UNIVERSIDAD
DE LA REPUBLICA
URUGUAY

FACULTAD DE INGENIERIA

Análisis de seguridad del protocolo DLMS/COSEM en el contexto de Smart Grids: Estado del arte

Joaquín Márquez

Gabriel Rodríguez

Proyecto de grado en Ingeniería en Computación
Facultad de Ingeniería
Universidad de la República

Montevideo – Uruguay

Febrero de 2020

Tabla de contenidos

Capítulo 1

IoT

Nos encontramos ante un crecimiento cada vez mayor en la cantidad de dispositivos inteligentes que se encuentran conectados entre sí y a Internet. A través de redes cada vez más complejas dichos dispositivos intercambian datos y realizan acciones en el entorno donde se encuentran, adaptándose dinámicamente a éste. Surge así un nuevo paradigma tecnológico al que llamamos "Internet de las Cosas", o IoT en su sigla en inglés, denominando de esta manera al ecosistema generado por la interconexión de los dispositivos.

1.1. Definiciones

La expresión "Internet de las cosas" está ganando cada vez más y más popularidad. Fue utilizada por primera vez en 1999 por el británico Kevin Ashton, pionero en tecnología e investigador en el MIT, y se encuentra entre las tecnologías estratégicas con mayor tendencia a nivel mundial, abarcando cada vez más dispositivos e incrementando sus implicancias económicas año a año. [1]

A la hora de definir IoT, varias instituciones y agentes han realizado aportes y propuesto definiciones propias pero aún no se dispone de una única definición acordada y consensuada por todos éstos. Entre las definiciones propuestas se encuentran las que se presentan a continuación.

Por un lado, la agencia ENISA (Agencia en Ciberseguridad de la Unión Europea) define IoT como:

"Ecosistema ciberfísico de sensores y agentes interconectados, que da lugar a la toma inteligente de decisiones". [2]

El comité ISO/IEC, por su lado, brinda la siguiente definición:

"Infraestructura donde objetos, personas, sistemas y fuentes de información se encuentran interconectados entre sí y con servicios inteligentes que les permiten procesar información del mundo físico y virtual y reaccionar". [3]

El instituto IEEE también publica su propia definición de IoT en [4], describiéndolo como:

"Red cableada o inalámbrica de dispositivos conectados, únicos e identificables que son capaces de procesar datos y comunicarse entre ellos, con y sin el involucramiento humano".

Para la agencia ITU de la ONU, IoT se define como:

"Una infraestructura global para la sociedad de la información, permitiendo servicios avanzados al interconectar cosas (físicas y virtuales) basados en tecnologías de información y comunicación interoperables ya existentes y nuevas que continúan evolucionando". [5]

Definiciones desde otras perspectivas también han sido propuestas, como la siguiente del autor Stephan Haller:

"IoT es un mundo donde los objetos físicos son perfectamente integrados a la red de información y pueden convertirse en participantes activos de procesos de negocio". [6]

Es interesante observar cómo, si bien las definiciones surgen desde enfoques distintos, el concepto de conectividad entre objetos se encuentra presente en todas ellas, siendo uno de los elementos constitutivos de IoT.

Por último, es importante observar que los objetos en IoT necesitan conectividad entre sí, pero no así una conexión a internet propiamente dicha. Los objetos deberán poder enviar los datos recolectados a otros objetos capaces de procesarlos, y/o a través de una conexión a Internet. Es así que el uso de la palabra Internet en IoT debe ser vista solamente como una generalización que busca transmitir la idea de conectividad y no como un requerimiento técnico necesario. [2]

1.2. Consideraciones iniciales

Según el último reporte sobre tecnologías móviles de la compañía Ericsson de junio de 2019, en 2018 se contabilizaron alrededor de 8.600 millones de dispositivos IoT en todo el mundo, y se estima que dicha cifra aumente a 22.300 millones para

el año 2024. [7]

Según afirman los autores en [1], nos encontramos muy cerca de ser testigos del surgimiento de un mega mercado, donde mercados como los de automatización del hogar y la construcción, generación y distribución de energía eléctrica, logística y automotriz, así como también el de telecomunicaciones y tecnología de la información, van a converger de forma constante.

IoT es la evolución natural de la computación, y está demostrando tener una naturaleza penetrante, al encontrarse en el centro de una inmensa cantidad de infraestructuras críticas y no críticas. Su pertinencia es cada vez mayor en casi todos los aspectos de la vida cotidiana. IoT tiene la capacidad de agregar inteligencia a objetos de uso común, permitiendo aumentar la utilidad de los mismos, obtener mayor información y aumentar la automatización. [2]

Desde el punto de vista del usuario, IoT no es una tecnología que se experimente ni utilice en sí misma, sino que el mismo irá notando la presencia de cada vez más dispositivos conectados entre sí. Actividades diarias que en un principio no tenían puntos de contacto, se ven interconectadas exponenciando sus capacidades, creando nuevos formatos y modelos de negocio. [1]

En [1] se observa cómo en IoT se combinan la presión que ejerce el avance tecnológico y la búsqueda humana por más, en un contexto de cada vez más conectividad y en un ambiente donde suceden una infinidad de sucesos. Se genera así, en palabras de los autores, una extensión lógica del poder de computación de una máquina hacia el ambiente, transformándose éste en una interfaz en sí misma. Esta combinación hace de IoT un paradigma fuerte, imparable, rápido y extremadamente disruptivo.

IoT ha cambiado las formas en que se comunican máquinas con otras máquinas, con su "tecnología operacional" (OT), con nuevas plataformas IT que les agregan nuevas capacidades, y finalmente con los propios humanos los cuales utilizan y controlan dichas máquinas. [8]

Es aquí donde se presenta uno de los tantos desafíos de IoT, la necesidad de entender y mejorar la interacción humana con las máquinas. Según [1], cada vez más, IoT afectará las vidas de todas las personas en mayor y menor medida, con la posibilidad de que esto no sea transparente a las mismas. Dispositivos de distinta índole se comunicarán y enviarán datos mutuamente sin el consentimiento explícito de los usuarios, con posibles acciones no esperadas y consecuencias no intencionadas. Estas posibilidades, una vez percibidas, podrán aumentar la ansiedad de los usuarios

y plantean varios dilemas a resolver.

IoT generará nuevas dificultades que los autores de [1] llaman de "integridad contextual", principio que refiere a que no se espera, por parte del usuario, que información suministrada para ser utilizada en un contexto sea utilizada en otro. Existirá entonces algo así como un "contrato social" entre personas y objetos, donde todas sus ramificaciones éticas deberán ser consideradas.

Por otro lado, ENISA advierte en [2] que IoT conlleva desafíos adicionales. Estos nuevos ecosistemas aún se encuentran en una fase inmadura, enfrentándose a la fragmentación en la definición de estándares y a problemáticas de seguridad en un entorno para nada homogéneo, donde cada mercado, industria y aplicación tiene un uso diferente y particular de la tecnología.

