.
- (ii) Parte de los soportes aportados corresponde a hechos posteriores al periodo evaluado (1 de enero al 31 de marzo de 2026). En particular, los acuerdos de confidencialidad fueron suscritos entre el 16 y el 21 de abril de 2026 y las bitácoras de salida y retorno aportadas corresponden al 20 de abril de 2026. De lo anterior se concluye que, durante el periodo evaluado, los controles asociados a dichos soportes no se encontraban operando, conclusión que se refleja en los resultados y en las conclusiones del presente informe

3. MARCO NORMATIVO O CRITERIOS DE AUDITORÍA, EVALUACIÓN O SEGUIMIENTO

- **Ley 87 de 1993.** Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- **Ley 527 de 1999.** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000.** Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014.** Ley de Transparencia y del Derecho de Acceso a la

Información Pública.

- **Decreto 1078 de 2015.** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Resolución 02277 de 2025.** Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia. Modelo de Seguridad y Privacidad de la Información (MPSI)
- **Decreto 1083 de 2015.** Decreto Único Reglamentario del Sector de Función Pública, aplicable en materia de viáticos y comisiones de los servidores públicos.
- **Resolución MinTIC 1519 de 2020.** Por la cual se definen los estándares y directrices para publicar información en los canales oficiales de las entidades públicas.
- **Manual Operativo de MIPG, versión 6.1 de 2026.** Política de Gobierno Digital. Departamento Administrativo de la Función Pública (DAFP).
- **Guía para la Gestión Integral del Riesgo en Entidades Públicas (DAFP) Versión 7 de agosto 2025.**

Y demás normas aplicables al objeto de esta verificación.

4. METODOLOGÍA

La verificación se ejecutó en cumplimiento del Plan Anual de Auditoría 2026, aprobado por el Comité Institucional de Coordinación de Control Interno en sesión

No. 1 del 27 de marzo de 2026. La apertura formal del ejercicio se realizó mediante el memorando radicado 20262000032303 del 13 de abril de 2026, dirigido a la Coordinadora del GIT de Comunicaciones.

La información evaluada fue suministrada por el proceso mediante correo electrónico del 22 de abril de 2026, en respuesta al memorando de inicio de la verificación especial al proceso de Comunicaciones, a través del documento denominado "*Informe de Control Interno*", el proceso atendió los cuarenta y dos (42) requerimientos formulados por la oficina de Control Interno, adjuntando los soportes documentales correspondientes para su verificación y análisis.

Adicionalmente, la Oficina de Control Interno aplicó procedimientos de aseguramiento independientes sobre la información suministrada.

Las técnicas de auditoría aplicadas fueron:

- **Consulta:** Formulación de (42) preguntas y solicitudes de información al personal responsable del proceso.
- **Inspección:** Análisis y revisión de documentos, registros, procedimientos e inventarios aportados por el proceso en atención al requerimiento. Se realizó consulta de la documentación disponible en DARUMA y revisión de la cadena de valor institucional.
- **Revisión de Comprobantes:** Verificación de la validez y soporte documental de la información suministrada.
- **Procedimientos Analíticos:** Comparación de controles reportados frente a la evidencia aportada para identificar diferencias. Entre ellos se realizó el cruce del inventario de bienes reportado por el proceso frente a la base oficial de inventarios de la Entidad, revisión de la cadena de valor institucional.
- **Rastreo:** Verificación de la integridad e integralidad de la información presentada.

Cada observación consignada en este informe se encuentra soportada en los correos, documentos y demás soportes suministrados el 22 de abril de 2026, cuya identificación (nombre de archivo, imagen o correo de origen) se referencia en la fuente de cada tabla, imagen o cita incluida en el Numeral 6.

La Oficina de Control Interno no validó ni aprobó documentos que, al momento de la verificación, se encontraban en construcción o borrador; estos fueron considerados únicamente para establecer el estado de formalización documental existente durante el periodo evaluado.

5. RESUMEN EJECUTIVO

La Oficina de Control Interno con el propósito de evaluar el cumplimiento de los lineamientos relacionados con la seguridad de la información, la gestión de información reservada y confidencial, la administración de redes sociales institucionales, la custodia de los equipos asignados al Grupo Interno de Trabajo de Comunicaciones y la gestión de riesgos asociados al proceso, efectuó verificación de los controles implementados.

Como resultado de la verificación realizada, se identificaron oportunidades de mejora en aspectos relacionados con la formalización documental de controles, procedimientos y lineamientos internos, los cuales constituyen elementos fundamentales para garantizar la adecuada gestión de los riesgos asociados al proceso.

Entre las principales situaciones observadas se encuentran:

- Acuerdos de confidencialidad pendientes de formalización para algunos integrantes del proceso.
- Ausencia de lineamientos documentados para la gestión integral de información reservada y confidencial.
- Falta de procedimientos formalizados para la atención de incidentes relacionados con pérdida, hurto o daño de equipos.
- Debilidades en la trazabilidad y control de activos asignados al proceso derivadas de la ausencia de inventarios periódicos, registros consolidados de salidas y retornos.
- Debilidades en la formalización del proceso de entrega y recibo de la coordinación del GIT
- Falta de documentación de controles relacionados con dispositivos de almacenamiento externo y respaldos de información.
- Inexistencia de procedimientos formalizados para la gestión de material audiovisual sensible y la administración de redes sociales institucionales
- Limitada articulación entre los controles definidos en el mapa de riesgos y las evidencias que permitan verificar su ejecución y efectividad.

Los resultados obtenidos permiten concluir que el proceso cuenta con controles operativos básicos que apoyan el desarrollo de sus actividades; sin embargo, requiere fortalecer la formalización, documentación y evidencia de operación de dichos controles para incrementar su efectividad, asegurar la adecuada gestión de los riesgos identificados y fortalecer el Sistema de Control Interno.

6. PRINCIPALES SITUACIONES DETECTADAS / RESULTADOS

En desarrollo de la presente verificación, la Oficina de Control Interno, con el fin de evaluar la gestión del proceso de comunicaciones, llevó a cabo la verificación de los siguientes aspectos, a partir de la revisión y análisis de la información y evidencias suministradas por el proceso:

Tabla 1.

Aspectos evaluados en la verificación

No	Componente de control	Requerimientos evaluados	Aspectos clave evaluados
1	Gestión de la información reservada y confidencial	1, 2, 3, 4, 5, 28, 29, 30, 36, 37, 38, 39, 40, 41 y 42	Acuerdos de confidencialidad, protocolos de información, clasificación, criticidad, conflictos de interés, datos personales
2	Seguridad de la información digital	8, 11, 17, 31, 32, 33, 34 y 35	Backups, repositorio institucional, metadatos, transferencia de archivos, integridad de publicaciones, configuraciones de seguridad
3	Custodia y administración de equipos	6, 7, 9, 10, 12, 13, 14, 15 y 16	Inventario, control de salida/retorno, pólizas, pérdida de equipos, viáticos, empalme de coordinación
4	Redes sociales institucionales	19, 20, 21, 22, 23, 24 y 25	Políticas de uso de las Redes Sociales, gestión de accesos, flujo de publicación, monitoreo, gestión de crisis, directrices del Ministerio de Transporte y la Presidencia de la República
5	Gestión de riesgos y controles	18, 26 y 27	Mapa de riesgos, estructura del GIT, roles y funciones, empalme de coordinación

Fuente: Elaboración propia OCI

A continuación, se presentan los resultados de la verificación, organizados en cinco componentes de control.

6.1 GESTIÓN DE LA INFORMACIÓN RESERVADA Y CONFIDENCIAL

Para este componente se analizaron los mecanismos implementados para garantizar la confidencialidad, reserva y adecuado tratamiento de la información; los lineamientos, políticas o protocolos para la clasificación, manejo, almacenamiento, transferencia y eliminación segura de información confidencial; los controles para prevenir pérdida, fuga o uso indebido; los acuerdos de confidencialidad del personal; el procedimiento para el manejo de información confidencial; las capacitaciones en seguridad de la información; los controles sobre eventos y cubrimientos institucionales; las restricciones sobre dispositivos personales; los niveles de criticidad de la información; la clasificación del personal con acceso a información sensible; los mecanismos para gestión de conflictos de interés; los protocolos para

información del Despacho del Superintendente; los controles para prevenir filtraciones; los mecanismos de trazabilidad sobre acceso y difusión de información; y las publicaciones en redes sociales que involucran datos personales.

Producto del análisis de la información presentada por el proceso se encontró:

Acuerdos de confidencialidad:

La dependencia informa que cuenta con un Acuerdo de Confidencialidad suscrito por la totalidad de los integrantes del Grupo de Comunicaciones, constituyéndose en un mecanismo formal orientado a promover la reserva y el adecuado manejo de la información institucional.

La respuesta evidencia únicamente un control de carácter documental y de compromiso individual, sin aportar información sobre otros mecanismos administrativos, operativos o tecnológicos implementados para garantizar la confidencialidad, integridad y adecuado tratamiento de la información gestionada por el proceso.

En particular, no se identifican controles relacionados con la gestión de accesos, segregación de funciones, trazabilidad de actividades, clasificación de la información, almacenamiento seguro, protección de datos personales, monitoreo de cumplimiento o atención de incidentes de seguridad de la información.

Por lo anterior, la información suministrada permite evidenciar la existencia de un mecanismo de control, pero no resulta suficiente para demostrar de manera integral el esquema de protección de la información implementado por el proceso de Comunicaciones.

Así mismo, se identificó que se tienen Acuerdos de Confidencialidad suscritos por nueve (9) de los diez (10) integrantes del GIT. No obstante, las firmas se realizaron entre el 16 y el 21 de abril de 2026. Es decir, durante el periodo evaluado (enero-marzo de 2026) nueve (9) de los diez (10) integrantes del GIT carecían de acuerdo de confidencialidad suscrito, por lo que dicho control no se encontraba operando en ese periodo. La Coordinadora del área, a la fecha de este informe, no registra suscripción del acuerdo, como se consolidó en la siguiente tabla:

Tabla 2. Acuerdos de confidencialidad

ACUERDOS DE CONFIDENCIALIDAD				
No.	Nombre	Sí	No	Fecha suscripción
1	Jeisson Diaz Duarte	X		16/04/2026
2	Ledys María Rodríguez Sanchez	X		16/04/2026
3	Diana Lorena Jiménez Martínez	X		16/04/2026

4	Maria Camila Reyes Hernandez	X		16/04/2026
5	Mariana Velasquez Salazar		X	sin firma
6	Edith Natalia Araque Bermúdez	X		16/04/2026
7	Valentina Sandoval Castañeda	X		16/04/2026
8	Wilmer Fabian Arenas Robayo	X		21/04/2026
9	Wilson Armando Mueses Cuaran	X		16/04/2026
10	Andrea del Pilar Mancera Rojas	No registra con acuerdo de confidencialidad		

Fuente: Elaboración propia

Se recomienda gestionar la suscripción y formalización inmediata de los acuerdos de confidencialidad pendientes, incluyendo el de la Coordinadora del grupo, y establecer un control periódico que asegure su actualización y cumplimiento para todo el personal vinculado al proceso

Lineamientos y protocolos de gestión de la información:

A la fecha de la verificación, el proceso no cuenta con lineamientos, políticas ni procedimientos documentados y formalmente aprobados para la clasificación, manejo, almacenamiento, transferencia, respaldo y eliminación segura de información confidencial o reservada. El proceso manifestó que tiene previsto adelantar, en coordinación con la Oficina Asesora de Planeación, la construcción de los documentos correspondientes

Lo anterior representa una debilidad en el diseño y formalización de controles relacionados con la gestión de la información, generando riesgos asociados al acceso no autorizado, pérdida, alteración, divulgación indebida o disposición inadecuada de información que pueda tener carácter reservado o confidencial.

Se recomienda priorizar la elaboración, aprobación, divulgación e implementación de los lineamientos correspondientes, así como definir responsables, mecanismos de seguimiento y controles que permitan garantizar su aplicación efectiva.

Controles para prevenir pérdida o fuga de información:

El proceso informa la implementación de controles orientados a prevenir la pérdida, fuga o uso indebido de la información, entre los cuales se encuentran el uso exclusivo de canales institucionales autorizados, la asignación de responsables para la administración de redes sociales y plataformas colaborativas, la utilización del correo electrónico institucional, el almacenamiento centralizado en la nube corporativa y las restricciones de acceso al personal del área.

Asimismo, se señala que el proceso se encuentra respaldado por los controles tecnológicos, de seguridad perimetral y monitoreo administrados por la OTIC, lo cual

contribuye a mitigar riesgos asociados al acceso no autorizado y a la fuga de información.

No obstante, la respuesta no permite evidenciar de manera suficiente la formalización de dichos controles ni su aplicación efectiva, toda vez que no se aportan procedimientos, lineamientos, registros o soportes que permitan verificar su implementación. De igual manera, no se identifican controles específicos relacionados con el uso de dispositivos personales, aspecto requerido expresamente en la solicitud de información.

Adicionalmente, no se observa información relacionada con mecanismos de trazabilidad, monitoreo periódico de accesos, gestión de privilegios, control de transferencia de archivos o procedimientos para la detección y atención de incidentes asociados a la pérdida o fuga de información.

Por lo anterior, si bien se evidencian controles básicos de carácter administrativo y tecnológico, se recomienda fortalecer su documentación, formalización y evidencia de operación, con el fin de demostrar su efectividad dentro del Sistema de Control Interno.

Procedimiento para manejo de información confidencial:

El proceso informa que, a la fecha de la evaluación, no dispone de un procedimiento documentado para la consulta, manejo y control de la información confidencial o reservada dentro del proceso de Comunicaciones. Asimismo, manifiesta que se adelantará la construcción de dicho documento en coordinación con la Oficina Asesora de Planeación y que la ruta institucional para su consulta será definida una vez este sea aprobado y socializado.

La respuesta evidencia que actualmente no existen lineamientos formalizados que regulen de manera específica las actividades relacionadas con el acceso, consulta, manejo, custodia y control de la información que pueda tener carácter confidencial o reservado dentro del proceso.

Adicionalmente, no se aportan soportes documentales ni se identifica una ruta institucional vigente para la consulta de procedimientos asociados a esta materia, por lo que no es posible verificar la existencia de controles formalmente establecidos ni la adopción de criterios uniformes para la gestión de este tipo de información.

