Enviado x mail
21-4-18 M

cno
Consejo Nacional de Operación

Bogotá D. C., 25 de abril de 2018

Doctor
Andres Felipe Rios Velásquez
Jefe de proyecto Verificaciones Quinquenales
Applus Norcontrol Ltda.
Calle 117 # 69 – 46
Ciudad

Asunto: Respuesta a inquietudes de empresas verificadoras de la Resolución CREG 038 de 2014.

Estimado Doctor Rios:

Como resultado de la realización del taller realizado el 16 de abril de 2018 con los verificadores de la Resolución CREG 038 de 2014, la Secretaria Técnica del Comité Asesor de Comercialización CAC y un representante de dicho organismo, el Presidente e integrantes de la Comisión de Ciberseguridad del CNO, y la asesora jurídica y el Secretario Técnico del Consejo Nacional de Operación, para tratar algunas inquietudes que hay sobre los Acuerdos 701 de 2014, 1004 de 2017 y 1043 de 2018, se estableció un plazo hasta el 17 de abril a las 5 p.m. para recibir por correo electrónico las preguntas de los verificadores.

Se recibieron dentro del plazo indicado las siguientes preguntas:

A. Consorcio Negawatt – ACI

PREGUNTA 1. Acerca de la aplicabilidad temporal de los acuerdos del taller, en el caso de que sea necesario reemplazar un componente del sistema de comunicación (por ejemplo, ante una falla del Modem), en una frontera

registrada ante el ASIC en fecha anterior al 10 de agosto de 2017 y que en su momento había realizado las adecuaciones para cumplir el Acuerdo CNO 701 de 2014, la pregunta es:

- Al tener que cambiar el dispositivo, por ejemplo en una fecha posterior a la expedición de otro de los acuerdos (por ejemplo el CNO 1043 del 26 de febrero de 2018), ¿El agente puede reemplazar el dispositivo dañado por uno del mismo modelo y referencia al que estaba instalado (teniendo en cuenta que este le permitía cumplir el acuerdo vigente a su fecha de inscripción), o es necesario que el representante tenga que adecuar todo el sistema de comunicaciones de la frontera para cumplir el nuevo acuerdo vigente al momento de reemplazar el modem?

- Esto, teniendo en cuenta que para lograr el cumplimiento del nuevo acuerdo, es posible que no implique únicamente el cambio del modem por otro modelo con características adicionales, sino que además, puede ser necesario realizar adecuaciones a los componentes físicos del medio de comunicación y/o adicionar nuevos equipos (firewall, enrutadores, etc.), así como implementar modificaciones de "software" en el nodo donde está el concentrador de datos del CGM.

RESPUESTA

Para la verificación del cumplimiento de las funcionalidades mínimas (numeral 3.2. de los acuerdos 701, 1004 y 1043 del CNO), ante el reemplazo de cualquier componente del sistema de comunicación (por ejemplo un módem), se debe aplicar el acuerdo que se encontraba vigente en el momento en que el representante de la frontera comercial implementó la solución. Ante un daño de uno de los elementos del sistema, el cambio o reemplazo se debe hacer como mínimo por elementos con características y funcionalidades equivalentes, manteniendo el cumplimiento del acuerdo bajo el cual se implementó la solución.

PREGUNTA 2. El acuerdo CNO 701 de 2014 en el numeral 3.2 del Anexo, da unas alternativas para el cumplimiento de las condiciones mínimas de seguridad e integridad de las comunicaciones, así:

- La pregunta es: ¿Qué características técnicas o requerimientos mínimos de seguridad informática deben cumplir los "mecanismos de protección de datos" que se plantean como alternativa en el texto resaltado, en el ámbito de aplicación del acuerdo, al momento de una verificación del cumplimiento del código de medida por parte del RF o de un tercero verificador?

RESPUESTA

Como está previsto en el numeral 3.1 de los Acuerdos 701, 1004 y 1043, los mecanismos de protección de datos deben brindar integridad y confidencialidad de la información transmitida.