Las soluciones y los proveedores IoT actuales, si bien han progresado, necesitan hacerlo mucho más para poder desbloquear todo el potencial de IoT como paradigma. Mejoras en las plataformas y dispositivos IoT serán esenciales para poder ejecutar técnicas de análisis de datos cada vez más complejas, como el aprendizaje automático y la inteligencia artificial. [8]

Si bien es claro que IoT ya está teniendo un impacto significativo en el mundo, aún nos seguimos encontrando frente tecnologías y modelos de negocio inmaduros, a los que les falta continuar evolucionando y desarrollándose. [8]

El potencial que tiene IoT en obtener resultados exitosos en diferentes áreas es realmente alto, ya sea en la medicina, haciendo posibles sistemas capaces de obtener retroalimentación sobre nuestro estado de salud, o en la industria, generando la mejor distribución de recursos posible. IoT permitirá la toma de decisiones cada vez más inteligentes, basadas en información en tiempo real y de otras fuentes, y que podrá ser utilizada por áreas cada vez más diversas. [1]

Nuevas ideas, conceptos y tecnologías aparecen de forma constante, mientras que otros desaparecen por ser incompatibles o inviables. Es así que dentro del concepto IoT, que es en sí mismo disruptivo, otras tecnologías también potencialmente disruptivas podrán influir en la dirección del desarrollo tecnológico y las discusiones políticas y societales relacionadas. [1]

1.3. Componentes

Los ecosistemas IoT tienen un alto grado de complejidad, con un variado número de elementos que los componen con distintas características. En [2] los autores detallan y describen los mismos de la siguiente manera:

- *"Things" o "cosas"*
  En el contexto de IoT, una "cosa" es un objeto físico o virtual capaz de ser identificado e integrado en una red de comunicación. Una de sus características principales es su capacidad de comunicación con otras "cosas", es necesario que los objetos puedan intercambiar datos a través de algún medio. Además, estos objetos son manejados por sistemas inteligentes que se encargan de monitorearlos y controlarlos. De esta forma, distintos tipos de datos obtenidos por los objetos son recuperados y procesados, y a partir de ellos decisiones inteligentes son tomadas.

- *Toma inteligente de decisiones*
  Se incorpora la noción de que las cosas realizan acciones dentro del ecosistema. Es en este sentido en el que se requiere que exista una toma inteligente de decisiones que resulten en acciones específicas que brinden valor.
  Surge la necesidad de disponer de técnicas para el análisis y manejo de la inmensa cantidad de datos que los dispositivos generan que nos permitan extraer toda la información valiosa posible. La capacidad e inteligencia de la toma de decisiones dependerá casi en su totalidad de la información de la que se disponga.
  Por otro lado, el análisis no necesariamente debe realizarse localmente, sino que puede ser delegado a otro elemento del ecosistema.

- *Sensores y "actuators"*
  En el nivel físico, los sensores pueden medir distintos indicadores físicos, químicos o biológicos definidos, y en el nivel digital, recolectan información sobre las redes y aplicaciones con las que interacciona o es parte. Los sensores son una de las piezas fundamentales del ecosistema IoT, dado que permiten monitorear el ambiente y contexto en el que opera. A partir de los datos recabados por los sensores, los sistemas pueden adaptarse dinámicamente y optimizar procesos.
  Por otro lado, los "actuators" son aquellos responsables de mover o controlar un sistema o mecanismo. Podría decirse que operan en sentido inverso a los sensores, dado que generan, a partir de una entrada eléctrica, una acción física.

Los sensores funcionan como dispositivos de entrada, obteniendo datos del entorno que luego serán procesados, mientras que los "actuators" serían los dispositivos de salida, ejecutan decisiones en base a la información procesada.

- *Sistemas embebidos*
  Los sensores y "actuators", además de poder ser parte del ecosistema por sí solos, pueden también encontrarse embebidos en sistemas con capacidades adicionales. Entre ellas, se encuentran las capacidades de conexión a redes (ya sean LAN o la nube) y de ejecutar software. Los sistemas embebidos pueden disponer de una memoria y de una unidad de procesamiento para poder analizar y procesar los datos recabados por su cuenta. El diagrama de la figura 1.1 muestra la estructura de un sistema embebido.

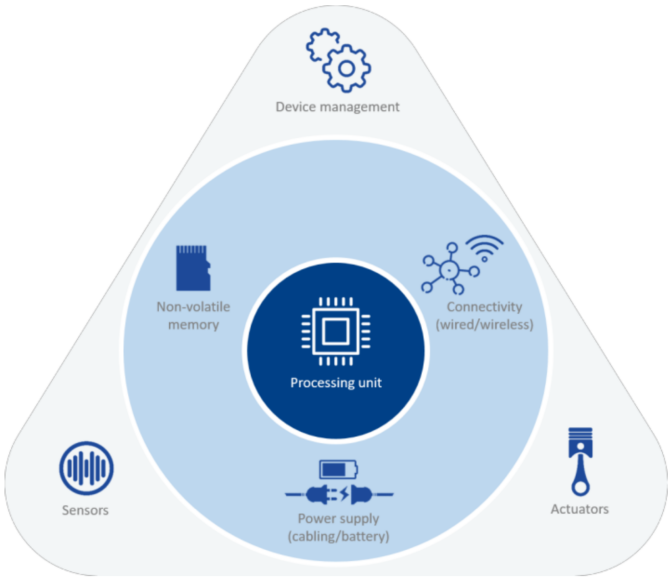

Figura 1.1: Estructura de un sistema embebido IoT [2]

- *Comunicaciones*
  Dada la gran variedad de dispositivos y objetos que forman parte de este ecosistema, los sistemas de comunicación dependen de la capacidad tanto para transmitir como para recibir unidades de información de manera estructurada. Las cosas y los servicios con los que se comunican pueden estar tanto cerca como lejos físicamente, dando lugar al uso de tipos diferentes, pero interoperables, de redes. Éstas gozan de diferentes grupos de propiedades como QoS, resiliencia, seguridad y capacidad de ser gestionadas.
  Los protocolos de comunicación usados en IoT pueden ser tanto inalámbricos como basados en cableado. Se utilizan protocolos de radio de corto y largo alcance, de redes móviles inalámbricas y de comunicaciones cableadas tanto

basadas en IP como no, conformando un gran abanico de protocolos posibles. La tabla de la figura 1.2 lista diferentes protocolos usados en IoT agrupados por capa de comunicación. La capa de enlace controla la conexión entre dispositivos a través de enlaces físicos, tanto cableados como inalámbricos, por ejemplo, entre varios sensores o entre un sensor y el gateway que lo conecta a internet.

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

Figura 1.2: Tabla de protocolos de comunicación para IoT por capa [2]

Los componentes de un ecosistema IoT también son descritos en [8]. En este caso, la descripción y categorización de los componentes se realiza con un enfoque distinto, más general y a alto nivel que en el caso anterior:

- *Dispositivos físicos*
  Serían las llamadas "cosas" del ecosistema. Para estos autores, las cosas son siempre dispositivos físicos, y no pueden ser virtuales, afirmándose que la identidad como objeto físico es algo en común entre todas las "cosas" en distintos campos de aplicación. Estos dispositivos pueden tener cierto nivel de poder de computación, además de poder estar conectados a otros dispositivos, plataformas y/o ecosistemas IoT.

- *Edge o "borde"*
  El concepto de "borde" hace referencia al dominio operacional del ecosistema. Es decir, es donde los componentes operacionales se conectan, comunican e interactúan. El "borde" típicamente consiste de sensores, controladores, actuators, componentes de comunicación, gateways y los dispositivos físicos en sí mismos.
  El componente de comunicación puede consistir de una red o redes de área local independiente donde los componentes se conectan usando uno o más protocolos y cero o más routers, para conectarse a un gateway borde, hub o bus, que a su vez se conecta a redes más grandes o soluciones en la nube.

