Capítulo 8: Aspectos Legales de Sistemas AMR

8.1. Introducción

El marco en el que redes interdependientes y sistemas de distribución proporcionan un flujo confiable de productos y servicios es conocido como Infraestructura Crítica. El término abarca un amplio espectro de servicios fundamentales como son la generación y distribución de electricidad, el suministro de agua o telecomunicaciones, los sistemas de transporte y el suministro de combustibles. La evolución de las tecnologías de la información y la comunicación han facilitado la manipulación, el almacenamiento y el transporte de enormes volúmenes de datos e información. Este hecho ha motivado el uso de la tecnología de la información para dar soporte a las infraestructuras críticas logrando una prestación de servicios económicamente rentables y eficientes en tiempo.

Por otro lado, el uso de infraestructuras de Tecnología de la Información (TI), implica la exposición de infraestructuras críticas a nuevos riesgos relacionados con la seguridad de los datos y los potenciales peligros de operación de estos sistemas.La seguridad de un sistema está fuertemente relacionada con el concepto de fiabilidad definida como la capacidad de un sistema para prestar servicio de forma eficaz y sin interrupciones. Esto implica que cualquier manipulación o alteración no autorizada en el sistema debe ser prevenida y/o detectada.

En el caso concreto de un sistema AMR, la importancia de salvaguardar el acceso a los datos deriva de la gravedad de las posibles consecuencias que conllevaría un acceso indebido a la información del sistema [9]:

- Fraude mediante la alteración de la lectura del contador para reducirlo por debajo de los niveles de consumo reales.
- Obtención del control de ciertos dispositivos con capacidad para desconectar la alimentación de un determinado electrodoméstico en el hogar del abonado.
- Posibilidad de acceso a los datos de consumo de un abonado con intenciones maliciosas. Por ejemplo, un bajo consumo indica que el usuario está fuera de casa durante largos períodos de tiempo lo que podría ser aprovechado para realizar un robo.
- Capacidad para desconectar todo el suministro.

8.2. Integridad y Seguridad de los Datos

La seguridad de los sistemas AMR debe ser una prioridad fundamental. En este sentido es habitual el uso de mecanismos de seguridad como la autenticación y el cifrado en cada una de las capas que componen este tipo de sistemas.

Para proteger la privacidad del cliente y asegurar la integridad los datos, cada paquete de información que es enviado desde el contador al software del centro de control del sistema y viceversa debe ser autenticado y cifrado de extremo a extremo. El objetivo de estas medidas de seguridad es evitar ataques externos, manipulación o falsificación de datos, suplantación de dirección y cualquier intento de fraude o manipulación en el sistema en general [9].

El software de gestión debe incorporar un modelo de seguridad para acceder, recuperar, visualizar, exportar y modificar los datos, basado en roles y responsabilidades. Los usuarios del software del centro de control deben ser agrupados en grupos de usuarios con permisos de acceso asignados de acuerdo con roles específicos definidos de antemano.

Cada acción llevada a cabo en el sistema debe ser almacenada en el registro de eventos. Este almacenamiento de las acciones puede ser empleado como un elemento de mantenimiento preventivo. Si hubiera una pérdida de datos en el sistema, haciendo uso del registro de eventos y de una copia de seguridad de datos, sería posible volver el sistema a un estado previo a la pérdida ocurrida. Por otra parte, si alguien hiciera (deliberadamente o no) un mal uso del sistema sería posible verificar el registro para determinar quién ha sido el responsable.

8.2.1. Integridad de los Datos

El software de un sistema AMR debe ser instalado en un centro de control seguro con una red de acuerdo con los estándares de seguridad. Así, dado que el acceso al sistema debe ser gestionado en el centro de control, el software AMR debe hacer uso de clave de seguridad para validar el acceso de las diversas aplicaciones a los datos. Para proteger al sistema ante ataques externos o accesos indebidos a los datos, ésta clave debe expirar en un número configurable de minutos.

El software del sistema debe integrarse con los mecanismos de seguridad de la base de datos de modo que la configuración de los datos almacenados no pueda ser visualizada y/o modificada por terceras partes no autorizadas. Así mismo, el acceso a los datos temporales, a la espera de ser tratados por una aplicación de nivel superior, debe ser también protegidos a través de mecanismos de seguridad.

