

Bogotá D.C., 16 de marzo de 2018

Doctor
GERMÁN CASTRO FERREIRA
Director Ejecutivo
Comisión de Regulación de Energía y Gas - CREG
Ciudad

CREG 16 MAR 2018 16:06

Asunto: Respuesta como parte interesada al recurso de apelación interpuesto por ENERTOTAL S.A. E.S.P. contra el Acuerdo 1004 de 2017.

Respetado doctor Castro:

De manera atenta y como parte interesada en la actuación relacionada con el recurso de apelación interpuesto por Enertotal S.A. E.S.P. contra el Acuerdo 1004 de 2017, el cual, en cumplimiento de lo dispuesto por el artículo 37 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo fue comunicado el 27 de febrero de 2018 por la Comisión de Regulación de Energía y Gas al Consejo Nacional de Operación (radicado S-2018-000835), nos permitimos dar respuesta en los siguientes términos:

En primer lugar, se hará referencia a la competencia legal del CNO para la expedición de los acuerdos de operación, a continuación al mandato regulatorio en virtud del cual se expidieron los Acuerdos 701 de 2014, 1004 de 2017 y a los antecedentes de los acuerdos antes mencionados. Posteriormente se hará referencia a los elementos centrales de análisis y las conclusiones sobre las pretensiones del recurso de apelación interpuesto por Enertotal contra el Acuerdo 1004 de 2017.

a. Competencia legal del CNO

En el artículo 36 de la Ley 143 de 1994 se prevé lo siguiente:

"Créase el Consejo Nacional de Operación que tendrá como función principal acordar los aspectos técnicos para garantizar que la operación integrada del sistema interconectado nacional sea segura, confiable y económica, y ser el órgano ejecutor del reglamento de operación."

Las decisiones del Consejo Nacional de Operación podrán ser recurridas ante la Comisión de Regulación de Energía y Gas." (Subrayado fuera de texto)

b. Antecedentes regulatorios

- La Resolución CREG 038 de 2014, por la cual se expidió el Código de Medida, estableció en el literal g) del artículo 8 lo siguiente: *"Todos los sistemas de medición deben contar con los mecanismos de seguridad física e informática dispuestos en el artículo 17 de esta resolución."*

- En el artículo 15 del Código de Medida se establece lo siguiente:

"Registro y lectura de la información. Las fronteras comerciales con reporte al ASIC deben contar con medidores de energía activa y reactiva de tal manera que permitan, como mínimo, el registro horario de las transacciones de energía en el primer minuto de cada hora y con los equipos necesarios para realizar la lectura, interrogación y reporte de la información en los siguientes términos:

(...)

d) El procedimiento de interrogación remota de los medidores, el procesamiento y consolidación de las lecturas en las bases de datos de los Centros de Gestión de Medidas y el reporte de las lecturas al ASIC debe realizarse de manera automática."

- Del Artículo 17 de la Resolución CREG 038 de 2014 se resalta lo siguiente:

"Protección de datos. Los representantes de las fronteras deben asegurar que los medidores, tanto el principal como el de respaldo, de las fronteras comerciales con reporte al ASIC cuenten con un sistema de protección de datos así:

-
- a) El almacenamiento de las mediciones y parámetros de configuración del medidor debe realizarse en memoria no volátil.
- b) La interrogación local y remota de las mediciones y la configuración de los parámetros del medidor debe tener como mínimo dos (2) niveles de acceso y emplear contraseña para cada usuario.
- c) La transmisión de los datos entre el medidor y el Centro de Gestión de Medidas y entre este último y el ASIC deben sujetarse a los requerimientos mínimos de seguridad e integridad definidos por el CNO de acuerdo con lo señalado en el párrafo de este artículo.

(...)

Los RF deben adecuar los sistemas de medición, bases de datos y sus procedimientos dentro de los 24 meses siguientes a la entrada en vigencia de la presente resolución, para dar cumplimiento a lo señalado en este artículo.

Parágrafo 1. Las condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC deben ser definidas por el CNO considerando: los riesgos potenciales, la flexibilidad, escalabilidad, interoperabilidad, eficiencia y economía para el intercambio de los datos de las mediciones y el acceso a los diferentes sistemas de información.

Tales condiciones mínimas deben ser publicadas dentro de los cuatro (4) meses siguientes a la entrada en vigencia de la presente resolución.

Antes de adoptar las condiciones mínimas, el CNO debe poner en conocimiento del Administrador del Sistema de Intercambios Comerciales, ASIC, del Comité Asesor de Comercialización, CAC, y agentes y demás interesados, la propuesta de condiciones mínimas de seguridad e integridad para la transmisión de las lecturas de las fronteras comerciales para sus comentarios.” (Subrayado fuera de texto)

- En el Artículo 18 del Código de Medida se prevé lo siguiente:

“Centro de Gestión de Medidas, CGM. (...) La interrogación de los medidores debe sujetarse a lo establecido en el artículo 17 de esta resolución y emplear

los canales de comunicación, tanto primarios como de respaldo, que el RF considere necesarios para garantizar el reporte de las lecturas de los medidores.

