COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

"Revisión del marco regulatorio para la gestión de riesgos de seguridad digital" Documento de respuestas a observaciones y propuesta alternativa

Capital Intelectual

Mayo de 2018

vive digital para la gente

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

CONTENIDO

Introducción **4**

1. Cambios realizados a la propuesta regulatoria **5**

2. Partes interesadas que presentaron observaciones a la primera publicación **6**

3. Observaciones de carácter general a la primera publicación **8**

3.1 Sobre la necesidad de desarrollar mesas de trabajo con la Industria. 8

3.2 Sobre la necesidad de involucrar otros actores de la cadena de Valor. 8

3.3 Sobre la necesidad de coordinación con otras agencias del estado en el marco de la implementación del CONPES 3854 10

3.4 Sobre el alcance que debe darse a los incidentes de seguridad. 12

3.5 Sobre la inclusión de CHINA como experiencia relevante. 13

3.6 Sobre la necesidad de adelantar AIN 14

3.7 Concepto del Ministerio de Justicia y del Derecho 14

3.8 Sobre la Agenda Regulatoria CRC 2017-2018 15

3.9 Sobre la necesidad de fomentar modelos de autorregulación 16

3.10 Sobre el proceso participativo 19

3.11 Sobre la confidencialidad de los datos 20

3.12 Sobre la necesidad de interacción en casos de ciberataque 21

4. Observaciones al articulado del proyecto de resolución de la primera publicación **21**

4.1 Sobre las definiciones: 21

4.2 Sobre la información de incidentes de seguridad: 25

4.3 Sobre los reportes de incidentes de seguridad a las autoridades: 30

4.4 Seguimiento a gestión de incidentes 36

4.5 Sobre el SGSI 38

Anexo – Análisis costo efectividad **44**

A1 Medidas de Seguridad de Red 47

A1.1 Propuesta regulatoria (Medidas de Seguridad de Red) 47

A1.2 Descripción de las alternativas analizadas (Medidas de Seguridad de Red). 48

A1.3 Análisis de efectividad (Medidas de Seguridad de Red). 51

A1.4 Análisis de costos (Medidas de Seguridad de Red). 52
A1.5 Análisis comparativo de los costos y efectividad de las alternativas (Medidas de Seguridad de Red) 55
A2 Previsiones frente a los incidentes de seguridad 55
A2.1 Propuesta regulatoria (Incidentes de seguridad) 55
A2.2 Descripción de las alternativas analizadas (Incidentes de seguridad). 56
A2.3 Análisis de efectividad (Incidentes de seguridad) 60
A2.4 Análisis de costos (Incidentes de seguridad) 61
A2.5 Análisis comparativo de los costos y efectividad de las alternativas (Incidentes de seguridad) 64
A3 Previsiones de reporte a autoridades 64
A3.1 Propuesta regulatoria (Previsiones de reporte a autoridades) 64
A3.2 Descripción de las alternativas analizadas (Reporte a autoridades). 65
A3.3 Análisis de efectividad (Reporte a autoridades). 66
A3.4 Análisis de costos (Reporte a autoridades). 68
A3.5 Análisis comparativo de los costos y efectividad de las alternativas (Reporte a autoridades). 70

Introducción

A continuación se presenta el documento de respuesta a las observaciones allegadas por los interesados en el proyecto "Revisión del marco regulatorio para la gestión de riesgos de seguridad digital", en el marco del cual se publicó el 24 de noviembre de 2017 la propuesta de resolución *"Por la cual se modifica el artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones"*[1] y su correspondiente documento de soporte, documentos sobre los cuales se recibieron observaciones hasta el 19 de diciembre de 2017 en cumplimiento de lo establecido en el artículo 2.2.13.3.2 del Decreto 1078 de 2015.

El mencionado proyecto fue incluido en la agenda regulatoria 2017-2018 a raíz de la aprobación de la Política Nacional de Seguridad Digital, contemplada en el CONPES 3854 de 2016, esta política establece una nueva visión de inclusión de las múltiples partes interesadas en la gestión de la seguridad digital, y reconoce la responsabilidad compartida de mantener un entorno digital seguro, así como la necesidad de fortalecer las capacidades de todos para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

Teniendo en cuenta la importancia del sector de telecomunicaciones en materia de seguridad digital, el plan de acción del CONPES 3854 identificó que la CRC debía ajustar, dentro del marco de sus competencias, el marco normativo del sector TIC en el periodo inicial de implementación de dicha política 2017-2018 teniendo en cuenta el enfoque de gestión de riesgos de seguridad digital.

En esta misma línea, en diciembre de 2017, el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, presentó a consideración el Modelo Nacional de Gestión de Riesgos de Seguridad Digital con el objetivo de que las entidades públicas, privadas y mixtas, operadores de infraestructuras críticas cibernéticas y la ciudadanía en general mejorarán sus capacidades de gestión de riegos de seguridad digital[2].

Así, una vez analizadas las observaciones presentadas, así como las demás iniciativas planteadas por otras entidades en materia de gestión de la seguridad digital, y después de adelantar mesas de trabajo

---

1 Se invita las múltiples partes interesadas a consultar los documentos disponibles en la página web de la CRC: https://www.crcom.gov.co/es/pagina/ciberseguridad

2 Se invita las múltiples partes interesadas a consultar la propuesta de MINTIC en Urna de Cristal: http://www.urnadecristal.gov.co/construccion-modelo-gestion-riesgo-seguridad-digital

con las múltiples partes interesadas, este documento responde a los comentarios allegados y da claridad sobre las modificaciones realizadas a la propuesta de resolución.

1. Cambios realizados a la propuesta regulatoria

A continuación, se resumen los principales cambios efectuados con posterioridad a la etapa de discusión sectorial que están reflejados en el proyecto de resolución adjunto; para mayor información, sobre cada uno de estos aspectos se remite a las respuestas detalladas de las secciones 3 y 4 del presente documento.

Temática	Principales Cambios
Artículo 1. Definiciones	Se cambia la definición de Incidente de seguridad, se elimina la definición de integridad del servicio, se adiciona la definición de Sistema de Gestión de seguridad de la Información (SGSI). Para más información sobre estos cambios se remite a la respuesta 4.1.1 en el presente documento.
Artículo 2. Temática: Políticas de gestión de seguridad de la Información	Se mantiene la implementación de Sistemas de Gestión de Seguridad de la Información, sin embargo, se cambia el marco de implementación que será a través de un marco de autorregulación siguiendo la familia de estándares ISO/IEC 27000. Para más información sobre estos cambios se remite a las respuestas 4.5.2 (ISO 27000) y 3.9 (Autorregulación) del presente documento.
Artículo 2. Temática: Información de Incidentes	Se eliminan los umbrales de afectación de servicio a partir de los cuales debían reportase los incidentes, se cambia el campo de información a almacenar de "Causa del incidente" a "Categoría del incidente", estas categorías se alinean con la familia de estándares ISO/IEC 27000. Para más información sobre estos cambios se remite a las respuestas de la sección 4.2 del presente documento.
Artículo 2. Temática: Reporte a autoridades	Se modifica el momento de reporte a las autoridades para que el mismo no interfiera con la gestión del incidente, modificando la obligación de reporte de incidentes de seguridad de la información a las autoridades dentro de los 120 minutos subsecuentes a la detección, la cual aplicará únicamente cuando se trate de incidentes "serios" o "muy serios" según la clasificación adoptada en la propuesta de Anexo 5.8.

	Para más información sobres estas modificaciones se remite a la respuesta 4.3.1
Artículo 3. Clasificación de severidad de incidentes	Se adiciona el Articulo 3, el cual adopta la clasificación de severidad de incidentes necesaria para determinar la necesidad de reporte a las autoridades. Para más información sobres estas modificaciones se remite a la respuesta 4.3.1
Artículo 4. Seguimiento a gestión de incidentes	Se modifica el periodo de recolección de información de incidentes de seguridad de la información el cual partirá desde enero de 2019, (se evidenció en las mesas de trabajo que los datos de 2018, pueden mostrar desviaciones significativas respecto a promedios históricos, lo que puede afectar el desarrollo de una línea base de frecuencia e impacto de incidentes de seguridad digital)
Artículo 5. Vigencia y derogatoria	Se modifica la entrada en vigencia de la resolución, la misma permite un periodo de 12 meses para la implementación de los sistemas de gestión de seguridad de la información.

De acuerdo con el procedimiento establecido en el artículo 2.2.13.3.2 del Decreto 1078 de 2015, la propuesta regulatoria es sometida a consideración del Sector a partir de su publicación por el término de 10 días hábiles. Los comentarios serán recibidos a través del correo electrónico: seguridad.digital@crcom.gov.co, vía fax al (+57 1) 3198301, a través las redes sociales de la CRC en Twitter (@CRCCol) o en la página de Facebook "Comisión de Regulación de Comunicaciones", o en las oficinas de la CRC ubicadas en la Calle 59A Bis No. 5 – 53 Piso 9, Edificio Link Siete Sesenta, de la ciudad de Bogotá D.C.

No serán tenidos en cuenta los comentarios que se reciban respecto de disposiciones que no estén contenidas en la propuesta publicada.

2. Partes interesadas que presentaron observaciones a la primera publicación

En el periodo de publicación antes indicado, la CRC recibió observaciones de los siguientes agentes interesados:

1. Colombia Telecomunicaciones S.A. E.S.P.

2. Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.
3. Colombia Móvil S.A. E.S.P.
4. Virgin Mobile Colombia S.A.S.
5. Comunicación Celular Comcel S.A.
6. DIRECTV Colombia Ltda.
7. NAP Colombia -CCIT
8. Level 3 Colombia S.A.
9. Fundación Karisma
10. Jeimy J. Cano M.

Es de anotar que, en atención a las observaciones recibidas en materia de participación y discusión sectorial, la CRC realizó mesas de trabajo adicionales adelantadas en el primer trimestre de 2018, con la participación de:

- Presidencia de la Republica
- MINTIC
- colCERT
- IFX Networks Colombia
- Colombia Telecomunicaciones S.A. E.S.P.
- Empresa de Telecomunicaciones de Bogotá S.A. E.S.P
- Colombia Móvil S.A. E.S.P.
- Comunicación Celular Comcel S.A.
- DIRECTV Colombia Ltda.
- NAP Colombia -CCIT
- Fundación Karisma, Jeimy J. Cano M.

Asimismo, se recibieron observaciones posteriores a las mesas de discusión, las cuales también se responden en este documento por parte de:

- ANDESCO

3. Observaciones de carácter general a la primera publicación

3.1 Sobre la necesidad de desarrollar mesas de trabajo con la Industria.

3.1.1 COLOMBIA TELECOMUNICACIONES
El operador solicita tener en cuenta que cualquier decisión en torno a la gestión de riegos de seguridad digital puede impactar los procesos y esquemas que ya se encuentran implementados en la compañía, por lo que consideran de gran importancia que estos procesos de revisión de normas se realicen a través de mesas de trabajo en las que puedan analizar de manera detallada el alcance de posibles medidas regulatorias que la CRC considere implementar.

CRC Al respecto se aclara que esta Comisión es consciente de los múltiples procesos y procedimientos involucrados en la gestión de la seguridad de la información; es así como, atendiendo a las observaciones recibidas se llevaron a cabo mesas de trabajo con las múltiples partes interesadas durante el primer trimestre de 2018 las cuales se trataron los siguientes temas: i) Definiciones y Necesidades de información (Mesa 1 - 2 de febrero de 2018), ii) Sistemas de Gestión de Seguridad de la Información (Mesa 2 - , 8 de febrero de 2018) y iii) Reporte a autoridades y Análisis de Impacto Normativo (Mesa 3 - 15 de febrero de 2018). Se recuerda que este proyecto incluye todas las actividades de encuestas sectoriales, documento de soporte de análisis de resultados de la encuesta, benchmarking internacional, recomendaciones y demás elementos que soportan la propuesta inicial, además de las mesas de trabajo mencionadas, lo cual refleja el nivel de detalle que la Comisión ha incorporado en la propuesta de revisión del marco regulatorio.

3.2 Sobre la necesidad de involucrar otros actores de la cadena de Valor.

3.2.1 COLOMBIA TELECOMUNICACIONES
Manifiesta que antes de imponer obligaciones a los PRST, es necesario revisar toda la cadena de valor y verificar no solo los alcances sino la necesidad de hacer que otros agentes, incluso de otros sectores, también cuenten con responsabilidades y obligaciones claras y concretas, para evitar desequilibrios que afecten la capacidad de innovación de empresas como Telefónica, quienes consideran de vital importancia los temas de seguridad de la información.

CRC Respecto a esta observación, se resalta que el documento soporte identifica roles y responsabilidades, así como partes de la cadena de valor distintas de los operadores de comunicaciones, incluyendo los usuarios. Así mismo, este documento menciona que los operadores de comunicaciones

tienen características especiales como habilitadores de la transformación digital en otros sectores. Sin embargo, el proyecto se centra en lo establecido en el CONPES 3854 de 2016 es decir en *"ajustar el marco regulatorio del sector TIC. (…) teniendo en cuenta asuntos necesarios para la gestión de riesgos de seguridad digital, como la protección de usuarios de comunicaciones o el régimen de calidad de las redes de telecomunicaciones*". Aún así, el documento soporte que acompaña la resolución reconoce las responsabilidades y obligaciones de otros actores de la cadena de valor, teniendo presente que el CONPES 3854 propone otras acciones encaminadas a desarrollar dichas obligaciones, y las mismas están siendo adelantadas por entidades diferentes a la CRC como MINTIC, MINEDUCACION, MINDEFENSA y MINJUSTICIA.

3.2.2 COMCEL

Respecto a la responsabilidad de los usuarios frente a los incidentes de seguridad

"Que el Titulo II de la Resolución CRC 5050 de 2016, "Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones", que entrará en vigencia el 1^0 de enero de 2018, establece en el Capítulo 1 como uno de los derechos de los usuarios el de recibir protección de la información que cursa a través de la red del operador, quien debe garantizar la inviolabilidad de las comunicaciones". (Subrayado fuera de texto)

Señala que, si bien es cierto, el PRST debe tomar todas las medidas necesarias para garantizar la inviolabilidad de comunicaciones en los servicios que prestan, el usuario por su parte también tiene deberes de cuidado; por ende, los ataques que están dirigidos a los usuarios no pueden ser responsabilidad del operador. Mencionan que muchas de las violaciones a la seguridad son resultado de las acciones voluntarias de usuarios donde suministran información o descargan aplicaciones de sitios que comprometen su seguridad: phising, pharming, sitios que albergan malware, entre otros, los cuales exceden las esfera y responsabilidad del PRST.

Por tanto, considera importante que dentro del análisis que debe realizar esta Comisión, se tenga presente este aspecto, y se aclare, que tanto el usuario como el PRST que presta el servicio de comunicaciones, tienen responsabilidades y deberes frente a los incidentes de seguridad.

CRC Se recuerda que el documento soporte identifica roles y responsabilidades, así como partes de la cadena de valor distintas de los operadores de comunicaciones, incluyendo los usuarios. Así mismo, se propone acciones concretas para mejorar la gestión de riesgos de seguridad digital por parte de los usuarios. Sin embargo, como se menciona en la respuesta 3.2.1, se considera que el CONPES 3854 propone otras acciones encaminadas a desarrollar esta obligación, y las mismas están siendo

adelantadas por entidades diferentes a la CRC como MINTIC y MINEDUCACIÓN para que los usuarios tomen conciencia de los riesgos existentes en las redes y su papel activo para evitarlos.

3.3 Sobre la necesidad de coordinación con otras agencias del estado en el marco de la implementación del CONPES 3854

3.3.1 TELEFÓNICA - COMCEL

TELEFÓNICA Señala la importancia de que exista una completa coordinación entre las entidades que se encuentran desarrollando las disposiciones del CONPES 3854 de 2016, teniendo en cuenta la publicación reciente que hizo el MinTIC del Modelo Nacional de Gestión de Riesgos de Seguridad. Indican que dicho documento si bien abarca un amplio espectro de sectores y de tipo de entidades incluye al sector de Telecomunicaciones. Resaltan que de una buena coordinación entre entidades también depende el éxito en la implementación y uso de este modelo, lo cual sería para el avance del país hacia la economía digital.

En la misma línea, COMCEL solicita seguir la metodología del MinTIC, que propende por un esquema participativo y voluntario de las partes. Es decir, sugieren que la Comisión debería expedir una guía informativa que proponga lineamientos para el sector sin llegar a la regulación, sobre todo cuando se trata de un aspecto donde según ellos no se ha demostrado la necesidad de regulación.

CRC Esta Comisión ha reconocido y analizado los diferentes eslabones involucrados en las cadenas de valor digitales, y reconoce las diferentes obligaciones y responsabilidades en materia de seguridad digital que recaen en cada uno de ellos. Por lo anterior, se resalta que el documento soporte incluye un análisis del rol de los usuarios, así como recomendaciones a MinTIC en ese sentido. De otra parte, frente a la conveniencia de adoptar un enfoque como el propuesto por MINTIC en el modelo nacional de gestión de riesgos de seguridad digital, se remite a la respuesta 4.3.5.

La motivación para la propuesta regulatoria, emerge del análisis realizado por esta Comisión y expuesto en detalle en el documento de soporte de la propuesta de resolución. Entre las principales motivaciones se resaltan la creciente importancia de la seguridad digital en la operación de cualquier empresa del ecosistema digital, la baja confianza y sus consecuencias en la frecuencia de las interacciones y actividades del entorno digital, la baja adopción de mejores prácticas de seguridad digital (IPv6, DNSSEC, RPKI, BCP 38) en los operadores colombianos, la falta de información de frecuencia e impacto de los incidentes de seguridad digital y la falta de cooperación entre los operadores de redes y servicios de comunicaciones con las autoridades nacionales encargadas de la seguridad y defensa del entorno digital.

3.3.2 COMCEL

Manifiesta la importancia de la coordinación entre entidades del sector como la CRC, el MinTIC y la SIC, con el fin de ser coherentes con las normas previamente expedidas, como el CONPES. Proponen evitar la duplicidad de información entregada a estas entidades, por ejemplo la Circular No. 02 de 2015 de la SIC, establece que se deben reportar los incidentes de seguridad; así como, evitar aumentar el número de reportes ya realizados por los PRSTM, los cuales representan una carga operativa importante para los mismos, máxime cuando el MinTIC manifestó en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital, que los reportes para las entidades privadas son una invitación "como ejercicio colaborativo en el fortalecimiento de la seguridad digital del país".

CRC Se recuerda que el reporte a la SIC mencionado en la observación, está limitado únicamente a los casos de pérdida, robo y/o acceso no autorizado de **datos personales**, por lo que el alcance de dicho reporte es distinto al del proyecto de resolución en la propuesta de la CRC. En consecuencia, no existiría ninguna duplicidad de reporte de incidentes entre lo estipulado en este proyecto y la Circular de la SIC.

Adicionalmente, es de resaltar que esta entidad mantiene una constante comunicación con MINTIC y las demás entidades mencionadas en su observación. Esta misma aclaración fue realizada por los representantes de MINTIC a las múltiples partes interesadas en las mesas de trabajo realizadas por esta Comisión. La invitación de ese Ministerio debe entenderse dentro de su función de promover el establecimiento de una cultura de las Tecnologías de la Información y las Comunicaciones en el país, y el carácter voluntario del Modelo Nacional de Seguridad Digital debe entenderse como una recomendación dentro de las funciones que le han sido asignadas.

