RESOLUCIÓN No. DE 2017

"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 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 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 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 el Título II de la Resolución CRC 5050 de 2016, *"Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones",* que entrará en vigencia el 1° de enero de 2018, establece en el Capítulo 1 como uno de los derechos de los usuarios el de recibir protección de la información que cursa a través de la red del operador, quien debe garantizar la inviolabilidad de las comunicaciones.

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 reconoce plenamente la recomendación mencionada, y establece 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 que la protección del entorno digital es un factor de trascendente 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, 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 del sector de Tecnologías de la Información y las Comunicaciones, 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 en el marco de lo anterior, los estudios realizados identificaron el potencial de adoptar la implementación de sistemas de gestión de seguridad de la información de acuerdo con las definiciones en la recomendación UIT-T X.1051 para mejorar las capacidades de gestión de la información según las mejores prácticas internacionales de riesgos de seguridad digital.

Que los estudios realizados identificaron la necesidad de contar con información estadística sobre los incidentes de seguridad, su impacto y causas, tanto para el desarrollo de políticas regulatorias basadas en hechos, como para permitir a las autoridades nacionales encargadas de la ciberseguridad y ciberdefensa, la coordinación y asesoría necesarias frente a incidentes de seguridad digital.

Que la CRC, en cumplimiento de lo establecido en el artículo 2.2.13.3.2 del Decreto 1078 de 2015, publicó el 24 de noviembre de 2017 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.

Que a efectos de surtir el trámite de abogacía de la competencia ante la Superintendencia de Industria y Comercio, la CRC mediante radicado número XXX del X de XX de 2017 remitió a dicha Entidad el contenido de la propuesta regulatoria, su respectivo documento soporte, el cuestionario al que hace referencia la Resolución número 44649 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

[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

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 2017, y posteriormente presentado y aprobado por los miembros de la Sesión de Comisión el XX de XX de 2017, 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:

*"**Incidente de seguridad:** una violación de la seguridad o una pérdida de integridad que podría tener un impacto en la operación de redes y servicios de telecomunicaciones electrónicas*

***Integridad del servicio:** capacidad de un servicio para cumplir sus objetivos sin degradaciones excesivas, una vez obtenido. La integridad del servicio está determinada principalmente por las características de transmisión de la red."*

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, el cual quedará de la siguiente manera:

*"**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 (UIT-T 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.

***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)	*1h-2h*	*2h-4h*	*4h-6h*	*6h-8h*	*>8h*

Usuarios afectados					
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.

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."*

ARTÍCULO 3. **SEGUIMIENTO A GESTIÓN DE INCIDENTES.** Los proveedores de servicios de internet y telefonía deberán remitir a la CRC antes del 31 de enero de 2019, la información sobre incidentes de seguridad, correspondiente al periodo comprendido entre el 1º de enero y el 31 de diciembre de 2018, 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 4. 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 el 1º de enero de 2019. Esta Resolución deroga las disposiciones que le sean contrarias.

Dada en Bogotá D.C. a los

PUBLÍQUESE Y CÚMPLASE

XXXXXXXX
Presidente

GERMÁN DARÍO ARIAS PIMIENTA
Director Ejecutivo

C.C. 30/10/2017 Acta 1124
S.C. XX/XX/2017 Acta XX

Revisado por: Coordinación de Capital Intelectual
Elaborado por: