TÍTULO DEL TRABAJO DE GRADO

ESTRATEGIAS DE SEGURIDAD EN SMART GRIDS

AUTORES

DAVID FERNANDO GALVIS CASTELLANOS 1098803412

UNIDADES TECNOLÓGICAS DE SANTANDER
FACULTAD DE CIENCIAS NATURALES E INGENIERÍAS
TÉCNICO PROFESIONAL EN INSTALACIÓN DE REDES ELÉCTRICAS
BUCARAMANGA
29 DE MAYO DE 2018

TÍTULO DEL TRABAJO DE GRADO
ESTRATEGIAS DE SEGURIDAD EN SMART GRIDS

AUTORES
DAVID FERNANDO GALVIS CASTELLANOS 1098803412

Trabajo de Grado para optar al título de:
TÉCNICO PROFESIONAL EN INSTALACIÓN DE REDES ELÉCTRICAS

DIRECTOR
FABIO ALFONSO GONZÁLEZ

GRUPO DE INVESTIGACIÓN EN ENERGÍA- GIE

UNIDADES TECNOLÓGICAS DE SANTANDER
FACULTAD DE CIENCIAS NATURALES E INGENIERÍAS
TÉCNICO PROFESIONAL EN INSTALACIÓN DE REDES ELÉCTRICAS
BUCARAMANGA
29 DE MAYO DE 2018

Nota de Aceptación

_____

_____

_____

_____

_____
Firma del jurado

_____
Firma del Jurado

DEDICATORIA

Quiero dedicar este trabajo que representa la culminación de un ciclo en mi carrera profesional a mi familia quien fue mi base para lograr esta meta en mi vida y siempre me apoyaron en este duro camino para ser un gran profesional.

A mi madre y mi abuela quien ya se encuentra en el cielo, quienes me enseñaron que no hay que rendirse en cada adversidad que se nos presente en el camino de la vida y que los trabajos o actividades que se desempeñen en la vida laboral hay que hacerlas con dedicación y amor.

A mi hermano y mi padre que fueron de gran apoyo para culminar este ciclo de mi carrera profesional.

AGRADECIMIENTOS

Quiero agradecer de todo corazón a los profesores del área de electricidad quienes me aportaron un pedazo de conocimiento de cada uno y a mi tutor del proyecto Fabio Alfonso González quien fue de gran ayuda para mí, por haber aportado su conocimiento dedicación y paciencia para culminar mi trabajo.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN EJECUTIVO

La siguiente investigación se direccionó a las redes inteligentes (Smart grids) y sus respectivos dispositivos de medida como lo son los Smart meters, donde se trabajaron cuatro objetivos especialmente; se buscó indagar acerca del sistema de seguridad que tiene cualquier red de telecomunicación y en este caso de telemedida para conocer sus puntos débiles donde algún malware pueda ingresar a la red y causar daños al sistema. En segunda medida se busca identificar si estos sistemas de seguridad se pueden implementar a los Smart grids, además de describir los nuevos sistemas de seguridad en una red o el mejoramiento de los existentes; el tercer objetivo es conocer la dimensión y el esquema tanto interno como externo del Smart meter y así entender el funcionamiento de él y cuál es la diferencia del medidor de energía eléctrica convencional; El último objetivo pero no menos importante es indagar la infraestructura de una base centralizada en donde se procese y almacene toda la información que arroja el Smart meter.

El proyecto de forma indirecta realiza la importancia del uso de las energías alternativas y el beneficio que traerá a la generación de energía eléctrica con las posibilidades que proporciona el planeta, ya sea solar, eólica, hidráulica entre otras, y de esta forma procurar al medio ambiente y al usuario con una energía más limpia.

PALABRAS CLAVE. Comunicación, Redes Inteligentes, Seguridad, Smart Grids, Smart meter

INTRODUCCIÓN

La energía eléctrica se ha convertido en un recurso vital para el desarrollo de nuestra sociedad, sin embargo, la demanda máxima se ha incrementado en las últimas décadas ya que gran parte de las cosas que se hacen en la cotidianidad requieren del suministro eléctrico, y su infraestructura de distribución es casi obsoleta; por esta razón las entidades que trabajan en innovación y tecnología promueven el desarrollo de alternativas de eficiencia para que el nuevo sistema de distribución de energía eléctrica sea fiable y seguro.

Los Smart grids consiste en un conjunto de redes de comunicación, distribución y transporte de energía eléctrica, donde crean un sistema bidireccional entre el usuario final y las empresas comercializadoras del servicio de energía eléctrica para que dicha función sirva para enviar la información de consumo al centro de datos y almacenamiento para que sea procesada y permita ser más eficiente el servicio de energía eléctrica y al mismo tiempo cada usuario obtenga información de posibles actualizaciones del sistema o avisos de desconexión del servicio para reparaciones de fallas detectadas en menor tiempo; los Smart grids también adquieren la posibilidad de hacer más sencilla la integración a la red eléctrica la generación con fuentes renovables.

Cuando se habla de Smart grids, también se hace mención al equipo de medida inteligente, mejor conocido como (Smart Meters), este dispositivo cumple con la misma función de un medidor de energía convencional que es medir el consumo de energía, además el Smart meter tiene la capacidad de comunicar el medidor con el centro de datos o con otro smart meter y al mismo tiempo puede recibir información que le envíe el centro de datos; uno de los retos principales es la gestión y control del consumo eléctrico, para que el usuario tenga la capacidad de promover el ahorro de energía; estos equipos inteligentes también son aplicados para los demás servicios públicos como lo son el agua y gas, pero en este documento solo se hablará del funcionamiento que trae en sí para el servicio de energía eléctrica.

Con la implementación de los Smart grids al sistema de energía eléctrica, las empresas de generación y distribución eléctrica buscan reducir las interrupciones del servicio debido a la poca interconectividad de los medidores convencionales y el sistema de distribución; la innovación para el sistema de comunicación en Smart grids busca varios aspectos para ser eficientes y confiables tales como la interconectividad de distintas redes de comunicación, gestión y control de datos, mejoramiento de velocidad y cobertura de señal inalámbrica y demás.

La seguridad de información se ha convertido en un tema bastante importante para la implementación de los Smart grids y Smart meters, ya que en medio del envío de datos hacia un centro de datos se pueden ocasionar posibles pérdidas de información y fraudes; para dicha protección se crean distintos protocolos de seguridad para permitir que el sistema sea seguro y confiable.

1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

Actualmente el funcionamiento de la transmisión y distribución de la energía eléctrica efectúan parte de las expectativas, pero cuando llegan al usuario final se generan problemas y no cumplen con lo que se esperaba. Durante el paso de los años, las estadísticas indican que se tendrá un sobrio crecimiento de la demanda, una fuerte alza de las energías renovables y una necesidad de potencia balanceada y estable.

Con el paso del tiempo, los combustibles fósiles como lo son el carbón, combustóleo y gas natural se van agotando en el mundo y cada vez son más caros para las plantas de generación de energía eléctrica; estos combustibles tienen un poder calorífico que están directamente asociados a sus componentes de carbono y de hidrógeno que complican el proceso de generación y crean unos derivados que afectan notable y negativamente al medio ambiente. (Martin, 2001)

Por otra parte, surge el problema de los picos de demanda que exige a las empresas generadoras de energía al activar plantas especiales para la satisfacción de estas necesidades que son únicamente utilizadas en estos lapsos de tiempo ya que afectan directamente a las facturas que el usuario paga. Para ello se implementarían los contadores inteligentes o mejor conocidos como Smart meters, que ayudarán a la combinación de las energías renovables, pero tendría incidencias de una eventual amenaza como lo es la interrupción de la red eléctrica, pérdida de disponibilidad del sistema y control de la red eléctrica. (Diaz Andrade & Hernandez, 2011)

En la actualidad, el buen funcionamiento de la energía eléctrica es muy alto, pero aún existe una gran pérdida de comunicación a la falta de electricidad en determinadas ocasiones ya que no hay un sistema íntegro de comunicación usuario-red como tal, por lo que en ocasiones las empresas no detectan apagones hasta que los usuarios no dan aviso y por consecuencia de ello, el fallo eléctrico no detectado a tiempo podría ocasionar un fallo en cascada debido a las sobrecargas que se producen. Los nuevos sistemas de Smart grids pueden hacer que las empresas distribuidoras de energía eléctrica tengan un conocimiento de toda la red para que puedan detectar un fallo a priori y tengan una reacción rápida.

Otro tema de preocupación es la inversión a nuevas infraestructuras ya que las actuales que están haciendo la generación de energía eléctrica fueron creadas hace muchos años y por lo tanto tienen una tecnología muy arcaica; si se hace esta inversión a las nuevas infraestructuras se abrirán las puertas a sistemas y procesadores inteligentes y más rápidos la cual harán que la generación,

distribución y la gestión de energía sea más económica. (Observatorio Industrial del sector de la electronica, 2011)

Con lo expuesto anteriormente se propone resolver la siguiente pregunta de investigación: ¿Qué estrategias de seguridad, se han propuesto para evitar la pérdida de información en redes inteligentes?

1.2. JUSTIFICACIÓN

La integración de las redes inteligentes son el futuro de las distintas ramas de electricidad, ya sea generación, distribución o comercialización, pero la infraestructura que se tiene en el presente no está diseñada para las nuevas tecnologías que se espera el mundo moderno, con el paso de los días, la demanda de la energía eléctrica va en dirección creciente y para la generación de estos picos de demanda se implementan plantas generadoras de electricidad que son las causantes de CO_2 (Dióxido de Carbono) las cuales provocan el efecto invernadero; la importancia de la implementación de los Smart grid en un país en desarrollo como lo es Colombia sería significativa, ya que reducirán los reportes de fallas, harán una mejor lectura en los medidores y detectarán el robo de energía. (Leguizamón, 2015)

Con la llegada de los Smart grids, los operadores de potencia de energía eléctrica llegarán al tope de su funcionamiento debido a las altas demandas de energía, si esta situación llegase a suceder, se podría presentar un estado de vulnerabilidad al sistema, por lo cual se han estudiado diversas situaciones para tener estudios más a fondo y tener controlado cada punto de colapso del sistema (Velasco Martinez, Angeles Camacho, & Garcia Martinez, 2012)

En caso que los Smart meters no cumplan con el objetivo de la infraestructura de la seguridad, se podrían ocasionar diferentes anomalías al sistema como el fraude y pérdida de privacidad del usuario consumidor de la energía eléctrica; podría afectar la parte económica para las compañías creadoras de estos contadores como a las compañías generadoras, ya que un fallo en la seguridad puede llegar a manipular las lecturas del contador y llegarle información falsa a la central de datos, otra posibilidad entre muchas sería el manejo del control de conexión y desconexión de la red eléctrica remota que podría afectar a millones de usuarios. (Spain, 2016)

Esta investigación es muy importante y vital llevar a cabo ya que sería abrir las puertas a la nueva generación de la tecnología y tener conocimiento sobre lo que sustentará el día de mañana; el conocimiento de esta investigación también será muy importante para las UTS y en particular para el grupo de Investigación en Energía GIE, ya que esta tecnología cobijará a todos y podrán así sacarles provecho a los resultados logrados con este trabajo.

1.3. OBJETIVOS

1.3.1 OBJETIVO GENERAL

Determinar las características de seguridad que deben cumplir los equipos utilizados en los sistemas distribuidos de energía, evaluando las estrategias que se proponen para reducir la vulnerabilidad ante ataques a los que puedan ser expuestos

1.3.2 OBJETIVOS ESPECÍFICOS

- Establecer márgenes de error que tienen los Smart meters para saber qué tan vulnerables son ante un ataque mediante la revisión de la estructura de los existentes.

- Determinar las herramientas software que se pueden utilizar para incrementar la seguridad en las redes inteligentes.

- Presentar la estructura típica de un Smart meter, para identificar su modo de operación y determinar su eficiencia en las redes inteligentes.

- Definir la infraestructura que se requiere para implementar estrategias de seguridad que garantice un buen funcionamiento de la red en toda su estructura.

2. MARCO REFERENCIAL

2.1. MARCO AMBIENTAL

Como tal, el entorno de seguridad para los Smart grids no tiene represalias con el medio ambiente ya que no requiere recursos naturales significativos, sin embargo, se busca implementar las energías renovables para que se acoplen con los Smart grids y así generar el cambio del pensamiento y habito del consumo de energía eléctrica del usuario final**.** Gracias a esto, se consigue *igualar la curva de consumo diaria*, de manera que el consumo de energía se reparta de manera uniforme y así evitar los altos índices de picos de demanda, maximizando el aprovechamiento de las infraestructuras actuales y la utilización de las energías no convencionales. (Ecointeligencia, 2014)

La implementación de los Smart grids en las ciudades sostenibles dará una solución al cambio climático ya que estos producirán menos emisiones de gases de efecto invernadero a través de un incremento en la eficacia y la implementación de las energías renovables. En diciembre de 2011 en Estados Unidos se hizo un estudio donde revelaba que las energías renovables limpias generaban una capacidad instalada de 565 GW, donde contaba con la participación de la energía eólica 239 GW, centrales hidroeléctricas 184 GW, energía de residuos y biomasa 57 GW, energía fotovoltaica 73 GW, energía geotérmica 11 GW, y la energía de las corrientes marinas 0.6 GW; con la ayuda de los Smart grids optimizará la integración y fiabilidad de estos recursos de energía renovable en la infraestructura de la red existente. (Lee, Paredes, & Lee, 2012)

2.2. MARCO LEGAL

De acuerdo con lo expuesto en la ley 1715 de 2014, “se tiene como objetivo iniciar el desarrollo y la utilización de las fuentes no convencionales de energía, principalmente aquellas de carácter renovable, en el sistema energético nacional, mediante su integración al mercado eléctrico, su participación en las zonas no interconectadas y en otros usos energéticos como medio necesario para el desarrollo económico sostenible, la reducción de emisiones de gases de efecto invernadero y la seguridad del abastecimiento energético. Con los mismos propósitos se busca promover la gestión eficiente de la energía, que comprende tanto la eficiencia energética como la respuesta de la demanda”.

La finalidad de la presente ley fue “establecer el marco legal y los instrumentos para la promoción del aprovechamiento de las fuentes no convencionales de energía, principalmente aquellas de carácter renovable, lo mismo que para el fomento de la inversión, investigación y desarrollo de tecnologías limpias para producción de

energía, la eficiencia energética y la respuesta de la demanda, en el marco de la política energética nacional. Igualmente, tiene por objeto establecer líneas de acción para el cumplimento de compromisos asumidos por Colombia en materia de energías renovables, gestión eficiente de la energía y reducción de emisiones de gases de efecto invernadero, tales como aquellos adquiridos a través de la aprobación del estatuto de la Agencia Internacional de Energías Renovables (Irena) mediante la Ley 1665 de 2013". (Senado de Colombia, 2014)

En la resolución 40072 del 29 de Enero de 2018 "establece los mecanismos para incorporar la infraestructura de medición avanzada en el servicio público de energía eléctrica, en donde define una ruta para la integración de los Smart Grids en la nación colombiana haciendo reconocer que la infraestructura de medición avanzada es una de las tecnologías habilitadoras para la implementación de las demás tecnologías en redes inteligentes".

De acuerdo a esta norma, la Comisión de Regulación de Energía y Gas (CREG), tendrá un plazo de un año (12 meses) para establecer las condiciones en la integración de la infraestructura de medición avanzada en la prestación del servicio público domiciliario de energía eléctrica en el Sistema Interconectado Nacional (SIN). Los objetivos propuestos son los enunciados a continuación:

- Facilitar esquemas de eficiencia energética, respuesta de la demanda y modelos de tarifación horaria.
- Permitir la incorporación en los sistemas eléctricos, entre otras, de tecnologías de autogeneración, almacenamiento, generación distribuida y vehículos eléctricos.
- Mejorar la calidad del servicio a través del monitoreo y control de los sistemas de distribución.
- Dinamizar la competencia en la comercialización minorista de energía eléctrica y generar nuevos modelos de negocio y servicios.
- Gestionar la reducción de las pérdidas técnicas y no técnicas.
- Reducir los costos de la prestación del servicio de energía eléctrica.