3.3.3 DIRECTV

Señala que, a pesar de los fundamentos técnicos, económicos y sociales de la iniciativa propuesta por esta Comisión, los medios propuestos en el proyecto de resolución desconocen y contradicen la convergencia de los servicios TIC y la necesidad de flexibilizar las cargas regulatorias del sector. Es así como expresan, que este proyecto tiene como consecuencia ahondar las asimetrías regulatorias entre los servicios tradicionales y los nuevos modelos de negocios basados en Internet. En principio, consideran que, debe reconocerse que si bien los PRST son actores preponderantes del ecosistema de la seguridad digital, no son los únicos responsables de salvaguardar y garantizar la confidencialidad y la integridad de la información que se procesa en los servicios de comunicación digital. En concreto, son los nuevos modelos de provisión contenidos quienes en mayor medida usufructúan dichos datos, por lo que resulta preocupante que esta obligación regulatoria afecte exclusivamente a los PRST.

Adicionalmente, expresan que, hoy en día por un principio de responsabilidad corporativa DIRECTV dispone de estrictas políticas internas que mitigan los riesgos de asociados a ataques cibernéticos. Por tanto, implementar una regulación específica a los PRST resulta innecesario e incrementa cargas administrativas.

CRC El alcance que se propone para el proyecto de Resolución se centra en alcanzar los objetivos del CONPES 3854 de 2016 y en ajustar el marco normativo para la gestión de riesgos de seguridad digital en el sector TIC. No obstante, la Comisión reconoce que los operadores de comunicaciones no son los únicos responsables de salvaguardar y garantizar la confidencialidad y la integridad de la información que se involucra en los servicios de comunicación digital. Sin embargo, el CONPES 3854 prevé acciones y estrategias en cabeza de otras entidades para alcanzar esos objetivos.

De otra parte, celebramos el hecho que DIRECTV cuente con políticas internas que mitigan los riesgos informáticos. Sin embargo, es de resaltar que resulta necesario que todos los operadores cuenten con políticas de seguridad de la información de acuerdo con las características y necesidades de su red, lo cual es lo propuesto en el proyecto.

3.3.4 Jeimy Cano

Señala la importancia de contextualizar las acciones en el marco de seguridad digital que se define en el documento de la OCDE, para así mantener la alineación con el CONPES 3854.

CRC El documento de la OCDE es en efecto una de las fuentes principales tenidas en cuenta para el desarrollo del proyecto. Precisamente esa visión del documento OCDE de crear las condiciones para la gestión de riesgos de seguridad digital es la que se propone para implementar sistemas de gestión de seguridad de la información.

3.4 Sobre el alcance que debe darse a los incidentes de seguridad.

COLOMBIA TELECOMUNICACIONES

Manifiesta que el alcance de la resolución debe ser sobre aquellos incidentes que pueden ser identificados por el PRST dentro de su red, y para los elementos sobre los cuales pueda tener control, indica que no es posible determinar las acciones que realizan los usuarios sobre sus dispositivos o equipos cuando los mismos están conectados a Internet, por ejemplo, la descarga de archivos maliciosos, no instalación de herramientas de seguridad o deshabilitación de las mismas, acceso a sitios desconocidos que puedan infectar su dispositivo, etc.

Menciona además que la identificación de un incidente de seguridad se realiza con base en comportamientos atípicos que pueda presentar el tráfico, a partir de la gestión de red que se realiza sobre la operación de la misma, comportamientos que se analizan para establecer si son causados por algún evento de seguridad. Solicitan que este alcance sea explícito en la redacción final.

CRC Es de aclarar que la propuesta de modificación del artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016, hace referencia a *"criterios y procedimientos en los procesos de gestión de seguridad de sus redes"* teniendo en cuenta que los dispositivos o equipos de los usuarios son clasificados como equipos terminales para el acceso a las redes de comunicaciones, a juicio de esta Comisión la redacción propuesta es clara respecto a que los eventos e incidentes de seguridad no hacen parte de las previsiones en cuestión, con excepción de los Equipos Terminales de Red (Modems, Routers, ONT, ONU, entre otros).

3.5 Sobre la inclusión de CHINA como experiencia relevante.

TIGO UNE

Manifiesta que en el documento soporte esta Comisión toma como relevante la experiencia de China, dada la implementación de leyes relacionadas con la ciberseguridad. No obstante, mencionan que diversos países del mundo, entre estos Estados Unidos y algunos países de Europa, han criticado constantemente el actuar del Gobierno Chino en cuanto a sus métodos y herramientas para intervención del Internet.

Expresan que dicho país, cuenta con una clasificación de "No Libre" conforme la Freedom House en su estudio *"Freedom on the Net",* dado los obstáculos de acceso, las limitaciones de contenidos, así como las violaciones a los derechos de los usuarios de Internet.

Por lo que todos estos tópicos han desembocado en bloqueo de redes sociales y aplicaciones, así como la implementación de medidas gubernamentales y policivas de bloqueo de contenido de tipo político y social, e igualmente el arresto de disidentes a partir de información y datos dispuestos en Internet.

Por lo anterior solicitan a la CRC revisar la conveniencia de incluir países que no hayan alcanzado estándares de seguridad que sirvan de guía para Colombia.

CRC A juicio de esta Comisión el realizar un benchmarking no implica ubicar las mismas posiciones, sino identificar el statu quo internacional. Dicho comparativo internacional identifica las políticas públicas y regulatorias sobre gestión de seguridad digital en desarrollo en el mundo. El identificar y conocer una ley de ciberseguridad con componentes técnicos relevantes, como es el caso de China, no implica que

esta Comisión asuma posiciones al respecto. Considerando que China es uno de los actores globales importantes en la materia, dejarlo de lado se considera inconveniente.

3.6 Sobre la necesidad de adelantar AIN

COMCEL
Menciona que en el CONPES 3854 de 2016, sobre la Política Nacional de Seguridad Digital, en su página 22, establece que esta Comisión debe adelantar el Análisis de Impacto Normativo (AIN) de que trata el CONPES 3816 de 2016, con el fin de realizar el ajuste del marco regulatorio en materia de seguridad digital.
En este sentido consideran fundamental el ejercicio de AIN al proyecto de resolución examinado, con el fin de examinar la proporcionalidad de las obligaciones propuestas, así como la eventual duplicidad de reportes, sin perder de vista que los PRST son los más interesados en conservar la seguridad de sus redes, y en tal sentido toman todas las medidas necesarias adoptando los más altos estándares de seguridad.

CRC Frente a la observación de COMCEL sobre la necesidad de adelantar Análisis de Impacto Normativo (AIN) al proyecto de resolución, se acoge el comentario de acuerdo con lo dispuesto en el CONPES 3854 de 2016, donde se establece que *"la Comisión de Regulación de Comunicaciones (CRC) ajustará en 2017 el marco regulatorio del sector TIC. Lo anterior, lo hará teniendo en cuenta asuntos necesarios para la gestión de riesgos de seguridad digital, como la protección de usuarios de comunicaciones o el régimen de calidad de las redes de telecomunicaciones. Esto se hará aplicando la metodología de Análisis de impacto normativo, establecida en el Documento CONPES 3816"*. Ahora bien, teniendo presente que este proyecto es clasificado como de bajo impacto, se anexa al presente documento el Análisis de Impacto Normativo de tipo cualitativo adelantado, el cual es suficiente para conocer si la intervención a realizar en este proyecto se justifica y si la misma es proporcionada.

3.7 Concepto del Ministerio de Justicia y del Derecho

CLARO
Manifiesta que el CONPES, le solicita igualmente al Ministerio de Justicia y Derecho, conceptuar sobre la coherencia constitucional y legal de las propuestas que presenten las entidades para modificar el marco legal y regulatorio de la seguridad digital. Es decir, que este proyecto regulatorio de la CRC en cumplimiento del CONPES debe ser sometido al concepto previo del Ministerio de Justicia y del Derecho

antes de nacer a la vida jurídica, de lo contrario la CRC estaría contraviniendo la disposición del CONPES y por lo tanto el acto administrativo estaría viciado de nulidad desde su nacimiento.
Solicitan a la CRC, confirme la fecha en la cual tiene proyectado que el Ministerio de Justicia y del Derecho, conceptuar sobre este proyecto regulatorio.

CRC Frente a la observación de COMCEL sobre la necesidad de que el Ministerio de Justicia y Derecho, conceptúe sobre la coherencia constitucional y legal de la propuesta regulatoria, el CONPES 3854 de 2016, establece exactamente lo siguiente:

> *"E2.2. Adecuar el marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes (DE2) El Ministerio de Justicia y del Derecho conceptuará sobre la coherencia constitucional y legal de las propuestas, que presenten el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, la Superintendencia de Industria y Comercio, el Departamento Administrativo Dirección Nacional de Inteligencia (DNI) y la Unidad de Información y Análisis Financiero (UIAF), para adecuar el marco legal y regulatorio relacionado con temas de seguridad digital, en torno a la dinámica de la economía digital y sus incertidumbres inherentes. Esta adecuación se llevará a cabo bajo el marco de los principios fundamentales de la política nacional de seguridad digital.*
> *Por su parte, la Comisión de Regulación de Comunicaciones (CRC) ajustará en 2017 el marco regulatorio del sector TIC. Lo anterior, lo hará teniendo en cuenta asuntos necesarios para la gestión de riesgos de seguridad digital, como la protección de usuarios de comunicaciones o el régimen de calidad de las redes de telecomunicaciones. Esto se hará aplicando la metodología de Análisis de impacto normativo, establecida en el Documento CONPES 3816"*

De este texto es claro que es exigible el concepto del Ministerio de Justicia y del Derecho únicamente para las propuestas que presenten el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, la Superintendencia de Industria y Comercio, el Departamento Administrativo Dirección Nacional de Inteligencia (DNI) y la Unidad de Información y Análisis Financiero (UIAF). Precisamente, lo referente a la CRC se encuentra en párrafo aparte aclarando que la CRC debe acogerse a los asuntos necesarios para la gestión de riesgos de seguridad digital, como la protección de usuarios de comunicaciones o el régimen de calidad de las redes de telecomunicaciones, aplicando la metodología de Análisis de impacto normativo establecida en el Documento CONPES 3816, y no se le hizo exigible la solicitud de concepto objeto del presente comentario.

3.8 Sobre la Agenda Regulatoria CRC 2017-2018

COMCEL
Resalta que en el CONPES 3854 de 2016 se define en su plan de acción que la CRC debía realizar una revisión del marco normativo del sector TIC en materia de seguridad de las comunicaciones, para apoyar el objetivo de crear las condiciones de forma que las múltiples partes interesadas gestionen los

riesgos de seguridad digital en sus actividades socioeconómicas, y se genere confianza en el uso del entorno digital, en atención a lo cual la CRC incluyó dentro de su Agenda Regulatoria 2017-2018 el proyecto denominado "Revisión del marco regulatorio para la gestión de riesgos de seguridad digital". Indican así, que la CRC estableció en su agenda regulatoria, el proyecto de revisión del marco regulatorio para gestión de seguridad digital, con un cronograma que incluía decisión regulatoria para el 4Q de 2017.

Es decir, a juicio de dicho operador, no se cumplió con los términos establecidos en la agenda regulatoria, mencionan que esta Comisión pretende expedir una regulación que genera altos impactos al sector, y que dada su complejidad requiere de un análisis a fondo, de la realización de mesas de trabajo, como se realizaron en su momento para expedir el CONPES, ya que pretende imponer unas obligaciones desproporcionadas en comparación con los objetivos del mencionado CONPES.

En consecuencia, solicitan a la CRC, que el proceso regulatorio se surta con la observancia de todas las garantías necesarias, como la publicación del Análisis de Impacto Normativo y el cumplimiento del cronograma inicialmente establecido.

CRC Frente a la observación de COMCEL sobre la necesidad de que el proceso regulatorio se surta con la observancia de todas las garantías necesarias, como la publicación del Análisis de Impacto Normativo, los términos establecidos en la agenda regulatoria y el cumplimiento del cronograma inicialmente establecido, la CRC cumplió con el compromiso del CONPES de adelantar y publicar el estudio durante 2017. Frente a los cambios en los tiempos previstos, se debe mencionar en primer lugar que la agenda regulatoria contiene plazos de carácter indicativo tal y como se dispone en el artículo 2.2.13.2.1 del Decreto Único Reglamentario 1078 de 2015 *"**Plan estratégico y agenda regulatoria.** Las Comisiones de Regulación tendrán la obligación de definir un plan estratégico para períodos mínimos de cinco (5) años y una agenda regulatoria anual de carácter indicativo".*

En segundo lugar, es de resaltar que precisamente los cambios en cronograma se dieron como respuesta a la solicitud del sector de brindar un espacio participativo adicional a los ya desarrollados, llevándose a cabo 3 mesas de trabajo realizadas en febrero de 2018, posteriores al análisis de comentarios recibidos del sector en el mes de diciembre de 2017. Como producto de las discusiones y el debate desarrollado en dichas mesas de trabajo, se tiene previsto volver a publicar el proyecto regulatorio con sus respectivos ajustes para discusión del sector, y se espera terminar el proyecto para segundo trimestre de 2018. Finalmente, en relación con el AIN le sugerimos revisar comentario previo donde la CRC da repuesta a las observaciones.

3.9 Sobre la necesidad de fomentar modelos de autorregulación

DIRECTV - ANDESCO

Propone que en congruencia con la política de prevención recientemente expedida por el Ministerio (PREVENTIC), esta Comisión opte por diseños normativos que se basen en la autorregulación, donde a través de las lógicas del mercado y la competencia se logre una cultura de cumplimiento para adquirir reputación y confianza en el consumidor por parte de los PRST. Al respecto, a nivel internacional, encuentran que la UIT ya promueve la co-regulación, donde el regulador y los regulados trabajan juntos con responsabilidades divididas, en un mundo donde convive la regulación y la autorregulación. Esto es fomentado precisamente por "la complejidad y la naturaleza cambiante del ecosistema TIC"[1]. Esta postura regulatoria, además de simplificar el marco regulatorio actual, brinda señales positivas para la realización de inversiones en el sector.

Adicionalmente, aconsejan que en aras de promocionar la flexibilización y simplificación regulatoria y normativa, se atiendan las sugerencias incluidas en la Agenda Empresarial 2018-2022 realizada recientemente por el Consejo Gremial Nacional –CGN-. En particular, el CGN propone disminuir la regulación mediante "i) Smart Regulation que propenda por la eficacia de la regulación, con mínimos costos y que permita la consecución de los objetivos de interés público, (ii) iniciativas como el 2x1 en materia regulatoria, que consiste en que por cada regulación nueva que se quiera implementar, se deben eliminar dos existentes (…)".

Exponen que una estrategia basada en la autoregulación se podría complementar con beneficios a nivel de imagen o reputación; por ejemplo, crear un sello del marco de seguridad y otorgarlo a compañías que demuestren cumplimiento. En este sentido, los operadores no estarían sujetos a mayores obligaciones regulatorias, pero tendrían mayores incentivos para mantener altos estándares de seguridad digital.

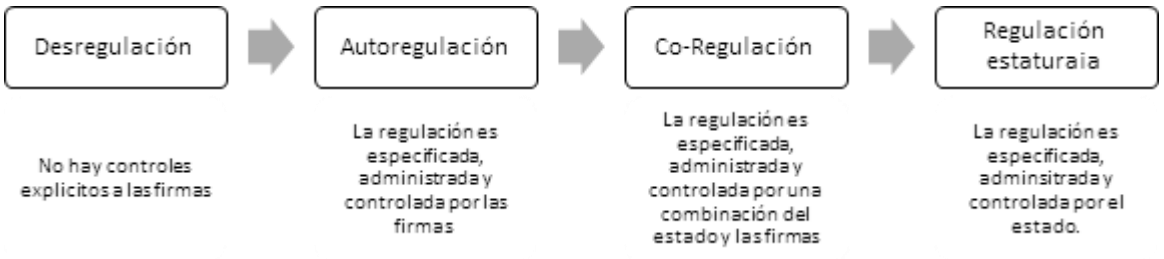
Por su parte, ANDESCO ha enviado una propuesta de redacción así para el artículo sobre sistemas de gestión de seguridad de la información así:

> *"ARTÍCULO 2. Autorregulación y adopción de Políticas de Seguridad Digital. Los proveedores de redes y servicios de comunicaciones deben adoptar una política de autorregulación sobre seguridad digital que contemple la utilización de recursos técnicos y logísticos tendientes a garantizar la seguridad digital de los servicios de telecomunicaciones, y la información manejada, procesada o almacenada durante la prestación de los mismos, implementando para ello un Sistema de Gestión de Seguridad de la Información, siguiendo los estándares de la familia de normas ISO/CEI 27000 de acuerdo con las características y necesidades propias de la red y del negocio.*

El proveedor deberá adoptar un proceso de evaluación, gestión y tratamiento de riesgos de seguridad digital, conforme con las buenas prácticas existentes sobre la materia."

CRC El proyecto adelantado por esta Comisión se centra en el mandato del CONPES 3854 de 2016 de ajustar el marco normativo para la gestión de riesgos de seguridad digital en el sector TIC y a eso se ha limitado el alcance del mismo. Este proyecto busca tener unos parámetros comunes, pero son los operadores los llamados a decidir el alcance específico de sus políticas de gestión de riesgos de seguridad de la información y sus políticas de gestión de incidentes de seguridad de la información, de acuerdo con las condiciones propias de su operación. En este sentido, las modificaciones realizadas a la propuesta acogen parcialmente esta observación y proponen la implementación de dichas políticas en un marco flexible y ajustado a la realidad de cada PRST.

Al respecto, esta Comisión ha analizado el alcance que debe tener la decisión, usando como referencia un modelo lineal que clasifica la intervención como un punto en el espectro entre desregulación y regulación estatutaria clásica (Peter Vass, 2005). Este modelo, aunque limitado (a menudo es difícil categorizar un esquema regulatorio en una sola dimensión), es una generalización de las conceptualizaciones más sofisticadas de regulación y autorregulación adoptadas por varias organizaciones, como la Better Regulation Task Force (BRTF) del Reino Unido y el Consejo Nacional del Consumidor (CNC) de este mismo país, e internacionalmente, por la OCDE, y la Comisión Europea.



En particular, en la categoría de **co-regulación** se clasifican las intervenciones donde el Estado se limita a establecer un marco normativo que deberá ser seguido por las firmas o asociaciones particulares para elaborar de manera **autónoma** sus propios procesos y modelos, dentro de un marco señalado, y donde el Estado generalmente se encarga de verificar o supervisar que los llamados autorregulados cumplan los mismos.

En este sentido, la propuesta actual podría clasificarse como un esquema de co-regulación dentro de la categoría de autorregulación. En este caso el marco general es la familia de estándares ISO/IEC 27000, y es en este marco que los PRST pueden determinar de manera autónoma el alcance de sus políticas de seguridad de la información.

La propuesta actual recoge la intención de dar a los proveedores de servicios de comunicaciones la autonomía suficiente para desarrollar y evolucionar sus políticas de seguridad de la información. Esta autonomía es especialmente efectiva en un ambiente caracterizado por un alto grado de innovación como el de la ciberseguridad. La propuesta introduce además los mecanismos mediante los cuales el Estado puede supervisar la efectividad de dichas Políticas (almacenamiento y reporte de incidentes) y dependiendo de los resultados eventualmente trascender a un esquema de desregulación o de regulación prescriptiva clásica. Estos mecanismos de transparencia son un componente fundamental de las políticas de autorregulación.

Por su parte, la propuesta del sello del marco de seguridad es una idea que puede considerarse para revisiones futuras de esta temática, cuando se alcancen mayores niveles de gestión de seguridad digital a nivel transversal en el sector TIC.