Entendiendo por integridad como el conjunto de condiciones que deben cumplir los datos para garantizar que la información se mantiene sin cambios, a menos que las modificaciones sean autorizadas, es decir que la información debe llegar a su destino sin cambios. Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Por confidencialidad como la propiedad del sistema de información que consiste en garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

PREGUNTA 3. El acuerdo CNO 1043 de 2018 en el numeral 3.2 del Anexo da unas alternativas para el cumplimiento de las condiciones mínimas de seguridad e integridad de las comunicaciones, 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 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."

- La pregunta es: ¿Qué características técnicas mínimas o requerimientos de seguridad informática deben cumplir los algoritmos de cifrado robusto que se plantean como alternativa en el texto subrayado? ¿Qué definiría que un sistema de cifrado sea "robusto" en el ámbito de aplicación del acuerdo, al momento de una verificación del cumplimiento del código de medida por parte del RF o de un tercero verificador?

RESPUESTA

La robustez de un algoritmo de cifrado se refiere a que sea un algoritmo que garantice la integridad y confidencialidad de la información transmitida y que haya sido probado y comúnmente aceptado en la industria.

PREGUNTA 4. Los 3 acuerdos analizados en el taller exigen el cumplimiento de unos requisitos específicos para las claves o contraseñas que deben ser configuradas en los medidores de energía de la siguiente manera:

- La pregunta es: ¿Al momento de las verificaciones extraordinarias o quinquenales por parte de un firma verificadora, contempladas en la resolución CREG 038 de 2014, el representante de frontera estaría obligado a entregar las contraseñas de los diferentes niveles de acceso al tercero verificador, o es posible entregar un soporte documental firmado, que certifique por parte del RF, el cumplimiento de los requisitos mencionados por los acuerdos?

- Esta pregunta se hace debido a que la divulgación de las contraseñas de acceso a los medidores puede afectar negativamente las condiciones de seguridad e integridad del sistema de medida, sobre todo, teniendo en cuenta que toda la información entregada a las firmas verificadoras dentro de los procesos de verificación de la CREG 038/2014, debe hacerse pública.

RESPUESTA

Como una buen práctica, no debería exigirse al representante de frontera comercial la entrega de las contraseñas de los niveles de acceso. Dado que el Acuerdo prevé que deben haber dos contraseñas para cada uno de los niveles, en principio se debería solicitar la política y/o procedimientos de

determinación y cambio de contraseñas para los niveles de acceso y el registro del cumplimiento de la política y/o procedimientos en la hoja de vida. De otra parte, si el medidor tiene el registro del cambio de contraseña, eso puede ser evidenciado. Adicionalmente, para la revisión de la configuración de los parámetros de la contraseña, si el medidor lo permite, como mínimo debería revisarse que no se usen las contraseñas por defecto, probándolas en el medidor.

PREGUNTA 5. Con respecto a los acuerdos del CNO 701/2014, 1004/2017 y 1043/2018, queremos consultar: ¿si el incumplimiento, específicamente de los mecanismos de cifrado en el medio de comunicaciones del acuerdo CNO que le sea aplicable, se constituye como un incumplimiento con afectación a la medida reportada, y llevaría a la declaración en falla de la frontera por parte del ASIC, o sería un incumplimiento del código sin afectación a la medida?

- Precisando, que en ambos casos se requiere que el agente realice la adecuación y normalización del incumplimiento del acuerdo correspondiente, y luego debe solicitar una verificación extraordinaria para poder cumplir el código de medida.

RESPUESTA

Teniendo en cuenta que la pregunta formulada se refiere a si el incumplimiento de

las funcionalidades mínimas previstas en un acuerdo del CNO constituyen un incumplimiento con afectación a la medida reportada, de manera atenta le informamos que el Consejo no tiene la competencia legal para dar respuesta a su inquietud, por tratarse de un tema de competencia regulatoria.

B. Applus Norcontrol

PREGUNTA 1. Acceso nivel 1 y/o 2 en medidores de forma local y/o remota.

