COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

"Revisión del marco regulatorio para la gestión de riesgos de seguridad digital" Documento de respuesta a segunda fase de observaciones

Versión Sesión de Comisión

Capital Intelectual
Coordinador: Claudia X. Bustamante
Líder: Felipe Sarmiento

Octubre de 2018

vive digital para la gente

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

CONTENIDO

Introducción **3**

1. Cambios realizados a la segunda propuesta regulatoria **4**

2. Partes interesadas que presentaron observaciones a la segunda publicación **5**

3. Observaciones de carácter general a la segunda publicación **5**

3.1 Sobre los incidentes de terceras partes 5

3.2 Sobre la necesidad de coordinación con otras entidades del estado en el marco de la implementación del CONPES 3854 6

3.3 Sobre el marco legal para la gestión de incidentes en infraestructuras criticas cibernéticas 7

3.4 Sobre las actividades de vigilancia y control 8

3.5 Sobre la necesidad de involucrar otros agentes de la cadena de valor 9

3.6 Sobre la vigencia 10

3.7 Sobre el análisis de impacto 11

3.8 Sobre la responsabilidad de los usuarios 12

4. Observaciones al articulado de la segunda publicación del proyecto de resolución **14**

4.1 Sobre las definiciones: 14

4.2 Sobre la información de incidentes de seguridad de la información: 14

4.3 Sobre los reportes de incidentes de seguridad de la información 16

4.4 Seguimiento a la gestión de incidentes de seguridad de la información. 21

Anexo – Análisis costo efectividad **21**

A1 Medidas de Seguridad de Red 25

A2 Previsiones frente a los incidentes de seguridad 33

A3 Previsiones de reporte a autoridades 42

Introducción

Desde el segundo semestre de 2017, la CRC inició el desarrollo del proyecto denominado *"Revisión del marco regulatorio para la gestión de riesgos de seguridad digital"*[1] con el objetivo de actualizar las previsiones en materia de seguridad digital en el sector de las telecomunicaciones y alinearlas a la visión de responsabilidad compartida y gestión del riesgo de seguridad digital en las múltiples partes interesadas propuesta en el CONPES 3854 de 2016[2].

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, considerando para ello un enfoque de gestión de riesgos de seguridad digital.

De acuerdo con este mandato, la CRC publicó una propuesta regulatoria inicial en materia de seguridad digital el 24 de noviembre de 2017, sobre la cual se recibieron observaciones hasta el 19 de diciembre de 2017. Posteriormente el 16 de mayo de 2018 esta entidad publicó una segunda propuesta regulatoria ajustada teniendo en cuenta las observaciones y comentarios allegados por el sector, la academia y la sociedad civil, así como un primer documento de respuesta a observaciones[3]. Esta segunda propuesta regulatoria fue sometida a una segunda fase de discusión sectorial hasta el 30 de mayo de 2018.

Así, una vez analizadas las observaciones presentadas durante las dos fases de comentarios, y después de adelantar mesas de trabajo con las múltiples partes interesadas, este documento responde a los comentarios allegados en la segunda fase y da claridad sobre las modificaciones realizadas a la segunda propuesta de resolución.

---

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 Política Nacional de Seguridad Digital, CONPES 3854 de 2016, disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

3 La segunda publicación de la propuesta, incluyo un primer documento de respuesta a observaciones y un anexo de análisis costo efectividad de alternativas, los cuales pueden consultarse en: https://www.crcom.gov.co/es/pagina/ciberseguridad

1. Cambios realizados a la segunda propuesta regulatoria

A continuación, se resumen los principales cambios efectuados a la segunda propuesta regulatoria; para más 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 agrega la referencia a la fuente de las definiciones (Familia de estándares ISO/IEC 27000:2016)
Artículo 2. Temática: Políticas de gestión de seguridad de la Información	Sin modificaciones respecto a la versión del proyecto de resolución publicado el 16 de mayo de 2018.
Artículo 2. Temática: Información de Incidentes	Sin modificaciones respecto a la versión del proyecto de resolución publicado el 16 de mayo de 2018.
Artículo 2. Temática: Reporte a autoridades	Se amplía el plazo para el reporte a colCERT de incidentes "Muy Serios" (Clase IV) y "Serios" (Clase III) a 24 horas hábiles.
Artículo 3. Clasificación de severidad de incidentes	Sin modificaciones respecto a la versión del proyecto de resolución publicado el 16 de mayo de 2018.
Artículo 4. Seguimiento a gestión de incidentes	Se amplía hasta 31 de marzo de 2020 el plazo para la presentación a la CRC de la información sobre incidentes de seguridad del 2019.
Artículo 5. Vigencia y derogatoria	Se amplía a dieciocho (18) meses a partir de la publicación, la entrada en vigencia de las obligaciones de implementación de Sistemas de Gestión de Seguridad de la Información y reporte de incidentes a autoridades

2. Partes interesadas que presentaron observaciones a la segunda publicación

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

1. Telefónica
2. Comunicación celular COMCEL
3. ETB
4. TIGOUNE
5. ANDESCO
6. CCIT – NAP Colombia

3. Observaciones de carácter general a la segunda publicación

3.1 Sobre los incidentes de terceras partes

3.1.1 CCIT – NAP Colombia

La agremiación manifiesta que la resolución no menciona el impacto potencial que puede generar un proveedor y/o tercero que esté relacionado con la prestación de los servicios y que se vea afectado por incidentes de seguridad, NAP Colombia inquiere cual debería ser la clasificación cuando un incidente ocurra a un proveedor internacional y afecte la prestación de los servicios a nivel nacional. Según esta agremiación debería precisarse la forma de reportar este tipo de afectación.

CRC Se recuerda a la agremiación que la versión anterior de la propuesta de resolución incluía la categoría *"Fallas externas al operador"*[4], sin embargo durante la fase de discusión sectorial, mesas de trabajo y primera respuesta a observaciones, esta clasificación se descartó en cuanto las partes interesadas manifestaron que este tipo de incidentes ya son reportados a través del régimen de calidad y sus obligaciones asociadas, si el incidente no ocurre en la red del operador, entonces el mismo puede considerarse un incidente de indisponibilidad del servicio, por lo que el reporte del mismo a colCERT como incidente de seguridad de la información -si esta fuera la causa del mismo-, tendría un carácter voluntario.

[4] Propuesta inicial de resolución publicada el 24/11/2017, disponible en: https://www.crcom.gov.co/recursos_user/2017/actividades_regulatorias/ciberseguridad/Proyecto_Resolucion_seguridad_digital_VPublicar.pdf

3.2 Sobre la necesidad de coordinación con otras entidades del estado en el marco de la implementación del CONPES 3854

3.2.1 COMCEL

Para el operador, teniendo en cuenta que los incidentes relacionados con datos personales ya deben ser reportados a la Delegatura para la Protección de Datos Personales de la SIC, ese tipo de incidentes deberían encontrarse explícitamente excluidos de esta propuesta para evitar duplicidad de reportes.

