N.º 51

EMPRESA NACIONAL PROMOTORA DEL DESARROLLO TERRITORIAL S.A

ASESORÍA DE CONTROL INTERNO

SEGUIMIENTO AL CUMPLIMIENTO DE LAS POLÍTICAS DE INFORMACIÓN Y COMUNICACIÓN DE ENTERRITORIO S.A. ESTABLECIDAS EN LOS PRINCIPIOS 13, 14 Y 15 DEL COMPONENTE 4 (MODELO DE REFERECIA COSO 2013), IMPLEMENTADOS MEDIANTE LA CIRCULAR BÁSICA JURÍDICA CE 006/25 DE LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA - SEMESTRE I DE 2026

PERIODO EVALUADO:
"Semestre I de 2026"

Elaborado:
OCTUBRE DE 2026

CONTENIDO

INFORMACIÓN GENERAL: 3

DESARROLLO DEL INFORME: 3

OBJETIVO 3

ALCANCE 3

LIMITACION DEL ALCANCE 4

MARCO LEGAL 4

RESULTADOS DEL SEGUIMIENTO 5

CONCLUSIONES 7

INFORMACIÓN GENERAL:

NOMBRE DEL INFORME:	*SEGUIMIENTO AL CUMPLIMIENTO DE LAS POLÍTICAS DE INFORMACIÓN Y COMUNICACIÓN DE ENTERRITORIO S.A. ESTABLECIDAS EN LOS PRINCIPIOS 13, 14 Y 15 DEL COMPONENTE 4 (MODELO DE REFERENCIA COSO 2013), IMPLEMENTADOS MEDIANTE LA CIRCULAR BÁSICA JURÍDICA CE 006/25 DE LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA - SEMESTRE I DE 2026*
TIPO DE INFORME:	*Informe de seguimiento*
DESTINATARIOS:	*Armando Vivas Salamanca* *Gerente Tecnologías de la Información* *María Camila Ceballos Caicedo* *Gerente Grupo de Comunicaciones*
FUENTE DE INFORMACIÓN:	*Gestión de Tecnologías de la Información / Grupo de Comunicaciones*
EMITIDO POR:	*Orlando Correa Núñez*
AUDITOR:	*Luisa Fernanda Ríos Giraldo*

DESARROLLO DEL INFORME:

OBJETIVO

Evaluar el cumplimiento de las políticas de información y comunicación de ENTerritorio S.A. establecidas en los Principios 13, 14 y 15 del Componente 4 (Modelo de referencia COSO 2013), implementados mediante la Circular Básica Jurídica CE 006/25 de la Superintendencia Financiera de Colombia, correspondientes al Semestre I de 2026. Lo anterior, con el propósito de contribuir al mejoramiento continuo de la Sociedad.

ALCANCE

El seguimiento comprendió el Semestre I de 2026 (1 de enero a 30 de junio de 2026) e incluye la verificación del cumplimiento de: a) Los requerimientos del numeral 3.4 del Capítulo IV de la CE 006/25 y de los numerales conexos 3.1.8, 3.1.17, 4.1.1, 4.1.4.1 y 4.4.4.1 a 4.4.4.6; (3.4.1 – Política de Información y Comunicación; 3.1.8 – Política de Seguridad de la Información; 3.1.17 – Plan Estratégico de Tecnología;

4.1.1 – Funciones de la Junta Directiva; 4.1.4.1 – Funciones de la Junta Directiva, solicitudes de información; 4.4.4.1 a 4.4.4.6 – Funciones de la Alta Gerencia en materia de información y comunicación) y b) Los Principios 13 (calidad de la información), 14 (comunicación interna) y 15 (comunicación externa) de COSO 2013, como marco de referencia. Comprende los procesos de Gestión de Tecnologías de la Información y Gestión de las Comunicaciones y, para los aspectos cuya evidencia reposa en otras instancias, la Secretaría General, la Alta Gerencia y el Grupo de Planeación y Desarrollo Organizacional.

LIMITACIÓN DEL ALCANCE

No se obtuvo la información correspondiente a los órganos de gobierno, requerida para verificar los numerales 4.1.4.1, 4.4.4.3, 4.4.4.5 y 4.4.4.6 de la CE 006/25 (4.1.4.1 – Funciones de la Junta Directiva: solicitudes de información; 4.4.4.3 – Funciones de la Alta Gerencia: comunicar al personal las políticas y decisiones de la Junta Directiva; 4.4.4.5 – Funciones de la Alta Gerencia: monitoreo de los controles del subnumeral 3.3; 4.4.4.6 – Funciones de la Alta Gerencia: entrega oportuna de información a la Junta Directiva y a los órganos de gobierno): actas, solicitudes y convocatorias de la Junta Directiva y actas de seguimiento de la Alta Gerencia. Las áreas evaluadas manifestaron no tener acceso a ella por su carácter reservado y trasladaron la solicitud a la Secretaría General Junta Directiva Oficina Jurídica, el 5 de octubre de 2026, sin que se recibiera respuesta a la fecha de emisión del presente informe. En consecuencia, los resultados de dichos numerales se establecieron con la información disponible.

Adicionalmente, mediante el memorando conjunto Rad. 202612010103393 del 29 de septiembre de 2026, el Grupo de Tecnologías de la Información y el Grupo de Comunicaciones manifestaron no contar con acceso, por su carácter reservado, a la información de los numerales 8, 14, 16, 17 y 18 de la Matriz para orientación de la Respuesta (actas de aprobación de la Junta Directiva sobre la Política de Seguridad de la Información, el Plan Estratégico de Tecnología y la Política de Información y Comunicación; solicitudes de información de la Junta Directiva; socialización al personal de las políticas y decisiones de la Junta Directiva; actas de seguimiento de la Alta Gerencia a los controles del subnumeral 3.3; y convocatorias de entrega anticipada de información a la Junta Directiva), e instaron a canalizar la solicitud ante Gobierno Corporativo. En consecuencia, los resultados de dichos numerales también se establecieron con la información disponible.

MARCO LEGAL

i. Circular Básica Jurídica, Circular Externa 006 de 2025 de la Superintendencia Financiera de Colombia y sus modificaciones: Parte I, Título I, Capítulo IV (Sistema de Control Interno), numeral 3.4, Información y Comunicación.
ii. Principios: 13, 14 y 15 (COSO 2013). (Principio 13 – la organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno; Principio 14 – la organización comunica internamente la información necesaria para apoyar el funcionamiento del control interno; Principio 15 – la organización se comunica con los grupos de interés externos sobre los aspectos que afectan el funcionamiento del control interno)
iii. Decreto Ley 1962 de 2023, por el cual se homogenizan las disposiciones que regulan la gobernanza y los regímenes de las entidades públicas de servicios financieros. Su artículo 9 transforma a ENTerritorio en sociedad anónima de economía mixta.
iv. Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado, y sus modificaciones. Decreto 1083 de 2015, modificado por

el Decreto 1499 de 2017 **"**MIPG, Dimensión 6 – Seguimiento, Evaluación y Control Integral (Política de Control Interno)".

MARCO DE REFERENCIA TÉCNICO

i. COSO 2013 – Marco Integrado de Control Interno: Componente de Información y Comunicación, Principios 13, 14 y 15.
ii. NTC-ISO/IEC 27001:2022 y su Enmienda 1:2024, Sistemas de gestión de seguridad de la información, requisitos.

RESULTADOS DEL SEGUIMIENTO

Antecedentes del Seguimiento

En cumplimiento del Plan Anual de Auditorías 2026, la Asesoría de Control Interno adelantó el seguimiento al cumplimiento de la Circular Básica Jurídica (Circular Externa 006 de 2025) de la Superintendencia Financiera de Colombia, Parte I, Título I, Capítulo IV – Sistema de Control Interno, en lo relacionado con el Componente 4: Información y Comunicación, para el Semestre I de 2026.

Este seguimiento se enmarca en las funciones que el numeral 4.5 del citado Capítulo asigna a la auditoría interna, u órgano que haga sus veces, respecto de la evaluación independiente del Sistema de Control Interno (SCI).

La Circular Externa 006 de 2025, vigente desde el 26 de junio de 2025, reexpidió el texto de la Circular Básica Jurídica y subrogó la Circular Externa 029 de 2014, manteniendo el Capítulo IV del SCI. Dentro de este, el numeral 3.4 define el Componente de Información y Comunicación como el proceso de intercambio de información con los grupos de interés internos y externos.

El numeral 3.4.1 dispone que la entidad debe contar con una política de información y comunicación que establezca, como mínimo: Que la información transmitida a los grupos de interés sea accesible, exacta, actualizada y protegida (3.4.1.1), que los sistemas de información tengan la capacidad de obtener, capturar y procesar datos de fuentes internas y externas seguras, ajustados a las necesidades y a los volúmenes de datos de la entidad (3.4.1.2), criterios para definir el tipo de información que se comunica a los grupos de interés según su importancia y criticidad (3.4.1.3), y canales específicos y exclusivos para la recepción de quejas y denuncias, con salvaguardas de anonimato y confidencialidad y diferenciados de los canales de quejas de los consumidores financieros (3.4.1.4).

A su vez, los numerales 4.1 y 4.4 del mismo Capítulo asignan a la Junta Directiva y a la Alta Gerencia responsabilidades en la aprobación de las políticas y planes asociados y, en la supervisión y comunicación de la información.

Por su naturaleza jurídica, ENTerritorio S.A. es una sociedad anónima de economía mixta vinculada al Ministerio de Hacienda y Crédito Público y subordinada al Grupo Bicentenario S.A.S., conforme al Decreto Ley 1962 de 2023.En su condición de entidad pública vigilada por la Superintendencia Financiera, le son aplicables la Ley 87 de 1993 y el Modelo Integrado de Planeación y Gestión (MIPG), adoptado mediante el Decreto 1083 de 2015, modificado por el Decreto 1499 de 2017.

Frente al tema, la Circular Básica Jurídica dispone que las entidades del sector público adopten el enfoque del Modelo Estándar de Control Interno (MECI), sin perjuicio de las instrucciones del Capítulo IV que les resulten aplicables.

Como marco de referencia técnico, el seguimiento toma los Principios 13, 14 y 15 del Marco Integrado de Control Interno COSO 2013, que desarrollan el componente de información y comunicación:

i. Principio 13, sobre la obtención y uso de información relevante y de calidad;
ii. Principio 14, sobre la comunicación interna;
iii. Principio 15, sobre la comunicación con los grupos de interés externos.

Complementariamente, se toma la norma NTC-ISO/IEC 27001:2022 y su enmienda 1:2024, en lo relacionado con la seguridad de la información que soporta los sistemas y canales de comunicación de la Sociedad.

Como antecedente institucional, en el Informe Anual de Gestión y Evaluación sobre la Eficacia del SCI – Vigencia 2025 (F-AU-10), presentado a la Asamblea General de Accionistas en 2026, la Asesoría de Control Interno calificó el Componente de Información y Comunicación con un nivel de cumplimiento del 86% para el segundo semestre de 2025.

En dicho informe se identificaron fortalezas en la existencia de canales de comunicación externa, líneas de denuncia y divulgación de planes institucionales. También se identificaron oportunidades de mejora en el monitoreo del Sistema de Gestión de Seguridad de la Información, la oportunidad en la respuesta a PQRDSF, la calidad de la información del catálogo documental y los controles de respaldo y acceso en los sistemas de información. Estos resultados se toman como línea base del presente seguimiento, con la salvedad de que corresponden a la vigencia 2025, según el documento referido.

Para el desarrollo del seguimiento, la Asesoría de Control Interno comunicó el inicio de la actividad mediante el memorando Rad. 202611010004873 del 16 de septiembre de 2026, al Grupo de Tecnologías de la Información (GTI).

Ese mismo día, mediante el memorando Rad. 202611010004893, solicitó a GTI y al Grupo de Comunicaciones la información y evidencias correspondientes, con plazo al 22 de septiembre de 2026. Con esa solicitud se adjuntó la "Matriz para orientación de la Respuesta", con los 18 numerales del requerimiento.

El 22 de septiembre de 2026, el GTI remitió respuesta mediante el memorando Rad. 202615010002353. La respuesta estaba estructurada por los Principios 13, 14 y 15 del modelo COSO 2013 e incluía tres anexos:

i. El Manual de Políticas de Gobierno de Datos M-TI-02 V01;
ii. La Matriz de Aplicaciones 2026;
iii. El reporte de calificación de SecurityScorecard del 22 de septiembre de 2026.

El Grupo de Comunicaciones no remitió pronunciamiento dentro de ese plazo.

Efectuada la verificación de la información recibida frente a los 18 numerales, la Asesoría de Control Interno comunicó el resultado y reiteró la información pendiente mediante el memorando Rad. 202611010005093 del 23 de septiembre de 2026, con plazo al 24 de septiembre de 2026. Junto con ese memorando se remitió el instrumento con el cruce de la información efectuado.

El 25 de septiembre de 2026, el GTI manifestó por correo electrónico que su respuesta había atendido el Rad. 202611010004873 y que no había tenido conocimiento de la matriz. Informó además que adelantaba, en conjunto con el Grupo de Comunicaciones, la preparación de la respuesta a los numerales pendientes.

La Asesoría de Control Interno a través de comunicación electrónica del 25 de septiembre de 2026, precisó que el Rad. 202611010004873 correspondía al aviso de inicio del seguimiento y no contenía solicitud de información, y que el requerimiento con sus 18 numerales se había formulado mediante el Rad. 202611010004893.

Desarrollo del seguimiento

Como fuentes de evidencia se utilizaron:

i) La información aportada por las áreas responsables,
ii) Los documentos consultados por la Asesoría de Control Interno en el Catálogo de Documental de la Sociedad,
iii) El Informe Anual de Gestión y Evaluación sobre la Eficacia del SCI – Vigencia 2025, con la salvedad de que corresponde al seguimiento realizado en el 2025.

Metodología

- El seguimiento se desarrolló conforme con el Programa de Trabajo Informes Seguimientos de Ley (F-AU-33 V01, vigente desde el 12 de junio de 2025). El marco profesional aplicado fue el Marco Internacional para la Práctica Profesional de la Auditoría Interna del Instituto de Auditores Internos (IIA), junto con las Normas Globales de Auditoría Interna del Instituto de Auditores Internos (IIA), vigentes desde el 9 de enero de 2025, y la Guía para la Gestión Estratégica y el Fortalecimiento de la Auditoría Interna en Entidades Públicas – Versión 5 – Julio de 2026".
- A partir de los criterios descritos en el alcance, la Asesoría de Control Interno estructuró una matriz con 18 numerales de verificación. Cada numeral quedó asociado a su criterio normativo, al principio COSO 2013 correspondiente y a la referencia de la NTC-ISO/IEC 27001:2022. Frente al tema, la Asesoría de Control Interno, puso a disposición de las áreas como instrumento orientador la matriz referida, para la consolidación de la respuesta. (Ver Anexo No.1)
- La evaluación se enfocó en el diseño de los controles, es decir, en la existencia, aprobación, vigencia y contenido mínimo de las políticas, planes y mecanismos de control exigidos. Cuando el soporte documental disponible lo permitió, también se evaluó su operación durante el Semestre I de 2026.
- Para la obtención y el análisis de los soportes, se aplicaron las siguientes técnicas de auditoría:
- Consulta, mediante la solicitud formal de información a las áreas responsables,
- Inspección documental de la respuesta y de los anexos aportados,
- Rastreo y cruce de la información, comparando lo solicitado, lo afirmado en la respuesta y lo efectivamente soportado,

- Verificación en fuentes institucionales, mediante la consulta del Catálogo Documental de la Sociedad.
- De manera complementaria, se utilizó como evidencia disponible, el Informe Anual de Gestión y Evaluación sobre la Eficacia del SCI – Vigencia 2025, por cuanto permite identificar el avance institucional en la materia.
- En la valoración de los soportes documentales, se consideraron los criterios de pertinencia, suficiencia, confiabilidad y correspondencia con el periodo evaluado. Las afirmaciones de las áreas que no estuvieron acompañadas de soporte documental no se tomaron como evidencia de cumplimiento. Los documentos generados con posterioridad al periodo o sin aprobación formal se valoraron únicamente como referencia.

Frente al tema, mediante el memorando Rad. 202612010107393 del 6 de octubre de 2026, el Grupo de Tecnologías de la Información y el Grupo de Comunicaciones respondieron al Rad. 202611010005093. La respuesta se recibió un día después del plazo fijado (5 de octubre de 2026).

En ella, el GTI manifestó que *"no posee información ni soportes adicionales por entregar"*. Indicó que durante el periodo evaluado *"no envió ningún reporte, acta o comunicación a la Junta Directiva"* y que la Junta *"tampoco ha formulado solicitudes de información ni requerimientos específicos a este grupo de trabajo"*. Por su parte, el Grupo de Comunicaciones señaló que durante el periodo no recibió solicitudes de información de la Junta Directiva.

Resultado de seguimiento

A continuación, se presenta el resultado del análisis efectuado por la Asesoría de Control Interno:

1. **<u>Política de Información y Comunicación: Contenido mínimo y aprobación por la Junta Directiva</u>**

- **Criterios CE 006/25: 3.4.1 y 4.1.1 m)**

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
P13, P14 y P15 (contenido de la política); P2 (aprobación y supervisión de la Junta Directiva)	Criterio: 3.4.1 (Política de información y comunicación, con los contenidos mínimos de los subnumerales 3.4.1.1 a 3.4.1.4) y 4.1.1 lit. m) (aprobación por la Junta Directiva). 4.1.1 lit. m (Política de información y comunicación)	Exige que la entidad cuente con una Política de Información y Comunicación formalmente aprobada por la Junta Directiva, vigente a la fecha de corte, con control de versiones dentro del Sistema de Gestión.

- **Observación Número 1 – Política de Información y Comunicación sin la totalidad de los contenidos mínimos exigidos por la CE 006/25**

Criterios:

i. Circular Básica Jurídica (CE 006/25), Parte I, Título I, Capítulo IV:
   a. Numeral 3.4.1: *"La política de información y comunicación debe establecer, como mínimo"*, lo dispuesto en los subnumerales 3.4.1.1 (características de la información), 3.4.1.2 (sistemas de información), 3.4.1.3 (criterios de selección de información) y 3.4.1.4 (canales de comunicación para quejas y denuncias);
   b. Numeral 4.1.1 lit. m): Asigna a la Junta Directiva la aprobación de la política de información y comunicación.

ii. COSO 2013:
   a. Principios 13, 14 y 15: La organización obtiene y utiliza información relevante y de calidad, y la comunica interna y externamente;
   b. Principio 2: *"el consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno"*.

Condición: La Sociedad cuenta con la Política de Comunicaciones O-CO-01 V04, vigente desde el 4 de octubre de 2024 y con control documental. Según certificación del Secretario Técnico (E) de la Junta Directiva, la política fue aprobada por ese órgano en sesión ordinaria del 31 de octubre de 2023, previo aval del Comité de Gobierno Corporativo del 23 de octubre de 2023. Dicha aprobación corresponde a la versión 03; la versión 04, corresponde a un cambio de imagen institucional y razón social. El control de modificaciones del documento no registra la aprobación de la Junta Directiva.

El contenido de la política es propio de la comunicación organizacional (narrativa institucional, imagen, medios, redes y productos audiovisuales) y no incluye la totalidad de los contenidos mínimos exigidos por la norma, dado que: i) Se omite el atributo de exactitud de la información y limita su alcance a la información publicada en los canales autorizados (3.4.1.1), ii) No contiene lineamientos sobre los sistemas de información (3.4.1.2), iii) No define criterios de selección de la información según su importancia y criticidad, sino que remite al Plan de Acción de Comunicaciones y a la Matriz de Comunicaciones del SIG, instrumentos que, una vez verificados, tampoco los establecen (3.4.1.3), iv) No establece canales específicos, exclusivos y diferenciados para quejas y denuncias, ni salvaguardas de anonimato, confidencialidad y protección al denunciante, y somete las denuncias al procedimiento general de PQRSDF, P-RC-01 (3.4.1.4).

Se precisa que, los demás documentos relacionados con el componente no suplen estas brechas:

i. La Política Institucional de Seguridad de la Información O-RI-01 V04, aprobada por la Junta Directiva el 24 de septiembre de 2024, atiende el numeral 3.1.8 y solo complementa el atributo de protección de la información.
ii. El Manual de Políticas de Gobierno de Datos M-TI-02 V01 desarrolla elementos de calidad y fuentes de datos, pero no se encuentra aprobado ni vigente.

Se deja constancia de que la Circular Externa 008 de 2023 (circular predecesora, sustituida por la CE 006/25 a partir del 26 de junio de 2025) ya contenía atributos equivalentes para la política de información y comunicación; por tanto, la observación se refiere a la ausencia de una revisión formal y documentada frente al texto vigente de la norma.

Causa:

i. La Política de Comunicaciones fue formulada con un enfoque de comunicación organizacional, orientado a la narrativa e imagen institucional, y no como la política del componente de información y comunicación del Sistema de Control Interno.
ii. Los contenidos del componente están a cargo de distintos procesos, sin una instancia que los integre en un solo instrumento:
    a. Gestión de las Comunicaciones, la Política de Comunicaciones;
    b. Gestión del Riesgo, la Política de Seguridad de la Información;
    c. Gestión de Tecnologías de la Información, el Manual de Gobierno de Datos;
    d. el Grupo de Servicios Administrativos, los canales de denuncia, según lo informado por las áreas.
iii. El Manual de Políticas de Gobierno de Datos se encuentra en trámite de firma por parte de la Presidencia desde diciembre de 2025, según lo indicado por la dependencia (en la ejecución del presente seguimiento).