Las funciones propuestas se listan a continuación:

- Almacenamiento: Permitir el almacenamiento de datos en el medidor avanzado.
- Comunicación Bidireccional: Permitir la comunicación en dos direcciones con el usuario y los elementos de la AMI.
- Ciberseguridad: Brindar soporte de comunicaciones de datos seguras.
- Sincronización: Permitir la sincronización automática y remota de tiempos entre el medidor avanzado y la AMI.

- Actualización y Configuración: Posibilitar la actualización y configuración local y remota del medidor avanzado referente al software, intervalos de lectura, tarifas, entre otros.
- Acceso al Usuario: Proporcionar información al usuario a través de un medio de visualización normalizado que puede ser, entre otros, plataformas web, computadores, aplicaciones para telefonía móvil o monitores exclusivos.
- Lectura: Permitir la lectura local y remota de las variables y eventos generados por el medidor avanzado.
- Medición Horaria: Soportar la implementación de esquemas de opciones de tarifas horarias.
- Conexión, Desconexión y Limitación: Permitir de forma remota y local la conexión, desconexión y la limitación del suministro de energía.
- Anti-fraudes: Facilitar la prevención y detección de fraudes.
- Registro de medición bidireccional: Permitir la medición y registro de las transferencias de energía en dos direcciones, desde y hacia la red eléctrica o de entrada y salida del medidor avanzado.
- Calidad del servicio: Proporcionar medidas sobre la duración de las indisponibilidades en el servicio de energía eléctrica.
- Prepago: Soportar la implementación de modo prepago, permitiendo al usuario pagar el servicio de energía por adelantado. (Ministerio de Minas y Energía, 2018)

2.3. MARCO TEÓRICO

Las redes inteligentes o comúnmente llamadas Smart Grids son redes de distribución eléctricas combinadas con recientes tecnologías de información que pueden acoplar de manera inteligente la conducta y las acciones de los usuarios conectados, ya sean los generadores o consumidores que tiene el fin que la red eléctrica sea eficiente, sostenible, económica y tenga la capacidad de garantizar el abastecimiento de electricidad. (Rubia, 2011)

Las Smart grids van de la mano con las energías renovables, ya que uno de los objetivos de las Smart grids es reducir las emisiones de gases de efecto invernadero, y estas son alternativamente más limpias para el medio ambiente ya que se encuentra en nuestro planeta como fuentes ilimitadas cuya marca de contaminación es prácticamente nula (Calvo, 2012), algunas de las energías renovables son:

ENERGÍA HIDRÁULICA: Su concepto se generaliza en producir energía eléctrica haciendo valer el despliegue del agua desde una altura considerable, es decir, se consigue de la producción de la energía cinética y potencial de la fuerza y del flujo

del agua; dentro de su proceso, hace que el agua desembalsada baje con cierta potencia y así generar una rotación constante en la turbina, por medio de esta rotación constante se deriva la energía cinética y está es transformada a energía eléctrica. (Gonzalez, 2012)

ENERGÍA EÓLICA: Es una de las formas de energía solar ya que los vientos son ocasionados por el calentamiento disparejo de la atmosfera por el sol, también son causadas por las alteraciones de la superficie y la propia rotación de la tierra (Tecnología, 2013); este recurso es una de las energías más exuberantes y renovables de la naturaleza. Deriva de la transformación de la energía cinética que traen las masas de aire en movimiento hacia energía mecánica y luego a energía eléctrica. (Vercelli, 2012)

ENERGÍA SOLAR: La energía solar proviene de la emisión electromagnética del sol, con base a esta energía solar se puede obtener energía eléctrica de dos maneras distintas:

- Transformación térmica en temperatura elevada: Su distinción radica en incorporar unos colectores para convertir la energía que emite el sol, en energía eléctrica.
- Conversión Fotovoltaica: Para ellos son utilizadas unas plataformas o paneles solares para transformar la energía solar en energía eléctrica. (Edenhofer, y otros, 2011)

ENERGÍA GEOTÉRMICA: Es una de las energías renovables menos conocidas pero su utilización en sí es realmente provechosa para el consumo de los usuarios; está aprovecha el calor del interior de la tierra y climatizar aguas y ser utilizadas a través de bombas geotérmicas (calefacción y refrigeración) para generar energía eléctrica. (Gonzalez, 2012)

En la mayoría de los países industrializados como Estados Unidos, Brasil, Arabia Saudita y México los medidores de energía están siendo totalmente cambiados por medidores electrónicos y digitales, sus ejemplares más avanzados son nombrados como contadores inteligentes o Smart meters; una de las cualidades de un contador inteligente es que es bidireccional (transmitir y recibir información), su función es medir el consumo de energía como lo hace un medidor cotidiano, pero éste tendrá la capacidad de comunicación permitiendo que los datos sean monitoreados remotamente y se muestren en un aparato dentro de la casa o que su información sea transmitida al exterior de forma segura, como también podrá recibir información como lo son el coste de tarifas o cambiarlo al tipo pre pagado. A su vez el concepto de bidirección hace alusión de poder medir el flujo de potencia en ambas direcciones, una vía que entra al Smart meter de cada usuario, y otra que sale de este. (Sierra, 2012)

Actualmente en Colombia solo están llevando a cabo investigaciones sobre el impacto que pueda tener la implementación de estos dispositivos, puesto que la visión está planteada para el año 2030; lo más cercano que está Colombia a este avance tecnológico es al proyecto PRICE-GDE que es la gestión de la demanda, este proyecto se basa en el desarrollo de un sistema de monitoreo de consumo de los clientes diseñando nuevas vías de información hacia ellos, el sistema está fundamentado en protocolos abiertos e interoperables los cuales pretende optimizar el consumo eléctrico en su conjunto mediante contadores inteligentes (Smart meters). (UPME, 2016)

Para las industrias de generación y comercialización, el proyecto de Smart grids les parece muy atractivo ya que los bienes económicos y ambientales son innegables; sin embargo, los especialistas en seguridad informática afirman que el riesgo de tener un ataque al sistema informático está muy presente en el desarrollo del proyecto que puede afectar a la calidad del servicio y la privacidad del consumidor. (Rodriguez, 2012)

Cuando se habla de seguridad se tiene que hablar del sistema SCADA, que viene de las siglas: “Supervisory Control And Data Acquisition”, que quiere decir, sistema de adquisición de datos y control supervisor, en principio se crearon para acobijar las necesidad de un sistema de control centralizado para procedimientos industriales en áreas geográficamente muy grandes; pero con el paso del tiempo y el desarrollo de tecnologías inteligentes, este sistema está quedando por fuera del círculo de la seguridad y tendrá que ser modificado. (Corrales, 2007)

Actualmente el control de la protección de las redes eléctricas las tiene el sistema SCADA (Supervisión, Control y Adquisición de Datos) donde se define que es un sistema para realizar software para computadores que permite controlar y supervisar información y procesos industriales a distancia, pero este sistema tiene puntos débiles para la llegada de los Smart grids ya que no permite la autentificación del usuario, no percibe cuando entra un virus que puede robar información o dejar un daño permanente para ataques futuros.

En la distribución eléctrica, las Smart grids tendrán buen acoplamiento al sistema ya que traerán enormes beneficios tanto en el desarrollo tecnológico en nuestro país y en el plan de mejoramiento al medio ambiente; para satisfacción del usuario y del medio ambiente, las Smart grids tendrán una función en la distribución de energía eléctrica que será reunir y registrar cierta información en distintos sitios de su infraestructura, a partir de esa información el sistema tomará la mejor decisión para tener una mejor eficiencia en la distribución y en parte ayudará a reducir la pérdida de energía.

Los mecanismos de protección para los Smart grids se basará en el diseño de los Smart meters o contadores inteligentes que tendrán en sí coprocesadores para cifrar y descifrar la información, también tendrá ciertas herramientas para que las empresas de distribución y comercialización, puedan utilizar en la creación de algoritmos para ajustar el consumo de la energía del usuario. (Rodriguez, 2012)

3. ESTADO DEL ARTE

3.1. ESTRUCTURA DE LOS SMART METER

Las estructuras internas de las redes inteligentes contienen dos secciones que gracias a ellas se les puede llamar “inteligentes”; la primera sección trae consigo una red de distribución que contiene líneas de distribución de energía eléctrica y fuentes de energía convencionales y no convencionales como lo son las hidroeléctricas, quema de combustibles fósiles y energía fotovoltaica, campos eólicos respectivamente. (Rodriguez, 2012)

La segunda sección de una red inteligente es la red de datos, en donde se encuentran los dispositivos de medición inteligente llamados Smart meter, centros de almacenamiento y procesamiento de datos, y sistemas que recolecten dichos datos; los Smart meter son dispositivos de medición inteligente que contienen un hardware que a su vez tienen procesadores, diferentes velocidades de frecuencia, almacenamiento interno y memoria RAM con distintas capacidades según su fabricante. (Rodriguez, 2012)

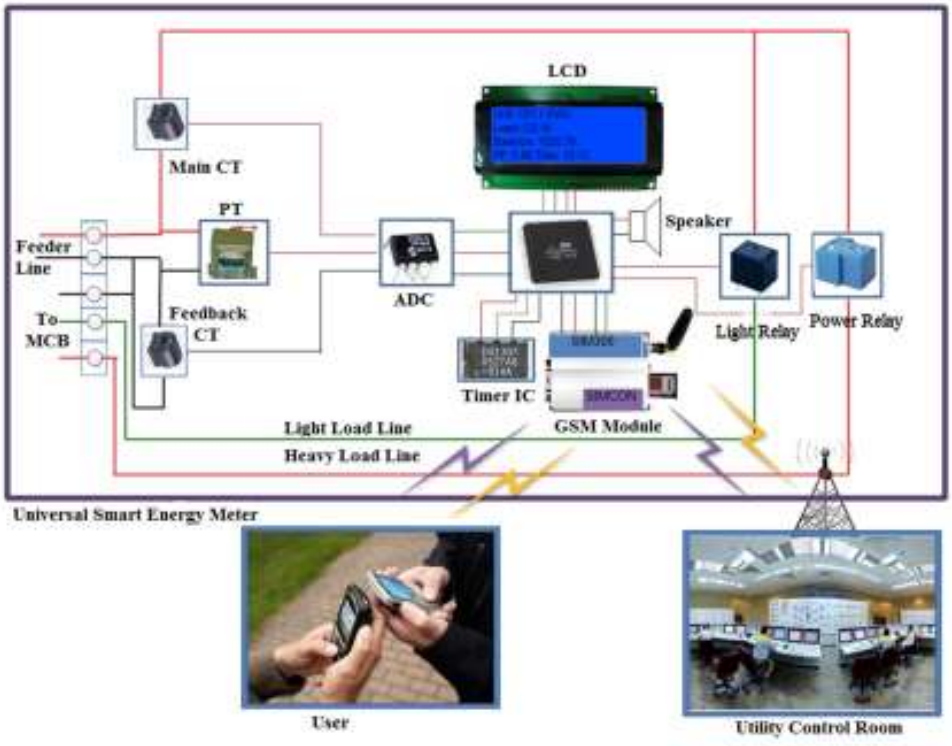
El Smart meter ha sido una idea bastante sólida tanto para las empresas generadoras de energía como para los usuarios que consumen dicha energía, ya que proporciona diferentes aplicaciones que no se encuentran en los medidores electromecánicos y electrónicos tales como la lectura de energía consumida en tiempo real, sistemas bidireccionales, conexión y desconexión remota del sistema, detección de fallas en tiempos mínimos y demás; en la actualidad existe la posibilidad de tener energía prepagada, donde se otorgan beneficios y genera satisfacción para el consumidor, sus principales beneficios son la rentabilidad, eficiencia y mejoramiento del sistema. (Labib, y otros, 2017)

Una de las alternativas más atractivas para la medición inteligente es por medio de la comunicación celular; la red móvil tiene varias ventajas gracias a su buena cobertura de señal, su amplia opción de ahorro de dinero y tiempo para la construcción de una infraestructura que sea viable para la telecomunicación, además, un estudio reveló que la población mundial tiene más accesibilidad a la red móvil que a la disponibilidad de suministro de energía eléctrica que sea fiable; en países de bajos recursos o también llamados tercermundistas se fortalece esta posibilidad de medición inteligente y así obtener mayor oportunidad de conexión de energía fiable y confiable para la gente de bajos recursos. (Labib, y otros, 2017)

En el diseño de los medidores inteligentes se planea conectar entre sí, tres aspectos que tengan una reacción en cadena, como lo es la interactividad del usuario con el Smart meter y la comunicación eficiente del medidor inteligente con el centro de control. En donde cada sujeto cumple un objetivo para el buen funcionamiento del

sistema de medida inteligente; el centro de control podrá tener acceso al ajuste o cambios de las tarifas, tendrá la autoridad de conectar y desconectar el medidor inteligente a la red, y si llegado el caso de una posible desconexión, el centro de control podrá reconectarlos; la función del medidor inteligente será tomar las lecturas del consumo de energía eléctrica y enviarlas de manera inmediata al centro de control, y por último conlleva al usuario final, quien envía los mensajes de confirmación hacia el centro de control después de cada operación que haga el Smart meter.

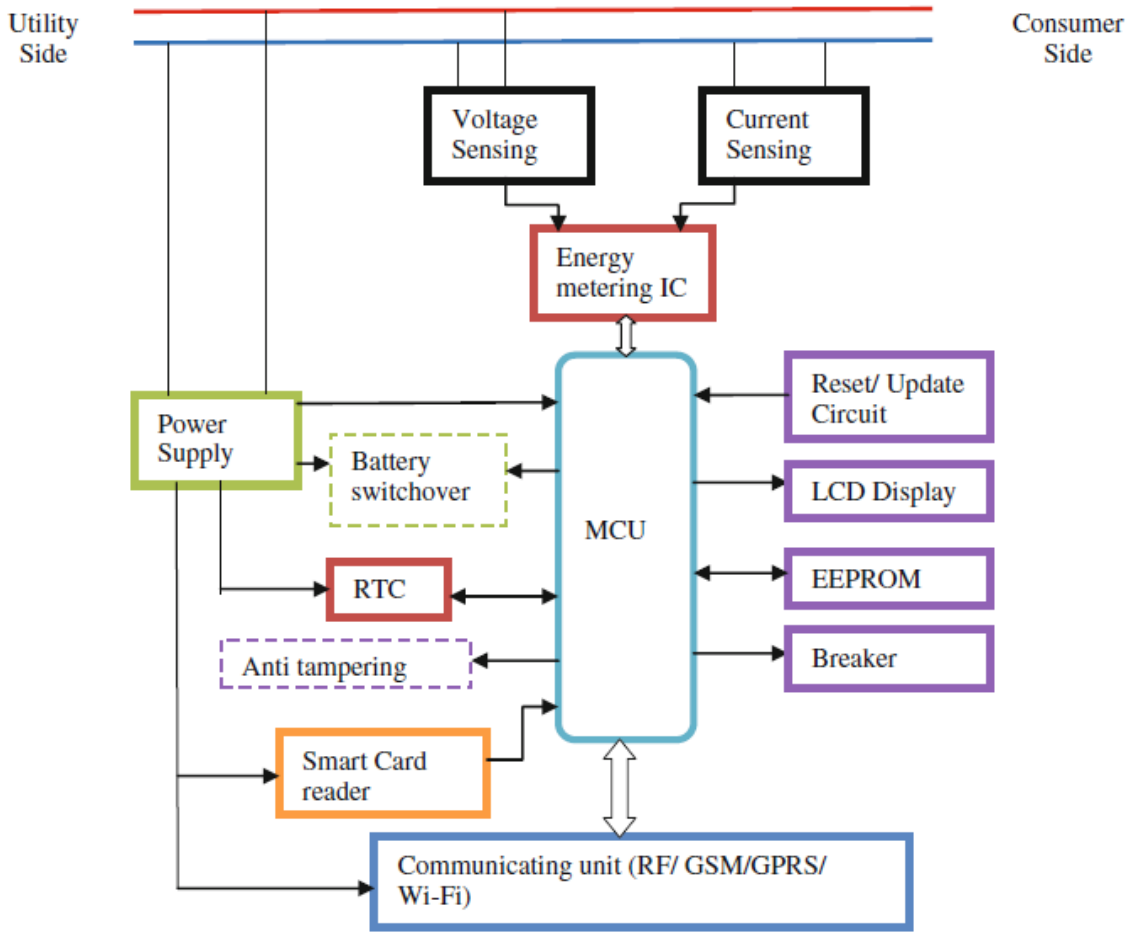
Figura 1. Intercomunicación Entre el Usuario, Medidor y Centro de Control



