RESOLUCIÓN No. **8371** DE 2026

*«Por la cual se resuelve el recurso de reposición interpuesto por **ESTRATEC S.A.S.** en contra de la Resolución CRC 8283 de 2026, por la cual se recupera el código corto **898988**, para la provisión de contenidos y aplicaciones a través de SMS o USSD»*

LA COORDINACIÓN DEL GRUPO INTERNO DE TRABAJO DE RELACIONES CON GRUPOS DE VALOR DE LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES

En ejercicio de sus facultades legales, y en especial las que le confiere los numerales 12 y 13 del artículo 22 de la Ley 1341 de 2009, el artículo 2.2.12.1.1.1 del Decreto 1078 de 2015, el artículo 6.1.1.9 de la Resolución CRC 5050 de 2016, el artículo 7 de la Resolución CRC 580 de 2025 y,

CONSIDERANDO

1. ANTECEDENTES

Mediante la Resolución CRC 8283 del 7 de julio de 2026, la Comisión de Regulación de Comunicaciones, (en adelante **CRC**), resolvió recuperar el código corto **898988**, el cual había sido asignado a **ESTRATEC S.A.S.**[1], identificada con el NIT 830.121.553-1, en adelante **ESTRATEC**, por haberse configurado la causal de recuperación establecida en el numeral 6.4.3.2.8 del artículo 6.4.3.2 de la Resolución CRC 5050 de 2016, la cual establece que procederá la recuperación del código corto «Cuando a través de esta numeración se envíen mensajes en nombre de terceros que no hayan autorizado expresamente y por escrito su envío o su contenido».

La Resolución CRC 8283 de 2026 fue notificada personalmente a **ESTRATEC**, el 7 de julio de 2026. Dentro del término establecido[2], **ESTRATEC** presentó recurso de reposición en contra de esta, el cual fue radicado internamente bajo el número 2026817154 del 23 de julio de 2026.

Posteriormente, el 24 de julio de 2026, presentó un anexo bajo el radicado interno 2026817200, con el asunto «Re: Respuesta Comunicación - Aplicación numeral 2.1.19.7.6 del artículo 2.1.19.7 de la Resolución CRC 5050 de 2016-CODIGO CORTO 87701» mediante el cual presentó Anexo No. 1 al recurso de reposición contra la Resolución CRC 8283 de 2026. Sin embargo, este pronunciamiento fue presentado una vez vencido el término para interponer el recurso de conformidad con lo previsto en el artículo 76 y en el numeral 1 del artículo 77 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA). En consecuencia, por su presentación extemporánea, no será objeto de análisis al resolver el recurso de reposición.

Por su parte, el recurso de reposición interpuesto por **ESTRATEC** el 23 de julio de 2026, cumple con lo establecido en los artículos 76 y 77 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA), esta Comisión procederá con su análisis y estudio.

2. DEL RECURSO DE REPOSICIÓN INTERPUESTO

Antes de que esta Comisión se pronuncie sobre los argumentos expuestos por **ESTRATEC** en su recurso, es necesario señalar que el recurso de reposición es un medio jurídico a través del cual la parte interesada controvierte las decisiones o actos que ponen fin a las actuaciones administrativas, en el caso puntual, la decisión de recuperar un código corto, para que el funcionario que dictó la decisión revise nuevamente su contenido y, si lo considera legal y

[1] Resolución CRC 5058 del 09 de diciembre 2016
[2] El término para presentar el recurso de reposición vencía el 23 de julio de 2026.

oportuno, lo aclare, modifique o revoque[3]. Así, frente al recurso de reposición, la doctrina ha manifestado que «(…) se ha considerado históricamente como recurso connatural al Estado de derecho; en especial al derecho fundamental a la controversia de toda decisión administrativa. Se funda esta tesis en el criterio de que no existe acto administrativo sin control, se trata, pues, del más elemental de todos los recursos para garantizar el principio de la contradicción y debido proceso (…)».

ESTRATEC en su escrito de reposición contra la Resolución CRC 8283 de 2026, presenta los antecedes del caso, y solicita su revocatoria integral por lo expuesto en los siguientes cargos: i) falsa motivación general: imposición de un régimen de responsabilidad objetiva no previsto en la regulación; ii) inexistencia de la causal 6.4.3.2.8 – interpretación objetiva e irrazonable de la obligación de autorización; iii) inexistencia de la causal 6.4.3.2.8 – la única autorización para el envío de mensajes de texto debe ser otorgada por Nutresa; iv) desproporción de la medida y uso cuasi-sancionatorio de la recuperación; v) improcedencia del traslado a la Superintendencia de Industria y Comercio, a la Fiscalía General de la Nación y al Ministerio de Tecnologías de la Información y las Comunicaciones.

De esta manera, para resolver el recurso de reposición interpuesto, se analizarán los cargos formulados en este, revisando nuevamente la información que reposa en el expediente. A continuación, los argumentos expuestos por **ESTRATEC** y las consideraciones de la **CRC** sobre cada uno de estos:

(i) FALSA MOTIVACIÓN GENERAL: IMPOSICIÓN DE UN RÉGIMEN DE RESPONSABILIDAD OBJETIVA NO PREVISTO EN LA REGULACIÓN

ESTRATEC sostiene que la resolución impugnada incurre en falsa motivación al fundamentar su decisión en un régimen de responsabilidad objetiva que, a su juicio, carece de sustento en la Resolución CRC 5050 de 2016 y en el ordenamiento jurídico colombiano. Asimismo, afirma que en la Resolución CRC 8283 de 2026 no se controvirtió su manifestación de que nunca tuvo relación contractual, comercial ni de ninguna otra naturaleza con **BANCO POPULAR** en conexión con el código corto **898988**.

Al respecto, señala que la CRC limitó su pronunciamiento a indicar: «Así, aunque ESTRATEC haya señalado que no autorizó, promovió ni consintió el envío de comunicaciones en nombre del BANCO POPULAR y que adoptó medidas posteriores como la inactivación de cuentas, fortalecimiento de controles y monitoreo de usos anómalos, durante la actuación administrativa no se acreditó la existencia de una autorización previa, expresa y por escrito otorgada por dicha entidad para el envío de mensajes en su nombre».

En ese sentido, **ESTRATEC** reitera que, como indicó en sus observaciones del 5 de junio de 2026, su única relación contractual relacionada con las quejas presentadas el 23 de abril de 2026 era con **NUTRESA,** y que nunca celebró un acuerdo comercial con el **BANCO POPULAR** asociado al código corto **898988** que hiciera necesaria dicha autorización.