3.10 Sobre el proceso participativo

Fundación KARISMA

Resaltan que la CRC tiene mejores prácticas de solicitud de comentarios que otras entidades del Gobierno en su sector. En particular, otorgar un plazo de 15 días hábiles (descontando festivos) para el análisis de un documento es más sensible que otras prácticas. Ahora bien, sugieren que se pueden mejorar otras prácticas: publicar el cronograma del proceso participativo, su metodología y acompañar el documento con un informe técnico que dé cuenta del proceso que llevó a que la CRC produjera esta reglamentación —los modelos que usaron, los argumentos que los llevaron a tomar las elecciones que tomaron, etcétera—.

CRC Frente a la observación de KARISMA de mejorar prácticas participativas en los proyectos regulatorios, se aclara que ya es una realidad, pues dentro del presente proyecto la CRC publicó un informe técnico donde se explica la motivación inicial de la propuesta, divulgó los cronogramas de participación junto con la publicación de la propuesta, documento soporte y proyecto de resolución; y posteriormente se realizaron las invitaciones para las mesas de trabajo solicitadas por los agentes interesados en la temática propuesta, las cuales se llevaron a cabo en el primer trimestre de 2018.

Lo anterior, en cumplimiento del Decreto Único Reglamentario 1078 de 2015 donde en su Capítulo 3, artículo 2.2.13.3.2 y artículo 2.2.13.3.3 se define el marco que debe aplicar la CRC en cuanto a la publicidad de proyectos de regulación, así como el contenido mínimo del documento que haga públicos los proyectos de regulación de carácter general, no tarifarios.

3.11 Sobre la confidencialidad de los datos

KARISMA

Manifiestan que se puede hacer un paralelo a lo que existe en la Unión Europea (UE) —Directiva n°2009/136/CE, artículo 3—, que establece que los operadores de telecomunicaciones tienen la obligación de notificar a las autoridades de aquellos incidentes de seguridad en donde se ven comprometidos datos personales. Es de notar que en 2018, con la entrada en vigor del Reglamento 2016/679 sobre protección de datos artículo 33), la notificación se ha generalizado a otras entidades y sin que haya ningún criterio de porcentaje de personas afectadas. Solamente existe una obligación de notificación de las brechas de seguridad en donde se afectan datos personales.

Por lo tanto, sugieren complementar este proyecto de resolución, extendiendo explícitamente la obligación de notificación frente a pérdidas de integridad y de confidencialidad, en particular cuando hay involucrados datos personales.

Proponen adoptar una aproximación similar a la europea en la que cualquier brecha de seguridad que comprometa datos personales debe ser notificada a las autoridades competentes del Estado, incluso si concierne a una sola persona.

CRC Frente a la observación de KARISMA sobre la necesidad de adoptar una aproximación similar a la europea en la que cualquier brecha de seguridad que comprometa datos personales deba ser notificada a las autoridades competentes del Estado, incluso si concierne a una sola persona, conforme a lo que rige para la Unión Europea (UE) —Directiva n°2009/136/CE, no es posible atender el comentario puesto que es un tema ya cubierto en las normas nacionales de acuerdo con lo dispuesto en la Ley Estatutaria 1581 de 2012, donde se establece en su artículo 17 que es la Superintendencia de Industria y Comercio, a través de una *Delegatura para la Protección de Datos Personales, quien ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.* Aunado a lo anterior, vemos que es el Congreso de la República quien está legitimado para adoptar cambios normativos y protocolos en materia de datos personales.

Lo anterior no choca con lo que ya ha sido implementado y aplicado en el sector TIC frente al manejo de datos personales, pues como se puede observar del proyecto de resolución publicado, en la parte motiva del mismo se deja plasmado que el artículo 53 de la Ley 1341 de 2009 consagra el derecho de los usuarios a "recibir protección en cuanto a su información personal, y que le sea garantizada la inviolabilidad y el secreto de las comunicaciones y protección contra la publicidad indebida, en el marco de la Constitución Política y la Ley". Y que las anteriores disposiciones guardan armonía con las normas expedidas en el marco de la Comunidad Andina de Naciones, en particular la Decisión 638 de 2006 que obliga a garantizar el derecho de los usuarios a "la privacidad e inviolabilidad de sus telecomunicaciones,

así como al mantenimiento de la reserva de todos los datos personales vinculados al servicio adquirido y que han sido suministrados a terceros, salvo en los supuestos de excepción que prevea su normativa interna".

3.12 Sobre la necesidad de interacción en casos de ciberataque

Jeimy Cano
Indica que no se especifica cómo deben responder las empresas de telecomunicaciones frente a un ciberataque. En este sentido, habría que entender qué es un ciberataque y cómo se coordina la acción de respuesta o contención, para lo cual debe estar articulado con el comando conjunto cibernético. Pregunta si es posible categorizar un ciberataque como causa de un incidente o definitivamente se requiere una definición distinta.

CRC Respecto a esta observación, se hace explicito que el CONPES 3854 ha dispuesto que sea el colCERT el encargado de coordinar las acciones relacionadas con ciberataques. El esquema que se propone en el proyecto es que los operadores realicen un reporte inicial al colCERT (5.1.2.3.3 de la propuesta), para que luego esa entidad coordine las acciones necesarias dentro de la institucionalidad para dar respuesta a los mismos en caso de necesitar respuesta.

4. Observaciones al articulado del proyecto de resolución de la primera publicación

4.1 Sobre las definiciones:

4.1.1 COLOMBIA TELECOMUNICACIONES – ETB – TIGOUNE – COMCEL - NAP COLOMBIA

Estos operadores manifiestan que las definiciones propuestas en el proyecto resultan demasiado amplias para su aplicación, consideran que con las definiciones propuestas no sería posible determinar el límite entre violaciones a la seguridad y pérdidas de integridad, adicionalmente ETB y Colombia Telecomunicaciones, indican que la referencia a "degradaciones excesivas", no indica el porcentaje de desempeño a partir del cual se puede empezar a hablar de una degradación excesiva, así mismo según estos operadores podría entenderse que la degradación de un canal de transmisión haría parte del grupo de incidentes que se deberían reportar, aun cuando los mismos no necesariamente estén relacionados con temas de seguridad de la información, aducen que las definiciones propuestas resultan ambiguas y de difícil aplicación.

Por último, Colombia Telecomunicaciones, TIGO-UNE, NAP Colombia y COMCEL, manifiestan que las definiciones de "Evento de Seguridad de la Información" e "Incidente de seguridad de la información" dispuestas en el estándar ISO/IEC 27001 permiten acotar en mejor medida y con mayor claridad el alcance esperado en el proyecto de resolución.

CRC Sobre el particular es de mencionar que las definiciones inicialmente propuestas estaban atadas al concepto de integridad del servicio por dos razones, i) se consideraba beneficioso atar los incidentes de seguridad a aquellos que afectan los servicios de comunicaciones para evitar riesgos de reporte de incidentes poco significativos, ii) la definición propuesta inicialmente para los incidentes de seguridad se adoptó de acuerdo con el documento *Technical Guideline on Incident Reporting* publicado por la Agencia Europea para la seguridad de las redes y la información ENISA[3], la misma incorpora el concepto de "Integridad de red". Por tanto, teniendo en cuenta las observaciones presentadas por las múltiples partes interesadas y las conclusiones de la mesa de trabajo adelantada el 01 de febrero de 2018, la definición de Incidente de Seguridad originalmente propuesta ha sido reemplazada por la definición de "Incidente de Seguridad de la Información" según lo dispuesto en el estándar ISO/IEC 27001. Con estos cambios se reconoce la alta adopción que la familia de estándares ISO/IEC 27000 tiene en los operadores colombianos. Se espera que las modificaciones introducidas permitan una adopción más natural por parte de los PRST que ya habrían implementado dicho estándar, así mismo su alta adopción a nivel global facilita la obtención de insumos de capacitación y despliegue en aquellos operadores que aún no han adoptado dicho estándar.

Frente a la observación según la cual no se establecieron umbrales de desempeño a partir de los que se podría determinar la presencia de una "degradación excesiva" en la definición de "Integridad de servicio", es de aclarar que la misma es tomada de la Recomendación ITU-R M.1224-1 *Vocabulary of terms for International Mobile Telecommunications*, y su uso en la literatura sobre la materia no requiere de definiciones de umbrales específicos. Sin embargo, teniendo presente las modificaciones realizadas a la definición de "Incidente de Seguridad", se ha eliminado esta definición.

Por último, frente a la pertinencia de adoptar las definiciones de Evento de Seguridad de la Información e Incidente de seguridad de la información planteadas en el estándar ISO/IEC 27001, y de acuerdo con las observaciones presentadas y las conclusiones de la mesa de trabajo correspondiente, se acoge esta observación, y dicha modificación se evidenciará en la redacción de este artículo.

---

[3] ENISA (2014). Technical Guideline on Incident Reporting. Disponible en: https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting

4.1.2 ETB

El operador solicita aclarar el concepto de "Afectación significativa", del artículo 5.1.2.3.2. INCIDENTES DE SEGURIDAD, así mismo pide que se indique si en la tabla referente deben considerarse afectaciones significativas aquellos incidentes que tengan una afectación en cantidad de usuarios y duración correspondientes con las casillas marcadas con la palabra "SI".

CRC Respecto a la observación de ETB, se aclara que la tabla originalmente propuesta en el Artículo 5.1.2.3.2. tenía el objetivo de categorizar las afectaciones significativas teniendo en cuenta las variables de duración del incidente y usuarios afectados, sin embargo, de acuerdo con las observaciones presentadas al concepto de Afectación significativa, ha sido eliminado, junto con la tabla asociada.

4.1.3 TIGOUNE

Para el operador la definición de integridad del servicio en el proyecto de Resolución no resulta técnica, y se encontraría alejada del núcleo del objeto regulatorio sobre la seguridad digital, a su juicio la misma se desvía a aspectos concernientes con el Régimen de Calidad del Servicio. Manifiesta no encontrar referencias técnicas para soportar qué se debe entender por degradaciones excesivas, por lo cual sugiere eliminar dicha definición del proyecto regulatorio.

CRC Respecto a la observación de TIGOUNE, se aclara que la definición es tomada de la Recomendación ITU-R M.1224-1 *Vocabulary of terms for International Mobile Telecommunications*, sin embargo, teniendo en cuenta otras observaciones allegadas (ver respuesta 4.1.1) la definición de Integridad del Servicio ha sido eliminada.

4.1.4 COMCEL

Manifiesta que las definiciones propuestas en el proyecto de resolución desconocen y pasan por alto, el glosario del CONPES 3854 de 2016 que incorporaría las definiciones del documento "Directrices de la OCDE sobre gestión del riesgo de la seguridad digital para la prosperidad económica y social" (2015).

Según el operador, la CRC estaría haciendo interpretaciones particulares acerca de las definiciones, que se alejan de la teoría general de la seguridad digital y del estado del arte en la materia. Indica que esto podría evidenciarse al analizar la propuesta de definición de Incidente, la cual no incluye "eventos de seguridad" y en cambio hace referencia a "violación de la seguridad" lo cual se distanciaría de las fuentes consultadas por el operador OCDE, la UIT e ISO 27000.

Así mismo, para la definición de Integridad, aduce que la propuesta de la CRC dista de las definiciones de la OECD e ISO 27000.

El operador incluye una tabla comparativa y una síntesis de las distintas definiciones adoptadas para el modelo de riesgos de seguridad digital, el CONPES 3854, ISO 27000 y UIT-T E.409

Por último, manifiesta que la CRC no debe realizar interpretaciones de las definiciones que ya están incluidas en el CONPES ni crear nuevas definiciones y sugiere eliminar el artículo de definiciones.

CRC En relación con las observaciones presentadas por COMCEL, se hace explicito que las definiciones originalmente propuestas fueron adoptadas de recomendaciones y normas internaciones especializadas, (*Technical Guideline on Incident Reporting,* publicada por la Agencia Europea para la Seguridad de las Redes y la Información ENISA y *Vocabulary of terms for International Mobile Telecommunications* publicada por la UIT), por lo que las mismas no son interpretaciones de la CRC, sin embargo, teniendo en cuenta otras observaciones allegadas (ver respuesta 4.1.1) se han incorporado las definiciones de Evento de Seguridad de la Información e Incidente de Seguridad de la información, en línea con lo observado por COMCEL, lo cual se verá reflejado en la redacción del artículo.

4.1.5 KARISMA

La fundación considera que las definiciones propuestas se encuentran demasiado enfocadas al concepto de "integridad del servicio". Manifiestan que esta Comisión estaría haciendo un uso inadecuado de la palabra "integridad"; consideran que el texto propuesto quiere orientarse a la "disponibilidad del servicio".

La Fundación cita el estándar ISO 27000, en particular el tratamiento que se da en la norma a la seguridad de la información como manera de preservar la disponibilidad (propiedad de estar accesible y utilizable a pedido de una entidad autorizada de la información, en los horarios previstos), la confidencialidad (propiedad de que la información no esté disponible o sea divulgada a individuos, entidades o procesos no autorizados) y la integridad (cualidad de exactitud y exhaustividad de la información) de los datos.

Por esta razón indican que la resolución debe tratar explícitamente esos tres temas y, en particular, la confidencialidad de la información de las personas que es recolectada, almacenada, procesada y transmitida por los proveedores de redes y servicios de telecomunicaciones. Sobre este particular la Fundación considera que la definición (cf. tabla) de "afectación significativa" debería ser mucho más

estricta en cuanto a la cantidad de personas afectados. A juicio de Karisma la fuga de datos personales que impacte 1.000 personas, no cumpliría necesariamente con el criterio de 1% que establece el proyecto. No obstante, se trataría de un incidente grave que podría impactar fuertemente a las personas afectadas.

CRC En primer lugar, es de aclarar que el concepto de Integridad propuesto originalmente en la redacción de este artículo debe entenderse en línea con la literatura técnica sobre redes e interconexiones de red[4] y no como tradicionalmente se usa en la técnica sobre seguridad de la información, donde el término "Integridad" de manera general se refiere a la propiedad que tienen los datos o las comunicaciones cuando no han sido alterados o modificados, por lo tanto se hace explícito que la redacción original era intencional y no se trataba de un uso inadecuado de la palabra "Integridad" (ver respuesta 4.1.1).

En segundo lugar, frente a las observaciones sobre los conceptos de disponibilidad, confidencialidad e Integridad propuestos en el estándar ISO/IEC 27001, si bien esta Comisión coincide en que el tratamiento presentado en la norma es apropiado, no se considera necesario incorporar estas definiciones para alcanzar los objetivos planteados en el proyecto, de acuerdo con las conclusiones presentadas en la respuesta 4.1.1 resulta suficiente con la definición de eventos e incidentes de seguridad de la información.

Finalmente, respecto a los umbrales definidos para "afectación significativa" se aclara que este concepto ha sido eliminado de la propuesta (ver respuesta 4.1.2). Adicionalmente, se recuerda que incidentes que involucren datos personales son competencia de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, por lo que los umbrales originalmente definidos no le serían aplicables a este tipo de incidentes.

4.2 Sobre la información de incidentes de seguridad:

4.2.1 COLOMBIA TELECOMUNICACIONES -COMCEL

COLOMBIA TELECOMUNICACIONES manifiesta no tener claridad sobre el tipo de información al que hace referencia el Artículo ni el tiempo por el cual deba ser almacenada la misma, indica además que si se hace referencia a información como logs de sistemas, estos solo son consultados y almacenados de manera temporal, mientras se realiza la investigación sobre el posible evento y/o incidente de seguridad,

[4] Ward, K, 1995, 'The Impact of Network Interconnection on Network Integrity'. British Telecommunications Engineering

porque el tamaño de este tipo de archivos sería bastante alto, lo que, según el operador generaría altas inversiones lo que, de acuerdo con el operador, resultaría ineficiente.

Asimismo, manifiesta que la información que almacena actualmente contiene los soportes relacionados con los resultados del proceso de investigación y diagnóstico del incidente y que proviene de las alertas del sistema de gestión, entre otro tipo de evidencias que consideran relevante para el correcto diagnóstico de la situación.

El operador solicita a la CRC aclarar si el almacenamiento de la información se refiere únicamente al reporte mencionado en el artículo.

Frente a este Punto COMCEL señala que, debido a los costos y esfuerzos operativos para almacenar la información, la misma debería almacenarse únicamente por 6 meses.

CRC Frente a las observaciones allegadas, se aclara que la información que debe ser almacenada y puesta a disposición es la referida en la tabla contenida en el proyecto de resolución para el artículo 5.1.3.2 y que cuenta con los campos de Fecha del incidente, Servicio Afectado, Número de Usuarios afectados, Duración, y Categoría del incidente, por tanto, información adicional como logs de sistemas puede ser enviada de manera voluntaria a la entidad responsable, colCERT.

Ahora bien, teniendo en cuenta que el CONPES 3854 busca también contribuir al fortalecimiento del colCERT como entidad coordinadora de la gestión de incidentes de seguridad de la información para las autoridades colombianas, y es un aspecto tratado en la propuesta regulatoria de la CRC, se considera que con un nivel importante de colaboración, el almacenamiento de la información a largo plazo sobre los incidentes, puede ser responsabilidad del colCERT por lo que se acoge la observación de COMCEL, lo cual quedará plasmado en la redacción del artículo.

4.2.2 COLOMBIA TELECOMUNICACIONES – TIGOUNE – COMCEL

Manifiestan que en este mismo artículo (5.1.2.3.2. INCIDENTES DE SEGURIDAD) se presentaría una duplicidad con las obligaciones del régimen de calidad, indican que la información solicitada cuando se identifique un incidente de seguridad en el proyecto de resolución, la cual incluye: Fecha del Incidente, Servicio afectado, Número de usuarios afectados, Duración y Causa del incidente, sería incompatible con la denominación "incidente de indisponibilidad", por cuanto el régimen de calidad que se está modificando con esta resolución, determina ya una metodología de medición de la disponibilidad del servicio y unos umbrales de cumplimiento de acuerdo con el ámbito de medición, además de establecer

una definición de afectación de servicio y un procedimiento de reporte a la autoridad de vigilancia con las razones por las cuales hubo indisponibilidad.

Por lo tanto, COLOMBIA TELECOMUNICACIONES propone que, para evitar posibles malas interpretaciones al momento de determinar la "indisponibilidad" y el servicio afectado, se use la siguiente redacción:

"En este campo deberá indicarse el o los servicios con afectación por incidentes de seguridad, de acuerdo con los umbrales cuantitativos de la tabla XX"

Por su parte el operador TIGO UNE sugiere la eliminación de las tipologías con causas distintas a actores y/o software malicioso.

CRC Respecto a estas observaciones, teniendo en cuenta las modificaciones realizadas a la definición de Incidente de Seguridad, y atendiendo a que la misma ya no incorpora elementos de integridad o disponibilidad del servicio, se acogen las sugerencias, modificando la redacción para mantener el alcance de la información solicitada acotada a la dimensión de seguridad de la información.

4.2.3 COLOMBIA TELECOMUNICACIONES - COMCEL

Respecto al campo "Causa del incidente", COLOMBIA TELECOMUNCACIONES y COMCEL solicitan a la Comisión hacer una revisión de las tipologías que se incluyen en el reporte, manifestando su desacuerdo con la inclusión de las tipologías para fenómenos naturales y fallas externas al operador, las cuales a su juicio no harían referencia a eventos o incidentes de seguridad y ya estarían siendo reportados a través de las obligaciones impuestas en el régimen de calidad.

COLOMBIA TELECOMUNICACIONES manifiesta entender la motivación del artículo, sin embargo, solicita a la Comisión evitar que los PRST tengan que realizar un doble reporte de la información y que lo que se solicite a través de este proyecto de resolución se limite únicamente a la dimensión de seguridad de la información.