- *Plataforma*
  La plataforma IoT es un sistema integrado físico y virtual que utiliza varias aplicaciones y componentes para proveer servicios IoT totalmente interoperables y la habilidad de controlarlos. Una plataforma típica usualmente contiene

o interactúa con los siguientes dominios:

- *Control*
  Consta de las funciones ejecutadas por los mecanismos de control de los dispositivos. En el ambiente industrial, los sistemas de control usualmente están físicamente cerca de los dispositivos. En cambio, en otras áreas, los sistemas de control también pueden estar conectados remotamente.
- *Operaciones*
  Optimiza las operaciones necesarias para los mecanismos de control. Incluye pronósticos, optimización, monitoreo y diagnóstico, suministro e implementación, y gestión.
- *Información*
  Es responsable de recolectar, transformar, persistir y modelar los datos para hacer posible la toma inteligente de decisiones, la ejecución de operaciones y mejoras al sistema.
- *Aplicación*
  Consiste en el programa principal, conjunto con su interfaz de usuario y su lógica y reglas. Es el responsable de implementar la lógica que hará posibles las funcionalidades del sistema IoT.
- *Dominio de negocio*
  Típicamente separado de las funciones principales del sistema, se trata de la integración de las funcionalidad IoT con otras aplicaciones como CRMs, pagos, facturación, y otros.

1.4. Requerimientos y desafíos

Al adentrarnos en la complejidad del paradigma IoT, nos encontramos ante una gran variedad de requerimientos, que a su vez pueden considerarse desafíos en sí mismos dada la realidad de constantes cambios en la cual opera IoT.

A continuación, se presentan los principales requerimientos o desafíos en los que IoT deberá continuar avanzando:

- *Interconectividad*
  Como ya se ha mencionado antes, uno de los aspectos básicos de IoT es la necesidad de conectividad entre todos sus elementos.
  Las arquitecturas actuales de comunicación en IoT son muy variadas, utili-

zando distintas combinaciones de opciones en cuanto a redes, dispositivos y servicios. Actualmente, gran parte de las comunicaciones se realizan a través de VPNs o redes públicas dedicadas. Las plataformas IoT permiten la comunicación entre grandes grupos empresariales, habilitando niveles de recolección de datos y colaboración que antes no eran posibles con infraestructuras tradicionales. [8]

Un aspecto importante adicional, es la necesidad de que la conectividad permita la mutua identificación entre los objetos que interactúan. La conexión entre las cosas deberá ser establecida en base a la identidad de las mismas. Existen variadas formas de definir y establecer dicha identidad. Las plataformas IoT deberán ser capaces de manejar de forma adecuada dicha variedad en la identificación, formalizando los procesos. [5]

En cuanto a las redes de comunicación, para que permitan la mayor automatización posible, es necesario que dispongan de técnicas y mecanismos de autogestión, autoconfiguración, autorecuperación, auto optimización y autoprotección. De esta manera, las redes deberán ser capaces de adaptarse a diferentes dominios de aplicación, a diferentes ambientes de comunicación y a grandes cantidades y varios tipos de dispositivos. [5]. Nuevos protocolos, con nuevos algoritmos, se encontrarán en constante evolución para hacer esto posible, siendo diseñados con las necesidades específicas de IoT en mente. [9]

- *Heterogeneidad*

  En IoT, nos referimos con heterogeneidad a la diversidad de dispositivos y su performance, redes, protocolos, plataformas, políticas, dominios de aplicación, entre otros, por la cual está compuesta. [10]

  La heterogeneidad está en la naturaleza de IoT, uno de sus desafíos será desarrollar procesos compartidos que permitan abstraerla, logrando el máximo provecho de las funcionalidades de los dispositivos. La búsqueda de formas cada vez más efectivas para manejar la complejidad de IoT será constante. [9]

  Uno de los mayores problemas de la heterogeneidad es la ausencia de servicios de seguridad común, esto debilita la interoperabilidad y consume más recursos y performance en la comunicación entre dispositivos. Además, desarrollar políticas de seguridad y actualizaciones en este contexto es muy complejo. Es por esto que la definición de estándares para los distintos aspectos de IoT es de vital importancia, unificando de forma clara la heterogeneidad del sistema. Las personas y procesos involucrados en el sistema luego deberán cumplir de forma estricta los mismos. [10]

- *Interoperabilidad*

  El concepto de interoperabilidad puede ser definido como la habilidad para hacer cooperar distintos sistemas y dispositivos de una manera eficiente. [9]
  La interoperabilidad necesita ser asegurada entre los sistemas, los cuales son altamente heterogéneos y distribuidos, para hacer posibles el suministro y consumo de una gran variedad de información y servicios. [5]
  Las soluciones IoT actuales se caracterizan por distintos niveles de integración e interoperación. Muchas veces integrar implica hacer que sistemas logren operar entre sí cuando no fueron diseñados originalmente para ello. Sin embargo, aún no siendo algo holísticamente disponible, entre las compañías puede existir cierto grado de integración e interoperación entre sus productos, donde tecnologías de distintos niveles son integradas. [8]
  En muchos casos, la integración está basada en modelos de uso común, donde los protocolo IP y HTTP son usados conjunto con REST APIs. La interoperabilidad semántica entre industrias es una característica de IoT que se encuentra en auge y que recibe cada vez más atención. Dicha integración permitirá el uso compartido de datos entre industrias y proveerá lo necesario para el desarrollo de nuevos modelos de negocio. [8]

- *Escalabilidad*

  La escalabilidad es uno de los desafíos más importantes que tiene IoT, y se trata de encontrar las maneras más eficientes de lidiar con el crecimiento sostenido en el número de dispositivos. En otras palabras, "la escalabilidad es la habilidad de un sistema o red de manejar la escala de crecimiento de cualquier ambiente sin efectos en la performance". El crecimiento ininterrumpido de la cantidad de dispositivos tiene un gran impacto en la performance de la red. [9]
  En el contexto de un sistema de este tipo, escalabilidad refiere al número de sensores y "actuators" conectados al sistema, a las redes que los conectan, a la cantidad de datos asociados al sistema y su velocidad de movimiento, y también a la cantidad de poder de procesamiento requerido. El número de sensores puede ser muy grande y el número de transacciones asociadas puede ser aún mayor. Esto es adicionalmente multiplicado en casos como el de autos conectados a servicios de datos de tráfico y clima. IoT deberá ser capaz de proveer mensajería y procesamiento de datos que sea escalable y que se logre adaptar a un creciente número de interacciones y generación de mensajes y datos. [11]
  El número de dispositivos que necesitan ser controlados y que se comunican entre ellos será al menos un orden de magnitud más grande que el de los dispo-

sitivos conectados actualmente a internet. La proporción de las comunicaciones desencadenadas por dispositivos en comparación a las desencadenadas por los humanos aumentará significativamente, yendo hacia un modelo de comunicación donde el dispositivo es el nuevo y predominante iniciador. [5]