Fuente: (Labib, y otros, 2017)

En la Figura 2 se muestra un diagrama de bloques de los componentes de un medidor inteligente tales como, sistemas de comunicación, fuentes de alimentación, microcontrolador, sistemas de detección de diferencia de potencial y corriente, donde todos y cada uno de ellos se complementan entre sí para desarrollar funciones como la actualización del sistema, fecha y hora, almacenamiento y procesamiento de datos, y copias de seguridad

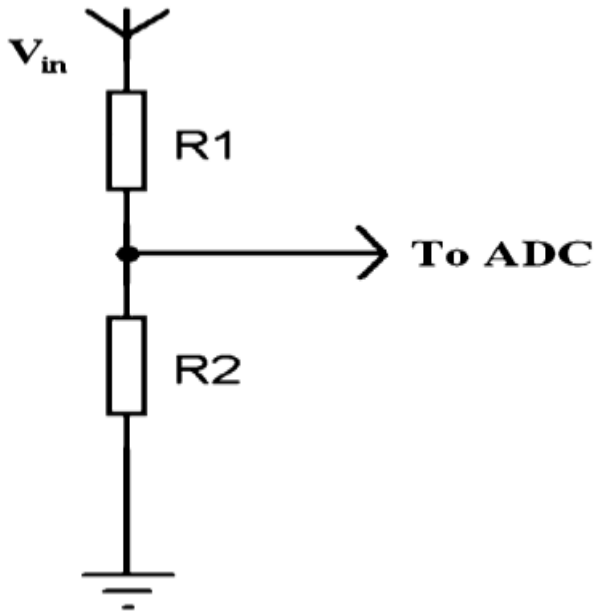
Figura 2. Estructura del Hardware de un Smart Meter



Fuente: (Weranga, Kumarawadu, & Chandima, 2014)

El sistema de detección de diferencia de potencial es un sensor que trae en su interior un conjunto de resistencias donde se configuran como un divisor, los valores de las resistencias son calculadas matemáticamente para que el voltaje de entrada sea divido y así acoplarse al rango del chip que toma las lecturas del consumo de energía; la tensión de entrada se le inyecta a la resistencia 1 (R1) y el nodo del medio hace referencia a la salida como se muestra en laFigura 3, la resistencia 2 (R2) va directamente conectado a la tierra. (Weranga, Kumarawadu, & Chandima, 2014)

Figura 3. Configuración de Resistencias



Fuente: (Weranga, Kumarawadu, & Chandima, 2014)

Así como hay sistemas de detección de tensión, también existen sistemas de corriente, donde se manejan distintos sensores de corriente que se pueden incorporar en los Smart meter, los más comunes son:

- -Resistencias Shunt
- -Sensores lineales basados en efecto Hall

Las resistencias shunt están diseñadas y fabricadas con un valor demasiado pequeño para no generar cambios cuando entre en contacto con la disipación de calor del Smart meter, estas resistencias se conectan en modo serie para que el paso de la corriente no tenga más caminos por donde pueda derivarse, conociendo el valor de las resistencias shunt y la corriente se puede hallar el voltaje y así obtener una señal de salida que se incorpora al chip de medida. (Weranga, Kumarawadu, & Chandima, 2014)

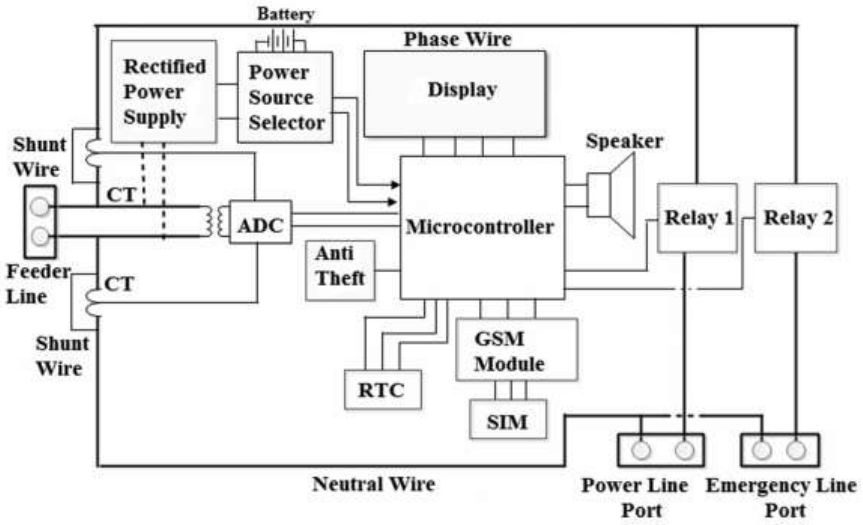
Los sensores de corriente basados en el efecto hall son dispositivos que traen en su interior un canal de conducción de corriente eléctrica, donde cumple la función

de transportar dicha corriente por el canal conductor y generar un campo magnético para tener como resultado una diferencia de potencial adecuada. (Weranga, Kumarawadu, & Chandima, 2014)

La Figura 4, presenta la estructura general desarrollada en el proyecto USEM, que traduce “medidor inteligente de energía universal”; en su interior se contemplan componentes tales como:

- Fuente de alimentación rectificada
- Selector de fuente de energía
- 2 Relés
- Microcontrolador ATmega2560
- Módulo GSM
- Entradas de alimentación
- Puerto de emergencia
- Reloj en tiempo real (RTC)
- TC.
- TP

Figura 4. Esquema Interno del Smart Meter



Fuente: (Labib, y otros, 2017)

Cada componente cumple con una función en específico. En su entrada contiene un TC y un TP quien transforma la corriente y el potencial eléctrico respectivamente y son inyectados directamente a un par de buses de 12 bits; el microcontrolador es alimentado por las señales digitales amplificadas de corriente y potencial eléctrico para cumplir con la función de calcular el producto VA “potencia activa”, los VAR “potencia reactiva”, el FP “factor de potencia”, y la energía consumida y con ello

ayuda a que el controlador LCD se actualice en tiempo real ; el funcionamiento del reloj en tiempo real (RTC) es tomar lecturas de energía consumida en tiempos reales, para cumplir con distintos objetivos como lo son el plan de factura moderada, actualización del software y avisos de conexión y desconexión de la red. (Labib, y otros, 2017)

De igual manera, el Smart meter tiene en su interior un sistema GSM (sistema global de comunicación móvil), el sistema GSM técnicamente se considera una tecnología antigua, ya que es de segunda generación (2G), pero gracias a este sistema se pudo y se puede mejorar aún más la calidad del transporte de comunicación e información, ya sean notas de audio, imágenes, videos, llamadas entre otras. El sistema GSM (sistema global de comunicación móvil), es un sistema que van de la mano con la red celular, ya que ambos son complementados por un amplio esquema de circuitos que manejan conjuntos de celdas, bandas, y frecuencias distintas para evitar interferencia entre ellos; este sistema crea comunicaciones de manera inalámbrica y funciona para todos los dispositivos que se consideran “SMART”, donde se traslada de un dispositivo a otro distintos tipos de datos; este sistema se maneja para los Smart meter por sus características de transporte de información y su rápida accesibilidad de usuarios en la misma vía sin interferir los datos de cada uno de ellos. La tarjeta SIM se utiliza como un mecanismo de seguridad para la protección del sistema GSM, ya que contiene en su interior el número telefónico, código del sistema operativo, código de identificación personal (PIN), código personal de desbloqueo (PUK), y el estado de la tarjeta SIM, donde todas estas características se complementan en conjunto para crear una clave y algoritmo de autenticación para asegurar la protección y privacidad de la información cuando se transporta por la red, y así evitar que la información no sea manipulada por terceras personas, utilizando claves cifradas o encriptadas. Para crear un sistema de autenticación se lleva a cabo cierto procedimiento donde se envía a un dispositivo inteligente un dígito aleatorio de 128 bits, el dispositivo inteligente hace una lectura de 32 bits con los datos del dígito aleatorio y el algoritmo cifrado de autenticación, al calcular la lectura de 32 bits del dispositivo inteligente, el sistema GSM verifica los cálculos para certificar la identidad del dispositivo, y finalmente, si los cálculos coinciden con el sistema GSM se podrá crear el puente de comunicación. (Porras, 2012)

Para su finalización se da a conocer en la Figura 5 la apariencia externa de un medidor inteligente de energía eléctrica.

Figura 5. Apariencia Externa del Smart Meter

Fuente: (Energetika, 2016)

Uno de los grandes desafíos que tiene el diseño y fabricación de un smart meter es la precisión de la lectura de las cargas; una posible solución para este tema es la creación de una lámina que en su interior traerá componentes como convertidores de potencial eléctrico, corriente alterna y relés para calibrar dicha lectura de la energía consumida. (Zakariae, Hajar, Belkasem, & Elhassane, 2017)

En la Figura 6 se muestra el funcionamiento de esta lámina de calibración, donde el convertidor de AC-AC crea una diferencia de potencial y una corriente alterna con un valor raíz media cuadrática o mejor conocido como RMS y así generar un cambio de fase entre la diferencia de potencial y la corriente; y el trabajo de los relés es el cambio de señal. (Zakariae, Hajar, Belkasem, & Elhassane, 2017)

- **Infraestructura de Medición Avanzada (AMI)**

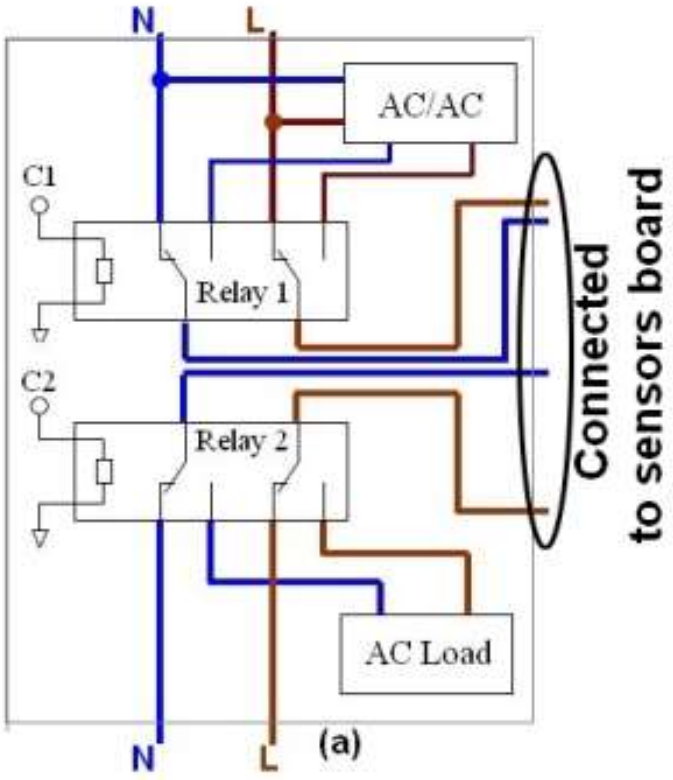
Una de los mayores beneficios que otorgan los Smart grids centradas en la parte eléctrica es la medición inteligente, ya que trae consigo dos vías o comúnmente llamados bidireccionales, donde podrá tomar lecturas de voltaje y corriente y enviarlas de manera remota a la central de datos, conectará y/o desconectará del servicio según sea la orden que se le dé al sistema de operación. (Ortega, 2012)

- **Sistema de Gestión de Cortes (OMS)**

A diferencia de los medidores electromecánicos y electrónicos, cuando se presentan problemas en ellos, las empresas comercializadoras del servicio energético no tenían conocimiento alguno, hasta que el usuario presentará un reporte de fallas en el equipo; con la gestión de cortes se podrá detectar el problema

en tiempo remoto y así tener una reparación o reconexión a la red de manera eficiente y ágil. (Ortega, 2012)

Figura 6. Diseño de Lámina de Calibración



Fuente: (Zakariae, Hajar, Belkasem, & Elhassane, 2017)

Tanto los equipos de medida inteligente como el sistema de medición avanzada traen muchos beneficios para el sistema eléctrico, sobretodo en la transmisión y comercialización del servicio de energía eléctrica. Tales beneficios son.

- Facturas de consumo de energía más exactas
- Lecturas en tiempo real
- Acoplamiento de energías renovables para generación de carga
- Detección de posibles fraudes
- Reparación de fallas en el sistema y mantenimiento en tiempos casi inmediatos
- Esquemas de precios variables (Hernandez, 2014)

3.2. FALENCIAS DE SEGURIDAD EN TECNOLOGÍAS INTELIGENTES

Aunque en Europa y América del norte ya se han hecho grandes avances con relación a los Smart meters y el buen uso de la energía con base a esta tecnología, aun se presenta uno de los grandes problemas que tiene el avance de los Smart grids como lo es la seguridad de ésta; a medida que esta tecnología vaya en crecimiento, presentará consigo unas falencias de seguridad como lo puede ser la falla en las lecturas de consumo de potencia en el usuario final de los Smart meters, lo cual representaría grandes pérdidas económicas para las empresas comercializadoras e industrias fabricantes de los equipos. (SPAIN, 2016)

Según un estudio, demostró que los sistemas de seguridad actuales como lo son (SCADA), no son muy válidos para las nuevas tecnologías que se quiere implementar en el sector eléctrico, ya que estos software no fueron creados para las necesidades de los Smart meters tales como la autentificación del usuario, sistemas de acceso y captación de intrusos al sistema (González, Galván Bobadilla, & Camacho Peréz, 2012)

El simple hecho de la integración de la tecnología inteligente al sistema de red eléctrica abre una gran grieta para la intrusión de virus y malware a la infraestructura del sistema; las consecuencias que puede traer estas intrusiones no solo afectaría a la distribución de red eléctrica, ya que esta infraestructura está interconectada entre sí con otras infraestructuras, como lo son las comunicaciones, el sistema financiero, bombeos y transporte de agua potable, servicios de salud y demás. (Sáez & Collado, 2015)

Así como existen virus y malware para provocar daños al sistema de la red eléctrica inteligente, también hay usuarios que buscan el objetivo de obtener el servicio eléctrico de manera más económica de forma ilegal alterando los datos en la infraestructura del sistema de la red eléctrica; también hay usuarios que buscan un daño más complejo, como lo es la obtención de información privada y la modificación de ella respectivamente, donde podría ocasionar interrupciones y apagones del servicio eléctrico; la clasificación de estos usuarios se les conoce como pasivos y activos respectivamente como se muestra en la Tabla 1, donde el pasivo se introduce al sistema buscando beneficio propio, mientras que el activo intenta hacer daños inminentes al sistema en general. (Sáez & Collado, 2015)

El servicio del plan prepagado del servicio eléctrico ha sido visto de buena manera por algunos usuarios, más, sin embargo, trae consigo mismo distintos puntos vulnerables que algunos usuarios no lo toman de la mejor manera; las críticas más destacadas son la falta de actualización del sistema, configuraciones del plan, y observando por el lado de los Smart grids, tiene poca compatibilidad con la microgeneración. (Labib, y otros, 2017)

