RESOLUCIÓN No. DE 2018

"Por la cual se modifica el artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones"

LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES

En ejercicio de sus facultades legales, especialmente las conferidas por la Ley 1341 de 2009, y

CONSIDERANDO

Que de conformidad con lo dispuesto en el artículo 4 de la Ley 1341 de 2009, es función del Estado intervenir en el sector de las Tecnologías de la Información y las Comunicaciones -TIC-, para promover condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red, así como la seguridad informática y de redes.

Que este mismo artículo, señala que la intervención del Estado en el sector de las TIC, tiene como una de sus finalidades proteger los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de los servicios.

Que de conformidad con lo dispuesto en el numeral 3 del artículo 22 de la Ley 1341 de 2009, por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones, la Comisión de Regulación de Comunicaciones 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, la cual, le es aplicable a todos los proveedores de redes y servicios de telecomunicaciones.

Que el artículo 53 de la Ley 1341 de 2009 en su numeral 9, entre otros, consagra el derecho de los usuarios a *"recibir protección en cuanto a su información personal, y que le sea garantizada la inviolabilidad y el secreto de las comunicaciones y protección contra la publicidad indebida, en el marco de la Constitución Política y la Ley".*

Que las anteriores disposiciones guardan armonía con las normas expedidas en el marco de la Comunidad Andina de Naciones, en particular la Decisión 638 de 2006 que obliga a garantizar el derecho de los usuarios a *"la privacidad e inviolabilidad de sus telecomunicaciones, así como al mantenimiento de la reserva de todos los datos personales vinculados al servicio adquirido y que han sido suministrados a terceros, salvo en los supuestos de excepción que prevea su normativa interna".*

Que el Título II de la Resolución CRC 5050 de 2016, *"Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones",* establece en el Capítulo 1 como uno de los derechos de los usuarios el de recibir protección de la información que cursa a través de la red del operador, quien debe garantizar la inviolabilidad de las comunicaciones.

Que el Título V de la Resolución CRC 5050 de 2016, *"Régimen de Calidad para los Servicios de Comunicaciones",* contempla en el Capítulo 1 disposiciones en materia de seguridad de redes, según

el marco de referencia de seguridad de la UIT establecido en las recomendaciones de la serie UIT-T X.800, con el fin de garantizar la seguridad de las redes, la integridad de los servicios, y evitar la interceptación, interrupción, e interferencia en la prestación de los servicios.

Que la Organización para la Cooperación y el Desarrollo Económico (OCDE), desarrolló en 2015 la recomendación *"Digital Security Risk Management for Economic and Social Prosperity"*[1] donde plantea que, para aprovechar los beneficios asociados con el entorno digital, las partes interesadas deben apartarse de abordar la seguridad digital únicamente desde una perspectiva técnica aislada y deben integrar la gestión de riesgos digitales en su proceso de toma de decisiones económicas y sociales.

Que el Documento CONPES 3854 de 2016 estableció la Política Nacional de Seguridad Digital, donde se reconoce plenamente la recomendación mencionada, y se establecen lineamientos y planes de acción para 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, considerando la protección del entorno digital como un factor de importancia para preservar la seguridad de la Nación y su economía.

Que el citado CONPES 3854 de 2016 definió en su plan de acción que la CRC debía realizar una revisión del marco normativo del sector TIC en materia de seguridad de las comunicaciones, en el marco de sus competencias, para apoyar el objetivo de crear las condiciones para que las múltiples partes interesadas gestionen los riesgos de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, en atención a lo cual la CRC incluyó dentro de su Agenda Regulatoria 2017-2018 el proyecto denominado *"Revisión del marco regulatorio para la gestión de riesgos de seguridad digital"*.

Que tomando como insumo los elementos antes expuestos, así como la adopción de mejores prácticas internacionales en gestión de riesgos de seguridad digital, y el estado actual de las redes de los Proveedores de Redes y Servicios de Telecomunicaciones, esta Comisión identificó la necesidad de adaptar la regulación a las mejores prácticas en gestión de riesgos de seguridad de la información, por lo que se requiere la modificación de las disposiciones relacionadas con la seguridad de redes en el Capítulo 1 del Título V de la Resolución CRC 5050 de 2016.

