CRC
Comisión de Regulación de Comunicaciones
República de Colombia

REPÚBLICA DE COLOMBIA

RESOLUCIÓN No. 2258 DE 2009

"Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007"

LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES

En ejercicio de sus facultades legales y en especial las conferidas por los artículos 4 y 55 de la Ley 1341 de 2009, y

CONSIDERANDO

Que los artículos 22 y 23 de la Resolución CRT 1732 de 2007, por la cual se adoptó el *Régimen de Protección de los Derechos de los Suscriptores y/o Usuarios de los Servicios de Telecomunicaciones*, establecieron las características generales que se deben cumplir para la seguridad de los datos e informaciones y la inviolabilidad de las comunicaciones.

Que los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007, *Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones,* establecieron las características generales para garantizar la seguridad de la red y la integridad de los servicios.

Que la Ley 1341 de 2009 determinó el marco general del sector de las Tecnologías de la Información y las Comunicaciones (en adelante TIC), que incluye, entre otros aspectos, la protección al usuario, la calidad del servicio y las potestades del Estado en relación con la regulación de redes y servicios.

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 para el desarrollo de dicho sector.

Que el artículo 4° de la Ley 1341 antes referido, 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 el artículo 53 de la Ley 1341 de 2009 consagra el derecho de los usuarios a "[r]*ecibir protección en cuanto a su información personal, y que le sea garantizada la inviolabilidad y el secreto de las comunicaciones y protección contra la publicidad indebida, en el marco de la*

Constitución Política y la Ley", y que la CRC es el organismo competente para expedir la regulación en materia de protección al usuario en lo que se refiere a servicios de comunicaciones.

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 "[l]*a 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 la protección del ciberespacio es un factor de trascendente importancia para preservar la seguridad de la nación y su economía, y que para avanzar en este objetivo, se requiere de un marco regulatorio que asegure la protección de los aspectos vulnerables de la infraestructura de la información que se adapte a las necesidades del entorno. En tal sentido, los estudios desarrollados por la CRC recomiendan adoptar medidas complementarias a las dispuestas en las Resoluciones CRT 1732 y 1740 de 2007, con el propósito de establecer condiciones asociadas a la inviolabilidad de las comunicaciones y la seguridad de los datos e informaciones, garantizar la seguridad de la red así como la integridad de los servicios.

Que los estudios antes mencionados han tenido en cuenta lo dispuesto en los tratados internacionales adoptados en el marco de la Asamblea General de la Naciones Unidas, en particular la Resolución 55/63 sobre "Lucha contra la Utilización de la Tecnología de la Información con Fines Delictivos" y la Resolución 56/121, relativa a la "Lucha contra la Utilización de la Tecnología de la Información con fines Delictivos", así como también los trabajos realizados por el Comité Interamericano contra el Terrorismo (CICTE), plasmados en la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, que se adoptó para cumplir con lo encomendado por la Asamblea General de Organización de los Estados Americanos en su Resolución AG/RES.1939 (XXXIII-O/03)] "Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética".

Que la CRC, en cumplimiento de lo establecido en el Decreto 2696 de 2004, publicó el 2 de octubre de 2009 la propuesta regulatoria contenida en el documento denominado "*Aspectos regulatorios asociados a la Ciberseguridad*" así como el proyecto de resolución "*Por la cual se modifica los artículos 22 y 23 de la Resolución 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución 1740 de 2007*", para comentarios de los diferentes agentes interesados.

Que en atención a lo anterior, se recibieron comentarios a la propuesta regulatoria dentro del plazo definido para tales efecto de diversos agentes los cuales fueron revisados y analizados por la CRC, tal como consta en el "*Documento de Respuesta a comentarios del sector realizados al proyecto de resolución "Por la cual se modifica los artículos 22 y 23 de la Resolución 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución 1740 de 2007*", el cual, en cumplimiento del Decreto 2696 de 2004, una vez finalizado el plazo definido por la CRC para recibir comentarios del sector, fue elaborado y posteriormente, aprobado por el Comité de Expertos Comisionados tal como costa en el Acta 693 del 18 de diciembre de 2009.