La ausencia de procedimientos documentados incrementa el riesgo de interpretaciones discrecionales, accesos no autorizados, divulgación indebida de información, deficiencias en la trazabilidad de las actuaciones y dificultades para la rendición de cuentas frente al tratamiento de información sensible.

Se recomienda priorizar la elaboración, aprobación, divulgación e implementación del procedimiento correspondiente, definiendo claramente responsables, niveles de

acceso, mecanismos de autorización, controles de trazabilidad, criterios de conservación y disposición final de la información, así como los mecanismos de seguimiento para verificar su cumplimiento.

Capacitación en seguridad de la información:

Frente al requerimiento relacionado con la capacitación del personal del Grupo de Comunicaciones en seguridad de la información, manejo de información reservada y protección de datos, el proceso informó que actualmente se encuentra en fase de detección de necesidades de capacitación y que tiene proyectado solicitar espacios de sensibilización en dichas materias.

La información suministrada no permitió evidenciar la realización de capacitaciones específicas durante la presente vigencia, ni se aportaron soportes documentales que acrediten procesos de formación relacionados con seguridad de la información, protección de datos personales o manejo de información reservada.

En consecuencia, se considera que el requerimiento no fue atendido de manera suficiente, evidenciándose oportunidades de mejora orientadas al fortalecimiento de competencias y cultura de seguridad de la información dentro del proceso, con el fin de mitigar riesgos asociados al manejo inadecuado de activos de información institucional.

Controles en eventos y cubrimientos institucionales:

Los controles para evitar la captura o difusión no autorizada de información sensible durante eventos se basan exclusivamente en el deber de reserva y la ética profesional de los integrantes. No existe un manual documental específico sobre esta materia.

La información suministrada no permitió evidenciar controles formalmente documentados de carácter técnico, operativo o administrativo orientados a prevenir la divulgación no autorizada de información sensible, tales como restricciones de acceso, lineamientos de custodia, mecanismos de autorización, controles de almacenamiento o protocolos específicos para cubrimientos institucionales.

Así mismo, el proceso indicó que no dispone de un manual documental específico sobre esta materia.

En consecuencia, se evidencia oportunidades de mejora relacionadas con la formalización e implementación de controles preventivos que mitiguen riesgos asociados a fuga de información, uso indebido de contenidos institucionales y afectaciones reputacionales.

Restricciones sobre dispositivos personales:

Frente al requerimiento relacionado con la existencia de restricciones o lineamientos para el uso de dispositivos personales en el desarrollo de actividades del proceso, el

Grupo de Comunicaciones informó que actualmente reconoce la necesidad de estandarizar el uso de dispositivos externos y que las actuaciones del personal se rigen principalmente por los compromisos de reserva y confidencialidad suscritos por cada integrante del equipo.

La información aportada no permitió evidenciar la existencia de políticas, lineamientos o procedimientos formalmente documentados relacionados con el uso de celulares personales, memorias USB, nubes personales o correos no institucionales para el manejo de información institucional o confidencial.

Así mismo, no se identificaron controles técnicos, mecanismos de restricción, monitoreo o supervisión específicos orientados a prevenir el uso indebido, almacenamiento no autorizado o transferencia inadecuada de información institucional.

En consecuencia, se evidencia oportunidad de mejora de fortalecimiento en materia de seguridad de la información y formalización de controles aplicables al uso de dispositivos y medios personales dentro del proceso.

Niveles de criticidad y clasificación de la información:

Frente al requerimiento relacionado con la definición de los niveles de criticidad de la información manejada por el proceso y cómo estos inciden en los controles aplicados, el Grupo de Comunicaciones informó que no se han definido formalmente niveles de criticidad para la información que administra, por lo que no se encuentra documentada la relación entre dicha clasificación y los controles aplicados para su protección y gestión.

El proceso indica que en el documento de “*Manejo de medios de comunicación*”, se está elaborando un espacio especial para definir los niveles de dificultad de los temas que conciernen a la Superintendencia de Transporte, documento dirigido a los directivos con el fin de prepararlos para eventuales vocerías.

La respuesta evidencia que el proceso no cuenta actualmente con una metodología formal para la clasificación de la información según niveles de criticidad. Aunque se adelanta una iniciativa relacionada con la categorización de temas para fines comunicacionales, esta no constituye una clasificación integral de la información institucional ni permite identificar claramente cómo la criticidad de la información determina la aplicación de controles específicos de acceso, tratamiento, almacenamiento, protección o divulgación.

En consecuencia, no es posible evidenciar la relación entre los niveles de criticidad de la información y los controles implementados, debido a que dichos niveles aún no han sido definidos formalmente.

Frente al requerimiento relacionado con la clasificación formal del personal del Grupo de Comunicaciones como usuario con acceso a información sensible o estratégica, y los controles diferenciales aplicados frente a otros procesos.

La respuesta permite evidenciar que no existe una clasificación formal de usuarios basada en el nivel de acceso a información sensible o estratégica. Si bien se reconoce la naturaleza de las funciones desempeñadas por el Grupo de Comunicaciones y la responsabilidad asociada al manejo de información institucional, esta condición no se encuentra respaldada por lineamientos, procedimientos o actos administrativos que establezcan perfiles de acceso diferenciados.

De igual manera, aunque los acuerdos de confidencialidad constituyen un mecanismo de control relevante, estos corresponden a controles generales aplicables al personal y no evidencian necesariamente la existencia de controles diferenciales específicos para quienes gestionan información estratégica. No se identifican medidas complementarias relacionadas con segregación de funciones, perfiles de acceso especiales, restricciones tecnológicas, trazabilidad, autorizaciones especiales o monitoreo reforzado sobre la información administrada por el proceso.

Por lo anterior, no se logra demostrar que existan controles diferenciados formalmente definidos y aplicados en función del acceso a información sensible o estratégica.

Se recomienda definir y documentar los niveles de criticidad de la información que administra, estableciendo los controles de acceso, manejo, conservación y divulgación aplicables a cada nivel. Asimismo, formalizar la asignación de perfiles de acceso para los servidores y contratistas que gestionan información sensible o estratégica, de manera que se implementen controles diferenciados acordes con sus responsabilidades y el riesgo asociado a la información administrada.

Gestión de conflictos de interés e información privilegiada:

Se analizó la información remitida sobre los mecanismos para la gestión de conflictos de interés y el uso indebido de información privilegiada, evidenciándose que el proceso señala como principal control los acuerdos de confidencialidad suscritos por el personal. Adicionalmente, se informó que se encuentra en elaboración un documento con restricciones sobre el manejo de la información y el uso de equipos; sin embargo, no se aportaron soportes que permitan evidenciar su existencia, avance o proceso de elaboración. Asimismo, se reconoció la identificación de posibles riesgos asociados al uso de redes y equipos en beneficio de terceros. En este contexto, la falta de documentación que respalde los controles informados limita la verificación de su implementación y debilita la gestión preventiva frente a conflictos de interés y al uso indebido de información privilegiada.

Protocolo para información del Despacho del Superintendente:

Se evidenció que la Entidad no cuenta con protocolos formalmente establecidos para el manejo de la información proveniente del Despacho del Superintendente. Si bien existen prácticas operativas que restringen inicialmente el acceso a determinada información a través del Coordinador de Comunicaciones, no se encuentran documentados los niveles de acceso, responsabilidades de custodia, criterios de clasificación, canales autorizados de difusión ni procedimientos para la gestión de incidentes asociados a posibles fugas de información.

Esta situación limita la capacidad institucional para garantizar un tratamiento uniforme, controlado y basado en riesgos de la información estratégica generada desde el Despacho, constituyendo una oportunidad de fortalecimiento de los controles de seguridad de la información y gobierno de datos.

Trazabilidad y control sobre filtraciones:

Frente al requerimiento relacionado con los controles establecidos para evitar filtraciones de información estratégica o confidencial hacia medios de comunicación, terceros o redes sociales antes de su divulgación oficial, Se evidenció que el principal control implementado para prevenir la filtración de información estratégica o confidencial corresponde a la suscripción de acuerdos de confidencialidad por parte del personal del Grupo de Comunicaciones. No Se observaron controles adicionales formalmente definidos relacionados con la clasificación de la información, restricciones de acceso, monitoreo, trazabilidad, autorizaciones de divulgación o gestión de incidentes de seguridad de la información. Esta situación podría limitar la efectividad de los mecanismos de prevención frente a riesgos de divulgación no autorizada de información institucional, constituyendo una oportunidad de fortalecimiento del sistema de control interno y de seguridad de la información.

Frente al requerimiento relacionado con la existencia de controles de trazabilidad sobre quién accede, edita o difunde información sensible dentro del proceso, y qué herramientas se utilizan para ello, el proceso manifestó que la información es gestionada por la Coordinación, el encargado de redes sociales y los diseñadores, quienes participan en su transformación, revisión, aprobación y difusión. Sin embargo, no se evidencia la existencia de controles formalizados que permitan garantizar la trazabilidad completa sobre quién accede, modifica, aprueba o difunde la información sensible durante cada etapa del proceso.

Adicionalmente, la respuesta señala que actualmente se realiza un seguimiento de las actividades de los integrantes del grupo, pero que este no se encuentra totalmente organizado ni documentado, y que se encuentra pendiente la elaboración de un documento para formalizar dichos controles.

Por lo anterior, se identifica una oportunidad de mejora relacionada con el diseño, documentación e implementación de mecanismos de trazabilidad que permitan registrar y consultar de manera oportuna las acciones realizadas sobre la información, así como las herramientas utilizadas para tal fin, fortaleciendo los principios de responsabilidad, seguimiento y control dentro del proceso.

Publicaciones con datos personales en redes sociales:

Frente al requerimiento relacionado con la publicación de información personal de servidores públicos o terceros en las redes sociales institucionales, el Grupo de Comunicaciones informó situaciones asociadas a la vinculación de cuentas personales con redes sociales institucionales durante la administración del anterior coordinador, así como la utilización de un avatar personal en la cuenta institucional de Instagram y la asociación del algoritmo de dicha red social con contenidos ajenos al sector transporte.

Adicionalmente, el proceso manifestó tener conocimiento de actuaciones adelantadas por Control Interno Disciplinario relacionadas con estos hechos.

La respuesta suministrada no permitió identificar de manera específica si durante el periodo evaluado se realizaron publicaciones que contuvieran datos personales de servidores públicos o terceros, ni se precisó el tipo de información divulgada, los mecanismos de autorización y validación aplicados, el cumplimiento de las disposiciones en materia de protección de datos personales, la existencia de reclamaciones por parte de titulares de la información o las acciones correctivas implementadas por el proceso.

Lo anterior, refleja debilidad en los controles relacionados con la administración de redes sociales institucionales, la protección de datos personales y la trazabilidad de las publicaciones efectuadas en los canales oficiales de la Entidad. Estas condiciones incrementan el riesgo de incumplimiento de las disposiciones normativas en materia de protección de datos, uso inadecuado de activos digitales institucionales, pérdida de control sobre la información divulgada y posibles afectaciones a la imagen y reputación institucional, por lo que se requiere fortalecer los mecanismos de control, monitoreo y supervisión asociados a estos procesos.

6.2 SEGURIDAD DE LA INFORMACIÓN DIGITAL

Para este componente se revisaron las configuraciones o medidas de seguridad implementadas en los equipos del proceso (bloqueo, cifrado, controles de acceso); los controles para el uso de dispositivos de almacenamiento externo; los procedimientos de respaldo de información (backups); los controles para la transferencia de archivos a terceros; el procedimiento para la gestión de material audiovisual sensible o no publicado; los controles para la revisión y depuración de

metadatos en archivos; el repositorio institucional centralizado y sus controles de acceso; y los mecanismos para garantizar la integridad de la información publicada.

Producto del análisis de la información presentada por el proceso se encontró:

Configuraciones de seguridad en equipos:

El proceso informó que los equipos asignados al proceso de Comunicaciones operan bajo las configuraciones de seguridad estandarizadas y administradas por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), incluyendo controles de acceso mediante credenciales institucionales, bloqueo automático por inactividad y protocolos de seguridad de red.

Lo anterior, permite evidenciar la existencia de controles básicos de seguridad lógica implementados de manera centralizada por la Entidad, lo que contribuye a reducir riesgos asociados al acceso no autorizado y al uso indebido de los recursos tecnológicos.

No obstante, la información suministrada es de carácter general y no permite determinar con precisión el alcance de las medidas de protección implementadas sobre los equipos utilizados por el proceso. En particular, no se identifican controles relacionados con cifrado de información, protección de dispositivos de almacenamiento removibles, herramientas de seguridad de endpoint, autenticación reforzada o mecanismos específicos para la protección de la información contenida en los equipos.

Adicionalmente, no se aportan soportes o evidencias que permitan validar las configuraciones de seguridad reportadas ni verificar su aplicación efectiva sobre los equipos asignados al proceso.

Dispositivos de almacenamiento externo:

Se evidenció que el Grupo de Comunicaciones no dispone de controles específicos formalmente documentados para la gestión y uso de dispositivos de almacenamiento externo, tales como memorias USB, discos duros externos o tarjetas SD utilizados en el desarrollo de sus actividades, ni cuenta con una política interna específica.

Durante la verificación se informó que el proceso aplica de manera general las políticas y lineamientos institucionales relacionados con el uso de herramientas tecnológicas y la seguridad de la información. Sin embargo, no se aportó evidencia de procedimientos, controles o mecanismos específicos orientados a la administración, custodia, autorización, protección, transferencia o eliminación de información contenida en medios de almacenamiento externos utilizados para la producción y gestión de material audiovisual.

La ausencia de controles específicos sobre estos dispositivos incrementa el riesgo de pérdida, alteración, fuga de información, propagación de software malicioso y uso no autorizado de contenidos institucionales, especialmente considerando el volumen de material audiovisual que administra el proceso.

En consecuencia, se recomienda documentar e implementar controles específicos para el uso de dispositivos de almacenamiento externo, incluyendo criterios de autorización, responsables de custodia, mecanismos de protección de la información, escaneo de seguridad, control de transferencias, respaldo de contenidos y disposición final de los medios, en concordancia con las políticas institucionales de seguridad de la información.