En el proceso de fabricación debe instalarse una contraseña para asegurar el control de acceso a cada contador. Puesto que los contadores serán manipulados por un número elevado de instaladores, la política de seguridad debe asumir la posibilidad de

que algunos de los instaladores se vean tentados a manipular los dispositivos. Una vez operativos, los contadores contienen datos valiosos que deben ser transferidos de forma segura a la compañía eléctrica.

Como hemos visto, los contadores cuentan, en general, con dos puertos de comunicación. El puerto de comunicación PLC/Mesh Radio para la conexión con el concentrador de datos aguas arriba y el puerto de configuración local. El acceso a cada uno de estos puertos debe ser preservado durante las fases de transporte, instalación y operación del sistema.

Adicionalmente, una vez que los aparatos son instalados y puestos en funcionamiento, no es necesario que los instaladores tengan acceso. Por tanto, el personal de instalación no necesita tener acceso a las contraseñas y claves de seguridad que podrían facilitar el libre acceso a estos puertos. La única excepción sería el personal encargado de modificar el programa de los contadores de forma previa a la instalación. Para estos casos la herramienta de configuración puede hacer uso de una contraseña única para reprogramar el contador. Estas contraseñas son transportadas como contraseñas cifradas AES (Advanced Encryption Standard) de modo que el operador no visualice la contraseña real.

8.2.2. Seguridad de los Datos

La norma ANSI/CEA-709 / EN 14908 regula la seguridad y la fiabilidad de las redes de control sobre líneas eléctrica, empleadas en los sistemas AMR cuyas comunicaciones usan PLC, en lo que respecta a las capas físicas y de enlace.

En lo que respecta a la seguridad en la capa de aplicación, a fin de aumentar la fiabilidad del sistema y la seguridad, cada fabricante de contadores hace generalmente uso de mecanismos de seguridad adicionales. Entre estos mecanismos destacan el uso de claves extendidas y cifrado de seguridad multicapa.

La comunicación entre los contadores y los concentradores de datos debe ser asegurada en ambos sentidos haciendo uso de la autenticación ANSI/CEA-709 / EN 14908 en el caso de comunicación PLC. La clave de autenticación debe ser instalada en el contador en el proceso de fabricación, siendo su conocimiento imprescindible para modificar los parámetros de red o escribir en las tablas del contador.

Los concentradores de datos, generalmente basados en IP, deben incluir las mismas normas de seguridad y fiabilidad en la comunicación aguas abajo y emplear estándares abiertos y seguros para la comunicación WAN aguas arriba con el centro de control. El software del sistema y los concentradores de datos deben autenticarse mutuamente. Algunas opciones de autenticación son CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft CHAO), o 160 bit SHA-1 (Secure Hash Algorithm 1). La transferencia de datos a través de la WAN entre los concentradores de datos y el software del centro de control debe ser autenticada y encriptada

utilizando módems GSM (Groupe Spécial Mobile), GPRS (General Packet Radio Services), EDGE (Enhanced Data rates for GSM of Evolution), etc. Adicionalmente, es posible establecer una VPN (Virtual Private Network) entre todos los puntos con el fin de mejorar la seguridad.

8.3. Diseño e Ingeniería de la Seguridad de los Datos

El proceso de diseño e ingeniería de seguridad incluye el desarrollo de planes detallados y diseño de sistemas, controles y funciones de seguridad. El objetivo es obtener planes y políticas que satisfagan los requisitos de seguridad predefinidos para un sistema dado y garantizar su seguridad mediante la prevención de mal uso o ataques externos maliciosos al sistema.

El resultado es un conjunto de reglas y directrices que deben ser tomadas en consideración desde la propia fase de diseño e implementación del sistema, hasta que el sistema quede obsoleto incluyendo las fases de desarrollo intermedias. A continuación, se detallan las claves para garantizar la seguridad de la información en un sistema AMR [9].

8.3.1. Seguridad en el Tiempo

Un sistema que es seguro hoy no garantiza que será seguro mañana.

La garantía de la seguridad de la información a través de los sistemas automáticos de lectura de contadores requiere una planificación cuidadosa y exhaustiva desde las primeras etapas de desarrollo del sistema. La seguridad del software ha sido tradicionalmente tratada como una cuestión secundaria, lo que obviamente resulta en un nivel de seguridad cuestionable.

La importancia de abordar la seguridad en todas las etapas del desarrollo del sistema AMR incluye el momento en el que se vuelve obsoleto y debe ser eliminado de la producción.