Que la CRC, en cumplimiento de lo establecido en el artículo 2.2.13.3.2 del Decreto 1078 de 2015, publicó la propuesta regulatoria contenida en el documento denominado *"Revisión del marco regulatorio para la gestión de riesgos de seguridad digital"* así como el proyecto de resolución, "*Por el cual se modifica el artículo 5.1.2.3 del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones",* para comentarios de los diferentes agentes interesados durante el lapso comprendido entre el 24 de noviembre y el 19 de diciembre de 2017.

Que en el desarrollo de la mencionada propuesta regulatoria, esta Comisión generó espacios de discusión adicionales con las múltiples partes interesadas a través de mesas de trabajo[2] donde se discutieron las temáticas objeto de comentarios, y fueron escuchadas las diferentes posturas y propuestas de los operadores y agentes del sector.

Que mediante la Ley 170 de 1994[3], Colombia se adhirió a la Organización Mundial del Comercio, y teniendo en cuenta que dicha organización ha escogido a la ISO (International Standard Organization) como la entidad internacional responsable de la estandarización de normas técnicas y que para el caso de la electrotecnia, la ISO cuenta con la IEC (International Electrotechnical Commission), la cual ha desarrollado la familia de estándares ISO/IEC 27000 dentro de la categoría de Tecnologías de la Información, para establecer una serie de mejores prácticas internacionales para la adecuada gestión de los activos de información a través de Sistemas de Gestión de Seguridad de la Información.

---

1 OCDE. (2015). *Digital Security Risk Management for Economic and Social Prosperity.* Recuperado de http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

2 Se efectuaron tres mesas de trabajo (2 de febrero de 2018, 8 de febrero de 2018, y 15 de febrero de 2018) con la participación de: Colombia Telecomunicaciones S.A. E.S.P., Empresa de Telecomunicaciones de Bogotá S.A. E.S.P., Colombia Móvil S.A. E.S.P., Virgin Mobile Colombia S.A.S., Comunicación Celular Comcel S.A., DIRECTV Colombia Ltda., CCIT-NAP Colombia, IFX Networks Colombia, Fundación Karisma, Jeimy J. Cano M., MINTIC, colCERT, y Presidencia de la Republica.

3 *"Por medio de la cual se aprueba el Acuerdo por el que se establece la "Organización Mundial de Comercio (OMC)", suscrito en Marrakech (Marruecos) el 15 de abril de 1994, sus acuerdos multilaterales anexos y el Acuerdo Plurilateral anexo sobre la Carne de Bovino"*

Que dentro de los estudios realizados en el desarrollo de esta propuesta, se identificó el potencial que la implementación de Sistemas de Gestión de Seguridad de la Información, como los descritos en el estándar ISO/IEC 27001, tienen para mejorar las capacidades de gestión de Seguridad Digital de las múltiples partes interesadas.

Que la implementación de dichos Sistemas de Gestión de Seguridad de la Información puede darse en un marco de autorregulación, donde los proveedores de servicios de comunicaciones desarrollen políticas de gestión de seguridad de la información, de acuerdo con su contexto específico de operación y vulnerabilidades, siguiendo para ello un estándar reconocido como mejor práctica internacional.

Que esta aproximación permite a las múltiples partes interesadas la flexibilidad y adaptabilidad requeridas en campos del conocimiento con un alto grado de innovación como lo es el de la seguridad digital, y que la misma requiere de sistemas y procesos efectivos de transparencia.

Que tomando como insumo los elementos antes expuestos, los estudios realizados, y ejerciendo la función otorgada por el legislador a esta Comisión en el numeral 19 de artículo 22 de la Ley 1341 de 2009, se identificó la necesidad de contar con información estadística sobre la frecuencia de los Incidentes de Seguridad de la Información, su impacto y causas, para brindar el nivel de transparencia requerido para monitorear la implementación de los sistemas de gestión de seguridad de la información, para el desarrollo de otras políticas públicas y regulatorias de seguridad digital basadas en hechos, y para permitir a las autoridades nacionales encargadas de la ciberseguridad y ciberdefensa los niveles de coordinación y asesoría previstos en el CONPES 3854 de 2016.

Que a efectos de surtir el trámite de abogacía de la competencia ante la Superintendencia de Industria y Comercio, la CRC remitió[4] a dicha Entidad el contenido de la propuesta regulatoria, su respectivo documento soporte, el cuestionario al que hace referencia la Resolución número 44649 de 2010 y los comentarios recibidos de los agentes interesados.