- *Procesamiento de datos*
  El procesamiento inteligente de los datos obtenidos es una funcionalidad clave de un sistema IoT. La habilidad de distribuir sensores ampliamente y recopilar datos de manera rápida y efectiva facilita nuevas formas de colaboración. [8]
  Actualmente, los sistemas IoT también usan modelos semánticos de los datos que produce para poder utilizarlos de forma más práctica e intuitiva, y para facilitar la interoperación de los componentes del sistema. La generación de modelos y abstracciones semánticas que logren abarcar y describir la información característica de distintas entidades permiten generar entendimientos y niveles de información que van más allá de los datos recabados en sí mismos. El nivel adecuado de abstracción es útil a la hora de manejar situaciones en tiempo real, dado que todas las fuentes de información son capaces de concordar en la semántica de la información que están proporcionando. [8]
  Una gran cantidad de sistemas IoT avanzados dependen del análisis de grandes cantidades de datos. Tienen la necesidad, por ejemplo, de extraer patrones analizando datos históricos que puedan ser usados para conducir decisiones sobre acciones futuras. La extracción de información útil a partir de datos complejos, como por ejemplo videos, es un ejemplo más de un análisis que requiere grandes cantidades de procesamiento. La habilidad de explotar datos existentes para obtener nuevos conocimientos y la necesidad de combinar diferentes conjuntos de datos de formas novedosas son características esperables de ser parte de un sistema IoT. Es así que comúnmente los sistemas IoT son buenos ejemplos del llamado Big Data. [11]
  Big Data es una nueva expresión que describe a la información masiva, ya sea estructurada o no, que es difícil de manejar con bases de datos y técnicas de software tradicionales. Básicamente, se define Big Data como un volumen grande de datos. Un conjunto de datos es considerado como Big Data si cumple las 4 Vs (valor, volumen, velocidad y variedad). [9]
  Es así que los recursos utilizados en el sistema IoT necesitan ser optimizados para Big Data. Grandes cantidades de datos deberán ser capaces de ser enviados, accedidos, transformados y procesados de forma rápida y eficiente. Las herramientas analíticas y enfoques tradicionales pueden no ser capaces de escalar y cumplir con los requerimientos de rendimiento. Por cuánto tiempo

mantener almacenados los datos también se vuelve un aspecto importante a tener en cuenta. [11]

Por otro lado, otro aspecto importante a mencionar es que la locación física donde los datos son almacenados puede encontrarse regulada por distintas leyes, las cuales varían de país en país. Este es particularmente el caso de la información de identificación personal (PII), los datos sobre el estado de salud y los registros financieros. Es de esta manera que cualquier sistema IoT tendrá que tener en cuenta las reglas sobre soberanía de datos, y almacenar y procesar los mismos solamente en las locaciones permitidas por las regulaciones. [11]

- *Calidad del servicio (QoS)*

  La calidad del servicio, como un requerimiento no funcional, es la "capacidad de proveer un servicio satisfactorio" por los distintos proveedores y sistemas. Debido a la naturaleza heterogénea de IoT, la calidad del servicio del sistema IoT en general referirá a la capacidad de los proveedores de proveer dichos servicios. [12]

  Es necesario brindar confianza sobre las operaciones de los sistemas IoT debido a las regulaciones de las distintas industrias y sectores, y también debido a las normas y expectativas de las distintas partes interesadas. [11]

  En muchos de estos escenarios heterogéneos, los sistemas IoT necesitarán garantizar niveles requeridos de confianza y latencia de forma de poder proveer servicios de alta calidad a los usuarios finales. La calidad del servicio (QoS) como requerimiento deberá ser satisfecha de forma explícita a diferentes niveles. A nivel de redes, estándares técnicos específicos de comunicación serán necesarios para asegurar la entrega de paquetes de manera confiable y dentro de los tiempos demandados y esperados. Por otro lado, a nivel de la aplicación, soporte explícito de protocolos de aplicación y diseño de nuevos e innovadores algoritmos de asignación de recursos serán obligatorios para poder manejar accesos concurrentes e implementar una gestión adecuada de los recursos. [13]

  La aplicabilidad de distintos parámetros de calidad dependen del dominio específico de aplicación en combinación con las tecnologías usadas y proveedores. La satisfacción sobre la calidad del servicio de un sistema IoT se define a través de varios parámetros de calidad. Dichos parámetros son vistos desde distintas perspectivas y dimensiones; la perspectiva del usuario y la aplicación, los aspectos específicos de la red y su operador, los nodos borde y los recursos del sistema de comunicación, y las perspectivas desde las distintas tecnologías. [13]

Los parámetros de calidad desde la perspectiva del usuario requerirán la combinación de todos los esquemas para poder proveer la calidad de servicio requerida, acordada y aceptada por los usuarios. Un sistema IoT efectivo que provee servicios satisfactorios desde el punto de vista del usuario puede no ser lo suficientemente eficiente desde la dimensión de los operadores y los recursos del sistema, y vice versa. [13]

- *Seguridad*

  Las amenazas y riesgos relacionados a los dispositivos, sistemas y servicios IoT son variados, y evolucionan rápidamente. Con un gran impacto en la seguridad y privacidad, el mundo de las amenazas en IoT es extremadamente amplio. Es así que es importante entender qué necesita ser asegurado y desarrollar medidas de seguridad específicas para proteger a IoT de ataques. [2]

  Las interrogantes sobre la seguridad y confiabilidad de un sistema IoT distribuido y heterogéneo son problemas difíciles donde sus soluciones deben poder escalar y evolucionar conjunto con los sistemas. [11]

  La protección de datos será necesaria, donde se buscará dar respuesta a un significante número de preocupaciones en cuanto a la privacidad de los datos, sobre todo los pertenecientes a los individuos. Lograr la certeza de que estos sistemas son seguros (tanto desde el punto de vista informático como físico), resilientes y que cumplen las expectativas de todas las partes interesadas es un objetivo exigente. Cuanto más datos sobre personas, transacciones financieras y otras operaciones sean recolectados, refinados y almacenados, los desafíos relativos a la soberanía de la información y la seguridad aumentan. [11]

  En la siguiente sección se profundizará en este punto, introduciendo más en detalle la problemática de seguridad en el contexto de sistemas IoT.

Capítulo 2

Seguridad en IoT

Cada vez depositamos más confianza en dispositivos inteligentes e interconectados para cada aspecto de nuestra vida. Los dispositivos se transforman así en el blanco de numerosos ataques que tienen el potencial de poner en peligro la privacidad de las personas y amenazar la seguridad pública. Es así que la seguridad informática (security) es una de las mayores preocupaciones en relación a IoT, que necesita ser abordada conjunto con la necesidad de seguridad física (safety), dado que ambas están intrínsecamente relacionadas con el mundo físico. [2]

Cuando hablamos de seguridad nos referimos a la condición de un sistema de estar protegido contra el acceso no intencionado o no autorizado, modificaciones y daños. El comportamiento seguro de un sistema no es total. Ningún sistema IoT puede comportarse de forma segura en todos los contextos. Es por eso que se deberán establecer explícitamente cuales son los comportamiento seguros esperados por las partes interesadas en los contextos más relevantes. [14]

La certeza sobre la seguridad de un sistema es frecuentemente evaluada en términos de riesgos. Los elementos de un riesgo de seguridad incluyen una amenaza (alguien o algo que tiene la intención de hacer daño), el recurso objetivo (que tiene valor), una potencial vulnerabilidad o debilidad del recurso que la amenaza explota, y contramedidas que intentan reducir la probabilidad e impacto de cualquier incidente de seguridad. [14]

Las propiedades que necesitan ser garantizadas para proveer la seguridad de la información y los recursos del sistema son confidencialidad, integridad y disponibilidad, también referidos con el acrónimo CIA (confidentiality, integrity and availability). [14]