Que el documento mencionado en el considerando anterior fue presentado a los miembros de la Sesión de Comisión el 21 de diciembre de 2009.

En virtud de lo expuesto,

RESUELVE

ARTÍCULO 1º. Adicionar al artículo 1.8 de la Resolución CRT 1740 de 2007, las siguientes definiciones:

"

7. ***Autenticación:*** *Proceso destinado a permitir al sistema asegurar la identificación de una parte.*

8. ***Autorización**: Proceso de atribución de derechos o concesión de permisos para realizar determinadas actividades y su relación con determinados procesos, entidades, personas jurídicas o naturales.*

9. ***Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.*

10. ***Ciberseguridad**: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.*

11. ***Confidencialidad de datos:** Impedir que los datos sean divulgados sin autorización.*

12. ***Disponibilidad:** Acceso por parte de una entidad autorizada a la información y sistemas informáticos, cuando esta entidad lo requiera.*

13. ***Entidad**: Persona natural o jurídica, organización, elemento perteneciente a un equipo o a un programa informático.*

14. ***Infraestructura crítica**: Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación.*

15. ***Integridad de datos:** Propiedad o característica de mantener la exactitud y completitud de la información.*

16. ***Interceptación**: Es la adquisición, visualización, captura o copia de contenido, datos o parte de contenido de una comunicación transmitida por medio alámbrico, electrónico, óptico, magnético, u otras formas, realizada durante la transmisión, utilizando medios electrónicos, mecánicos, ópticos o electromagnéticos.*

17. ***Interferencia**: Es la acción de bloquear, ocultar, impedir o interrumpir la confidencialidad, la integridad de programas computacionales, sistemas computacionales, datos o información, mediante la transmisión, daño, borrado, destrucción, alteración o supresión de datos, de programas de computación o tráfico de datos.*

18. ***Interrupción**: Es el evento causado por un programa computacional, una red de telecomunicaciones o sistema computacional que interfiere o destruye un programa computacional, una red de telecomunicaciones, datos e información que esta contenga.*

19. ***No repudio:** Servicio que tiene como objetivo garantizar la disponibilidad de pruebas que pueden presentarse a terceros y utilizarse para demostrar que un determinado evento o acción ha tenido lugar, con el propósito de evitar que una persona o una entidad niegue haber realizado una acción de tratamiento de datos, proporcionando prueba de dichas acciones en la red.*

20. ***Pharming**: Es la acción de modificar el servidor (DNS) Domain Name System, cambiando la dirección IP correcta por otra, de tal manera que haga entrar al usuario a una IP diferente con la creencia de que accede a un sitio personal, comercial o de confianza.*

21. ***Phishing:** Acto de enviar un correo electrónico cuyo objeto es engañar al usuario dirigiéndolo a una pagina Web falsa y por este medio, obtener de éste, información privada que será utilizada para fines no autorizados o ilícitos como el robo de identidad y de contraseñas.*

22. ***Software Malicioso (Malware):** Es un programa computacional que es insertado en un computador o sistema computacional sin autorización, con el objeto de comprometer la confidencialidad e integridad del sistema computacional, de la red de telecomunicaciones, datos y del tráfico de datos. Esta clase de programa se presenta en forma de virus, gusanos, y Troyanos electrónicos y demás, que se pueden distribuir a través de email, Web site, Shareware o freeware.*

CLO.

23. ***Vulnerabilidad:*** *Cualquier debilidad que pudiera explotarse con el fin de violar un sistema o de la información que contiene."*

ARTÍCULO 2º. Modificar el artículo 2.4 de la Resolución CRT 1740 de 2007, el cual quedará así:

*"**ARTÍCULO 2.4. SEGURIDAD DE LA RED.** Los proveedores de redes y/o 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/o 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. Tampoco cubre los servicios ofrecidos por proveedores de contenidos o de cualquier tipo de aplicación, a quienes corresponde 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/o 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 que respecta 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 aquel 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 señala o informa 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/o 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

CLO.

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."