CRC 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.

Se resalta que el reporte a la SIC es complementario, responde a necesidades diferentes, reporta información distinta tal como se puede ver en el Título VI de la Ley 1581 de 2012, que se refiere a los deberes de los responsables del tratamiento y encargados del tratamiento de datos personales, en particular en el literal n del artículo 17 se dictan los deberes de los responsables del tratamiento de los datos personales, y se da el punto de partida para el reporte de información objeto de discusión y presuntamente con las mismas características que el reporte propuesto en el proyecto de resolución.

Dicha obligación está desarrollada en el Capítulo Segundo: Registro Nacional De Bases De Datos –RNBD del Título V de la Circular Única que determina que el reporte de información está enmarcado en los incidentes de seguridad definidos así:

> *"(ii) Incidentes de seguridad. Se refiere a la **violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado**, que deberán **reportarse** al RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.*
>
> *(…)"*

Finalmente, el Manual de Usuario del Registro Nacional de Bases de Datos – RNBD define el alcance del reporte, exigiendo que: *"como mínimo, debe informarse el tipo de incidente, la fecha en que ocurrió y la fecha en que se tuvo conocimiento del mismo, la causal, el tipo de datos personales comprometidos y la cantidad de titulares afectados".*

En consecuencia, no existiría ninguna duplicidad de reporte de incidentes entre lo estipulado en este proyecto y en lo previsto en el Título VI de la Ley 1581 de 2012 desarrollado en el Título V de la Circular Única de la SIC.

3.2.2 ETB

ETB aduce que el proyecto sólo considera a ColCERT como receptor de los reportes de información. Sin embargo, el operador manifiesta que el Modelo de Gestión de Riesgos de Seguridad elaborado por MinTIC indica que *"los riesgos, amenazas y vulnerabilidades más importantes"* deben ser reportados a el CSIRT de Gobierno, –Centro Cibernético Policial de la Policía-. Lo que tendría como efecto que los PRST deban realizar reportes y trámites en diferentes entidades.

CRC Frente al comentario de ETB se aclara que el Modelo Nacional de Gestión de Riesgos de Seguridad Digital publicado por MinTIC en diciembre de 2017, no es un modelo gestión o de reporte de incidentes. En el mismo se busca centralizar los riesgos y vulnerabilidades con el fin de identificar acciones preventivas, el modelo diseñado por MinTIC no prevé el intercambio de información durante la detección o respuesta a incidentes, debe resaltarse además que dicho Ministerio ha manifestado que el modelo se encuentra en construcción, y además es de carácter voluntario, teniendo en cuenta lo anterior el reporte de riesgos (voluntario y en definición) no riñe de manera alguna con la propuesta presentada por la CRC para el reporte de incidentes por parte de los PRST. Esta condición fue expuesta por parte de los funcionarios de MinTIC que tuvieron oportunidad de aclarar el tema en las diferentes mesas de trabajo adelantadas en el primer semestre de 2018.

3.3 Sobre el marco legal para la gestión de incidentes en infraestructuras críticas cibernéticas

3.3.1 COMCEL

El operador interpreta a partir del CONPES 3854 que la obligación de reportar al ColCERT, recae únicamente sobre los propietarios u operadores de infraestructuras críticas; afirma además que estos operadores no se encontrarían definidos legalmente. Considera que la CRC ha concluido que los operadores de telecomunicaciones están incluidos entre los propietarios de infraestructura crítica sin un sustento legal.

Afirma además que la CRC estaría extralimitando sus funciones legales, al pretender establecer un reporte al ColCERT, a través del proyecto regulatorio CRC, porque los propietarios de la infraestructura crítica no están definidos legalmente, y en el caso en el que se definieran los operadores estarían obligados a presentar dos reportes sobre el mismo incidente.

CRC Frente a la observación según la cual se considera que la CRC se estaría extralimitando en sus funciones legales al establecer el reporte al ColCERT, es importante advertir que tal y como está plasmado en el proyecto de resolución publicado, y de conformidad con lo dispuesto en el numeral 3 del artículo 22 de la Ley 1341 de 2009, por el cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones, esta

Comisión está facultada para expedir toda la regulación de carácter general y particular en las materias relacionadas, entre otros, con los parámetros de calidad de los servicios, aplicable a todos los proveedores de redes y servicios de telecomunicaciones.

Es así como la fuente legal del reporte no procede de la definición de lo que se entiende por infraestructura crítica, sino que la misma surge en correspondencia con las competencias legales en temas de calidad y reportes de información.

En tal sentido, la importancia de reporte de información al ColCERT, no se limita a la definición de qué es una infraestructura crítica, sino que responde a la necesidad que al mediano y largo plazo esta información se encuentre consolidada en la entidad más idónea para tal fin. Adicionalmente, de acuerdo con lo previsto en el 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, 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.

3.4 Sobre las actividades de vigilancia y control

3.4.1 TELEFÓNICA

El operador manifiesta que dada la obligación de reportar los incidentes al colCERT, dentro de un plazo determinado, en el caso que los operadores no logren cumplir con los plazos de reporte establecidos, los PRST estarían en una posición de riesgo de incumplimiento y posibles multas por parte del Ministerio de TIC, en los términos del numeral 12 del artículo 64 de la Ley 1341 de 2009.

TELEFÓNICA, manifiesta que a pesar de lo anterior en el documento de respuesta a comentarios, literal *"A3.4 Análisis de costos (Reporte a autoridades)"*, la CRC indica que frente a la categoría de costo *"vigilancia y control", "No se evidencian actividades de vigilancia y control asociadas a la alternativa 2."* , para el operador si habrían actividades de vigilancia y control así como costos asociados a las mismas, tanto para las autoridades como para los PRST.

Según el operador, uno de los 5 ejes de trabajo del CONPES 3854, es la generación de "*mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico."* resalta en su observación la recomendación del CONPES de incrementar el intercambio de información, pero considera que la imposición de plazos para entrega de información no es la forma más conveniente de incentivar el proceso colaborativo.

CRC Frente a la observación de TELEFÓNICA, se procede a modificar el Anexo de análisis costo efectividad, no obstante se reitera que esta propuesta pretende proveer un marco amplio y flexible de forma que los operadores cuenten con lineamientos que les permitan implementar Sistemas de Gestión de Seguridad de la Información, lo cual incluye reportes a las partes interesadas, lo anterior conlleva a que las actividades de vigilancia y control sean de mínimo impacto, y se enfoquen en verificar la implementación del mencionado sistema y el reporte efectivo a las autoridades. Por lo anterior, esta Comisión manifiesta a manera de recomendación a la división de Vigilancia y Control de MinTIC, que podría monitorear y realizar seguimiento a los siguientes elementos documentales:

Tabla 1 Elementos recomendados de vigilancia y control

Elemento de la propuesta	Elementos documentales recomendados para vigilancia y control:
Planeación y definición del SGSI	- Análisis de riesgos. - Clasificación de riesgos e impactos. - Desarrollo de estrategias para gestionar el riesgo. - Selección de controles.
Implementación del SGSI	- Implementación de controles seleccionados. - Documentación del control y la supervisión de la implementación. - Entrenamiento y conciencia de riesgos de seguridad de la información en la organización.
Revisión de desempeño y Reportes a autoridades	- Detección de incidentes de seguridad durante la operación. - Monitoreo de sostenibilidad y efectividad de los controles. - Gestión de los reportes.

Fuente: Elaboración propia.

Respecto a los plazos, se remite al operador a la respuesta 4.3.2.

3.5 Sobre la necesidad de involucrar otros agentes de la cadena de valor

3.5.1 TIGOUNE

El operador considera necesario que en línea con las consultas que se encuentra realizando la CRC se determinen responsabilidades en materia de seguridad digital en OTTs, en tanto que los mismos serían corresponsables de la información de sus usuarios y en algunos casos la gestión de sus contenidos, y ellos también estarían potencialmente envueltos en ataques informáticos como los que son materia de discusión en este proyecto regulatorio.

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 servicios OTT. Así mismo, este documento menciona que los operadores de comunicaciones tienen características especiales como habilitadores de la digitalización en los distintos sectores económicos. 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* ". Aun 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.

Finalmente, debe reconocerse que actualmente no tenemos las competencias legales para incluir a los proveedores de servicios OTT dentro los destinatarios del presente proyecto regulatorio. No obstante, los servicios OTT, en tanto que son responsables de información de usuarios, están cobijados bajo el marco normativo de protección de datos personales vigilado por la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio, de cara al régimen de protección contenido en la Ley 1581 de 2012.

3.6 Sobre la vigencia

3.6.1 TIGOUNE -ETB- ANDESCO

El operador solicita que la aplicación del artículo 5.1.2.3, tenga vigencia a partir de junio de 2019, con la finalidad de realizar las adecuaciones y desarrollos necesarios para la remisión de la información.

Para ETB el tiempo de implementación sería demasiado corto, por lo que se solicitan que sea de 18 a 24 meses, para coordinar los ajustes en los servicios fijos y móviles.

ANDESCO por su parte solicita un plazo razonable para la implementación del artículo 5.1.2.3.3, de dieciocho (18) meses.

CRC Respecto al comentario allegado por el operador TIGOUNE, en el sentido de que la aplicación del artículo 5.1.2.3, tenga vigencia a partir de junio de 2019, con la finalidad de realizar las adecuaciones y desarrollos necesarios para la remisión de la información, encontramos que el mismo está alineado a la manera como se publicó el proyecto de resolución.

No obstante, y frente a los comentarios de otros actores como ETB y ANDESCO, coincidentes en que el periodo de implementación sea de 18 meses, esta Comisión considera que el mismo es un tiempo prudente para el desarrollo de las medidas regulatorias propuestas, por lo que se acepta el comentario.

3.7 Sobre el análisis de impacto

3.7.1 ETB

ETB manifiesta que las cargas operativas y financiera del almacenamiento de información, deben actualizarse y considerarse en el análisis de impacto normativo-

CRC Frente a lo manifestado por ETB, de contemplar tanto las cargas operativas y financieras del almacenamiento de información dentro del análisis de impacto Normativo, esta Comisión se permite recordar que, en las observaciones allegadas a la primera publicación del marco regulatorio para la Seguridad Digital[5], se expuso por parte de un operador la necesidad de adelantar Análisis de Impacto Normativo (AIN) al proyecto de resolución, comentario que fue acogido por esta Comisión y se aplicó la metodología de AIN establecida en el Documento CONPES 3816. Sin embargo, con base en la clasificación de impacto determinada para el proyecto, se anexó al documento de respuestas el AIN de tipo cualitativo, el cual para este caso específico resulta suficiente para conocer si la intervención a realizar en el proyecto se justifica y si la misma es proporcionada.

Ahora bien, respecto al comentario allegado por ETB se aclara que, en el Anexo de AIN sección *"A2 Previsiones frente a los incidentes de seguridad"*, se evaluó en la categoría *"mantenimiento de registro"*, el costo asociado al almacenamiento de la información sobre incidentes de seguridad, el cual arrojó lo siguiente:

"... 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…*

... 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.

[5] Publicadas el 16 de mayo de 2018 y disponibles en: https://www.crcom.gov.co/es/pagina/ciberseguridad

Categoría de costo	Alternativa 1	Alternativa 2	Alternativa 3 (Statu quo)
	✕✕	✕	-
Mantenimiento de registros	*La alternativa 1 no limita el tiempo de almacenamiento y su alcance incluye diversas 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.*	*La alternativa 2 limita el tiempo de almacenamiento de registros a 12 meses y acota las 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.*	*No se evidencian actividades de mantenimiento de registros asociadas al marco actual.*
Resultado	**0.66**	**0.33**	**0.0**

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…"

Con base en lo expuesto anteriormente se observa que el comentario recibido por ETB ya se encuentra incluido en la categoría de costo en mención, por lo cual no se acoge la observación. Adicionalmente también es importante aclarar que cada entidad será encargada de asumir el costo asociado al almacenamiento de la información de incidentes de seguridad. Así, si bien los requirentes de la información no van a cubrir los costos de almacenamiento de los operadores, los responsables del almacenamiento (colCERT) deben contar con su propia infraestructura y por lo tanto incurrirán también en costos asociados a mantenimiento de registros, situación que fue contemplada en el desarrollo de la propuesta regulatoria.

3.8 Sobre la responsabilidad de los usuarios

3.8.1 ETB

Para el operador las obligaciones y deberes de los usuarios frente a los incidentes de seguridad deben ser considerados en el proyecto no sólo desde el punto de vista de la creación del riesgo, sino desde la necesidad de exclusión o aclaración frente al reporte cuando el incidente se presente en infraestructura administrada por el usuario o por el uso que el usuario dé a sus dispositivos.

CRC Frente a la observación de ETB, es importante mencionar que el actual Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones (Resolución 5111 de 2017), en el Capítulo 1, Sección 2, Artículo 2.1.2.2, se estipulan las obligaciones de los usuarios, dentro de las que se encuentran:

"… 2.1.2.2.4 No cometer o ser partícipe de actividades de fraude.
2.1.2.2.5 Hacer uso de equipos terminales móviles homologados.
2.1.2.2.7 Hacer uso adecuado de las redes, de los servicios y de los equipos necesarios para la prestación de los mismos.
2.1.2.2.8 Informar al operador ante cualquier falla en la prestación del servicio…"

Adicionalmente, en el documento soporte del proyecto regulatorio para la Seguridad Digital se identificaron roles y responsabilidades, para los distintos actores, incluyendo los usuarios. Así, se proponen acciones concretas para mejorar la gestión de riesgos de seguridad digital por parte de los usuarios, lo anterior quedó inmerso en la Sección 6.2.2 del documento en mención:

"… ***Recomendación Usuarios***

En el presente estudio se observó que muchos de los incidentes digitales tienen origen directo en error humano, por lo cual es importante generar conciencia a los usuarios de telecomunicaciones respecto al uso adecuado de Internet. Así, iniciativas del Gobierno como "Ciudadanía Digital[6]" y "En TIC Confío[7]" son estrategias que abren espacios para educar al ciudadano en torno al buen uso de Internet.

Por un lado, Ciudadanía Digital ofrece 28 cursos a Colombianos mayores de 13 años que estén interesados en contenidos digitales, tres de estos cursos están relacionados con Seguridad Digital: I. Prevenir para estar seguros en digital[8], II. Experiencias digitales seguras[9] y III. Redes sociales y medios digitales, una oportunidad para los jóvenes[10]. Por otro lado, en TIC Confío ofrece a la ciudadanía herramientas para enfrentar los riesgos asociados al uso de nuevas tecnologías, como el phishing, el ciberacoso, la ciberdependencia y el abuso de menores de edad, entre otros. Esta última está dirigida a todos los ciudadanos y se realiza a través de la Cátedra Poder Digital, gratuita y de 45 minutos de duración[11]…"

---

6 La Ciudadanía Digital es el resultado de la transformación digital y productiva de los ciudadanos. Ante el reto de la economía digital, como país se tiene la meta de impulsar esa transformación en los próximos años. Para mayor información, ver: http://www.ciudadaniadigital.gov.co/627/w3-channel.html

7 Estrategia de promoción de uso responsable de internet y de las nuevas tecnologías del Ministerio de Tecnologías de la Información y las Comunicaciones. Ayuda a la sociedad a desenvolverse e interactuar responsablemente con las TIC, al tiempo que promueve la cero tolerancia con la pornografía infantil y la convivencia digital. Para mayor información, ver: https://www.enticconfio.gov.co/

8 Para mayor información, ver: http://www.ciudadaniadigital.gov.co/627/w3-article-60958.html

9 Para mayor información, ver: http://www.ciudadaniadigital.gov.co/627/w3-article-60956.html

10 Para mayor información, ver: http://www.ciudadaniadigital.gov.co/627/w3-article-60957.html

11 Para mayor información, ver: http://www.enticconfio.gov.co/

Asimismo, se recuerda que los dispositivos utilizados por los usuarios típicamente caen bajo la categoría de equipos terminales, por lo que para el caso específico de los incidentes de seguridad digital, los mismos ya estarían excluidos de la infraestructura del operador y las obligaciones de reporte asociadas.

Por lo expuesto anteriormente, se observa que esta Comisión es consciente que el usuario también cuenta con unas obligaciones y por tanto debe ser responsable de dar un uso adecuado a sus dispositivos. Es así como la observación presentada por ETB ya se encuentra incluida dentro de la propuesta regulatoria y no es necesario adicionar otra referencia respecto al tema.

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

4.1 Sobre las definiciones:

4.1.1 NAP COLOMBIA

La agremiación sugiere incluir en las definiciones de evento, incidente y sistema de gestión de seguridad de la información la cita o referencia bibliográfica explicita a los estándares a partir de los cuales se están adoptando dichas definiciones.

CRC Se acoge la observación y así se verá reflejado en el artículo.

4.2 Sobre la información de incidentes de seguridad de la información:

4.2.1 COMCEL

Para el operador la clasificación de "servicio afectado" no estaría en consonancia con el diseño de las redes de telecomunicaciones actuales, COMCEL manifiesta que para ofrecer los servicios de conectividad que demandan las nuevas tecnologías se cuenta con un alto grado de convergencia. y que, por lo tanto, resulta complejo diferenciar el servicio afectado. Asimismo, considera que la diferenciación no dará mayor valor analítico ni estadístico a la CRC o al colCERT. Por lo cual a su juicio debería eliminarse el campo "servicio afectado" del formato de reporte de información.

CRC Si bien la observación del operador frente a la naturaleza convergente de las redes actuales es pertinente, teniendo en cuenta que la manera en que los servicios son suministrados a los clientes finales, y considerando las capacidades de los operadores en sus diferentes sistemas de soporte a las operaciones, resulta claro que los operadores pueden diferenciar los servicios provistos a sus usuarios,

adicionalmente la desagregación de la información propuesta permitirá a los desarrolladores de política y tomadores de decisiones realizar análisis de impacto en los usuarios de servicios de comunicaciones de manera más detallada y considerando los servicios específicos. Por las razones expuestas no se acoge la observación presentada.

4.2.2 COMCEL

El operador manifiesta que, dada la diversidad de servicios prestados por los operadores, la convergencia de las redes de telecomunicaciones, y la variedad de usuarios, que ahora no son solo personas sino pueden ser también máquinas o servicios que consumen recursos de red, calcular el número de usuarios afectados resultaría complejo y significaría una gran carga operativa para las áreas de gestión de incidentes de los operadores. Por lo tanto, sugieren que el campo usuarios afectados sea eliminado del reporte o se unifique el criterio utilizado para internet y telefonía móvil, es decir, que se trate de un número potencial de usuarios afectados.

CRC Como se mencionó en la respuesta 4.2.1, teniendo en cuenta las capacidades actuales de los operadores en sus diferentes sistemas de soporte a las operaciones, los operadores pueden diferenciar el servicio utilizado por sus usuarios, por su parte el criterio para telefonía móvil emerge de desarrollos normativos consolidados en el régimen de Calidad, en el cual se evidenció que el criterio de número potencial de usuarios es necesario únicamente debido al nomadismo inherente a los usuarios de servicios móviles, por lo tanto dicho criterio no es necesario en redes fijas, adicionalmente la desagregación de la información propuesta permitirá a los desarrolladores de política y tomadores de decisiones realizar análisis de impacto en los usuarios de servicios de comunicaciones de manera más detallada y considerando la afectación real a los usuarios. Por las razones expuestas no se acoge la observación presentada.

4.2.3 COMCEL

Según COMCEL, la categoría de incidente denominada "*Denegación del servicio*" está directamente ligada a la indisponibilidad del recurso, servicio o acceso a información, para el operador, la discusión sectorial había llegado a la conclusión de que esta categoría no haría parte de los reportes exigidos en este proyecto de resolución, porque es una dimensión que ya hace parte de los reportes relacionados con el régimen de calidad y por tanto se debe eliminar del presente proyecto.

CRC Debe ponerse de presente que la categoría *"Denegación del servicio"* si bien está ligada a la disponibilidad de un recurso, la misma tiene características específicas que la diferencian de la medición de disponibilidad de elementos de red, en particular en cuanto los mismos son incidentes orientados a afectar la capacidad de un sistema o red, es de destacar que la categoría "Denegación del Servicio" fue propuesta por COMCEL para la clasificación de incidentes durante las mesas de trabajo y en las

observaciones presentadas a esta Comisión durante la primera fase de discusión sectorial[12], de acuerdo con lo anterior no se acoge la observación presentada.