La propiedad de confidencialidad refiere a que la información no sea accesible ni revelada a individuos, entidades o procesos no autorizados. Violaciones en la confidencialidad pueden ocurrir por el boca a boca, impresiones, copias, emails, o a través de vulnerabilidades en el software que le permiten a los atacantes leer o filtrar datos. Se le denomina filtración de datos a la transferencia no autorizada de datos leídos gracias a exploits en lugares donde un atacante tiene el control. Estos datos pueden ser usados para chantajes u otros propósitos. El control de acceso y el cifrado son algunos de las herramientas en favor de la confidencialidad. [14]

Por otro lado, la propiedad de integridad se asegura de que ninguna modificación o destrucción de información se lleve a cabo. Entre las herramientas utilizadas, se encuentran los hashes, checksums, anti-virus y firmas, todos tienen el objetivo de que no se realicen cambios en el sistemas, en el código y en otros elementos que controlan los procesos físicos del sistema. La integridad de datos, subpropiedad de la integridad, asegura que ninguna parte no autorizada modifique datos ni tome el control del sistema sin que sea detectado. [14]

Por último, la disponibilidad es la propiedad que refiere a brindar acceso a la información de forma oportuna, confiable y a demanda, a los usuarios autorizados. Los sistemas responsables de controlar los procesos físicos deben ser capaces de ser controlados y vigilados por operadores humanos. Un operador puede necesitar intervenir en caso de un ataque, por ejemplo para dar de baja el sistema. Por lo general, los controles de disponibilidad implican procesos redundantes y controles sobre los cambios. A veces, incluyen actividades de seguridad que intentan buscar y mitigar vulnerabilidades en el software, las cuales reducen la confiabilidad de los procesos y pueden implicar un uso inadecuado de los recursos con consecuencias negativas sobre el sistema. [14]

Es importante observar que las contramedidas tradicionales de seguridad no pueden ser directamente aplicadas a las tecnologías IoT debido a los diferentes estándares y capas de comunicación involucradas. Además, el gran número de dispositivos interconectados despierta problemas de escalabilidad y hace necesaria una infraestructura flexible capaz de encargarse de las amenazas de seguridad en un ambiente muy dinámico. [15]

Las propiedades de seguridad de los sistemas son usualmente descritas en función de modelos de seguridad. Estos modelos describen típicamente las entidades reguladas por una política de seguridad específica y las reglas que constituyen esa política. Crear y mantener un modelo de seguridad holístico capaz de lidiar con los cambios dinámicos de los sistemas IoT es cada vez más difícil. La continua incorporación

de dispositivos que involucran diferentes fabricantes, diferentes sensores y diferentes enfoques de seguridad sobre el acceso físico, está incrementando la complejidad de forma exponencial. Soluciones para varios problemas de seguridad deben aún ganar consenso en la comunidad. [8]

Los sistemas IoT actuales fueron usualmente construidos con un enfoque industrial antiguo, conectando sensores, dispositivos y componentes existentes de infraestructura además de servicios. El paradigma IoT está introduciendo nuevos niveles de exposición para cada uno de esos elementos. Las plataformas IoT actuales contienen soluciones tecnológicas pertenecientes a una gran variedad de proveedores, cada uno de los cuales se enfoca en proveer componentes heterogéneos con niveles individuales de seguridad. Las medidas de seguridad dentro de los componentes IoT, si es que existen, no fueron diseñadas para tener en cuenta las dependencias que surgen de las capacidades de conectividad, manejo de datos y recolección de información. [8]

Por ejemplo, los dispositivos industriales usualmente carecen de mecanismos de autenticación adecuados, al haber sido diseñados para ser usados en ambientes físicamente protegidos y aislados. Como parte del IoT de hoy, estos dispositivos son interconectados con muchos otros, especialmente sistemas back-end, que padecen de todos los ya bien conocidos defectos de seguridad inherentes al business IT. Si un atacante gana acceso a una plataforma business IT, explotando una vulnerabilidad de seguridad del navegador por ejemplo, es muy probable que también logre acceso a dispositivos industriales débilmente protegidos. Esto puede resultar en daños severos e incluso en incidentes de seguridad física. Por lo tanto, la introducción de un número masivo de endpoints en el área de consumo y en el área industrial crea un campo fértil para la explotación de enlaces con protección débil. Mejorar la seguridad de dichos endpoints y de la comunicación entre los dispositivos y asegurar la credibilidad del dispositivo y la información, para lo que hasta ahora había sido un conjunto de sistemas homogéneos y completamente cerrados, presenta nuevos desafíos. Es así que métodos de análisis profundo sobre los riesgos y amenazas como también herramientas de gestión de las plataformas IoT serán requeridas. [8]

2.1. Requerimientos de seguridad

Como ya se ha mencionado anteriormente, IoT se caracteriza por estar conformado por tecnologías heterogéneas que proveen servicios innovadores en distintos dominios de aplicación. En este escenario, la satisfacción de requerimientos de se-

guridad y privacidad juega un rol fundamental. Es de esperar que este alto nivel de heterogeneidad, en conjunto con la gran escala de los sistemas IoT, magnifique las amenazas de seguridad del internet actual. [15]

Es así que el paradigma IoT presenta nuevos desafíos que hacen necesario que se definan requerimientos de seguridad distintos a los ya conocidos en el contexto IT. En [8] los autores analizan los distintos requerimientos de IoT, y presentan los siguientes requerimientos en el contexto de la seguridad de los sistemas. Pocos sistemas IoT actuales cumplen estos requerimientos de seguridad, pero es importante definirlos y promoverlos debido a la criticalidad de los desafíos de IoT hacia el futuro. Los requerimientos presentados son:

- Desarrollar políticas de seguridad end-to-end y capacidad de gestión de riesgos, que integren todos los componentes y las políticas de sus subsistemas en un solo sistema IoT
- La plataforma del sistema IoT deberá proveer capacidad de monitoreo de los dispositivos y de detección de anomalías. Para esto serán importantes las capacidades adicionales de coordinación y análisis de los datos para determinar eventos. La capacidad del sistema de ser resiliente y tolerante a fallas es otro aspecto importante a ser requerido.
- Además de gestionar la política del sistema IoT, la plataforma deberá proveer capacidad de gestión de los identificadores del sistema, siendo capaz de correlacionarlos entre subsistemas, gestionarlos de forma federada, garantizar su seguridad y gestionar su autenticidad, en especial la responsabilidad y no repudio sobre los datos.
- Seguridad adaptativa, receptiva y cooperativa son capacidades adicionales importantes que deberán ser soportadas a nivel de la plataforma del sistema. Los sistemas necesitan ser capaces de adaptarse, aprendiendo e incorporando nueva información sobre amenazas y creando y ejecutando planes de acción para combatir las mismas.
- Los sistemas necesitan ser capaces de responder rápida y apropiadamente a amenazas y ataques, mitigando el mayor daño posible.
- Los sistemas necesitan ser capaces de diagnosticar problemas cooperativamente e implementar planes de mitigación y prevención de problemas de seguridad entre los distintos subsistemas del sistema, los cuales pueden ser propiedad de diferentes entidades.