Se detallan a continuación las etapas del modelo de desarrollo.

1. Especificación de Requisitos

   Los requisitos de seguridad, incluyendo la identificación de la información a proteger, los diferentes niveles de seguridad y los derechos de acceso, deben ser recogidos en los requerimientos tanto funcionales como no funcionales del sistema.

   En el caso de un sistema AMR deben protegerse las lecturas periódicas de los contadores y los datos del perfil de clientes. Sin embargo, puesto que los procesos son también los recursos, es vital proteger también la activación/desactivación de los servicios.

2. Análisis y Diseño

   Denota la identificación de posibles ataques maliciosos y vulnerabilidades del sistema, y el planteamiento de las medidas para garantizar la fiabilidad y la seguridad del sistema.

3. Implementación

Durante el proceso de desarrollo del sistema deben aplicarse los mecanismos de seguridad más adecuados, como protocolos de seguridad informática con métodos de cifrado, cortafuegos, mecanismos de control de acceso de los usuarios, y elección de emplazamientos físicos seguros para los componentes hardware del sistema.

4. Integración y Pruebas

Una vez ha sido implementado el sistema, antes de la puesta en producción, deben integrarse y probarse los diversos componentes del sistema. Desde una perspectiva de seguridad deben ejecutarse ataques contra el sistema para verificar la resistencia del sistema ante ataques malintencionados. Si fuera necesario, se desarrollarían acciones correctivas en base a los resultados de estas pruebas.

Todos los componentes del sistema incluyendo contadores, servidores del centro de control e infraestructura de comunicación deben ser testeados.

5. Mantenimiento

Garantizar la seguridad de la información en esta fase es un proceso en curso. Una vez que el sistema AMR se encuentra en producción, la seguridad debe ser garantizada mediante la ejecución periódica de análisis del sistema y auditorias de seguridad para evaluar el estado del sistema desde un punto de vista de la seguridad.

El objetivo de las auditorias es realizar una inspección completa del sistema, incluyendo componentes físicos y lógicos, como por ejemplo la inspección de la seguridad de los emplazamientos físicos de los equipos o los métodos de cifrado de seguridad de los protocolos utilizados. Dada la naturaleza cambiante de este tipo de sistemas en los que las aplicaciones existentes son continuamente ajustadas o nuevos servicios son añadidos y puesto que nuevas amenazas surgen todos los días, estas auditorias son muy importantes para acomodar los nuevos requisitos de seguridad si fuera necesario.

6. Obsolescencia

Además de los procesos anteriormente descritos, resulta crucial incluir una fase adicional en la vida del sistema, durante el cual el sistema sea progresivamente sacado de producción.

¿Qué sucede con los datos una vez que el sistema esta permanentemente fuera de servicio? Normalmente cuando el sistema deja de estar en producción los datos no son eliminados, sino que siguen siendo confidenciales y deben ser protegidos contra accesos no autorizados. Los procedimientos de seguridad para esta fase

deben ser cuidadosamente planificadas con antelación incluyendo por ejemplo, donde se van a almacenar los datos o quién tendrá acceso a los mismos.

8.3.2. Amplitud del Sistema

El concento de amplitud implica garantizar la seguridad de la información para todos los componentes del sistema AMR, incluyendo los componentes físicos y lógicos, la red del sistema y las interacciones entre estos componentes. La importancia de este aspecto se debe a la naturaleza de los sistemas de tecnología de la información (altamente interconectados) lo que facilita el acceso desde redes tanto internas como externas.

Para garantizar la seguridad de la información en todo el sistema es necesario identificar todos los componentes del mismo y elegir el método más apropiado para cada uno de estos componentes.

Las interacciones entre estos componentes son fundamentalmente intercambios de información a través de medios de red que aumentan el nivel de exposición a ataques externos (los datos transmitidos son más vulnerables que los datos almacenados). Por esto, es necesario para prestar especial atención a la seguridad tanto física como lógica de los medios de interacción de los sistemas AMR para garantizar que la información se mantiene intacta y confidencial.

8.3.3. Profundidad del Sistema

El concepto de profundidad se refiere a la protección de la información de los sistemas AMR a todos los niveles dentro de cada componente del sistema incluyendo las capas física, de red, de operación, de soporte y de aplicación.