CRC Respecto a los comentarios allegados sobre el campo Causa del incidente, y teniendo en cuenta los argumentos presentados, así como las conclusiones de la mesa de trabajo llevada a cabo el 08 de febrero de 2018, se modifica el campo *Causa del Incidente*, reemplazándose por *Categoría del Incidente.* En el mismo se han eliminado todas aquellas categorías asociadas a disponibilidad del servicio y se enfocan en la dimensión de seguridad de la información tal como se indica en el comentario. Así mismo, para estandarizar estas categorías se adoptan las categorías presentes en el Anexo B del estándar internacional ISO/IEC 27035-*1* - *"Information security incident management",* las cuales corresponden

a: *Denegación de servicio, Acceso no autorizado, Malware, Abuso, Recopilación de información de sistema,* y así se verá reflejado en la redacción del Artículo.

4.2.4 COMCEL

Indica que el mapeo de incidentes, de acuerdo con lo propuesto por la Comisión, implicaría intervenir y ver el tráfico de todos los usuarios, y que, de ser así, el proyecto de resolución estaría en contra de la neutralidad de red y de la ley de protección de datos personales. Asimismo, el operador manifiesta que no existe una forma operativa práctica de hacer este proceso.

El operador solicita realizar los siguientes ajustes al artículo:

1. Usuarios afectados:

"Nota: El porcentaje de usuarios afectados, se calculará sobre la base total de usuarios del ~~servicio específico de comunicaciones~~ operador de acuerdo con el último trimestre reportado.

%Usuarios afectados = Usuarios potencialmente afectados/base total de usuarios del operador

Se considera, que el número potencial de usuarios afectados son aquellos usuarios que hayan utilizado el servicio de manera continua al menos las últimas 4 semanas durante el mismo intervalo de tiempo (día y hora) en el que se presentó el incidente de seguridad y que dejaron de utilizarlo como resultado del incidente de seguridad."

2. Servicio afectado:

La indisponibilidad incluida en este campo se encontraría ya desarrollada en el Régimen de calidad, COMCEL considera que la CRC está cometiendo un error al incluir la indisponibilidad cuando está tratando de categorizar los incidentes de seguridad. Sugiere eliminar la palabra indisponibilidad, en su lugar incluir la palabra seguridad.

Se entiende que este numeral se refiere a incidentes de seguridad que afectan la infraestructura a través del cual el operador presta el servicio de transmisión de datos y llamadas de voz.

3. Duración: sugiere la siguiente redacción:

"Duración: En este campo debe indicarse el tiempo en horas de ~~indisponibilidad del~~afectación del servicio debido al incidente de seguridad."

4. Causa del incidente:

A juicio del operador las causas de incidentes listadas no atienden a eventos relacionados con seguridad, por lo cual sugieren eliminar las causas anteriores y tener en cuenta las siguientes:
a. Denegación de Servicio: Incidentes relacionados con ataques de denegación de servicios (DOS) o denegación de servicios distribuida (DDoS).
b. Infección por malware: Incidentes provocados por malware (virus, gusanos, troyanos, bombas lógicas, spyware, rootkits, ransomware)
c. Vulnerabilidad: Cualquier tipo de incidente provocado por la explotación de una vulnerabilidad en sistema.

CRC Frente a las observaciones presentadas por COMCEL, se aclara que la información solicitada no requiere de manera alguna la intervención del tráfico de los usuarios. Se invita al operador a explicar de manera concreta en qué medida sería necesario intervenir este tráfico, dado que no resulta claro cómo ha llegado a esta conclusión y de acuerdo con los análisis adelantados por la Comisión, el requerimiento de información de que trata el Artículo, se encuentra en línea con los estándares internacionales que no prevén este nivel de intervención ni contravención alguna a los principios de Neutralidad de Red.

En relación con las observaciones específicas planteadas, se considera que el porcentaje de usuarios afectados debe calcularse sobre los servicios y no sobre la base total de usuarios, esta distinción permite entender de manera más granular el impacto de los incidentes sobre los servicios suministrados. Para los campos *Servicio Afectado* y *Duración,* las observaciones son pertinentes y así se reflejará en la redacción del artículo; como respuesta a las observaciones presentadas para el campo *Causa del Incidente* se invita a consultar la respuesta 4.2.3 donde se explican las modificaciones realizadas.

4.2.5 ANDESCO

La agremiación propone una redacción donde sugiere un reporte de incidentes "críticos" con una periodicidad de 20 días a la CRC, dicho reporte incluiría la descripción del incidente, la fecha y si el mismo requiere o no de intervención del colCERT, en la misma redacción se propone que el almacenamiento de incidentes sea por 12 meses y se realizaría según la clasificación de colCERT.

CRC Frente a la propuesta de ANDESCO, se recuerda el objetivo del CONPES 3854 de fortalecer las capacidades del colCERT como entidad coordinadora de la gestión de incidentes de seguridad de la

información para las autoridades colombianas. En este sentido, el reporte periódico propuesto no permite la gestión de incidentes "críticos" por parte de las autoridades, en los cuales se considera beneficiosa la cooperación entre las múltiples partes interesadas. Adicionalmente, la clasificación interna del colCERT, aunque adecuada para su misionalidad, puede resultar difícil de integrar dentro de los Sistemas de Gestión de Seguridad de la Información propuestos, dado que los criterios de clasificación no necesariamente se encuentran alineados con la familia de estándares ISO/IEC 27000, y se definen de acuerdo con las "características potenciales del ciberdelincuente". Por lo anterior, no se acoge la observación.

En cuanto al hecho que sea la CRC la responsable de almacenar la información de incidentes de seguridad de la información, consideramos que con una adecuada cooperación entre las múltiples partes interesadas, es posible que a largo plazo el colCERT, así como las otras entidades encargadas de la seguridad y defensa del entorno digital (CCOC y CCP), cuenten con los insumos de información para mejorar sus capacidades operativas. Si bien la información de incidentes de seguridad de la información resulta valiosa para la CRC a la hora de establecer una línea base sobre frecuencia e impacto de los incidentes en el sector, así como para evaluar la eficacia del marco regulatorio de seguridad digital, dicha información cobra aun mayor relevancia en el accionar de las entidades nacionales encargadas de la ciberseguridad y ciber defensa, y resulta fundamental para que las mismas se conviertan en los puntos focales a la hora de obtener información sobre el estado de la seguridad digital en Colombia.

4.3 Sobre los reportes de incidentes de seguridad a las autoridades:

4.3.1 COLOMBIA TELECOMUNICACIONES - COMCEL

Los operadores manifiestan que la propuesta de reportar los incidentes dentro de las 2 horas subsecuentes a su detección resultaría inviable, aducen que es imposible determinar la causa de un incidente en 2 horas, dado que de acuerdo con COLOMBIA TELECOMUNICACIONES la identificación de un incidente de seguridad parte de la detección de comportamientos atípicos de tráfico a través de la gestión que se realiza sobre la red u otras alertas, por lo que en la mayoría de los casos se requeriría una investigación, y análisis que sobrepasa las 2 horas, por lo que COLOMBIA TELECOMUNICACIONES solicita modificar la redacción para que el tiempo de reporte sea a partir de la identificación de la causa. De otra parte, COMCEL considera que este reporte debe ser eliminado.

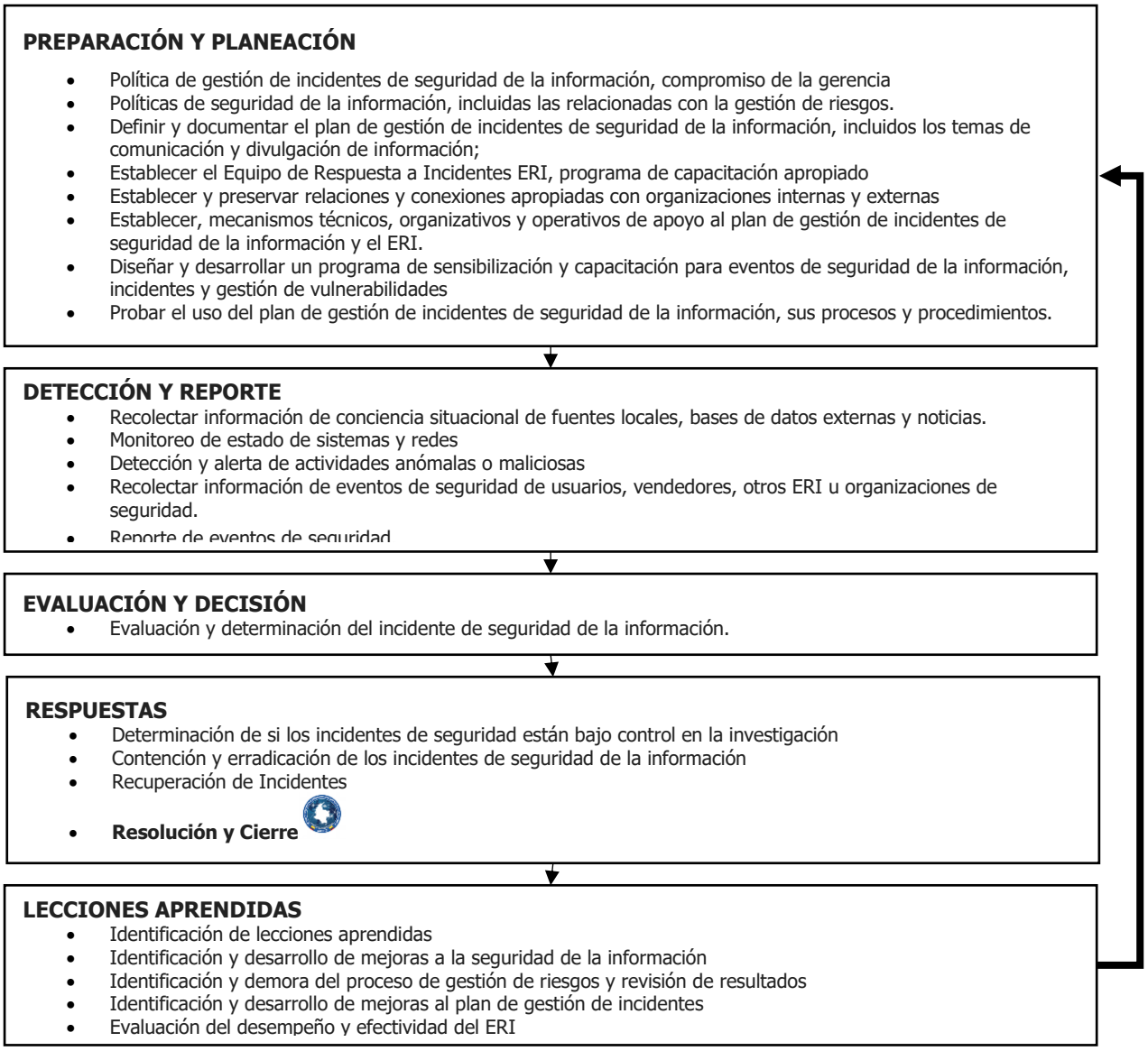
CRC Teniendo en cuenta los argumentos planteados y las conclusiones de la mesa de trabajo, llevadas a cabo el 15 de febrero de 2018, donde se discutieron las diferentes opciones de reporte de información a las autoridades, incluyendo la opción de eliminar esta obligación, esta Comisión reconoce que la identificación de las causas, vectores y demás información pertinente a los Incidentes de Seguridad de

la Información, requiere de actividades de investigación que pueden resultar inviables bajo la propuesta inicial de reporte dentro de las 2 horas subsecuentes a la identificación. Por lo anterior, y si bien la política de gestión de incidentes puede variar en cada organización, típicamente es posible identificar cinco fases para la gestión de Incidentes – Ver Ilustración 1(ISO/IEC 27035-1), para no afectar el proceso normal de gestión de incidentes. Por tanto, la CRC propone que el reporte a las autoridades se realice de forma posterior en la fase de respuestas, esto es, después del cierre del incidente y antes de las actividades de la fase de lecciones aprendidas, en línea con lo discutido en la mesa de trabajo indicada.

Dentro de las conclusiones de la citada mesa, se encontró también que la colaboración y reporte a las autoridades resulta necesaria cuando se trata de Incidentes de Seguridad de la Información clasificados como "Críticos" o "Muy Serios", o en general, aquellos que pueden generar un alto impacto a las operaciones. Por lo anterior, y ante la necesidad de estandarizar el criterio de evaluación con el cual se determinará los incidentes que deben ser reportados en la fase de detección, se propone utilizar una clasificación equivalente al Anexo C del estándar ISO/IEC 27035-2:2016. En dicho anexo se clasifican los incidentes de acuerdo con su severidad utilizando la escala de la Ilustración 2.

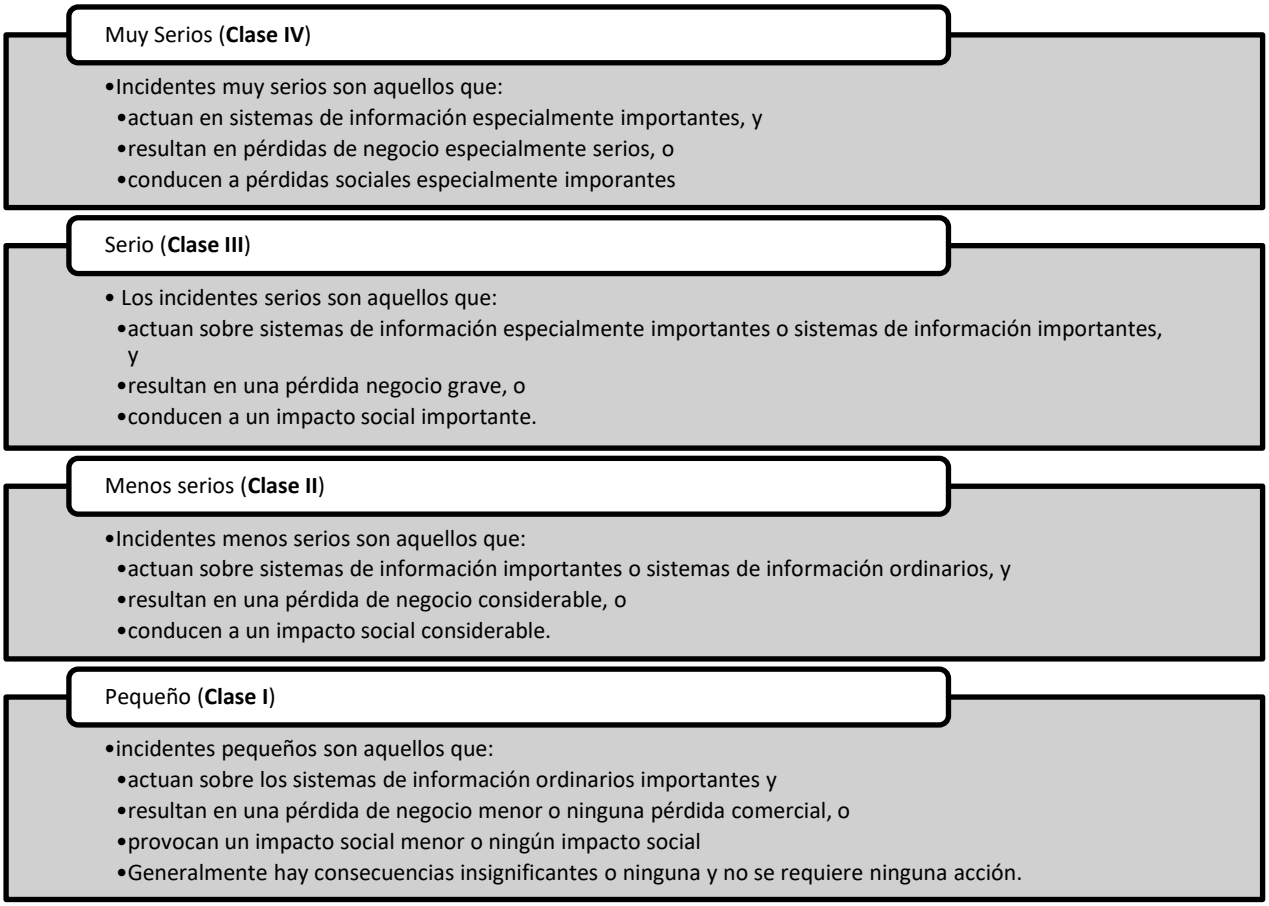
En particular, la redacción del artículo retoma la ejemplificación del anexo y se propone que, cuando los incidentes actúen sobre sistemas de información importantes o resulten en pérdidas graves para la organización, o impliquen pérdidas sociales importantes (Clases IV y III), los PRST realicen un reporte inicial con la información disponibles a colCERT. Por lo tanto, si bien no se acogen de manera textual las observaciones presentadas, si se realizan ajustes orientados a atender los comentarios allegados.

Ilustración - Fases de la gestión de incidentes de seguridad de la Información



Fuente: ISO/IEC 27035-1:2016

Ilustración 1 Clasificación de severidad de los incidentes



Fuente: ISO/IEC 27035-2:2016

4.3.2 COLOMBIA TELECOMUNICACIONES – COMCEL

De otra parte, COLOMBIA TELECOMUNICACIONES y COMCEL solicitan que se establezca el procedimiento mediante el cual se van a reportar los incidentes, el canal correspondiente, la responsabilidad y las obligaciones que colCERT tendrá sobre la información que va a ser reportada, así como el uso que se le va a dar a la misma, manifiestan que esta información resultaría confidencial dada su sensibilidad al exponer eventos que afectaron el desempeño de la red y la prestación de los servicios de telecomunicaciones. Es información que debe ser tratada de manera confidencial.

CRC Frente a las observaciones presentadas, se hace explicito que de acuerdo con las previsiones del CONPES 3854 de 2016, es el colCERT la entidad llamada a convertirse en el punto focal nacional para la gestión de incidentes digitales en Colombia, en esta misma línea se estableció en dicha política el objetivo estratégico E.4.2. Adecuar el marco jurídico para abordar la protección y defensa del entorno nacional (DE2) en donde se dispone que, "*La adecuación del marco jurídico deberá buscar, además, el reporte obligatorio de incidentes cibernéticos al colCERT por parte de los propietarios u operadores de infraestructuras críticas cibernéticas nacionales y demás partes interesadas, con las previsiones respectivas de confidencialidad, privacidad, entre otros aspectos.*" , por lo cual el desarrollo normativo realizado por la CRC responde a la necesidad de crear las condiciones para que el sector de las comunicaciones se encuentre alineado con los objetivos estratégicos nacionales en materia de seguridad digital.

Adicionalmente, en la mesa de trabajo del 8 de febrero de 2018, el colCERT presentó a las múltiples partes interesadas los mecanismos de reporte de información disponibles, así como las previsiones de seguridad y confidencialidad de la información adoptadas por dicha entidad. Es importante resaltar también que los operadores pueden determinar el nivel de reserva que debe darse a la información entregada y manifestarlo expresamente a la entidad receptora de la información, ello siempre y cuando cumpla con los requisitos de reserva de la información dispuestos en la Ley 1712 de 2012. Por último, esta Comisión ha realizado recomendaciones específicas al colCERT para la creación de una plataforma de reporte de incidentes.

4.3.3 ETB

El operador solicita tiempo para la aplicación e implementación de los nuevos procedimientos que le permitan dar cumplimiento a las disposiciones en materia de reporte de incidentes, sugieren que este tiempo no sea inferior a 6 meses.

CRC Respecto al comentario allegado por el operador, en el sentido de otorgar un plazo suficiente para la implementación de los procedimientos y disposiciones de la resolución, se aclara que la vigencia de la resolución Artículo 4, ya se define un plazo superior al propuesto por el operador.