Además de las funciones ya señaladas, el CGM empleado por el representante de la frontera debe realizar las establecidas en el Anexo 3 de la presente resolución.

El almacenamiento de los datos en el CGM debe garantizar la integridad de las mediciones registradas y su disponibilidad por un período de al menos dos (2) años contados a partir del día de la lectura. Además, debe cumplir con los requisitos de protección de los datos establecidos en el artículo 17 de la presente resolución.

(...)

El RF debe asegurar la adecuación de los sistemas de medición y sus procedimientos dentro de los 24 meses siguientes a la entrada en vigencia de la presente resolución para dar cumplimiento a lo señalado en este artículo. Superado el plazo establecido, el único mecanismo de reporte de las lecturas es el señalado en el artículo 37 de esta resolución." (Subrayado fuera de texto)

- En el artículo 22 de la misma resolución se prevé lo siguiente:

"Acceso al sistema de medición. El representante de la frontera debe asegurar el acceso al sistema de medición, asociado a la frontera comercial, para efectos de las verificaciones establecidas en este Código y en la regulación.

(...)

El RF debe documentar y suministrar el procedimiento y los requisitos técnicos para el acceso local y/o remoto a los medidores e informar al solicitante los datos de usuario y contraseña que se requieran para cumplir con lo señalado en este artículo.

El procedimiento y los requisitos técnicos deben cumplir las condiciones de seguridad e integridad establecidas en el parágrafo 1 del artículo 17 de este Código y estar disponibles dentro de los diez (10) meses siguientes a la entrada en vigencia de esta resolución." (Subrayado fuera de texto)

Por último, debe tenerse presente que la fecha de publicación de la Resolución CREG 038 de 2014 fue el 14 de mayo de 2014, a partir de la cual entró en vigencia el Código de Medida.

c. Antecedentes CNO de los Acuerdos 701 de 2014 y 1004 de 2017

En cumplimiento de lo previsto en el parágrafo 1 del artículo 17 de la Resolución CREG 038 de 2014 y atendiendo los criterios establecidos por la regulación, como se desprende de los antecedentes antes mencionados, el CNO expidió el Acuerdo 701 que entró en vigencia el 16 de septiembre de 2014, por el cual se aprobó el documento de "*Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC*".

En el numeral 3.2. del documento en mención del Acuerdo 701 de 2014 se estableció lo siguiente sobre las funcionalidades mínimas del intercambio de datos:

"El intercambio de datos o capa de comunicaciones entre un nodo donde se conecta el medidor de energía y otro nodo donde está el concentrador de datos del CGM, deberá contar con mecanismos de cifrado; tales como VPN, IPSEC, cifrado por firewall, QoS o aquellos que los sustituya o mejoren, o mecanismos de protección de datos. En los casos en que el medidor tenga embebida la tarjeta de comunicaciones con la funcionalidad de encriptación se considera esta como el nodo y aplica la definición." (...) (Subrayado fuera de texto)

Con ocasión de algunas inquietudes recibidas en el CNO, sobre las funcionalidades mínimas cuando se utilicen redes celulares, el 11 de agosto de 2017 se expidió el Acuerdo 1004, que sustituyó a partir de esa fecha el Acuerdo 701 y precisó las funcionalidades mínimas así:

"3.2 Funcionalidades mínimas:

Para fronteras comerciales con reporte al ASIC, el intercambio de datos o capa de Comunicaciones entre un nodo donde se conecta el medidor de energía y otro nodo donde está el concentrador de datos del CGM, deberá

contar con mecanismos que aseguren la confidencialidad, integridad y no repudio de la información por medio de cifrado como: VPN IPSEC o VPN SSL o APN celular privado a través de tecnología 4G, o aquellos que los reemplacen y mejoren. Para redes de datos inferiores a 4G se debe utilizar VPN IPSEC o VPN SSL. En los casos en que el medidor tenga embebida la tarjeta de comunicaciones con la funcionalidad de cifrado, se considera esta como el nodo y aplica la definición.” (Subrayado fuera de texto)

d. Elementos de análisis

- Dadas las inquietudes que se han presentado sobre la aplicación de los acuerdos en el tiempo, se aplica el principio general de la irretroactividad de la ley, entendido como el fenómeno según el cual la ley nueva rige todos los hechos y actos que se produzcan a partir de su vigencia. Cuando se trata de situaciones jurídicas en curso, que no han generado situaciones consolidadas ni derechos adquiridos en el momento de entrar en vigencia la nueva ley, ésta entra a regular dicha situación en el estado en que esté, sin perjuicio de que se respete lo ya surtido bajo la ley antigua.
- En el Acuerdo 701 de 2014 se estableció que el intercambio de datos, sin importar el canal de comunicación empleado debe contar con mecanismos de cifrado o de protección de datos, o cifrado en el medidor.
- En el Acuerdo 1004 de 2017 se estableció que el intercambio de datos, sin importar el canal de comunicación empleado debe contar con mecanismos de cifrado, o cifrado en el medidor. Cuando se utilicen redes celulares inferiores a 4G se debe utilizar VPN IPSEC o VPN SSL. En caso de contar con APN celular privado a través de tecnología 4G entre un nodo donde se conecta el medidor de energía y otro nodo donde está el concentrador de datos del CGM, no se requiere cifrado adicional.
- El plazo regulatorio previsto en el artículo 17 y 18 de la Resolución CREG 038 de 2014 para que los representantes de fronteras comerciales adecuaran los sistemas de medición, bases de datos y dieran cumplimiento a lo señalado en el artículo antes mencionado fue de 24 meses siguientes a la entrada en vigencia de la resolución, es decir, hasta el 14 de mayo de 2016.

- Para efectos de la verificación y el cumplimiento del artículo 17 y 18 de la Resolución CREG 038 de 2014, las fronteras comerciales con reporte al ASIC existentes o nuevas debieron cumplir con lo previsto en el Acuerdo 701 de 2014 a partir del 16 de septiembre de 2014 y hasta el 10 de agosto de 2017.

e. Respuesta a los argumentos del recurso

1. La siguiente afirmación del recurso de apelación de Enertotal en el sentido que: (...) "*los requerimientos técnicos que trae la reciente modificación del ACUERDO 701 a través del ACUERDO CNO 1004 publicada en agosto de 2017, obligan a reemplazar los equipos de comunicación que se usan actualmente para el proceso de lectura de medidores de fronteras comerciales con reporte al ASIC.*" no es cierta por las siguientes razones:

El Acuerdo 701 de 2014 fue expedido el 16 de septiembre de 2014 y estuvo vigente hasta el 10 de agosto de 2017, teniendo en cuenta la fecha de entrada en vigencia del Acuerdo 1004 que lo sustituyó.

Sobre la aplicación del Acuerdo 1004 del 11 de agosto de 2017, se debe aclarar que el mismo rige a partir de la fecha de su expedición (11 de agosto de 2017) y bajo el principio general de interpretación de las normas en el tiempo, no es retroactivo a situaciones que se hayan consolidado bajo la vigencia del Acuerdo 701 de 2014. Por lo que los representantes de fronteras comerciales que cumplieron con el plazo regulatorio previsto en el artículo 17 del Código de Medida lo hicieron con base en lo previsto en el Acuerdo 701 de 2014 y no les es exigible la aplicación del Acuerdo 1004.

Respecto a las funcionalidades mínimas y bajo la vigencia del Acuerdo 701 de 2014, si los representantes de fronteras comerciales utilizan como canal de comunicación redes celulares (4G, 3G o 2G), para el intercambio de datos o capa de comunicaciones entre un nodo donde se conecta el medidor de energía y otro nodo donde está el concentrador de datos del CGM, deben contar con mecanismos de cifrado o mecanismos de protección de datos.

A partir de la entrada en vigencia del Acuerdo 1004 de 2017, es decir del 11 de agosto de 2017 y hasta el 25 de febrero de 2018¹, los representantes de fronteras comerciales tendrán que dar cumplimiento a lo previsto en las funcionalidades mínimas allí previstas y cuando el canal de comunicación empleado sea una red celular 4G, el mecanismo cifrado utilizado debe ser una APN y si se utiliza una red celular inferior a 4G debe utilizarse como mecanismo de cifrado una VPN IPSEC o VPN SSL. Si a la fecha de expedición del Acuerdo 1004 de 2017, es decir, a partir del 11 de agosto de 2017 había fronteras comerciales con reporte al ASIC que no cumplieron con lo establecido en los artículos 17 y 18 de la Resolución CREG 038 de 2014 sobre el plazo de adecuación de los sistemas de medición, bases de datos y procedimientos, les es aplicable lo previsto en el Acuerdo 1004.

2. Sobre la afirmación que se hace indicando que: (...) "*Actualmente los equipos de comunicación instalados bajo el ACUERDO 701 (vigente desde el año 2014 y previo a las exigencias del período de aplicación del código de medida - año 2016) tiene disponible tecnología 2G y/o 3G y son incapaces de establecer una VPN.*" , debe aclararse que bajo el Acuerdo 701 de 2014 se exige que para el intercambio de datos, sin importar el canal de comunicación empleado, debe contarse con mecanismos de cifrado o de protección de datos, o cifrado en el medidor. Adicionalmente y teniendo en cuenta que el plazo de 24 meses previsto en los artículos 17 y 18 de la Resolución CREG 038 de 2014 venció el 14 de mayo de 2016, la verificación del cumplimiento de dicha obligación, para las fronteras con reporte al ASIC existentes en ese periodo de tiempo, debe hacerse con base en lo previsto en el Acuerdo 701 de 2014.

3. Sobre el cuestionamiento a las razones técnicas de la modificación de las funcionalidades mínimas en el Acuerdo 1004 de 2017, se analizó el componente de seguridad y se encontró que cuando se utilizan redes celulares 4G con APN privado para el intercambio de datos, no se requiere una seguridad adicional, ya que es que una tecnología que usa un cifrado robusto y adecuado. Sin embargo, para las tecnologías celulares anteriores a la 4G existen múltiples estudios y reportes públicamente disponibles que expresan como ha sido posible romper los mecanismos de cifrado ofrecido

¹ Teniendo en cuenta la fecha de entrada en vigencia del Acuerdo 1043 de 2018 que sustituyó el Acuerdo 1004 de 2017.

por estas, lo que dejaría expuestos los datos de la medida a la interceptación y manipulación, afectando su seguridad e integridad, por lo que no se pueden seguir considerando como tecnologías que provean la seguridad requerida a futuro, haciéndose necesario considerar tecnologías modernas para las nuevas fronteras y nuevos proyectos de aseguramiento. Se adjunta concepto técnico especializado contratado por el Consejo en el que se detallan las vulnerabilidades de las redes 2G y 3G².

4. Respecto a los comentarios sobre los costos de implementación de las funcionalidades mínimas de los acuerdos, es importante referirse a que el CNO en ejercicio de las funciones legales del artículo 36 (Ley 143 de 1994) acuerda los aspectos técnicos para garantizar una operación segura, confiable y económica de la operación del SIN y ejecuta el reglamento de operación. Cuando se da cumplimiento a los mandatos regulatorios, se hace en el marco del ejercicio de las funciones legales. Por lo que el Consejo no tiene la competencia legal para tratar asuntos comerciales. Adicionalmente y en cumplimiento del Decreto 2238 de 2009 del Ministerio de Minas y Energía, las discusiones y decisiones del Consejo se deben referir exclusivamente a los aspectos técnicos de la operación segura, confiable y económica del SIN. No obstante lo anterior, sobre la solución presentada en su comunicación, en la que plantea que (...) *"para el establecimiento de VPN entre el CGM y cada uno de los medidores se requiere la implementación de un "UTM" (Unified Threat Management - Gestión Unificada de Amenazas). (Firewall, sistema de detección y prevención de intrusos), que soporte VPN en el número de puntos de medida que tenga cada comercializador y/o operador de red que puede tener un sobrecosto dentro de la nueva arquitectura propuesta; así mismo, el establecimiento y mantenimiento de una VPN incrementa exponencialmente la capacidad y por tanto el costo."* debemos aclarar que es sólo una de las posibles soluciones que hay para la implementación de los mecanismos de seguridad planteados en el Acuerdo 1004. Y desde el punto de vista técnico, es conveniente recordar que la interrogación de todos los medidores no se requiere simultáneamente y durante todo el tiempo, por lo que las soluciones pueden contemplar el subir los mecanismos de cifrado y comunicación para la medición y bajarlos al finalizar la indagación, por lo que con una distribución adecuada se requerirían menos conexiones simultáneas, bajando los costos requeridos.

² Santamaría Rafael. Concepto Técnico evaluación y valoración comentarios CNO 1004. Diciembre 2017

5. Respecto a las menciones que se hacen sobre la vida útil, se reitera que los equipos y demás adecuaciones realizadas por los representantes de fronteras comerciales para dar cumplimiento al Acuerdo 701 de 2014 no deben ser reemplazados hasta finalizar su vida útil. Sin embargo, adquirir tecnologías que salieron al mercado desde principios de la década de 1990 como es el caso de 2G y 3G en el 2000, que ya cuentan con múltiples vulnerabilidades ampliamente difundidas, con la intención de mantenerlas por 10 años, puede abrir una brecha en la seguridad de las mismas, que no puede ser ignorada ya que los nuevos proyectos deben buscar la mejor tecnología disponible para que durante su vida útil se mantengan los requisitos de confidencialidad, integridad, disponibilidad y no repudio, como lo solicita la regulación vigente.

6. Sobre la mención que se hace a que el CNO no cumplió con lo dispuesto en el numeral 8 del artículo 8 de la Ley 1437 de 2011 y lo establecido en el artículo 17 de la Resolución CREG 038 de 2014, respecto a la divulgación antes de la aplicación de cualquier norma, con el fin de recibir opiniones, sugerencias o propuestas alternativas de los interesados, el Consejo decidió desarrollar la etapa de socialización de la modificación del Acuerdo 701, como dispone el artículo 17 de la Resolución CREG 038 de 2014.

Es así como, con posterioridad a la expedición del Acuerdo 1004 de 2017 se recibieron inquietudes de algunos agentes del SIN sobre las modificaciones allí incluidas y sobre la aplicación de los Acuerdos 701 y 1004 en el tiempo, para efectos de su cumplimiento y verificación.

Previa recomendación del Comité Legal, el Consejo en la reunión 98 del 20 de noviembre de 2017 decidió socializar el documento de *"Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC"* y la propuesta de acuerdo, por los siguientes medios:

- Página WEB del CNO

- Un aviso en un diario de amplia circulación que salga el viernes, sábado y domingo, que invite a consultarlo en la página y a enviar comentarios

-
- La expedición de una Circular dirigida a los representantes de fronteras comerciales que invite a consultarlo en la página y a enviar comentarios
 - Envío al ASIC para comentarios
 - Envío al CAC para comentarios

El Consejo publicó el documento de "*Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC*" y la propuesta de acuerdo en la página WEB del CNO, los envió al CAC y al ASIC, expidió la Circular 22 del 24 de noviembre de 2017 dirigida a los agentes del SIN, y publicó el 24, 25 y 26 de noviembre de 2017 en el periódico El Tiempo un aviso dirigido a los representantes de fronteras comerciales a conocer los mismos documentos y enviar sus comentarios hasta el 3 de diciembre de 2017.

Dentro del plazo previsto para recibir comentarios de la Circular 22 de 2017, se recibieron comentarios de las siguientes empresas: GECELCA S.A. E.S.P., ELECTRICARIBE S.A. E.S.P. (intervenida), CELSIA S.A. E.S.P., AES CHIVOR S.A. E.S.P., DICEL S.A. E.S.P., ENERTOTAL S.A. E.S.P., RUITOQUE S.A. E.S.P., EMCALI EICE E.S.P., INTERCOLOMBIA S.A. E.S.P., XM S.A. E.S.P. y EPM E.S.P.

La Comisión de Ciberseguridad analizó los comentarios recibidos y les dio respuesta en documento que fue revisado y avalado por el Comité Tecnológico, el cual recomendó al Consejo la expedición de un nuevo Acuerdo y la publicación del documento de respuestas en la página WEB del CNO.

Finalmente, el Consejo expidió el 26 de febrero de 2018 el Acuerdo 1043 que sustituyó el Acuerdo 1004 de 2017, el cual fue publicado en la página WEB del CNO. El documento de respuestas a los comentarios recibidos también fue publicado en la página WEB del CNO el 26 de febrero de 2018 y mediante correo electrónico fue enviado a las empresas que habían enviado comentarios, entre las que se encuentra Enertotal S.A. E.S.P.

En el documento anexo del Acuerdo 1043 "Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC" se mejoró la redacción del numeral 3.2 para dar mayor claridad y se hizo una modificación así (texto subrayado):

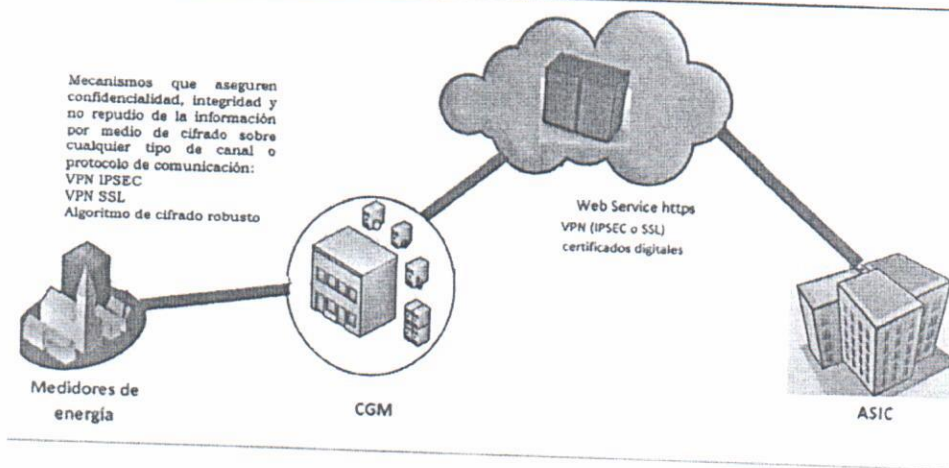
"3.2. Funcionalidades mínimas:

Para fronteras comerciales con reporte al ASIC, el intercambio de datos o capa de comunicaciones entre un nodo donde se conecta el medidor de energía y otro nodo donde está el concentrador de datos del CGM, deberá contar con mecanismos que aseguren la confidencialidad, integridad y no repudio de la información por medio de cifrado sobre cualquier tipo de canal o protocolo de comunicación; con una de las siguientes alternativas: VPN IPSEC, VPN SSL, algoritmo de cifrado robusto, o aquellas que las sustituyan o aquellas que las mejoren.

En los casos en que el medidor tenga embebida la tarjeta de comunicaciones con la funcionalidad de cifrado, se considera esta como el nodo y aplica la definición.

En caso de contar con APN celular privado a través de tecnología 4G entre un nodo donde se conecta el medidor de energía y otro nodo donde está el concentrador de datos del CGM, no se requiere cifrado adicional.

El intercambio de datos entre el CGM y el ASIC deberá realizarse a través de https sobre redes privadas virtuales (IPSEC o SSL), autenticadas con certificados digitales en doble vía para asegurar la confidencialidad, integridad y no repudio.



El cumplimiento de las medidas de seguridad mínimas deberá verificarse mediante auditorías internas ejecutadas por un área independiente a quien realiza la configuración y mantenimiento de estos controles." (...)

Adicionalmente y dadas las inquietudes sobre la aplicación de los Acuerdos 701 de 2014 y 1004 de 2017 para efectos del cumplimiento y verificación de lo señalado en los artículos 17 y 18 de la Resolución CREG 038 de 2014, se estableció en el artículo segundo del Acuerdo 1043 de 2018 lo siguiente:

(...)"- El periodo de vigencia del Acuerdo 701 inició el 14 de septiembre de 2014 hasta el 10 de agosto de 2017.

- El periodo de vigencia del Acuerdo 1004 inició el 11 de agosto de 2017 y hasta el 25 de febrero de 2018."

f. Conclusiones

El Consejo Nacional de Operación ha dado cumplimiento al mandato regulatorio previsto en el artículo 17 de la Resolución CREG 038 de 2014 en el marco del ejercicio de sus funciones legales.

La definición en los Acuerdos 701 de 2014, 1004 de 2017 y 1043 de 2018 de las condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC han tenido en cuenta las consideraciones del parágrafo

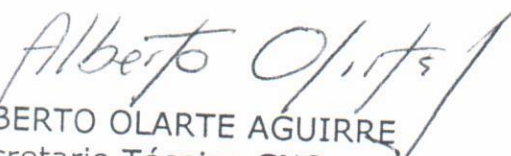
1 del artículo 17 de la Resolución CREG 038 de 2014 sobre los riesgos potenciales, la flexibilidad, escalabilidad, interoperabilidad, eficiencia y economía para el intercambio de los datos de las mediciones y el acceso a los diferentes sistemas de información.

Las modificaciones introducidas en los acuerdos antes mencionados tienen un respaldo técnico y como ya se ha mencionado, no imponen obligaciones retroactivas. Al respecto, es importante hacer énfasis en el deber del CNO de estar siempre en proceso de actualización, y en su función legal de expedir acuerdos técnicos, debe ser dinámico para así responder a los nuevos retos que trae la tecnología y garantizar confiabilidad y seguridad a la operación del Sistema.

Respecto del requisito de socialización del documento del Acuerdo 1004, se cumplió y como resultado se expidió el Acuerdo 1043 de 2018, que aclaró la vigencia de los Acuerdos 701 de 2014 y 1004 de 2017 para efectos de la verificación de que trata la Resolución CREG 038 de 2014.

Por lo anterior, y dado que el Consejo Nacional de Operación expidió un nuevo acuerdo que sustituyó el Acuerdo 1004 de 2017 y sobre el cual versan las pretensiones del recurso de apelación interpuesto por Enertotal S.A. E.S.P se ha configurado un hecho superado.

Atentamente,


ALBERTO OLARTE AGUIRRE
Secretario Técnico CNO

Adjunto lo anunciado

3. Vulnerabilidades en Redes Celulares

3.1 Principales problemas de seguridad en Redes 2G

Las debilidades en algoritmos de cifrado (algoritmo A3 para autenticación, algoritmo A5 para encriptación, algoritmo A8 para generación de claves) causadas por la obsolescencia tecnológica, facilitan los ataques cibernéticos. La antigüedad de los algoritmos de cifrado y las nuevas tecnologías disponibles permiten realizar ataques de fuerza bruta o utilizar tablas de salida para comprometer las comunicaciones. Por ejemplo, GSM solo autentica la red al usuario pero no el usuario a la red, por lo tanto es posible conectarse a una red falsa sin saberlo [4].

El modelo de seguridad ofrece confidencialidad y autenticación, pero capacidades limitadas de autorización y no repudio. Algunos de los algoritmos criptográficos para la seguridad son A5 / 1 y A5 / 2, garantizando la privacidad de voz en el aire. Sin embargo se ha probado que ambos algoritmos han sido vulnerados:

- A5 / 2 es vulnerable a ataques de texto cifrado en tiempo real.
- A5 / 1 es vulnerable con un ataque de tabla de arco iris.

Las principales preocupaciones de seguridad con respecto a GSM son:

- El tráfico de comunicaciones y señalización en la red no está protegido.
- No registra los ataques activos en la red evitando que sea posible identificar su fuente.
- La red GSM es tan segura como las redes fijas a las que se conectan.
- La interceptación de tráfico solo se considera como una mejora posterior.
- La identidad de la terminal al momento de conectarse a una red 2G, no asegura su confiabilidad.

Algunos de los principales ataques son [4]:

- **Ataque del hombre en el medio (*Man-in-the-middle*):** Este atacante se posiciona entre el usuario objetivo y una red que escucha y modifica el tráfico.
- **Eavesdropping:** El atacante escucha a escondidas las señales y las conexiones de datos.
- **Suplantación de la red:** el atacante envía señalización y datos al usuario objetivo, pretendiendo ser una BST (estación base) de una red genuina.
- **Suplantación de usuario:** el intruso envía datos de señalización a la red pretendiendo ser originados por el usuario objetivo.

En resumen, teniendo en cuenta las vulnerabilidades de la red en cuanto la autenticación de doble vía y a pesar de contar con protocolos de cifrado, las vulnerabilidades presentes en las redes 2G representan un riesgo inminente en

EVALUACIÓN Y VALORACIÓN DE COMENTARIOS CNO1004

cuanto a disponibilidad y por lo tanto no se recomienda su uso para infraestructura crítica [4]. A pesar de poder implementar módems que permiten funciones de cifrado avanzadas para cumplir los requisitos de integridad y confidencialidad, la disponibilidad se ve comprometida por las vulnerabilidades mismas de la red.