4.2.4 TELEFÓNICA

El operador considera que debe eliminarse la categoría denominada "Abuso" y que se define como "*la violación de las políticas de seguridad del sistema de información de una organización*". Argumenta que las demás categorías como la denegación de servicio, acceso no autorizado y malware ya se consideran una violación a las políticas de seguridad, por lo que el abuso ya estaría implícito en las demás categorías

CRC Se recuerda al operador que la clasificación propuesta es una referencia a la sugerencia de la norma ISO 270035-1:2016 Anexo B, si bien es cierto que dichos incidentes pueden clasificarse de manera general en la categoría de "Abuso", dado que los mismos tienen categorías específicos, se espera que la categoría "Abuso", esté reservada para otro tipo de incidentes, potencialmente desconocidos o imposibles de categorizar en el resto de opciones, de ahí el valor de mantener esta categoría, por esta razón no se acoge la observación presentada.

4.2.5 TIGOUNE

Respecto de la cantidad de información a incluir en el reporte, el operador manifiesta que los PRST solo podrían reportar, a partir de su detención, los campos de fecha del incidente, servicio afectado y categoría del incidente, debido que serían los únicos campos disponibles ante eventos o incidentes que se están desarrollando y sobre los que se adelantan medidas de contención.

CRC Se recuerda a TIGOUNE que para los incidentes que tienen plazo de reporte, severidad "Clase III" o severidad "Clase IV", la resolución dispone que el reporte inicial se haga con "la información disponible al momento del reporte", por lo tanto, la observación está incorporada en la redacción actual de la propuesta.

4.3 Sobre los reportes de incidentes de seguridad de la información

4.3.1 CCIT

NAP Colombia considera que el registro de incidentes de seguridad de la información a reportar debería limitarse únicamente a los incidentes en el marco de la prestación de servicios de comunicaciones y no de forma general.

---

[12] Primer documento de respuesta a observaciones, pág. 29, disponible en: https://www.crcom.gov.co/uploads/images/files/Dto%20Rtas%20Comentarios%20Seguridad%20redes_publicar.pdf

CRC Respecto a la observación presentada por CCIT, es preciso recordar que dentro del marco regulatorio para la seguridad digital se pueden presentar incidentes que, aunque no estén directamente relacionados con la prestación de servicios de comunicaciones, pueden afectar la prestación de estos. No obstante y como quedó redactado en el proyecto de resolución propuesto, los operadores, de manera autónoma, podrán determinar el alcance y las condiciones de funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI). Lo anterior quedó incluido de la siguiente manera:

"... ARTÍCULO 2. GESTIÓN DE SEGURIDAD EN REDES DE TELECOMUNICACIONES....

> *... **5.1.2.3.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**: 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..."*

Por lo tanto, frente a este comentario se aclara que el reporte de incidentes se encuentra integrado en el SGSI, donde los operadores cuentan con la autonomía para dar el alcance que consideren a los reportes de información, razón por la cual la observación se entiende ya acogida en la redacción actual del artículo en cuestión.

4.3.2 CCIT- COMCEL-TELEFÓNICA-TIGOUNE-ANDESCO-ETB

CCIT, COMCEL, y ETB consideran que el tiempo de 120 minutos para incidentes de categoría III y IV es muy corto para los procesos de detección y clasificación, resaltan que de presentarse incidentes "serios" o "muy serios" el esfuerzo se concentraría en la contención del incidente y no en el reporte de este. En partícular COMCEL solicita su eliminación o modificación por un reporte trimestral.

Frente a este mismo punto TELEFÓNICA consideran que para determinar el nivel de severidad de un incidente de seguridad, teniendo en cuenta las tres categorías de impacto (importancia de los sistemas de información, pérdidas de negocio, e impacto social) que implica análisis de información de comportamientos de los sistemas, alarmas, logs, entre otros, que no siempre puede realizarse en 120 minutos, por lo cual solicita que el reporte de este tipo de incidentes sean reportados luego del cierre del incidente.

Para TIGOUNE, teniendo en cuenta la modalidad de operación de los equipos de respuesta a incidentes, cualquier tiempo de reporte debería establecerse en días hábiles, para el caso específico de los incidentes de categoría III y IV, consideran que el reporte requeriría de 24 horas (hábiles) desde la detención.

ANDESCO solicita que el reporte de estos incidentes se realice al cierre de los mismos.

CRC Frente a la propuesta de COMCEL de eliminar el reporte de incidentes de categorías III y IV, o de convertir dicho reporte en un reporte trimestral, nos permitimos aclarar que la CRC ha definido como objetivos específicos en materia de intercambio de información en esta propuesta:

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.

La propuesta de un reporte trimestral, como el sugerido por COMCEL, permitiría lograr los objetivos 1 y 2, sin embargo, debe tenerse en cuenta que, el reporte de incidentes, y más aún el reporte de incidentes de mayor impacto (categorías III y IV) es el insumo principal para un grupo de respuesta a emergencias informáticas, por eso, dentro de los estudios realizados para la presente propuesta, se identificó que, para que el colCERT pueda alcanzar la visión que el CONPES 3854 dispone para él, es decir el de ser el *"punto focal nacional para la gestión de incidentes digitales en Colombia"*, es necesario que la frecuencia de reporte permita la gestión de los incidentes y no simplemente su registro. Por esta razón no se acoge la observación de COMCEL. De manera análoga y siendo válido el mismo argumento, tampoco resultan viables las propuestas de TELEFÓNICA y ANDESCO de realizar el reporte al cierre de los incidentes.

Frente a la propuesta de TIGOUNE, se acoge la observación y así se verá reflejado en el artículo.

4.3.3 COMCEL

El operador manifiesta que colCERT se encontraría desarrollando un protocolo nacional de protección y defensa para la infraestructura crítica cibernética, donde a su vez, se contemplaría la entrega de un reporte de información. Por lo tanto, el operador sugiere a la CRC, dar aplicación al artículo 4 del Decreto MinTIC 3484 de 2012[13], en el sentido de evitar duplicidad en los requerimientos de información periódica para los operadores, ya que, según COMCEL de expedirse dicho protocolo, los operadores tendrán que entregar dos reportes de información sobre el mismo incidente.

[13] *"Por el cual se crea el Sistema de Información y las comunicaciones COLOMBIA TIC"*

CRC Frente al comentario de COMCEL es importante tener presente que actualmente no existe el protocolo nacional de protección y defensa para la infraestructura cibernética referido por el operador en su comentario, por lo anterior será solo en el momento que ello se materialice, si llegase a materializarse, cuando se proceda con la revisión y los ajustes que se consideren pertinentes, como parte del control ex post de la regulación que expide la CRC.