Posible impacto:

i. Los canales de recepción de denuncias comparten medios y procedimiento con las PQRSDF, sin salvaguardas de anonimato ni de protección al denunciante,
ii. No existen criterios de selección de la información por grupo de interés según su importancia y criticidad.
iii. Incumplimiento de los numerales 3.4.1 y 4.1.1 lit. m) de la CE 006/25 ante la Superintendencia Financiera de Colombia.
iv. Transmisión de información inexacta o desactualizada a los grupos de interés, y comunicación de información sin consideración de su criticidad.
v. Afectación reputacional de la Sociedad.

Recomendación para el GTI y Grupo Comunicaciones:

i. Formular o actualizar la Política de Información y Comunicación con el enfoque del componente del Sistema de Control Interno, incorporando expresamente los contenidos mínimos de los subnumerales 3.4.1.1 a 3.4.1.4 de la CE 006/25.
ii. Designar un responsable de la consolidación del componente que articule, en dicha política o mediante remisiones expresas, los lineamientos de comunicaciones, seguridad de la información, gobierno de datos y canales de denuncia.
iii. Someter la política actualizada a aprobación de la Junta Directiva y registrar la aprobación en el control de modificaciones. Concluir la aprobación del Manual M-TI-02 y establecer una revisión periódica de las políticas frente a los cambios normativos de la Superintendencia Financiera.

2. <u>Calidad de la información: Metodología de validación para garantizar su exactitud y actualización</u>

- **Criterio CE 006/25: 3.4.1.1**

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)

Principio 13 de COSO 2013 (Componente Información y Comunicación): *"La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno"*, en relación con los Principios 14 y 15.	3.4.1.1 Calidad de la información	Exige que la Sociedad *" obtenga o genere y utilice información relevante y de calidad para apoyar el funcionamiento del control interno"* Verificación de *metodología de validación de los criterios indicados en la norma*

- **Observación Número 2 – Ausencia de una metodología de validación de calidad de datos aprobada y aplicada que garantice la exactitud y la actualización de la información**

Criterio

i. Circular Básica Jurídica (CE 006/25), Parte I, Título I, Capítulo IV, numeral 3.4.1.1: *"La información transmitida a los grupos de interés debe ser accesible, exacta, actualizada y protegida."*
ii. COSO 2013, Principio 13: *"La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno"*, en relación con los Principios 14 y 15.
iii. Ley 87 de 1993, artículo 2, literal e): *"Asegurar la oportunidad y confiabilidad de la información y de sus registros."*

Condición: La Sociedad no cuenta con una metodología de validación de calidad de datos formalmente definida, aprobada y aplicada durante el Semestre I de 2026.

El Manual de Políticas de Gobierno de Datos M-TI-02 V01, aportado por el GTI (Rad. 202615010002353), establece definiciones, roles y lineamientos generales: Gestión mensual de la calidad por parte de los Data Stewards, rutinas ETL y fuentes únicas. Sin embargo, no define dimensiones medibles, reglas de validación, umbrales de aceptación, indicadores ni formato de registro, y asigna a otros roles la definición de las reglas de negocio y de la calidad requerida. Por lo tanto, la afirmación del GTI según la cual el documento *"define las reglas de negocio, criticidad y ciclo de vida de la información"* no se encuentra soportada.

El Manual no se encuentra aprobado ni vigente: No registra vigencia, el aprobador no ha firmado y solo 2 de los 8 revisores lo han firmado. Registra firmas de elaboración del 30 de diciembre de 2025 y, según el GTI, está en trámite de firma por parte de la Presidencia. En su comunicación del 6 de octubre de 2026 (Rad. 202612010107393), el GTI no informó su aprobación ni se allegaron soportes adicionales. El *"marco metodológico provisional basado en mejores prácticas de la industria"* referido por el GTI no está documentado, y no se cuenta con evidencia de su aplicación.

Como avance institucional, el Informe SCI 2025 registró la existencia de controles sobre la integridad, disponibilidad y confidencialidad de la información. En la misma vigencia identificó debilidades en la exactitud y actualización de la información, en los siguientes aspectos: i) Fallas persistentes en la validación de saltos en consecutivos del ERP, ii) Inconsistencias en la disponibilidad y calidad de informes del catálogo documental, iii) Deficiencias de completitud, consistencia e integridad en los expedientes contractuales, y iv) Desactualización de las tablas de retención documental.

Causas:

i. La formalización del marco de gobierno de datos no ha concluido. El Manual M-TI-02, instrumento base para la gestión de la calidad de los datos, continúa en trámite de aprobación desde diciembre de 2025, sin que se haya informado un plazo para su expedición.
ii. La gestión de la calidad de los datos se ha supeditado a la aprobación del Manual. El GTI indicó que la Sociedad se encuentra en *"la fase de formalización técnica y procedimental"*. Mientras tanto, la operación se adelanta bajo un marco provisional no documentado, sin un procedimiento operativo de validación independiente de esa aprobación.
iii. No se evidenció la designación de los roles definidos en el Manual (Data Stewards, administradores y responsables de datos), en los cuales el documento delega la definición de las reglas de negocio y de los niveles de calidad requeridos.

Posible impacto:

i. Las debilidades de exactitud y actualización identificadas en la vigencia 2025 no cuentan con un mecanismo sistemático de detección, medición y corrección que permita demostrar su cierre.
ii. Incumplimiento del numeral 3.4.1.1 de la CE 006/25.

Recomendaciones al GTI y Grupo de Comunicaciones:

i. Establecer, con la Presidencia, un plazo para la expedición del Manual de Políticas de Gobierno de Datos M-TI-02 y hacer seguimiento hasta su aprobación.
ii. Documentar y aprobar, sin supeditarlo a la expedición del Manual, un procedimiento operativo de validación de calidad de datos para los conjuntos de datos críticos. Este debe definir dimensiones y reglas de validación, umbrales de aceptación, frecuencia, indicadores y formato de registro, y conservar evidencia de su aplicación periódica.
iii. Designar formalmente a los responsables de datos y Data Stewards y definir las reglas de negocio y los niveles de calidad requeridos para los datos de su propiedad.

3. Calidad de la información: indicadores para medir su exactitud, actualización, accesibilidad y protección

- **Criterio CE 006/25: 3.4.1.1**

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
Principio 13 de COSO 2013 (Componente Información y Comunicación): *"La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno."*	3.4.1.1 características de la información	Exige reportar indicadores de calidad de la información que cubran de forma explícita sus cuatro atributos: exactitud, actualización, accesibilidad y protección (seguridad) de la información. El 3.4.1.1 exige que la información sea *"accesible, exacta, actualizada y protegida"*. Los indicadores son el medio de auditoría para verificar que esos atributos se cumplen y se monitorean.

- **Observación Número 3 – Ausencia de indicadores medidos y reportados sobre los atributos de calidad de la información**

Criterio:

i. Circular Básica Jurídica (CE 006/25), Parte I, Título I, Capítulo IV, numeral 3.4.1.1: *"La información transmitida a los grupos de interés debe ser accesible, exacta, actualizada y protegida."*
ii. Numeral 4.4.4.2: Asigna a la Alta Gerencia informar a la Junta Directiva y a los comités sobre el funcionamiento de los sistemas de información, con indicadores.
iii. COSO 2013, Principio 13: *"La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno."* Uno de sus puntos de enfoque es mantener la calidad a lo largo del procesamiento.
iv. Ley 87 de 1993, artículo 2, literal e): *"Asegurar la oportunidad y confiabilidad de la información y de sus registros."*

Condición: Durante el Semestre I de 2026 no se reportaron indicadores de calidad de la información que cubran de forma específica los atributos de exactitud, actualización, accesibilidad y protección.

Los soportes aportados por el GTI no corresponden a indicadores:

i. El reporte de SecurityScorecard es una captura puntual del 22 de septiembre de 2026, posterior al periodo, limitada a la superficie externa del dominio institucional.
ii. Los archivos de turnos de enero a junio de 2026 corresponden a la programación del personal de monitoreo, sin resultados de medición.
iii. El Manual M-TI-02 V01, sin aprobación, solo enuncia que los indicadores *"deben estar diseñados"*.

[Situación 1 – Atributo de protección] Para el atributo de protección, el Manual M-RI-06 V07, aprobado por la Junta Directiva el 28 de enero de 2026, define indicadores sobre la cobertura y actualización del EDR, los incidentes atendidos y las actividades de capacitación. No se cuenta con los soportes documentales de las mediciones del periodo ni los informes SOC del semestre.

[Situación 2 – Atributos de exactitud y actualización] La exactitud y la actualización no cuentan con indicador definido ni con medición. En los documentos de seguimiento del PETI (septiembre de 2026), el GTI declara tres hechos:

i. De los cuarenta y dos indicadores del plan, solo dos cuentan con valor medido (2 de 42 ≈ 4,8 %),
ii. La medición de calidad de los datos carece de umbral de aceptación mientras no se formalice la política de gobierno del dato,
iii. El reporte de disponibilidad del operador no se ha consolidado como serie.

En el Rad. 202612010107393, el GTI manifestó que no posee soportes adicionales y que durante el periodo no envió ningún reporte a la Junta Directiva. Como avance institucional, el Informe SCI 2025 registró informes SOC mensuales de monitoreo de seguridad, y el GTI reporta una medición del 98% de accesibilidad del portal web en 2025.

Causa:

i. Los indicadores están enunciados pero no operacionalizados. Así lo declara el GTI en el Informe Semestral del PETI: Las fichas definen indicadores sin método reproducible ni medición.
ii. La medición de la exactitud y la actualización depende de la formalización de la política de gobierno del dato. El documento PROY04 advierte que *"Mientras la política no se formalice, la medición carece de criterio de aceptación"*, y el Manual M-TI-02 sigue sin aprobación, como ya se indicó anteriormente.
iii. No existe un esquema que integre en un tablero o reporte único los indicadores de los cuatro atributos, ni una línea de reporte periódico hacia la Alta Gerencia y la Junta Directiva.

Posible impacto:

i. Durante el Semestre I de 2026, la Junta Directiva no recibió información sobre la calidad de la información ni sobre el funcionamiento de los sistemas.
ii. La Sociedad no puede demostrar con datos que la información que transmite a sus grupos de interés es exacta, actualizada, accesible y protegida.
iii. Deterioro no detectado de la calidad de la información y de la disponibilidad de los sistemas, que podría afectar la toma de decisiones y los reportes a los órganos de control y a la Superintendencia Financiera.
iv. Incumplimiento de los numerales 3.4.1.1 y 4.4.4.2 de la CE 006/25.

Recomendación al GTI y Grupo Comunicaciones:

i. Operacionalizar los indicadores de calidad de la información con hoja de vida para cada uno (fórmula, fuente, meta o umbral, frecuencia y responsable), de manera que cubran los cuatro atributos del numeral 3.4.1.1.
ii. Para la exactitud y la actualización, adoptar umbrales de aceptación provisionales para los conjuntos de datos críticos, sin esperar la aprobación del Manual M-TI-02, y ajustarlos una vez se formalice la política de gobierno del dato.
iii. Consolidar los indicadores en un reporte periódico dirigido a la Alta Gerencia y a la Junta Directiva, incluyendo las mediciones del M-RI-06 V07 (EDR y capacitación) y los informes SOC mensuales como fuente para la protección.