Teniendo en cuenta que los medidores traen contraseñas de fabricante por defecto, las cuales son idénticas tanto para el nivel de acceso 1 como para

el nivel de acceso 2, y que es la misma en todos los medidores de la misma referencia o marca, se hace necesario clarificar la aplicabilidad y el sentido del artículo 17:"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."

Desde el punto de vista técnico es claro que el sentido de la regulación busca tener diferentes contraseñas para los accesos 1 y 2, es decir, que la contraseña 1 sea diferente de la contraseña 2 y que además, estas sean diferentes entre medidores (sin password genéricos del fabricante) tal y como esta expresado en el numeral 3.2 del acuerdo 701 del 2014, 1004 del 2017 y 1043 del 2018. "esta clave será única por nivel de acceso en cada medidor." "deberá ser definida por cada representante de frontera RF, sin exceder un periodo de 2 años."

Teniendo en cuenta que en la situación actual durante la revisión de las hojas de vida se verifica que de lo anteriormente expuesto no se deja el registro, dejando así dos posibilidades: 1. que realizan los cambios pero no se deja el reporte en la hoja de vida de acuerdo a lo expresado en el artículo 17 protección de datos: "mantener un registro de los accesos al medidor de nivel de acceso 2 en la hoja de vida" y la otra posibilidad es que no se esté realizando dichos cambios dentro de límite máximo de periodicidad definida por los acuerdos 701 del 2014, 1004 del 2017 y 1043 del 2018 de CNO.

Sin embargo, teniendo en cuenta la forma como quedó redactado CREG 038 del 2014: "dos (2) niveles de acceso y emplear contraseña para cada usuario.", los RF en su mayoría han adoptado que pueden tener contraseñas por defecto e incluso que puede ser la misma para nivel 1 y 2. Lo cual fue clarificado en el numeral anterior del CNO en todos los acuerdos. Teniendo en cuenta lo solicitado por la regulación se hace necesario determinar:

¿Si el alcance de las verificaciones quinquenales incluye la verificación de la aplicación del numeral 3.2 de los acuerdos emitidos por el CNO? ó ¿si solamente se limita a la validación del procedimiento de los parámetros, procedimientos y políticas de operación del CGM? o ¿si se debe verificar la validación de accesos con contraseñas en campo?, si se determina que es esta última, solicitamos indicar el método para la realización de verificación.

Se debe tener en cuenta que en el artículo 22 de la resolución Creg 038 de 2014 define lo siguiente: (subrayado fuera de texto)

"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".

De otra parte, se hace énfasis en que para garantizar la integridad y confidencialidad de la información expresada en forma general por los RF (protección de datos de los usuarios.), no se solicitan los password en sitio, sino la aplicación de los mismos mediante el acceso de nivel 1 (descarga de datos del medidor o diagrama vectorial) y mediante la actualización horaria del medidor (acceso nivel 2). La ejecución de este procedimiento se ha realizado en forma local o en forma remota dependiendo de la disponibilidad del RF y de los medios tecnológicos disponibles al momento de la verificación.

Sin embargo, dentro de la resolución se especifica que se deben garantizar ambos accesos, tanto el local como el remoto: "interrogación local y remota".

En tal sentido, se hace indispensable dar claridad sobre la forma y alcance de aplicabilidad, de lo expresado en el artículo 17 literal b de la resolución Creg 038 de 2014, al momento de evaluar la conformidad durante las verificaciones quinquenales.

RESPUESTA

Damos respuesta a las preguntas formuladas (texto subrayado) así: teniendo en cuenta lo previsto en el artículo 24 de la Resolución CREG 038 de 2018, el procedimiento técnico de verificación de los sistemas de medición en el que se establecen las actividades requeridas para llevar a cabo la verificación debe ser definido por el CAC. Por lo anterior, el Consejo no tiene la competencia legal para definir el alcance de las actividades que incluye la verificación del cumplimiento del artículo 17 de la Resolución CREG 038 de 2014.