4.3.4 TIGOUNE

El operador señala que la identificación de ciber incidentes requiere de interacción con diversos actores como proveedores de antivirus, casas de software, fabricantes de equipos, e involucra interacciones de ingeniería, operaciones, entre otros. Indica que una vez identificado el incidente y desplegada la comunicación con los actores relevantes, se establecen variables probables que están sujetas de

verificación de toda la cadena de actores referidos, lo cual requeriría de tiempos razonables para sus análisis, generando que la detención inicial sea apenas preliminar y requiera el análisis en las horas o días subsecuentes a la identificación del comportamiento anormal.

El operador sugiere a la CRC la modificación del articulado, de forma que se presente la obligación de un reporte inicial básico en el que se dé cuenta de la presencia de un incidente de seguridad en investigación, y más adelante se pueda remitir el resto de la información incluyendo lo solicitado respecto a la fecha del incidente, servicio afectado, etc.

CRC Respecto a la observación presentada por el operador, esta Comisión agradece las sugerencias presentadas y se aclara que las mismas han sido acogidas parcialmente en la redacción de este Artículo (ver respuesta 4.3.1).

4.3.5 COMCEL

Manifiesta que el Modelo Nacional de Gestión de Seguridad Digital, publicado por MinTIC, señala que los incidentes de seguridad no deben ser reportados o comunicados a autoridad alguna de forma obligatoria. COMCEL considera que ese documento reconoce el trabajo hasta ahora realizado por las empresas en materia de seguridad digital y valora el carácter voluntario de los reportes de información.

CRC Frente al comentario de COMCEL se aclara que el Modelo Nacional de Gestión de Riesgos de Seguridad Digital publicado por MinTIC en diciembre de 2017, es un modelo de Gestión de Riesgos, no de gestión o de reporte de incidentes. El carácter voluntario del reporte de **riesgos** no riñe de manera alguna con la propuesta presentada por la CRC para el reporte de incidentes, tal cual como los funcionarios de MinTIC tuvieron oportunidad de aclarar en la mesa de trabajo del 8 de febrero de 2018.

4.3.6 NAP Colombia

Los miembros del NAP Colombia consideran que la propuesta presentada no debe ser la forma de interactuar con el colCERT, solicitan que este organismo establezca un mecanismo de contacto abierto y estándar para la notificación de los incidentes. Manifiestan que los mecanismos dispuestos por colCERT no son permitidos en la mayoría de los ISPs para el manejo de correo, como sería el caso de PGP/GPG. NAP Colombia sugiere que colCERT debería brindar los mecanismos para que el reporte sea fácil y rápido a los ISPs ya que de lo contrario se convertirá en una tarea que demora la prioridad del manejo del incidente. Señalan que los campos que se especifican en la página del ColCERT no son los mismos que están en la resolución.

NAP Colombia considera necesaria una nueva mesa de trabajo para acordar cuáles son los objetivos del colCERT frente al reporte de incidentes, de manera que los ISPs vean cuál es el beneficio que se está buscando con el reporte de incidentes. Finalmente, considera que el ColCERT debe garantizar la confidencialidad y los datos de los ISPs.

CRC Esta Comisión concuerda con la observación presentada por NAP Colombia, por esta razón se han realizado las recomendaciones específicas al colCERT, de forma que esta entidad desarrolle una plataforma de reporte de información de incidentes de seguridad digital, abierta, segura y que ofrezca las garantías de confidencialidad requeridas por los PRST y demás actores del entorno digital. En esta línea se ha modificado el momento de reporte de los incidentes (ver respuesta 4.3.1), para que dicho reporte no afecte la prioridad del tratamiento que debe darse a los incidentes al interior de las organizaciones. Se recuerda además que la entrega de información adicional a la entidad en mención, en el proyecto de resolución es de carácter voluntaria por parte de los PRST.

Finalmente, frente a la observación sobre la necesidad de adelantar nuevas mesas de trabajo, dichas mesas se desarrollaron durante febrero de 2018.

4.3.7 Jeimy Cano

El académico manifiesta la necesidad de que cada incidente deba ser reportado al colCERT, indica además que cada organización debería generar un registro de lecciones aprendidas, que será de obligatoria consulta interna cada vez que se presente una iniciativa de seguridad o de sistemas de información que apalanque un tema particular de negocio o de telecomunicaciones.

CRC La CRC está de acuerdo con la observación presentada. Sin embargo, aun cuando se reconoce el valor agregado del registro de lecciones aprendidas, este componente de la política de gestión de incidentes de seguridad de la información se ha mantenido de carácter voluntario, al tratarse de aspectos que deben definirse de acuerdo con las necesidades propias de cada organización.

4.4 Seguimiento a gestión de incidentes

4.4.1 COLOMBIA TELECOMUNICACIONES

Respecto a este artículo, COLOMBIA TELECOMUNICACIONES manifiesta entender que esta Comisión requiere un reporte de incidentes que se hayan presentado a lo largo del año 2018, según lo informado en la reunión llevada a cabo el 18 de noviembre de 2017 en la CRC con algunos PRST, donde se discutió

la falencia importante de datos, estadísticas e información que permita tomar decisiones frente a la pertinencia de nuevas medidas regulatorias en torno al tema de seguridad digital.

Por lo anterior, manifiestan estar de acuerdo que sin información suficiente no es conveniente la imposición de cargas regulatorias ni la expedición de normas con nuevas obligaciones para los regulados, por tanto y en ese mismo sentido, consideran que este reporte no requiere ser solicitado a través de una nueva regulación, sino a través de un requerimiento de información, como otros que ha realizado la CRC en el pasado.

Adicionalmente y como lo han mencionado, el Modelo Nacional de Riesgos de Seguridad Digital, expedido recientemente por el Ministerio de TIC para comentarios del sector, basa su propuesta en un modelo de múltiples partes interesadas bajo un modelo colaborativo y de "construir sobre lo construido", en donde establece reportes de incidentes de forma voluntaria para las entidades de tipo privado. Por lo que consideran que este proyecto de resolución debería estar en línea con este modelo, que será la herramienta de referencia para manejo de riesgos de la seguridad digital a nivel nacional. Así, solicitan a esta Comisión, de manera respetuosa, tomar en consideración esta propuesta.

CRC Frente a la recomendación según la cual no se requeriría de la expedición de regulación adicional para realizar el seguimiento a los incidentes, la CRC tiene la visión que al mediano y largo plazo esta información se encuentre consolidada en la entidad más idónea para tal fin, que para este caso es colCERT. Sin embargo, este reporte inicial y de solicitud no periódica, permite definir condiciones homogéneas para la información a reportar. Por tanto, esta definición previa de las condiciones permite a los operadores adaptar sus procesos y procedimientos para capturar la información solicitada. Ahora bien, si se realiza la solicitud a través de un requerimiento particular de información, es posible que algunos operadores no puedan entregar la información histórica solicitada debido a incompatibilidades con sus procesos o que la consecución de esta sea complicada e implique reprocesos.

Finalmente, frente a la alineación de esta propuesta con el Modelo de Gestión de Riegos de Seguridad Digital publicado por MINTIC, se invita al operador a consultar la respuesta 4.3.5.

4.4.2 COMCEL

Reiteran, que el tema de seguridad de la información no requiere la expedición de una regulación, argumentando que traería más cargas operativas y financieras, que verdaderos beneficios para el sector y mucho menos para los usuarios. Por lo tanto, sugieren mantener este reporte de información y a

partir de la información allí recolectada, y luego de un análisis que involucre a todos los interesados y a las autoridades que menciona el CONPES, determinar si se requiere o no regulación.

Sin perjuicio de lo anterior, manifiestan que de implementarse cualquier lineamiento como el propuesto, se requiere un plazo de un año para integrar los servicios de telefonía e Internet fija y móvil al CSOC (Cyber Security Operation Center) lo cual implica aprobación de presupuesto, selección de proveedores e implementación técnica, por lo tanto, solicitan que la implementación de esta resolución no se realice antes del 2020.

CRC Respecto a la recomendación presentada por el operador, se recuerda que en la encuesta diagnóstica adelantada por la CRC en septiembre y octubre de 2017, se identificó que más del 50% de los operadores de servicios de comunicaciones en Colombia ya adoptan o están certificadas en el estándar ISO/IEC 27001 propuesto en el proyecto de resolución, razón por la cual no resulta claro cuáles serían las altas cargas operativas y financieras a que hace referencia la observación. Ahora bien, las previsiones del Régimen de Calidad referentes a la seguridad de la información que se están modificando con este proyecto no son nuevas, y por el contrario, las mismas solo se están actualizando a las mejores prácticas y a la realidad sectorial como se expone en el documento de soporte que acompaña el proyecto de resolución.

Frente a la solicitud de plazo de implementación, se recuerda que la integración o no de cada uno de los servicios prestados por el operador al CSOC hace parte del análisis de riesgos y de la definición de política de gestión de incidentes de cada operador y no necesariamente se desprenden como obligación de este proyecto de resolución, por lo anterior no se acoge la observación.

4.4.3 LEVEL 3

Solicitan se indique expresamente en la resolución cuáles son los tipos de incidentes de seguridad que eventualmente deberían ser reportadas a colCERT, en caso de aprobarse la propuesta de resolución.

CRC La CRC ha dispuesto las definiciones específicas de Incidentes de Seguridad de la Información en el artículo 1 del proyecto de resolución basadas en el estándar ISO/IEC 270001, así se hace explícito que es con base en esta definición que debe realizarse el reporte a colCERT.

4.5 Sobre el SGSI

4.5.1 ETB

Respecto a la implementación de la necesidad de ampliar el alcance del Sistema de Gestión de Seguridad de la Información actual de los servicios de Data Center (3 salones para los activos de información tecnológico) a los servicios de Voz e Internet fijo y móvil (infraestructura tecnológica a nivel nacional). Ese alcance no lo tiene ningún operador. Se hace explicito que en el caso de ETB la inversión en tiempo es no menor a 18 meses con el recurso necesario (que bien podría considerar una contratación o recurso humano propio con dedicación total), por lo que solicitan que la resolución considere un tiempo de implementación acorde a la obligación exigida, y no de aplicación inmediata.

CRC Se aclara a ETB que, de acuerdo con las modificaciones realizadas al alcance del SGSI, la integración o no de cada uno de los servicios prestados por el operador dentro del SGSI hace parte del análisis de riesgos y de la definición de política de gestión de incidentes de cada operador, y no necesariamente se desprenden como obligación de este proyecto de resolución. Así mismo, se recuerda también que el proyecto de resolución incluye un plazo de implementación de 12 meses, por lo tanto, no se acoge la observación presentada.

4.5.2 TIGOUNE

Respecto de la implementación de sistemas de gestión de la seguridad de la información, y dado que compañías como TigoUne ya tienen desarrollado un modelo de gestión de seguridad digital conforme con las mejores prácticas e igualmente con certificaciones en ISO 27001, sugieren que la CRC no limite la gestión de las empresas que podrían ir en contra de las dinámicas propias implantadas en los procesos corporativos en materia de seguridad digital. Además, indican que el artículo propuesto no contempla un análisis costo-beneficio de las medidas, así mismo, tampoco contempla el detalle de lo que implicaría para los operadores colombianos su implementación tanto en tiempos de desarrollos como de onerosas cargas. Al respecto, no sobra recordar que la implementación de cualquier recomendación de la UIT generaría impactos en todos los elementos de red.

Sugieren modificar el artículo 5.1.2.3.1 propuesto, de forma que el articulado se exprese como recomendaciones de la CRC más no como obligaciones regulatorias, esto debido al impacto que puede implicar cambios operacionales que afectarían las dinámicas procedimentales actualmente implementadas en empresas como TigoUne. Proponen que dichas recomendaciones sean monitoreadas mediante estudios específicos tipo encuesta, como el realizado recientemente.

CRC Frente a lo manifestado por TIGOUNE, y de acuerdo con los argumentos presentados en las observaciones y las conclusiones de las mesas de trabajo adelantas en febrero de 2018, se modificó la

redacción del Artículo 5.1.2.3.1, de forma que la misma reconozca los avances y desarrollos de los operadores, en particular se propone la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con el estándar ISO/IEC 27001 y con las características y necesidades propias de las redes de cada operador. Por lo anterior, se elimina la propuesta inicial de que el SGSI sea implementado alrededor de la recomendación UIT-T X.1051, por lo que se acoge parcialmente la observación presentada.

4.5.3 VIRGIN

Señalan la necesidad de hacer exigibles las implementaciones contenidas en la propuesta regulatoria a partir del año 2020. Lo anterior teniendo en cuenta que dichas disposiciones implican una serie de desarrollos y cambios operacionales cuya puesta en marcha para este operador tardarían más de 1 año.

CRC Respecto a la observación de VIRGIN, se solicita al operador aclarar las razones específicas por las cuales la implementación de un Sistema de Gestión de Seguridad de la Información le requieren el tiempo sugerido, sin embargo atendiendo a la necesidad de eventuales ajustes para la puesta en marcha de las políticas de gestión de seguridad de la información dispuestas por los operadores, se ha modificado al entrada en vigencia de la resolución a 12 meses después de su publicación.

4.5.4 COMCEL

Señalan que el CONPES solicita a esta Comisión ajustar el marco regulatorio del sector TIC, teniendo en cuenta aspectos como la protección de usuarios o el régimen de calidad, más no le solicita a la CRC imponer la implementación de un SGSI a los operadores, máxime cuando no se han identificado las verdaderas necesidades del sector y el análisis de costo beneficio derivado de su implementación.

Indican que el alcance que se pretende dar al mismo es excesivo, mencionando un sistema de gestión de seguridad de la información, de la gestión de riesgos y de la gestión de incidentes de seguridad. Proponen, que el alcance se limite únicamente, a la gestión de incidentes de seguridad y no extenderlo a incidentes de disponibilidad como erróneamente consideran, lo propone la CRC, dado que los mismos ya se encuentran establecidos en el Régimen de Calidad, generando reportes duplicados e injustificados para el tratamiento de gestión de incidentes de seguridad.

Sugieren, realizar mesas de trabajo con el sector para evidenciar las necesidades en cuanto a seguridad digital, y una vez construidas las conclusiones proceder a proponer el ajuste al marco regulatorio, solo en el caso que sea necesario.

Manifiestan que para gestionar incidentes de seguridad, no es necesario implementar un Sistema de Gestión de Seguridad de la Información-SGSI. Sería suficiente, como lo demuestra la experiencia mundial, la implementación, ya sea de un Centro de Operaciones de Seguridad -SOC, o un computer security incident response team -CSIRT, que serían los encargados de gestionar Incidentes de Seguridad, al interior de la operación de una empresa.

Aducen que la implementación de un sistema de gestión de seguridad de la información como lo plantea el proyecto regulatorio requiere la intervención de toda la red, para que le aplique a todos los servicios. Sin embargo, no se encuentra sustentada la necesidad que este SGSI se requiera para todos los servicios y procedimientos de una compañía.

Indican que un SGSI, conllevaría la utilización de mayores recursos, y que dichos rubros que no estarían incluidos para el 2018 ni para el 2019. Aducen que la desaceleración del sector dificultaría dichas inversiones.

En este contexto, proponen que la CRC como organismo regulador encargado de promover la competencia y la inversión en el sector, según lo ordenado en los artículos 2 y 19 de la Ley 1341 de 2009, (i) garantice un marco regulatorio que promueva la competencia en igualdad de condiciones, (ii) reconozca los esfuerzos en inversión que han adelantado algunos operadores participantes en la industria TIC, y (iii) genere los estímulos necesarios para incentivar la inversión actual y futura por parte de todos los concurrentes.

CRC Se invita al operador a consultar el documento soporte que acompañó el proyecto de resolución, publicado en noviembre 2017, donde se evidenciaron las necesidades y problemáticas ligadas a la gestión de incidentes de seguridad de la información de parte de los PRST. Ahora bien, la implementación de SGSI es una mejor práctica de industria ya difundida por un alto porcentaje de operadores, en lo que respecta al alcance planteado originalmente para la implementación de estos SGSI, se aclara que el mismo ha sido modificado y la nueva propuesta se encuentra alineada con el estándar ISO/IEC 27001 y prevé que la implementación se realice de acuerdo con las características y necesidades propias de las redes de cada operador.

4.5.5 NAP Colombia

Proponen la siguiente redacción para este artículo:

"5.1.2.3.1. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
Los proveedores de redes y servicios de telecomunicaciones deben utilizar los recursos técnicos y logísticos tendientes a mantener la confidencialidad, la integridad y la disponibilidad de los servicios de telecomunicaciones y la información manejada, procesada o almacenada durante la prestación de los mismos, siguiendo la recomendación de la Unión Internacional de Telecomunicaciones UIT-T X.1051 – Código de prácticas en materia de controles de seguridad de la información basados en la norma ISO/IEC 27002:2013.

La selección de los controles de seguridad debe basarse en el resultado del proceso de identificación, análisis y evaluación de riesgos de seguridad, de acuerdo con el estándar internacional para la de Gestión de Riesgos ISO 31000:2009 y siguiendo el marco de gestión de la seguridad de la información descrito en la recomendación UIT-T X.1052, así como las categorías de controles de seguridad para organizaciones de telecomunicaciones definidos en la Recomendación UIT-T X.1051."

CRC La CRC agradece la propuesta de redacción y aclara que la misma ha sido tenida en cuenta para la modificación realizada, se recuerda también que la nueva propuesta se encuentra alineada con el estándar ISO/IEC 27001 (ver respuesta 4.5.1).

4.5.6 DIRECTV

Sugiere que esta Comisión revise los tiempos de implementación de la resolución, ya que incorporar nuevos Sistemas de Gestión de Seguridad de la Información (SGSI) toma por lo general entre 18 y 24 meses. Asimismo, proponen que respecto a los reportes de información en los incidentes de seguridad, se haga claridad en que se garantiza la confidencialidad de la información suministrada. En ese sentido, debe enfatizarse que el Grupo de Respuesta de Emergencias Cibernéticas (colCERT) será el único poseedor de dicha información estadística, y que el uso de la misma obedecerá únicamente como insumo para la formulación de políticas públicas en materia de seguridad digital para mitigar riesgos y vulnerabilidades asociadas.

CRC La CRC aclara que una vez revisado el alcance propuesto para los SGSI, y teniendo en cuenta que la propuesta se encontraría alineada con los desarrollos actuales de los operadores, estima que un plazo de 12 meses a partir de la publicación de la resolución resultaría suficiente para la implementación de la misma.

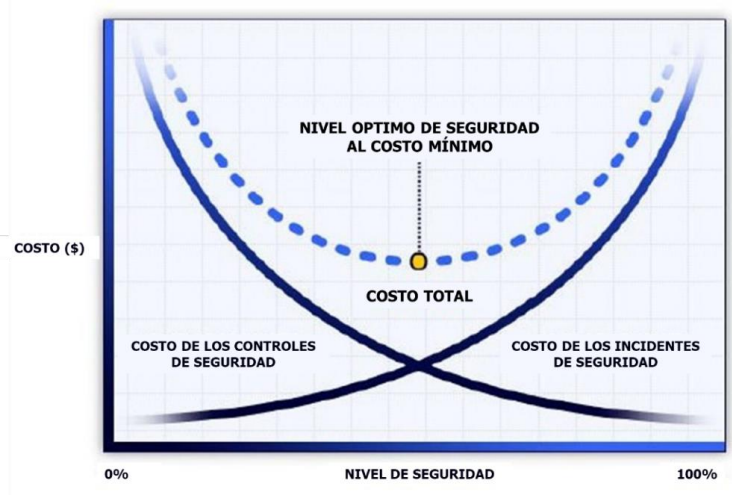
Frente a la observación sobre la información entregada al Grupo de Respuesta de Emergencias Cibernéticas (colCERT) se remite a la respuesta 4.3.2.