Explica que la referencia al banco en los mensajes no obedeció a una decisión de **ESTRATEC** ni de **NUTRESA**, sino a terceros no autorizados que utilizaron indebidamente las credenciales API de **NUTRESA** para introducir contenido fraudulento de phishing y/o smishing. Según el análisis forense adelantado por **ESTRATEC,** expone que la cuenta «14774 Grupo Nutresa_OTP», con usuario API «api.vr3tc», fue utilizada para los envíos fraudulentos entre el 16 y el 17 de abril de 2026, durante el periodo de exposición de las credenciales. Los mensajes imitaban comunicaciones del **BANCO POPULAR** e incluían enlaces acortados a páginas falsas destinadas a sustraer datos bancarios.

Afirma que el análisis atribuyó el incidente al abuso de las credenciales de **NUTRESA,** sin vulneración, intrusión o compromiso de la infraestructura, sistemas o datos propios de **ESTRATEC,** ni afectación de información bajo su custodia relacionada con **BANCO POPULAR**. Añade que no se encontraron elementos para atribuir a **NUTRESA** responsabilidad o negligencia en la exposición de sus credenciales. Destaca que la detección y contención ocurrieron en pocas

[3] López Blanco, Hernán F. «Instituciones de Derecho Procesal Civil Colombiano», Tomo I, Novena Edición, Bogotá - Colombia, 2005. p 749. «Sin duda alguna la reposición, junto con el recurso de apelación, constituyen los dos más importantes, por ser los que con mayor frecuencia utilizan las partes, de ahí el interés de conocer con el detalle los mismos. Este recurso busca que el mismo funcionario que profirió la decisión sea el que vuelva sobre ella y, si es del caso reconsiderarla, en forma total o parcial, lo haga; es requisito necesario para su viabilidad, que se motive el recurso al ser interpuesto, esto es, que por escrito o verbalmente si es en audiencia o diligencia, se le expongan al juez las razones por las cuales se considera que su providencia está errada, con el fin de que proceda a modificarla o revocarla, por cuanto es evidente que si el juez no tiene esa base, le será difícil, por no decir imposible, entrar a resolver.»

horas, mediante la suspensión y rotación inmediata de las credenciales comprometidas, y que los controles preventivos bloquearon los envíos de prueba del atacante, evitando una escalada mayor, sin fuga de datos ni afectación de la continuidad del servicio a otros clientes.

La sociedad sostiene que la resolución impugnada no controvierte ni desvirtúa estos hechos, pero parece considerarlos irrelevantes. Ubica allí el vicio de falsa motivación denunciado, pues considera que, al afirmar que su condición de proveedor tecnológico, la intervención del cliente en los contenidos y la exposición de las credenciales no la eximen de responsabilidad, la decisión elimina la imputación subjetiva y convierte la causal 6.4.3.2.8 en un mecanismo de responsabilidad objetiva y absoluta, ajeno a los principios de razonabilidad, proporcionalidad e imputabilidad que invoca con fundamento en el artículo 3 del CPACA.

Argumenta que ese razonamiento exigiría al asignatario anticipar qué entidad sería suplantada por un tercero y obtener previamente su autorización para un envío que nunca solicitó, diseñó ni quiso realizar. Considera que se trata de una carga jurídica y materialmente imposible, contraria al principio según el cual nadie está obligado a lo imposible y carente de fundamento en la Resolución CRC 5050 de 2016, la Ley 1341 de 2009 y el ordenamiento jurídico colombiano.

Finalmente, sostiene que la causal busca sancionar el uso indebido del recurso por su titular o por quienes actúan bajo su autorización, y no la victimización del titular por conductas delictivas de terceros. Por ello, afirma que equiparar a **ESTRATEC**, como víctima de un acceso no autorizado mediante credenciales comprometidas, con un asignatario que voluntariamente envía mensajes sin autorización desnaturaliza la causal y establece una responsabilidad objetiva y absoluta que la Resolución CRC 5050 de 2016 no contempla ni autoriza.

- **Consideraciones de la CRC**

Frente a este argumento, esta Comisión considera necesario precisar que las actuaciones de recuperación de códigos cortos no son de carácter sancionatorio.

Lo anterior, toda vez que la recuperación de recursos de identificación corresponde a una materialización de la función de administración de los recursos de identificación y en la verificación de una causal expresamente prevista en la regulación vigente. Los numerales 12 y 13 del artículo 22 de la Ley 1341 de 2009 y el artículo 2.2.12.1.2.5 del Decreto 1078 de 2015 sustentan la administración y recuperación de estos recursos públicos, cuya asignación no confiere propiedad al asignatario.

Así las cosas, no es posible afirmar que la recuperación de un código corto en virtud de la configuración de las causales dispuestas en la regulación se pueda calificar como una sanción. En esa medida, la decisión de recuperación de un código corto no requiere que la CRC haga un análisis de responsabilidad subjetiva.

En definitiva, las actuaciones administrativas de recuperación de recursos de identificación se enmarcan únicamente en el ejercicio de la facultad de administración de estos recursos, a cargo de la CRC, y no se corresponden a las características propias del ejercicio de la potestad sancionatoria. En particular, dichas actuaciones no tienen por objeto determinar la comisión de una conducta susceptible de sanción ni exigen la concurrencia de los elementos propios del derecho sancionador como la atribución de una competencia legal expresa, la tipicidad, la antijuridicidad y la culpabilidad de la conducta, la existencia de un procedimiento previo orientado a garantizar el debido proceso y la observancia del principio de proporcionalidad entre la conducta y la sanción.

Por este motivo, no es razonable, en ninguna circunstancia, exigir de esta Comisión la verificación del cumplimiento de las condiciones excepcionales que permiten la aplicación de un régimen de responsabilidad objetiva[4] en el marco del desarrollo de una actuación administrativa de recuperación de códigos cortos.

Asimismo, es de indicar que la decisión sobre la continuidad de la asignación del recurso de identificación tiene un objeto diferente de la determinación de responsabilidad por la comisión de una conducta fraudulenta. Por consiguiente, la afirmación de que **ESTRATEC** no diseñó ni consintió los mensajes de texto (SMS) debe examinarse atendiendo al objeto de la actuación administrativa de recuperación y la causal objeto de análisis, sin equiparar esta con un procedimiento destinado a sancionarla como autora del ataque informático y/o el determinar que

[4] Corte Constitucional, Sentencia C-616 de 2002.

fue víctima de una falla en sus sistemas de seguridad que derivo en el envío de SMS a usuarios del servicio de telecomunicaciones móviles, sobre lo cual esta Comisión carece de competencias.

