Consejo Nacional de Operación

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

1. Objetivo

Mediante el presente documento se definen 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.

2. Antecedentes

La CREG a través de la Resolución 038 de 2014, por la cual se modifica el Código de Medida contenido en el Anexo general del Código de Redes, en su artículo 17 establece:

Artículo 17. 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 parágrafo de este artículo.*

Los niveles de acceso que trata el literal b) son:

1. *Nivel de acceso 1: Lectura de la identificación de la frontera comercial, las mediciones realizadas y los parámetros configurados en el medidor.*
2. *Nivel de acceso 2: Configuración de las funciones de tiempo y/o fecha, calibración, configuración de los parámetros y restauración del equipo así como el nivel anterior.*

El representante de la frontera debe administrar el acceso al medidor, estableciendo una lista de usuarios, contraseñas y niveles de acceso otorgados, además debe mantener un registro de los accesos al medidor de Nivel de acceso 2 en la hoja de vida de que trata el artículo 30 de esta resolución, cuando aplique.

El registro de acceso debe identificar como mínimo la fecha y hora de acceso, la persona o funcionario, propósito del acceso, actividades realizadas y la constancia de que el medidor quedó operando correctamente.

La base de datos que almacene las lecturas de los equipos de medida de las fronteras comerciales debe contar con niveles de acceso para consulta y mantener logs de registro de la afectación, ya sea modificación, adición o borrado de la información almacenada en esta.

Los sistemas de protección de datos deben contar con un procedimiento detallado y documentado que evidencie el cumplimiento de los requisitos de este artículo y establezca las políticas y lineamientos de seguridad física e informática existentes para la protección de la información.

Cuando se realice un cambio del representante de la frontera comercial, el RF saliente debe entregar la información de usuarios y contraseñas, así como el registro de los accesos de Nivel de acceso 2 al medidor y la configuración del mismo. La información deber ser suministrada en un plazo no mayor a cinco (5) días hábiles y no podrá afectar los procesos de registro y la fecha de entrada en operación comercial de la frontera por el cambio de representante.

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.

Todos los agentes que tengan acceso a las lecturas de las mediciones de acuerdo con lo señalado en el artículo 22 deben aplicar los requisitos legales vigentes sobre la protección de datos de los usuarios."

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. (…)

Adicionalmente, en el numeral 5 del literal a) del Anexo 8 de la Resolución CREG 038 de 2014 se prevé lo siguiente:

"El procedimiento empleado para la interrogación, el almacenamiento, la consolidación de las mediciones en el CGM y el reporte de estas al ASIC deber ser automático."

3. Condiciones mínimas de seguridad e integridad para la transmisión de lecturas desde los medidores hacia el Centro de Gestión de Medidas (CGM) y entre este último y el Administrador del Sistema de Intercambios Comerciales (ASIC)

Los CGM deben adoptar las condiciones mínimas de seguridad e integridad establecidas en el presente documento, bajo los siguientes criterios base y las funcionalidades mínimas exigidas en la Resolución CREG 038 de 2014 y aquellas que considere el agente puedan facilitar la gestión de la administración de la información.

3.1. Definiciones:

Flexibilidad: Es la capacidad que tiene un sistema de información de adaptarse a nuevas condiciones de operación sin afectar su desempeño.

Escalabilidad: Es la capacidad de un sistema de información de acoplarse con nuevos módulos funcionales mediante sus interfaces con el fin de mejorar sus capacidades, brindar nuevos servicios o adaptarse a nuevas condiciones operativas.

Interoperabilidad: Es la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada[1].

La seguridad de la información: Es el conjunto de medidas preventivas que permiten resguardar y proteger la información, buscando mantener la confidencialidad, disponibilidad e integridad de la misma, además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad[2].

Confidencialidad: Es 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[3].

[1] Definición IEEE
[2] Definición de NTC-ISO/IEC 27001
[3] Definición de NTC-ISO/IEC 27001

Integridad: Es 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.

No-repudio: Se previene la negación de la autoría de una acción que tuvo lugar o reclamar la autoría de una acción que no se llevó a cabo.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por una entidad (Persona, organización, proceso, etc.) autorizada cuando ésta lo requiera[4].

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad[5]

Confiabilidad de un Sistema de Información: Un sistema de información es confiable cuando ejecuta o desarrolla sus funciones correctamente dentro de unas condiciones establecidas y procesa la información con características de calidad aceptables acorde con las políticas y requerimientos predefinidos.

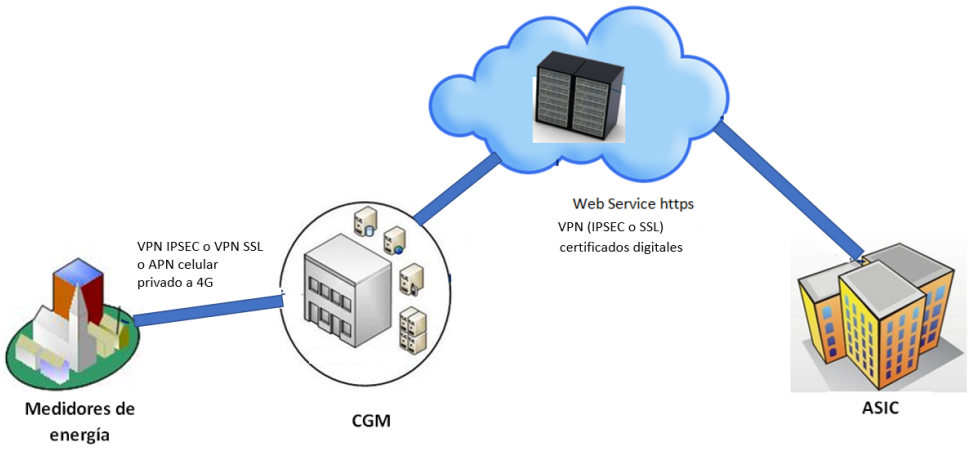
3.2. Funcionalidades mínimas:

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.

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

[4] Definición de NTC-ISO/IEC 27001, ISO/IEC 13335-1:2004
[5] Definición de NTC-ISO/IEC 27000

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.

Los niveles mínimos de seguridad para los cuatro (4) subsistemas involucrados para etapas de la transmisión de la información, desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC, serán:

a) **Medidor**: Para establecer comunicación del usuario con el medidor se deben cumplir como mínimo los siguientes requerimientos:

i. *Clave o contraseña:* funcionalidad disponible y configurable en el medidor.

- ✓ Esta clave será única por nivel de acceso en cada medidor.
- ✓ Política de reemplazo de manera periódica. La periodicidad de cambio de la clave o contraseña deberá ser definida por cada Representante de la Frontera RF, sin exceder un periodo de dos años.
- ✓ Se debe establecer un estándar de seguridad para cada tipo de medidor de acuerdo con las mejores características disponibles en este.
- ✓ Las claves deberán establecerse usando las características de seguridad máximas disponibles en el medidor.

ii. *Pérdida de comunicación remota*: En el caso de que no se disponga de comunicación remota, se deberá contar con una funcionalidad para que una vez se realice la interrogación local del medidor a través del software
propietario, se permita el cargue de la información del archivo descargado en sitio al CGM, generando la respectiva trazabilidad del evento en el sistema (registro en medidor y CGM).

iii. Sincronización: Debe garantizar la sincronización de la hora local de los medidores en sitio, o de manera remota a través del CGM.

iv. Parámetro de Identificación: Número de serie del medidor. Solo se podrá descargar información del medidor si su número de serie corresponde con el indicado en la Hoja de Vida; si la descarga es remota a través del CGM, esta funcionalidad será desarrollada de forma automática por el CGM.

v. El medidor debe proporcionar la funcionalidad para preservar la integridad de los datos almacenados, incluyendo la integridad del firmware.

b) **Requisitos del CGM**

i. Deberán utilizarse mecanismos de autenticación y autorización que permitan identificar al usuario que accederá al CGM

ii. Deberán mantenerse registros de acceso y de actividad por lo menos por dos (2) años, los cuales deben contener como mínimo la siguiente información:

- Fecha y hora de acceso
- Identificación (usuario)
- Registro de las actividades realizadas
- Registro de todas las modificaciones hechas en el medidor.

iii. Se debe incluir medidas de seguridad en los datos para protegerlos de corrupción, fraude, manipulación y acceso no autorizado.

iv. Dependiendo del tipo de comunicaciones físicas se deben apropiar protocolos de seguridad para asegurar que los datos sean protegidos durante la comunicación.

v. Se deben proveer métricas para mantener un sistema seguro y confiable. La siguiente lista es un ejemplo de un posible set de

métricas pero otras métricas normalmente provistas por los sistemas son aceptables:

- Falla del enlace
- Cambio de enlace
- Levantamiento de enlace
- Calidad de enlace

vi. El sistema debe ser capaz de garantizar la integridad de datos intercambiados en todo momento. Es necesario asegurar que los datos no son modificados por cualquier entidad no autorizada durante la comunicación o el acceso local a los datos. Para esto, se deben implementar algoritmos de encriptación de la información transmitida entre los elementos que hacen parte del sistema de comunicación.

c) Acceso a la base de datos desde el CGM

i. Deberán utilizarse mecanismos de autenticación y autorización que permitan identificar al usuario que accederá a la base de datos que almacena las medidas a través del CGM para consulta.

ii. Deberán mantenerse registros de acceso y de actividad por lo menos por dos (2) años, los cuales deben contener como mínimo la siguiente información:

- Fecha y hora de acceso
- Identificación (usuario)
- Registro de las actividades realizadas (modificación, adición o borrado de la información almacenada)
- Propósito según el nivel de acceso
- Registro de todas las modificaciones hechas en la base de datos.