4. <u>Sistemas de información: Capacidad para obtener, capturar y procesar datos de fuentes internas y externas seguras</u>

- **Criterio CE 006/25: 3.4.1.2**

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
Principio 13 de COSO 2013 (Componente Información y Comunicación): *"La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno."*	3.4.1.2 sistemas de información	Exige identificar las fuentes de información utilizadas por el SIAR para la gestión de riesgos y mantener un inventario de los sistemas de información institucionales, señalando su capacidad frente a los volúmenes de datos que procesan. El 3.4.1.2 exige que los sistemas *"tengan la capacidad de obtener, capturar y procesar datos de fuentes internas y externas seguras"*, ajustados a las necesidades y volúmenes de la entidad.

- **Observación Número 4 – Inventario de sistemas de información, sin capacidad por sistema y sin identificación de las fuentes de información del SIAR**

Criterio:

i. Circular Básica Jurídica (CE 006/25), Parte I, Título I, Capítulo IV, numeral 3.4.1.2: *"Los sistemas de información de las EV deben tener la capacidad de obtener, capturar y procesar datos procedentes de fuentes internas y externas seguras, y transformarlos en información que tenga valor para las EV. Los sistemas deben ajustarse de acuerdo con las necesidades de las EV y los volúmenes de datos que deban ser procesados."*
ii. COSO 2013, Principio 13: *"La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno"*. Incluye como punto de enfoque la captura de fuentes de datos internas y externas.
iii. Estatuto de Auditoría Interna E-AU-01 V01, numeral 4.1: autoriza a la Asesoría de Control Interno a *"Tener acceso irrestricto: a registros, sistemas, personal y bienes, incluyendo información bajo control de terceros"*.
iv. Como referencia técnica, NTC-ISO/IEC 27001:2022, controles A.5.9 (inventario de información y otros activos asociados) y A.8.6 (gestión de la capacidad).

Condición: La Sociedad cuenta con un inventario de aplicaciones (Matriz de aplicaciones Ent 2026, 44 registros), pero este no permite demostrar que los sistemas de información tengan la capacidad de obtener, capturar y procesar datos de fuentes internas y externas seguras, ajustada a los volúmenes que procesan.

El inventario presenta estas limitaciones conforme a los soportes documentales aportados:

i. No registra la capacidad de los sistemas ni los volúmenes de datos que procesan,
ii. No identifica las fuentes de información que alimentan el SIAR,
iii. Incluye tres aplicaciones que su descripción declara absorbidas o reemplazadas (S1003, S1009 y S1015),
iv. No registra el estado ni la criticidad de los activos,
v. Registra dos veces el portal web,
vi. Omite sistemas referidos por el GTI (Office 365, los componentes de la arquitectura de datos y el aplicativo SIRI del SIAR),
vii. Carece de código, versión, fecha y aprobación.

La capacidad instalada solo se reporta de forma agregada por ambiente en un documento posterior al periodo (Diagnóstico Institucional de TI, septiembre de 2026), sin asociarla a cada sistema. Las herramientas tecnológicas del SIAR fueron identificadas en el Informe SCI 2025, pero no se cuenta con la identificación de las fuentes de datos que las alimentan ni su validación por el Grupo de Gestión de Riesgos.

El GTI afirmó que el inventario está *"activo y controlado"* e incluye la criticidad CID, afirmaciones que no corresponden con el soporte aportado. Los documentos del PETI señalan que la criticidad de negocio no está definida por sistema y que la Sociedad opera 32 aplicaciones en producción, mientras que el inventario tiene 44 registros.

Adicionalmente, el GTI indicó que entrega a esta Asesoría un resumen del inventario y que mantiene los campos técnicos *"bajo la custodia y administración exclusiva de la Dirección de TI"*. Esa restricción impidió verificar el inventario completo.

La Matriz de Riesgos SIAR 2026 reconoce el manejo de aplicaciones obsoletas como causa de riesgo, sin que se evidencie el registro de su materialización.

Causa:

i. El inventario de sistemas de información no está formalizado como instrumento del Sistema de Gestión, con responsable, periodicidad de actualización y campos mínimos (estado, propietario, criticidad, capacidad y volumen). Adicionalmente, no refleja los retiros, los reemplazos ni las nuevas plataformas.
ii. No se evidenció un proceso de gestión de la capacidad por sistema que contraste la capacidad instalada con los volúmenes de datos procesados.
iii. No hay articulación documentada entre el GTI y el Grupo de Gestión de Riesgos para identificar y validar las fuentes de información del SIAR.
iv. El GTI aplica un criterio restrictivo sobre el acceso a los campos técnicos del inventario, que no considera las facultades de la auditoría interna previstas en el Estatuto de Auditoría Interna.

Posible impacto:

i. El inventario de sistemas presenta registros de aplicaciones que ya no operan, omisiones y diferencias frente a otras fuentes aportadas por el GTI.
ii. La Asesoría de Control Interno no pudo verificar el inventario completo de los sistemas de información.
iii. Afectación de la gestión de activos de información del SGSI.
iv. Incumplimiento del numeral 3.4.1.2 de la CE 006/25.

Recomendaciones al GTI y al Grupo de Comunicaciones:

i. Establecer un proceso de gestión de la capacidad que, para los sistemas críticos, contraste periódicamente la capacidad instalada con los volúmenes de datos procesados y los proyectados.
ii. Identificar y documentar, en conjunto entre el GTI y el Grupo de Gestión de Riesgos, las fuentes de información internas y externas que alimentan el SIAR, con su validación por parte de este último.

5. <u>Aprobación por la Junta Directiva de la Política de Seguridad de la Información, el Plan Estratégico de Tecnología y la Política de Información y Comunicación</u>

Criterio CE 006/25: 4.1.1 lit. h), l), m)

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
Principio 2 de COSO 2013 (Componente Ambiente de Control): "El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno". Se relaciona con el Principio 12, en cuanto a la formalización de políticas y planes; con el Principio 11, respecto de la Política de seguridad de la información (lit. h) y del Plan estratégico de tecnología (lit. l); y con los Principios 13, 14 y 15, respecto de la Política de información y comunicación (lit. m).	4.1.1 lit. h), l), m) Aprobación por la Junta Directiva de la Política de Seguridad de la Información, el Plan Estratégico de Tecnología y la Política de Información y Comunicación	El numeral 4.1.1 de la CE 006/25 dispone que "La JD u órgano que haga sus veces debe aprobar los siguientes documentos y políticas", entre ellos la "Política de seguridad de la información" (lit. h), el "Plan estratégico de tecnología" (lit. l) y la "Política de información y comunicación" (lit. m)

- **Observación Número 5 – Plan Estratégico de Tecnología sin aprobación de la Junta Directiva y deficiencias de trazabilidad en el registro de las aprobaciones**

Criterio:

i. Circular Básica Jurídica (CE 006/25), Parte I, Título I, Capítulo IV, numeral 4.1.1: *"La JD u órgano que haga sus veces debe aprobar los siguientes documentos y políticas: (…) h. Política de seguridad de la información. (…) l. Plan estratégico de tecnología. m. Política de información y comunicación."*
ii. COSO 2013, Principio 2: *"El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno."*

Condición: Con base en la información aportada por el GTI y el Grupo de Comunicaciones, de los 3 documentos que el numeral 4.1.1 de la CE 006/25 exige que apruebe la Junta Directiva y que fueron objeto de este seguimiento, se evidenció la aprobación de 2:

i. Política de Seguridad de la Información: Aprobada en sesión del 24 de septiembre de 2024, según la tabla de aprobación del documento O-RI-01 V04. La actualización del Manual M-RI-06 V07 fue aprobada en sesión del 28 de enero de 2026.
ii. Política de Comunicaciones: Aprobada en sesión ordinaria del 31 de octubre de 2023, según certificación del Secretario Técnico (E) de la Junta Directiva.

No se evidenció la aprobación del Plan Estratégico de Tecnología 2024-2027 por la Junta Directiva. Según el Informe Semestral del PETI elaborado por el GTI, el plan fue aprobado por el Comité Institucional de Gestión y Desempeño el 20 de diciembre de 2023, y la Junta Directiva aprobó específicamente sus 14 proyectos, el 26 de junio de 2024. Esta última aprobación no fue soportada por la instancia responsable. El informe define al Comité Institucional de Gestión y Desempeño como la instancia *"de aprobación de políticas, directrices y planes"*.

Se identificaron también deficiencias de trazabilidad en el registro de las aprobaciones:

i. La certificación de aprobación de la Política de Comunicaciones no identifica el código ni la versión del documento aprobado.
ii. El control de modificaciones de la O-CO-01 Política de Comunicaciones no registra la aprobación de la Junta Directiva.
iii. No se cuenta con las actas de aprobación de ninguno de los tres documentos.

La solicitud de soportes que el Grupo de Comunicaciones trasladó a la Secretaría General no incluyó este numeral.

Causa:

i. Esquema interno de aprobación no armonizado con la norma. La Sociedad aplica un esquema en el cual el Comité Institucional de Gestión y Desempeño aprueba los planes institucionales y la Junta Directiva aprueba únicamente los proyectos del portafolio, según lo descrito por el GTI. Ese esquema no se ha armonizado con el numeral 4.1.1 lit. l) de la CE 006/25, que asigna a la Junta Directiva la aprobación del Plan Estratégico de Tecnología.

Posible impacto

i. La Junta Directiva no ha ejercido la aprobación del Plan Estratégico de Tecnología que le asigna la norma. Esto limita su supervisión sobre los desarrollos tecnológicos de la Sociedad, sus riesgos y su justificación técnica y financiera.
ii. La trazabilidad entre las decisiones de la Junta Directiva y las versiones de los documentos aprobados no puede verificarse a partir de los propios documentos.
iii. Incumplimiento del numeral 4.1.1 lit. l) de la CE 006/25,
iv. Ejecución de un plan tecnológico sin el respaldo formal del máximo órgano de dirección, con efecto en la asignación de recursos y en la priorización de los proyectos.

Recomendación para el GTI y Comunicaciones:

i. Someter el Plan Estratégico de Tecnología 2024-2027 a aprobación de la Junta Directiva, conforme al numeral 4.1.1 lit. l) de la CE 006/25, y ajustar el esquema interno de aprobación de planes para que los documentos enunciados en dicho numeral sean aprobados por la Junta Directiva.
ii. Incorporar en el control de modificaciones de las políticas y planes aprobados por la Junta Directiva la sesión, la fecha y el acta de aprobación.