El numeral 6.4.3.2.8 del artículo 6.4.3.2 de la Resolución CRC 5050 de 2016 contempla la recuperación cuando se envían, mediante la numeración asignada, mensajes en nombre de terceros que no han autorizado expresamente y por escrito su envío o contenido. Su texto no condiciona la configuración de la causal a la existencia de una relación contractual entre el asignatario y el tercero suplantado, ni exige que el primero haya elaborado personalmente los mensajes de texto (SMS). Incorporar esas condiciones supondría restringir el supuesto regulatorio a circunstancias que la regulación vigente no contempla. Por ello, la ausencia de vínculo comercial entre **ESTRATEC** y el **BANCO POPULAR** no desvirtúa, por sí misma, la causal: lo que corresponde establecer es si el recurso fue utilizado para enviar comunicaciones presentadas como provenientes del banco y si este autorizó su envío o contenido.

En el caso concreto, el fundamento probatorio no se limita a que **ESTRATEC** hubiera omitido aportar una autorización con el **BANCO POPULAR**. La resolución identifica la comunicación de **BANCO POPULAR**, radicada bajo el número 2026808792 del 23 de abril de 2026, en la que la entidad negó expresamente haber autorizado los mensajes de texto (SMS) y aportó capturas de pantalla. A ello se suma que la explicación de la recurrente reconoce el envío de comunicaciones fraudulentas mediante la cuenta de su cliente. Así, su argumento controvierte las consecuencias jurídicas de esos hechos, pero no niega la utilización del código corto para cursar los mensajes de texto (SMS) ni acredita consentimiento del banco.

Desde el punto de vista técnico, el acceso a una plataforma mediante credenciales API y la autorización para enviar mensajes en nombre de una entidad son aspectos diferentes. Según la explicación aportada por **ESTRATEC**, los atacantes utilizaron las credenciales de una cuenta legítima de **NUTRESA**. De ese relato se desprende que la identificación de la cuenta utilizada permite explicar el mecanismo del incidente, pero no acredita que **BANCO POPULAR** hubiera autorizado los contenidos. Asimismo, que no se hubiera comprometido la infraestructura propia de **ESTRATEC** es compatible con que su servicio de mensajería hubiera sido utilizado indebidamente a través de credenciales expuestas. Por tanto, el hecho de que sus sistemas hayan sido vulnerados no desvirtúa que los mensajes objeto de la actuación administrativa hayan sido enviados a través de su plataforma.

En igual sentido, la ausencia de extracción de información bajo custodia de **ESTRATEC** y la continuidad del servicio a los demás clientes describen el alcance del incidente, pero no desvirtúan la suplantación alegada. Conforme al propio relato de la recurrente, los mensajes dirigían a los destinatarios hacia páginas falsas para obtener sus datos bancarios. Ese mecanismo no requiere que previamente se hayan extraído datos del banco desde los sistemas del integrador. De esta manera, la afirmación de que no existió fuga de información en la plataforma responde a un aspecto técnico distinto del uso del código corto para distribuir mensajes que aparentaban proceder de **BANCO POPULAR.**

Tampoco puede aceptarse que el modelo Software as a Service (SaaS) excluya, por su sola naturaleza, las obligaciones regulatorias del asignatario. El artículo 2.1.18.6 de la Resolución CRC 5050 de 2016, modificado por la Resolución CRC 7356 de 2024, exige expresamente a los PCA e integradores tecnológicos asignatarios de códigos cortos emplear herramientas para prevenir fraudes mediante SMS o USSD y efectuar controles periódicos sobre su efectividad. Esta disposición evidencia que la función tecnológica de intermediación está comprendida en el ámbito de prevención regulatoria, aunque el integrador no produzca directamente los contenidos.

En cuanto a la supuesta imposibilidad de obtener anticipadamente autorizaciones de todas las entidades que pudieran ser suplantadas, el argumento atribuye a la regulación un alcance que no se desprende de ella. La condición de autorización se refiere a los terceros en cuyo nombre se envían los mensajes, no a la totalidad de entidades públicas y privadas existentes. El análisis recae sobre comunicaciones concretas cursadas mediante el recurso asignado. En consecuencia, la CRC no exige anticipar la identidad que seleccionaría un delincuente; verifica si los mensajes efectivamente enviados reunían la condición regulatoria. La intervención del atacante explica, según la recurrente, cómo se produjeron los envíos, pero no convierte esos mensajes en comunicaciones autorizadas ni demuestra que la exigencia normativa sea imposible de cumplir.

Las medidas de suspensión de cuentas, rotación de credenciales y bloqueo de envíos de prueba deben valorarse por su alcance de contención y prevención de nuevos eventos, lo cual hace parte de las obligaciones que se le atribuyen al asignatario, de acuerdo con lo establecido en el artículo 2.1.18.6 de la Resolución CRC 5050 de 2016. Sin embargo, su adopción no modifica las

condiciones en que se enviaron los mensajes ya recibidos por los usuarios. Tampoco el bloqueo de determinados intentos permite concluir que todos los envíos no autorizados fueron impedidos, pues el propio recurso reconoce que algunos se materializaron. Esto no equivale a considerar irrelevante la reacción de **ESTRATEC**: significa distinguir entre la eficacia de las medidas posteriores y su capacidad para desvirtuar los hechos que dieron lugar a la actuación.

Finalmente, el reproche de falsa motivación exige examinar si la decisión se sustentó en hechos inexistentes, en una apreciación equivocada de estos o en la omisión de circunstancias probadas determinantes para resolver. Bajo ese examen, la explicación del incidente informático no demuestra, por sí sola, que sean falsos los hechos relativos al envío de mensajes y a la ausencia de autorización del banco. La respuesta al cargo debe apoyarse en esa correspondencia entre los hechos acreditados y la causal aplicada, valorando expresamente los soportes del recurso. La condición de víctima que invoca **ESTRATEC** no excluye automáticamente la evaluación regulatoria del uso del código corto, así como la ocurrencia del ataque tampoco autoriza a presumir su culpabilidad en el fraude.

En consecuencia, las razones generales de inconformidad no tienen vocación de prosperar ni proporcionan fundamento para revocar la Resolución CRC 8283 de 2026.