Que una vez atendidas las observaciones recibidas durante todo el proceso de discusión del presente proyecto, se elaboró el documento que contiene las razones por las cuales se aceptan o rechazan los planteamientos expuestos, el cual fue puesto a consideración del Comité de Comisionados de la Entidad y fue aprobado mediante Acta No. XX del XX de XX de 2018, y posteriormente presentado y aprobado por los miembros de la Sesión de Comisión el XX de XX de 2018 según consta en el Acta No. XX.

En virtud de lo expuesto,

RESUELVE

ARTÍCULO 1. DEFINICIONES. Adicionar al Título I de la Resolución CRC 5050 de 2016, las siguientes definiciones:

*"**Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.*

***Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.*

***Sistema de Gestión de Seguridad de la Información:** parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información."*

[4] Mediante radicado número XXX del X de XX de 2018.

ARTÍCULO 2. GESTIÓN DE SEGURIDAD EN REDES DE TELECOMUNICACIONES. Modificar el artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016, por las razones expuestas en la parte motiva de la presente resolución, el cual quedará así:

*"**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.

***5.1.2.3.2. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.** Los proveedores de servicios de telecomunicaciones deberán identificar, almacenar como mínimo 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 externos 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)*

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 los 120 minutos subsecuentes a la detección del incidente, con la información disponible al momento del reporte.

De manera voluntaria los proveedores de redes y servicios de comunicaciones podrán entregar información adicional requerida por colCERT para la gestión del incidente."

ARTÍCULO 3. CLASIFICACIÓN DE SEVERIDAD DE LOS INCIDENTES. Adicionar el Anexo 5.8 a la Resolución CRC 5050 de 2016, el cual quedará así:

"ANEXO 5.8 CLASIFICACIÓN DE SEVERIDAD DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad de la información deberán considerar los siguientes factores para la clasificación de la severidad de incidentes de seguridad de la Información:

1) Importancia del sistema de información.
2) Pérdida de negocio.
3) Impacto social.

Esto de acuerdo con lo dispuesto en el estándar ISO/IEC 27035-2 (2016) en su anexo C y aquellas versiones posteriores de la misma:

*Muy Serios (**Clase IV**)*

Incidentes muy serios son aquellos que:
- *actuan en sistemas de información especialmente importantes, y*
- *resultan en pérdidas de negocio especialmente grave, o*
- *conducen a pérdidas sociales especialmente importantes*

*Serio (**Clase III**)*

Los incidentes serios son aquellos que:
- *actuan sobre sistemas de información especialmente importantes o sistemas de información importantes, y*
- *resultan en una pérdida negocio grave, o*
- *conducen a un impacto social importante.*

*Menos serios (**Clase II**)*

Incidentes menos serios son aquellos que:
- *actuan sobre sistemas de información importantes o sistemas de información ordinarios, y*
- *resultan en una pérdida de negocio considerable, o*
- *conducen a un impacto social considerable.*

*Pequeño (**Clase I**)*

Incidentes pequeños son aquellos que:
- *actuan sobre los sistemas de información ordinarios importantes y*
- *resultan en una pérdida de negocio menor o ninguna pérdida comercial, o*
- *provocan un impacto social menor o ningún impacto social*
- *Generalmente hay consecuencias insignificantes o ninguna y no se requiere ninguna acción.*

Fuente: Anexo C - Estándar ISO/IEC 27035-2:2016

***Importancia del sistema de información:** La importancia de los sistemas de información afectados por los incidentes de seguridad de la información se determina considerando la relevancia de las operaciones comerciales de la organización respaldadas por los sistemas de información. La importancia podría expresarse en relación con la seguridad nacional, el orden social, el desarrollo económico y el interés público, y la dependencia del negocio en los sistemas de información. Este enfoque clasifica la importancia del sistema de información en tres grandes niveles: sistema de información especialmente importante, sistema de información importante y sistema de información ordinario*