4.3.4 COMCEL -TIGOUNE

Los operadores manifiestan que el proyecto regulatorio incluye el envío de información confidencial directamente a colCERT, sin que a su juicio exista aún un sistema robusto que permita garantizar el envío seguro de la información, COMCEL resalta que esta información tendría un componente reputacional que puede estar sujeto a vulnerabilidades adicionales.

Para el operador la seguridad de esta información no solo se debe garantizar en el almacenamiento que de ella van a hacer la CRC y el colCERT, sino también que debe ser garantizada en los canales por los cuales esta información va a ser transmitida por los operadores, por lo que, a su juicio, sería inaceptable que el medio dispuesto principalmente sea un correo electrónico

Por su parte TIGOUNE considera necesario que de conformidad con el CONPES 3854 se pueda disponer de un protocolo con colCERT para la entrega de los reportes.

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 a nivel nacional para la gestión de incidentes digitales en Colombia. En tal sentido, y de acuerdo con lo expuesto 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, entre ellas el cifrado PGP de las comunicaciones a intercambiar.

El marco de la Ley 1712 de 2014 reglamentada por el Decreto 103 de 2015, dispone que toda información entregada a una entidad pública debe regirse bajo criterios claros definidos dentro del *TÍTULO II. DE LA PUBLICIDAD Y DEL CONTENIDO DE LA INFORMACIÓN.* Es importante tener presente que una vez mediante regulación general se estime pertinente que la información sea reportada, ésta adquiere el carácter de pública, y es el sujeto que entrega la información, en este caso los operadores, quienes tienen el deber de justificar y solicitar la reserva y/o confidencialidad de la misma a la entidad receptora.

En este sentido, es importante resaltar 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 (colCERT), ello siempre y cuando se cumpla con los requisitos de reserva de la información dispuestos en el *TÍTULO III. EXCEPCIONES ACCESO A LA INFORMACIÓN* de la Ley 1712 de 2014.

Por último, esta Comisión ha realizado recomendaciones específicas al colCERT para la creación de una plataforma de reporte de incidentes, y en este sentido que pueda proceder a definir el protocolo requerido que de las garantías necesarios a los PRST dentro del marco legal de la Ley 1712 de 2014.

4.3.5 TELEFÓNICA – TIGOUNE -ETB- ANDESCO

Estos operadores y la agremiación ANDESCO consideran que los incidentes con categoría I y II, son controlables gracias a las herramientas de gestión y control preventivo con las que cuentan, y no requerirían ser reportadas al colCERT, por lo que solicitan eliminar el reporte para estas categorías.

TIGOUNE y ETB adicionalmente argumentan que, el volumen de incidentes de categoría I y II es demasiado elevado y resultaría inviable establecer obligaciones de reporte en estas categorías.

CRC A juicio de esta Comisión si un incidente resulta fácil de controlar con herramientas de gestión y control preventivo, es posible que se trate de un "evento de seguridad de la información" y no de un incidente propiamente dicho, de cualquier forma, la propuesta de resolución da a los operadores un nivel de autonomía suficiente para definir el alcance que tendrán este tipo de eventos en su SGSI, de otra parte, frente a la observación de TigoUne y ETB, según la cual el volumen de incidentes en las categorías I y II es demasiado elevada y no permitiría el reporte, teniendo en cuenta que dichos incidentes se reportan al momento del cierre, es posible que los operadores reporten este tipo de incidentes de manera agrupada, lo cual facilitaría la gestión de las distintas partes interesadas.

4.3.6 ETB

El operador considera que los niveles de seguridad a pesar de ser definidos conforme a la familia de estándares ISO/IEC ISO27000, tienen componentes cualitativos, y es posible que se presenten divergencias al no tener parámetros cuantitativos en su definición. A su juicio la valoración de pérdidas de negocio se tornaría compleja debido a la generalidad del estándar.

CRC Frente a la observación del operador sobre posibles divergencias debidas a elementos cualitativos en la propuesta de clasificación de severidades, se aclara que, si bien estas situaciones pueden suceder, la alternativa de clasificación con definición de umbrales cuantitativos para las pérdidas sociales, pérdidas de negocio e importancia de los sistemas involucrados, aunque tiene la ventaja de eliminar dichas potenciales divergencias, también tiene el efecto de incrementar el tiempo de clasificación, adicionalmente la clasificación cuantitativa de estas variables requeriría de un acervo de información estadística significativa que no es de dominio público, por las razones expuestas en los análisis realizados durante el desarrollo de la propuesta se decidió adoptar parámetros cualitativos que, sin embargo, incorporan criterios para reducir la discrecionalidad.

4.4 Seguimiento a la gestión de incidentes de seguridad de la información.

4.4.1 TIGOUNE

El operador solicita que el reporte del año 2019 se de en marzo de 2020, con la finalidad de preparar la información del periodo 2019 que se solicitado, así como para establecer protocolos que les permitan resguardar la información solicitada.

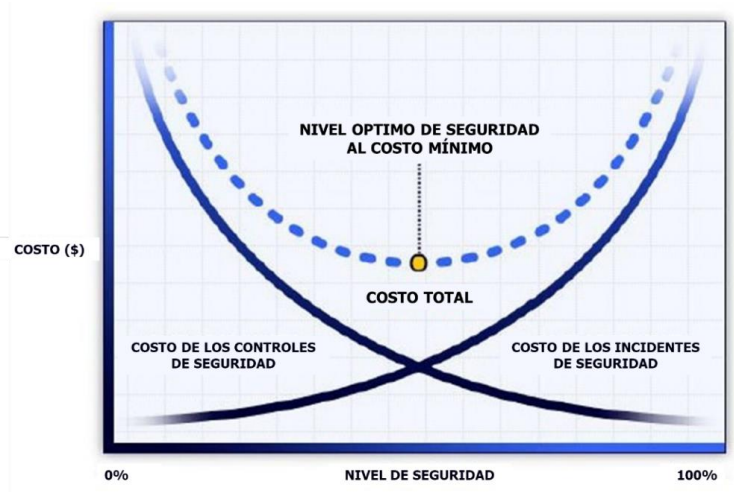
CRC Respecto al comentario allegado por el operador, en el sentido de otorgar un plazo para presentar el reporte de información sobre incidentes de seguridad, correspondiente al periodo comprendido entre el 1º de enero y el 31 de diciembre de 2019, el mismo es aceptado y se modificó la fecha en el proyecto regulatorio con base en lo propuesto por TigoUne, hasta el 31 de marzo de 2020.

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 linea, 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.