- A nivel del borde del sistema, se necesitará la capacidad de autenticar y autorizar los distintos productos y dispositivos, y determinar su identidad, a su vez que la capacidad de controlar el acceso desde y hacia dichos dispositivos en base a su identidad.
- Los dispositivos necesitan ser capaces de adaptarse al framework de seguridad utilizado con respecto a los recursos físicos y la robustez de la seguridad.
- Los dispositivos necesitarán capacidades cada vez mayores de resiliencia y tolerancia a fallas.
- En el futuro los dispositivos IoT deberán tener la capacidad adicional de facilitar y ejecutar detección de anomalías en el borde del sistema, posiblemente mitigando ataques y detectando fallas donde y cuando ocurran en lugar de solo contribuir con información para ser procesada de forma remota.
- En general, la gestión de la política de seguridad es un problema que se encuentra en el nivel de la plataforma, pero los dispositivos más capaces necesitarán capacidad de gestionar esas políticas por su cuenta, tanto para encargarse de políticas locales que pueden ser necesitadas in situ como de aquellas que necesitan ser gestionadas por la plataforma como parte de estrategias de políticas de seguridad más comprensivas.
- Los dispositivos necesitarán cada vez mayores capacidades de gestión de su identificación para facilitar la autenticación con otros dispositivos, y deberán ser diseñados con la capacidad de proteger su identidad. Si los dispositivos en sí mismos no pueden proveer estas funcionalidades, servicios en el borde del sistema necesitan funcionar como intermediarios en la comunicación de los dispositivos con el sistema IoT.
- El borde del sistema deberá proveer una identificación apropiada de los productos y dispositivos, poder confirmar la confianza de los datos obtenidos por ellos y gestionar la correlación de identificadores entre los sistemas.

Los autores de [8] además presentan en detalle los siguientes requerimientos de seguridad, con énfasis en el IoT del futuro:

- *Identificadores seguros y gestión de los mismos*
  Los sistemas IoT futuros consistirán de una incontable cantidad de actores y componentes, embebidos en sistemas heterogéneos que deberán confiar entre ellos a diferentes niveles. Datos correctos, completos y oportunos son el corazón de todo sistema IoT. Distintas tecnologías son requeridas para asegurar la inte-

gridad de los datos y su autenticidad así como su entrega y procesamiento sin interferencias ni manipulaciones. Esto mayormente requiere tecnologías escalables y eficientes por encima de las infraestructuras de clave pública actuales (PKIs) para identificar dispositivos y objetos inteligentes. Nuevas tecnologías son necesarias para asignar identidades únicas a las cosas, éstas deberán ser escalables y no deberán permitir la clonación ni suplantación de identidad. Además, nuevos sistemas de gestión de identidad federados son requeridos para recopilar, integrar y procesar datos heterogéneos en diferentes sistemas.

- *Preservar la privacidad en contextos multifacéticos y dinámicos*
  Los sistemas IoT son más que la suma de sus partes, por lo que los problemas en la privacidad se vuelven aún más complejos. Las consideraciones sobre la privacidad que pueden hacerse a bajo nivel pueden diferir de las preocupaciones generadas a nivel de la aplicación o del análisis de datos, y las violaciones de privacidad en cualquier nivel afectan al sistema entero.
  Una vez que la comunicación es introducida entre componentes, incluso a un bajo nivel, la superficie potencial de violaciones de la privacidad aumenta. Debido a que los dispositivos usualmente tienen capacidades computacionales y de almacenamiento extremadamente limitadas (si es que las tienen), métodos innovadores para agregar seguridad a los contenidos de los stream de datos, tales como cifrado embebido y ligero, son requeridos. Los dispositivos a veces utilizan esquemas de comunicación hop-to-hop que no son capaces de soportar cifrado end-to-end. Esto necesita entonces del desarrollo e inclusión de nuevos esquemas de intercambio de claves y protocolos de ruteo.
  El acceso remoto a los datos de un dispositivo ejemplifica un caso en el cual la privacidad está en riesgo, pero incluso los servicios con acceso intencional a esos datos presentan desafíos para la privacidad de los usuarios. Los servicios que acceden a los datos de manera esperada, ya sea una empresa de servicios públicos, el fabricante del dispositivo o un proveedor de aplicación, generan superficies de ataque adicionales para violar la confidencialidad de los datos de los usuarios, implicando que éstos son tan privados como sea la seguridad de las entidades que tienen acceso a ellos. Con el advenimiento de que los datos son almacenados, transmitidos y procesados a través de infraestructuras compartidas, las plataformas IoT del futuro requerirán servicios y tecnologías innovadoras para imponer controles de acceso adecuados y proteger los datos almacenados en caso de incidentes.
  Adicionalmente, nuevas tecnologías, tales como controles sobre el uso de los datos, serán requeridas para proveer a los usuarios con la habilidad de con-

trolar qué sucede con sus datos una vez que se encuentran en manos de otros. Ésta no es solamente una propiedad deseable para la satisfacción del cliente, sino también un desafío legal para las compañías y un derecho para los usuarios finales en muchas jurisdicciones. Implementaciones de sistemas IoT futuros estarán obligadas a buscar maneras para tanto controlar localmente la exposición de los datos como para interrelacionarse con una variedad de otros sistemas mientras se continúa garantizando la privacidad end-to-end.

- *Establecimiento de confianza*
  Las infraestructuras técnicas actuales para el establecimiento de confianza entre partes tienen como objetivo la asociación entre una clave criptográfica y el dueño de esa clave en la forma de un usuario humano u organización. Mientras que los enfoques descentralizados tales como Web of Trust (WoT) existen, prácticamente la gran mayoría de las infraestructuras usadas, como las PKIs basadas en autoridades de certificación, son organizadas alrededor de un conjunto de entidades comúnmente aceptadas como confiables, que pueden establecer relaciones de confianza transitiva a través de la certificación cruzada. Tales infraestructuras tienen problemas bien conocidos, que no están limitados a IoT. Por ejemplo, el pasado reciente ha mostrado que la confianza puesta en dichas entidades no es justificada en todos los casos, dado que certificados criptográficos han sido expedidos para usuarios no autorizados. Además, el registro, emisión y revocación de certificados, y especialmente la certificación cruzada, son procesos pesados que requieren de un significante trabajo manual y que tiene que ser llevado a cabo primero antes de que la comunicación entre dispositivos pueda tomar lugar. Esto hace a las infraestructuras centrales de establecimiento de confianza inaccesibles para la mayorías de los escenarios en IoT, donde la confianza debe ser establecida a demanda con pares que no fueron previamente registrados y que son desconocidos, sin la interacción de un usuario. Es así que algoritmos nuevos y más ligeros de establecimiento de confianza son requeridos.

- *Análisis de amenazas y gestión de riesgos*
  Cuando se consideran los requerimientos de seguridad y las funcionalidades, el balance entre el rendimiento y la seguridad sigue siendo crucial en la actualidad, incluso con tecnologías más avanzadas de mayor rendimiento soportando implementaciones de seguridad. Dependiendo de las propiedades respectivas de aplicación IoT, existe la necesidad de soportar arquitecturas que provean funcionalidades de seguridad correspondientes a requerimientos de seguridad

variantes. Especialmente, los tres requerimientos clave son adaptabilidad, capacidad de respuesta y cooperatividad.

Los sistemas IoT futuros necesitan incorporar adaptabilidad que es la capacidad de agregar contramedidas preventivas al sistema cada vez que una nueva amenaza es identificada. Para esto se utiliza una técnica llamada PDCA (plan, do, check, act) que es ampliamente conocida. PDCA es una manera de lidiar con el descubrimiento de nuevas amenazas a través de un proceso continuo que involucra la identificación de la nueva amenaza, el análisis sobre cómo enfrentarla, la planificación sobre cómo implementar contramedidas, y luego la ejecución de la implementación en sí y su evaluación.