ARTÍCULO 3º. Modificar el artículo 22 de la Resolución CRT 1732 de 2007, el cual quedará así:

"ARTÍCULO 22. INVIOLABILIDAD DE LAS COMUNICACIONES. *Los proveedores de redes y/o servicios de telecomunicaciones, deben asegurar los principios (confidencialidad, integridad y disponibilidad) y servicios de seguridad (autenticación, autorización y no repudio) de la información, requeridos para garantizar la inviolabilidad de las comunicaciones, la información que se curse a través de ellas y los datos personales de los suscriptores y/o usuarios, en lo referente a las redes y/o servicios suministrados por dichos operadores. Corresponderá a los proveedores de acceso a Internet tomar tales medidas en relación con las redes y los servicios suministrados por ellos, y en consecuencia no les serán exigibles medidas relacionadas con contenidos, servicios y aplicaciones provistos por otros proveedores. El secreto de las telecomunicaciones se extiende a las comunicaciones de voz, datos, sonidos o imágenes y a la divulgación o utilización no autorizada de la existencia o contenido de las mismas.*

Salvo orden emitida de forma expresa y escrita por autoridad judicial competente, los proveedores de redes y/o servicios de telecomunicaciones, siempre y cuando sea técnicamente factible, no pueden permitir, por acción u omisión, la interceptación, violación o repudio de las comunicaciones que cursen por sus redes. Si la violación proviene de un tercero, y el proveedor de redes y/o servicios de telecomunicaciones tiene conocimiento de dicha violación, debe tomar de inmediato las medidas necesarias para que la conducta cese y denunciar ante las autoridades competentes la presunta violación. Para ello, deberán implementar procesos formales de tratamiento de incidentes de seguridad de la información propios de la gestión de seguridad del proveedor."

ARTÍCULO 4º. Modificar el artículo 23 de la Resolución CRT 1732 de 2007, el cual quedará así:

"ARTÍCULO 23. SEGURIDAD DE LOS DATOS E INFORMACIONES. *Los proveedores de redes y/o servicios de telecomunicaciones, adoptarán mecanismos que garanticen el manejo confidencial, la integridad y disponibilidad de los datos de los suscriptores y/o usuarios, los cuales sólo pueden ser intercambiados con otros proveedores para efectos de la prevención y control de fraudes en las telecomunicaciones y el cumplimiento de las obligaciones regulatorias que así lo exijan.*

Los datos suministrados por los suscriptores y/o usuarios para efectos de la adquisición de servicios o la atención de peticiones, no pueden ser usados por los proveedores de redes y/o servicios de telecomunicaciones para la elaboración de bases de datos con fines comerciales o publicitarios, distintos a los directamente relacionados con los servicios ofrecidos por el operador, salvo que medie autorización expresa y escrita del suscriptor y/o usuario.

PARÁGRAFO. *Los proveedores de redes y/o servicios de telecomunicaciones no tienen la obligación ni asumen responsabilidad en la identificación del tipo de información que cursa por sus redes, en los términos de los diferentes tipos de datos previstos en la Ley 1266 de 2008."*

ARTÍCULO 5º. VIGENCIA. La presente resolución rige a partir de su publicación en el Diario Oficial, modifica en lo pertinente los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007 y deroga todas aquéllas disposiciones que le sean contrarias.

CLO.

ARTÍCULO 6º. PLAZO DE IMPLEMENTACIÓN. Los proveedores de redes y/o servicios de telecomunicaciones deberán dar aplicación a lo dispuesto en los artículos 2º, 3º y 4º de la presente resolución a partir del primero (1°) de julio de 2010, fecha en la cual deberán remitir a la CRC un informe en el que se especifique el detalle de las medidas adoptadas en cumplimiento de la misma.

PUBLÍQUESE Y CÚMPLASE

MARIA DEL ROSARIO GUERRA DE LA ESPRIELLA
Presidente

CRISTHIAN LIZCANO ORTIZ
Director Ejecutivo

NS/RDD/DAB
CE 18/12/09. Acta 693
SC 21/12/09. Acta 220