Anexo – Análisis costo efectividad

La Comisión de Regulación de Comunicaciones (CRC), reconoce la importancia de la adecuada asignación de recursos tanto privados como públicos en la prestación de los servicios de comunicaciones, en esta misma línea, en las diversas etapas de discusión sectorial solicitaron realizar un análisis de impacto normativo, que evaluara los potenciales costos y efectividad que tendría la propuesta para solucionar las problemáticas evidenciadas en el proceso de construcción de la misma, es en este contexto que se presenta este anexo con los resultados de dicho análisis.

Si bien el análisis cuantitativo de costos y beneficios es la forma idónea de seleccionar entre diferentes alternativas regulatorias, para el caso específico de las alternativas identificadas en el desarrollo del proyecto de resolución en mención existen algunas limitaciones para realizar este tipo de análisis:

1) Las alternativas identificadas incluyen la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI). La premisa de implementación de estos sistemas parte del supuesto que las firmas realizan un análisis de riesgos y determinan el nivel óptimo de seguridad al costo mínimo, de acuerdo con su contexto específico de operación y vulnerabilidades, razón por la cual no es posible realizar una generalización de los costos de implementación y mantenimiento de los controles de seguridad a través de variables como tamaño, base de clientes, etc.



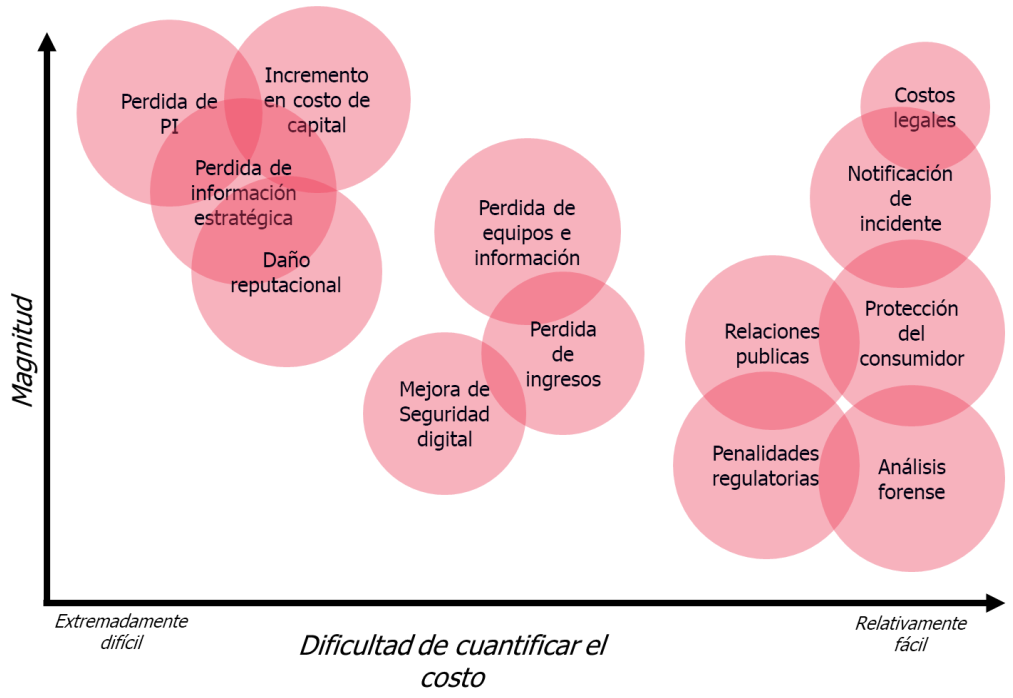
Fuente: Open Web Application Security Project - CISO AppSec Guide: Reasons for Investing in Application Security

2) No se cuenta con un conjunto de datos centralizado de incidentes de seguridad de la información, tal cual como se expone en el documento soporte, actualmente Colombia presenta una deficiencia de información estadística sobre incidentes de seguridad de la información y sus

causas, razón por la cual no se cuenta con cifras que permitan evaluar de manera general los costos de los incidentes de seguridad

3) Los incidentes de seguridad de la información no necesariamente tienen como resultado un impacto material, como por ejemplo una interrupción comercial, robo de datos o pérdida de infraestructura. Cuando una empresa es víctima de un evento cibernético adverso, puede enfrentar un rango de categorías de pérdida, algunas de las cuales son fáciles de observar y cuantificar, y otras no.

Ilustración 2 Componentes del costo de un incidente de seguridad de la información



Fuente:

(2018) The Cost of Malicious Cyber Activity to the U.S. Economy, estudio de McKinsey para el Departamento de Estado de EE. UU. -https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Teniendo en cuenta las limitaciones expuestas, y con el objetivo de evaluar los costos de cada una de las alternativas propuestas se propone una ponderación de nueve categorías de costo, tomadas de la

metodología RBM (Regulatory Burden Measure)[5]. La misma se considera relevante en la medida en que permite la desagregación de los costos asociados al cumplimiento de marcos normativos y regulatorios. La ponderación se realiza utilizando una escala de 1 a 3 (máxima evaluación positiva o negativa) de acuerdo con las potenciales actividades que resultarían necesarias para el cumplimiento de cada una de las alternativas regulatorias.

Categoría de costo	Descripción	Ejemplo
Notificación	Las empresas se enfrentan a costos de notificación cuando tienen que informar ciertos eventos a una entidad, ya sea antes o después de que el evento haya tenido lugar.	Una empresa debe notificar a una entidad los incidentes de fuga de datos personales.
Educación	Las empresas se enfrentan a costos de educación para estar al día con los requisitos regulatorios.	Una empresa necesita obtener los detalles de la nueva legislación y comunicar los nuevos requisitos al personal.
Permisos	Las empresas se enfrentan a estos costos al solicitar y mantener el permiso para realizar una actividad.	Una empresa necesita realizar una certificación de equipos antes de poder realizar una interconexión.
Compras	Las empresas se enfrentan a estos costos cuando tienen que comprar un servicio (consultorías/asesorías) o un producto (materiales o equipos) para cumplir con una regulación.	Una empresa necesita adquirir asesoría legal (servicio) o tener un sistema de firewall específico (producto).
Mantenimiento de registros	Las empresas se enfrentan a este tipo de costos para mantener actualizados los documentos legales.	Una empresa necesita mantener un registro de los incidentes de seguridad de la información que suceden en la operación.

[5]Herramienta desarrollada por el gobierno australiano para calcular el costo de las medidas regulatorias, más información en: https://rbm.obpr.gov.au/help.aspx?path=%2fUsing+the+Compliance+Cost+Calculator%2f2.About+cost+categories.txt

Vigilancia y control	Las empresas enfrentan costos de control cuando cooperan con auditorías, inspecciones y actividades de cumplimiento normativo.	Una empresa necesita supervisar a un inspector del gobierno cuando el inspector verifica si una empresa cumple con los marcos de seguridad propuestos.
Publicación y documentación	Las empresas enfrentan costos de publicación cuando tienen que presentar documentos para terceros.	Una empresa necesita publicar en su página web su política de seguridad de la información y un reporte anual de incidentes.
Procesales	Las empresas enfrentan costos no administrativos impuestos por algunas regulaciones.	Una empresa debe realizar exámenes de penetración anuales de sus sistemas.
Retrasos	Las empresas enfrentan costos cuando las demoras administrativas ocasionan gastos y pérdida de ingresos.	Una empresa necesita esperar a que se apruebe su plan de gestión de incidentes antes de poder iniciar operaciones.

Fuente: Regulatory burden measurement framework – Gobierno Australiano.

De otra parte, para evaluar la efectividad de cada una de las alternativas se propone una ponderación respecto al cumplimiento de los objetivos regulatorios.

A1 Medidas de Seguridad de Red

A1.1 Propuesta regulatoria (Medidas de Seguridad de Red)

Exposición de la necesidad regulatoria
Necesidad que motivó la propuesta regulatoria: La CRC evidenció una brecha entre el estado actual de las previsiones para la seguridad de las redes en Colombia y el modelo planteado en la Política Nacional de Seguridad Digital esbozado en el CONPES 3854 de 2016, el cual busca "*Fortalecer las capacidades de las múltiples partes interesadas para identificar,* ***gestionar, tratar y mitigar los riesgos de seguridad digital*** *en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.*", debido a que la medidas actuales están basadas en recomendaciones de la serie

UIT-T X.800 que no incorporan todos los elementos asociados a la gestión de riesgos de seguridad digital.

Objetivos de la propuesta regulatoria:

1) Fortalecer las capacidades de los PRST para identificar, gestionar, tratar y mitigar los riesgos de seguridad de la información
2) Proporcionar un marco/estructura razonablemente completa que permita la evaluación y tratamiento integral de riesgos de seguridad de la información de acuerdo con las prioridades comerciales y de seguridad de cada organización.
3) Proporcionar incentivos para actualizar y, cuando sea necesario, mejorar periódicamente la política de seguridad de la información.
4) Suministrar confianza respecto a las capacidades de administración de seguridad de la información en el sector de las telecomunicaciones a los usuarios, autoridades, inversores, propietarios y otras partes interesadas.
5) Definir formalmente los procesos y procedimientos asociados a la gestión de la seguridad de la información, permitiendo que las mismas sean discutidas, analizadas y vigiladas de manera consistente y clara.

A1.2 Descripción de las alternativas analizadas (Medidas de Seguridad de Red).

Alternativas consideradas
Alternativa 1: Propuesta publicada
El texto de la propuesta regulatoria publicada el 24 de noviembre de 2017, establece lo siguiente frente a la temática objeto de análisis: *"**ARTICULO 5.1.2.3 GESTIÓN DE SEGURIDAD EN REDES DE TELECOMUNICACIONES.** Los proveedores de redes y servicios de telecomunicaciones deben atender las siguientes criterios y procedimientos en los procesos de gestión de seguridad de sus redes:* ***5.1.2.3.1. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:** Los proveedores de redes y servicios de telecomunicaciones deben utilizar los recursos técnicos y logísticos tendientes a garantizar la confidencialidad, la integridad y la disponibilidad de los servicios de telecomunicaciones y la información manejada, procesada o almacenada durante la prestación de los mismos, implementando para ello un Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con las características y necesidades propias de su red, siguiendo la recomendación de la Unión Internacional de Telecomunicaciones UIT-T X.1051 – Código de prácticas en materia de controles de seguridad de la información basados en la norma ISO/CEI 27002 para organizaciones de telecomunicaciones.* *El SGSI implementado debe ser acorde con el marco de gestión de la seguridad de la información descrito en la recomendación UIT-T X.1052, así como las categorías de controles de seguridad*

para organizaciones de telecomunicaciones definidos en la Recomendación UIT-T X.1051, como lo son: gestión de activos (UIT-T X.1057), gestión de incidentes (UIT-T X1056), gestión de riesgos (UITT X.1055), gestión de políticas (UIT-T X.1054), gestión de organización y personal, adquisición de sistemas y capacidades, gestión de operaciones y de mantenimiento."
Alternativa 2: Propuesta basada en los comentarios allegados durante la etapa de discusión y en las mesas de trabajo adelantadas.
"ARTICULO 5.1.2.3 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN REDES DE TELECOMUNICACIONES. *Los proveedores de redes y servicios de telecomunicaciones deben atender los siguientes criterios en los procesos de gestión de seguridad de sus redes:* ***5.1.2.3.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN:*** *Los proveedores de redes y servicios de comunicaciones deben adoptar una Política de Seguridad de la Información que contemple la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), tendiente a garantizar la confidencialidad, la integridad, la disponibilidad de los servicios de comunicaciones y la información manejada, procesada o almacenada durante la prestación de los mismos, siguiendo para ello la familia de estándares ISO/IEC 27000.* *En la implementación de dicho SGSI, los proveedores de redes y servicios de comunicaciones podrán, de manera autónoma, determinar el alcance y las condiciones de funcionamiento del SGSI, teniendo en cuenta las características propias de su red, su contexto de operación y sus riesgos.* *La política adoptada deberá ser compatible con la identificación, almacenamiento y reporte de información de incidentes de seguridad de la información de que tratan los Numerales 5.1.2.3.2. y 5.1.2.3.3. del presente artículo."*
Alternativa 3: Regulación vigente - Artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución Compilatoria CRC 5050 de 2016.
*"**ARTÍCULO 5.1.2.3. SEGURIDAD DE LA RED.** Los proveedores de redes y servicios de telecomunicaciones que ofrezcan acceso a Internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo. Para tal efecto, deberán informar en su página Web sobre las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtros antivirus y la prevención de spam, phishing, malware entre otras. La responsabilidad a cargo de los proveedores de redes y servicios de telecomunicaciones que ofrezcan acceso a Internet no cubre los equipos del cliente, dado que los mismos son controlados directamente por el usuario del servicio. Los proveedores de contenidos o de cualquier tipo de aplicación deberán tomar las respectivas medidas de seguridad de conformidad con lo que para el efecto disponga la normatividad que les sea aplicable.*

Además de las medidas de seguridad antes descritas, los proveedores de redes y servicios de telecomunicaciones que ofrezcan acceso a Internet deberán implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT en lo relativo a las recomendaciones pertenecientes a las series X.800 dictadas por este organismo, al menos en relación con los siguientes aspectos, y en lo que aplique para cada entidad que interviene en la comunicación:

1) Autenticación: Verificación de identidad tanto de usuarios, dispositivos, servicios y aplicaciones. La información utilizada para la identificación, la autenticación y la autorización debe estar protegida (Recomendaciones UIT X.805 y UIT X.811).

2) Acceso: Prevenir la utilización no autorizada de un recurso. El control de acceso debe garantizar que sólo los usuarios o los dispositivos autorizados puedan acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones (Recomendaciones UIT X.805 y UIT X.812).

3) Servicio de No repudio: Es aquél que tiene como objeto recolectar, mantener, poner a disposición y validar evidencia irrefutable sobre la identidad de los remitentes y destinatarios de transferencias de datos. (Recomendaciones UIT X.805 y X.813).

4) Principio de Confidencialidad de datos: Proteger y garantizar que la información no se divulgará ni se pondrá a disposición de individuos, entidades o procesos no autorizados (Recomendaciones UIT X.805 y X.814).

5) Principio de Integridad de datos: Garantizar la exactitud y la veracidad de los datos, protegiendo los datos contra acciones no autorizadas de modificación, supresión, creación o reactuación, y señalar o informar estas acciones no autorizadas (Recomendaciones X.805 y X.815).

6) Principio de Disponibilidad: Garantizar que las circunstancias de la red no impidan el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones (Recomendación X.805).

Los proveedores de redes y servicios de telecomunicaciones a través de redes móviles, además de las soluciones de seguridad antes descritas, deberán implementar modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación, utilizando modelos de cifrados, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122."

A1.3 Análisis de efectividad (Medidas de Seguridad de Red).

Para determinar la efectividad de las alternativas propuestas, se analizó el cumplimiento de cada una respecto de los objetivos dispuestos en el proyecto regulatorio, los cuales se describen en el numeral 0 del presente Anexo.

Respecto a la valoración de las alternativas, se asigna un puntaje máximo de 3 si la alternativa cumple con el objetivo en mayor o menor medida y se asigna el mismo peso a cada objetivo (20%), de forma que la propuesta más efectiva será aquella que se aproxima al máximo puntaje, es decir 3.

	Objetivo 1	Objetivo 2	Objetivo 3	Objetivo 4	Objetivo 5	Resultado (Max 3)
Alternativa 1	✓✓ Se identifica que esta alternativa permite a los PRST fortalecer sus capacidades en la mayor parte de las áreas de gestión de seguridad de la información.	✓✓✓ Se identifica que esta alternativa proporciona un marco integral para el tratamiento de los riesgos de acuerdo con las prioridades comerciales y de seguridad.	✓✓✓ Se identifica que esta alternativa incluye procesos y actividades encaminadas a mantener una política de seguridad de la información actualizada.	✓ Si bien la alternativa identificada es una recomendación internacional sectorial que puede dar confianza a las múltiples partes interesadas, existen marcos con mayor reconocimiento.	✓ Los procesos y procedimientos del marco se encuentran definidos, sin embargo, los procesos de auditoria y vigilancia no han sido desarrollados al mismo nivel de otros estándares.	**2**
Alternativa 2	✓✓✓ Se identifica que esta alternativa permite a los PRST fortalecer sus capacidades en todas las áreas de gestión de seguridad de la información.	✓✓✓ Se identifica que esta alternativa proporciona un marco integral para el tratamiento de los riesgos de acuerdo con las prioridades comerciales y de seguridad.	✓✓✓ Se identifica que esta alternativa incluye procesos y actividades encaminadas a mantener una política de seguridad de la información actualizada.	✓✓ La alternativa propone la adopción de la mejor práctica con mayor reconocimiento en la industria para la gestión de incidentes de seguridad de la información, razón por la cual se considera que la misma brinda confianza a las múltiples partes interesadas, no se asigna el	✓✓✓ Los procesos y procedimientos del marco se encuentran definidos, así como eventuales procedimientos de vigilancia y auditoría.	**2.8**

				máximo puntaje debido a que la certificación se propone como voluntaria.		
Alternativa 3 (statu quo)	- Se identifica que esta alternativa no permite a los PRST fortalecer sus capacidades de gestión de seguridad de la información, el marco solo define principios generales sin introducir el concepto de gestión de riesgos de seguridad de la información.	- Se identifica que esta alternativa no proporciona un marco integral para el tratamiento de los riesgos ni tampoco tiene en cuenta las prioridades comerciales sino únicamente las prioridades de seguridad.	✓ Se identifica que esta alternativa incluye la necesidad de mantener las "amenazas" y "vulnerabilidades" bajo control y menciona las necesidades de actualización en este sentido, sin profundizar en procesos específicos de actualización.	✓ Si bien la alternativa identificada es una recomendación internacional sectorial que puede dar confianza a las múltiples partes interesadas, existen marcos con mayor reconocimiento.	✓ El marco define los principios generales y los conceptos asociados a la gestión de la seguridad de la información, sin embargo, los procesos de auditoría y vigilancia no han sido desarrollados.	**0.6**

A1.4 Análisis de costos (Medidas de Seguridad de Red).

Respecto a la valoración de las características de costo de las diferentes alternativas, se asigna un puntaje de 1 a 3 dependiendo del nivel de impacto en las diferentes categorías de costos para las múltiples partes interesadas, cada valoración es ponderada con un peso proporcional (11,11%), por lo que la propuesta considerada de menor impacto en los costos será aquella que se aproxima al mínimo puntaje, es decir 0.