La capa física comprende los elementos hardware de cada componente, mientras que la capa de red abarca los elementos físicos y lógicos que facilitan el intercambio de información entre los actores del sistema AMR transmitiendo información a través de medios los de comunicación.

El sistema operativo da soporte a la capa software, diseñada para controlar el hardware del sistema con el fin de permitir a los usuarios y programas de aplicación para hacer uso del mismo. La capa de soporte incluye un conjunto de aplicaciones que extienden la funcionalidad del sistema operativo a fin de apoyar las aplicaciones en ejecución. Por último, la capa de aplicación da soporte a los programas en operación para lograr el objetivo predefinido del sistema.

Además de hacer cumplir las medidas de seguridad en todos los componentes del sistema, la seguridad debe también aplicarse en cada una de sus capas utilizando herramientas de seguridad adecuadas para cada capa.

8.3.4. Actores del Sistema

Los diferentes actores del sistema deben contar una interfaz segura a través de la cual beneficiarse de los servicios disponibles y realizar tareas que requieran acceso y manipulación de la información del sistema [9]. Para ello deben considerarse desde las primeras etapas del diseño del sistema, los siguientes aspectos:

1. Definición de los activos de información

   La información almacenada en los servidores de un sistema AMR comprende datos de distinta naturaleza y sensibilidad, lo que implica también que los grados de seguridad requeridos son diversos. Esto implica que la información que está siendo generada y mantenida debe estar clasificado en diferentes categorías en función de su nivel de confidencialidad.

   El estándar ISO / IEC 27002 detalla la clasificación de los activos de información.

2. Definición de las clases de usuario

   Para definir las clases de usuario del sistema es necesario identificar a los diversos actores del sistema y sus respectivos requisitos de acceso a la información. En un sistema AMR se incluyen entre otros administradores, operadores, proveedores de energía y consumidores. Cada uno de estos usuarios se corresponde con clases de usuario diferentes en función de la información a la que pueden acceder y el nivel de manipulación permitido sobre dicha información.

3. Definición de roles

   El objetivo de este paso es combinar las clases de usuario con las categorías de información haciendo uso de roles. Para ello es necesario asignar a los actores del sistema AMR, categorizados de acuerdo con las clases de usuario definidas en el paso 2, privilegios de acceso y manipulación adecuados de acuerdo con la clasificación establecida en el paso 1.

4. Derechos de acceso a activos físicos y lógicos

   Además de los activos de información, los sistemas AMR cuentan con otro tipo de activos que también requieren protección. Estos activos pueden ser de carácter físico o lógico como por ejemplo la salas de servidores o el sistema operativo y las aplicaciones AMR. Los privilegios de acceso al sistema de cada actor deben ser asignados de modo que tengan acceso a los activos necesarios para llevar a cabo su trabajo previniendo la visualización o manipulación de otros activos que no forman parte de sus derechos de acceso predefinidos.

5. Registros de seguridad

   Los registros de seguridad deben almacenar automáticamente los eventos que se produzcan en el sistema a fin de proporcionar un modo de rastrear la actividad en

el sistema y diagnosticar problemas. El registro de eventos resulta de gran utilidad en situaciones en violación de seguridad debido a errores internos o malas prácticas. Haciendo uso de estos registros es posible analizar las incidencias, restaurar valores de medidas y modificar las políticas de seguridad para evitar que tales escenarios se repitan.

6. Capacitación de usuarios

Proporcionar a los usuarios formación sobre cómo utilizar el sistema es una parte básica de la implementación de un sistema. Durante este proceso, una serie de sesiones de formación a medida deben ser impartidas a cada grupo de usuarios.

De este modo, mediante la definición de actores se garantiza la seguridad de la información definiendo los roles de cada actor dentro del sistema y monitorizando sus comportamientos para certificar el uso legal del sistema.

8.4. Regulación Normativa del Sector

En lo referente a la exactitud de los equipos de medida de energía eléctrica, los estándares fundamentalmente aplicables son:

- ANSI C12.20 en Estados Unidos.
- IEC 62053 en Europa.
- UNE-EN62053 en España.

8.4.1. Normativa en USA

Los sistemas AMR son ampliamente promovidos en Estados Unidos. Así, de conformidad con la sección 1253 (e) (3) del Acta de Política Energética de 2005 (EPAct 2005), la Comisión Federal Reguladora de la Energía (FERC) del gobierno de los Estados Unidos reportó en 2009 un aumento del interés con respecto a la demanda de energía eléctrica y los sistemas AMR [46].