Respaldo de información (backups):

Se evidenció que el Grupo de Comunicaciones realiza el almacenamiento de la información institucional a través de las herramientas tecnológicas administradas por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), la cual tiene a su cargo la gestión de los mecanismos de respaldo, almacenamiento y control de acceso sobre los repositorios institucionales.

Durante la revisión se observó que la respuesta no permite identificar de manera precisa los procedimientos establecidos para el respaldo de la información asociada al proceso, ni suministra información específica sobre la periodicidad de las copias de seguridad, los responsables de su ejecución, la ubicación de almacenamiento de los respaldos, las personas autorizadas para acceder a ellos y la ruta o medio institucional dispuesto para su consulta.

Asimismo, no se aportaron documentos, procedimientos, instructivos o evidencias que permitieran verificar la aplicación de los controles de respaldo sobre la información generada por el proceso, incluyendo archivos audiovisuales, equipos de cómputo, dispositivos móviles y demás activos tecnológicos utilizados en el desarrollo de sus actividades.

La ausencia de información detallada y de soportes verificables limita la evaluación de la suficiencia de los controles implementados para garantizar la disponibilidad, integridad y recuperación de la información administrada por el proceso.

Transferencia de archivos a terceros:

El proceso informó que el intercambio de información y material audiovisual se realiza mediante herramientas corporativas institucionales como OneDrive y SharePoint, las cuales permiten gestionar permisos de acceso y niveles de edición. Así mismo, el proceso indicó que la transferencia de archivos se realiza bajo supervisión de la coordinación y que la trazabilidad de versiones se mantiene dentro de los repositorios oficiales de la Entidad.

La información suministrada no permitió evidenciar la existencia de procedimientos formalmente documentados relacionados con mecanismos de autorización, cifrado, monitoreo o control específico de transferencias de información hacia terceros. De igual forma, el proceso manifestó no contar con un manual independiente de cifrado aplicable a este tipo de intercambio de archivos.

En consecuencia, se evidenciaron oportunidades de mejora relacionadas con la formalización de controles de seguridad de la información, mecanismos de protección de archivos y lineamientos aplicables a la transferencia de información institucional a terceros.

Gestión de material audiovisual sensible:

No se dispone de un procedimiento documentado para la gestión del material audiovisual sensible o no publicado que establezca tiempos de conservación, criterios de acceso y disposición final. El proceso aplica criterios de reserva profesional, pero sin respaldo procedimental formal.

El proceso informó que actualmente aplica criterios de confidencialidad y reserva profesional en el manejo de este tipo de información, así como las directrices generales de la Política de Seguridad y Privacidad de la Información de la Entidad. Adicionalmente, indicó que se encuentra identificada como acción de mejora la creación de un inventario de activos de información audiovisual orientado a fortalecer la trazabilidad y control del contenido no publicado.

No obstante, la información suministrada no permitió evidenciar un procedimiento formalmente documentado que establezca tiempos de conservación, criterios de acceso, responsables de custodia, mecanismos de autorización, ni lineamientos específicos relacionados con la disposición final del material audiovisual sensible o no publicado.

En consecuencia, se evidenciaron oportunidades de mejora en la formalización y documentación de controles asociados al manejo, conservación y protección del material audiovisual institucional.

Depuración de metadatos en archivos:

El proceso informó que actualmente realiza validaciones técnicas sobre el material audiovisual y documental antes de su divulgación, aplicando criterios orientados a minimizar la exposición de información sensible no deseada durante los procesos de edición y exportación de archivos. Así mismo, manifestó que se encuentra proyectando la adopción de directrices específicas para la limpieza de metadatos en archivos destinados a ciudadanía y medios externos.

No obstante, la información suministrada no permitió evidenciar la existencia de herramientas automatizadas, protocolos formalmente documentados o controles específicos para la revisión y depuración de metadatos en archivos institucionales.

Adicionalmente, aunque se indicó la designación de un funcionario encargado de la organización y preservación de esta documentación, se informó que a la fecha no se ha presentado informe relacionado con dicha gestión.

En consecuencia, se evidenciaron oportunidades de fortalecimiento relacionadas con la formalización de controles preventivos orientados a mitigar riesgos asociados a la divulgación involuntaria de información sensible contenida en metadatos de archivos institucionales.

Repositorio institucional centralizado:

El proceso utiliza OneDrive como repositorio institucional en la nube para el material audiovisual y las comunicaciones oficiales, con controles de acceso basados en el principio de necesidad de saber. Esta es una fortaleza del proceso; sin embargo, se identifican oportunidades de mejora en la documentación formal de los procedimientos de administración y respaldo.

El proceso informó que la custodia de dicha información se realiza a través de un repositorio institucional en la nube (OneDrive) e indicó que los controles de acceso se gestionan bajo el principio de "*necesidad de saber*", limitando los permisos de consulta y edición únicamente al personal autorizado del proceso de Comunicaciones. Adicionalmente, señaló que la herramienta permite mantener trazabilidad sobre archivos, versiones y modificaciones, contando además con mecanismos de respaldo y seguridad soportados por las políticas institucionales de tecnologías de la información.

En consecuencia, se considera que el requerimiento fue atendido de manera general, evidenciándose la existencia de controles básicos asociados al almacenamiento, acceso y respaldo de la información institucional administrada por el Grupo de Comunicaciones.

Se identifican oportunidades de mejora relacionadas con la formalización documental de los procedimientos de administración del repositorio, definición de responsables, clasificación de accesos y lineamientos específicos sobre respaldo y recuperación de información.

Integridad de la información publicada:

El proceso distribuye comunicados en PDF a periodistas mediante un canal de WhatsApp y publica contenidos en la página web institucional. Ante publicaciones erróneas, se gestiona la corrección directa con el medio (fe de erratas). No se

identificaron controles documentados de control de versiones, trazabilidad de cambios ni mecanismos formales de monitoreo posterior a la publicación.

El proceso informó sobre los canales utilizados para la divulgación de contenidos institucionales, tales como el envío de comunicados y material fotográfico a periodistas mediante un canal de WhatsApp y la publicación de información en la sección de noticias de la página web institucional.

No obstante, la respuesta suministrada no permitió evidenciar controles específicos orientados a garantizar la integridad de la información publicada, tales como mecanismos de control de versiones, restricciones de edición, registros de modificaciones, controles de acceso, trazabilidad de cambios o procedimientos para la corrección y actualización de contenidos y prevenir alteraciones no autorizadas de la información institucional una vez publicada.

Se identifican oportunidades de mejora relacionadas con la formalización y documentación de controles que permitan garantizar la integridad, autenticidad y trazabilidad de la información divulgada a través de los diferentes canales institucionales.

6.3 CUSTODIA Y ADMINISTRACIÓN DE EQUIPOS

Para este componente se revisaron los mecanismos de custodia, control y aseguramiento de los equipos asignados al proceso (cámaras, micrófonos, drones, celulares, trípodes, memorias, entre otros), el lugar de resguardo dentro de las instalaciones y las condiciones de custodia fuera de la Entidad; la relación de bienes asignados con los soportes de asignación y responsabilidad; los inventarios periódicos y actas de verificación; el procedimiento de control de salida y retorno de activos; el procedimiento ante pérdida, hurto o daño de equipos; las pólizas de seguro de los equipos asignados; la relación de eventos del primer trimestre de 2026 con uso de equipos fuera de la Entidad; los soportes de registro de salida y reingreso; y los soportes de viáticos y comisiones con su legalización.

Producto del análisis de la información presentada por el proceso se encontró:

Custodia y ubicación de los equipos:

El Grupo de Comunicaciones indicó que los equipos del proceso (cámaras, micrófonos, drones, trípodes, memorias y demás elementos audiovisuales, entre otros) reposan en los escritorios de los funcionarios del GIT y para garantizar su control, se ha implementado un mecanismo de registro obligatorio ante el personal de seguridad y recepción en cada salida y retorno de los bienes, sin embargo, no se aportó evidencia verificable de dicho mecanismo.

Durante la verificación se observó que los mecanismos de custodia y control no se encuentran formalmente documentados en un procedimiento que establezca de

manera específica las responsabilidades sobre los equipos, las condiciones de almacenamiento dentro de las instalaciones, los criterios para su asignación temporal, así como los controles aplicables cuando los bienes son utilizados fuera de la Entidad

Igualmente, se identificó oportunidad de mejora en la consolidación y actualización permanente del inventario de equipos del proceso, incluyendo registros de asignación, responsables, ubicación, novedades y trazabilidad de los activos durante las actividades institucionales externas.

En consecuencia, la Oficina de Control Interno recomienda formalizar e implementar procedimientos y registros que permitan fortalecer la custodia, control y seguimiento de los equipos audiovisuales, definiendo responsables, condiciones de resguardo, mecanismos de verificación periódica y controles para los traslados y uso de los bienes fuera de las instalaciones de la Superintendencia de Transporte.

Inventario y actas de asignación:

Como resultado del cruce de información efectuado entre el inventario institucional y el inventario suministrado por el Grupo de Comunicaciones mediante el archivo (Inv Comunicaciones.xlsx), se evidenció concordancia entre los bienes reportados por el proceso y los registrados en la base oficial de inventarios de la Entidad. En total, se identificaron (24) bienes, entre los cuales se encuentran; cámaras fotográficas, cámara de video, lente de cámara, trípodes, micrófonos, mini dron, computadores, CPU, teléfonos, memorias y backing institucional.

En la revisión del inventario aportado por el proceso, se observó el reporte de ocho (8) bienes en condición de faltantes, los cuales se relaciona a continuación:

Tabla 3. Elementos reportados como faltantes

PLACA	FECHA DE ADQUISICION	DESCRIPCION NORMALIZADA	DESCRIPCION DETALLADA	ESTADO DE SERVICIO
8707	9/10/2018	TELEFONO	GSM SAMSUNG J4 DS LTE	FALTANTE
9185	30/09/2022	MICROFONO	INALAMBRICO DIGITAL	FALTANTE
9186	30/09/2022	VIDEO CAMARA	VIDEO CAMARA	FALTANTE
9188	30/09/2022	BACKING	AJUSTABLE CON IMPRESIÓN EN BANNER 13 OZ 300X200CM	FALTANTE
9359	24/10/2023	COMPUTADOR	PORTATIL	FALTANTE
9562	14/11/2024	TELEFONO	CELULAR	FALTANTE
9576	14/11/2024	MEMORIA	TARJETA SD	FALTANTE
9577	14/11/2024	MEMORIA	TARJETA SD	FALTANTE

Fuente: Inventario suministrado por el proceso en correo electrónico del 22 de abril de 2026, repositorio "Inv Comunicaciones.xlsx"

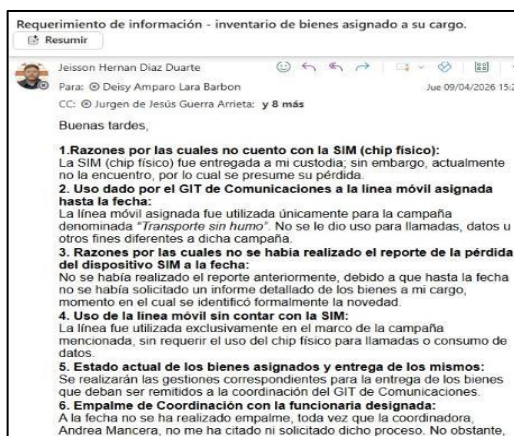
La anterior, situación requiere validación y seguimiento por parte de las dependencias responsables de la administración de bienes, con el fin de verificar las actuaciones adelantadas para su regularización y determinar la posible existencia de riesgos asociados a pérdida de activos institucionales. Así mismo, este aspecto será objeto de revisión por parte de la Oficina de Control Interno en el marco del "*Seguimiento a la administración de bienes de la Superintendencia*"

La permanencia de los ocho (8) bienes públicos en condición de faltante sin que se evidencie gestión administrativa oportuna ni verificación de las pólizas de seguro correspondientes puede generar posible riesgo de connotación fiscal: de no adelantarse las actuaciones administrativas pertinentes, dichos bienes podrían terminar en una baja por pérdida no recuperada, con la consecuente afectación del patrimonio público. En virtud de su rol de aseguramiento, la Oficina de Control Interno se abstiene de cuantificar o gestionar directamente dicha exposición patrimonial, y remite el asunto a las dependencias responsables de la administración de bienes para su regularización, sin perjuicio de que este aspecto será objeto de verificación en el marco del "Seguimiento a la administración de bienes de la Superintendencia".

Por otra parte, se evidenció que no se cuenta con las actas de entrega y responsabilidad debidamente actualizadas a nombre de la Coordinadora entrante, debido a la falta de formalización del proceso de empalme. Al respecto, se identificaron comunicaciones electrónicas en las cuales el coordinador saliente expone las situaciones relacionadas con los bienes a su cargo, así como un requerimiento de la Coordinadora entrante solicitando la realización del empalme y la entrega formal de los elementos, con el fin de garantizar su adecuado uso y control.

Imagen 1.

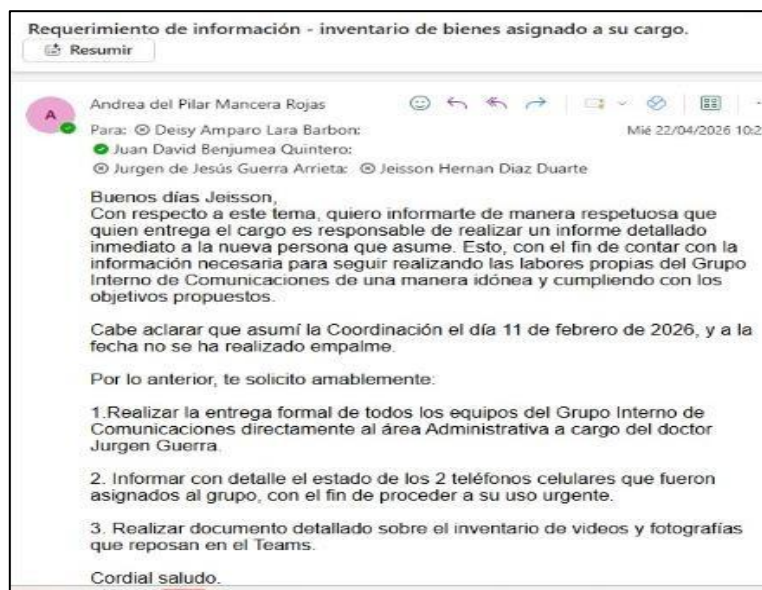
Situación relacionada con los bienes.