6. <u>Política de Seguridad de la Información: Vigencia y cumplimiento de los 6 controles mínimos</u>

Criterio CE 006/25: 3.1.8

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)

P11 (principal) y P12 – Actividades de Control; en relación con P13 – Información y Comunicación y P4 – Ambiente de Control. La aprobación por la Junta Directiva (4.1.1 lit. h) se relaciona con P2.	3.1.8 Política de Seguridad de la Información	Exige mantener vigente una Política de Seguridad de la Información que evidencie el cumplimiento de seis controles mínimos: acuerdos de confidencialidad; control de acceso físico y lógico; protocolo de atención de incidentes; herramientas antimalware; capacitación; y administración centralizada de la seguridad. "Son los lineamientos que definen los controles que deben implementar las EV para asegurar y proteger la información, los cuales incluyen, entre otros mecanismos, los siguientes: a. Celebrar acuerdos de confidencialidad. b. Permitir el acceso a sistemas, programas y datos exclusivamente a usuarios autorizados en virtud de sus funciones, entre otros, a través de: i. Controles de acceso físico y lógico que comprendan autorización, autenticación y control de acceso. ii. Protocolo de manejo de incidentes. iii. Herramientas para la prevención y detección de código malicioso, virus, entre otros. iv. Capacitaciones de personal y usuarios, en caso de ser procedente. v. Administración centralizada de la seguridad. c. Los demás que defina la EV."

Con base en los soportes documentales aportados, se identificó que, el diseño de los controles exigidos por el numeral 3.1.8 se encuentra documentado en la política, el manual y las obligaciones contractuales del operador tecnológico, en concordancia con los Principios 11 y 12 de COSO 2013.

7. Plan Estratégico de Tecnología: Vigencia y contenido mínimo de sus cinco componentes

Criterio CE 006/25: 3.1.17

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
P11 (controles generales sobre la tecnología), en relación con P6, P7 y P9 (objetivos, riesgos y cambios asociados a los desarrollos tecnológicos) y P4 (capacitación). La aprobación por la Junta Directiva (4.1.1 lit. l) se relaciona con P2.	3.1.17 Plan Estratégico de Tecnología	Exige mantener vigente un Plan Estratégico de Tecnología que cubra cinco componentes: Evaluación de la infraestructura actual; cronograma de corto, mediano y largo plazo; capacitaciones; mitigación del riesgo operacional y de ciberseguridad; y justificación técnica y financiera. **3.1.17. Plan estratégico de tecnología** *Son los desarrollos tecnológicos para el corto, mediano y largo plazo definidos por las EV, teniendo en cuenta los riesgos, la prioridad e impacto de cada objetivo.* *Este plan debe contemplar, al menos, los siguientes aspectos:* *a. Evaluación del estado actual de la infraestructura tecnológica de la EV.* *b. Cronograma de actividades y objetivos que se ejecutarán en el corto, mediano y largo plazo en materia de desarrollos tecnológicos.* *c. Capacitaciones de personal y usuarios para la implementación de los desarrollos, en caso de ser aplicable.* *d. Mecanismos para la mitigación del riesgo operacional y de ciberseguridad asociados a la implementación y al funcionamiento de los desarrollos tecnológicos.* *e. Justificación técnica y financiera de los desarrollos a implementar, indicando su prioridad e impacto en las actividades de la entidad.*

- **Observación Número 6 – Plan Estratégico de Tecnología con cobertura parcial de los contenidos mínimos del numeral 3.1.17**

Criterio:

i. Circular Básica Jurídica (CE 006/25), Parte I, Título I, Capítulo IV, numeral 3.1.17: El plan estratégico de tecnología "debe contemplar, al menos, los siguientes aspectos: a. Evaluación del estado actual de la infraestructura tecnológica de la EV. b. Cronograma de actividades y objetivos que se ejecutarán en el corto, mediano y largo plazo en materia de desarrollos tecnológicos. c. Capacitaciones de personal y usuarios para la implementación de los desarrollos, en caso de ser aplicable. d. Mecanismos para la mitigación del riesgo operacional y de ciberseguridad asociados a la implementación y al funcionamiento de los desarrollos tecnológicos. e. Justificación técnica y financiera de los desarrollos a implementar, indicando su prioridad e impacto en las actividades de la entidad".

ii. Numeral 4.1.1 lit. l) (aprobación por la Junta Directiva, ver numeral 8). COSO 2013, Principio 11: "La organización selecciona y desarrolla actividades de control generales sobre la tecnología para apoyar la consecución de los objetivos".

Condición: La Sociedad cuenta con un PETI 2024-2027 vigente durante el Semestre I de 2026, del cual se publicó en la web institucional el Resumen Ejecutivo V.1. El documento completo no fue aportado ni se encuentra en el Catálogo Documental, donde solo reposan las versiones 2012-2014 y 2015-2018. Frente a los contenidos mínimos del numeral 3.1.17, el resumen presenta un diagnóstico cualitativo sin línea base de infraestructura, una hoja de ruta semestral por proyecto sin actividades por horizonte, la capacitación y la seguridad como drivers y proyectos sin asociarse a cada desarrollo, y una priorización de proyectos sin justificación financiera ni análisis de impacto.

El seguimiento del plan presenta debilidades que fueron precisadas por el GTI:

[Situación 1 - Deficiencias de reporte y medición del seguimiento] Interrupción del reporte mensual entre junio y agosto de 2026, 2 de 42 indicadores con medición (4,8 %) y numeración de proyectos distinta a la del plan publicado.

Se precisa que, el Acta N.° 103 del Comité Institucional de Gestión y Desempeño (CIGD), con corte al 30 de marzo de 2026, registra que el PETI 2026 presenta un avance real del 15,8 % frente a un avance esperado del 27,6 %, lo que confirma una ejecución inferior a la programada. Este reporte trimestral de avance al CIGD es un mecanismo distinto del seguimiento mensual por los 42 indicadores internos que describe el GTI, y no suple las debilidades de reporte y medición señaladas en esta situación.

[Situación 2 - Concentración de responsabilidad] Los 14 proyectos a cargo de un solo profesional, con el riesgo de continuidad que ello implica.

Causa:

i. El PETI se formuló y se hace seguimiento conforme a los lineamientos de la Política de Gobierno Digital y de la Circular Externa 008 de 2023, según el marco normativo de su informe de seguimiento, sin una verificación frente a los contenidos mínimos del numeral 3.1.17 de la Circular Básica Jurídica vigente.

ii. El plan completo no se incorporó al Sistema de Gestión con código, versión y control de modificaciones; solo se publicó su resumen ejecutivo.
iii. El seguimiento del plan se concentra en un solo profesional y sus indicadores se encuentran enunciados pero no operacionalizados, según lo argumentado por el GTI.

Posible Impacto:

i. No es posible verificar el contenido completo del plan ni rastrear el avance reportado contra los proyectos del plan publicado,
ii. El seguimiento del semestre no cuenta con mediciones de sus indicadores ni con reporte continuo.
iii. Implementación de desarrollos tecnológicos sin evaluación de sus riesgos operacionales y de ciberseguridad ni justificación financiera documentada,
iv. Incumplimiento del numeral 3.1.17 de la CE 006/25.

Recomendación para el GTI y Grupo de Comunicaciones

i. Incorporar el PETI 2024-2027 completo al Sistema de Gestión, con código, versión y control de modificaciones, y complementarlo con los contenidos mínimos del numeral 3.1.17: Evaluación cuantificada de la infraestructura actual, cronograma de actividades de corto, mediano y largo plazo, capacitación por desarrollo, mecanismos de mitigación del riesgo operacional y de ciberseguridad, y justificación técnica y financiera con prioridad e impacto.
ii. Adoptar una tabla de equivalencias de la numeración de proyectos entre el plan y sus informes de seguimiento, restablecer el reporte mensual, operacionalizar los indicadores de las fichas de proyecto y evaluar la distribución de responsabilidades en la ejecución y el reporte del plan.

8. <u>Criterios de selección de la información: Definición del tipo de información que se comunica a los grupos de interés según su importancia y criticidad</u>

Criterio CE 006/25: 3.4.1.3

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
P14 (comunicación interna) y P15 (comunicación externa), en relación con P13 (información relevante y de calidad	3.4.1.3	Exige definir los criterios que usa la Sociedad para determinar qué tipo de información debe comunicarse a los distintos grupos de interés internos y externos, según su importancia y criticidad. "Las EV deben establecer criterios para definir el tipo de información que debe ser comunicados a los diferentes grupos de interés internos y externos, en atención a su importancia y criticidad."

- **Observación Número 7 – Ausencia de criterios para definir el tipo de información que se comunica a los grupos de interés según su importancia y criticidad**

Criterio:

i. Circular Básica Jurídica (CE 006/25), Parte I, Título I, Capítulo IV, numeral 3.4.1.3 (Criterios de selección de información): *"Las EV deben establecer criterios para definir el tipo de información que debe ser comunicados a los diferentes grupos de interés internos y externos, en atención a su importancia y criticidad."*
ii. COSO 2013:
    a. Principio 14: *"La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del control interno."*
    b. Principio 15: *"La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno."*
    c. Ambos en relación con el Principio 13 (información relevante y de calidad).

Condición: La Sociedad no tiene establecidos criterios para definir el tipo de información que se comunica a los grupos de interés internos y externos en atención a su importancia y criticidad.

La Política de Comunicaciones O-CO-01 V04 remite esa definición al Plan de Acción de Comunicaciones y a la Matriz de Comunicaciones del SIG, y se refiere únicamente a la *relevancia* de la información, sin incluir su criticidad. Revisados los soportes documentales aportados, ninguno de ellos, establece dichos criterios:

i. El Plan de acción del Programa de Comunicación estratégica 2026 define productos y canales de comunicación corporativa, orientados a la imagen institucional.
ii. El Cronograma de publicación SIG 2026 programa 180 publicaciones internas sobre los sistemas de gestión, dirigidas exclusivamente a los colaboradores. En el primer semestre de 2026 registra la ejecución de 35 de 78 publicaciones programadas (45%) y 21 sin estado registrado. Dos publicaciones figuran como completadas, aunque sus observaciones indican que no se realizó la difusión.
iii. La Matriz de recolección de información registra los insumos solicitados a 19 proyectos para comunicación externa, sin fechas ni campos de validación por parte de los líderes.

Ninguno de los instrumentos incluye campos de grupo de interés, importancia o criticidad, ni cuenta con código, versión o aprobación. La clasificación de la información por criticidad definida en el Manual M-RI-06 V07 (información pública, clasificada y reservada) no está articulada con ellos.

Como avance institucional, el Informe SCI 2025 registró que la Sociedad tiene definidas y divulgadas las políticas, medios y canales de comunicación externa.

Causa:

i. La política delega los criterios sin definirlos: La Política de Comunicaciones remite a instrumentos operativos que fueron diseñados para programar contenidos y publicaciones, no para establecer criterios de selección de la información. Además, la política solo considera la relevancia y omite la criticidad.
ii. Los instrumentos operativos no están formalizados: El cronograma, la matriz de recolección y el plan de acción no forman parte del Sistema de Gestión, no tienen campos que identifiquen el grupo de interés, la importancia y la criticidad de la información, y no registran aprobación.

iii. No hay articulación con la clasificación de la información**:** No existe coordinación documentada entre el Grupo de Comunicaciones y los responsables del Sistema de Gestión de Seguridad de la Información para que la clasificación definida en el Manual M-RI-06 V07 (Manual de Políticas de Seguridad de la Información) oriente qué información puede comunicarse a cada grupo de interés.
iv. El registro de la ejecución carece de control**:** No se verifica que el estado de las publicaciones en el cronograma corresponda a su ejecución real.