(ii) INEXISTENCIA DE LA CAUSAL 6.4.3.2.8 – INTERPRETACIÓN OBJETIVA E IRRAZONABLE DE LA OBLIGACIÓN DE AUTORIZACIÓN

ESTRATEC sostiene que la CRC aplica la causal 6.4.3.2.8 de la Resolución CRC 5050 de 2016 bajo una lógica puramente objetiva, al considerar suficiente la ausencia de una autorización expresa y escrita en el expediente para recuperar el código corto, sin valorar las circunstancias que originaron los mensajes. Afirma que esta interpretación le impone una carga imposible, pues exigir la autorización del **BANCO POPULAR** supone obtener anticipadamente el consentimiento de una entidad cuya identidad fue utilizada por terceros sin conocimiento previo de **ESTRATEC, NUTRESA** ni del propio banco. Añade que esa exigencia reproduce el engaño de los atacantes, al tratar los mensajes como si provinieran legítimamente de la entidad suplantada.

Argumenta que, incluso si la causal admitiera algún grado de responsabilidad basado en la constatación objetiva de la ausencia de autorización, no podría aplicarse de manera absoluta. Invoca las sentencias C-616 de 2002 y C-038 de 2020 para sostener que la responsabilidad objetiva está proscrita, salvo excepciones, por los principios de dignidad humana y culpabilidad. Señala que ni la Resolución CRC 5050 de 2016 ni otra norma establecen ese régimen para la recuperación de códigos cortos y que el numeral 6.4.3.2.8 no excluye expresamente la exigencia de un elemento de imputación.

La recurrente afirma que la CRC atribuyó ese alcance a la causal mediante interpretación administrativa, sin habilitación normativa o jurisprudencial ni explicación de por qué la recuperación estaría comprendida en las excepciones reconocidas por la Corte Constitucional. Por ello, sostiene que el debido proceso exige valorar las circunstancias reales de los hechos, particularmente: **i)** el conocimiento efectivo del uso no autorizado; **ii)** la capacidad técnica y jurídica para obtener o controlar la autorización; y **iii)** una omisión reprochable del asignatario frente a ese conocimiento.

Sostiene que, en el presente caso, ninguno de los elementos concurre:

> «(i) ESTRATEC no tuvo conocimiento alguno de que su plataforma estaba siendo utilizada para el envío de mensajes que invocaban la identidad de BANCO POPULAR, sino hasta el momento en que dicha entidad radicó su queja ante la CRC. Con anterioridad a ese momento, ESTRATEC desconocía por completo la existencia de la exposición de credenciales de NUTRESA y el consecuente uso indebido de su plataforma por parte de terceros no autorizados.
>
> (ii) ESTRATEC jamás tuvo, ni pudo razonablemente haber tenido, ningún vínculo jurídico con BANCO POPULAR que le permitiera, siquiera en teoría, gestionar o solicitar una autorización de su parte. La exigencia de una autorización previa presupone, necesariamente, la existencia de algún grado de relación o cercanía entre quien debe obtenerla y quien debe otorgarla; en este caso, dicha relación nunca existió, ni pudo haber existido, pues la sola aparición de la identidad de BANCO POPULAR en los mensajes fue un hecho sobreviniente, imprevisible y ajeno a la voluntad de ESTRATEC.

(iii) Una vez ESTRATEC tuvo conocimiento de la situación (a través de la queja de BANCO POPULAR), actuó de manera inmediata y diligente, adoptando las medidas de contención ya referidas. No existe en el expediente elemento alguno que permita inferir negligencia, tolerancia o beneficio indebido por parte de ESTRATEC frente a los hechos investigados.»[5]

Señala que, al prescindir de este análisis y limitarse a una constatación puramente formal y objetiva (esto es, que la autorización de BANCO POPULAR no obra en el expediente), sostiene que la resolución impugnada desconoce que la causal 6.4.3.2.8 exige una valoración razonada de las circunstancias particulares del caso, y no una aplicación mecánica y automática que prescinda de todo elemento de imputación.

Sostiene que, aceptar la interpretación de la CRC equivaldría a convertir la recuperación de códigos cortos en una consecuencia automática e ineludible frente a cualquier incidente de seguridad informática sufrido por el asignatario, sin importar su origen, su previsibilidad, ni la diligencia desplegada una vez conocidos los hechos, interpretación que ninguna norma de la Resolución CRC 5050 de 2016 exige, y que resulta manifiestamente desproporcionada frente a la finalidad de la causal analizada.

- **Consideraciones de la CRC**

Frente al argumento expuesto, esta Comisión considera que la recurrente parte de una equiparación entre la recuperación de un recurso de identificación y la imposición de una sanción por la conducta de los terceros que ejecutaron el fraude. La recuperación se fundamenta en las funciones de administración de recursos públicos de numeración y tiene por objeto determinar la procedencia de mantener su asignación conforme a las condiciones regulatorias. Esta distinción corresponde al criterio sostenido por la CRC sobre la naturaleza de la medida. En consecuencia, el análisis no exige establecer que **ESTRATEC** haya sido autora del ataque informático, sino verificar los presupuestos que habilitan la recuperación del recurso utilizado y motivar su aplicación al caso concreto.

Las sentencias C-616 de 2002 y C-038 de 2020 deben examinarse dentro de ese marco. La primera estudió la sanción de clausura de establecimientos vinculada al decomiso de mercancías por infracciones aduaneras; la segunda analizó la responsabilidad solidaria del propietario del vehículo por infracciones detectadas mediante medios tecnológicos. Sus consideraciones sobre culpabilidad e imputación personal se refieren al ejercicio de la potestad sancionadora estatal. Por ello, su invocación no demuestra, por sí sola, que toda decisión administrativa desfavorable constituya una sanción ni que la recuperación de los recursos de identificación deba someterse automáticamente al mismo juicio de responsabilidad.

Ahora bien, tampoco es exacto que la decisión se haya sustentado exclusivamente en la ausencia de una autorización en los términos establecidos en la Resolución CRC 5050 de 2016. La Resolución CRC 8283 de 2026 recopila toda la información que reposa en el expediente de la actuación administrativa, entre esto, identifica la comunicación de **BANCO POPULAR,** radicada bajo el número 2026808792 del 23 de abril de 2026, mediante la cual informó sobre mensajes enviados desde el código corto **898988,** aportó capturas y negó expresamente haber autorizado su envío o contenido. Asimismo, recoge las explicaciones de **ESTRATEC** sobre la utilización de la cuenta de **NUTRESA** y la posible exposición de sus credenciales. La motivación, por tanto, comprende elementos sobre la utilización del recurso, la suplantación de la identidad del banco y la ausencia de su consentimiento.