Fuente: datos suministrados en correo electrónico del 22 de abril de 2026, punto 7

Imagen 2.

Solicitud de empalme y entrega formal de elementos.



Fuente: datos suministrados en correo electrónico del 22 de abril de 2026, punto 7

La ausencia de inventarios periódicos limita la capacidad de asegurar la existencia, ubicación, estado y trazabilidad de los equipos asignados al proceso, incrementando el riesgo de pérdida, deterioro, uso inadecuado o inconsistencias en el control de los activos.

En consecuencia, la Oficina de Control Interno recomienda implementar y formalizar un procedimiento de inventario periódico para los equipos del Grupo de Comunicaciones, definiendo periodicidad, responsables, mecanismos de verificación y documentación de resultados mediante actas o reportes de control, con el fin de fortalecer la gestión y salvaguarda de los bienes asignados al proceso.

Control de salida y retorno de activos:

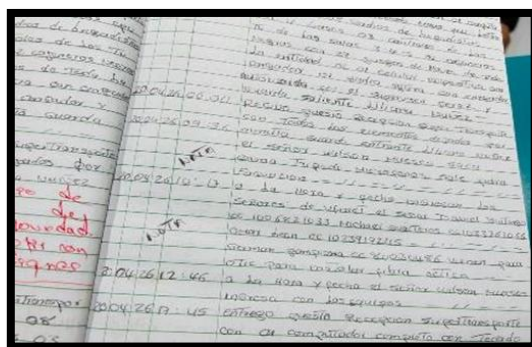
Se evidenció que el control de salida y retorno de los equipos asignados al Grupo de Comunicaciones se realiza mediante el mecanismo de registro administrado por el personal de seguridad y recepción de la Entidad, quienes verifican la salida y el posterior ingreso de los bienes cuando son utilizados fuera de las instalaciones, sin que exista un procedimiento documentado que establezca las actividades, responsables y registros complementarios.

No se presentó la relación de los eventos realizados durante el primer trimestre de 2026 en los cuales se utilizaron equipos institucionales fuera de las instalaciones de la Entidad, ni aportó información relacionada con el tipo de equipo utilizado, fecha de uso, evento desarrollado y responsable a cargo de los bienes el listado consolidado de eventos del primer trimestre de 2026 en los que se utilizaron equipos fuera de la Entidad, ni los soportes de registro de salida y reingreso del período evaluado.

Las imágenes de bitácora aportadas corresponden al 20 de abril de 2026, fecha posterior al período evaluado, como se aprecia en las siguientes imágenes:

Imagen 3.

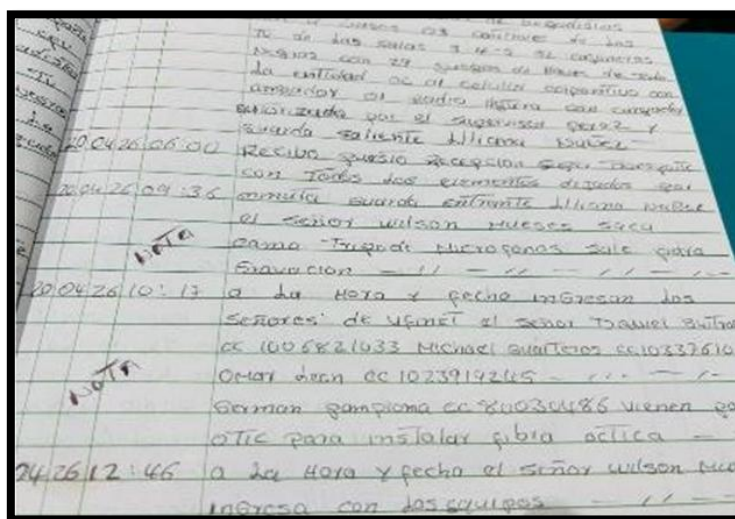
Registro en bitácora 1.



Fuente: Información enviada por correo electrónico el 22 de abril de 2026

Imagen 4.

Registro en bitácora 2



Fuente: Información enviada por correo electrónico el 22 de abril de 2026

Durante la revisión se observó que la dependencia no aportó evidencia de un procedimiento formalmente documentado que establezca las actividades, responsables, registros, puntos de control y lineamientos para la autorización, seguimiento y devolución de los equipos. Asimismo, no se identificó la ruta institucional o documento oficial mediante el cual pueda consultarse dicho procedimiento.

La ausencia de lineamientos documentados y de registros complementarios específicos para el proceso limita la trazabilidad de los activos, dificulta el seguimiento de las responsabilidades asociadas a su uso y aumenta el riesgo de pérdida, uso no autorizado o inconsistencias en el control de los bienes institucionales.

En consecuencia, la Oficina de Control Interno recomienda formalizar y documentar el procedimiento para el control de salida y retorno de los equipos asignados al Grupo de Comunicaciones, definiendo responsables, mecanismos de autorización, registros de préstamo, evidencias de entrega y devolución, así como la ruta institucional para su consulta, con el fin de fortalecer el sistema de control interno y la gestión de los activos del proceso.

Procedimiento ante pérdida, hurto o daño:

El proceso indicó que se acoge a los lineamientos institucionales establecidos por la Entidad para la gestión y reporte de novedades relacionadas con bienes institucionales, incluyendo situaciones de pérdida, hurto o daño de los equipos asignados al proceso.

No obstante, no aportó evidencia de un procedimiento específico o documento que describa de manera detallada las actividades a desarrollar ante la ocurrencia de estos eventos, incluyendo responsables, tiempos de reporte, instancias de notificación, mecanismos de seguimiento y acciones de mitigación para reducir el impacto operativo y administrativo derivado de la afectación de los activos.

Se verificó en los correos aportados que el chip SIM de un celular institucional fue reportado como presuntamente extraviado, situación que no había sido formalmente comunicada con anterioridad

La pérdida reconocida de la SIM institucional y su reporte tardío trascienden la debilidad de custodia y configuran un riesgo de connotación fiscal: de haber permanecido activa y facturando la línea con posterioridad a la pérdida, o de haber sido utilizada por un tercero, los consumos y cargos no institucionales generados durante dicho lapso podrían constituir un pago de lo no debido y un eventual detrimento patrimonial. En consecuencia, sin que la Oficina de Control Interno ejecute directamente esta actuación, se recomienda a la dependencia competente cuantificar la facturación de la línea desde la fecha presunta de pérdida y verificar si se dispuso

oportunamente la suspensión del servicio, con el fin de dimensionar el eventual detrimento y adelantar las acciones de recobro a que haya lugar.

Asimismo, se identificó que la respuesta hace referencia a la futura elaboración de una guía interna; sin embargo, dicha herramienta aún no se encuentra implementada ni formalizada, por lo que no constituye un control vigente para el periodo objeto de evaluación.

La ausencia de lineamientos específicos documentados puede generar incertidumbre frente a la actuación oportuna de los responsables, afectar la trazabilidad de los eventos y aumentar el riesgo de pérdida de información, interrupción de actividades o debilidades en la gestión de los bienes institucionales.

En consecuencia, la Oficina de Control Interno recomienda documentar y divulgar un procedimiento o instructivo que establezca claramente las acciones a seguir en caso de pérdida, hurto o daño de los equipos asignados al proceso, definiendo responsables, tiempos máximos de reporte, canales de comunicación, acciones de mitigación y mecanismos de seguimiento, en concordancia con las disposiciones institucionales aplicables.

Pólizas de seguro:

El proceso no aportó las pólizas de seguro correspondientes a los equipos asignados al proceso ni suministró información relacionada con su cobertura, amparos, vigencia o condiciones de aseguramiento, tal como fue solicitado en el requerimiento.

La respuesta presentada se limitó a indicar que, según información suministrada por el anterior coordinador, la documentación relacionada con las pólizas se encuentra bajo custodia de la Dirección Administrativa, por ser la dependencia encargada de la adquisición y administración de los bienes institucionales. No se adjuntó evidencia documental ni se realizaron las gestiones necesarias para obtener y remitir la información requerida.

La ausencia de información y soportes impidió a la Oficina de Control Interno verificar la existencia, vigencia y suficiencia de los mecanismos de aseguramiento aplicables a los equipos asignados al proceso, así como validar los riesgos cubiertos y las condiciones de protección patrimonial de dichos activos.

Viáticos y comisiones:

Se revisó la información remitida por proceso correspondiente a los soportes de viáticos y comisiones del personal, incluyendo evidencias de aprobación y ejecución. Se evidenció la relación de comisiones para los meses de enero, febrero y marzo de 2026, junto con sus respectivos soportes documentales, tales como tiquetes y resoluciones. Para el mes de enero, se observó que la comisión fue prorrogada mediante la Resolución 995 para su ejecución en febrero. Asimismo, se verificó un

tiquete correspondiente a comisión en las ciudades de Nariño, Cauca y Valle del Cauca, con fechas entre el 23 y 25 de febrero de 2026, tal como se observa en las siguientes tablas

Tabla 4.

Viáticos y comisiones enero 2026

Comisiones realizadas en el mes de enero 2026			
Resolución	Mes	Funcionarios	Ciudad
912	Enero	Jeisson Hernán Diaz Duarte	Buenaventura
913		Ana Isabel Jiménez castro	
914		Dina Rafaela Sierra Rochels	
915		Alfredo Enrique Piñeres Olave	

Fuente: Elaboración propia conforme a datos suministrados en correo electrónico del 22 de abril de 2026, COMISIONES

Tabla 5.

Viáticos y comisiones febrero 2026

Comisiones realizadas en el mes de febrero de 2026			
Resol / Prorroga	Mes	Funcionarios	Ciudad
995 / 912	Enero / Febrero	Jeisson Hernán Diaz Duarte	Buenaventura
Operativo integral de presencia territorial (Nariño – Cauca – Valle del Cauca) Superintendencia Delegada de Concesiones e Infraestructura (SDCI) Del 23 al 25 de febrero de 2026			

Fuente: Elaboración propia conforme a datos suministrados en correo electrónico del 22 de abril de 2026, COMISIONES

Imagen 5: Tiquete (Nariño – Cauca – Valle del Cauca)

E-Ticket
[paginaEticketHeader]

Logo: **SuperTransporte** LDC Internet: **ACN2PVJ** Fecha Emisión: 17:55 17/02/2026 Agencia: **SUPERINTENDENCIA DE TRANSPORTE**

Vuelos
Fecha Emisión: **17:55 17/02/2026** Cia: Avianca - Localizador: AJPWVB
Emisor: YENNY SOLANO DUMAR GDS: Amadeus - Localizador: AJPWVB

Pasajeros

Nombre	Trayecto	Aerolínea	Viajero frecuente	E-Ticket
JEISSON HERNAN DIAZ DUARTE	BOG-PPN/CLO-BOG	Avianca		134-5527641711

Itinerario

Salida	Llegada	Duración	Aerolínea	Vuelo	Clase	Asientos	Equipaje
Bogota (BOG) 23/02/2026 - 07:05 El Dorado	Popayan (PPN) 23/02/2026 - 07:05 Guillermo León Valencia	—	Avianca	2906	Standard economy / (P) CLASSIC	11	1
Cali (CLO) 25/02/2026 - 21:00 Alfonso B. Aragón	Bogota (BOG) 25/02/2026 - 22:00 El Dorado	—	Avianca	9236	Standard economy / (T) CLASSIC	11	1

Tarifas

Pasajeros	Tipo	Aerolínea	Pago	Moneda	Tarifa	Fee	Tasa	Total
JEISSON HERNAN DIAZ DUARTE	ADT	Avianca	Cash	COP	806,803.00	89,643.00	182,070.00	1,078,516.00
Total General				COP	806,803.00	89,643.00	182,070.00	1,078,516.00

Reglas de la tarifa
[Reglas tarifarias](#)

Centro de costo

Código	Descripción	Porcentaje
1	FUNCIONAMIENTO	100

Información General
Presentarse con la debida anticipación en el aeropuerto

Fuente: Elaboración propia conforme a datos suministrados en correo electrónico del 22 de abril de 2026, *COMISIONES*

Tabla 6. Viáticos y comisiones Marzo 2026

Comisiones realizadas en el mes de febrero de 2026			
CDP	Mes	Funcionario	Ciudad
9526	Marzo	Jeisson Hernán Díaz Duarte	Buenaventura
77226	Abril	Wilson Armando Mueses Cuaran	Medellín

Fuente: Elaboración propia conforme a datos suministrados en correo electrónico del 22 de abril de 2026, *COMISIONES*

En la información suministrada, no se identificaron las legalizaciones correspondientes a las comisiones del período evaluado. Esta situación constituye una condición susceptible de generar riesgo fiscal, dado que se trata de viáticos desembolsados cuya ejecución y justificación documental no quedó acreditada mediante la legalización. La ausencia de legalización podría generar pagos de lo no debido si la comisión no se ejecutó o no se encuentra debidamente justificada; los valores no legalizados son susceptibles de recuperación conforme al régimen aplicable. Se recomienda a la dependencia competente requerir la legalización de las comisiones pendientes o, de no acreditarse su procedencia, adelantar las actuaciones de recobro que correspondan, conforme al Decreto 1083 de 2015 y a los procedimientos internos de tesorería.

6.4 REDES SOCIALES INSTITUCIONALES

Para este componente se analizaron los incidentes de seguridad de la información o relacionados con redes sociales durante el período evaluado; las políticas, lineamientos, protocolos o procedimientos formales para la gestión de redes sociales institucionales; los controles para la administración, custodia y control de accesos a las cuentas institucionales (incluyendo autenticación multifactor, gestión de usuarios y contraseñas, y control de accesos de contratistas); el flujo de validación, aprobación y publicación de información en redes sociales; el monitoreo de redes sociales; el protocolo para la gestión de crisis en redes sociales y comunicaciones oficiales; y las directrices vigentes del Ministerio de Transporte y la Presidencia de la República en materia de comunicaciones oficiales.

Producto del análisis de la información presentada por el proceso se encontró:

Incidentes de seguridad en redes sociales:

El proceso informó que durante el periodo evaluado no se presentaron incidentes de seguridad de la información relacionados con las redes sociales institucionales, tales como accesos no autorizados, hackeos, publicaciones no autorizadas, pérdida de acceso o intentos de suplantación. Sin embargo, no se aportaron registros o reportes que permitan validar esta afirmación, ni se identificó un procedimiento específico documentado para la gestión, recuperación y continuidad operativa ante incidentes en redes sociales institucionales

Si bien el proceso indicó que, ante una eventual contingencia, se aplicarían los protocolos institucionales administrados por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), no se suministró la ruta documental, procedimiento o lineamiento que permita identificar las actividades, responsables, tiempos de respuesta y mecanismos de recuperación aplicables a este tipo de incidentes.

La ausencia de procedimientos específicos para la gestión de incidentes asociados a redes sociales puede afectar la capacidad de respuesta oportuna ante eventos que comprometan la disponibilidad, integridad o reputación institucional de los canales digitales administrados por el proceso.

Políticas y procedimientos para redes sociales:

El proceso informó que se encuentra adelantando actividades de actualización y fortalecimiento de sus protocolos de interacción digital, así como la elaboración de un manual orientado a regular aspectos relacionados con la administración de accesos, gestión de crisis, monitoreo de contenidos y demás actividades asociadas a la operación de los canales institucionales en redes sociales. No obstante, dicho documento aún no ha sido formalizado, aprobado ni incorporado al Sistema de Gestión de Calidad.

Asimismo, no se aportó documentación vigente que permitiera verificar lineamientos específicos relacionados con la administración de usuarios y accesos, mecanismos de autenticación, procedimientos de publicación de contenidos, monitoreo de cuentas, interacción con la ciudadanía, gestión de incidentes o crisis reputacionales y trazabilidad de las actuaciones realizadas en las plataformas digitales institucionales.

La ausencia de lineamientos formalmente documentados y aprobados incrementa el riesgo de inconsistencias operativas, debilidades en la asignación de responsabilidades, dificultades en la gestión de incidentes y limitaciones para garantizar la trazabilidad y control de las actuaciones realizadas en las redes sociales institucionales.

Control de accesos a cuentas institucionales:

El proceso indicó que la administración de las credenciales de las redes sociales institucionales se encuentra centralizada en el Grupo de Comunicaciones y que el acceso a las cuentas es restringido a personal previamente autorizado por la coordinación del área. Asimismo, se informó que la asignación y revocatoria de accesos se realiza bajo supervisión directa de la coordinación y que, en el caso de contratistas, existen obligaciones de confidencialidad y mecanismos de supervisión a cargo del respectivo supervisor contractual.

Se observó que la información suministrada no permite verificar la existencia de procedimientos formalmente documentados que regulen la gestión integral de accesos a las redes sociales institucionales. En particular, no se aportó evidencia relacionada con mecanismos de autenticación multifactor, políticas de administración y cambio de contraseñas, registros de asignación y revocatoria de usuarios, controles de segregación de funciones, bitácoras de acceso, revisiones periódicas de privilegios o procedimientos específicos para la desvinculación de usuarios con acceso a las cuentas institucionales.

Asimismo, no se suministraron soportes que permitieran verificar los mecanismos de monitoreo y seguimiento aplicados sobre los accesos otorgados a contratistas o terceros, ni la forma en que se controla la trazabilidad de las actuaciones realizadas por estos usuarios dentro de las plataformas administradas por el proceso.

La ausencia de lineamientos documentados y de evidencias verificables limita la capacidad de garantizar la adecuada administración de accesos privilegiados y aumenta el riesgo de uso indebido, pérdida de control sobre las cuentas institucionales o afectación de la seguridad de la información.

Flujo de validación y publicación de contenidos:

El proceso suministró una descripción general de las actividades desarrolladas para la gestión de contenidos institucionales, indicando etapas asociadas a la recepción de

solicitudes, análisis de oportunidad, elaboración de mensajes, diseño de piezas y aprobación previa a la publicación.

La información aportada no permitió evidenciar de manera integral un procedimiento formalmente documentado que establezca los responsables en cada etapa, los mecanismos de trazabilidad para la edición, corrección o eliminación de publicaciones, así como la ruta o medio oficial para su consulta.

Monitoreo de redes sociales:

El proceso informó que actualmente se encuentra adelantando actividades de fortalecimiento y estandarización asociadas a la interacción y respuesta en redes sociales, indicando además que se trabaja en la definición de un manual de estilo y lineamientos de interacción ciudadana.

No se identificaron herramientas formalizadas de monitoreo, responsables designados, lineamientos de interacción con la ciudadanía, tiempos y tono de respuesta definidos, ni articulación documentada con el proceso de PQRS.

Protocolo de gestión de crisis:

El proceso informó que la gestión de crisis está reglamentada bajo el código GCI-FR-008; sin embargo, dicho documento no fue identificado en la cadena de valor de la Entidad.

Al revisar en el aplicativo DARUMA, se identificaron dos documentos asociados (manual y protocolo) no aportados ni mencionados por el proceso, registrados en el Sistema de Gestión de Calidad bajo los códigos:

GCM-PT-001 Protocolo de Crisis para Manejo con los Medios de Comunicación y Ante la Opinión Pública V1

GCM-MA-003 Gestión de la Comunicación en Situaciones de Crisis V4

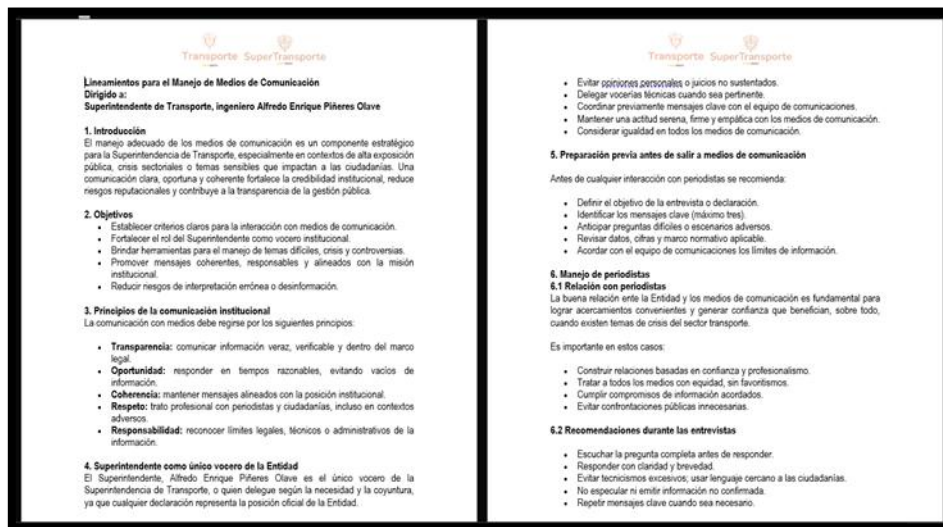
El proceso no aportó evidencia del comité de crisis, ni de las rutas establecidas para el manejo de crisis en La Superintendencia y en medios digitales.

En los soportes aportados por el proceso se observó el documento denominado "*Lineamientos para el Manejo de Medios de Comunicación*", Con los objetivos:

- *Establecer criterios claros para la interacción con medios de comunicación.*
- *Fortalecer el rol del Superintendente como vocero institucional.*
- *Brindar herramientas para el manejo de temas difíciles, crisis y controversias.*
- *Promover mensajes coherentes, responsables y alineados con la misión institucional.*
- *Reducir riesgos de interpretación errónea o desinformación.*

Imagen 6.

Manejo de medios de comunicación.



Fuente: Imagen suministrada según datos suministrados en correo electrónico del 22 de abril de 2026, CRISIS - Manejo de medios de comunicación.docx

El anterior documento está dirigido al Superintendente en versión borrador, dado que no cuenta con radicado ni está formalmente aprobado e integrado al sistema de gestión de la entidad.

Se recomienda revisar, actualizar y formalizar la documentación relacionada con la gestión de crisis institucionales, asegurando que los procedimientos, protocolos, manuales y demás documentos aplicables se encuentren debidamente identificados, alineados, vigentes y publicados en el Sistema de Gestión de Calidad. Asimismo, documentar y socializar las rutas de actuación, los responsables, los mecanismos de escalamiento y la conformación del comité de crisis, conservando las evidencias de su implementación y funcionamiento, con el fin de garantizar una respuesta oportuna, coordinada y verificable ante situaciones que puedan afectar la imagen, reputación o gestión institucional.

Directrices del Ministerio de Transporte y la Presidencia:

El proceso informó que adopta y aplica las directrices del Ministerio de Transporte y la Consejería Presidencial de Comunicaciones en materia de identidad visual, uso de marca y mensajes institucionales. No obstante, no se allegaron las directrices vigentes como documentos formales ni se documentaron los mecanismos internos de verificación de su cumplimiento.

Por lo anterior, la Oficina de Control Interno recomienda mantener un repositorio actualizado de las directrices emitidas por las entidades rectoras en materia de

comunicaciones institucionales, así como documentar los mecanismos de seguimiento y control implementados para asegurar su aplicación uniforme en todos los canales oficiales de comunicación.

Vinculación de cuentas institucionales con perfiles personales:

De acuerdo con la información reportada por el proceso se evidenció que las redes sociales institucionales de la Superintendencia de Transporte estuvieron vinculadas a cuentas personales del anterior coordinador. En particular, la cuenta institucional de Instagram institucional tenía configurada como imagen de perfil un avatar personal, y el algoritmo de la plataforma se encontraba asociado a temáticas ajenas al sector transporte. El proceso informó la existencia de un proceso de Control Interno Disciplinario frente al anterior coordinador por estos hechos.

La situación descrita evidencia debilidades en la administración y control de los activos digitales institucionales, particularmente en la gestión de accesos, perfiles y configuraciones de las redes sociales oficiales, lo que podría generar riesgos reputacionales, afectación de la imagen institucional, uso inadecuado de canales oficiales y pérdida de control sobre la información y contenidos divulgados a través de estos medios.

6.5 GESTIÓN DE RIESGOS Y CONTROLES

Para este componente se revisaron el mapa de riesgos del proceso de Gestión de Comunicaciones y los soportes que evidencian la implementación y ejecución de los controles definidos para su mitigación, seguimiento y evaluación; los responsables de la administración del proceso y de las redes sociales institucionales, la estructura y conformación del Grupo de Comunicaciones, la segregación de funciones, los roles, niveles de autoridad y líneas de reporte; y el procedimiento de entrega y recibo de funciones en la Coordinación del GIT, incluyendo la resolución de designación de la actual coordinadora, el informe de entrega de funciones y los soportes del proceso de empalme.

Producto del análisis de la información presentada por el proceso se encontró:

Mapa de riesgos del proceso:

El proceso aportó el Mapa de Riesgos de Gestión de Comunicaciones con las respectivas evidencias de ejecución correspondientes al primer trimestre 2026. Dicho mapa contempla dos (2) riesgos de gestión y un (1) riesgo de integridad pública.

En el marco de la verificación realizada, se evaluó la alineación de los riesgos identificados con el objetivo del proceso y las funciones asignadas al Grupo de Comunicaciones, establecidas en la Resolución 8564 de 2021 *"Por la cual se expide la Resolución Única de Grupos Internos de Trabajo de la Superintendencia de Transporte"* modificada por la Resolución 2065 de 2022 del 29 de junio de 2022.

Artículo 2.15.4. Así como la pertinencia de los controles establecidos para su tratamiento.

Alineación de los riesgos identificados con los objetivos del proceso y las funciones del grupo:

El análisis evidenció que los tres riesgos identificados por el proceso guardan relación con actividades fundamentales asociadas a la gestión de la información institucional, la administración de los canales de comunicación y la protección de la información sensible.

Los riesgos de gestión relacionados con la divulgación de comunicados con inconsistencias y la publicación de información desactualizada en redes sociales presentan una alineación directa con el objetivo del proceso, orientado a divulgar la gestión institucional y fortalecer el posicionamiento de la Entidad ante sus grupos de interés. Por su parte, el riesgo de integridad pública asociado al fraude interno y al uso indebido de información privilegiada se relaciona con la protección de la información institucional y la integridad de la gestión comunicacional.

No obstante, se observó que la cobertura del mapa de riesgos resulta limitada frente al alcance integral de las funciones asignadas al Grupo de Comunicaciones. Si bien los riesgos identificados abordan aspectos relacionados con la divulgación de información y la administración de redes sociales, no se evidenciaron riesgos asociados a la gestión de crisis comunicacionales, eventos institucionales, administración de la imagen corporativa, gestión contractual en materia de comunicaciones, preservación de archivos multimedia y relacionamiento con medios.

En consecuencia, se considera que los riesgos identificados cubren parcialmente las responsabilidades del proceso, existiendo oportunidades de fortalecimiento que permitan ampliar la identificación de eventos que puedan afectar el cumplimiento de los objetivos institucionales y las funciones asignadas al Grupo de Comunicaciones.

Pertinencia de controles:

Riesgos de Gestión:

GC-01G Posibilidad de pérdida Reputacional por afectación de la imagen de la Entidad al socializar comunicados con inconsistencias debido manejo inadecuado de la información no oficial o reservada. Tiene definidos tres (3) Controles asociados a:

- Revisión de los formatos de solicitud de comunicados, campañas digitales y transmisiones por parte del Profesional Especializado de Comunicaciones.
- Validación y aprobación de los comunicados por parte del Superintendente de Transporte antes de su publicación.

- Verificación de la inclusión de documentos de apoyo tipo "ABC" cuando la información tenga componentes técnicos.

Los controles guardan relación con el riesgo identificado, toda vez que establecen mecanismos de revisión, validación y aprobación previos a la divulgación de la información institucional. En particular, la revisión de los formatos permite verificar la integridad y claridad de la información suministrada por las dependencias, mientras que la aprobación por parte del Superintendente constituye una instancia adicional de control antes de la publicación.