Posible impacto:

i. La selección de la información que se comunica no se fundamenta en su importancia ni en su criticidad.
ii. La comunicación sobre los sistemas de gestión se dirige a los colaboradores, sin cubrir otros grupos de interés internos y externos.
iii. Incumplimiento del numeral 3.4.1.3 de la CE 006/25.

Recomendaciones para GTI y Grupo de Comunicaciones:

i. Definir y documentar en la Política de Información y Comunicación, o en un instrumento derivado y aprobado, los criterios para establecer el tipo de información que se comunica a cada grupo de interés interno y externo, en atención a su importancia y criticidad.
ii. Articular la clasificación de la información del Manual M-RI-06 V07 y del Instructivo I-RI-01 (información pública, clasificada y reservada) con los instrumentos de comunicación, en coordinación con el Oficial de Seguridad de la Información.

9. <u>Canales de quejas y denuncias: exclusividad, anonimato, confidencialidad y garantías para su trámite</u>

Criterios CE 006/25: 3.4.1.4

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
P14 y P15 (líneas de comunicación separadas para la denuncia, internas y externas), en relación con P1 (compromiso con la integridad y los valores éticos, y tratamiento oportuno de las desviaciones).	3.4.1.4 Canales de quejas y denuncias	**3.4.1.4. Canales de comunicación** *Las EV deben contar con canales de comunicación específicos y exclusivos para la recepción de quejas y denuncias contra los funcionarios y administradores de las EV, o contra terceros contratados por las EV, tales como: líneas telefónicas, correos electrónicos, buzones especiales en el sitio web y otros mecanismos digitales, con el fin de que las personas que adviertan o conozcan eventuales irregularidades, incumplimientos normativos, violaciones al código de ética y conducta, u otros hechos o circunstancias que afecten o puedan afectar el adecuado funcionamiento del SCI, los pongan en conocimiento de los órganos competentes de las EV.* *Los canales de comunicación dispuestos para la recepción de quejas y denuncias deben contar con salvaguardas que garanticen el anonimato de los denunciantes y la confidencialidad de la información. Las EV deben diferenciar claramente estos canales de recepción de quejas y denuncias, de los canales de*

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
		formulación de quejas de los consumidores financieros derivadas de las fallas en la prestación de servicios o productos. Para la recepción y tratamiento de las quejas y denuncias se debe garantizar lo siguiente: *a. Protección a denunciantes frente a represalias.* *b. Capacitación a los funcionarios de las EV en esta materia.* *c. Instancias dentro de las EV que asumirán el trámite de las quejas y denuncias.* *d. Procesos eficientes que permitan su trámite de manera oportuna.*

- **Observación Número 8 – Canales de denuncia no diferenciados de los de PQRSDF y sin evidencia de salvaguardas de anonimato, confidencialidad y garantías para su trámite**

Criterio:

i. Circular Básica Jurídica (CE 006/25), Parte I, Título I, Capítulo IV, numeral 3.4.1.4 (Canales de comunicación): *"Las EV deben contar con canales de comunicación específicos y exclusivos para la recepción de quejas y denuncias contra los funcionarios y administradores de las EV, o contra terceros contratados por las EV (…). Los canales de comunicación dispuestos para la recepción de quejas y denuncias deben contar con salvaguardas que garanticen el anonimato de los denunciantes y la confidencialidad de la información. Las EV deben diferenciar claramente estos canales de recepción de quejas y denuncias, de los canales de formulación de quejas de los consumidores financieros (…). Para la recepción y tratamiento de las quejas y denuncias se debe garantizar lo siguiente: a. Protección a denunciantes frente a represalias. b. Capacitación a los funcionarios (…). c. Instancias dentro de las EV que asumirán el trámite (…). d. Procesos eficientes que permitan su trámite de manera oportuna."*

ii. COSO 2013:
   - Principios 14 y 15: Incluyen como punto de enfoque las líneas de comunicación separadas, internas y externas, para la denuncia.
   - Principio 1: *"La organización demuestra compromiso con la integridad y los valores éticos"*. Uno de sus puntos de enfoque es abordar oportunamente las desviaciones

Condición: La Sociedad dispone de canales para la recepción de peticiones, quejas, reclamos y denuncias: atención presencial, líneas telefónicas, formulario web, correos electrónicos y redes sociales. Fueron divulgados a funcionarios y contratistas durante el Semestre I de 2026 (envíos del 17 de marzo y 12 de mayo, según el Cronograma de publicación SIG). Sin embargo:

i. No hay canales específicos y exclusivos para denuncias contra funcionarios, administradores o terceros contratados, diferenciados de los de PQRSDF. La pieza *"¡Conoce nuestros canales de denuncia!"* presenta los mismos medios de las PQRSDF, el buzón quejasreclamosydenuncias@ y el flujo de radicación en LIRA son comunes, y la Política de Comunicaciones O-CO-01 V04 dispone que todas las quejas y denuncias se tramiten por el procedimiento de PQRSDF (P-RC-01).

ii. No se evidenciaron salvaguardas de anonimato y confidencialidad**.** La radicación en LIRA consigna la identificación del remitente.
iii. No se cuenta con evidencia de protección a los denunciantes frente a represalias, de capacitación de los funcionarios en el trámite de denuncias, de la instancia que asume su trámite ni de indicadores de oportunidad.
iv. El Grupo de Servicios Administrativos, responsable de los canales según lo informado por las áreas, no se cuenta con soportes documentales. El Informe SCI 2025 registró como fortaleza la existencia de denuncia anónima y como debilidad la respuesta extemporánea reiterada a las PQRDSF.

Causa:

La Política de Comunicaciones asimila las denuncias a las PQRSDF y las somete a un mismo procedimiento (P-RC-01), sin prever un canal diferenciado, de acuerdo a lo indicado en la Circular:

i. La responsabilidad sobre los canales está distribuida entre el Grupo de Servicios Administrativos (administración, recepción y trámite), el Grupo de Comunicaciones (monitoreo de redes y difusión) y el GTI (buzones de correo). No hay un responsable único que asegure las salvaguardas de anonimato, confidencialidad y protección al denunciante.
ii. No están documentados la instancia de trámite de las denuncias, los tiempos de atención ni los indicadores de oportunidad.
iii. No fue identificado un soporte documental que establezca un procedimiento para el monitoreo de PQRSDF en redes sociales, con tiempos máximos de traslado y radicación ni un registro controlado de los casos.

Efecto:

i. Las denuncias se reciben y tramitan por los mismos medios y procedimiento de las PQRSDF ciudadanas, con registro de la identidad del remitente.
ii. En el primer semestre de 2026 se presentaron demoras entre la recepción y la radicación de los casos detectados en redes sociales, un caso quedó sin radicar al cierre del semestre y el consolidado de seguimiento quedó incompleto.
iii. Exposición de la identidad de los denunciantes.
iv. Pérdida de confianza de funcionarios, contratistas y terceros en los mecanismos de denuncia.
v. Detección tardía de conductas contrarias a la integridad.
vi. Incumplimiento del numeral 3.4.1.4 de la CE 006/25.

Recomendación

i. Ajustar la Política de Comunicaciones para que las denuncias no se tramiten mediante el procedimiento de PQRSDF.
ii. Establecer un canal específico y exclusivo para denuncias (línea ética), diferenciado de los canales de PQRSDF, que permita la denuncia anónima y garantice la confidencialidad de la información y del denunciante. Designar un responsable único de su administración.
iii. Documentar la protección frente a represalias, la instancia responsable del trámite de las denuncias, los tiempos de atención y los indicadores de oportunidad.

iv. En caso de que no se haya efectuado, documentar el procedimiento de monitoreo de PQRSDF en redes sociales, con tiempos máximos de traslado y radicación y un registro controlado con fechas de recepción, traslado, radicación y respuesta.

10. Solicitudes de información de la Junta Directiva sobre el desarrollo y desempeño de los controles internos

Criterios CE 006/25: 4.1.4.1

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
P2 (supervisión del sistema de control interno por parte de la Junta Directiva), en relación con P14 (comunicación con el consejo de administración) y P16 (evaluaciones continuas e independientes).	4.1.4.1 Solicitudes de información de la Junta Directiva	4.1.4. Funciones de la Junta Directiva u órgano que haga sus veces respecto de la información y comunicación *Le corresponde a la JD u órgano que haga sus veces cumplir con las siguientes funciones:* **4.1.4.1.** *Solicitar toda la información que estime necesaria sobre el desarrollo y desempeño de los controles internos para cumplir con sus responsabilidades.*

El numeral 4.1.4.1 de la CE 006/25 asigna a la Junta Directiva la facultad de solicitar toda la información que estime necesaria sobre el desarrollo y desempeño de los controles internos, como parte de la supervisión que le corresponde sobre el Sistema de Control Interno (Principio 2 de COSO 2013). El ejercicio de esa facultad solo puede verificarse cuando las solicitudes y los pronunciamientos de ese órgano quedan documentados, tienen un responsable de atenderlos y cuentan con seguimiento hasta su cierre.

En el presente seguimiento no fue posible verificar el ejercicio de esta facultad durante el Semestre I de 2026. Las áreas consultadas manifestaron reserva sobre las actas de la Junta Directiva, el requerimiento fue trasladado a la Secretaría General de la junta Directiva oficina jurídica el último día del plazo y no se recibió respuesta.

Por otra parte, el Informe Anual de Gestión y Evaluación sobre la Eficacia del SCI – Vigencia 2025 evidenció que existen mecanismos formales de información hacia la Junta, pero también advirtió la necesidad de definir la periodicidad de ciertos reportes y de documentar los pronunciamientos que surjan en ese órgano.

En este contexto, las recomendaciones que se formulan buscan fortalecer la trazabilidad de la relación entre la Junta Directiva y la administración en materia de control interno, y asegurar el acceso de la auditoría interna a la información necesaria para evaluarla, conforme al Estatuto de Auditoría Interna aprobado por la Junta Directiva.

Recomendación a la Junta Directiva

i. Establecer un registro de las solicitudes de información y de los pronunciamientos que formulen la Junta Directiva y sus comités de apoyo sobre el desarrollo y desempeño de los

controles internos. El registro debe incluir el responsable de atenderlos, el plazo y su seguimiento hasta el cierre, conforme al numeral 4.1.4.1 de la CE 006/25.

ii. Definir el requisito y la periodicidad de los reportes que la Junta Directiva requiere sobre el sistema de control interno, en concordancia con la recomendación formulada en el Informe Anual de Gestión y Evaluación sobre la Eficacia del SCI – Vigencia 2025.