3.2 Vulnerabilidades Presentes en Redes 3G

El Sistema Universal de Telecomunicaciones Móviles (UTMS), estandarizado por 3GPP, es el sucesor de la tecnología de comunicación móvil 3G para GSM y GPRS. UMTS combina las interfaces aéreas W-CDMA, TD-CDMA o TD-SCDMA, el núcleo de parte de aplicación móvil (MAP) de GSM y la familia de códec de voz GSM. W-CDMA es la variante de telefonía móvil celular más popular de UMTS en uso. UMTS, utilizando W-CDMA, admite velocidades de transferencia de datos de hasta 14 Mbit / s en teoría, con Acceso a paquetes de enlace descendente de alta velocidad (HSDPA), aunque el rendimiento en redes desplegadas podría ser mucho menor para las conexiones de enlace ascendente y de enlace descendente [5].

La principal razón para el desarrollo e implementación de 3G fue proporcionar servicios de alta gama a numerosos usuarios en todo el mundo utilizando un teléfono universal. Sin embargo, esto aumentó el nivel de interacción entre los usuarios, los proveedores de servicios y los operadores del mercado y también aumentó la vulnerabilidad de las redes a los ataques externos. El marco de seguridad de UMTS se centró en abordar las debilidades en GSM al tiempo que mejoraba los métodos robustos e importantes ya exitosos.

La guía para la seguridad 3G (3GPP TR 33.900) recopila la descripción de ataques o amenazas identificados para UMTS, estos ataques explotan debilidades en el sistema y para algunos casos es posible que sean contrarrestados por alguna característica específica de la arquitectura de seguridad 3G [6].

Para lanzar ataques contra las redes 3G, un intruso debe tener las siguientes capacidades [7] y [8]:

- **Eavesdropping:** el intruso puede escuchar la señalización asociada con otros usuarios o sus conexiones de datos.
- **Suplantación de identidad de un usuario:** permite al intruso interactuar con la red como el usuario real.
- **Suplantación de identidad de la red:** permite al intruso interactuar con el usuario como si estuviera recibiendo señales de una red genuina.
- **Ataque de "Man-in-the-middle":** es una capacidad del intruso para interponerse entre dos partes que se comunican (un usuario y la red), lo que permite realizar diversas acciones, como escuchar, modificar, borrar, reordenar y reproducir los datos del usuario.
- **Compromiso de vectores de autenticación en la red:** el intruso toma el control de un vector de autenticación al comprometer nodos o enlaces de red.

EVALUACIÓN Y VALORACIÓN DE COMENTARIOS CNO1004

Cabe resaltar que para realizar un ataque, el intruso requiere una estación móvil (MS) modificada y/o una estación base (BS) modificada. Un atacante con las capacidades descritas anteriormente puede realizar los siguientes ataques contra los sistemas 3G [6]:

- **Denegación de Servicios (DoS):** los siguientes casos pueden dar como resultado la denegación total o parcial de servicios para el usuario objetivo:
 - a) **Suplantación de solicitud de cancelación de registro para usuarios:** si la red no puede autenticar mensajes, un atacante con una MS modificada puede enviar una solicitud de cancelación de registro a la red, la cual es cumplida por la red y simultáneamente envía instrucciones al Registro de ubicación de inicio (HLR) a hacer lo mismo.
 - b) **Campamento en una BS / MS falsa:** el atacante con una BS / MS modificada se coloca entre la Red de Servicio (SN) y el usuario objetivo.
 - c) **Suplantación de solicitud de actualización de ubicación:** en lugar de enviar solicitudes de cancelación de inscripción, el atacante envía una solicitud de actualización de ubicación desde un área diferente a aquella en la que el usuario se encuentra actualmente. Como resultado, el usuario es localizado en la nueva área.
- **Suplantación de la red y por lo tanto "Eavesdropping":** Estas intrusiones incluyen ataques donde el intruso se enmascara como una red genuina hacia el usuario.
 - a) **Al suprimir el cifrado entre el usuario objetivo y el intruso:** un atacante con una BS modificada tienta al usuario a acampar en su BS falsa y cuando se inicia el servicio, el intruso no habilita el cifrado.
 - b) **Al suprimir el cifrado entre el usuario objetivo y la red verdadera:** En este caso, durante la configuración de la llamada, las capacidades de cifrado de la MS son modificadas por el intruso y la red muestra que existe una falta de coincidencia genuina de los algoritmos de cifrado y autenticación. Después de esto, la red puede decidir establecer una conexión no cifrada: el intruso corta la conexión y suplanta la red al usuario objetivo.
 - c) **Al forzar el uso de una clave de cifrado comprometida:** el atacante con una BS / MS modificada y un vector de autenticación comprometido atraen al usuario a configurar una llamada mientras se encuentra en su falsa BS / MS. El atacante fuerza el uso de una clave de cifrado comprometida.
- **Captura de identidad:** Los usuarios móviles se identifican mediante identidades temporales, pero hay casos en los que la red solicita al usuario que envíe su identidad permanente en texto plano.
 - a) **Captura pasiva de identidad:** el atacante con una MS modificada espera pasivamente un nuevo registro o un bloqueo de la base de datos, ya que en tales casos se solicita al usuario que envíe su identidad en texto plano.
 - b) **Captura de identidad activa:** en este caso, el atacante con una BS modificada tienta al usuario a acampar en su BS y luego le pide que envíe su Identidad de Suscriptor Móvil Internacional (IMSI).