Se observa que los controles están orientados principalmente a verificar la calidad, completitud y autorización de la información, pero no abordan de manera específica la causa asociada al manejo de información no oficial o reservada. En este sentido, no se evidencian actividades de validación de clasificación de la información, restricciones de acceso, verificación de fuentes oficiales o mecanismos para asegurar que la información divulgada no corresponda a contenidos reservados o confidenciales.

Adicionalmente, el control N°3. relacionado con la elaboración de documentos tipo "ABC" tiene un enfoque pedagógico y de apoyo a la comprensión de la información técnica, por lo que su contribución a la mitigación del riesgo resulta indirecta.

En consecuencia, los controles para el riesgo GC-01G son parcialmente pertinentes, ya que contribuyen a reducir errores e inconsistencias en las comunicaciones; sin embargo, no mitigan de manera integral la causa principal asociada al uso o divulgación de información no oficial o reservada.

GC-02G Posibilidad de pérdida Reputacional por mantener datos desactualizados de la Entidad en las redes sociales verificadas (X, Facebook, Instagram y Tiktok) debido la falta de coordinación entre el equipo de comunicaciones y demás áreas para la publicación de información relevante de la Entidad. Tiene definido un (1) control, asociado a:

- Revisión mensual del estado de campañas y comunicados publicados en redes sociales mediante el archivo "Campañas Vigentes", determinando cuáles deben mantenerse, actualizarse o retirarse.

El control presenta una relación directa con el riesgo identificado, dado que está diseñado específicamente para verificar la vigencia y actualización de los contenidos publicados en redes sociales institucionales.

La actividad incorpora una periodicidad definida (mensual), un responsable identificado y una acción correctiva cuando se detecta información desactualizada, consistente en coordinar con las áreas responsables la actualización de los contenidos.

Sin embargo, el riesgo tiene como causa la falta de coordinación entre el equipo de comunicaciones y las demás dependencias para el suministro de información relevante. Aunque el control contempla la coordinación posterior a la identificación de contenidos desactualizados, no incorpora mecanismos preventivos que aseguren la comunicación oportuna de cambios por parte de las áreas generadoras de la información.

En consecuencia, el control es pertinente y coherente con el riesgo, dado que permite identificar y corregir información desactualizada. No obstante, podría fortalecerse mediante mecanismos formales de reporte periódico por parte de las dependencias responsables de la información institucional.

Riesgo de integridad pública:

GC-01C Posibilidad de afectación económica y reputacional por Fraude Interno y soborno entrante en el aseguramiento de la información sensible que debe suministrarse a terceros o publicar en medios, a causa de una indebida gestión de la información a la cual tiene acceso de forma privilegiada el Grupo Interno de Trabajo de Comunicaciones para beneficio particular o de un tercero. Tiene definido un (1) control asociado a:

- Suscripción de acuerdos de confidencialidad por parte de funcionarios y contratistas del equipo de comunicaciones.

El control guarda relación con el riesgo al establecer compromisos formales de confidencialidad para las personas que tienen acceso a información sensible. La suscripción de dichos acuerdos contribuye a generar responsabilidad individual respecto al tratamiento de la información institucional.

Sin embargo, el control tiene un carácter principalmente declarativo y administrativo, por lo que su capacidad para prevenir o detectar actos de fraude, soborno o uso indebido de información privilegiada resulta limitada. El acuerdo de confidencialidad no incorpora mecanismos de monitoreo, seguimiento o detección de accesos indebidos, filtraciones de información o conflictos de interés.

Adicionalmente, durante la verificación se observó que algunos acuerdos fueron suscritos de manera extemporánea respecto al período evaluado y que uno de ellos carecía de firma, situación que disminuye la efectividad del control.

En consecuencia, el control es pertinente, pero insuficiente para administrar integralmente el riesgo, dado que se limita a formalizar obligaciones de confidencialidad sin incluir controles preventivos o detectivos asociados a la gestión de información privilegiada. Su efectividad se ve además afectada por debilidades en su ejecución y oportunidad.

Finalmente, producto del análisis se observa que los controles definidos presentan relación con los riesgos identificados y, en términos generales, contribuyen a su mitigación. No obstante, se evidencia que algunos controles se enfocan en actividades de revisión documental o formalización de responsabilidades, sin abordar de manera integral las causas que originan los riesgos. Particularmente, se identifican oportunidades de mejora en materia de gestión de información reservada, coordinación interdependencias y protección de información privilegiada, mediante la incorporación de controles preventivos y detectivos que permitan incrementar la efectividad del tratamiento del riesgo.

Estructura organizacional y roles del GIT:

El proceso describió de forma general la estructura jerárquica del GIT, indicando que la toma de decisiones recae en funcionarios de planta y que el componente operativo de redes sociales es desarrollado por un contratista que desempeña el rol de administrador y productor de contenidos desde febrero de 2026, reportando directamente a la coordinación del grupo. Así mismo, indicó que las responsabilidades y niveles de autoridad se distribuyen conforme al objeto contractual de cada integrante, manteniendo diferenciación funcional para actividades relacionadas con gestión de crisis, interacción ciudadana y administración de credenciales de acceso.

La información aportada no permitió evidenciar de manera integral la estructura y conformación formal del Grupo de Comunicaciones, la segregación específica de funciones, la identificación detallada de roles y responsabilidades del personal de planta y contratistas, ni los mecanismos documentados que soporten los niveles de autoridad y líneas de reporte.

En consecuencia, se identifican oportunidades de fortalecimiento relacionadas con la formalización y documentación de la estructura funcional, roles y responsabilidades asociados a la gestión de comunicaciones y administración de redes sociales institucionales.

Proceso de empalme de la Coordinación:

El proceso informó que el empalme estaba programado para el 11 de febrero de 2026 con el inicio de funciones de la actual coordinadora. A la fecha de la verificación, el anterior coordinador no ha presentado el informe de entrega correspondiente, pese a los múltiples requerimientos realizados por la Secretaría General, la Dirección Administrativa y por la actual coordinadora desde febrero hasta abril de 2026.

Se verificaron los correos aportados, que evidencian:

- La Dirección Administrativa solicitó desde el 11 de febrero de 2026 la devolución de la línea celular Movistar No. 3174029245 junto con el equipo telefónico correspondiente.

Imagen 7.

Correos

De: Administrativa <administrativa@supertransporte.gov.co>
Enviado: miércoles, 11 de febrero de 2026 14:31
Para: Jeisson Hernan Diaz Duarte <jeissondiaz@supertransporte.gov.co>; Comunicaciones Supertransporte <comunicaciones@supertransporte.gov.co>
Cc: Jorgen de Jesús Guerra Arrieta <jurgenguerra@supertransporte.gov.co>; Yenny Sofia Solano Dumar <yennysolano@supertransporte.gov.co>; Harold Stevens Garcia Leon <HaroldGarcia@supertransporte.gov.co>; Fernando Rincon Rincon <fernandorincon@supertransporte.gov.co>
Asunto: Devolución línea de celular

Cordial saludo,

Respetados,

Previa instrucción comunicada por la Dirección Administrativa, amablemente se solicita la pronta devolución de la línea telefónica Movistar No. 3174029245, junto con su correspondiente teléfono celular.

Agradecemos su atención, atentos a su pronta respuesta.

Cordialmente,



Superintendencia de Transporte
 Dirección Administrativa
administrativa@supertransporte.gov.co
 Tel: 601 3526700
 Dg 25g # 95 A 85, Torre 3 Piso 1 y 4
www.supertransporte.gov.co

De: Fernando Rincon Rincon <fernandorincon@supertransporte.gov.co>
Enviado: miércoles, 25 de febrero de 2026 15:39
Para: Administrativa <administrativa@supertransporte.gov.co>; Jeisson Hernan Diaz Duarte <jeissondiaz@supertransporte.gov.co>; Comunicaciones Supertransporte <comunicaciones@supertransporte.gov.co>; Andrea del Pilar Mancera Rojas <andreamancera@supertransporte.gov.co>
Cc: Jorgen de Jesús Guerra Arrieta <jurgenguerra@supertransporte.gov.co>; Yenny Sofia Solano Dumar <yennysolano@supertransporte.gov.co>; Harold Stevens Garcia Leon <HaroldGarcia@supertransporte.gov.co>
Asunto: RE: Devolución línea de celular

Cordial saludo,

Respetados compañeros,

De conformidad con la trazabilidad de este correo electrónico y mientras se adelantan las actividades de alistamiento de los bienes requeridos, amablemente solicitamos favor confirmar si la Línea Celular Movistar No. 3174029245 es objeto de uso. Lo anterior, pues dicha línea celular es objeto de pago mensual, por lo tanto, debemos proceder su cancelación según corresponda.

Agradezco su amable atención, atento a su pronta respuesta.

Cordialmente,

/outlook.cloud.microsoft/mail/sentitems/id/AAQKADczYTViYzkwLTcyNjItNDVhZS04MGE2LTZlNDUyZWNIWQZyYgAQADbllRtwTxBEhL3LjYHrb...

6, 12:03 Elementos enviados: Andrea del Pilar Mancera Rojas - Outlook



Superintendencia de Transporte
 Profesional Especializado 2028 - 12
 Grupo de Servicios Generales y Recursos Físicos

Fernando Rincón Rincón
 fernandorincon@supertransporte.gov.co
 Tel: 601 3526700 Ext: 333
 Dg 25g # 95 A 85, Torre 3 Piso 4
www.supertransporte.gov.co

Fuente. Pantallazo relación de correos suministrados en correo electrónico del 22 de abril de 2026,

- Posteriormente, el 26 de febrero de 2026, el entonces Coordinador de Comunicaciones informó que la línea ya no era objeto de uso y que podía disponerse de ella según correspondiera. Al solicitarse la devolución de la SIM Card, el funcionario manifestó que no contaba con el chip físico.

Imagen 8.

Correos Devolución línea celular

De: Fernando Rincon Rincon <fernandorincon@supertransporte.gov.co>
Enviado: miércoles, 4 de marzo de 2026 16:22
Para: Jeisson Hernan Diaz Duarte <jeissondiaz@supertransporte.gov.co>; Administrativa <administrativa@supertransporte.gov.co>; Comunicaciones Supertransporte <comunicaciones@supertransporte.gov.co>; Andrea del Pilar Mancera Rojas <andreamancera@supertransporte.gov.co>
Cc: Jorgen de Jesús Guerra Arrieta <jurgenguerra@supertransporte.gov.co>; Yenny Sofia Solano Dumar <yennysolano@supertransporte.gov.co>; Harold Stevens Garcia Leon <HaroldGarcia@supertransporte.gov.co>
Asunto: RE: Devolución línea de celular

Cordial saludo,

Respetado Jeisson,

Agradezco su respuesta. Favor agradecemos la devolución de la Sim card en cuestión.

Cordialmente,

 Superintendencia de Transporte
Profesional Especializado 2028 - 12
Grupo de Servicios Generales y Recursos Físicos

Fernando Rincón Rincón
fernandorincon@supertransporte.gov.co
Tel: 601 3526700 Ext: 333
De 25º # 95 A 85, Torre 3 Piso 4
www.supertransporte.gov.co

https://outlook.cloud.microsoft/mail/sentitems/IdAQAQDczTVYzWLTyNjIiNDVlZS04MGE2LTZlNDUyZWVlMmVhZGQAD0lRwTxBHJ3LjYt...
12/4/26, 12:03 Elementos enviados: Andrea del Pilar Mancera Rojas - Outlook

De: Jeisson Hernan Diaz Duarte <jeissondiaz@supertransporte.gov.co>
Enviado: jueves, 26 de febrero de 2026 8:14
Para: Fernando Rincon Rincon <fernandorincon@supertransporte.gov.co>; Administrativa <administrativa@supertransporte.gov.co>; Comunicaciones Supertransporte <comunicaciones@supertransporte.gov.co>; Andrea del Pilar Mancera Rojas <andreamancera@supertransporte.gov.co>
Cc: Jorgen de Jesús Guerra Arrieta <jurgenguerra@supertransporte.gov.co>; Yenny Sofia Solano Dumar <yennysolano@supertransporte.gov.co>; Harold Stevens Garcia Leon <HaroldGarcia@supertransporte.gov.co>
Asunto: RE: Devolución línea de celular

Buenos días,

En respuesta a su solicitud, confirmamos que la línea celular Movistar No. 3174029245 ya no es objeto de uso, por lo que pueden proceder a disponer de ella según corresponda.

Agradecemos su gestión y quedamos atentos a cualquier requerimiento adicional.

 Superintendencia de Transporte
Coordinador de Comunicaciones
Jeisson Hernán Díaz Duarte
jeissondiaz@supertransporte.gov.co
Tel: 601 3526700 - 3124989229
De 25º # 95 A 85, Torre 3 Piso 1 y 4
www.supertransporte.gov.co

De: Jeisson Hernan Diaz Duarte <jeissondiaz@supertransporte.gov.co>
Enviado: jueves, 9 de abril de 2026 10:35
Para: Andrea del Pilar Mancera Rojas <andreamancera@supertransporte.gov.co>; Fernando Rincon Rincon <fernandorincon@supertransporte.gov.co>; Administrativa <administrativa@supertransporte.gov.co>; Comunicaciones Supertransporte <comunicaciones@supertransporte.gov.co>
Cc: Jorgen de Jesús Guerra Arrieta <jurgenguerra@supertransporte.gov.co>; Yenny Sofia Solano Dumar <yennysolano@supertransporte.gov.co>; Harold Stevens Garcia Leon <HaroldGarcia@supertransporte.gov.co>; Deisy Amparo Lara Barbon <deisylara@supertransporte.gov.co>; Diana Lorena Jimenez Martinez <dianaljimenez@supertransporte.gov.co>; Juan David Benjumea Quintero <juanbenjumea@supertransporte.gov.co>; Talento Humano ST <talentohumano@supertransporte.gov.co>
Asunto: RE: Devolución línea de celular

Buenos días, Andrea:

Tal como mencioné en correos anteriores, actualmente no cuento con la SIM. Pueden hacer uso de la línea, pero reitero que no dispongo del chip físico.

Quedo atento a cualquier comentario.

 Superintendencia de Transporte
Coordinador de Comunicaciones
Jeisson Hernán Díaz Duarte
jeissondiaz@supertransporte.gov.co
Tel: 601 3526700 - 3124989229
De 25º # 95 A 85, Torre 3 Piso 1 y 4
www.supertransporte.gov.co

Fuente. Pantallazo relación de correos suministrados en correo electrónico del 22 de abril de 2026,

Imagen 10.