Tomando en consideración los datos obtenidos en el informe de 2008, las estimaciones de respuesta a la demanda potencial consideran un escenario de implementación parcial de los sistemas AMR con unos 80 millones de contadores instalados en 2019. Los resultados ilustran cómo la respuesta a la demanda potencial aumenta en varios supuestos, tales como el número de clientes participantes y el uso de aparatos eléctricos "inteligentes" con tarifas eléctricas dinámicas en función de las condiciones del sistema [13].

Comparando el escenario de participación completo con el escenario de negocio tradicional, el informe estima que los programas de respuesta a la demanda podrían reducir para 2019 la carga hasta en 150 GW.

En julio de 2009, la FERC emitió la normativa sobre redes inteligentes para orientar y priorizar el desarrollo de los sistemas y dispositivos inteligentes, y adoptar una política de tarifa parcial para fomentar la inversión en tecnología de redes inteligentes. La Comisión señaló la evolución hacia las redes inteligentes como fundamental para afrontar los desafíos de respuesta a la demanda actuales, siendo prioritario el desarrollo de normas para mejorar la interoperabilidad y las comunicaciones entre los operadores del sistema y los recursos de respuesta a la demanda.

Al menos diez estados han emitido planes integrales de energía a largo plazo para permitir un mayor despliegue de sistemas AMR y de respuesta a la demanda incluyendo California, Hawai, Kentucky, Massachusetts, Michigan, Nebraska, Nueva Jersey, Ohio, Pennsylvania y Vermont. Los Estados y las compañías eléctricas han adoptado medidas específicas en lo referente a sistemas AMI y programas piloto de despliegue de contadores inteligentes, tarifas de precios dinámicos y respuesta automatizada a la demanda.

Los programas de tarificación dinámica se refieren al conjunto de tarifas ofrecidas a los clientes con un día de antelación o en tiempo real. Con este esquema, los precios son dinámicos en el sentido de que cambian en respuesta a eventos tales como horas de alta demanda, días extremadamente calurosos o las condiciones de fiabilidad.

La evaluación incluye un examen detallado de los obstáculos, incluidos los obstáculos reglamentarios para dar respuesta a la demanda, junto con recomendaciones sobre cómo abordar estos obstáculos:

- Intercambiar información de acuerdo con programas efectivos.
- Educar al cliente sobre los programas de respuesta a la demanda.
- Coordinar estrategias masivas de respuesta a la demanda.
- Mejorar y ampliar la interoperabilidad y los estándares abiertos.
- Coordinar políticas de respuesta a la demanda y eficiencia energética.
- Articular claramente el papel de la respuesta a la demanda en la planificación operacional y largo plazo, y la recuperación de los costos asociados.

8.4.2. Normativa en Europa

Bajo la Directiva 2006/32/CE del Parlamento Europeo y del Consejo de 5 de abril de 2006 sobre la eficiencia del uso final de la energía y los servicios energéticos y por la que se deroga la Directiva 93/76/CEE del Consejo, los Estados miembros de la Unión Europea están obligados a legislar con el fin de obtener información sobre el consumo con frecuencia suficiente.

Entre otros, el objetivo es regular el despliegue de los sistemas AMR en ciudades y pueblos como parte de la meta de aumentar la eficiencia energética.

Dicha Directiva fomenta la mejora de la eficiencia en el uso final de la energía en los Estados miembros aportando objetivos orientativos, así como mecanismos, incentivos y normas generales institucionales, financieras y jurídicas necesarias para eliminar los obstáculos existentes en el mercado y los defectos que impidan el uso final eficiente de la energía [45].

De acuerdo con el artículo 6, los Estados miembros, los distribuidores de energía, los operadores de sistemas de distribución y las empresas minoristas de venta de energía deben proporcionar información estadística agregada sobre los clientes finales a los organismos responsables del control y vigilancia de las normas establecidas en relación con los objetivos de ahorro energético. Esta información debe ser suficiente para elaborar y aplicar adecuadamente programas de mejora de la eficiencia energética, promover y efectuar el seguimiento de los servicios energéticos y de otras medidas de mejora de la eficiencia energética.