Tabla 1. Ataques Malignos al Sistema Eléctrico

Según Amenaza	Objetivo De Seguridad Afectado	¿Activo o Pasivo?	Ejemplos
Intercepción (cuando personal no autorizado obtiene acceso a datos, dispositivos o componentes del entorno virtual	Confidencialidad	Pasivo (por lo general no puede ser afectado pero puede ser prevenido con criptografía)	Denegación de servicios (o "DOS" Denial of service), espionaje, monitoreo de tráfico de datos
Modificación (cuando se obtiene acceso y se realizan modificaciones a datos, dispositivos o componentes del entorno virtual de forma deliberada e ilegal)	Integridad	Activo (Puede ser detectado con criptografía)	Modificación de señales de control, modificación de datos de sensores, modificación de información
Interrupción (cuando datos, dispositivos o componentes del entorno cibernético son destruidos o convertidos en no disponibles con el objetivo de retrasar, bloquear o perjudicar la comunicación de la red inteligente)	Disponibilidad	Activo (Puede ser detectado pero por lo general no se previene)	Eliminación de enrutamiento, interferencia de enlaces de comunicaciones, modificación de software para evitar ejecución precisa, borrado de datos
Fabricación (cuando personal no autorizado inserta objetos (por ejemplo datos o componentes) falsos en el sistema)	Autenticidad	Activo (Puede ser detectado con criptografía)	Ataques por saturación, inserción de señal de control falsas, (inserción de transacciones financieras falsas con fines de lucro)

Fuente: (Sáez & Collado, 2015)

En Estados Unidos y Europa ya se ha lanzado a los usuarios los nuevos equipos de medida, mejor conocido como Smart meter, quienes ya han instalado una cifra considerable de medidores inteligentes, pero esta primera generación de Smart meter se está considerando ante los usuarios como inservible y “tonto”, ya que los Smart meters no funcionan correctamente si no tienen buena cobertura de red

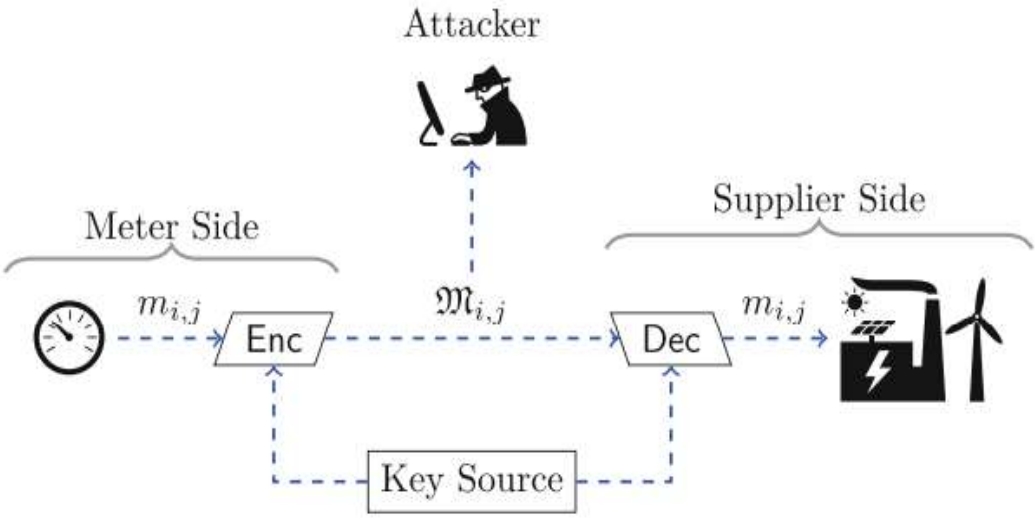
celular y por consecuencia envían lecturas falsas al sistema de distribución eléctrica y con esto conlleva a tener un costo elevado en la factura y no cumpliría con sus objetivos; otro defecto que tiene esta primera generación de medidores inteligentes es su falta de actualización de software, si el software no se actualiza, el equipo de medida inteligente se vuelve “tonto”, por lo tanto, el usuario dejará de tener suministro de energía eléctrica hasta que el operador técnico haga su respectiva revisión.

Vale aclarar que, aunque los Smart meter tienen interconexión con otro Smart meter, cada uno lee, procesa y registra datos para cada usuario, con la función de calcular el valor del consumo real y facturarlo, pero los expertos en materia de seguridad de información saben que la infraestructura de seguridad de los Smart grids no está concretamente sólida y puede ser violada para controlar estos datos que pueden ser usados para acciones diferentes. (Rodriguez, 2012)

Los datos de cada usuario básicamente definen como se comporta esta persona en su hogar, es decir, se puede saber la hora de llegada y salida de los habitantes, la cantidad de personas que habitan en ella, la cantidad de electrodomésticos conectados, y hasta saber si hay personas en la casa; con estos datos expuestos, las personas que buscan el mal ajeno tendrían acceso fácilmente a dichos datos, donde podrían manipularlos para sus propios bienes. (Rodriguez, 2012)

Los virus y malware también tienen un modelo a seguir para hacer cumplir su función en los Smart meters, que básicamente es extraer información privada y manipularla para beneficio propio; en el modelo de ataque adquieren el conocimiento de algunas funciones que tiene el software de seguridad de un contador inteligente; el modelo de ataque hace que el sistema no reconozca falencias de nivel lateral o fallas de funcionamiento del equipo, sin embargo, no pueden acceder a la información tan fácil, ya que la obtienen pero de manera encriptada o cifrada, por lo tanto no conoce la medición exacta de un Smart meter. (Borges de Oliveira, 2015)

Figura 7. Modelo de Ataque



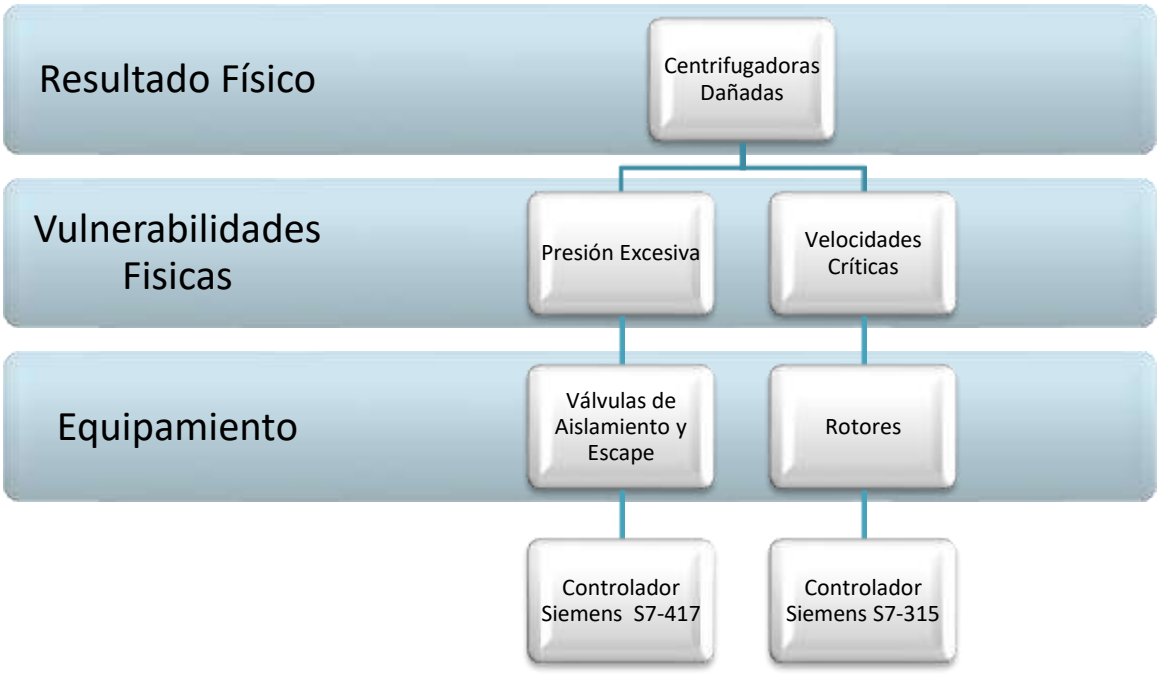
Fuente. (Borges de Oliveira, 2015)

3.3. SOFTWARE DE SEGURIDAD ACTUALES Y EL GUSANO STUXNET

Un estudio, reveló las causas del porque mil máquinas fueron autodestruidas en enero de 2010 localizadas en Iran, lo cual fue la entrada de un gusano cibernético a la red donde se penetró en los puntos más críticos que tenía el sistema operativo Windows; el gusano fue adentrándose al sistema durante varios meses para encontrar su objetivo lo cual era el controlador lógico programable (PLC) por sus sigla en inglés, que manejaban las máquinas para cumplir correctamente su funcionamiento, cuando el gusano penetró y entró al PLC, obtuvo control total del funcionamiento de las máquinas, con ello hizo que estas trabajaran con más intensidad, aparte tenía la capacidad de bloquear los interruptores de emergencia, lo cual permitieron que la empresa dejara fuera de servicio aproximadamente un veinte por ciento (20 %) de su maquinaria. (BBC, 2015)

El esquema muestra como el gusano stuxnet trabaja en las máquinas y hace que se autodestruyan por medio de exagerada carga de funcionamiento.

Figura 8. Esquema del Trabajo Stuxnet



Fuente: (Guillermo, 2013)

Con el fácil ingreso de este virus a un sistema de red privado, se generan muchas dudas en cuanto a estos sistemas de seguridad que se encuentran hoy por hoy protegiendo nuestra privacidad; la implementación de nuevas tecnologías inteligentes requiere de una infraestructura de seguridad más sólida que sea capaz de detectar el fallo más mínimo que afecte al sistema.

Dentro de los retos que se avienen para las redes inteligentes está el establecer una arquitectura de seguridad que proteja la información contenida en particular en los Smart meter; blindar los canales por los cuales se transporta la información protegiendo los sistemas antiguos que usaban software en particular los que contienen el SCADA, de forma tal que se proteja la red de un ciberataque, el cual podría conllevar a daños físicos y hasta el extremo de poner en peligro la seguridad de las personas. A continuación, en la Tabla 2, se mencionan las normas o estándares que deben incluir el software que se desarrolla para proteger los sistemas industriales y los datos de las personas, propuestos por el Instituto Nacional de Normas y Tecnología-NIST, en los Estados Unidos. (González, Galván Bobadilla, & Camacho Peréz, 2012)

Tabla 2. Estándares propuestos por el NIST

Norma	Título	Aplicación
IEEE 1711	Estándar de prueba de un protocolo criptográfico para la seguridad cibernética de subestaciones de enlaces seriales	Subestaciones eléctricas
IEEE 1686	Seguridad para dispositivos electrónicos inteligentes	Subestaciones de dispositivos eléctricos inteligentes
NERC CIP 002-009	Seguridad cibernética identificación de activos críticos	Sistema eléctrico
IEC PAC 62559	Metodología intelligrid para el desarrollo de requerimientos de sistemas eléctricos	Sistemas eléctricos
OPC-UA Industrial OPC	Unified Architecture	Sistemas de automatización
Security Profile for Advanced Metering Infrastructure v 1.0	Perfil de seguridad de la infraestructura de medición avanzada	Sistemas de adquisición de datos
DHS Cyber Security Procurement Language for Control Systems	Lenguaje de adquisición DHS de seguridad cibernética para sistemas de control	Sistemas de control
NIST SP 800-82	Guía para sistemas de control industrial de seguridad (ICS)	Sistemas de control y de adquisición de datos
ISA SP100	Estándar industrial de redes inalámbricas	Sistemas de control inalámbrico
ISA SP 99	Automatización industrial y seguridad de sistemas de control	Automatización y sistemas de control
IEC 62351	Partes 1-8 Sistemas de gestión de energía e intercambio de información asociada)	Sistemas de información y de comunicaciones (dispositivos
NISTIR 7628 vol. 1,2 y3	Directrices de seguridad cibernética para el smart grid	Red eléctrica inteligente (smart grid)
NIST SP 800-53	Guía para la evaluación de controles de seguridad en	Organizaciones y sistemas de información federal

Norma	Título	Aplicación
	los sistemas de información federal y organizaciones	
ISO 27000	Sistema de gestión de la seguridad de la información	Sistemas de información de organizaciones públicas o privadas
NIST FIPS 140-2	Requerimientos de seguridad para módulos criptográficos	Sistemas de información
OASIS WS	Estándares de seguridad OASIS	Servicios web

Fuente: (González, Galván Bobadilla, & Camacho Peréz, 2012)

3.4. NUEVAS MODALIDADES DE SEGURIDAD PARA LA LLEGADA DE LAS REDES INTELIGENTES

Primero que todo, vale aclarar que los términos seguridad y privacidad no hacen alusión semejante; el concepto de privacidad en el Smart metering hace referencia a la manera en que se protege o divulga la información personal de cada usuario mientras se transporta su información a la base de datos, el usuario tiene derecho a que personas que buscan el mal, no tengan conocimiento alguno sobre su información personal, además, gracias a la privacidad, el usuario tiene la autoridad de revelar o divulgar su información a entidades públicas como él quiera. (Ur-Rehman, Zivic, & Ruland, 2015)

La seguridad conlleva a un significado más técnico, ya que se plantean sistemas centralizados, protocolos, soluciones; la meta de la seguridad es tener los datos personales de cada usuario protegidos, y para ello, se tiene en cuenta cuatro aspectos importantes como lo son la confidencialidad, integridad, disponibilidad, y consistencia. (Orallo, 2004)

- **Confidencialidad:** Es la garantía que se le da a cada usuario que está conectado a cualquier sistema de comunicación o servicio público, ya sea, agua, gas natural, energía eléctrica, o calefacción, que sus datos personales sean altamente protegidos. (Funes, 2013)

- **Integridad:** Se refiere a mantener con plenitud y exactitud todos los datos ingresados por el usuario desde un principio y no se puedan modificar sin consentimiento de él. (Alegsa, 2016)

- **Disponibilidad:** Los datos y la información de cada usuario deben estar siempre disponibles para cualquier eventualidad, ya sea si lo requiere la central de datos, o el mismo autor de la información. (Orallo, 2004)

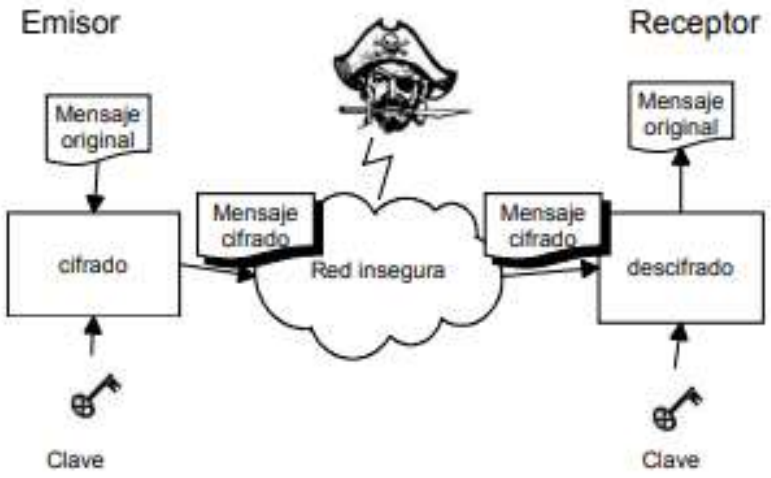
- **Consistencia:** Conlleva a tener certeza de que la información ingresada por el usuario no haya sido alterada mientras se genera algún tipo de tarea o actividad que requieran de dicha información. (Orallo, 2004)

Las redes de comunicación e información, agencias bancarias, puestos de salud, seguridad nacional, redes de distribución eléctrica, entre otros., requieren de un sistema de seguridad altamente confiable debido a los datos y proyectos que manejan cada identidad; estudios demuestran que en la actualidad no protegen la información en su totalidad, es la forma más factible de tener un sistema seguro y estas son por medio de claves y códigos cifrados y los métodos de autentificación.

Las claves cifradas o mejor conocida como criptografía lleva el concepto de ocultar un mensaje, clave, datos personales y/o información a personas no autorizadas al conocimiento de estos parámetros, y tienen objetivos puntuales como lo es la denegación de la lectura de información por terceras personas, protección contra la alteración y manipulación de datos, verificación y confirmación de la llegada de la información a su destino acordado; la criptografía tiene como función transportar información de un ordenador y pasar por redes inseguras para llegar a una base de datos con la información intacta. (Orallo, 2004)

El fin del transporte de datos cifrados es garantizar su protección y evitar la suplantación de datos, con esto se logra que el medidor inteligente pueda ser certificado técnicamente (Camargo, Sáenz, & Rosas, 2014)

Figura 9. Criptografía de Información



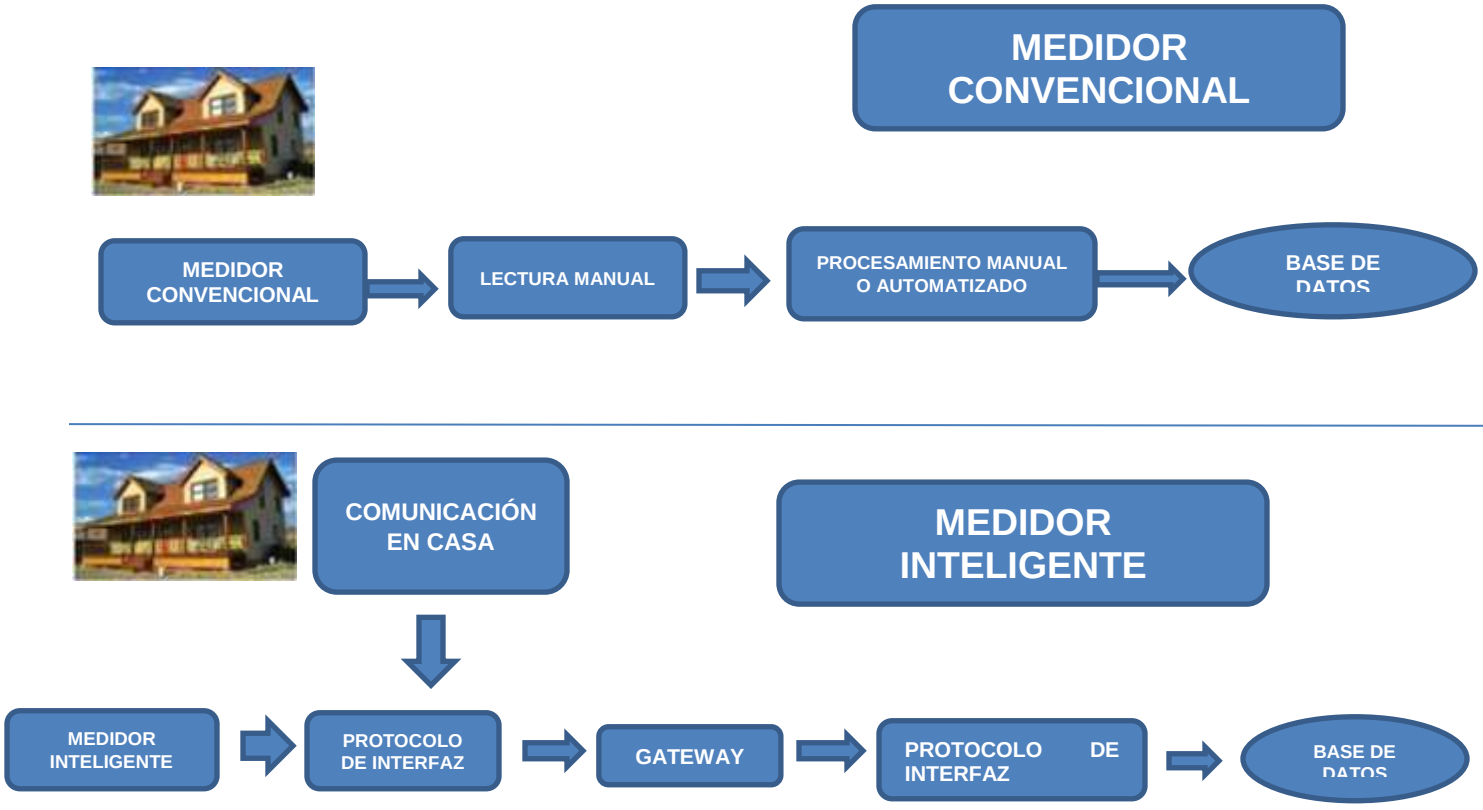
Fuente: (Orallo, 2004)

Investigaciones que se están llevando a cabo en Europa, revelan una nueva modalidad de comunicación entre el Smart meter y la base de datos; esta modalidad recibe el nombre de enfoque basado en Gateway, donde cumple con estándares de seguridad, confidencialidad e integridad; este enfoque de comunicación Gateway provee de un almacenamiento y una infraestructura bastante sólida para permitir que otras redes de comunicación ingresen al sistema, tales como GPRS, MBUS, PLC, MBUS inalámbrico, Zigbee, etc ; también estará configurada para que tenga la funcionalidad de extraer información del medidor inteligente y a su vez lleve dicha información a la red inteligente de manera segura, a esto se le conoce como bidireccional. (Orallo, 2004). Esta modalidad tiene altas diferencias a comparación de los medidores convencionales.

Figura 10. Diferencia Entre un Medidor Convencional y un Medidor Inteligente

MEDIDOR CONVENCIONAL VS MEDIDOR INTELIGENTE

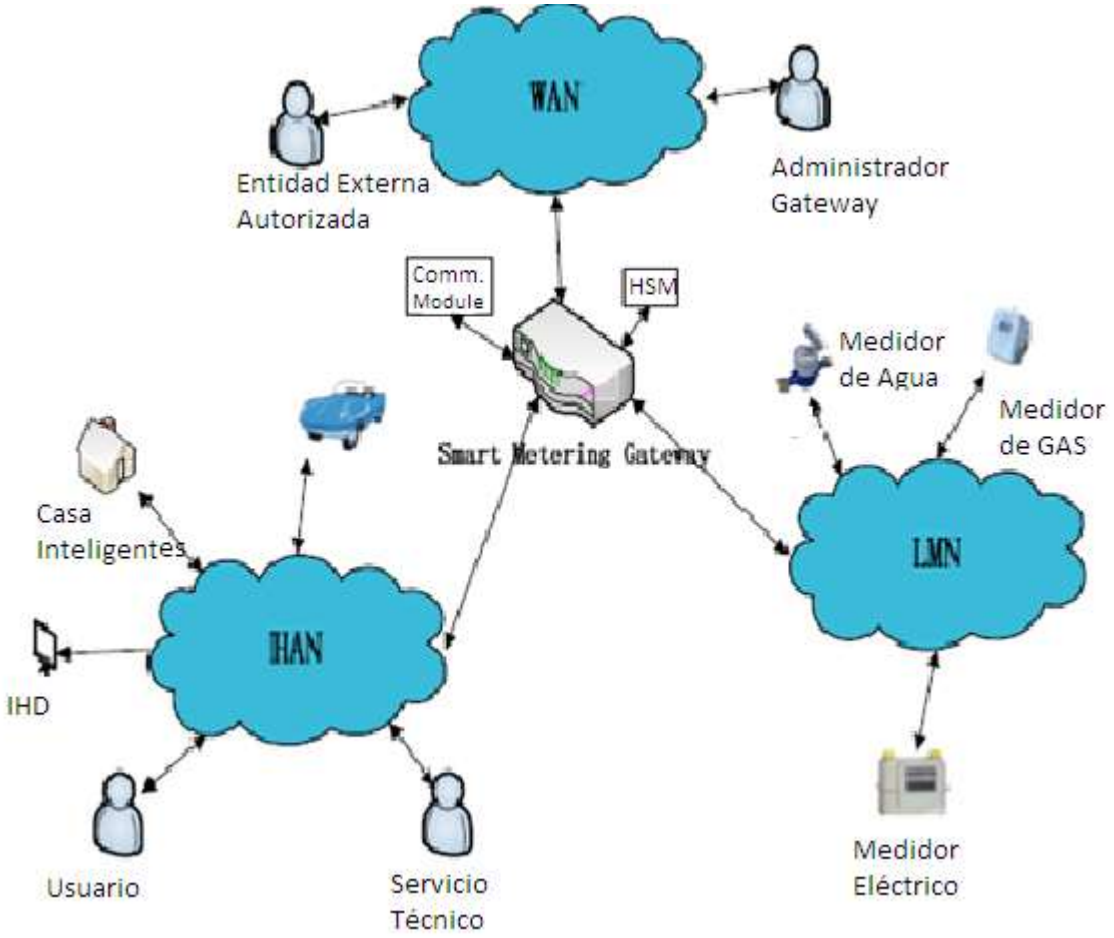
PALABRAS CLAVE



Fuente: (Hernandez, 2014)

La función bidireccional hace que la extracción de información se conecte a una red de área amplia (Wide Area Network - WAN) donde cumple una función de crear un enlace de comunicación entre los medidores inteligentes y las entidades encargadas de recibir información, que a su vez se conecta a una red de área local (Home Area Network-HAN) (smartme, 2013) , esto se refiere a que el medidor inteligente se enlace con otro dispositivo inteligente y el usuario tenga accesibilidad a toda la información; de esta manera se entrelazan todas estas funciones y se lleva a cabo una red de comunicación sólida y así llevar los datos de forma segura a la red centralizada.

Figura 11. Enfoque de Comunicación Gateway



Fuente: (Ur-Rehman, Zivic, & Ruland, 2015)

En Brasil existen varias investigaciones sobre protocolos de preservación de la intimidad, por sus siglas en inglés (PPP Privacy-Preserving Protocols), donde manejan cuatro procesos.

El PPP1 es un protocolo que se considera el más rápido en protección de medidores inteligentes de primera generación ya que el Smart meter toma las lecturas de la energía real consumida y el protocolo PPP1 hace una encriptación simétrica a la información inmediatamente, este protocolo aún no se considera el más seguro por su función unidireccional.

El proceso PPP2 contiene teorías matemáticas más complejas como lo son las curvas elípticas que son conocidas por ser una forma de encriptación muy antigua, las curvas elípticas en función de seguridad para los Smart meter maneja una multiplicación escalar para cifrar la información y otra para codificar la lectura de la medida, su desventaja en este segundo proceso es que no es escalable por el proveedor del servicio eléctrico, sin embargo, tiene buenas características como el acceso a la verificación de factura de cada usuario, además, los proveedores del servicio podrán detectar fallos de comunicación entre un medidor inteligente a otro.

El ciclo tres denominado PPP3 es el más adecuado para implementar a un sistema seguro para los Smart meter, ya que contiene todas las características del PPP2 y es más rápido.

Por último, pero no menos importante, se encuentra el ciclo PPP4 donde es más compleja que las tres mencionadas anteriormente y solo puede ser ejecutada con tecnologías muy avanzadas, dado que maneja un sistema criptográfico, donde toda la información suministrada del equipo inteligente de medida se desprende en un canal inalámbrico cuántico y lo mantiene oculto hasta que otros sistemas de cambio de información desee conocer y descifrar la información. Con base a estos protocolos de identidad preservada surge otra idea para mejorar la confidencialidad del sistema de comunicación entre medidores inteligentes y/o una base centralizada de datos, donde se puede crear un perfil anónimo utilizando un par de seudónimos para preservar la identidad del usuario, uno de estos seudónimos se utiliza para obtener la información de medidas de alta frecuencia y el otro para extraer las medidas de baja frecuencia. (Borges de Oliveira, 2015)

La mejor solución que se pueda encontrar para preservar la privacidad de datos de cada usuario que se encuentre interconectado al sistema de energía eléctrica es la encriptación homomórfica; dicha encriptación es un proceso matemático donde cumple la función de convertir un conjunto de información del usuario a otro conservando la información encriptada intacta, este tipo de sistema de encriptación permite hacer cálculos matemáticos complejos sin conocer con exactitud los datos que se encuentren en el cifrado.

El cifrado homomórfico se despliegan en un sistema criptográfico, donde se basa en los esquemas criptográficos parcialmente homomórficos que son caracterizados por tener mayor eficacia.

Los esquemas parcialmente homomórficos son aquellos sistemas de cifrado que realizan los procesos con una sola operación, bien sea la sumatoria o el producto, depende de su operación se le denominan esquemas probabilísticos o deterministas de forma multiplicativa, dentro de ellas se encuentra el cifrado de clave pública y privada como,RSA, ElGamal.

El sistema de criptografía RSA se le otorga ese nombre por homenaje a sus creadores (Ronald Rivest, Adi Shamir, Leonard Adleman); se puede considerar como el más viable para integrarlo en el esquema de seguridad de los Smart meters, ya que su algoritmo es técnicamente fácil de entender e interpretar, este sistema tiene cierta peculiaridad por servir a dos funciones distintas de privacidad como lo es el cifrado de los datos arrojados por el Smart meter y la autentificación legitima del usuario. El esquema de cifrado del RSA se basa en la factorización de números grandes para obtener bien sea una clave pública o privada, la obtención de dicha clave proviene de la multiplicación de dos números primos extensos, las amenazas que quieran interrumpir la comunicación entre los Smart meters y la base centralizada o robar información en el transcurso del transporte de la información de un extremo a otro tendrá que resolver todas las probabilidades de factorización. Para crear la clave pública, el sistema criptográfico RSA escoge dos números primos de más de 150 cifras cada uno y realiza su respectivo producto; después se elige cualquier numero primo relativo que sea -1 de cada uno de los números escogidos primeramente; obteniendo el conocimiento de estos dos números se genera la clave pública ya que cualquiera puede tener conocimiento de ella; La clave privada es la más atractiva para implementar la privacidad en los Smart meters, ya que en este proceso se debe tener un módulo inverso al número primo relativo que se menciona anteriormente, haciendo valer que el producto entre el modulo inverso del número primo relativo sea equivalente al módulo del número primo relativo, esta clave se mantiene en secreto y solo tendrá conocimiento de ella el usuario.

El sistema criptográfico ElGamal también es efectivo para el cifrado de información en redes inteligentes puesto que el algoritmo que maneja es similar al del RSA ya que tiene una complejidad de $\lambda=1/3$ por lo que le es muy difícil a los intrusos ingresar al sistema rompiendo o descifrando el algoritmo en un tiempo considerable.

3.5. ¿A DÓNDE VA LA INFORMACIÓN QUE EMITEN LOS SMART METERS?

Para crear la infraestructura de la central de datos a donde llega toda la información de los Smart meter para ser procesada, se deberá tener en cuenta dos redes de comunicación, como lo es la red de un área vecina (Neighbourhood Area Network –NAN), y una red de área residencial (Home Area Network-HAN).

La red de área residencial genera distintas funcionalidades, entre ellas se encuentra la forma de gestionar el consumo de energía eléctrica, controlar dicho consumo a través de monitores, mantenimiento de los sistemas de temperatura (calefactor, ventilación, aire acondicionado), además, esta red podrá programar las operaciones remotas para los Smart meter y todos los dispositivos Smart que se encuentren dentro del hogar. (Hernandez, 2014)

En la red de área vecina será la encargada de transportar toda la información y las lecturas de consumo de energía eléctrica que arrojan los Smart meter para llevarlos a una central de datos, también enviará mensajes de detección de fallas o requerimiento de un mantenimiento del sistema; en sus configuraciones está la opción de expandir la capacidad de memoria ya que los volúmenes de la información de todos los usuarios serán abundantes. (Hernandez, 2014)

A parte de estas redes de comunicación, se tienen en cuenta otras tres fases para la creación de una infraestructura de comunicación y almacenamiento de datos bastante sólida.

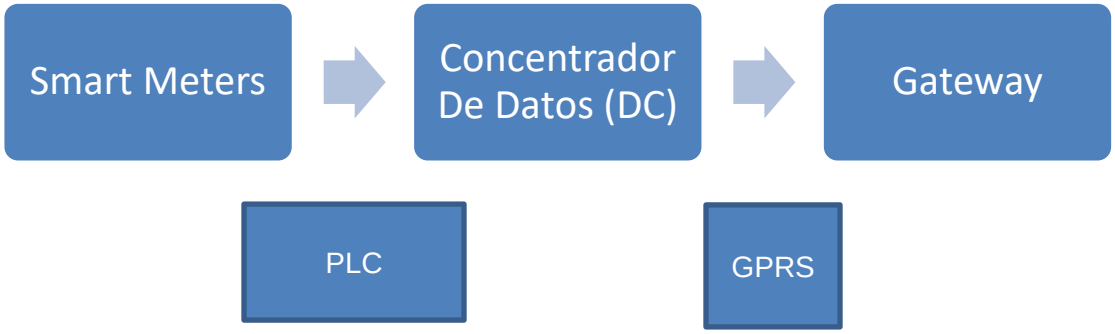
Concentrador de datos: Este concentrador de datos se utiliza como un hilo conductor entre los medidores inteligentes y la función de comunicación Gateway**,** donde coordina, monitorea, gestiona y supervisa todo el trayecto donde se transporta la información, convirtiéndolo en un sistema seguro y confiable. (Hernandez, 2014)

Base de datos: se podría definir como la caja fuerte de todo el sistema inteligente, ya que ahí es donde llegará toda la información para que sea almacenada y procesada; la base de datos tendrá distintos servicios tales como autenticación de información, validación y ajuste de datos, y cálculos de lecturas y valor de KWh para obtener distintos resultados y funciones como la facturación del servicio, envíos de actualizaciones, reducción de los voltajes pico, sustentar ante entidades superiores que el sistema funciona de manera correcta entre otros.

Protocolos de comunicación: En este apartado se manejará un controlador lógico programable(PLC) para obtener la comunicación entre el concentrador de datos y

los medidores inteligentes, y un servicio general de paquetes de radio (General Packet Radio Service, por sus siglas en inglés(GPRS)) para la comunicación entre la Gateway y el concentrador de datos.

Figura 12. Etapas de Comunicación



Fuente: Autor

Figura 13. Infraestructura del sistema Smart Metering

Fuente: (Codensa, 2016)

En Colombia, actualmente se creó la resolución número 40072 del 29 de enero del 2018 donde habla sobre la implementación de una infraestructura de medición avanzada(AMI) que se acople perfectamente a las necesidades de los colombianos como lo es la reducción de los costos por la prestación del servicio de energía eléctrica; con la incorporación de la nueva infraestructura de medición avanzada (AMI) tanto las empresas generadoras y distribuidoras de energía eléctrica como el usuario final podrán notar el cambio de la calidad del servicio gracias a la nueva infraestructura, ya que proporciona la comunicación y distribuye el flujo en dos direcciones; con base a esta resolución, la Comisión Reguladora de Energía y Gas (CREG) pondrá las condiciones en que se implementara esta nueva infraestructura y está predestinada a elaborarse en el año 2030 para asumir un cambio de más del 90% en el sistema de medida y comunicación del servicio de energía eléctrica; este proyecto tiene colaboraciones de universidades y entidades conocedoras del tema, tales como la universidad nacional de Colombia y la Unidad de Planeación Minero Energética (UPME).

Actualmente, las empresas generadoras de la región del Pácifico se han puesto en la tarea desde el año 2017 de cambiar en distintas partes de la región los medidores convencionales por los dispositivos de medida inteligentes en cantidades mínimas, pero se espera que en el transcurso del año 2018 se generen cambios de dichos medidores de manera considerable.

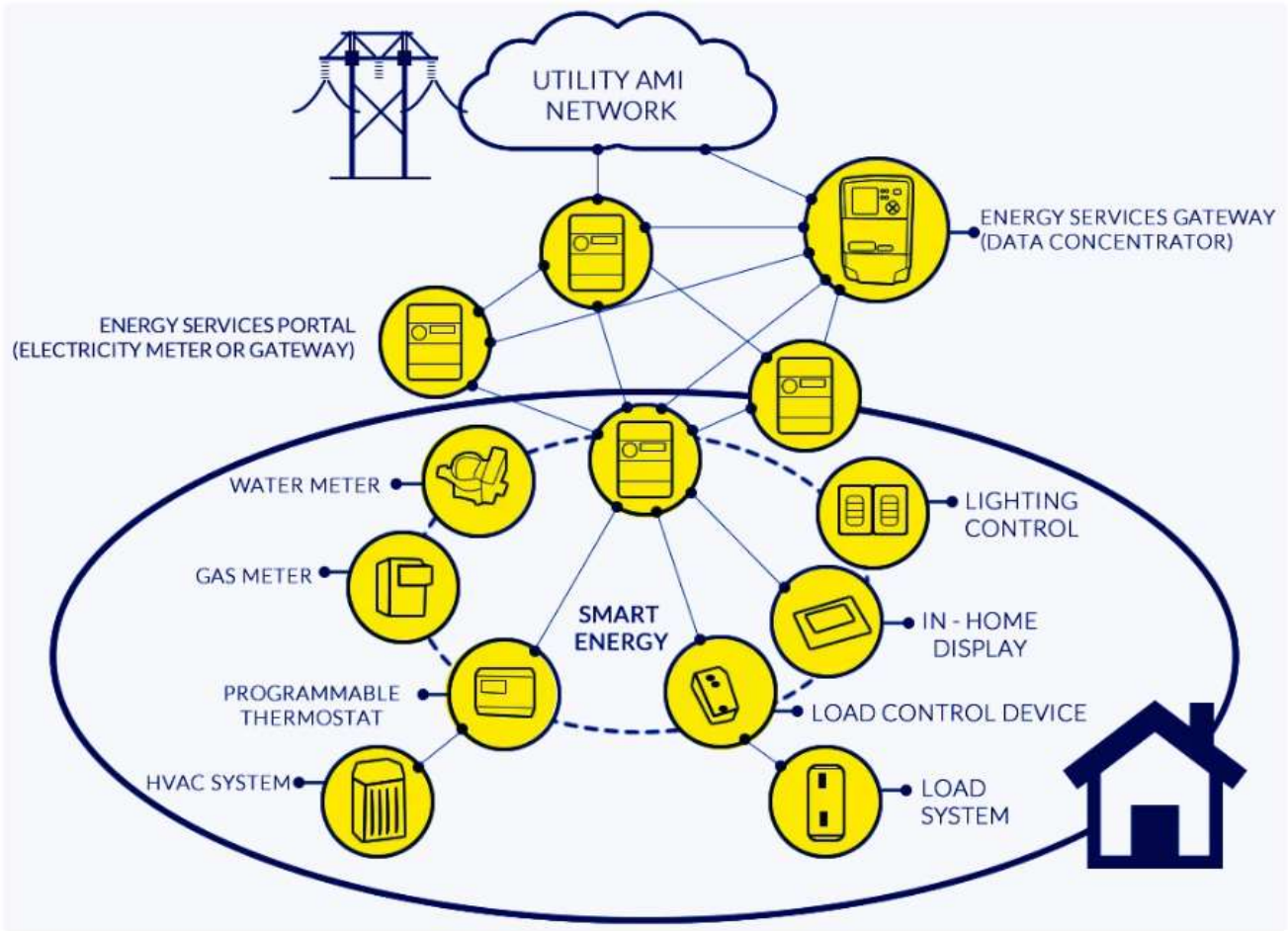
Como se ha mencionado anteriormente en este documento, la instalación de un medidor inteligente trae múltiples beneficios para el usuario final y en Colombia no es la excepción; entre esos beneficios para el usuario final esta:

- Una medición exacta del consumo de energía eléctrica
- Racionalización del servicio eléctrico
- Posibilidad de conexión del servicio a una microfuente de energía renovable
- Detección de fallas del sistema y reparación en tiempos cortos (CELSIA, 2018)

Existe una empresa en Colombia donde se promueve la innovación, investigación, diseño y comercialización de la telemedida en servicios públicos llamada TECUN, donde su mayor fortaleza es comercializar dispositivos avanzados de medida para satisfacer las necesidades de servicios públicos a los usuarios; esta empresa presenta una marca de medidor inteligente según su sistema de acometida (monofásico, bifásico trifilar, y trifásico) y un software para gestionar el sistema de medida.

También crean su propia infraestructura de medida inteligente llamada AMI TECUN-Linyang donde permite conocer el día y la hora exacta donde se genera el mayor consumo de energía eléctrica para que los usuarios conozcan y efectúen un mejor consumo del servicio adquirido, además reducirá las pérdidas de energía para que las empresas disminuyan su pérdida económica.

Figura 14. Infraestructura del Sistema



Fuente: (TECUN, 2017)

4. MATRIZ DE INVOLUCRADOS.

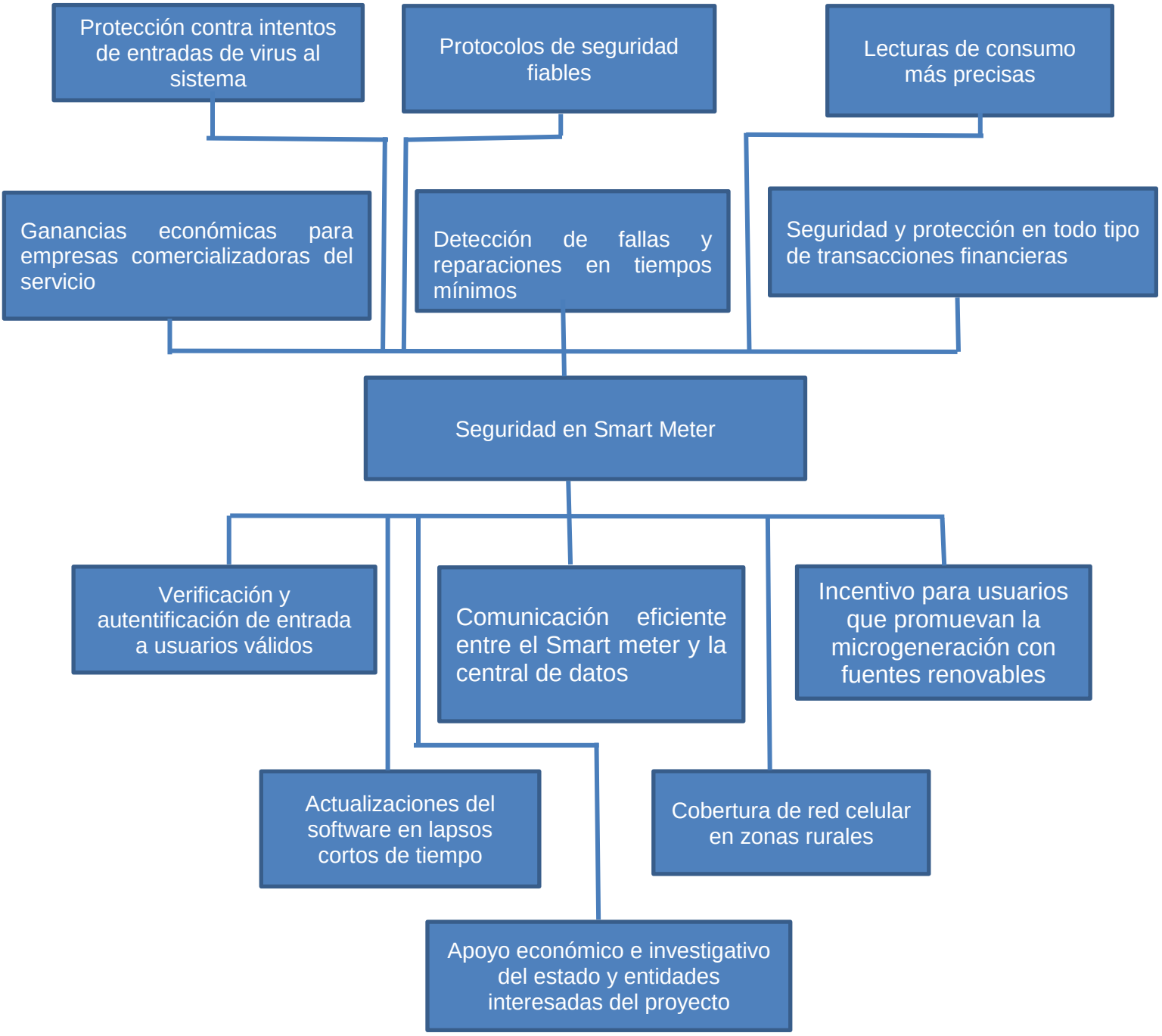
Tabla 3. Matriz de Involucrados.

Involucrado	Expectativa	Fuerza	Resultado
Empresas Generadoras y Distribuidoras de Energía Eléctrica	Muy Alta (5) ▪ Mantener y mejorar la sostenibilidad del sistema con la implementación de energías renovables ▪ Reducir la pérdida de electricidad en las redes de distribución eléctrica. ▪ Identificar problemas de la caída de la red y dar una respuesta inmediata ▪ Tener un sistema centralizado a base de la telemedida y que sea bidireccional ▪ Mejorar la seguridad del sistema antes y durante la implementación de las Smart grids	Buena (4) ▪ Explorar nuevos campos de generación de energía eléctrica con energías renovables como paneles solares, campos eólicos entre otros. ▪ Automatizar y monitorear con tecnologías avanzadas para el sistema de distribución ▪ Implementar de software que se encarguen de la seguridad del sistema	20
Empresas Desarrolladoras de Software Basadas en Seguridad	Alta (4) ▪ Incrementar utilidades para el desarrollo del sistema de seguridad	Alta (4) ▪ Establecer procedimientos de autentificación ▪ Realizar algoritmos de cifrado para la privacidad de datos	16

Involucrado	Expectativa	Fuerza	Resultado
Unidades Tecnológicas de Santander	Alta (4) ▪ Promover la investigación y el desarrollo tecnológico ▪ Contribuir con el medio ambiente ▪ cumplir su función social, entregando sistemas desarrollados in situ, que sean requeridos por la sociedad y el desarrollo del país	Baja (2) ▪ conseguir recursos de financiación de los proyectos	8
Comercializadores de Equipos de Medida	Alta (4) ▪ Satisfacción del usuario con el cambio de medidor convencional por el Smart meter ▪ Aceptación de las entidades encargadas en la distribución y generación de energía eléctrica ▪ Mayor correlación entre las tecnologías de comunicación y los equipos de medida	Baja (2) ▪ Suplantar medidores convencionales por medidores inteligentes ▪ Reducir la tarifa del consumo de energía eléctrica ▪ Actualización de software	8
Usuario Final	Muy Alta (5) ▪ Tener control en las tarifas ▪ Reducir costos ▪ Incrementar interacción con el centro de mando ▪ Convertir al consumidor en microgenerador	Baja (2) ▪ Controlar su consumo ▪ Planear su consumo ▪ Ahorrar energía ▪ Percibir que su información está segura Falta pruebas piloto ▪ Software no cumple con lo esperado	10

5. ÁRBOL DE PROBLEMAS

6. ÁRBOL DE OBJETIVOS.



7. ALTERNATIVAS DE SOLUCIÓN.

- La primera alternativa de solución es crear una infraestructura fiable y segura, con esquemas similares a la que está planteada en el desarrollo del documento, particularmente, estado del arte, donde se da a conocer el diseño y construcción del Smart meter y los distintos componentes que lo acompañan. Crear un sistema seguro para las Smart grids, conlleva realizar diversos componentes; la seguridad en los Smart meters va desde una infraestructura sólida, fiable y confiable, hasta los dispositivos inteligentes que estarán por dentro del hogar para que el usuario monitoree su consumo.

  Los Smart meters se crearon para registrar el volumen o cantidad de energía eléctrica usada en distintas horas por el usuario, con esta función se permite tener una factura del servicio más económica ya que el registro de energía es más preciso y no se registrarán en las facturas las “perdidas” de energía; otra característica de los medidores de energía inteligentes es su capacidad de tener doble vía de comunicación y paso del flujo de potencia.

  La finalidad de la bidirección del Smart meter es llevar la información de datos y lecturas de consumo que emiten los Smart meter y a su vez recibir información tales como avisos de mantenimiento del sistema, actualizaciones del software y demás, con esta función también se puede acreditar a aquellos usuarios que generan su propia energía con base a fuentes renovables y su recibo de facturación sea de un costo mínimo ya que no se cobraría la parte de generación.

  Dentro de la casa de cada usuario se instala un monitor llamado “In home”, el cual es un dispositivo que va directamente conectado con el Smart meter, y sirve para que los usuarios y operadores del sistema puedan acceder con más exactitud a la información del consumo de energía eléctrica, de esta manera los usuarios podrán tener la posibilidad de crear estrategias de ahorro de energía y así tener tarifas de menor costo y a su vez podrán estar actualizados de toda la información que reciba el Smart meter.

  Los Smart meter registrarán y monitorearán la información en intervalos de tiempo muy cortos para que sea más precisa, eficaz y segura; para realizar esta función es necesario tener en cuenta los protocolos de seguridad que tendrá los Smart meter, una red de área local y una red de área global; en los protocolos de seguridad se manejan diferentes aspectos como claves

encriptadas, sistemas de autentificación, fiabilidad y confidencialidad de la información.

Una red de área local es una red de telecomunicación de un terreno pequeño y sirve para gestionar su forma de conectar y comunicar los dispositivos smart que trabajen con energía eléctrica y se encuentren en el hogar de cada usuario, esta función permite la conectividad de los dispositivos y la red de distintas maneras, bien sea vía cable o inalámbrica; en cambio, la red de área global tiene mucha más cobertura y es capaz de extender la comunicación entre dispositivos Smart y lecturas de consumo de energía eléctrica en áreas de gran tamaño, como lo son entre ciudades, países y hasta continentes.

Toda la información que arrojan los Smart meter tienen que tener un lugar o punto de encuentro determinado para que dicha información sea procesada y almacenada, para ello, es necesario de un concentrador de datos que funciona como un hilo conductor entre los Smart meter y la central de datos ya que está situada entre estos dos componentes y está controlado por un PLC (controlador lógico programable)

Además del concentrador de datos es necesario hablar de una base de datos para ensamblar todas las piezas y determinar una infraestructura de comunicación y seguridad fiable, la base de datos es una parte fundamental para el sistema de comunicación y seguridad para los Smart meters y la Smart metering, en la base de datos se cumplen distintas funciones como cálculos de facturación de consumo, ajustes de datos, validación de funciones, almacenamiento y demás.

- La segunda alternativa de solución, surge del análisis de las consecuencias de la puesta en funcionamiento de los Smart meters y se basa en las nuevas problemáticas que se pueden presentar en la implementación de Smart grids como lo es la falsificación, robo y manipulación de datos al servicio de energía eléctrica y consiste en seguir con el sistema eléctrico tradicional donde actualmente no se encuentran este tipo de problemas.

  En el sistema de medida tradicional de energía eléctrica donde consiste en la visita de un operador enviado por la empresa comercializadora del servicio, para que registre la lectura del consumo y la envíe a un centro de almacenamiento y se lleve al proceso de facturación, donde se genera el valor del kilovatio/hora (KWh) y la diferencia de lectura entre el mes actual y el mes anterior, además de cobrar distintos aspectos como la generación, transmisión, distribución y demás.

8. MATRIZ DE MARCO LÓGICO.

Tabla 4. Matriz de Marco Lógico

Nivel	Resumen Narrativo de Objetivos	Indicadores	Medios de Verificación	Supuestos
Fin	Desarrollar un sistema de seguridad sólido para la implementación de Smart Grids	Construcción de una infraestructura que contengan protocolos de seguridad confiables	Código de datos válidos registrados en la comunicación entre el Smart meter y la central de datos	Aceptación de las empresas generadoras y distribuidoras del servicio eléctrico
Propósito	Generar que las Unidades Tecnológicas de Santander promueva la investigación y desarrollo tecnológico alrededor de la seguridad en Smart grids	Número de profesionales que promuevan y participen en Capacitaciones y seminarios para que el estudiante tenga mayor participación	Resultado de un software de seguridad prototipo y pruebas piloto	Contribución economica de los entes gubernamentales
Componentes	**C1.**Construir medidor inteligente	Smart meter seguro ensamblado	Pruebas de medición en Smart meter	Contar con el material presupuestado
	C2. Implementar un sistema de comunicación entre el Smart meter y la central de datos	Componentes que mejoren la comunicación entre el smart meter y la central de datos	Obtención de datos e información enviados en tiempos reales desde el Smart meter a la central de datos	Recolección de datos totalmente válidos
	C3. Implementar un sistema de seguridad	Protocolos de seguridad para el sistema de comunicación entre Smart meter y centro de datos	Pruebas de medidor inteligente con protocolos de seguridad fiables	Software requerido para la implementación de un sistema de seguridad

Nivel	Resumen Narrativo de Objetivos	Indicadores	Medios de Verificación	Supuestos
	C4. Elaborar infraestructura de un centro de datos para Smart meter	Centro de almacenamiento de datos, para que la información pueda ser procesada y guardada	Elaboración de una base de datos segura y confiable	Aceptación de empresas generadoras y distribuidoras del servicio de energía eléctrica
Actividades	**C1.1** Diseñar la estructura del Smart meter	Plan de trabajo para diseño de la estructura del medidor inteligente	Planos realizado en programas eficientes	Disponer del programa de diseño de la estructura
	C1.2 Adquirir componentes	Cotización y compra de componentes	Facturas de cotización y compra	Disponibilidad de materiales
	C1.3 Elaborar Smart meter	Creación de tarjeta compuesta por microcontroladores, transformadores de corriente y voltaje, módulo GPRS y demás	Evidencias por medio de fotografías tomadas en el proceso y muestra final del producto	Mano de obra capacitada para la construcción del Smart meter
	C2.1 Diseñar sistema de comunicación	Planes de diseño para el sistema de comunicación	Simulación del sistema de comunicación	Disponibilidad del programa de simulación de redes
	C2.2 Implementar sistema de comunicación	Comunicación segura y fiable entre Smart meter y centro de datos	Pruebas piloto del funcionamiento del sistema de comunicación	Disponer de microcontroladores y hardware
	C3.1 Diseñar sistema de seguridad	Sistema y protocolos de seguridad que cumpla con lo establecido	Pruebas piloto del funcionamiento del software	Tener el programa para diseñar el software y
	C3.2 Implementar sistema de seguridad al sistema de medición inteligente	Software de seguridad fiable y sólido	Simulación del software y hardware para sistema de medida inteligente	Satisfacción y aceptación por parte del usuario final y empresas del servicio eléctrico

Nivel	Resumen Narrativo de Objetivos	Indicadores	Medios de Verificación	Supuestos
	C4.1 Diseñar un servidor de almacenamiento	Planes de diseño para elaboración de base de datos	Simulaciones del sistema de almacenamiento	Disponibilidad de materiales y programa para ensamble
	C4.2 Crear base de datos	Infraestructura de comunicación y almacenamiento para la red eléctrica	Procesamiento de datos de manera eficiente	Aceptación de Empresas distribuidoras del servicio eléctrico

Fuente: Autor

9. DOCUMENTO TÉCNICO.

Tabla 5. Documento Técnico

ESTRATEGIAS DE SEGURIDAD EN SMART GRIDS	
Instituciones Formuladoras	Unidades Tecnológicas De Santander
Grupos de investigación vinculadas al proyecto	Grupo de Investigación en Energía- GIE
Instituciones de apoyo	• SENA • UIS • Colciencias • Asociación Nacional de Empresas de Servicios Públicos y comunicaciones ANDESCO • Corporación Centro de Investigación y Desarrollo tecnológico en el Sector Eléctrico CIDET
Pertinencia Con La Guía Sectorial	**GUÍA SECTORIAL:** **Tipología I.** Investigación y desarrollo experimental **Subtipología 1.3** Desarrollo experimental **Tipología VII.** Innovación **Subtipología 7.2** Innovación de proceso **Subtipología 7.5** Innovación social **Subtipología 7.6** Servicios de apoyo a la innovación **PAED:** **Apuesta País 1.** Producción científica ambiciosa con enfoque, gerencia y disciplina: **Objetivo 2:** Propiciar espacios de intercambio y generación de conocimiento entre la academia y el sector productivo con el fin de fortalecer el potencial de investigación, particularmente en los focos estratégicos definidos en la visión de CT en el departamento. **Apuesta País 2.** Empresas más sofisticadas e innovadoras: **Objetivo 1:** Impulsar la innovación tecnológica empresarial a través de la articulación entre el sector productivo, la academia y el sector público en los focos estratégicos definidos en la visión de CT el del departamento

Localización	Santander
Licencias y Permisos Requeridos	No Aplica
Análisis de Riesgos	**Ambientales:** Las condiciones climáticas extremas no afectan directamente al desarrollo del proyecto, puesto que son desarrollos de software y medios de comunicación celular. **Costo-Beneficio:** Incremento en el costo de los equipos, varios insumos están sujetos a la variación del dólar. **Esquemas Sociales:** El principal riesgo del proyecto es la resistencia al cambio, pues se requiere de transformar la mentalidad del usuario final para que accedan a modificar la nueva modalidad de medición inteligente y se capaciten en el uso de las TIC y su software de seguridad. **Dependencia Tecnológica:** Colombia al no ser un país desarrollado tecnológicamente, depende de los dispositivos para fabricar equipos de medida inteligente que se fabriquen en países desarrollados.
Impactos	**Académico:** Para la Institución, el proyecto genera un amplio beneficio ya que el proyecto en su desarrollo es interdisciplinario, permitiendo la aplicación del conocimiento adquirido por estudiantes de diversos programas académicos dirigidos por los diferentes grupos de investigación que puedan ser parte del proyecto. **Económico:** El desarrollo del dispositivo de medición inteligente y software de seguridad confiable genera un servicio de energía eléctrica eficiente, lo que garantiza una actividad económica benéfica para los fabricantes. **Social:** La disminución del costo facturado del consumo de energía eléctrica permite que el usuario pueda confiar más en el sistema de medición inteligente e invertirle a la microgeneración de energía con fuentes renovables

Fuente: Autor

10. HILO CONDUCTOR.

Tabla 6. Hilo Conductor

Actividades		Rubros	Descripción	Cantidad	Valor ($)	Tiempo	Total ($)
Construcción del Smart Meter	Diseño	Software	Solidworks	1	5.000.000		5.000.000
		Equipos	Equipos de Cómputo	1	1.500.000	1	1.500.000
		Recursos Humanos	Estudiantes	1	2.800.000	1	2.800.000
			Docentes	1	800.000	1	800.000
	Adquisición de piezas	Fuente	Alimentación rectificada	1	508.521	1	508.521
		Relés	Controlador de potencia	2	49.990	1	99.980
		Microcontrolador ATmega2560	Circuito Integrado Digital (STPM32, STPM33, STPM34)	1	94.859	1	94.859
		Módulo GSM	Tarjeta de Comunicación	1	55.620	1	55.620
		RTC	Reloj en tiempo real	1	7.000	1	7.000
		TC	Transformador de corriente (400 A/ 1-5 A)	1	36.725	1	36.725
		TP	Transformador de diferencia de potencial (400 v/110v)	1	190.000	1	190.000
	Ensamble	Recurso Humano	Estudiantes	1	2.800.000	1	2.800.000
			Docentes	1	800.000	1	800.000
		Herramienta	Kit de Herramientas Básicas	1	400.000	1	400.000
	Diseño		Estudiantes	1	2.800.000	1	2.800.000

Actividades		Rubros	Descripción	Cantidad	Valor ($)	Tiempo	Total ($)
Sistema de Comunicación		Recurso humano	Docentes	1	800.000	1	800.000
		Software	Packet tracer	1	2.000.000		2.000.000
		Equipos	Computador	1	1.500.000	1	1.500.000
	Implementación	Recurso humano	Estudiantes	1	2.800.000	1	2.800.000
			Docentes	1	800.000	1	800.000
		Equipos	Equipos de cómputo	1	1.500.000	1	1.500.000
Protocolos de Seguridad	Programar	Software	eMeter	1	32.000.000		32.000.000
	Implementación	Recurso humano	Estudiantes	1	2.800.000	1	2.800.000
			Docentes	1	800.000	1	800.000
		Equipos	Equipos de cómputo	1	1.500.000	1	1.500.000
Infraestructura de Almacenamiento	Validación	Recurso humano	Estudiantes	1	2.800.000	1	2.800.000
			Docentes	1	800.000	1	800.000
		Equipos	Equipos de cómputo	1	1.500.000	1	1.500.000
Total							69.492.705

Fuente: Autor

Tabla 7. Costos por Rubros

Costos Por Rubros	
Recursos Humanos	$ 21.600.000
Equipos y Software	$ 46.500.000
Materiales e Insumos	$1.392.705
Total	$ 67.492.705

Fuente: Autor

11. Anexos

11.1. Anexo 1. Medidor Monofásico LY-SM100 Módulo GPRS

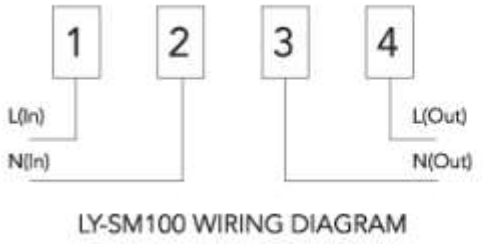
Características:

- Medida en 4 cuadrantes
- Conexión y desconexión remota
- Registro de alarmas
- Reloj en tiempo real

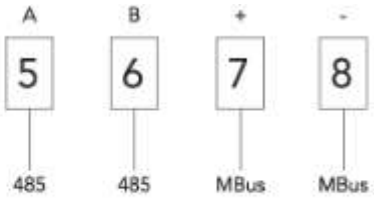
Especificaciones Técnicas

Registrador	LCD
Norma	IEC62053-21 IEC62052-11 IEC62053-23 IEC6205
Clase	1.0 Activa / 2.0 Reactiva
Voltaje	120V
Ib(Im)	5(80)A
Frecuencia	60 Hz
Constante	3200 Imp/kWh
Dispositivo de Corte	Relay Interno
Protocolo de comunicación	DLMS/COSEM
Grado protección	IP54
Puertos de Comunicación	GPRS RS485 M.Bus Puerto Óptico
Temperaturas	Operación: -25°C ~ +60°C Limite: -45°C ~ +70°C

Conexiones



LY-SM100 WIRING DIAGRAM



AUXILLARY TERMINAL WIRING DIAGRAM

11.2. Anexo 2. Medidor Trifásico LY-SM300CT con Módulo GPRS

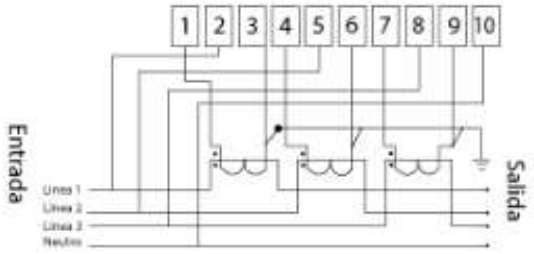
Características:
Medida en 4 cuadrantes
Grado de protección
Conexión y desconexión remota
Registro de alarmas
Reloj en tiempo real

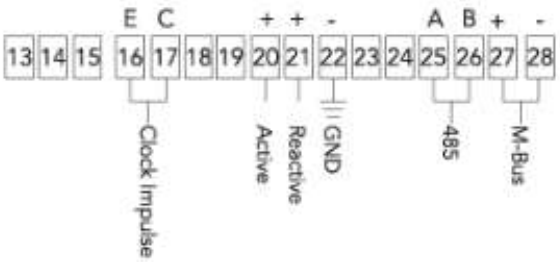
Especificaciones Técnicas

Registrador	LCD
Norma	IEC62053-21 IEC62052-11 IEC62053-23 IEC6205
Clase	1.0 Activa / 2.0 Reactiva
Voltaje	3x120/208V
Ib(Im)	1.5(6)A
Frecuencia	60 Hz

Constante	6400 Imp/kWh
Dispositivo de Corte	Relay Interno
Protocolo de comunicación	DLMS/COSEM
Grado protección	IP54
Puertos de Comunicación	GPRS RS485 M.Bus Puerto Óptico
Temperaturas	Operación: -25°C ~ +60°C Límite: -45°C ~ +70°C