Correo Requerimiento información – Inventario de bienes asignados

RE: Requerimiento de información - inventario de bienes asignado a su cargo.

Desde Andrea del Pilar Mancera Rojas <andreamancera@supertransporte.gov.co>

Fecha Mié 22/04/2026 10:23

Para Deisy Amparo Lara Barbon <deisylara@supertransporte.gov.co>; Juan David Benjumea Quintero <juanbenjumea@supertransporte.gov.co>; Jorgen de Jesús Guerra Arrieta <jurgenguerra@supertransporte.gov.co>; Jeisson Hernan Diaz Duarte <jeissondiaz@supertransporte.gov.co>

- Buenos días Jeisson,
Con respecto a este tema, quiero informarte de manera respetuosa que quien entrega el cargo es responsable de realizar un informe detallado inmediato a la nueva persona que asume. Esto, con el fin de contar con la información necesaria para seguir realizando las labores propias del Grupo Interno de Comunicaciones de una manera idónea y cumpliendo con los objetivos propuestos.

Cabe aclarar que asumí la Coordinación el día 11 de febrero de 2026, y a la fecha no se ha realizado empalme.

Por lo anterior, te solicito amablemente:

1. Realizar la entrega formal de todos los equipos del Grupo Interno de Comunicaciones directamente al área Administrativa a cargo del doctor Jorgen Guerra.
2. Informar con detalle el estado de los 2 teléfonos celulares que fueron asignados al grupo, con el fin de proceder a su uso urgente.
3. Realizar documento detallado sobre el inventario de videos y fotografías que reposan en el Teams.

Cordial saludo.



Superintendencia de Transporte
Grupo de Comunicaciones
Andrea del Pilar Mancera Rojas
andreamancera@supertransporte.gov.co
Dg 25g # 95 A 85, Torre 3 Piso 1 y 4
www.supertransporte.gov.co

Fuente. Pantallazo relación de correos suministrados en correo electrónico del 22 de abril de 2026

Por último, en los soportes no se aportó la resolución de designación de la actual coordinadora ni evidencia del proceso de entrega y recepción de credenciales de los sistemas institucionales.

Lo anterior, evidencia que existieron debilidades en la administración y custodia de bienes asignados al Grupo Interno de Comunicaciones, particularmente respecto de la SIM asociada a la línea celular institucional No. 3174029245, cuya pérdida fue reconocida por el servidor responsable sin que se evidencie un reporte oportuno de la novedad. Asimismo, se observan deficiencias en el proceso de entrega y empalme entre coordinadores, situación que afectó la trazabilidad de los bienes y la disponibilidad de información necesaria para garantizar la continuidad operativa del proceso.

6.6 SEGUIMIENTO PLAN DE MEJORAMIENTO PRODUCTO DE INFORMES ANTERIORES, HALLAZGOS Y ACCIONES DE LA AUDITORÍA, EVALUACIÓN Y SEGUIMIENTO

En la verificación de la herramienta Microsoft Planner, se identificó que se tiene en seguimiento un hallazgo con una acción formulada a cargo del proceso Gestión de Comunicaciones producto de la auditoria efectuada en la vigencia 2022.

HALLAZGO H01A-06may2022-AC-GCM: En la vigencia 2021, se realizaron 11 transmisiones en vivo, los cuales fueron difundidos en la red social Facebook, así mismo con el objeto de verificar el cumplimiento al procedimiento de Transmisión por Redes Sociales Código: GCM-PR-001 Versión: 2, el cual se encuentra publicado en la intranet, cadena de valor Proceso de Gestión de comunicaciones, se realizó la verificación de las evidencias aportadas por el equipo de comunicaciones y se validó el paso a paso de las actividades descritas en dicho procedimiento, se observó que los siguientes Facebook live no cumplieron a cabalidad con las siguientes actividades: Facebook Live: Lanzamiento de la 'Cartilla y Guía de Derechos y Deberes de los Usuarios del Servicio de Transporte Acuático' incumple con la actividad 1 Validar Requisitos de Entrada: Validar la solicitud frente a la política de operación; 2 Generar Solicitud: Manifestar la necesidad al área de comunicaciones de la Superintendencia; Tema Facebook Live: Rendición de cuentas, incumple con las actividades 1. Validar Requisitos de Entrada: Validar la solicitud frente a la política de operación; 2. Generar Solicitud: Manifestar la necesidad al área de comunicaciones de la Superintendencia; Proceso Gestión de Comunicaciones. 3. Revisar Información: Validar la necesidad; Tema Facebook Live: Guía para prestar de forma práctica y segura el servicio público de transporte fluvial' incumple con las actividades 1. Validar Requisitos de Entrada: Validar la solicitud frente a la política de operación; 2 Generar Solicitud: Manifestar la necesidad al área de comunicaciones de la Superintendencia Tema Facebook Live: Lanzamiento guía transporte de mascotas incumple con la actividad No. 4 Recomendaciones y/o Fecha de Ensayo: Enviar al área solicitante recomendaciones y/o aclaraciones respecto a la solicitud presentada con el fin de fortalecer la necesidad o tener más claridad al respecto; Tema Facebook Live: Las experiencias en infraestructura de transporte accesible e incluyente, sus proyecciones en el país y como la #Supertransporte promueve el cumplimiento de la normatividad, se incumple con las actividades 1. Validar Requisitos de Entrada: Validar la solicitud frente a la política de operación; 2 Generar Solicitud: Manifestar la necesidad al área de comunicaciones de la Superintendencia; Tema Facebook Live: Lanzamiento revista puntos cardinales se incumple con las actividades Validar Requisitos de Entrada: Validar la solicitud frente a la política de operación; Generar Solicitud: Manifestar la necesidad al área de comunicaciones de la Superintendencia; Revisar Información: Validar la necesidad; Remitir Recomendaciones y/o Fecha de Ensayo: Enviar al área solicitante recomendaciones y/o aclaraciones respecto a la solicitud presentada con

el fin de fortalecer la necesidad o tener más claridad al respecto; Tema Facebook Live: a #Supertransporte junto a Confecámaras dan a conocer la Guía para Atender Visitas Administrativas que realiza el ente de control incumple con las actividades Generar Solicitud: Manifestar la necesidad al área de comunicaciones de la Superintendencia; Revisar Información: Validar la necesidad; Remitir Recomendaciones y/o Fecha de Ensayo: Enviar al área solicitante recomendaciones y/o aclaraciones respecto a la solicitud presentada con el fin de fortalecer la necesidad o tener más claridad al respecto, por otra parte se aclara que respecto a la actividad Tema Facebook Live: Lanzamiento guía Comercio Electrónico Transparente incumple con las actividades Validar Requisitos de Entrada: Validar la solicitud frente a la política de operación; Revisar Información: Validar la necesidad; Remitir Recomendaciones y/o Fecha de Ensayo: Enviar al área solicitante recomendaciones y/o aclaraciones respecto a la solicitud presentada con el fin de fortalecer la necesidad o tener más claridad al respecto; y Tema Facebook Live: Lanzamiento ABC de funciones Aerocivil y Supertransporte se incumple con las actividades Validar Requisitos de Entrada: Validar la solicitud frente a la política de operación; Generar Solicitud: Manifestar la necesidad al área de comunicaciones de la Superintendencia, no obstante se evidenció que los 11 Facebook live transmitidos en la vigencia 2021, no emitieron el informe sobre las estadísticas del impacto del evento, estructurado como punto de control actividad No. 9 "Presentar Estadísticas Resultado: Con base en las métricas anteriores, generar el informe correspondiente para la evaluación del evento. ©: Informe", contraviniendo lo establecido en el procedimiento de Transmisión por Redes Sociales Código: GCM-PR-001 Versión: 2, Lo cual, puede obedecer a la ausencia de conocimiento, apropiación y socialización del procedimiento generando posibles reprocesos o materialización de los riesgos identificados en el mapa de procesos y/o incumplimiento del objetivo del proceso de Gestión de comunicaciones.

Acción: Revisar y actualizar la caracterización del proceso, así como del procedimiento GCM-PR-001 para transmisiones en vivo, con el fin de hacerlo más claro y flexible para el equipo de comunicaciones.

Fecha fin: 08/07/2022

Estado: Vencida

Análisis OCI:

Durante la vigencia 2024, el proceso reportó la actualización de la caracterización y del procedimiento GCM-PR-001 "*Transmisión por Redes Sociales*". Para verificar la efectividad de la acción, la Oficina de Control Interno seleccionó una muestra de cinco (5) de las (23) transmisiones en vivo realizadas durante el primer semestre de 2024. Como resultado de la verificación, evidenciando que los correos asociados a las actividades 1 y 2 del procedimiento no contenían información suficiente para garantizar la trazabilidad de las actuaciones, particularmente en aspectos como fecha de solicitud y respuesta, área solicitante, asunto, destinatario y sugerencias o ajustes.

Al respecto, el GIT de Gestión de Comunicaciones manifestó que algunas transmisiones eran programadas directamente en el plan de participación de la vigencia y, por tanto, no se originaban en una solicitud. No obstante, se observó que el procedimiento no contemplaba esta situación como una excepción ni establecía el mecanismo mediante el cual debía documentarse y garantizarse la trazabilidad de estas transmisiones. En consecuencia, no se evidenció plena efectividad de la acción frente a la necesidad de fortalecer la trazabilidad de las actividades previstas en el procedimiento, por lo que se recomendó ajustar el procedimiento y los documentos y/o registros asociados, con el fin de subsanar la causa del hallazgo.

Desde ese momento y a la fecha de la presente verificación, no se observa en el aplicativo **Planner** reporte de avance ni evidencias asociadas al cumplimiento de las actividades relacionadas con el ajuste recomendado, situación que limita la trazabilidad del seguimiento efectuado por el proceso respecto de esta acción.

Así mismo, al revisar la cadena de valor institucional, se evidenció que el proceso realizó una actualización de la caracterización en la vigencia 2025, mientras que el procedimiento **GCM-PR-001** conserva la versión 004, aprobada el 22 de septiembre de 2023, tal como se observa a continuación:

Imagen 11.

Historial versiones caracterización **GCM-CA-001**

Listado Maestro de Documentos									
Documentos / Listado Maestro de Documentos									
Sandra Lucia									
Agrupar por: Todos Área publicada Proceso publicado Tipo									
GCM-CA-001									
☐	Índex	Norma	Número	Código	Versión	F. Vigencia	Estado	Marca	Fecha de eliminación
☐	92	CA	★ Sin leer	Gestión De Comunicaciones	GCM-CA-001	005	2025-11-12	Activo	
☐	92	CA	★	Gestión De Comunicaciones	GCM-CA-001	004	2023-04-18	Desactualizado	12/11/25
☐	92	CA	★	Gestión De Comunicaciones	GCM-CA-001	003	2022-06-30	Desactualizado	05/06/23
☐	91	CA	★	Gestión De Comunicaciones	GCM-CA-001	002	2021-02-22	Obsoleto	

Fuente. Pantallazo Listado Maestro de Documentos DARUMA

Imagen 12.

Historial versiones procedimiento **GCM-PR-001**

Listado Maestro de Documentos Sandra Lucia

Documentos / Listado Maestro de Documentos

Agrupar por: **Todos** Área publicada Proceso publicado Tipo

Q GCM-PR-001

☐	Índex	Norma	Número	Código	Versión	F. Vigencia	Estado	Marca	Fecha de eliminación
☐	111	PR	★ Sin leer Transmisión Por Redes Sociales	GCM-PR-001	004	2023-09-22	Activo		
☐	111	PR	★ Transmisión Por Redes Sociales	GCM-PR-001	003	2022-06-30	Desactualizado		22/09/23
☐	110	PR	★ Transmisión Por Redes Sociales	GCM-PR-001	002	2021-02-22	Obsoleto		

Fuente. Pantallazo Listado Maestro de Documentos DARUMA

De la revisión de los documentos vigentes publicados en DARUMA, se evidencia que la acción formulada fue atendida en lo relacionado con la revisión y actualización documental de la caracterización del Proceso de Gestión de Comunicaciones y del procedimiento GCM-PR-001.

El procedimiento vigente corresponde a la versión 004, aprobada el 22 de septiembre de 2023, y presenta modificaciones respecto de versiones anteriores en las actividades, controles, responsables y documentos o registros asociados. En su versión vigente establece seis actividades para la gestión de las transmisiones en vivo: enviar solicitud, validar si la información es clara, elaborar el minuto a minuto, realizar la transmisión, elaborar los trinos y descargar las métricas. Así mismo, contempla como registro de esta última actividad un documento en PDF con las cifras arrojadas por las redes sociales.

De igual manera, la caracterización del proceso incorpora las transmisiones en vivo dentro de los productos y/o salidas del proceso y contempla actividades relacionadas con el seguimiento y evaluación de las estrategias de comunicación implementadas, así como con la medición de su impacto y efectividad.

En consecuencia, se evidencia el cumplimiento de la acción en términos de su ejecución documental, toda vez que se realizó la revisión y actualización de los

instrumentos comprometidos y se observa una simplificación del flujo de actividades, con definición de responsables y registros, aspectos que guardan correspondencia con el propósito de hacer el procedimiento más claro y flexible.

Sin embargo, la efectividad de la acción no se encuentra plenamente acreditada, teniendo en cuenta que, en la verificación realizada por la OCI, no se contó con evidencia suficiente que permitiera establecer que las modificaciones introducidas al procedimiento hubieran solucionado de manera efectiva la situación identificada respecto de la trazabilidad de las actividades y la apropiación y aplicación del procedimiento por parte del equipo de comunicaciones.

En particular, si bien el procedimiento vigente contempla como actividad la descarga de las métricas de las transmisiones y define un documento en PDF como registro, la documentación revisada para este seguimiento no permite establecer de manera suficiente la aplicación consistente del procedimiento actualizado en las transmisiones posteriores, ni verificar que los registros asociados a las diferentes etapas se estén generando y conservando de manera completa y trazable.

Por lo anterior, la Oficina de Control Interno considera que la acción fue cumplida en términos documentales, pero no se encuentra plenamente demostrada su efectividad operacional frente a la causa que originó el hallazgo.