En este contexto, identificar que los mensajes fueron enviados en nombre de BANCO POPULAR no implica que la Comisión haya considerado que procedían legítimamente de esa entidad ni que hubiera aceptado el engaño de los atacantes. Precisamente, la causal del numeral 6.4.3.2.8 comprende el envío de mensajes presentados en nombre de terceros sin su autorización expresa y escrita. Interpretar que solo comprende comunicaciones legítimamente originadas por el tercero privaría de alcance a la exigencia de autorización frente a supuestos de suplantación. En el caso analizado, la apariencia de procedencia bancaria atribuida a los mensajes y la negativa del banco constituyen aspectos complementarios del supuesto examinado.

La inexistencia de un contrato entre **ESTRATEC** y del **BANCO POPULAR** tampoco constituye una condición de exclusión prevista en la causal. La disposición no exige una relación comercial previa entre ambos, ni limita su aplicación a mensajes elaborados personalmente por el

[5] Radicado 2026817154 del 23 de julio de 2026.

asignatario. Por ello, la autorización requerida no consiste en obtener el consentimiento anticipado de todas las entidades que eventualmente pudieran ser suplantadas, sino en que las comunicaciones cursadas en nombre de un tercero cuenten con su consentimiento. El requerimiento efectuado durante la actuación buscaba verificar esa condición respecto de mensajes determinados; no imponía a **ESTRATEC** la obligación de conseguir retroactivamente una autorización para legitimar los mensajes de texto (SMS).

Desde la perspectiva técnica, la explicación sobre el uso indebido de credenciales API permite identificar el mecanismo mediante el cual, según la recurrente, se accedió al servicio de mensajería. Sin embargo, la autenticación mediante una cuenta de NUTRESA no acredita autorización de **BANCO POPULAR** para el contenido transmitido. Son verificaciones diferentes: las credenciales habilitan el acceso técnico a una cuenta, mientras que la autorización se refiere a la entidad en cuyo nombre se comunica. De acuerdo con el propio relato de **ESTRATEC**, los mensajes se cursaron mediante su plataforma utilizando credenciales comprometidas; por tanto, esa explicación no niega su envío a través del recurso asignado.

Respecto de los tres elementos propuestos por la recurrente, el conocimiento efectivo del incidente, la capacidad de control y la conducta desplegada son circunstancias que deben valorarse, pero su formulación como requisitos concurrentes no puede sustituir el supuesto expresamente establecido en la regulación. En particular, el artículo 2.1.18.6 de la Resolución CRC 5050 de 2016 exige a los PCA e integradores tecnológicos asignatarios emplear herramientas para prevenir fraudes mediante SMS o USSD y verificar periódicamente su efectividad. Su alcance preventivo permite descartar que todas las obligaciones del asignatario surjan únicamente cuando recibe una queja. Esto no significa que la ocurrencia del incidente pruebe automáticamente negligencia, sino que la ausencia de conocimiento previo no basta para excluir el examen de las condiciones bajo las cuales se utilizó el recurso.

Finalmente, la Resolución CRC 8283 de 2026 sí abordó el modelo SaaS, la exposición de credenciales y las medidas de contención, y explicó por qué no consideró que desvirtuaran la causal. La suspensión de cuentas y el restablecimiento de credenciales permiten valorar la respuesta al incidente, pero no modifican las condiciones de los mensajes previamente enviados. La decisión sobre el recurso debe valorar igualmente los soportes adicionales y justificar la adecuación de la recuperación a los hechos acreditados. Así, la respuesta al cargo no consiste en sostener que cualquier incidente informático produce necesariamente la recuperación, sino en demostrar que, en este caso, se materializó el supuesto regulatorio y explicar por qué las circunstancias alegadas no desvirtúan su aplicación, con observancia de las exigencias de motivación y proporcionalidad del CPACA.

En consecuencia, las razones de inconformidad no tienen vocación de prosperar ni proporcionan fundamento para revocar la Resolución CRC 8283 de 2026.

(iii) INEXISTENCIA DE LA CAUSAL 6.4.3.2.8 – LA ÚNICA AUTORIZACIÓN PARA EL ENVÍO DE MENSAJES DE TEXTO DEBE SER OTORGADA POR NUTRESA

ESTRATEC sostiene que la autorización exigida por el numeral 6.4.3.2.8 de la Resolución CRC 5050 de 2016 corresponde al tercero en cuyo nombre el asignatario decide voluntariamente enviar mensajes, por lo que presupone una relación de envío legítima y querida, y no una originada en el fraude de terceros. Afirma que, en este caso, la única relación de esa naturaleza es la existente con **NUTRESA**, remitente real y autorizado de los mensajes cursados mediante el código corto **898988** en condiciones normales de operación.

Señala que el **BANCO POPULAR** nunca fue remitente autorizado ni contraparte de **ESTRATEC** o **NUTRESA** respecto de dicho código, y que su nombre apareció exclusivamente por la explotación indebida de las credenciales API de **NUTRESA.** Por ello, considera que exigir la autorización del banco supondría acreditar una relación de envío que ninguna de las dos sociedades quiso ni diseñó y que constituye el objeto del delito del que fueron víctimas. En ese sentido, sostiene que la autorización de **NUTRESA,** que afirma haber acreditado, era la única jurídicamente relevante y exigible. Concluye que la causal del numeral 6.4.3.2.8. de la Resolución CRC 5050 de 2016 no se configura respecto a **ESTRATEC**.

- **<u>Consideraciones de la CRC</u>**

Frente a este argumento, la Comisión considera que **ESTRATEC** confunde la autorización de su cliente para utilizar el servicio de mensajería con la autorización del tercero en cuyo nombre se presentan las comunicaciones. El numeral 6.4.3.2.8 del artículo 6.4.3.2 de la Resolución CRC

5050 de 2016 contempla el envío de mensajes en nombre de terceros que no hayan autorizado expresamente y por escrito su envío o contenido.

Dicha disposición no limita el concepto de terceros a los clientes del asignatario ni incorpora la expresión «en cuyo nombre decide, de manera voluntaria, enviar mensajes a través del código corto asignado», introducida por la recurrente. En consecuencia, la interpretación de **ESTRATEC** restringe el alcance de la causal de recuperación al añadir condiciones que no están previstas en su texto. Por tanto, identificar a **NUTRESA** como cliente legítimo al que se vinculó el registro del envío del mensaje de texto no acredita, por sí mismo, la existencia de una autorización expresa y por escrito de **BANCO POPULAR** para el envío o el contenido de los mensajes presentados en su nombre.