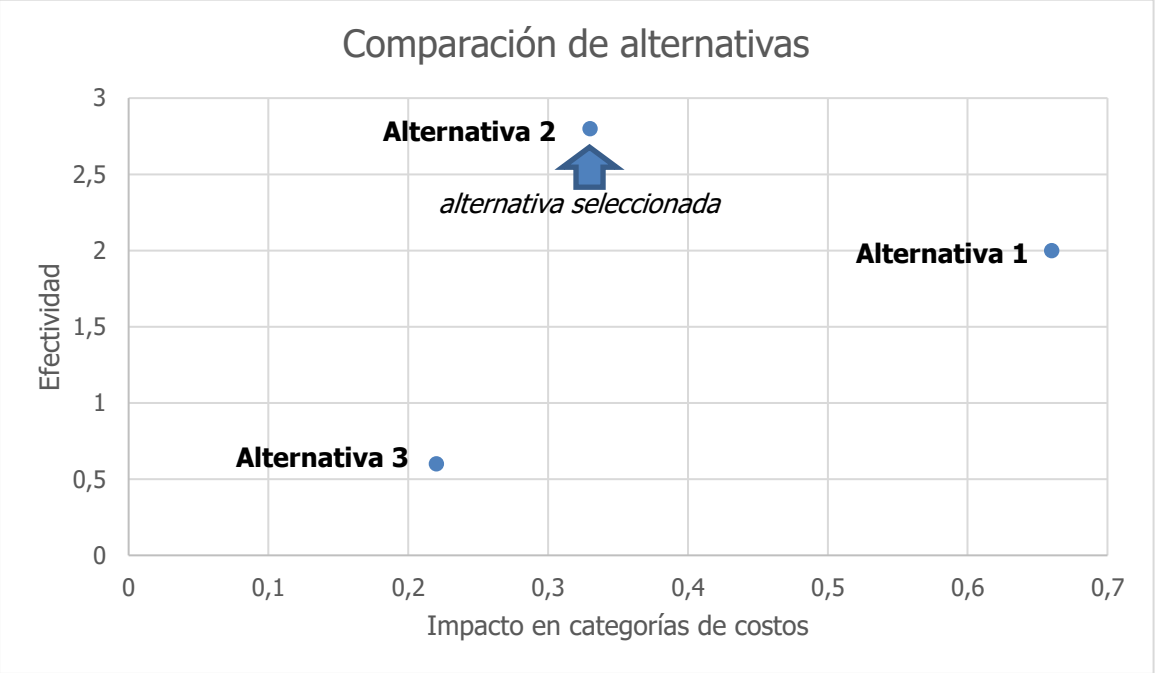
Categoría de costo	Alternativa 1	Alternativa 2	Alternativa 3 (Statu quo)
Notificación	- No se evidencian actividades de notificación asociadas a la alternativa 1.	- No se evidencian actividades de notificación asociadas a la alternativa 2.	- El marco normativo vigente al que hace referencia la alternativa 3 no requiere de actividades de notificación
Educación	✗✗ Tratándose de un marco de seguridad que no ha sido adoptado por ninguno de los	✗ El 52% de los PRST que operan en Colombia ya implementan el estándar ISO/IEC 27001[2],	✗ El marco normativo vigente al que hace referencia la alternativa 3 establece los

	PRST en Colombia, la alternativa 1 requeriría de actividades de educación y difusión al interior de las organizaciones, estas actividades podrían enmarcarse en las actividades del sistema de gestión de seguridad de la información para aquellas organizaciones que ya implementan este tipo de sistemas[6]	asimismo la prevalencia de este estándar entre los PRST que representan el 90% del mercado de Internet fijo es del 100% (si bien el estado de implementación varía tanto a nivel de certificación como de áreas o procesos de la organización cubiertos), por lo cual la alternativa 2 requeriría de menores actividades de educación respecto a la alternativa 2.	principios y dominios de seguridad de la información, sin embargo, las actividades de educación/difusión resultarían análogas a las de la alternativa 2 e inclusive potencialmente más costosas en cuanto no se contaría con la misma disponibilidad de recursos pedagógicos que ya han sido desarrollados para el marco propuesto en la alternativa 2.
Permisos	- No se evidencian actividades de permisos asociadas a la alternativa 1.	- No se evidencian actividades de permisos asociadas a la alternativa 2.	- No se evidencian actividades de permisos asociadas al marco actual.
Compras	✗✗ La implementación de la alternativa 1 podría requerir la adquisición de asesorías y equipos de acuerdo con los niveles de riesgos y prioridades de negocio y seguridad de cada firma, adicionalmente estos costos pueden ser mayores a los asociados a la alternativa 2, puesto que aun aquellas empresas que ya han implementado el estándar ISO 27001 podrían requerir realizar ajustes a los procesos implementados.	✗ La implementación de la alternativa 2 requeriría la adquisición de asesorías o equipos únicamente en el 48% de los operadores[2], adicionalmente el estándar propuesto modula los controles asociados a las prioridades de negocio y los riesgos de seguridad con el objetivo de reducir los costos de implementación.	- La implementación de los principios y dominios de seguridad a los que hace referencia la alternativa 3, se consideran ya realizados y por lo tanto constituyen la línea base comparativa para la comparación respecto a las otras alternativas propuestas.
Mantenimiento de registros	- No se evidencian actividades de mantenimiento de registros asociadas a la alternativa 1.	- No se evidencian actividades de mantenimiento de registros asociadas a la alternativa 2.	- No se evidencian actividades de mantenimiento de registros asociadas al marco actual.
Vigilancia y control	✗✗ La alternativa 1 propone un modelo basado en modificaciones a la alternativa 2, no cuenta con un estándar para cuerpos de acreditación u otras organizaciones externas, si	✗ La alternativa 2 propone el modelo de mayor difusión en la materia, dicho modelo tiene una larga trayectoria de desarrollo y metodología de vigilancia y auditoría e incluso tiene un estándar para cuerpos	✗ La información recopilada sobre las actividades de Vigilancia y control a los requisitos de la alternativa 3 (Información solicitada a Dirección de Vigilancia y Control – MINTIC) evidencian

[6] De acuerdo con la encuesta diagnóstica sobre gestión de riesgos de seguridad digital adelantada por la CRC como parte del desarrollo de la propuesta regulatoria en cuestión, se evidenció que el 52% de los PRST implementan el estándar ISO/IEC 27001 para la gestión de seguridad de la información.

	bien la implementación produce salidas y productos que facilitan la verificación (política de gestión de riesgos, política de gestión de incidentes, procedimientos, etc.) las autoridades de vigilancia y control deberán desarrollar herramientas de auditoría lo que puede incrementar los costos de vigilancia y control entre los diferentes agentes involucrados.	de acreditación u otras organizaciones externas (ISO 27007), las actividades de vigilancia y control pueden apalancarse de estos desarrollos y reducir los costos de vigilancia y control, de otra parte la implementación del estándar produce salidas y productos que facilitan la verificación (política de gestión de riesgos, política de gestión de incidentes, procedimientos, etc.)	que estos aspectos no generan costos adicionales de cumplimiento, en cuanto no hacen parte de los requerimientos evaluados por el área funcional SERTIC.
Publicación y documentación	-	-	-
	No se evidencian actividades de publicación de registros asociadas a la alternativa 1.	No se evidencian actividades de publicación asociadas a la alternativa 2.	No se evidencian actividades de publicación asociadas al marco normativo vigente (alternativa 3).
Procesales	-	-	-
	No se evidencian actividades de tipo procesal asociadas a la alternativa 1.	No se evidencian actividades de tipo procesal asociadas a la alternativa 2.	No se evidencian actividades de tipo procesal asociadas al marco normativo vigente (alternativa 3).
Retrasos	-	-	-
	No se evidencian costos por retrasos asociados a la alternativa 1.	No se evidencian costos por retrasos asociados a la alternativa 2.	No se evidencian costos por retrasos asociados al marco normativo vigente (alternativa 3).
Resultado	**0.66**	**0.33**	**0.22**

A1.5 Análisis comparativo de los costos y efectividad de las alternativas (Medidas de Seguridad de Red)



Fuente: Elaboración propia

De acuerdo con los análisis expuestos en esta sección, se evidencia que la alternativa que permite abordar de forma más efectiva las problemáticas evidenciadas en el curso del presente proyecto regulatorio respecto a las medidas de seguridad de red es la Alternativa 2, la cual corresponde a las medidas adoptadas en el proyecto de resolución artículo 2.

A2 Previsiones frente a los incidentes de seguridad

A2.1 Propuesta regulatoria (Incidentes de seguridad)

Exposición de la necesidad regulatoria
Necesidad que motivó la propuesta regulatoria:

Teniendo en cuenta la falta de información estadística sobre incidentes de seguridad de la información con impacto significativo en los servicios de comunicaciones, así como la ausencia de datos sobre las causas de los mismos, se considera importante proporcionar a las entidades encargadas de la seguridad digital en el país, a los responsables de formular políticas públicas en materia de seguridad digital, al público y a la industria en general, los insumos necesarios para generar un reporte estadísticamente relevante de los incidentes, que pueda evidenciar la frecuencia y el impacto de los mismos en el sector de las comunicaciones en Colombia.

Objetivos de la propuesta regulatoria:

1) Proporcionar a las múltiples partes interesadas información sobre la frecuencia y el impacto de los incidentes de seguridad de la información en el sector de las telecomunicaciones.

2) Contar con información estadística que aporte al desarrollo de políticas públicas y regulatorias de seguridad digital, y que contribuya a mejorar los planes generales de gestión de incidentes de seguridad de la información de los PRST.

3) Visibilizar las principales categorías de incidentes de seguridad de la información en el sector de las telecomunicaciones para apoyar los planes generales de gestión de incidentes y el desarrollo de políticas.

A2.2 Descripción de las alternativas analizadas (Incidentes de seguridad).

Alternativas consideradas
Alternativa 1: Propuesta publicada
El texto de la propuesta regulatoria publicada el 24 de noviembre de 2017, establece lo siguiente frente a la temática objeto de análisis: *"**5.1.2.3.2. INCIDENTES DE SEGURIDAD.** Los proveedores de servicios de internet y telefonía deberán identificar, almacenar y tener a disposición de las autoridades pertinentes la información sobre los incidentes de seguridad o de pérdida de integridad del servicio que hayan afectado de manera significativa su base de usuarios. Se entenderá por afectación significativa aquella que cumple con los umbrales cuantitativos definidos así:*

Duración del incidente (horas) / Usuarios afectados	*1h-2h*	*2h-4h*	*4h-6h*	*6h-8h*	*>8h*
1%-2%	*NO*	*NO*	*NO*	*NO*	*SI*

2%-5%	*NO*	*NO*	*NO*	*SI*	*SI*
5%-10%	*NO*	*NO*	*SI*	*SI*	*SI*
10%-15%	*NO*	*SI*	*SI*	*SI*	*SI*
>15%	*SI*	*SI*	*SI*	*SI*	*SI*

Nota: El porcentaje de usuarios afectados, se calculará sobre la base de usuarios del servicio específico de comunicaciones de acuerdo con el último trimestre reportado.

La información sobre el incidente de seguridad o pérdida de integridad debe incluir:

Fecha del Incidente	*Servicio afectado*	*Número de usuarios afectados*	*Duración*	*Causa del incidente*

1. ***Fecha del incidente:*** *En este campo deberá indicarse la fecha de inicio del incidente.*
2. ***Servicio afectado:*** *En este campo deberá indicarse el o los servicios afectados por el incidente de indisponibilidad:*
   a. *Internet Fijo.*
   b. *Internet Móvil.*
   c. *Telefonía fija.*
   d. *Telefonía Móvil.*

3. ***Número de usuarios afectados:*** *En este campo, para telefonía fija e internet fijo, debe indicarse el número de suscriptores afectados.*

   Para Internet y telefonía móvil, deberá indicarse el número potencial de usuarios afectados de acuerdo con el uso normal de la infraestructura afectada.

4. ***Duración:*** *En este campo debe indicarse el tiempo en horas de indisponibilidad del servicio.*

5. ***Causa del incidente:*** *En este campo debe indicarse la causa raíz del incidente de indisponibilidad del servicio, el operador deber indicar una de las siguientes categorías de causas raíz:*

   a. ***Error humano****: Esta categoría debe utilizarse cuando el incidente sea causado por un error humano durante la ejecución de actividades y procedimientos de operación de la infraestructura o aplicaciones del proveedor.*

   b. ***Error de sistema:*** *Esta categoría debe utilizarse cuando el incidente sea causado por fallos de sistema, bien sea de hardware o de software.*

c. ***Fenómenos Naturales:*** *Esta categoría debe utilizarse cuando el incidente se produce por daños causados por fenómenos naturales como incendios, terremotos, inundaciones, etc.*

d. ***Actores maliciosos:*** *Esta categoría debe utilizarse cuando los incidentes son causados por la acción deliberada de un actor u organización.*

e. ***Fallas externas al operador:*** *Esta categoría debe utilizarse cuando la causa raíz del incidente se presenta por causas fuera del control del operador, como por ejemplo incidentes causados por actores externos durante el mantenimiento de una vía, cortes prolongados de energía causados por el proveedor de energía eléctrica, etc.*

Alternativa 2: Propuesta basada en los comentarios allegados durante la etapa de discusión y en las mesas de trabajo adelantadas.

5.1.2.3.2. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. *Los proveedores de servicios de telecomunicaciones deberán identificar, almacenar hasta por un año y tener a disposición de las autoridades pertinentes la información sobre los incidentes de seguridad de la información.*

La información sobre el Incidente de Seguridad de la Información debe incluir:

Fecha del Incidente	*Servicio afectado*	*Número de usuarios afectados*	*Duración*	*Categoría del incidente*	*Nivel de severidad del incidente*

1. ***Fecha del incidente:*** *En este campo deberá indicarse la fecha de inicio del incidente.*
2. ***Servicio afectado:*** *En este campo deberá indicarse el o los servicios afectados por el incidente de indisponibilidad:*
   a. *Internet Fijo.*
   b. *Internet Móvil.*
   c. *Telefonía fija.*
   d. *Telefonía Móvil.*
3. ***Número de usuarios afectados:*** *En este campo, para telefonía fija e Internet fijo, debe indicarse el número de suscriptores afectados.*

   Para Internet y telefonía móvil, deberá indicarse el número potencial de usuarios afectados de acuerdo con el uso normal de la infraestructura afectada.

4. ***Duración:*** *En este campo debe indicarse el tiempo en horas de duración del incidente de seguridad de la información.*

5. ***Categoría del incidente:*** *En este campo debe indicarse la categoría del incidente de seguridad de la información, el operador deber indicar una de las siguientes categorías de causas raíz:*

    a. *Denegación de servicio: Denegación de servicio (DoS) y Denegación de servicio distribuida (DDoS) son una categoría amplia de incidentes con características en común. Estos incidentes causan que un sistema, servicio o red no opere a su capacidad prevista, usualmente causando la denegación completa del acceso a los usuarios legítimos.*

    b. *Acceso no autorizado: esta categoría de incidentes consiste en intentos no autorizados para acceder o hacer un mal uso de un sistema, servicio o red.*

    c. *Malware: Esta categoría identifica un programa o parte de un programa insertado en otro con la intención de modificar su comportamiento original, generalmente para realizar actividades maliciosas como robo de información, robo de identidad, destrucción de información y recursos, denegación de servicio, correo no deseado, etc.*

    d. *Abuso: Esta categoría de incidentes identifica la violación de las políticas de seguridad del sistema de información de una organización. No son ataques en el sentido estricto de la palabra, pero a menudo se informan como incidentes y requieren ser gestionados.*

    e. *Recopilación de información de sistema: Esta categoría de incidentes incluye las actividades asociadas con la identificación de objetivos potenciales y el análisis de los servicios que se ejecutan en esos objetivos (ej. probing, ping, scanning)*

6. ***Nivel de severidad de incidente:*** *En este campo, debe indicarse el nivel de severidad del incidente de seguridad de la información, teniendo en cuenta la importancia del sistema de información involucrado, las potenciales pérdidas de negocio y el posible impacto social, según lo dispuesto en el Anexo 5.8 de la presente Resolución:*

    a. *Muy Serio (Clase IV)*

b. Serio (Clase III) *c. Menos serio (Clase II)* *d. Pequeño (Clase I)*
Alternativa 3: Regulación vigente – en el Título V de la Resolución Compilatoria CRC 5050 de 2016.
El marco regulatorio vigente no tiene previsiones vigentes en materia de registro de incidentes de seguridad de la información.

A2.3 Análisis de efectividad (Incidentes de seguridad)

Para determinar la efectividad de las alternativas propuestas, se analizó el cumplimiento de cada una respecto de los objetivos dispuestos en el proyecto regulatorio, los cuales se describen en el numeral 0 del presente Anexo.

Respecto a la valoración de las alternativas, se asigna un puntaje máximo de 3 si la alternativa cumple con el objetivo en mayor o menor medida y se asigna el mismo peso a cada objetivo (20%), de forma que la propuesta más efectiva será aquella que se aproxima al máximo puntaje, es decir 3.

	Objetivo 1	**Objetivo 2**	**Objetivo 3**	**Resultado (Max 3)**
Alternativa 1	✓✓ La Alternativa 1 proporciona a las múltiples partes interesadas la información de frecuencia e impacto de los incidentes de seguridad de la información que afectaron de manera Significativa a la base de usuarios, sin embargo, los umbrales propuestos pueden limitar el alcance de la información de impacto (no se visibilizan los incidentes de "bajo impacto").	✓✓✓ La Alternativa 1 permite el análisis estadístico de la información de incidentes de seguridad de la información, sin embargo, al involucrar el concepto de integridad del servicio, esta información puede incluir incidentes que escapan la seguridad de la información.	✓✓ Si bien la propuesta de la Alternativa 1 categoriza los incidentes de seguridad de la información, las categorías propuestas podrían incluir elementos que escapan el SGSI y que se encontrarían categorizados en otras previsiones del régimen de calidad (ya categorizadas en las previsiones para *Afectación del servicio de comunicaciones*).	**2.33**

Alternativa 2	✓✓✓ La Alternativa 2 proporciona a las múltiples partes interesadas la información de frecuencia e impacto de los incidentes de seguridad de la información, la alternativa 2 adicionalmente está basada en la definición de eventos e incidentes de seguridad de la información del estándar ISO 27001, lo que permite que los incidentes se encuentren acotados y claramente definidos.	✓✓✓ La Alternativa 2 permite el análisis estadístico de la información de incidentes de seguridad de la información, al incorporar definiciones acotadas, la información estadística es pertinente al desarrollo de políticas de gestión de incidentes de seguridad de la información.	✓✓✓ La Alternativa 2 categoriza los incidentes de seguridad de la información, en línea con la familia de estándares ISO 27000 (específicamente las categorías propuestas en el estándar ISO 27035-1), las categorías se encuentran acotadas a la gestión de seguridad de la información.	**3**
Alternativa 3 (statu quo)	- El marco regulatorio actual no proporciona información sobre la frecuencia o el impacto de los incidentes de seguridad de la información a las múltiples partes interesadas.	- El marco regulatorio actual no permite análisis estadístico de la información de incidentes de seguridad de la información.	- El marco regulatorio vigente no permite la categorización de la información de incidentes de seguridad de la información.	**0.0**

A2.4 Análisis de costos (Incidentes de seguridad)

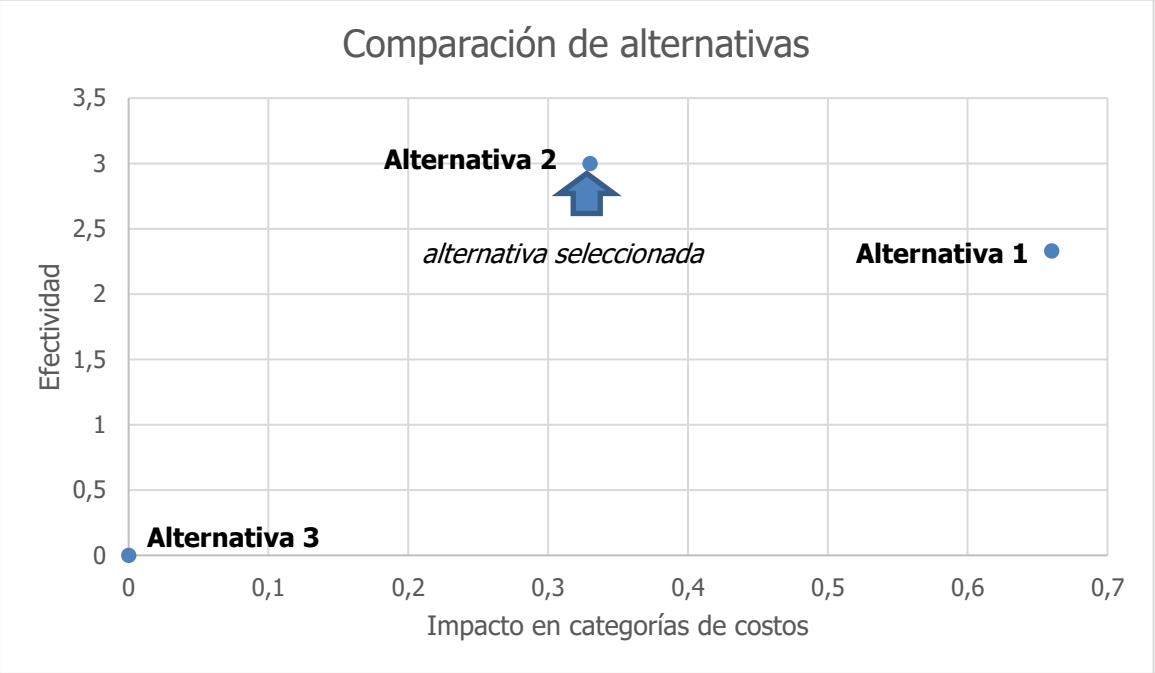
Respecto a la valoración de las características de costo de las diferentes alternativas, se asigna un puntaje de 1 a 3 dependiendo del nivel de impacto en las diferentes categorías de costos para las múltiples partes interesadas, cada valoración es ponderada con un peso proporcional (11,11%), por lo que la propuesta considerada de menor impacto en los costos será aquella que se aproxima al mínimo puntaje, es decir 0.