11. <u>Comunicación de la Alta Gerencia: Mecanismos de comunicación con las áreas e información a la Junta Directiva sobre los sistemas de información</u>

Criterio CE 006/25: 4.1.4.1

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
Principio 14 de COSO 2013 (Componente Información y Comunicación): "La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del control interno", en sus puntos de enfoque de comunicación interna con las áreas (4.4.4.1) y con el consejo de administración (4.4.4.2). Se relaciona con el Principio 13 (información oportuna y de calidad), con el Principio 2 (supervisión de la Junta Directiva), con el Principio 11 (controles generales sobre la tecnología) y con el Principio 16 (seguimiento mediante indicadores).	4.4.4.1 y 4.4.4.2 Comunicación de la Alta Gerencia	Exige evidenciar los mecanismos de comunicación efectiva entre áreas definidos por la Alta Gerencia y los indicadores de funcionamiento y disponibilidad de los sistemas de información y comunicación reportados a la Junta Directiva. 4.4.4.1. *Establecer mecanismos que garanticen la comunicación efectiva con las diferentes áreas de la EV para obtener de manera oportuna la información necesaria para el cumplimiento de sus funciones.* 4.4.4.2. *Informar a la JD u órgano que haga sus veces, así como a los comités de apoyo, sobre el funcionamiento y disponibilidad de los sistemas de información y comunicación de la EV. Para este efecto, deben establecerse los indicadores correspondientes.*

Frente al numeral 4.4.4.1 de la CE 006/25, la Sociedad cuenta con lineamientos de comunicación interna definidos en la Política de Comunicaciones O-CO-01, aprobada por la Junta Directiva. Durante el Semestre I de 2026 operaron canales de comunicación interna (correo masivo, intranet, pantallas y Viva Engage), según el Cronograma de publicación SIG 2026, que registró la ejecución de 35 de 78 publicaciones programadas. No obstante, estos lineamientos y canales se orientan a la difusión de información hacia los colaboradores. No se evidenciaron mecanismos definidos por la Alta Gerencia que garanticen la obtención oportuna de la información de las áreas para el cumplimiento de sus funciones. Además, la afirmación del GTI según la cual “Office 365 hace parte del inventario de herramientas de comunicación” institucional no corresponde con el inventario aportado. Como antecedente, el Informe SCI 2025 registró la presentación de informes de gestión de riesgos ante la Alta Dirección y recomendó articular el sistema de reporte de las tres líneas de aseguramiento para que esta ejerza el monitoreo.

Frente al numeral 4.4.4.2, el GTI manifestó expresamente que durante el periodo evaluado no envió ningún reporte, acta o comunicación a la Junta Directiva, y que los informes a ese órgano se elaboran cuando este los solicita. En consecuencia, no se informó a la Junta Directiva ni a sus comités de apoyo sobre el funcionamiento y la disponibilidad de los sistemas de información y comunicación, función que

la norma asigna a la Alta Gerencia sin condicionarla a una solicitud previa. Existen indicadores definidos en el contrato con el operador tecnológico (acuerdos de nivel de servicio de disponibilidad con medición mensual) y en el Manual de Políticas de Seguridad de la Información M-RI-06 V07 (indicadores del EDR). Sin embargo, no se cuenta con las mediciones, y el GTI reportó que la serie de disponibilidad del operador no se ha consolidado.

Recomendaciones a GTI y al Grupo de Comunicaciones (en conjunto con la Alta Gerencia)

i. Definir y documentar los mecanismos mediante los cuales la Alta Gerencia obtiene de manera oportuna la información de las áreas para el cumplimiento de sus funciones, tales como informes periódicos de gestión, espacios de seguimiento y reportes por línea de aseguramiento, en concordancia con la recomendación del Informe SCI 2025 sobre la articulación del sistema de reporte de las tres líneas de aseguramiento.
ii. Establecer un reporte periódico de la Alta Gerencia a la Junta Directiva y a sus comités de apoyo sobre el funcionamiento y la disponibilidad de los sistemas de información y comunicación, con una periodicidad definida y sin supeditarlo a la solicitud de ese órgano, conforme al numeral 4.4.4.2 de la CE 006/25.
iii. Consolidar los indicadores que soporten dicho reporte, a partir de las mediciones mensuales de disponibilidad exigibles al operador tecnológico según los acuerdos de nivel de servicio contratados y de los indicadores definidos en el Manual M-RI-06 V07, y conservar la serie histórica de sus resultados.
iv. Incorporar en el inventario de sistemas de información las herramientas de comunicación institucional que soportan la operación de la Sociedad, en particular la plataforma Office 365.

12. Socialización de las políticas y decisiones de la Junta Directiva a los funcionarios según sus roles y responsabilidades

Criterio CE 006/25: 4.4.4.3

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
Principio 14 de COSO 2013 (Componente Información y Comunicación): "La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del control interno". Se relaciona con el Principio 12 (despliegue de las políticas mediante procedimientos) y con los Principios 3 y 5 (estructuras, roles y responsabilidades a nivel de control interno).	4.4.4.3	4.4.4. Funciones de la Alta Gerencia respecto de la información y comunicación *Le corresponde a la AG cumplir con las siguientes funciones:* **4.4.4.3.** *Comunicar las políticas y decisiones adoptadas por la JD u órgano que haga sus veces, a los funcionarios de la EV de conformidad con sus roles y responsabilidades.*

El numeral 4.4.4.3 de la CE 006/25 asigna a la Alta Gerencia la función de comunicar a los funcionarios las políticas y decisiones adoptadas por la Junta Directiva, de conformidad con sus roles y responsabilidades. Esta función es la que permite que las directrices del máximo órgano de dirección se conozcan,

se apliquen en los procesos y sean exigibles a quienes deben cumplirlas (Principios 14, 12, 3 y 5 de COSO 2013).

En el presente seguimiento se observó (con base en los soportes documentales aportados) que la Sociedad cuenta con canales de comunicación interna en operación y con un cronograma de publicaciones para los sistemas de gestión, en el que se registró la divulgación de la Política Antisoborno durante el Semestre I de 2026. Sin embargo, no se evidenció la socialización del Manual de Políticas de Seguridad de la Información aprobado por la Junta Directiva en enero de 2026, la divulgación programada de la Política del SIAR no se inició y las publicaciones se dirigen de manera general a los colaboradores, sin diferenciarse según sus roles y responsabilidades. Adicionalmente, las áreas clasificaron esta evidencia como información reservada de la Junta Directiva, aunque corresponde a los canales que administra el Grupo de Comunicaciones. El Informe SCI 2025 ya había advertido la necesidad de fortalecer la divulgación e interiorización de las responsabilidades de cada dependencia frente a los documentos del SIAR y al esquema de líneas de aseguramiento.

Recomendaciones a GTI y al Grupo de Comunicaciones (en conjunto con la Alta Gerencia)

i. Establecer, dentro de la Política de Comunicaciones o en un procedimiento derivado, la socialización obligatoria de las políticas y decisiones adoptadas por la Junta Directiva a los funcionarios, con un plazo definido a partir de su aprobación y con indicación de los destinatarios según sus roles y responsabilidades.
ii. Socializar el Manual de Políticas de Seguridad de la Información M-RI-06 V07, aprobado por la Junta Directiva el 28 de enero de 2026, y ejecutar las divulgaciones programadas y no iniciadas de la Política del SIAR y del SGSI.
iii. Conservar la evidencia de cada socialización (pieza, fecha de envío, canal y destinatarios) y verificar periódicamente su cumplimiento. Para ello, coordinar con la Secretaría General que las decisiones de la Junta Directiva que requieran socialización sean informadas oportunamente al Grupo de Comunicaciones.

13. Monitoreo de la Alta Gerencia al funcionamiento de los controles y corrección de las fallas

- **Criterios CE 006/25: 4.4.4.5**

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
Principios 16 y 17 de COSO 2013 (Componente Actividades de Monitoreo): "La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema de control interno están presentes y en funcionamiento", y "La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la	4.4.4.5 Monitoreo de la Alta Gerencia al funcionamiento de los controles y corrección de las fallas	4.4.4. Funciones de la Alta Gerencia respecto de la información y comunicación *Le corresponde a la AG cumplir con las siguientes funciones:* 4.4.4.5. *Monitorear el funcionamiento de los controles descritos en el subnumeral 3.3. del presente Capítulo, y adoptar medidas que resulten necesarias para corregir las fallas que se presenten.*

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
alta dirección y el consejo, según corresponda". Se relaciona con los Principios 10, 11 y 12 (actividades de control descritas en el subnumeral 3.3) y con el Principio 5 (rendición de cuentas sobre el funcionamiento de los controles).		

El numeral 4.4.4.5 de la CE 006/25 asigna a la Alta Gerencia el monitoreo del funcionamiento de las actividades de control y la adopción de las medidas necesarias para corregir sus fallas, en concordancia con los Principios 16 y 17 de COSO 2013. Frente al tema, se identificó que el Comité Institucional de Gestión y Desempeño, recibió durante el Semestre I de 2026 reportes de avance del PETI, del SGSI y del PCN (actas n.° 97 de enero, 102 de mayo, 103 de julio y 105 de 2026), lo que constituye un monitoreo parcial, por parte de esta instancia de Alta Gerencia, circunscrito a los controles de tecnología del subnumeral 3.3.4. No obstante, no se evidenció que dicho monitoreo cubriera la totalidad de los controles del subnumeral 3.3 (ambiente de control, evaluación de riesgos, actividades de control general e información y comunicación), ni que sus resultados se hayan consolidado o comunicado formalmente a la Junta Directiva.

El Informe SCI 2025 ya había identificado fallas de control sin corrección evidenciada, planes de mejoramiento con actividades vencidas y la necesidad de articular el reporte de las tres líneas de aseguramiento para que la Alta Dirección ejerza su función de monitoreo.

Recomendaciones a GTI y al Grupo de Comunicaciones (en conjunto con la Alta Gerencia)

i. Establecer un mecanismo documentado de monitoreo por parte de la Alta Gerencia al funcionamiento de los controles del subnumeral 3.3. Este debe consolidar periódicamente, en el Comité de Presidencia o en la instancia que se defina, los reportes de la primera y la segunda línea de aseguramiento sobre los controles que presentan fallas, en concordancia con la recomendación del Informe SCI 2025 sobre la articulación del sistema de reporte de las tres líneas de aseguramiento.
ii. Dejar constancia en las actas de dicha instancia de las fallas de control analizadas, las medidas correctivas adoptadas, sus responsables y plazos, y hacer seguimiento a su cierre.
iii. Priorizar el cierre de las fallas de control identificadas en la vigencia 2025, en particular el incumplimiento de respaldos, las deficiencias en roles y perfiles del ERP, las fallas de validación de consecutivos y la elaboración del informe semestral de monitoreo del SGSI, y fortalecer el seguimiento a los planes de mejoramiento con actividades vencidas.