***Pérdida de Negocio o Pérdida Comercial**: Es la pérdida de negocios de la organización causada por incidentes de seguridad de la información, esta se determina considerando la gravedad del impacto de la interrupción del negocio debido al daño del hardware, software, funciones y datos de los sistemas de información. La gravedad del impacto puede depender del costo de recuperación del negocio a niveles de operación normales u otros efectos negativos de los incidentes de seguridad de la información, incluidas la pérdida de beneficios o*

costos de oportunidad. Este enfoque clasifica la pérdida de negocios en cuatro grandes niveles:

a) *Pérdida de negocio especialmente grave significaría parálisis generalizada de la empresa, al punto de perder la capacidad de operación empresarial, o daños muy graves a la confidencialidad, la integridad y la disponibilidad de datos comerciales importantes. Significaría un costo enorme de recuperación del negocio niveles normales y de eliminación de los efectos negativos. Una organización no podría soportar este nivel de pérdida de negocio.*

b) *Pérdida de negocio grave significaría la interrupción de las operaciones comerciales durante un período prolongado o una parálisis comercial localizada capaz de influir seriamente en la capacidad comercial o un daño grave a la confidencialidad, integridad y disponibilidad de los datos comerciales importantes. Significaría un alto costo de recuperación de negocio a niveles normales y de eliminación de los efectos negativos. Una organización podría soportar este nivel de pérdida comercial.*

c) *Pérdida de negocio considerable significaría la interrupción de las operaciones comerciales hasta el punto de influir considerablemente en la capacidad comercial o un daño considerable a la confidencialidad, integridad y disponibilidad de datos comerciales importantes. Significaría un costo considerable para recuperar el funcionamiento normal del negocio y eliminar los efectos negativos. Una organización podría soportar completamente este nivel de pérdida comercial.*

d) *Pérdida comercial menor significaría la interrupción de las operaciones comerciales por un corto período de tiempo en la medida en que influya en la capacidad comercial o un impacto menor en la confidencialidad, integridad y disponibilidad de datos comerciales importantes. Significaría un costo menor para recuperar el negocio a la operación normal y eliminar los efectos negativos.*

Impacto social: *Es el impacto en la sociedad causado por incidentes de seguridad de la información, se determina considerando la escala y el grado del impacto en la seguridad nacional, el orden social, el desarrollo económico y el interés público. Este enfoque clasifica el impacto social en cuatro niveles:*

a) *Impacto social especialmente importante es aquel que implicaría efectos adversos que abarcarán la mayoría de las áreas de uno o más departamentos o provincias, amenazando en gran medida la seguridad nacional, causando disturbios sociales, generando consecuencias extremadamente adversas para el desarrollo económico y/o dañando gravemente el interés público.*

b) *Impacto social importante es aquel que implicaría efectos adversos que abarcarán la mayoría de las áreas de una o más ciudades, amenazando la seguridad nacional, causando pánico social, produciendo consecuencias adversas significativas en el desarrollo económico y/o perjudicando el interés público.*

c) *Impacto social considerable es aquel que implicaría efectos adversos que abarcarían áreas parciales de una o más ciudades, con una amenaza limitada para la seguridad nacional, con alguna perturbación del orden social, con consecuencias adversas para el desarrollo económico o que influyen en el interés público.*

d) *Impacto social menor es aquel que significaría efectos adversos en un área parcial de una ciudad y pocas posibilidades de amenazar la seguridad nacional, el orden social, el desarrollo económico y el público."*

ARTÍCULO 4. **SEGUIMIENTO A GESTIÓN DE INCIDENTES.** Los proveedores de servicios de comunicaciones deberán remitir a la CRC antes del 31 de enero de 2020, la información sobre

incidentes de seguridad, correspondiente al periodo comprendido entre el 1º de enero y el 31 de diciembre de 2019, de acuerdo con lo definido en el numeral 5.1.2.3.2 del artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016.

ARTÍCULO 5. VIGENCIA Y DEROGATORIA. La presente Resolución rige en su totalidad a partir de la fecha de su publicación en el Diario oficial, con excepción de la modificación realizada al numeral 5.1.2.3.1 del artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016 la cual entrará en vigencia doce meses después de su publicación.

Dada en Bogotá D.C. a los

PUBLÍQUESE Y CÚMPLASE

XXX
Presidente

GERMÁN DARÍO ARIAS PIMIENTA
Director Ejecutivo

C.C. 30/10/2017 Acta 1124
C.C. 27/04/2018 Acta 1150
S.C. XX/XX/2018 Acta XX

Revisado por: Coordinación de Capital Intelectual