Se recomienda al proceso mantener evidencia trazable de la aplicación del procedimiento en las transmisiones realizadas, especialmente de las solicitudes, validaciones, minuto a minuto, enlaces de transmisión y métricas, con el fin de asegurar la apropiación del procedimiento y permitir verificar su efectividad.

7. CONCLUSIONES

7.1 Sobre la madurez del sistema de control interno del proceso

Al contrastar la evidencia recolectada con los niveles de madurez definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y en la dimensión de Gestión del Riesgo del Modelo Integrado de Planeación y Gestión (MIPG), el proceso se ubica en un nivel inicial/básico, en la medida en que los controles identificados operan de manera informal, dependen de la gestión individual de los responsables y carecen de documentación, formalización y evidencia sistemática de su ejecución, condiciones necesarias para alcanzar un nivel de madurez gestionado.

La mayoría de los controles evaluados en los cinco componentes no se encuentran formalizados mediante procedimientos documentados, lo que limita su verificabilidad, replicabilidad y efectividad como elementos del Sistema de Control Interno.

Adicionalmente, el cambio reciente en la coordinación del GIT, sin que se haya formalizado el proceso de empalme, podría generar una debilidad transversal que afecta la administración de activos, el control de accesos en redes sociales, la continuidad operativa y la trazabilidad de compromisos institucionales.

7.2 Sobre los riesgos identificados de mayor relevancia

Riesgo de fuga y divulgación no autorizada de información: La ausencia de lineamientos documentados, niveles de criticidad definidos y controles operativos sobre el uso de dispositivos personales, la transferencia de archivos, el manejo de material audiovisual sensible y los dispositivos de almacenamiento externo, incrementa el riesgo de acceso, pérdida, fuga o divulgación no autorizada de información reservada y confidencial gestionada por el GIT de Comunicaciones.

Riesgo sobre activos tecnológicos de alto valor: La falta de inventarios periódicos, actas de asignación actualizadas y procedimientos de custodia para equipos audiovisuales, tales como drones, cámaras y celulares, expone a la Entidad al riesgo de pérdida, deterioro, uso no autorizado y dificultades para establecer la responsabilidad y trazabilidad sobre los bienes públicos asignados al proceso.

Riesgo reputacional e institucional en redes sociales: La vinculación comprobada de cuentas institucionales con perfiles personales del anterior coordinador, la ausencia de políticas formalizadas y la falta de protocolos aprobados para la gestión de crisis constituyen factores de riesgo reputacional que deben ser atendidos de manera perentoria.

Riesgo en el proceso de empalme: La falta de formalización de la entrega de la Coordinación mantiene activos riesgos relacionados con la trazabilidad y responsabilidad sobre los bienes asignados, la gestión de accesos a sistemas y recursos institucionales, la transferencia de información y conocimiento, y la continuidad operativa del proceso.

Riesgo de integridad pública por fraude interno y uso indebido de información privilegiada: El proceso cuenta con acceso privilegiado a información sensible que debe suministrarse a terceros o publicarse en medios, dado el carácter cercano al Despacho del Superintendente del GIT de Comunicaciones. El único control definido para este riesgo —la suscripción de acuerdos de confidencialidad— tiene un carácter principalmente declarativo y administrativo, sin mecanismos preventivos o detectivos de monitoreo, seguimiento o detección de accesos indebidos, filtraciones de información o conflictos de interés. Su efectividad se ve además disminuida por debilidades en su ejecución y oportunidad, toda vez que nueve (9) de los diez (10) acuerdos fueron suscritos de manera extemporánea respecto al periodo evaluado y uno de ellos carece de firma. Lo anterior incrementa la posibilidad de afectación

económica y reputacional para la Entidad por fraude interno, soborno entrante o uso indebido de información privilegiada para beneficio particular o de un tercero.

Posible Riesgo fiscal por bienes faltantes y viáticos sin legalizar: La permanencia de ocho (8) bienes públicos asignados al proceso en condición de faltante, sin que se evidencie gestión administrativa oportuna para su regularización ni verificación de las pólizas de seguro correspondientes, así como la ausencia de legalización de las comisiones y viáticos del primer trimestre de 2026, constituyen situaciones susceptibles de generar riesgo fiscal para la Entidad. De no adelantarse oportunamente las actuaciones administrativas y de recobro que correspondan, dichas situaciones podrían derivar en una afectación del patrimonio público, sin que a la fecha se evidencien mecanismos que permitan acreditar su regularización o el inicio de las acciones pertinentes por parte de las dependencias responsables.

7.3. RECOMENDACIONES

Se sugieren las siguientes acciones al líder del proceso

Gestión de la información reservada y confidencial

- Elaborar, aprobar y publicar en el sistema de gestión institucional lineamientos y protocolos específicos para la clasificación, manejo, almacenamiento, transferencia, respaldo y eliminación segura de información confidencial o reservada del proceso, en coordinación con la OAP.
- Suscribir el Acuerdo de Confidencialidad con todos los integrantes del GIT, incluyendo a la coordinadora, al inicio de cada vinculación y con actualización anual, asegurando que las firmas queden registradas dentro del período al que corresponden.
- Definir y documentar los niveles de criticidad de la información gestionada por el proceso y los controles diferenciados aplicables a cada nivel, incorporando esta clasificación en los procedimientos institucionales.
- Establecer y formalizar controles operativos, tecnológicos y de trazabilidad que complementen los acuerdos de confidencialidad: restricciones sobre dispositivos personales, monitoreo de accesos, procedimientos de autorización para la difusión de información sensible y mecanismos de reporte de incidentes.
- Diseñar y aprobar un protocolo formal para el manejo de la información proveniente del Despacho del Superintendente, con niveles de acceso, responsabilidades, canales autorizados de difusión y procedimientos de gestión de incidentes.
- Formalizar e implementar mecanismos para la gestión de conflictos de interés y la prevención del uso indebido de información privilegiada, incluyendo lineamientos, declaraciones periódicas y actividades de sensibilización.

- Priorizar la inclusión del personal del GIT en programas de capacitación en seguridad de la información, protección de datos personales y manejo de información reservada, con los respectivos soportes documentales.
- Verificar y documentar el cumplimiento de la Ley 1581 de 2012 frente a publicaciones en redes sociales que incluyan información personal, estableciendo mecanismos de autorización y validación previa.
- Implementar controles de trazabilidad sobre quién accede, edita y difunde información sensible, apoyándose en las herramientas corporativas disponibles (SharePoint, OneDrive).

Seguridad de la información digital

- Solicitar a la OTIC la documentación técnica que acredite las configuraciones de seguridad implementadas en los equipos asignados al proceso, como soporte de control interno verificable.
- Definir y documentar controles específicos para el uso de dispositivos de almacenamiento externo, incluyendo criterios de autorización, escaneo de seguridad y protección de contenidos.
- Gestionar con la OTIC la documentación y socialización de los procedimientos de respaldo de información del proceso, incluyendo periodicidad, mecanismos de ejecución, responsables, ubicación de almacenamiento y ruta de consulta.
- Establecer un procedimiento documentado para la transferencia de archivos a terceros, con mecanismos de autorización, control de versiones y trazabilidad, haciendo uso de las funcionalidades de auditoría disponibles en SharePoint y OneDrive.
- Elaborar y aprobar un procedimiento para la gestión del material audiovisual sensible o no publicado, estableciendo tiempos de conservación, criterios de acceso, responsables de custodia y criterios de disposición final.
- Definir e implementar directrices y herramientas para la revisión y depuración de metadatos en archivos institucionales antes de su publicación o envío externo, y verificar el cumplimiento de las funciones asignadas al funcionario designado para esta labor.
- Formalizar los procedimientos de administración del repositorio institucional (OneDrive), incluyendo definición de responsables, clasificación de accesos, periodicidad del respaldo y mecanismos de recuperación ante incidentes.

Custodia y administración de equipos

- Implementar y formalizar un mecanismo de inventario periódico (mínimo trimestral) de los equipos asignados al GIT de Comunicaciones, con actas de

verificación física, designación de responsables por activo y actualización permanente del inventario.

- Gestionar con la Dirección Administrativa la actualización de las actas de entrega de equipos a nombre de la actual coordinadora y la obtención de las pólizas de seguro vigentes, manteniendo disponible la información sobre coberturas, amparos y vigencias.
- Establecer y documentar un procedimiento formal para el control de salida y retorno de equipos, con registros que incluyan fecha, responsable, activo, motivo y evidencia de devolución, articulado con el registro de vigilancia existente.
- Documentar y socializar el procedimiento para la gestión de novedades con bienes institucionales (pérdida, hurto o daño), con tiempos máximos de reporte, responsables, canales de comunicación y acciones de mitigación.
- Gestionar y reportar con la debida oportunidad la novedad relacionada con la presunta pérdida del chip SIM del celular institucional, adelantando las actuaciones administrativas correspondientes.
- Remitir los comprobantes de legalización de las comisiones del primer trimestre de 2026 que se encuentren pendientes.

Redes sociales institucionales

- Elaborar, aprobar e integrar al Sistema de Gestión de Calidad un marco documental para la gestión de redes sociales institucionales: políticas de administración de accesos, autenticación, procedimientos de publicación, monitoreo de contenidos, interacción ciudadana, gestión de crisis, protección de datos personales y trazabilidad de actuaciones.
- Implementar controles formalizados para la gestión de accesos a redes sociales: autenticación multifactor, política de gestión y cambio de contraseñas institucionales, registros de asignación y revocatoria de usuarios, y revocatoria inmediata de accesos al personal que se desvincula o traslada.
- Documentar y formalizar protocolos específicos para la atención de incidentes relacionados con redes sociales institucionales, definiendo mecanismos de reporte, escalamiento, recuperación de cuentas, continuidad operativa y comunicación de eventos, articulados con los procedimientos institucionales de gestión de incidentes de seguridad de la información.
- Documentar formalmente el flujo de validación, aprobación y publicación de contenidos en redes sociales, con responsables en cada etapa, mecanismos de trazabilidad de ediciones y correcciones, y ruta institucional de consulta.
- Formalizar los mecanismos de monitoreo de redes sociales y menciones a la Entidad, definiendo herramientas, responsables, lineamientos de interacción ciudadana y tiempos de respuesta, articulados con el proceso de PQRS.

- Revisar, actualizar y formalizar la documentación relacionada con la gestión de crisis institucionales, asegurando que los procedimientos, protocolos, manuales y demás documentos aplicables se encuentren debidamente identificados, alineados, vigentes y publicados en el Sistema de Gestión de Calidad.
- Verificar que todas las cuentas institucionales en redes sociales estén completamente dissociadas de perfiles o cuentas personales, con credenciales institucionales y bajo control exclusivo de la Entidad, y dar seguimiento a las actuaciones disciplinarias en curso.
- Mantener un repositorio actualizado de las directrices del Ministerio de Transporte y la Presidencia de la República, con los mecanismos internos de adopción y verificación de cumplimiento en los canales oficiales.

Gestión de riesgos y controles

- Realizar una revisión integral de su mapa de riesgos, tomando como referencia el objetivo del proceso y la totalidad de las funciones asignadas al Grupo de Comunicaciones en la Resolución 8564 de 2021, con el fin de identificar riesgos asociados a todas las actividades estratégicas, operativas, contractuales, documentales y de relacionamiento institucional bajo su responsabilidad
- Fortalecer los controles existentes mediante la incorporación de mecanismos preventivos, detectivos y de seguimiento que permitan gestionar de manera más efectiva las causas de los riesgos identificados, especialmente en aspectos relacionados con el manejo de información reservada, la actualización oportuna de contenidos institucionales y la protección de información privilegiada.
- Formalizar y publicar en el sistema de gestión un documento que establezca la estructura del GIT de Comunicaciones, los roles, responsabilidades, niveles de autoridad, segregación de funciones y líneas de reporte entre el personal de planta y los contratistas.
- Gestionar, con el apoyo de la Secretaría General y la Dirección Administrativa, el cierre formal del proceso de empalme de la Coordinación, con plazo perentorio para la entrega del inventario de bienes, informe de gestión, credenciales de plataformas y demás elementos bajo responsabilidad de la anterior coordinación.
- Adelantar, en coordinación con la Secretaría General, las actuaciones administrativas pertinentes frente al incumplimiento del anterior coordinador en la entrega oportuna de los bienes y el reporte de novedades sobre los mismos.
- Adoptar el acto administrativo de designación formal de la actual coordinadora con los efectos documentales requeridos y actualizar los registros de acceso y responsabilidad de los sistemas institucionales a su nombre.
- Establecer e institucionalizar un procedimiento formal para la entrega y recibo de cargos de Coordinación, que incluya inventario de bienes, accesos a

sistemas, compromisos en curso e informe de gestión, con plazos definidos y mecanismos de seguimiento institucional.

En atención a las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna, particularmente las relacionadas con la comunicación de resultados, seguimiento y monitoreo de las acciones derivadas de los trabajos de auditoría, la Oficina de Control Interno solicita al responsable del proceso formular el Plan de Mejoramiento correspondiente, en el cual se establezca, para cada recomendación contenida en el presente informe, la acción de mejora, responsable de su ejecución, fecha o plazo de cumplimiento y los soportes que permitan acreditar su implementación.

Lo anterior, con el propósito de facilitar el seguimiento a la disposición de las recomendaciones en el siguiente ciclo de verificación y determinar la efectividad de las acciones adoptadas. La Oficina de Control Interno realizará el seguimiento correspondiente de acuerdo con sus competencias y con los mecanismos institucionales establecidos para tal efecto. La verificación se realizó de conformidad con las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna y el Estatuto de Auditoría de la Entidad.


Firmado digitalmente por
Sandra Lucía López Pedreros
Fecha: 2026.08.18 09:02:39
-05'00'

Sandra Lucía López Pedreros
Jefe Oficina de Control Interno


Edy Johana Melgarejo Pinto
Profesional Especializado - OCI

Elaboró: Edy Johana Melgarejo Pinto, Profesional Especializado OCI 
Revisó: Sandra Lucía López Pedreros, Jefe Oficina de Control Interno
S:\OCI_2026\200-31 PLANES\200-31-13 PAA\PAA Verificaciones\Verificación proceso de comunicaciones