EVALUACIÓN Y VALORACIÓN DE COMENTARIOS CNO1004

- **Suplantación del usuario:** se describen varios mecanismos mediante los cuales, el intruso puede suplantar al usuario.
 - a) **Mediante el uso de un vector de autenticación comprometida:** el atacante con una MS modificada y acceso a un vector de autenticación comprometido logrando suplantar el usuario objetivo.
 - b) **Mediante el uso de una respuesta de autenticación interceptada:** el intruso con una MS modificada y mediante una respuesta de autenticación interceptada, logra suplantar el usuario objetivo.
 - c) **Secuestro de llamadas salientes en redes con encriptación deshabilitada:** un intruso con una BS / MS modificada engaña a un usuario objetivo para una llamada entrante, luego configura y ejecuta una llamada. El intruso modifica los elementos de señalización en la red de servicio suplantando al usuario. Luego, el intruso corta la conexión con el usuario objetivo y realiza llamadas fraudulentas a la suscripción del usuario.
 - d) **Secuestro de llamadas salientes en redes con encriptación habilitada:** en este caso, el intruso modifica las capacidades de cifrado de la MS suprimiendo el cifrado.
 - e) **Secuestro de llamadas entrantes en redes con cifrado deshabilitado:** un asociado del intruso realiza una llamada al usuario objetivo, que es retransmitida por el intruso hasta que se haya completado la autenticación y la configuración de la llamada. Si la red no habilita el cifrado, el intruso libera al usuario objetivo y usa la conexión para responder la llamada.
 - f) **Secuestro de llamadas entrantes en redes con encriptación habilitada:** en tales casos, además del método utilizado en la subsección (d), el intruso también suprime el cifrado.

Aunque la seguridad 3G presenta grandes avances con respecto a tecnologías anteriores y es capaz de contrarrestar diversos ciberataques, hay algunas deficiencias. Los datos del usuario a través del aire no garantizan protección de la integridad y la seguridad del dominio de red no se extiende al dominio del usuario. Algunos protocolos de UMTS envían texto plano al asignar un usuario. El secuestro de canal entre mensajes de protección de integridad aún es posible. Adicionalmente el algoritmo KASUMI o A5/3 el cual se utiliza para el cifrado de datos en la tecnología 3G se puede ver fácilmente vulnerado sin la necesidad de invertir muchos recursos computacionales y es posible recuperar 96 de los 128 bits de cifrado de las claves en unos pocos minutos y los 128 bits completos en menos de dos horas. Con esto se hace necesario garantizar la seguridad en las redes 3G con mecanismos adicionales a los que se incluyen por defecto, algunas de las soluciones más probadas y eficientes son las VPN site to site, específicamente las de tipo IPsec y SSL, también existen diversos métodos de cifrado de la información compatibles con 3G los cuales se pueden implementar ejecutando las respectivas pruebas de verificación.

Bibliografía

- [1] B. Mitchell, «2G, 3G, 4G, & 5G Explained - An Introduction to 2G, 3G, 4G & 5G Wireless,» 18 Diciembre 2017. [En línea]. Available: <https://www.lifewire.com/mobile-networking-explained-817468>. [Último acceso: 20 Diciembre 2017].
- [2] Open Signal, «Global State of Mobile Networks,» Agosto 2016. [En línea]. Available: <https://opensignal.com/reports/2016/08/global-state-of-the-mobile-network>. [Último acceso: 20 Diciembre 2017].
- [3] Open Signal, «State of Mobile Networks: Colombia 2017,» Mayo 2017. [En línea]. Available: <https://opensignal.com/reports-data/national/data-2017-07-colombia/report.pdf>. [Último acceso: 21 Diciembre 2017].
- [4] P. Paganini, «Critical infrastructures – Main threats for 2G and 3G mobile networks,» 13 Enero 2012. [En línea]. Available: <http://securityaffairs.co/wordpress/1603/security/gsm-mobile-networks.html>. [Último acceso: 21 Diciembre 2017].
- [5] S. Prakash, *STUDY AND IMPLEMENTATION OF 3G MOBILE SECURITY*, 2010.
- [6] A. Bais, W. T. Penzhorn y P. Palensky, «Evaluation of UMTS security architecture and services,» *IEEE*, p. Septiembre, 2006.
- [7] 3GPP, *ETSI TS 121 133 V4.1.0 - Universal Mobile Telecommunications System (UMTS) - Security Threads and Requirements*, 2001.
- [8] 3GPP, *3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security*, 2000.
- [9] Axon Group, «¿Conoce cuál es la Infraestructura Crítica en el Sector Eléctrico y que dice la Legislación Colombiana en Cuanto a su Protección a Nivel de Ciberseguridad?,» 08 Noviembre 2016. [En línea]. Available: <http://www.axongroup.com.co/conoce-cual-es-la-infraestructura-critica-en-el-sector-electrico-y-que-dice-la-legislacion-colombiana-en-cuanto-a-su-proteccion-a-nivel-de-ciberseguridad/>. [Último acceso: 23 Diciembre 2017].
- [10] Comando Conjunto Cibernético, «Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia. Edición 1.,» 1 Diciembre 2015. [En línea]. Available: <http://www.minambiente.gov.co/images/tecnologias-de-la-informacion-y->