La información podrá incluir datos pasados y deberá incorporar datos actuales sobre el consumo de los usuarios finales, incluidos los perfiles de carga, la segmentación de clientes y la localización geográfica de los clientes, preservando al mismo tiempo la integridad y la confidencialidad de la información de carácter privado o comercialmente sensible, de conformidad con la legislación comunitaria aplicable.

Por otro lado y de acuerdo con el artículo 13, referente a la medición y facturación informativa del consumo de energía, los Estados miembros deben velar porque siempre que sea técnicamente posible, financieramente razonable y proporcionado en relación con el ahorro de energía potencial, los clientes finales reciban contadores individuales a un precio competitivo, que reflejen exactamente el consumo real de energía del cliente final y que proporcionen información sobre el tiempo real de uso.

Dichos contadores deben ser proporcionados siempre que se realice una nueva conexión en un edificio nuevo o cuando se lleven a cabo obras de renovación de envergadura. Cuando se sustituya un contador existente, salvo que sea técnicamente imposible o no resulte rentable en comparación con los ahorros potenciales estimados, deberá proporcionarse un contador individual a un precio competitivo [14].

Los Estados miembros deben velar porque la facturación realizada por distribuidores de energía, operadores de sistemas de distribución y las empresas de venta de energía esté basada en el consumo real de energía, y se presente en términos claros y comprensibles facilitando con la factura información apropiada para que los clientes finales reciban las cuentas completas del coste energético actual. La facturación basada en el consumo real debe ser realizada con la frecuencia suficiente para permitir a los clientes regular su propio consumo de eléctrico.

Facturas, contratos y recibos al cliente final deben ser redactadas de forma clara y comprensible, incluyendo:

- Los precios reales actuales y el consumo real de energía.
- Preferentemente en forma gráfica, la comparación del consumo actual de energía del cliente final con el consumo durante el mismo período del año anterior
- La comparación con un usuario de energía medio, normalizado o de referencia perteneciente a la misma categoría de usuario.
- La información de contacto con las organizaciones de consumidores, las agencias de energía u organismos similares, incluidas las direcciones de Internet en donde puede encontrarse información sobre medidas de mejora de la eficiencia energética, perfiles comparativos del consumidor final y especificaciones técnicas de los equipos que utilizan energía eléctrica.

8.4.3. Normativa en España

El Real Decreto 809/2006 establece que a partir del 1 de julio de 2007, los equipos de medida a instalar para nuevos suministros de energía eléctrica hasta una potencia contratada de 15 kW y los que se sustituyan para los antiguos suministros deben permitir la discriminación horaria de las medidas y la telegestión. Asimismo, habilita al Ministerio de Industria, Turismo y Comercio para establecer un Plan de sustitución de contadores de medida antiguos por contadores que permitan la discriminación horaria de las medidas en todos los suministros de energía eléctrica hasta una potencia contratada de 15 kW.

El Plan de Sustitución de Contadores vigente en la actualidad obliga a la sustitución gradual de todos los contadores electromecánicos por contadores electrónicos capaces de trabajar con discriminación horaria y telegestión para finales de 2018 [47].

El denominado Plan Contador concede al consumidor la iniciativa para disfrutar del derecho a disponer de los nuevos equipos de medida. Para ello deberán pedir a la compañía distribuidora el adelanto de la sustitución de sus contadores, la cual dispondrá de un periodo máximo de 9 meses para atender tal solicitud.

Para los consumidores, la principal ventaja de disponer de un contador de nueva generación es que podrá gestionar de manera más eficiente sus consumos y beneficiarse de la Tarifa de Último Recurso con discriminación horaria, modalidad de tarificación que puede suponer importantes ahorros de alrededor del 10% a los abonados. Durante un año y con objeto de que los consumidores acogidos al Plan Contador puedan apreciar estos descuentos, las compañías eléctricas deben informarles de forma estimada en sus facturas del coste de la facturación que tendrían si estuvieran acogidos a la modalidad de Tarifa de Último Recurso con discriminación horaria.

A su vez, en la factura recibirán información del margen de ahorro de energía posible de cada consumidor, incluyendo la comparación entre el perfil de su suministro y el perfil de consumo tipo al que corresponde.

Los consumidores acogidos a este Plan podrán solicitar a la empresa comercializadora de último recurso el cambio a la tarifa de último recurso con la modalidad de discriminación horaria en cualquier momento y la sustitución de equipos de medida en aplicación del Plan Contador no dará lugar a coste alguno de instalación.