Conexiones





11.3. Anexo 3. Medidor Bifásico LY-SM200DC Módulo GPRS

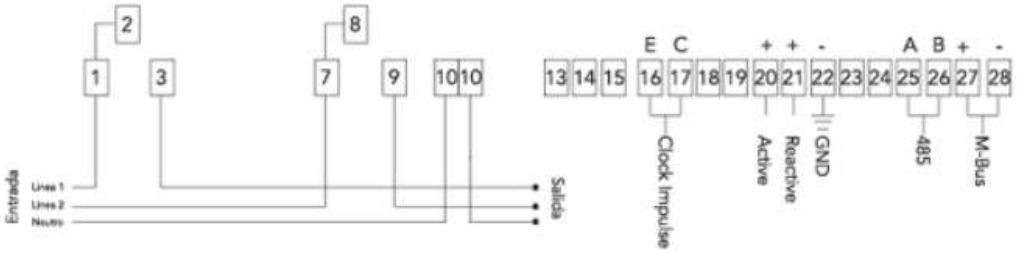
Características:

- Medida en 4 cuadrantes
- Grado de protección
- Conexión y desconexión remota
- Registro de alarmas
- Reloj en tiempo real

Especificaciones Técnicas

Registrador	LCD
Norma	IEC62053-21 IEC62052-11 IEC62053-23 IEC6205
Clase	1.0 Activa / 2.0 Reactiva
Voltaje	2x120/208V
Ib(Im)	10(100)A
Frecuencia	60 Hz
Constante	2200 Imp/kWh
Dispositivo de Corte	Relay Interno
Protocolo de comunicación	DLMS/COSEM
Grado protección	IP54
Puertos de Comunicación	GPRS RS485 M.Bus Puerto Óptico
Temperaturas	Operación: -25°C ~ +60°C Limite: -45°C ~ +70°C

Conexiones



11.4. Anexo 4. Medidor Trifásico LY-SM300DC Módulo GPRS

Características:

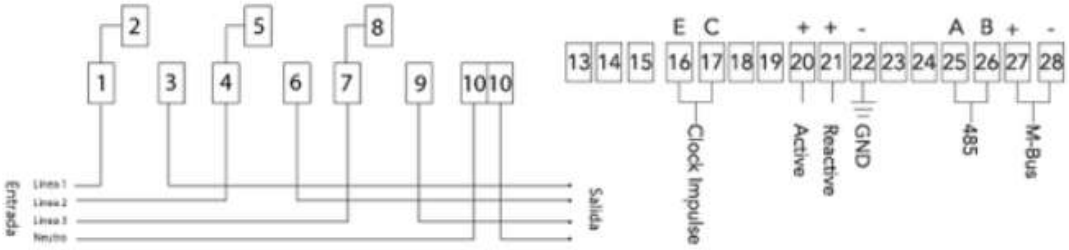
- Medida en 4 cuadrantes
- Grado de protección
- Conexión y desconexión remota
- Registro de alarmas
- Reloj en tiempo real

Especificaciones Técnicas

Registrador	LCD
Norma	IEC62053-21 IEC62052-11 IEC62053-23 IEC6205
Clase	1.0 Activa / 2.0 Reactiva
Voltaje	3x120/208V
Ib(Im)	5(100)A
Frecuencia	60 Hz

Constante	2400 Imp/kWh
Dispositivo de Corte	Relay Interno
Protocolo de comunicación	DLMS/COSEM
Grado protección	IP54
Puertos de Comunicación	GPRS RS485 M.Bus Puerto Óptico
Temperaturas	Operación: -25°C ~ +60°C Limite: -45°C ~ +70°C

Conexiones



12. CONCLUSIONES

- La alternativa de la implementación de Smart grids y el sistema de medida inteligente en la distribución de energía eléctrica es la solución más viable, ya que otorga múltiples beneficios tales como:
  - ✓ Intercambios bidireccionales de energía
  - ✓ Reducción del consumo
  - ✓ Detección de fraude y pérdidas de energía eléctrica
  - ✓ Reducciones del pico de demanda

- La estructura del Smart meter requiere especialmente del módulo GSM (sistema global de comunicación móvil) ya que por seguridad es la más recomendad, y su función es lograr el medio de comunicación de datos entre el Smart meter y el centro de datos por red celular, ya que se puede tener una rápida accesibilidad del usuario al sistema y se puede evitar por este medio la interferencia.

- Los Smart meters requieren de una alta cobertura de señal de red celular, para evitar posibles lecturas falsas y no tener por consecuencia una tarifación del consumo de energía eléctrica errónea, también es posible que no se pueda actualizar el software del dispositivo ni sus protocolos de seguridad y se podría convertir en un sistema vulnerable.

- Los protocolos de seguridad que se complementen con los Smart meters confirmarán la eficiencia del sistema, ya que con estos protocolos se podrá proteger la integridad y e información del usuario que se incorpore a la red por medio de códigos de verificación, información encriptada, sistemas de autentificación y demás.

- La implementación de la infraestructura de medición avanzada (AMI) en Colombia es un proyecto a largo plazo que resultará beneficioso tanto para las entidades distribuidoras y comercializadoras de energía eléctrica como para los usuarios que cuentan con pocos recursos económicos, ya que esto ayudará a conseguir una monitorización de la red con ayuda de la implementación de medidores inteligentes, conseguirá la disminución del pico de demanda energética y será amigable con el medio ambiente; y para los usuarios reducirá la tarifa en el consumo de energía eléctrica.

13. REFERENCIAS BIBLIOGRÁFICAS

Alegsa, L. (07 de Junio de 2016). *Definicion De Integridad De Datos*. Obtenido de http://www.alegsa.com.ar/Dic/integridad_de_datos.php

BBC, N. (11 de Octubre de 2015). El virus que tomó control de mil máquinas y les ordenó autodestruirse. *El virus que tomó control de mil máquinas y les ordenó autodestruirse*.

Berrio, L. H., & Zuluaga, C. (2014). Smart Grids y La Energía Solar Fotovoltaica Para La Generación Distribuida: Una Revision En El Contexto Energético Mundial. *Ingeniería y Desarrollo*, 376-377.

Borges de Oliveira, F. (Febrero de 2015). *On Privacy Preserving Protocolsfor Smart Metering Systems*.

Calvo, M. (23 de Marzo de 2012). *Que Son Las Energías Renovables*. Obtenido de https://twenergy.com/a/que-son-las-energias-renovables-516

Camargo, C., Sáenz, J., & Rosas, N. (2014). IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD EN MEDIDORES INTELIGENTES (SMART GRIDS). *INGENIUM*, 28-38.

Casellas, F., Velasco, G., Guinjoan, F., & Piqué, R. (s.f.). *El Concepto De Smart Metering En El Nuevo Escenario De La Distribuición Eléctrica*. Obtenido de https://upcommons.upc.edu/bitstream/handle/2117/9066/5025.pdf

CELSIA. (21 de Febrero de 2018). *Epsa moderniza medición del consumo de sus clientes con la instalación de medidores inteligentes.* Obtenido de http://www.celsia.com/es/sala-prensa/epsa-moderniza-medici243n-del-consumo-de-sus-clientes-con-la-instalaci243n-de-medidores-inteligentes

Codensa. (2016). *Medicion Inteligente*. Obtenido de https://www.codensa.com.co/medidor-de-energia-inteligente

Colombia, S. d. (13 de Mayo de 2014). Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1715_2014.html

Corrales, L. (Diciembre de 2007). *DPTO De Automatizacion Y Control Industrial.* Obtenido de Sistemas SCADA: http://bibdigital.epn.edu.ec/bitstream/15000/10020/2/PARTE%202.pdf

Department for business, E. a. (22 de Enero de 2013). *Smart meters: a guide*. Obtenido de https://www.gov.uk/guidance/smart-meters-how-they-work

Diaz Andrade, C. A., & Hernandez, J. C. (1 de Semtiembre de 2011). *Smart Grid: Las TICs y la modernización de las redes de energia electrica.* Obtenido de https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/viewFile/1075/1096

Ecointeligencia. (27 de Febrero de 2014). *La Smart Grids y Sus Fundamentos*. Obtenido de https://www.ecointeligencia.com/2014/02/smart-grid-fundamentos/

Edenhofer, O., Pichs-Madruga, R., Sokona, Y., Seyboth, K., Matschoss, P., Kadner, S., . . . von Stechow, C. (2011). *Fuentes De Energías Renovables y Mitigacion Del Cambio Climatico.* Obtenido de https://www.ipcc.ch/pdf/special-reports/srren/srren_report_es.pdf

Energetika. (06 de junio de 2016). *Red eléctrica inteligente con contadores inteligentes* . Obtenido de http://www.energetika-net.com/vijesti/energetsko-gospodarstvo/inteligentna-elektroenergetska-mreza-moguca-i-bez-pametnih-brojila-22979

Energía, M. d. (29 de Enero de 2018). *Resolución 40072*. Obtenido de https://www.minminas.gov.co/documents/10180//23517//47695-res_40072_290118.pdf

Funes, J. A. (25 de Abril de 2013). *Confidencialidad De La Informacion*. Obtenido de http://www.innsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html

González, I. R., Galván Bobadilla, I., & Camacho Peréz, S. (Octubre-Diciembre de 2012). *SEGURIDAD INFORMÁTICA PARA REDES INTELIGENTES*. Obtenido de https://www.ineel.mx//boletin042012/breve01.pdf

Gonzalez, R. (16 de Diciembre de 2012). Obtenido de https://twenergy.com/a/que-es-la-energia-geotermica-que-aplicaciones-tiene-108

Gonzalez, R. (09 de Mayo de 2012). Obtenido de https://twenergy.com/a/que-es-la-energia-hidraulica-426

Guillermo, J. (2 de Diciembre de 2013). *Stuxnet: historia del primer arma de la ciberguerra*. Obtenido de https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra

Hernandez, L. (16 de Junio de 2014). Obtenido de https://web.fdi.ucm.es/posgrado/conferencias/LuisHernandez-slides.pdf

Hernandez, L. (16 de Junio de 2014). *Smart Grids, smart Metering* . Obtenido de https://web.fdi.ucm.es/posgrado/conferencias/LuisHernandez-slides.pdf

Labib, L., Masum, B., G.M. Sultan , M. R., Md. Nazmus , S., Md. Golam , K., & Md. Rafiqul, I. (6 de julio de 2017). *Design and implementation of low-cost universal smart energy meter with demand*.

Lee, Y., Paredes, J. R., & Lee, S. H. (Agosto de 2012). *Las redes inteligentes de energia y su implementacion en ciudades sostenibles* . Obtenido de http://www.iadb.org/wmsfiles/products/publications/documents/37228055.pdf

Leguizamón, J. A. (2015). *IMPLEMENTACION DE UN SISTEMA DE SEGURIDAD PARA LAS COMUNICACIONES EN MEDIDORES INTELIGENTES DE BAJA TENSION EN SMART GRIDS .* Obtenido de http://www.bdigital.unal.edu.co/51047/1/80039559.2015.pdf

Lopéz, Á. J. (Febrero de 2012). *GESTIÓN DE LA ENERGÍA EN UNA RED INTELIGENTE* . Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/14698/PFC_Angel_J_Gonzalez_Lopez.pdf?sequence=1

Martin, C. (6 de febrero de 2001). *Incidencia ambiental de la generación de electricidad en centrales térmicas*. Obtenido de http://platea.pntic.mec.es/~cmarti3/2000/sesion/eema/termica.htm

Observatorio Industrial del sector de la electronica, t. d. (12 de Mayo de 2011). *SMART GRIDS Y LA EVOLUCIÓN DE LA RED ELECTRICA*. Obtenido de http://www.minetad.gob.es/industria/observatorios/SectorElectronica/Actividades/2010/Federaci%C3%B3n%20de%20Entidades%20de%20Innovaci%C3%B3n%20y%20Tecnolog%C3%ADa/SMART_GRIDS_Y_EVOLUCION_DE_LA_RED_ELECTRICA.pdf

Orallo, E. H. (2004). *Seguridad y privacidad en los sistemas informáticos*. Obtenido de ehernandez@disca.upv.es.

Ortega, E. M. (enero/junio de 2012). *REDES DE COMUNICACIÓN EN SMART GRIDS*.

Porras, E. (16 de Abril de 2012). *Tecnología GSM*. Obtenido de http://eve-ingsistemas-u.blogspot.com.co/2012/04/el-sistema-global-para.html

Ramirez, E. V., Ángeles Camacho, C., & García Martínez, M. (Enero-Marzo de 2013). *Redes De Transmision Inteligente. Beneficios y Riesgos*. Obtenido de http://www.sciencedirect.com/science/article/pii/S1405774313722273#!

Rodriguez, S. J. (2012). Retos De Seguridad En Redes Inteligentes. *Sistemas*, edicion 123.

Rodríguez, S. J. (1 de Abril de 2012). RETOS DE SEGURIDAD EN REDES INTELIGENTES. *Revista Sistemas*. Obtenido de http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no-123/item/94-retos-de-seguridad-en-redes-inteligentes

Rubia, J. L. (JUNIO de 2011). *ESTUDIO SOBRE EL ESTADO ACTUAL DE LAS SMART GRIDS* . Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/12120/PFC_Javier_Lorente_de_la_Rubia.pdf?sequence=1

Sáez, Y., & Collado, E. (2015). Seguridad cibernética en las redes eléctricas inteligentes. *Actualidad Tecnologica* , 1-15. Obtenido de Amenazas y desafios.

Sierra, C. A. (20 de marzo de 2012). *TECNOLOGIA AVANZADA PARA LA MEDICION DEL CONSUMO ENERGETICO EN LOS HOGARES*. Obtenido de http://cidei.net/smart-meters-tecnologia-avanzada-para-la-medicion-del-consumo-energetico-en-los-hogares/

smartme. (Enero de 2013). *Wide Area Network, Home Area Network*. Obtenido de http://www.smartme.co.uk/technical.html

Spain, S. G. (18 de Septiembre de 2016). *Garantizar La Seguridad Y Fiabilidad En Los Contadores Inteligentes*. Obtenido de http://smartgridspain.org/web/blog/2016/09/18/garantizar-la-seguridad-fiabilidad-los-contadores-inteligentes/

SPAIN, S. G. (2016 de septiembre de 2016). *GARANTIZAR LA SEGURIDAD Y FIABILIDAD EN LOS CONTADORES INTELIGENTES*.

Tecnología, A. (2013). *Energía eolica*. Obtenido de http://www.areatecnologia.com/electricidad/energia-eolica.html

TECUN. (2017). *Sistema AMI*. Obtenido de http://tecun.com/que-es-ami/

UPME. (ABRIL de 2016). *SMART GRIDS COLOMBIA VISION 2030.* Bogotá: Grupo Técnico Proyecto BID. Obtenido de SMART GRIDS COLOMBIA VISION 2030: http://www1.upme.gov.co/DemandaEnergetica/Smart%20Grids%20Colombia%20Visi%C3%B3n%202030/3_Parte3B_Proyecto_BID_Smart_Grids.pdf

Ur-Rehman, O., Zivic, N., & Ruland, C. (19 de Agosto de 2015). *Security Issues in Smart Metering Systems*. Obtenido de ieeexplore.ieee.org/document/7324615/

Velasco Martinez, E., Angeles Camacho, C., & Garcia Martinez, M. (01 de Febrero de 2012). *Redes De Transmision Inteligentes, Riesgos Y Beneficios.* Obtenido de http://www.sciencedirect.com/science/article/pii/S1405774313722273#!

Vercelli, A. (26 de Agosto de 2012). *Energía eolica*. Obtenido de http://www.energias.bienescomunes.org/2012/08/26/que-es-la-energia-eolica-3/

Weranga, K. S., Kumarawadu, S., & Chandima, D. P. (2014). Smart Metering Design and Applications. En K. S. Weranga, S. Kumarawadu, & D. P. Chandima, *Smart Metering Design and Applications* (págs. 27-32).

Zakariae, J., Hajar, C., Belkasem, T., & Elhassane, C. (20 de abril de 2017). *Diseño de una placa de calibración integrada en un smart meter*. Obtenido de https://ieeexplore.ieee.org/document/7934603/

Zapata, P. M. (2014). *Barreras Técnicas en las redes de transmisión eléctrica colombianas que dificultan la evolución a redes eléctricas inteligentes.*