Sin embargo, la prevención en seguridad muchas veces no es suficiente. Los sistemas IoT también necesitan ser capaces de responder apropiadamente y mitigar el daño. La creciente importancia que se les da a las medidas de respuesta a incidentes hacen ver que la capacidad de respuesta es también esencial para minimizar lo más posible el daño generado por un ataque, y para acelerar su recuperación. Esto puede ser logrado usando el proceso OODA (observe, orient, decide, act), donde primero se monitorea y evalúa la situación, luego se decide qué hacer y por último se actúa basado en la decisión en tiempo real.

La cooperatividad es otro requerimiento clave. Mientras que la creciente interdependencia de los sistemas IoT provee servicios cada vez más avanzados, existe la preocupación de que el daño causado por un ataque en un subsistema en particular tenga un impacto en los otros subsistemas interdependientes, resultando en un daño mayor y extensivo a lo largo de todo el sistema IoT. Lo que se necesita entonces para enfrentar esto es aplicar el concepto de cooperatividad teniendo diferentes subsistemas realizando evaluaciones de seguridad sobre los demás.

Es así que asegurar las plataformas IoT requiere del desarrollo de modelos dinámicos de seguridad y ataques que consideren tanto las diferentes capas de los sistemas por separado como en conjunto, como también todo el ciclo de vida de los sistemas. Deberán tener en cuenta el impacto que deja en el sistema las infracciones de seguridad en alguna de sus partes.

Incluso con la introducción de funcionalidades y capacidades avanzadas de seguridad, siempre permanecerá el riesgo, aunque sea mínimo, de que ocurran eventos con consecuencias fatales. El trade-off entre el nivel de seguridad y el costo depende altamente de las condiciones particulares del caso de uso. Naturalmente, necesitan haber métodos y modelos apropiados que permitan evaluar los riesgos y decidir sobre el trade-off entre seguridad y costo durante el

diseño e implementación de de los componentes del sistema IoT. La creciente complejidad de los sistemas IoT, los dispositivos y la plataforma del sistema requiere más información y soporte para un análisis y gestión de riesgos más avanzada, especialmente cuando se trata de ataques ciber físicos.
La evaluación de riesgos y sus métodos de gestión abarcando el ciclo de vida completo de sistemas complejos requiere nuevas tecnologías para recolectar y procesar datos referentes a la seguridad y para realizar análisis dinámico y online de amenazas basado en dichos datos. Los algoritmos de análisis requeridos deben producir advertencias con alta precisión y mínima cantidad de falsos positivos. Además, deben ser resilientes contra ataques de adversarios. Nuevos sistemas cooperativos de gestión de riesgos y protocolos de seguridad son requeridos para habilitar advertencias tempranas y capacidad de reacción.

- *Gestión de seguridad continua*
  Componentes vulnerables del sistema IoT pueden violar requerimientos de seguridad de cualquiera de las partes involucradas, como por ejemplo el proveedor de la plataforma o el consumidor del servicio IoT. Con el fin de mitigar esos riesgos, las auditorías de seguridad de los componentes de IoT comprueban si éstos satisfacen un conjunto de requerimientos de seguridad.
  Tradicionalmente, las auditorías de seguridad son tareas discretas produciendo resultados que se presumen válidos por determinado período de tiempo. Con respecto a IoT, ésta suposición de estabilidad no puede sostenerse, los atributos de los componentes IoT cambian con el paso del tiempo, con estos cambios siendo a veces difíciles de detectar y predecir. Además, solo considerar los niveles de seguridad de los componentes IoT por separado no es suficiente para reconocer que los servicios IoT son el resultado de tecnologías heterogéneas múltiples interactuando entre ellas.
  Conducir auditorías de seguridad en IoT requiere entonces de un acercamiento diferente capaz de detectar continuamente cambios en los servicios IoT, y evaluando su impacto en el nivel de seguridad en tiempo real. Además, tales métodos construyen los cimientos de las medidas de mitigación y prevención de seguridad que serán cada vez más necesarias para proteger los servicios IoT contra los atacantes.

2.2. Amenazas y riesgos

El número de amenazas de seguridad que afectan a los dispositivos IoT ha aumentado en los últimos años. La figura 2.1 ilustra algunos de los incidentes de seguridad, en el contexto de IoT, más importantes que han sido descubiertos y/o que tomaron lugar desde 2009, demostrando el gran crecimiento que tuvieron. Deberá tenerse en cuenta que esta lista no es exhaustiva, incluye solo los ejemplos más importantes. Dada la penetración aún mayor de IoT a lo largo del amplio espectro de actividades diarias e infraestructuras críticas, la ocurrencia de incidentes de ciberseguridad está destinada a crecer. [2]

Se ha llegado a un punto donde se han vuelto comunes las noticias y artículos sobre estos ataques. Estos ataques, en su gran mayoría, son relacionados a dispositivos que han sido violados o a sistemas que han sido comprometidos, incrementando al mismo tiempo el número de peligros a enfrentar. [2]

Es así que el análisis de riesgos es vital en el contexto de IoT. El riesgo, efecto de la incertidumbre, toma en cuenta la probabilidad de que un evento ocurra conjunto con el impacto que tendría si así lo hiciera. Entre los elementos que implican riesgos de seguridad se incluyen las amenazas y actores que pueden intentar explotar vulnerabilidades en el sistema a menos que contramedidas hayan sido desplegadas para mitigar el riesgo. Las amenazas pueden ser involuntarias o intencionales. El impacto de que un evento ocurra está comprendido por varios elementos de riesgo, incluyendo el valor del recurso involucrado, el daño a la reputación, potenciales responsabilidades, y consecuencias en la seguridad física debido al mal funcionamiento de procesos físicos. [14]

El "riesgo de negocio" es definido por el ICC como "el efecto de la incertidumbre sobre los objetivos", y el "riesgo de la seguridad de la información" como "el potencial de que una amenaza dada explote vulnerabilidades de un recurso o grupo de recursos y así genere daño a al sistema". En el contexto de la seguridad de la información se utiliza el término "amenaza" en vez del término más general "incertidumbre". [14]

La evaluación de riesgos es el proceso por el cual cada riesgo, y en especial riesgos de seguridad de la información, son caracterizados. Distintos enfoques para la evaluación de éstos son documentados en varios estándares. En particular, la evaluación de riesgos en el IoT industrial tiene características únicas al incluir posibles consecuencias físicas de errores y ataques. [14]

