Comisión de Regulación de Comunicaciones
República de Colombia

CRC
Radicación : *2010051564*
Fecha : 28/05/2010 - 15:08:44
Proceso : 4000 ATENCION CLIENTE Y RE... EXTERNAS
Destino : DNP - JUAN CAMILO GRANADOS
Asunto : COMENTARIOS PREBORRADO... CONPES- CIBERDEFENSA Y CIBERSEGURIDAD
CERTIFICADO ISO 9001 SC 1390-1
049-1

Cod. 4000
Rad. Mail 013552
Bogotá D.C.,

Doctor
JUAN CAMILO GRANADOS
Subdirector de Telecomunicaciones
DEPARTAMENTO NACIONAL DE PLANEACIÓN
Calle 26 # 13 - 19 - Edificio Fonade
Conmutador: (57+1) 381 50 00
Bogotá D.C.

Asunto: Comentarios al documento Preborrador – CONPES *"Lineamientos De Política para el desarrollo e impulso de la Ciberdefensa y la Ciberseguridad en Colombia"*

Respetado Doctor Granados:

De conformidad con la invitación efectuada a la Comisión de Regulación de Comunicaciones para presentar comentarios respecto del documento citado en la referencia, el presente escrito tiene por objeto exponer las inquietudes y consideraciones por parte de la CRC con relación al mismo, en su calidad de organismo regulador técnico del sector de Tecnologías de la Información y las Comunicaciones –TIC-.

DNP Rad No: 2010-663-020806-2
Fecha Rad.:03/06/2010 02:34:53 p.m. Us Rad: JTRIANA
Asunto :REMITRE COMENTARIOS AL DOCUMENTO PREBORRADOR CONPES
Destino :SUBDIRECCION DE TELECOMUNICACIONES

1. Sobre los Antecedentes del documento

Dentro de los antecedentes del documento se hace mención a la normatividad nacional vigente sobre seguridad de la información. En este contexto, la CRC estima pertinente la inclusión de la Resolución CRC 2258 de 2009, en donde se modifican los siguientes artículos:

- 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*, el cual establece las características generales que se deben cumplir para la seguridad de los datos e informaciones y la inviolabilidad de las comunicaciones.

- 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*, en donde se establecieron las características generales para garantizar la seguridad de la red y la integridad de los servicios.

Dentro de los principales objetivos de la Resolución CRC 2258 de 2009, se encuentra la obligación por parte de los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de 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.

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 seis aspectos:

1) Autenticación;
2) Acceso;
3) Servicio de No repudio;
4) Principio de Confidencialidad de datos;
5) Principio de Integridad de datos;
6) Principio de Disponibilidad;

En consecuencia, de manera atenta se solicita incluir dentro de los antecedentes del documento la existencia de la Resolución CRC 2258 de 2009.

2. Sobre el numeral *3. Debilidad en regulación y legislación* del capitulo *C. Ejes problemáticos* y el capitulo *VII. Recomendaciones*

Dentro del desarrollo del numeral *3, Debilidad en regulación y legislación* se indica lo siguiente:

> *"Se evidencia que **no existe una regulación adecuada** en cuanto al compromiso que deben tener todos los ISPs[1] con referencia a la preservación de logs[2] para que sirvan en determinado momento como prueba o contribuyan en las investigaciones de delitos informáticos." **NFT***

Dentro del capitulo VII Recomendaciones se señala lo siguiente:

> *"8. Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones **generar una normatividad que regule los periodos y condiciones mínimas para guardar los logs (historiales) de eventos para temas de investigación judicial** y fortalecimiento del sistema de verificación de datos en la asignación de licencias de operación y prestación de servicios. Esta normatividad deberá ser presentada a más tardar en el primer semestre de 2011." NFT*

Al respecto, la Comisión estima pertinente aclarar que la Resolución CRC 2258 de 2009, define en el artículo 20 lo siguiente:

> *"**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*

[1] Proveedores de servicios de internet (hoy en día en Colombia estos entes también brindan adicionalmente servicios de telefonía y televisión. Convirtiéndose de esta manera en unos prestadores de servicios integrales de telecomunicaciones).

[2] Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why, W5) un evento ocurre para un dispositivo en particular o aplicación.

integridad del servicio, para evitar la interceptación, interrupción, e interferencia del mismo...

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:*
...

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) NFT...***

Por otra parte, el artículo 3º de dicha Resolución precisa:

"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...*

...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."****NFT***

En consecuencia, la CRC de manera atenta recomienda profundizar al respecto en el análisis publicado e informar de manera específica sobre la existencia de una regulación asociada al servicio de No Repudio 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, de acuerdo a las recomendaciones de la UIT X.805 y X.813.

3. Sobre el capitulo *VII Recomendaciones*

Dentro de las recomendaciones descritas en el documento Pre-borrador CONPES se precisa la necesidad de creación de un Centro Nacional de Respuestas a Emergencias de Seguridad Informática por el Ministerio de Defensa Nacional y el Ministerio de Hacienda:

> ***"5. Encargar al Ministerio de Defensa Nacional la creación de un Centro Nacional de Respuesta a Emergencias de Seguridad Informática.*** *La creación de este centro no deberá superar los seis meses a la aprobación del presente documento."*

Respecto a lo anterior y teniendo en cuenta el capitulo 4° sobre infraestructuras criticas del estudio realizado por la Comisión de Regulación de Comunicaciones en el año 2008 "*Recomendaciones al Gobierno Nacional para la implementación de una Estrategia Nacional de Ciberseguridad", en donde* se elabora un primer ejercicio de identificación de las infraestructuras críticas del país, tomando como base del ejercicio las metodologías y políticas adoptadas en otros países pero adecuándolas a las condiciones del entorno colombiano, se concluye que existen como principales infraestructuras criticas en nuestro país, las del sector de telecomunicaciones, sector financiero, y sector de TI (Tecnologías de la información), a partir de las cuales se somete a consideración la creación de centros cuyo objetivo fundamental será el de compartir información acerca de las amenazas físicas y cibernéticos, vulnerabilidades, y eventos para ayudar a proteger la infraestructura crítica de nuestro país.

Con el objeto de proteger las infraestructuras críticas antes mencionadas, es necesario establecer un equipo de respuesta a incidentes CSIRT[3]. Estos centros reunirán información acerca de amenazas, vulnerabilidades y riesgos en la estructura física y del ciberespacio. Los miembros de este centro recibirán alertas en áreas específicas, las cuales contendrán las descripciones de las amenazas o vulnerabilidades, su nivel de gravedad y las posibles soluciones. Tras el análisis por expertos de la industria, las alertas serán entregadas a los participantes sobre la base de su nivel de servicio.

Por lo antes descrito, la CRC recomienda la creación de dos centros adicionales de respuestas a incidentes y emergencias de seguridad informática, el primero liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones, y el segundo por el Ministerio de Hacienda, en aras de proteger las Infraestructuras criticas de TIC y de los servicios financieros.

En tos términos expuestos se presentan los comentarios de la CRC sobre el Pre-Borrador CONPES de Ciberseguridad, esperando que los mismos contribuyan al análisis y la decisión que se adopte en beneficio de la seguridad de la información en Colombia.

Con un cordial saludo,

CRISTHIAN LIZCANO ORTIZ
Director Ejecutivo
Anexo: Resolución CRC 2258 de 2009
RDD

[3] Computer Security Incident Response Team (CSIRT)