Sostener que la autorización exigible debía provenir de **NUTRESA** resulta, además, contradictorio con los argumentos expuestos por **ESTRATEC** en el recurso, en los que reconoce que en el contenido de los mensajes se aprecia que se envió en nombre de **BANCO POPULAR** y alega haber sido víctima de suplantación y acceso fraudulento a sus plataformas. El hecho de que **NUTRESA** fuera su cliente y de que, según la recurrente, su usuario hubiera sido utilizado para efectuar los envíos presuntamente fraudulentos no modifica la identidad del tercero en cuyo nombre se presentaron las comunicaciones. En consecuencia, debe distinguirse entre el cliente a cuyo usuario se vincularon los envíos y la entidad en cuyo nombre se remitieron los mensajes: la autorización expresa y por escrito debía provenir de **BANCO POPULAR**, sin que una autorización de **NUTRESA** pudiera suplirla.

En el caso concreto, como ya se ha señalado, en el expediente de la actuación administrativa reposa que el **BANCO POPULAR,** informó sobre mensajes de texto (SMS) enviados desde el código corto **898988** que utilizaban su identidad corporativa e incluían enlaces falsos que simulaban su portal transaccional. Asimismo, el banco negó expresamente haber autorizado su envío o contenido y aportó capturas de pantalla. En consecuencia, la identificación del tercero cuya autorización se verifica responde a la identidad bajo la cual se presentaron los mensajes objeto de queja, y no exclusivamente a la titularidad de la cuenta utilizada para cursarlos.

Desde una perspectiva técnica, según la explicación de **ESTRATEC**, las credenciales API de **NUTRESA** fueron empleadas por terceros no autorizados. Esa circunstancia permite identificar la cuenta a través de la cual se habría utilizado la plataforma, pero no convierte a **NUTRESA** en autora o remitente legítima de los contenidos fraudulentos ni acredita el consentimiento de **BANCO POPULAR.** La titularidad de una cuenta, el uso de sus credenciales y la identidad que se atribuye el contenido del mensaje son elementos distintos. De hecho, la propia afirmación de que las credenciales fueron utilizadas sin autorización impide extender automáticamente la autorización ordinaria del cliente a los mensajes introducidos por los atacantes.

Aún, si se tiene por acreditada la autorización de **NUTRESA** para el envío de sus comunicaciones legítimas, esta no demuestra que el **BANCO POPULAR** hubiera consentido los mensajes que suplantaban su identidad. La autorización de una sociedad para sus propias comunicaciones no sustituye la de otra entidad en cuyo nombre se presentan mensajes diferentes. La recurrente no expone que **NUTRESA** estuviera facultada para autorizar comunicaciones en nombre del banco; por el contrario, sostiene que ambas sociedades eran ajenas a esa relación de envío. Por ello, la autorización invocada no desvirtúa la ausencia de consentimiento del tercero identificado en las comunicaciones cuestionadas.

Tampoco resulta acertado afirmar que verificar la autorización del banco equivale a exigir la acreditación de una relación comercial inexistente. El requerimiento busca establecer si los mensajes concretos contaban con el consentimiento exigido por la regulación, sin presuponer que el banco fuera cliente de **ESTRATEC** ni exigir que se obtenga retroactivamente una autorización. Que el banco no hubiera querido actuar como remitente es compatible con la suplantación denunciada y no excluye, por esa sola razón, el supuesto de envío de mensajes en su nombre sin autorización. Interpretar lo contrario permitiría excluir de la causal precisamente los mensajes cuya apariencia de procedencia fue construida sin consentimiento de la entidad suplantada.

Finalmente, la explicación sobre el acceso no autorizado debe valorarse para establecer las circunstancias del incidente, pero no altera la identidad del tercero cuya autorización resulta pertinente respecto de los mensajes examinados. La resolución impugnada abordó la exposición de credenciales y precisó que el modelo tecnológico y la intervención de terceros no transfieren las obligaciones asociadas al recurso asignado.

En consecuencia, la autorización de **NUTRESA** no basta para desvirtuar la causal respecto de las comunicaciones presentadas en nombre de **BANCO POPULAR**: acredita, en su caso, una relación legítima distinta, pero no el consentimiento necesario para los mensajes objeto de esta actuación.

En consecuencia, las razones generales de inconformidad no tienen vocación de prosperar ni proporcionan fundamento para revocar la Resolución CRC 8283 de 2026.

(iv) DESPROPORCIÓN DE LA MEDIDA Y USO CUASI-SANCIONATORIO DE LA RECUPERACIÓN

ESTRATEC expone que, la recuperación total y definitiva del código corto **898988** resulta en todo caso desproporcionada frente a los hechos acreditados. En la medida que, no se trata de un uso indebido consentido, tolerado o que hubiera reportado beneficio alguno a **ESTRATEC**, sino de un incidente de seguridad informática perpetrado por terceros criminales en contra de la plataforma y de un cliente de **ESTRATEC**, frente al cual esta actuó de manera inmediata y diligente mediante la intervención de su equipo de seguridad.

Expone que la resolución impugnada no explica por qué dichas medidas resultaban insuficientes para mitigar el riesgo identificado, ni evaluó alternativas menos gravosas que la privación definitiva del recurso de identificación, pese a que dicha privación produce, en la práctica, efectos equivalentes a los de una sanción, lo cual exigía de la CRC un análisis de proporcionalidad más riguroso del que efectivamente realizó.

- **Consideraciones de la CRC**

Frente a este argumento, se reitera que, la recuperación del código corto **898988** constituye el ejercicio de las competencias de regulación y administración de los recursos de identificación atribuidas a la CRC por los numerales 12 y 13 del artículo 22 de la Ley 1341 de 2009, modificada por la Ley 1978 de 2019. Estas facultades comprenden su recuperación cuando se configuren los presupuestos regulatorios, conforme al artículo 2.2.12.1.2.5 del Decreto 1078 de 2015 y a los artículos 6.1.1.8 y 6.4.3.2 de la Resolución CRC 5050 de 2016. La actuación de recuperación no es un procedimiento sancionatorio ni cuasi sancionatorio: su objeto es determinar la procedencia de mantener la asignación de un recurso público sujeto a condiciones de utilización, cuya asignación no confiere propiedad. Por tanto, los efectos desfavorables que su recuperación pueda generar para **ESTRATEC** no transforman, por sí mismos, su naturaleza administrativa en punitiva. Ello tampoco releva a la Comisión de motivar la decisión, valorar las pruebas y justificar su proporcionalidad frente a las circunstancias acreditadas.

Es por todo lo anterior, en los trámites de recuperación de códigos cortos el procedimiento aplicable no es el contenido en los artículos 47 a 52 del CPACA, correspondiente al procedimiento administrativo sancionatorio, sino el procedimiento establecido en los artículos 34 a 45, que corresponde al denominado procedimiento administrativo común y principal y al que refiere, rectamente interpretado, el artículo 6.1.1.8.1. de la Resolución CRC 5050 de 2016, que es el que efectivamente fue aplicado en esta actuación de recuperación.

Dado lo anterior, para efectos de la actuación de recuperación adelantada por la Comisión, que dio lugar a la resolución recurrida, la Comisión tuvo en cuenta las normas del procedimiento común y principal. Es por lo que, cuando la Comisión inició la actuación de recuperación, en aplicación del artículo 6.1.1.8.1. de la Resolución CRC 5050 de 2016 sobre el procedimiento de recuperación, se le comunicó a **ESTRATEC** acerca del inicio del trámite con el fin de garantizar su derecho a la defensa y al debido proceso.

En ese contexto, las medidas adoptadas por **ESTRATEC** después del incidente deben valorarse como actuaciones de contención y prevención, pero no tienen el efecto de eliminar los envíos realizados en nombre del **BANCO POPULAR** sin su autorización, ni de subsanar retroactivamente ese requisito. Tal como lo explicó la Resolución CRC 8283 de 2026, la reacción posterior no desvirtúa por sí sola la causal examinada. Aceptar que la sola adopción de correctivos posteriores impide recuperar el recurso haría inocua la causal, pues permitiría neutralizar su aplicación mediante actuaciones ejecutadas después de materializado el supuesto que la activa, incorporando una excepción no prevista en la regulación.

Además, las herramientas de prevención del fraude y la verificación periódica de su efectividad son obligaciones establecidas en el artículo 2.1.18.6 de la Resolución CRC 5050 de 2016; su cumplimiento no confiere inmunidad frente a la recuperación. En consecuencia, la diligencia

posterior alegada no impone el archivo de la actuación administrativa, ni garantiza la conservación del código, aunque debe ponderarse al justificar la necesidad y el alcance de la medida, sin confundir la configuración de la causal con la motivación de la decisión de recuperarlo.

En concordancia con lo anterior, el artículo 6.4.3.2 de la Resolución CRC 5050 de 2016 contempla expresamente la recuperación del código corto como consecuencia jurídica de la configuración de las causales allí previstas, entre ellas, el envío de mensajes en nombre de terceros que no hayan autorizado expresamente y por escrito su envío o contenido, conforme al numeral 6.4.3.2.8. Por consiguiente, la recuperación constituye una medida prevista en el régimen de administración de recursos de identificación, cuya adopción procede previa actuación administrativa y mediante decisión motivada. La implementación posterior de correctivos no sustituye esa consecuencia regulatoria ni obliga a la Comisión a mantener la asignación cuando se encuentre acreditada la causal y justificada la recuperación.

En consecuencia, el argumento no tiene vocación de prosperar ni proporciona fundamento para revocar la Resolución CRC 8283 de 2026.

(v) IMPROCEDENCIA DEL TRASLADO A LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, A LA FISCALÍA GENERAL DE LA NACIÓN Y AL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

ESTRATEC sostiene que los traslados del expediente a la Superintendencia de Industria y Comercio (SIC), la Fiscalía General de la Nación y el MinTIC presentan un vicio autónomo, pues la resolución impugnada no contiene una motivación específica, individualizada y suficiente que identifique, respecto de cada autoridad, los hechos que podrían configurar una infracción dentro de su competencia. Afirma que el artículo 21 del CPACA no establece una remisión automática y que la colaboración armónica exige identificar concretamente tales hechos, en cumplimiento del deber de motivación que atribuye al artículo 35 del mismo código.

Respecto del traslado a la Fiscalía, señala que la propia resolución reconoce que los hechos se originaron en la explotación no autorizada de las credenciales de un cliente por terceros ajenos a la relación contractual. Por ello, cuestiona que se remita el expediente por posibles ataques de smishing y phishing sin distinguir entre **ESTRATEC**, como víctima, y los terceros que realizaron el acceso. A su juicio, esta omisión la expone injustificadamente a una investigación penal e invierte la posición de denunciante y víctima que le correspondería.

En cuanto a la SIC, sostiene que la resolución menciona genéricamente un posible manejo de información contrario a la Ley 1581 de 2012, sin identificar los principios o derechos comprometidos, los datos personales afectados ni el tratamiento indebido atribuible a **ESTRATEC**. Añade que tampoco se determina una falla en sus medidas de seguridad ni su relación causal con la exposición de las credenciales de NUTRESA o el envío de los mensajes. Como antecedente, cita las Resoluciones CRC 8029 y 8057 de 2025 y 8128 de 2026, en las que únicamente se ordenó el traslado al MinTIC, para sostener que la remisión adicional a la SIC y a la Fiscalía requiere una justificación particular.

Finalmente, considera inconsistente que la CRC califique la recuperación como un procedimiento no sancionatorio, tramitado conforme a los artículos 34 a 45 del CPACA, y utilice sus resultados para remitir el expediente a autoridades con potestades sancionatorias y penales. Afirma que ello la expone a consecuencias de mayor gravedad sin las garantías propias de esas actuaciones y constituye una desviación de la finalidad del procedimiento de recuperación. En consecuencia, solicita dejar sin efecto los traslados ordenados en los artículos 2 y 3 de la resolución impugnada por falta de motivación específica, individualizada y suficiente.

- **Consideraciones de la CRC**

Frente a este cargo, la recurrente confunde la remisión del expediente con la apertura de una investigación en su contra y con una atribución anticipada de responsabilidad. El artículo 3 de la Resolución CRC 8283 de 2026 dispone comunicar los antecedentes a las autoridades destinatarias para lo de su competencia, sin ordenarles formular cargos, imponer sanciones o atribuir a **ESTRATEC** la autoría de una conducta delictiva. Asimismo, el apartado 4 de la resolución precitada distingue los asuntos que justifican cada remisión: posibles afectaciones al régimen de protección de datos personales, presuntos ataques de smishing y phishing, y un posible incumplimiento de la regulación sectorial.