Categoría de costo	Alternativa 1	Alternativa 2	Alternativa 3 (Statu quo)
Notificación	-	-	-

	El artículo propuesto en la Alternativa 1 incorpora el almacenamiento de la información más no su notificación, la cual se da en un esquema de solicitud particular, por lo tanto, no se consideran impactos de Notificación.	El artículo propuesto en la Alternativa 2 incorpora el almacenamiento de la información más no su notificación, la cual se da en un esquema de solicitud particular, por lo tanto, no se consideran impactos de Notificación.	El marco normativo vigente al que hace referencia la alternativa 3 no requiere de actividades de notificación
Educación	✗✗	✗	-
	Como parte de la implementación del almacenamiento de información de incidentes de seguridad de la información de la Alternativa 1, puede ser necesario el desarrollo de políticas de gestión de incidentes y su difusión al interior de las organizaciones, adicionalmente la categorización propuesta en la Alternativa 1 podría requerir un alcance de difusión mayor al incorporar elementos de "Integridad del servicio" no necesariamente asociados a la gestión de seguridad de la información.	La alternativa 2 propone el almacenamiento de información de incidentes de seguridad de la Información conforme a los criterios de clasificación del estándar ISO 27035-1 por lo que el alcance de las actividades de difusión se encuentran acotadas a la gestión de incidentes de seguridad de la información y el acervo de información disponible permite reducir los costos de educación respecto a la Alternativa 1.	El marco normativo vigente al que hace referencia la alternativa 3 no requiere de actividades de Educación.
Permisos	-	-	-
	No se evidencian actividades de permisos asociadas a la alternativa 1.	No se evidencian actividades de permisos asociadas a la alternativa 2.	No se evidencian actividades de permisos asociadas al marco actual.
Compras	✗✗	✗	-
	La implementación de la alternativa 1 podría requerir la modificación a los sistemas de gestión de incidentes implementados, el alcance de estas actividades se estima mayor a los asociados a la alternativa 2, puesto que involucra incidentes que pueden exceder el alcance cubierto por el eventual SGSI si el mismo ya se encontrara implementado.	La implementación de la alternativa 2 se encuentra acotada a los incidentes de gestión de seguridad de la información, en este sentido las adquisiciones necesarias para el cumplimiento de la alternativa propuesta se estiman menores a las de la Alternativa 1.	El marco normativo vigente al que hace referencia la alternativa 3 no incluye necesidades de compras puesto que no prevé ningún tipo de información de incidentes de seguridad de la información.
Mantenimiento de registros	✗✗	✗	-
	La alternativa 1 no limita el tiempo de almacenamiento y su alcance incluye diversas	La alternativa 2 limita el tiempo de almacenamiento de registros a 12 meses y acota las	No se evidencian actividades de mantenimiento de

	categorías asociadas a la "Integridad del servicio" por lo que las actividades asociadas al mantenimiento de registros podrían tener un impacto moderado en esta categoría de costo.	categorías del estándar ISO 27035-1, por lo cual se estima que las actividades asociadas al mantenimiento de registros podrían ser menores respecto a la alternativa 1.	registros asociadas al marco actual.
Vigilancia y control	-	-	-
	No se evidencian actividades de vigilancia y control asociadas a la alternativa 1.	No se evidencian actividades de vigilancia y control asociadas a la alternativa 2.	No se evidencian actividades de vigilancia y control asociadas al marco normativo vigente (alternativa 3).
Publicación y documentación	-	-	-
	No se evidencian actividades de publicación de registros asociadas a la alternativa 1.	No se evidencian actividades de publicación asociadas a la alternativa 2.	No se evidencian actividades de publicación asociadas al marco normativo vigente (alternativa 3).
Procesales	-	-	-
	No se evidencian actividades de tipo procesal asociadas a la alternativa 1.	No se evidencian actividades de tipo procesal asociadas a la alternativa 2.	No se evidencian actividades de tipo procesal asociadas al marco normativo vigente (alternativa 3).
Retrasos	-	-	-
	No se evidencian costos por retrasos asociados a la alternativa 1.	No se evidencian costos por retrasos asociados a la alternativa 2.	No se evidencian costos por retrasos asociados al marco normativo vigente (alternativa 3).
Resultado	**0.66**	**0.33**	**0.0**

A2.5 Análisis comparativo de los costos y efectividad de las alternativas (Incidentes de seguridad)



Fuente: Elaboración propia

De acuerdo con los análisis expuestos en esta sección, se evidencia que la alternativa que permite abordar de forma más efectiva las problemáticas evidenciadas en el curso del presente proyecto regulatorio respecto a la información de Incidentes de Seguridad de la Información es la Alternativa 2, la cual corresponde a las medidas adoptadas en el proyecto de resolución artículo 2.

A3 Previsiones de reporte a autoridades

A3.1 Propuesta regulatoria (Previsiones de reporte a autoridades)

Exposición de la necesidad regulatoria
Necesidad que motivó la propuesta regulatoria:

Tanto el documento soporte desarrollado por la CRC como el CONPES 3854, identificaron la necesidad de fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, en particular la estrategia E4.4 del citado CONPES establece que "*La adecuación del marco jurídico deberá buscar, además, el reporte obligatorio de incidentes cibernéticos al colCERT por parte de los propietarios u operadores de infraestructuras críticas cibernéticas nacionales y demás partes interesadas, con las previsiones respectivas de confidencialidad, privacidad*"

Por su parte, la encuesta diagnóstica realizada por la CRC en el desarrollo de este proyecto regulatorio revela que solo el 23% de los PRSTs en Colombia, coordinan sus acciones de gestión de incidentes de seguridad de la información con el colCERT.

Objetivos de la propuesta regulatoria:

1) Generar mecanismos para impulsar la cooperación en materia de seguridad digital entre los prestadores de servicios de comunicaciones y el colCERT

2) Centralizar la información sectorial de incidentes de seguridad de la información en la entidad responsable de su gestión.

3) Brindar los insumos de información necesaria al colCERT para que realice las actividades de gestión y sensibilización de incidentes en beneficio de las múltiples partes interesadas

A3.2 Descripción de las alternativas analizadas (Reporte a autoridades).

Alternativas consideradas
Alternativa 1: Propuesta publicada
*"**5.1.2.3.3 REPORTE DE INCIDENTES A LAS AUTORIDADES.** Cuando se presenten incidentes de seguridad que afecten significativamente la integridad del servicio de acuerdo con los umbrales definidos en el numeral 5.1.2.3.2 del presente artículo, y la causa del incidente sea por actores maliciosos, los proveedores de redes y servicios de telecomunicaciones deberán enviar por medios electrónicos, dentro de las 2 horas subsecuentes a la determinación del incidente, un reporte al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) que incluya los elementos descritos en el respectivo artículo (fecha del incidente, servicio afectado, número de usuarios afectados, duración, causa del incidente) y una descripción del incidente, así como de las acciones llevadas a cabo por el proveedor para mitigar o resolver el incidente."*

Alternativa 2: Propuesta basada en los comentarios allegados durante la etapa de discusión y en las mesas de trabajo adelantadas.
5.1.2.3.3 REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN A LAS AUTORIDADES. *Cuando se presenten incidentes de seguridad de la información, los proveedores de redes y servicios de comunicaciones deberán enviar por medios electrónicos, después del cierre del incidente, esto es después de su contención erradicación o recuperación, un reporte al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) que incluya los elementos descritos en el numeral 5.1.2.3.2 del presente artículo, (fecha del incidente, servicio afectado, número de usuarios afectados, duración, categoría de incidente) y una descripción del incidente, así como de las acciones llevadas a cabo por el proveedor para mitigar o resolver el incidente.* *Si el incidente sería clasificado de severidad clase III "Serio" o severidad clase IV "Muy Seria", según lo dispuesto en el Anexo 5.8 de la presente Resolución, esto es, si el incidente actúa sobre sistemas de información importantes o resulta en pérdidas graves para la organización, o implica pérdidas sociales importantes, los proveedores de redes y servicios de comunicaciones deberán enviar un reporte al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) dentro de los 120 minutos subsecuentes a la detección del incidente, con la información disponible al momento del reporte.* *De manera voluntaria los proveedores de redes y servicios de comunicaciones podrán entregar información adicional requerida por colCERT para la gestión del incidente."*
Alternativa 3: Regulación vigente – en el Título V de la Resolución Compilatoria CRC 5050 de 2016.
El marco regulatorio vigente no tiene previsiones vigentes en materia de registro a autoridades de seguridad de la información.

A3.3 Análisis de efectividad (Reporte a autoridades).

Para determinar la efectividad de las alternativas propuestas, se analizó el cumplimiento de cada una respecto de los objetivos dispuestos en el proyecto regulatorio, los cuales se describen en el numeral 0 del presente Anexo.

Respecto a la valoración de las alternativas, se asigna un puntaje máximo de 3 si la alternativa cumple con el objetivo en mayor o menor medida y se asigna el mismo peso a cada objetivo (20%), de forma que la propuesta más efectiva será aquella que se aproxima al máximo puntaje, es decir 3.

	Objetivo 1	Objetivo 2	Objetivo 3	Resultado (Max 3)
Alternativa 1	✓✓ La Alternativa 1 propone un esquema de reporte de incidentes que permite la cooperación, además esta última se da bajo características de oportunidad (120min) entre el colCERT y los prestadores de servicios de comunicaciones. Sin embargo, el alcance del reporte es solo de incidentes con "afectación significativa" a la integridad del servicio, por lo cual no se visibilizan otros incidentes que podrían ser pertinentes para las acciones de coordinación del colCERT	✓✓ La Alternativa 1 permite la centralización de la información de incidentes de seguridad de la información, pero solo de aquellos con "afectación significativa" a la integridad del servicio, por lo cual solo estos podrían entrar a ser gestionados por colCERT	✓✓ El esquema de reporte de información de incidentes de seguridad a las autoridades, propuesto en la Alternativa 1, realiza una categorización de la información que excluye incidentes "no significativos" por lo que no apoya por completo el desarrollo de planes generales de gestión de incidente y planes de desarrollo	**2**
Alternativa 2	✓✓ La Alternativa 2 permite la coordinación oportuna solo para aquellos incidentes sobre sistemas de información importantes o que resulten en pérdidas graves para la organización, o que impliquen pérdidas sociales importantes, en esta medida la acción de coordinación de colCERT estaría limitada a aquellos incidentes considerados "críticos". Para los demás el esquema de coordinación no prevé tiempos estimados por lo que la coordinación se da en los criterios de oportunidad determinados por los operadores de servicios de comunicaciones.	✓✓✓ La Alternativa 2 permite la centralización de la información de incidentes de seguridad, sin discriminar sobre su impacto en la integridad del servicio, por esta razón esta Alternativa se valora con un puntaje superior a la Alternativa 1 respecto de la alineación con este objetivo.	✓✓✓ La Alternativa 2 brindaría la información de los incidentes de seguridad de la información suficientes para desarrollar planes de sensibilización optimizados.	**2.33**
Alternativa 3 (statu quo)	- El marco regulatorio actual no contempla mecanismos de coordinación entre los prestadores de servicios de comunicaciones y las autoridades	- El marco regulatorio actual no permite análisis estadístico de la información de incidentes de seguridad de la información.	- El marco regulatorio vigente no permite la categorización de la información de incidentes de seguridad de la información.	**0.0**

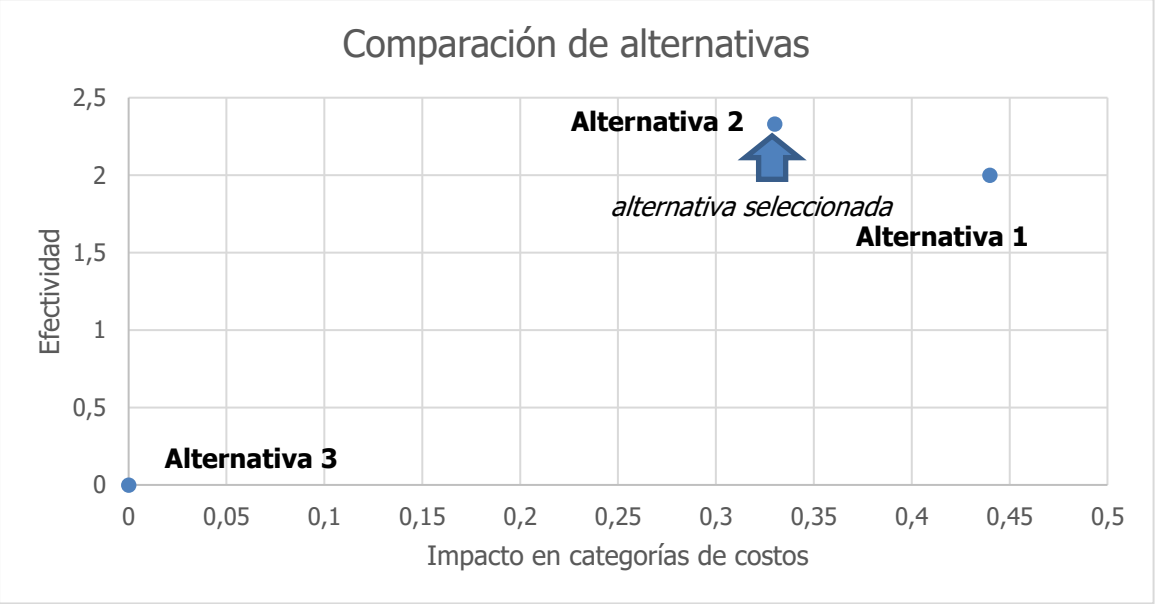
A3.4 Análisis de costos (Reporte a autoridades).

Respecto a la valoración de las características de costo de las diferentes alternativas, se asigna un puntaje de 1 a 3 dependiendo del nivel de impacto en las diferentes categorías de costos para las múltiples partes interesadas, cada valoración es ponderada con un peso proporcional (11,11%), por lo que la propuesta considerada de menor impacto en los costos será aquella que se aproxima al mínimo puntaje, es decir 0.

Categoría de costo	Alternativa 1	Alternativa 2	Alternativa 3 (Statu quo)
Notificación	✗✗	✗	-
	El artículo propuesto en la Alternativa 1 incluye la notificación de todos los incidentes de seguridad de la información con afectación significativa a la integridad del servicio, al colCERT, dentro de los 120 minutos subsecuentes a su detección, este alcance de notificación temprana ha sido considerado oneroso por algunas partes interesadas, de acuerdo con lo manifestado en las mesas de trabajo adelantas por la CRC sobre esta temática.	La Alternativa 2 propone la notificación de los incidentes de seguridad, al colCERT, durante la fase de cierre de incidentes, se mantiene el umbral de 120 minutos únicamente para incidentes sobre sistemas de información importantes o que podrían resultar en pérdidas graves para la organización, este alcance revisado se estima de menor impacto que el propuesto en la Alternativa 1.	El marco normativo vigente al que hace referencia la alternativa 3 no requiere de actividades de notificación
Educación	-	-	-
	No se evidencian actividades de permisos asociadas a la alternativa 1.	No se evidencian actividades de permisos asociadas a la alternativa 2.	El marco normativo vigente al que hace referencia la alternativa 3 no requiere de actividades de Educación.
Permisos	-	-	-
	No se evidencian actividades de permisos asociadas a la alternativa 1.	No se evidencian actividades de permisos asociadas a la alternativa 2.	No se evidencian actividades de permisos asociadas al marco actual.
Compras	-	-	-
	La notificación de incidentes no requiere de compra de productos o servicios especializados, la misma se da dentro de la implantación del SGSI y el mecanismo dispuesto para el envío de información por parte del colCERT es el de sistemas de correo electrónico con cifrado PGP	La notificación de incidentes no requiere de compra de productos o servicios especializados, la misma se da dentro de la implantación del SGSI y el mecanismo dispuesto para el envío de información por parte del colCERT es el de sistemas de correo electrónico con cifrado PGP	El marco normativo vigente al que hace referencia la alternativa 3 no incluye necesidades de compras puesto que no prevé ningún tipo de reporte de incidente a las autoridades
	-	-	-

Mantenimiento de registros	Los eventuales costos de mantenimiento de registros han sido considerados dentro del análisis para la sección 2.3	Los eventuales costos de mantenimiento de registros han sido considerados dentro del análisis para la sección 2.3	Los eventuales costos de mantenimiento de registros han sido considerados dentro del análisis para la sección 2.3
Vigilancia y control	-	-	-
	No se evidencian actividades de vigilancia y control asociadas a la alternativa 1.	No se evidencian actividades de vigilancia y control asociadas a la alternativa 2.	No se evidencian actividades de vigilancia y control asociadas al marco normativo vigente (alternativa 3).
Publicación y documentación	-	-	-
	No se evidencian actividades de publicación de registros asociadas a la alternativa 1.	No se evidencian actividades de publicación asociadas a la alternativa 2.	No se evidencian actividades de publicación asociadas al marco normativo vigente (alternativa 3).
Procesales	-	-	-
	No se evidencian actividades de tipo procesal asociadas a la alternativa 1.	No se evidencian actividades de tipo procesal asociadas a la alternativa 2.	No se evidencian actividades de tipo procesal asociadas al marco normativo vigente (alternativa 3).
Retrasos	✗✗	✗	-
	Se identifica que la alternativa 1 puede generar retrasos en la gestión de incidentes de seguridad de la información, el desarrollo de información detallada como análisis de causas, dentro de los 120 minutos subsecuentes a la detección, requiere de acciones que pueden retrasar las actividades de contención generando potenciales costos de retraso.	El reporte que se mantiene dentro de los 120 minutos en la alternativa 2 (sistemas de información importantes o que podrían resultar en pérdidas económicas y sociales) incluye únicamente un reporte inicial sin información detallada, la cual puede ser entregada de forma voluntaria por los operadores evitando retrasos en la gestión de incidentes.	No se evidencian costos por retrasos asociados al marco normativo vigente (alternativa 3).
Resultado	**0.44**	**0.22**	**0.0**

A3.5 Análisis comparativo de los costos y efectividad de las alternativas (Reporte a autoridades).



Fuente: Elaboración propia

De acuerdo con los análisis expuestos en esta sección, se evidencia que la alternativa que permite abordar de forma más efectiva las problemáticas evidenciadas en el curso del presente proyecto regulatorio respecto al reporte a las autoridades de seguridad de la Información es la Alternativa 2, la cual corresponde a las medidas adoptadas en el proyecto de resolución artículo 2.