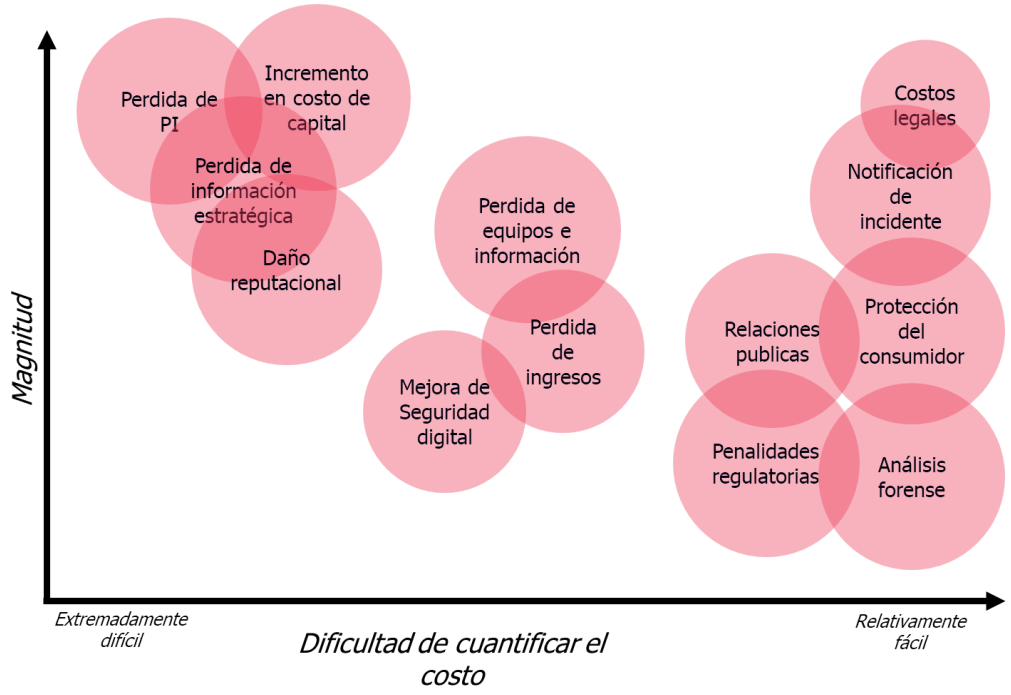


Fuente: Open Web Application Security Project - CISO AppSec Guide: Reasons for Investing in Application Security

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 1 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)[14]. 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.

[14]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

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.
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 máximo puntaje debido a que la certificación se propone como voluntaria.	✓✓✓ Los procesos y procedimientos del marco se encuentran definidos, así como eventuales procedimientos de vigilancia y auditoría.	**2.8**
Alternativa 3 (statu quo)	- Se identifica que esta alternativa no	- Se identifica que esta alternativa no	✓ Se identifica que esta alternativa	✓ Si bien la alternativa identificada es	✓ El marco define los principios generales y los	**0.6**

	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.	proporciona un marco integral para el tratamiento de los riesgos ni tampoco tiene en cuenta las prioridades comerciales sino únicamente las prioridades de seguridad.	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.	una recomendación internacional sectorial que puede dar confianza a las múltiples partes interesadas, existen marcos con mayor reconocimiento.	conceptos asociados a la gestión de la seguridad de la información, sin embargo, los procesos de auditoría y vigilancia no han sido desarrollados.	

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.

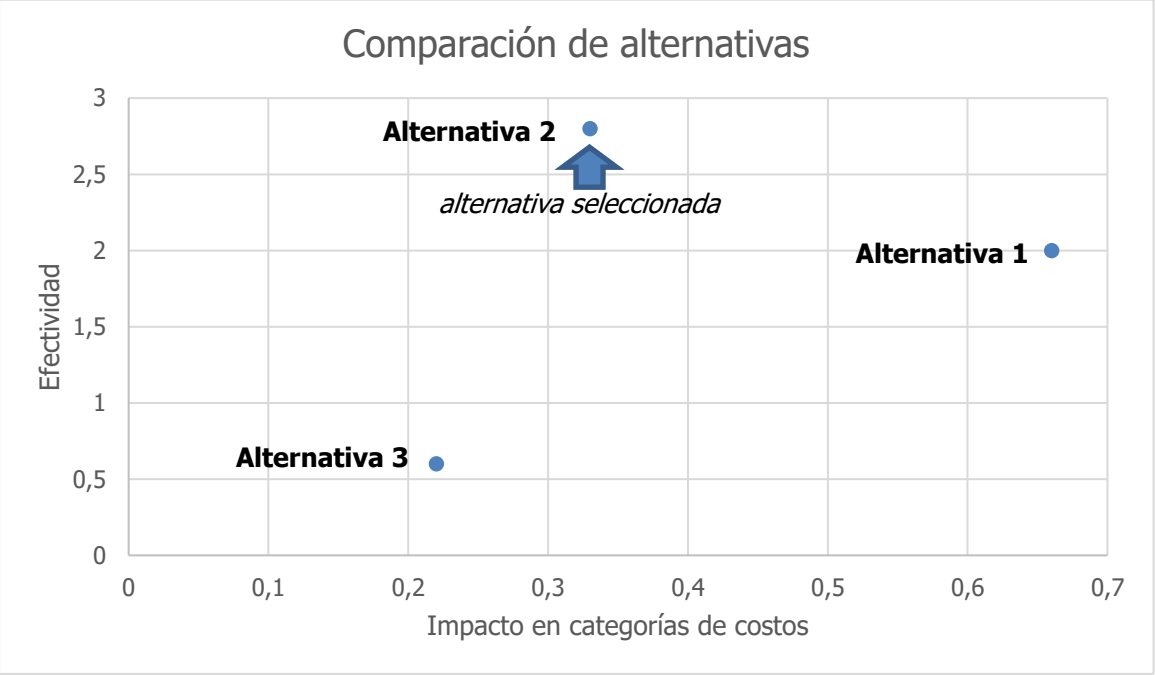
Categoría de costo	Alternativa 1	Alternativa 2	Alternativa 3 (Statu quo)
Notificación	-	-	-
	No se evidencian actividades de notificación asociadas a la alternativa 1.	No se evidencian actividades de notificación asociadas a la alternativa 2.	El marco normativo vigente al que hace referencia la alternativa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

	organizaciones que ya implementan este tipo de sistemas[15]	de menores actividades de educación respecto a la alternativa 2.	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 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	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 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	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 que estos aspectos no generan costos adicionales de cumplimiento, en cuanto no hacen parte de los requerimientos evaluados por el área funcional SERTIC.