PREGUNTA 2. Si se tiene el sistema de comunicación en falla afecta o no afecta el sistema de medida.

Si se tiene sistema de comunicación en falla (no transmite), a pesar que el medidor registre las mediciones realizadas, ¿se considera que existe una afectación en el sistema de medida?, lo anterior teniendo en cuenta que puede afectar los reportes de información en los tiempos requeridos (48 horas) ocasionando que al momento de no tener los datos reales se estime mediante curva típica y en dicho caso consideramos que hay afectación de la medida, ya que los valores estimados son diferentes a lo realmente registrado en el medidor. Sin embargo, si se tiene un sistema de comunicación en buenas condiciones a pesar de no contar con los mecanismos de cifrado o de protección de datos exigidos en el acuerdo 701 del CNO, se define como no cumple respecto a la resolución Creg 038 de 2014 sin afectación en el sistema de medida a las fechas en que se realizó la verificación.

RESPUESTA

Teniendo en cuenta que la pregunta formulada se refiere al tratamiento de los hallazgos en los sistemas de medición, de manera atenta le informamos que el Consejo no tiene la competencia legal para dar respuesta a su inquietud por tratarse de un tema regulatorio (Resolución CREG 038 de 2014).

PREGUNTA 3. ¿Los acuerdos CNO 701 del 2014, 1004 del 2017 y 1043 del 2018 no establecen si el remplazo de un equipo de comunicación de una frontera existente se acepta el acuerdo que le aplicaba o se exige cumplimiento de acuerdo vigente definir aplicación para este tipo de casos?

RESPUESTA

Para la verificación del cumplimiento de las funcionalidades mínimas (numeral 3.2. de los acuerdos 701, 1004 y 1043 del CNO), ante el reemplazo de cualquier componente del sistema de comunicación (por ejemplo un módem), se debe aplicar el acuerdo que se encontraba vigente en el momento en que el representante de la frontera comercial implementó la

solución. Ante un daño de uno de los elementos del sistema, el cambio o reemplazo se debe hacer como mínimo por elementos con características y funcionalidades equivalentes, manteniendo el cumplimiento del acuerdo bajo el cual se implementó la solución.

PREGUNTA 4. Solicitamos el favor de definir los criterios que se deben tener en cuenta por parte de los verificadores quinquenales con respecto a mecanismo de cifrado robusto en cuanto a las condiciones mínimas de cumplimiento.

RESPUESTA

La robustez de un algoritmo de cifrado se refiere a que sea un algoritmo que garantice la integridad y confidencialidad de la información transmitida y que haya sido probado y comúnmente aceptado en la industria.

PREGUNTA 5. Solicitamos el favor de definir los criterios que debe cumplir un mecanismo de protección datos para los diferentes tipos de comunicación, como son por vía inalámbrica. Ethernet con IP publica fija, o IP a través de firewall, fibra óptica, satelital, línea telefónica e intranet.

RESPUESTA

Como está previsto en el numeral 3.1 de los Acuerdos 701, 1004 y 1043, los mecanismos de protección de datos deben brindar integridad y confidencialidad de la información transmitida.

Entendiendo por integridad como el conjunto de condiciones que deben cumplir los datos para garantizar que la información se mantiene sin cambios, a menos que las modificaciones sean autorizadas, es decir que la información debe llegar a su destino sin cambios. Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

cno

Consejo Nacional de Operación

Por confidencialidad como la propiedad del sistema de información que consiste en garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

Atentamente,

Alberto Olarte

ALBERTO OLARTE AGUIRRE
Secretario Técnico

CC: Dra. Olga Pérez
Secretaria Técnica CAC

Dra. Lina Maria Ruiz Sierra
Dirección Información Operación y Mercado

Av. calle 26 No. 69-63 Oficina 408 Teléfonos: 7023029 – 7023026 - 7021892
E-Mail aolarte@cno.org.co - Internet: www.cno.org.co - Edificio Torre 26
Bogotá, D.C.- Colombia