Al respecto, la Corte Constitucional en sentencia C-138 de 2015 se pronunció respecto del principio de separación de poderes y autonomía de las entidades del Estado:

> «El principio de separación de poderes es un pilar esencial del constitucionalismo moderno y una garantía fundamental del Estado de derecho. Su propósito es evitar la concentración del poder en un solo órgano, asegurando una distribución equilibrada de competencias y la existencia de mecanismos de control mutuo entre las distintas ramas del poder público. En este sentido, el artículo 113 de la Constitución Política establece la independencia funcional de los órganos del Estado, pero también consagra el deber de colaborar armónicamente en la consecución de los fines estatales.»

Asimismo, de acuerdo con lo señalado por la Corte Constitucional en la Sentencia C-246 de 2004[6], la separación de poderes exige respetar la autonomía e independencia de los órganos estatales, sin impedir su coordinación para el cumplimiento de los fines del Estado. En este sentido, la colaboración armónica permite articular la actuación de las distintas autoridades, pero no autoriza a modificar la distribución de competencias ni a que una entidad asuma funciones atribuidas a otra.

En este marco, el traslado del expediente no implica una atribución de responsabilidad a **ESTRATEC**, sino que permite que las autoridades destinatarias evalúen los hechos y determinen, de manera autónoma y en ejercicio de sus respectivas competencias, si procede iniciar investigaciones o adelantar otras actuaciones. La remisión no predetermina el sentido de sus decisiones ni sustituye la valoración que les corresponde efectuar. Por consiguiente, el análisis de la CRC consiste en identificar los hechos que ameritan su evaluación por otras autoridades y justificar su remisión, sin que deba demostrar previamente todos los elementos de una eventual infracción cuya investigación y decisión exceden sus competencias.

Respecto de la Fiscalía General de la Nación, los mensajes que presuntamente suplantaban la identidad del **BANCO POPULAR** e incorporaban enlaces falsos, junto con la explicación de la propia recurrente sobre el uso no autorizado de credenciales, constituyen circunstancias concretas que justifican poner los hechos en conocimiento de la autoridad penal. El artículo 67 de la Ley 906 de 2004 establece el deber del servidor público de comunicar a la autoridad competente los delitos investigables de oficio de cuya comisión tenga conocimiento. Exigir que la CRC determine previamente quién perpetró el acceso o cuál es la posición procesal definitiva de cada interviniente supondría trasladarle funciones de investigación penal. La condición de víctima alegada por **ESTRATEC** es compatible con la remisión y puede ser esclarecida dentro de la actuación competente; no constituye una razón para impedir que se investiguen los hechos que la propia sociedad atribuye a terceros.

En relación con la SIC, debe distinguirse entre la seguridad de acceso a la plataforma y la licitud del tratamiento de los datos utilizados para cursar las comunicaciones. Desde el punto de vista técnico, la ausencia de intrusión en la infraestructura no resuelve, por sí sola, cómo se obtuvieron o utilizaron los datos de los destinatarios ni quién intervino en ese tratamiento. Estas son cuestiones por esclarecer, no infracciones que puedan darse por demostradas a partir del incidente. Precisamente, los artículos 19 y 21 de la Ley 1581 de 2012 atribuyen a la SIC la vigilancia del régimen y la facultad de adelantar investigaciones y solicitar información. Por tanto, la remisión debe entenderse como una solicitud de evaluación de los hechos y de sus eventuales implicaciones en materia de datos personales, sin afirmar que existió una filtración o una falla de seguridad atribuible a **ESTRATEC** que no haya sido acreditada.

En cuanto al MinTIC, el vínculo con sus competencias radica en el posible incumplimiento de las disposiciones regulatorias que gobiernan la utilización del código corto, particularmente la exigencia prevista en el numeral 6.4.3.2.8 de la Resolución CRC 5050 de 2016. La remisión permite que ese Ministerio evalúe, dentro del ámbito establecido en los artículos 63 y siguientes de la Ley 1341 de 2009, si procede una actuación independiente. La recuperación decretada por la CRC no sustituye dicha evaluación ni determina automáticamente una sanción: corresponde al Ministerio establecer los presupuestos de responsabilidad y garantizar la defensa y contradicción en el procedimiento aplicable.

Tampoco existe incompatibilidad entre la naturaleza no sancionatoria de la recuperación y la comunicación de hechos a autoridades con competencias sancionatorias o penales. La naturaleza del procedimiento de origen no impide que sus documentos sean puestos en conocimiento de otra autoridad, ni convierte sus conclusiones en prueba incontrovertible dentro de una actuación

[6] Corte Constitucional, Sentencia C-246 de 2004.

posterior. Cada entidad debe valorar autónomamente la información, determinar si procede actuar y observar las garantías y exigencias probatorias correspondientes. La coordinación entre autoridades no autoriza a eludir esas garantías, pero tampoco exige que la CRC adelante un procedimiento sancionatorio o penal para comunicar hechos que exceden su competencia.

Finalmente, la sola referencia a decisiones anteriores con distintos destinatarios no demuestra la improcedencia de estos traslados: sería necesario acreditar la equivalencia de sus circunstancias relevantes. La justificación de las remisiones debe examinarse frente a los hechos de este expediente y al alcance limitado de comunicar información, sin anticipar responsabilidad.

En consecuencia, el argumento no tiene vocación de prosperar ni proporciona fundamento para revocar la Resolución CRC 8283 de 2026.

En virtud de lo expuesto,

RESUELVE

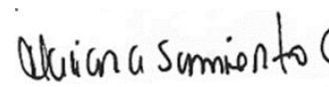
ARTÍCULO 1. Admitir el recurso de reposición presentado por **ESTRATEC S.A.S.** en contra de la Resolución CRC 8283 de 2026.

ARTÍCULO 2. Negar las peticiones formuladas por **ESTRATEC S.A.S.** y, en consecuencia, confirmar integralmente la Resolución CRC 8283 de 2026, por las razones expuestas en la parte motiva del presente acto administrativo.

ARTÍCULO 3. Notificar personalmente la presente Resolución al representante legal de **ESTRATEC S.A.S.** o a quien haga sus veces, de conformidad con lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, advirtiéndole que contra la misma no procede ningún recurso.

Dada en Bogotá D.C., a los 23 días del mes de septiembre de 2026.

NOTIFÍQUESE Y CÚMPLASE



MARIANA SARMIENTO ARGÜELLO
Coordinadora de Relaciones con Grupos de Valor

Trámite ID: 110896
Elaborado por: Brayan Andrés Forero Sierra
Revisado por: Luisa Fernanda Barrera Fuentes