14. <u>Entrega oportuna de información a la Junta Directiva y a los órganos de gobierno: antelación definida en el reglamento</u>

- **Criterios CE 006/25: 4.4.4.6**

Principio COSO	Criterio CE 006/25	Solicitud (Matriz de orientación)
Principio 14 de COSO 2013 (Componente Información y Comunicación): "La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del control interno", en su punto de enfoque de comunicación con el consejo de administración. Se relaciona con el Principio 13 (información relevante y oportuna) y con el Principio 2 (supervisión de la Junta Directiva).	4.4.4.6	4.4.4. Funciones de la Alta Gerencia respecto de la información y comunicación *Le corresponde a la AG cumplir con las siguientes funciones:* **4.4.4.6.** *Preparar y entregar con la antelación definida en su reglamento, a la JD u órgano que haga sus veces y a los diferentes órganos de gobierno, la información necesaria sobre los temas a tratar en cada reunión ordinaria o extraordinaria del respectivo órgano colegiado.*

El numeral 4.4.4.6 de la CE 006/25 exige a la Alta Gerencia preparar y entregar a la Junta Directiva y a los órganos de gobierno, con la antelación definida en su reglamento, la información necesaria para cada sesión. Esto permite a esos órganos deliberar y decidir con conocimiento suficiente, en ejercicio de la supervisión que les corresponde (Principio 2 de COSO 2013). En el presente seguimiento no fue posible verificar el cumplimiento de esta función. No se cuenta con el reglamento que define la antelación ni las convocatorias del periodo, y la solicitud fue trasladada a la Secretaría General el último día del plazo, sin respuesta. El Informe SCI 2025 ya había recomendado definir el requisito y la periodicidad de la información que se presenta a la Junta Directiva.

Recomendaciones

1. Verificar que el reglamento de la Junta Directiva y de sus comités de apoyo defina expresamente la antelación con la que debe entregarse la información de cada sesión ordinaria y extraordinaria. Divulgar dicha antelación a las áreas responsables de preparar la información.
2. Dejar constancia, en cada convocatoria, de la fecha de envío de la información a los miembros del órgano colegiado y de la fecha de la sesión, de manera que pueda verificarse el cumplimiento de la antelación reglamentaria.
3. Establecer un calendario de preparación de la información para las sesiones de la Junta Directiva que defina, por tema, el área responsable y la fecha límite de entrega a la Secretaría General, en concordancia con la recomendación del Informe SCI 2025.

Consolidado de observaciones:

N.°	Apartado del informe	Criterio CE 006/25	Observación / resultado
1	Política de Información y Comunicación: contenido mínimo y aprobación por la Junta Directiva	3.4.1 y 4.1.1 lit. m)	Observación N.° 1 – Política de Información y Comunicación sin la totalidad de los contenidos mínimos exigidos por la CE 006/25.
2	Calidad de la información: metodología de validación para garantizar su exactitud y actualización	3.4.1.1	Observación N.° 2 – Ausencia de una metodología de validación de calidad de datos aprobada y aplicada que garantice la exactitud y la actualización de la información.

N.°	Apartado del informe	Criterio CE 006/25	Observación / resultado
3	Calidad de la información: indicadores para medir su exactitud, actualización, accesibilidad y protección	3.4.1.1	Observación N.° 3 – Ausencia de indicadores medidos y reportados sobre los atributos de calidad de la información.
4	Sistemas de información: capacidad para obtener, capturar y procesar datos de fuentes internas y externas seguras	3.4.1.2	Observación N.° 4 – Inventario de sistemas de información sin capacidad por sistema y sin identificación de las fuentes de información del SIAR.
5	Aprobación por la Junta Directiva de la PSI, el PETI y la Política de Información y Comunicación	4.1.1 lit. h), l) y m)	Observación N.° 5 – Plan Estratégico de Tecnología sin aprobación de la Junta Directiva y deficiencias de trazabilidad en el registro de las aprobaciones.
6	Política de Seguridad de la Información: vigencia y cumplimiento de los seis controles mínimos	3.1.8	Sin observación. El diseño de los controles se encuentra documentado en la Política O-RI-01, el Manual M-RI-06 y las obligaciones contractuales del operador tecnológico.
7	Plan Estratégico de Tecnología: vigencia y contenido mínimo de sus cinco componentes	3.1.17	Observación N.° 6 – Plan Estratégico de Tecnología con cobertura parcial de los contenidos mínimos del numeral 3.1.17.
8	Criterios de selección de la información según su importancia y criticidad	3.4.1.3	Observación N.° 7 – Ausencia de criterios para definir el tipo de información que se comunica a los grupos de interés según su importancia y criticidad.
9	Canales de quejas y denuncias: exclusividad, anonimato, confidencialidad y garantías para su trámite	3.4.1.4	Observación N.° 8 – Canales de denuncia no diferenciados de los de PQRSDF y sin evidencia de salvaguardas de anonimato, confidencialidad y garantías para su trámite.
10	Solicitudes de información de la Junta Directiva sobre el desarrollo y desempeño de los controles internos	4.1.4.1	Recomendación
11	Comunicación de la Alta Gerencia: mecanismos de comunicación con las áreas e información a la Junta Directiva sobre los sistemas de información	4.4.4.1 y 4.4.4.2	Recomendación
12	Socialización de las políticas y decisiones de la Junta Directiva a los funcionarios según sus roles y responsabilidades	4.4.4.3	Recomendación
13	Monitoreo de la Alta Gerencia al funcionamiento de los controles y corrección de las fallas	4.4.4.5	Recomendación
14	Entrega oportuna de información a la Junta Directiva y a los órganos de gobierno	4.4.4.6	Recomendación.

CONCLUSIONES

Como resultado del seguimiento al cumplimiento del Componente 4 (Información y Comunicación) del Capítulo IV de la Circular Básica Jurídica (CE 006/25) de la Superintendencia Financiera de Colombia, correspondiente al Semestre I de 2026, la Asesoría de Control Interno concluye que ENTerritorio S.A. cuenta con elementos documentados y en operación que soportan el componente. Sin embargo, estos elementos no cubren de manera integral los requerimientos de la norma, y persisten brechas en la formalización, la medición y el reporte de la información, así como en los canales de denuncia y en la trazabilidad de la información de los órganos de gobierno.

Fortalezas identificadas: La Sociedad cuenta con:

a. Una Política de Comunicaciones aprobada por la Junta Directiva y con control documental;
b. Una Política Institucional de Seguridad de la Información y un Manual de Políticas de Seguridad de la Información, aprobados por la Junta Directiva y vigentes durante el periodo, que, junto con las obligaciones contractuales del operador tecnológico, documentan el diseño de los controles mínimos exigidos por el numeral 3.1.8;
c. Un Plan Estratégico de Tecnología 2024-2027 vigente y publicado, con un portafolio de proyectos priorizados;
d. Un inventario de aplicaciones;
e. Canales de comunicación interna en operación y canales de recepción de peticiones, quejas, reclamos y denuncias divulgados durante el semestre.

Como avance institucional, el Informe Anual de Gestión y Evaluación sobre la Eficacia del SCI – Vigencia 2025 registró una calificación del 86% para el Componente de Información y Comunicación.

De las brechas en la política y en la calidad de la información: La Política de Comunicaciones no contiene la totalidad de los contenidos mínimos exigidos por el numeral 3.4.1. Los contenidos del componente se encuentran dispersos en documentos de distinta naturaleza y nivel de aprobación, sin una política integradora. En relación con la calidad de la información, la Sociedad: No cuenta con una metodología de validación de calidad de datos aprobada y aplicada, no reporta indicadores que midan la exactitud, la actualización, la accesibilidad y la protección de la información y tiene el Manual de Políticas de Gobierno de Datos pendiente de aprobación.

A su vez, el inventario de sistemas de información no registra la capacidad de los sistemas frente a los volúmenes de datos que procesan, no identifica las fuentes de información del SIAR y presenta debilidades de actualización y control documental.

Frente a las brechas en la planeación tecnológica y en la comunicación con los grupos de interés: El Plan Estratégico de Tecnología: No fue aprobado por la Junta Directiva, conforme lo exige el numeral 4.1.1 lit. l), sino por el Comité Institucional de Gestión y Desempeño, cubre parcialmente los contenidos mínimos del numeral 3.1.17 y Presenta debilidades en su seguimiento.

Por otra parte, la Sociedad no ha establecido criterios para definir el tipo de información que se comunica a cada grupo de interés según su importancia y criticidad. Los canales de denuncia comparten medios y procedimiento con las PQRSDF, sin evidencia de salvaguardas de anonimato, confidencialidad y protección a los denunciantes, en los términos del numeral 3.4.1.4.

De la información de los órganos de gobierno. No se obtuvo evidencia, para el periodo evaluado, de los siguientes aspectos: i) Las solicitudes de información de la Junta Directiva sobre los controles internos, ii) Los mecanismos de la Alta Gerencia para obtener información de las áreas, iii) El reporte a la Junta Directiva sobre el funcionamiento y disponibilidad de los sistemas de información, (que el GTI manifestó no haber realizado), iv) La socialización a los funcionarios de las políticas y decisiones de la Junta Directiva, y v) La entrega anticipada de información a la Junta Directiva. Frente al monitoreo de la Alta Gerencia a los controles, se identificó evidencia de un monitoreo parcial a través del Comité Institucional de Gestión y Desempeño (actas 97, 102, 103 y 105), circunscrito a los controles de tecnología del subnumeral 3.3.4, sin que se evidenciara que cubriera la totalidad del subnumeral 3.3 ni que sus resultados se hayan consolidado o comunicado formalmente a la Junta Directiva. No obstante lo anterior, la ACI reiteró lo indicado en el Informe Anual de Gestión y Evaluación sobre la Eficacia del SCI – Vigencia 2025, dada la pertinencia del análisis frente a los aspectos no evidenciados en el presente seguimiento.

Las áreas evaluadas manifestaron no tener acceso a esta información por su carácter reservado. Al respecto, la Asesoría de Control Interno precisó que dicha reserva no es oponible a la auditoría interna, conforme al numeral 4.1 del Estatuto de Auditoría Interna aprobado por la Junta Directiva.

Recomendación general. En consecuencia, se formularon 8 observaciones y recomendaciones orientadas a: Integrar y formalizar la Política de Información y Comunicación con sus contenidos mínimos, documentar y aplicar los mecanismos de validación y medición de la calidad de la información, actualizar el inventario de sistemas de información, someter a aprobación de la Junta Directiva el Plan Estratégico de Tecnología; establecer criterios de selección de la información por grupo de interés, implementar un canal de denuncias exclusivo y con garantías y fortalecer la trazabilidad y el reporte de la información entre la Alta Gerencia y la Junta Directiva.

Atentamente, ORLANDO CORREA NUÑEZ

Firmado digitalmente por ORLANDO CORREA NUÑEZ
Fecha: 2026.10.26 09:01:34 -05'00'

ORLANDO CORREA NÚÑEZ
Asesor con Funciones de Control Interno
Elaboró: **Luisa Fernanda Ríos Giraldo – contratista – Asesoría de Control Interno**