[15] 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.

	incrementar los costos de vigilancia y control entre los diferentes agentes involucrados.	verificación (política de gestión de riesgos, política de gestión de incidentes, procedimientos, etc.)	
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	✓✓✓	✓✓✓	✓✓✓	**3**

	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.	
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)

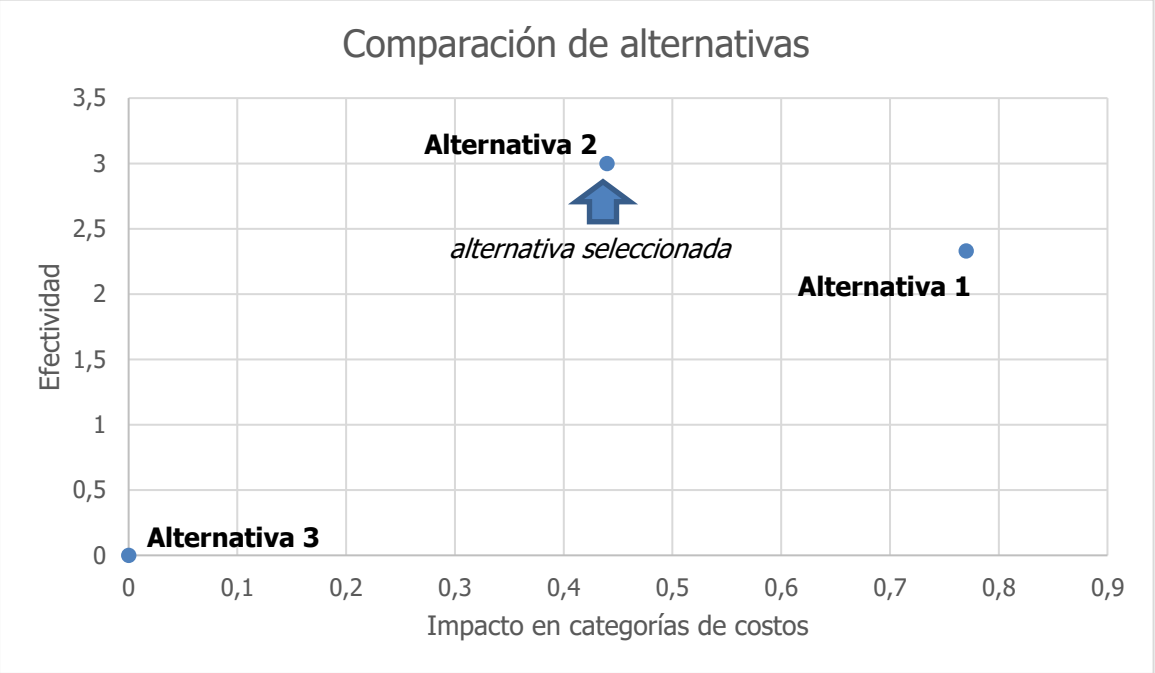
Respecto a la valoración de las características de costo de las diferentes alternativas, se asigna un puntaje de 1 a 3 dependiendo del nivel de impacto en las diferentes categorías de costos para las múltiples partes interesadas, cada valoración es ponderada con un peso proporcional (11,11%), por lo 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	- El artículo propuesto en la Alternativa 2 incorpora el	- El marco normativo vigente al que hace referencia la

	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.	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.	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 encuentra acotado 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 categorías asociadas a la "Integridad del servicio" por	La alternativa 2 limita el tiempo de almacenamiento de registros a 12 meses y acota las categorías del estándar ISO 27035-1, por lo cual se estima	No se evidencian actividades de mantenimiento de registros asociadas al marco actual.

	lo que las actividades asociadas al mantenimiento de registros podrían tener un impacto moderado en esta categoría de costo.	que las actividades asociadas al mantenimiento de registros podrían ser menores respecto a la alternativa 1.	
Vigilancia y control	✗	✗	-
	Se esperan costos bajos de vigilancia y control en cuanto se trata de un marco de referencia con vigilancia solo documental de los principales elementos de diseño e implementación	Se esperan costos bajos de vigilancia y control en cuanto se trata de un marco de referencia con vigilancia solo documental de los principales elementos de diseño e implementación	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	**0.77**	**0.44**	**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 fuera 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, 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 las 24 horas hábiles 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	- El marco regulatorio actual no permite análisis estadístico de la información de incidentes	- El marco regulatorio vigente no permite la categorización de la información de incidentes de seguridad de la información.	**0.0**

	comunicaciones y las autoridades	de seguridad de la información.		

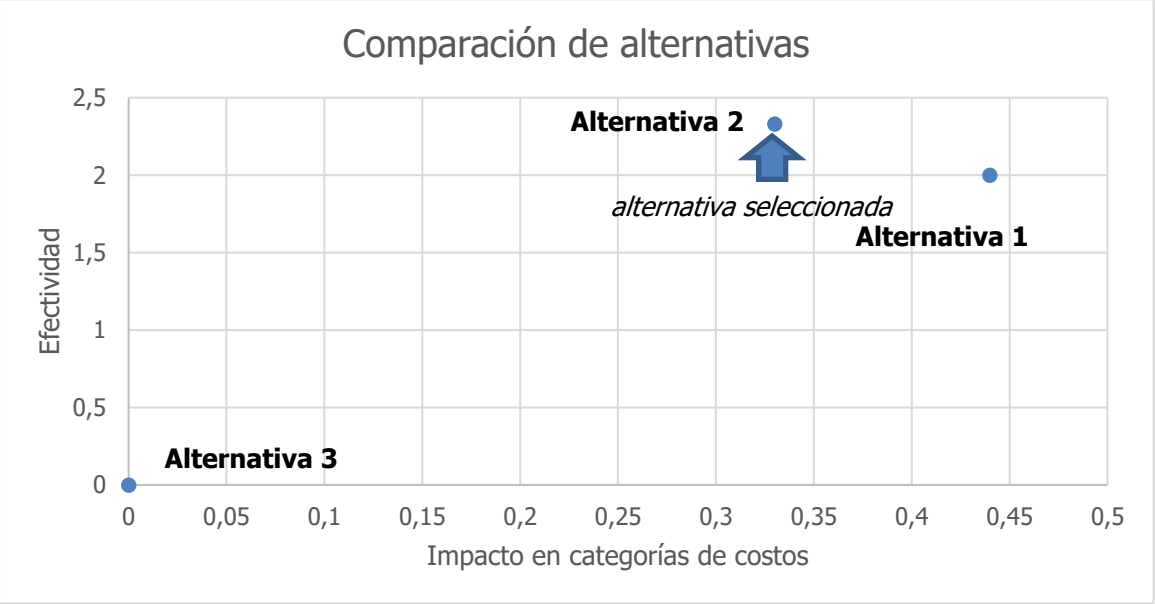
A3.4 Análisis de costos (Reporte a autoridades).

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	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	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

	sistemas de correo electrónico con cifrado PGP	correo electrónico con cifrado PGP	
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.	El reporte estará sujeto a verificación documental por parte de vigilancia y control, lo que se espera que tenga costos bajos para esta categoría.	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 diferencia la severidad del incidente, y pone un límite de tiempo únicamente para los incidentes más graves. Adicionalmente, para los casos con limite de tiempo 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, estos elementos reducen los costos asociados respecto a la Alternativa 1.	No se evidencian costos por retrasos asociados al marco normativo vigente (alternativa 3).
Resultado	**0.44**	**0.33**	**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.