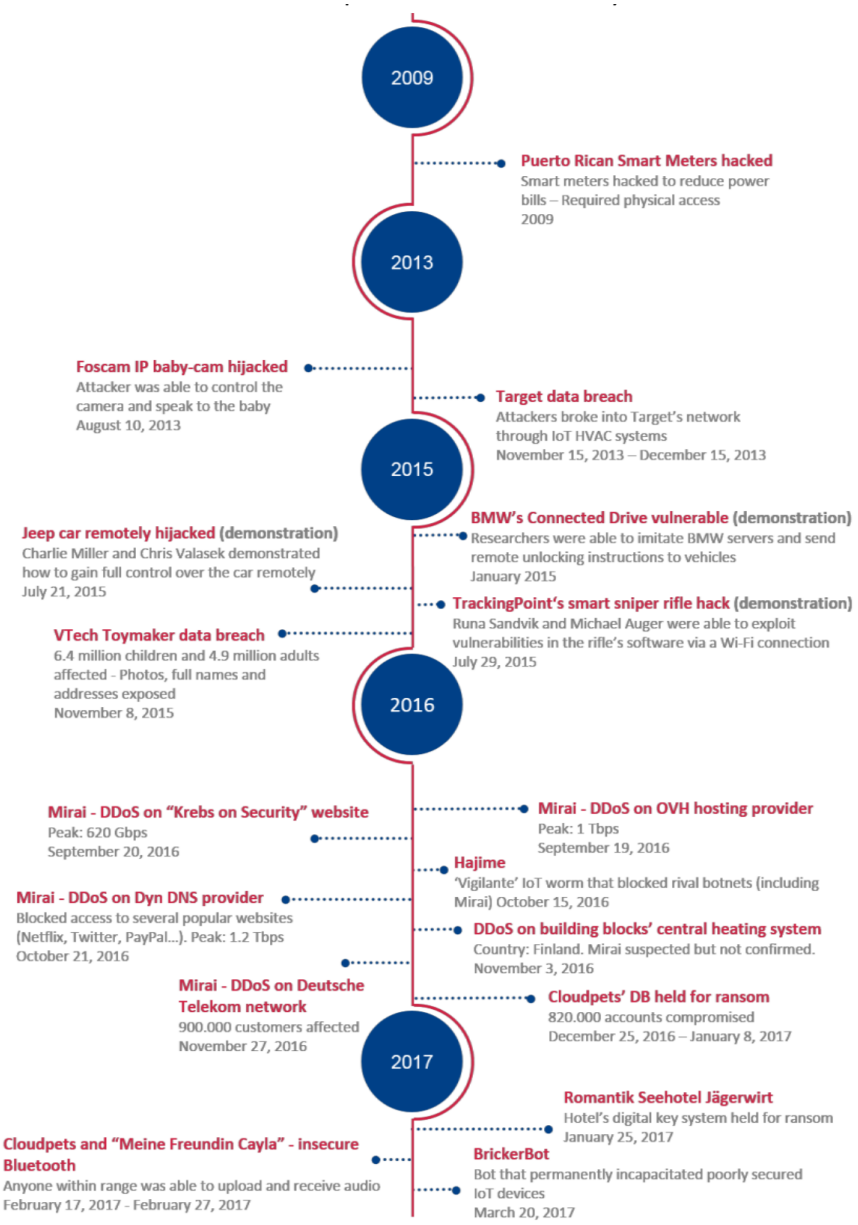

Figura 2.1: Línea de tiempo indicativa de incidentes de seguridad [2]

Las amenazas más comúnmente discutidas provienen de atacantes maliciosos que desean interrumpir o alterar el sistema, robar información o causar daño, pero incluso sistemas adecuadamente asegurados deben responder por fallas en el ambiente operativo, tales como condiciones ambientales o climáticas extremas. El término "amenaza", entonces, debería de interpretarse de una manera amplia que incluya cualquier consecuencia o incidente que pueda interferir con el uso normal y esperado del sistema subyacente. [14]

Mientras que no es práctico anticipar cada amenaza posible, un modelo de seguridad fuerte que contemple grandes cambios en el ambiente operativo puede mitigar el impacto de varias situaciones no planeadas. [14]

Identificar amenazas y consecuencias requiere de un entendimiento del sistema en general y su implementación. A los elementos de IoT que se encuentren expuestos a posibles ataques se les denomina superficie de ataque. Tanto el crecimiento en el número de tecnologías como el aumento de la complejidad aumentan la superficie de ataque y las vulnerabilidades del sistema, incrementando los riesgos. [14]

Cada uno de esos elementos pueden ser vulnerables a través de un vector de ataque, un mecanismo por el cual un ataque puede tener lugar. Los vectores de ataque incluyen ataques físicos, ataques de red, ataques contra el software, ataques a los operadores y ataques en las cadenas de suministro de los elementos que comprometen el sistema. Cada industria tiene un conjunto específico de vectores de ataque, así como cada tecnología. El impacto de cada tipo de ataque depende del sistema, el diseño y las prioridades de negocio. [14]

La existencia de algunos componentes físicos puede incrementar la superficie de ataque por ser más susceptibles de alteraciones. Por ejemplo, el equipamiento expuesto al público tiene una superficie de ataque mayor que el equipamiento que se encuentra detrás de perímetros de seguridad en sitios industriales dedicados. Además, los sistemas digitales diseñados para prevenir daño en el equipamiento o heridas a los trabajadores tendrán una atención garantizada mayor en el proceso de evaluación de riesgos, especialmente cuando riesgos de seguridad no son mitigados con protecciones físicas adicionales. [14]

Como no es viable eliminar todos los riesgos de un sistema, debemos gestionarlos para que la energía y recursos ya invertidos en un sistema estén balanceadas contra el efecto de resultados no deseados. Este balanceo debe estar basado en una evaluación realista de las amenazas, los riesgos que generan y cómo pueden prevenir al sistema de cumplir sus funciones esperadas. [14]

Una de las posibilidades es proceder sin seguridad, y aceptar todos los riesgos. Es también posible gastar excesivos recursos en seguridad al punto de que ya no justifiquen las ganancias. Para gestionar los riesgos, las organizaciones deberán evaluar y decidir en qué partes de un programa de seguridad se invertirá, luego periódicamente reevaluar tanto los riesgos como la eficacia de las medidas tomadas. [14]

Los riesgos de seguridad pueden ser abordados en diferentes maneras [14]:

- *Eliminación*
  Se busca eliminar totalmente los riesgos para evitar cualquier exposición. Por lo general, la no presencia de riesgos sólo puede ser lograda quitando totalmente del sistema la funcionalidad que lo causa.

- *Mitigación*
  Se implementan medidas compensatorias para reducir el impacto de una amenaza inevitable. La mitigación de riesgos es la estrategia más aplicable cuando no se pueden eliminar los riesgos completamente. Se implementa con un enfoque sistemático de las seguridad del software, auditorías y gestión de actualizaciones y correcciones.

- *Transferencia*
  Se busca transferir el riesgo a un tercero. Más comúnmente esto se da en la forma de seguros, cuando un riesgo es aceptado por un tercero a cambio de un pago. Transferir los riesgos es una técnica común para incidentes de alto impacto y poco frecuentes que tienen costos de mitigación excesivamente altos. La transferencia de riesgos también puede ser lograda al traspasar los costos a los clientes, o al tercerizar servicios.

- *Aceptación*
  No se busca reducir el riesgo, simplemente se lo acepta. Esta estrategia es usualmente aplicada cuando el costo de mitigar la amenaza excede el costo de que dicho incidente adverso ocurra.

El riesgo residual es el riesgo que permanece luego de que todas las contramedidas han sido implementadas. Cuando todas las vulnerabilidades conocidas fueron removidas, quedan las que aún no se conocen. Pueden permanecer riesgos debido a suposiciones incorrectas sobre la seguridad del sistema o la confianza sobre las personas que acceden a este. El riesgo residual debe ser rastreado para priorizar operaciones de seguridad adicionales, justificar las decisiones de seguridad tomadas y determinar cuándo se ha llegado a un balance entre costos versus eficacia de los controles de seguridad. Disponer de métricas vigentes ayuda a controlar los defec-

tos de forma continua así como a crear y aplicar acciones correctivas de manera oportuna y eficiente. [14]

Los ataques modernos abarcan un amplio rango de medios y motivos posibles. Entre los enfoques para enumerar ciber amenazas y métodos de ataque se incluyen la lista de vectores de ataque como las de OWASP, o el enfoque de identificación de amenazas STRIDE, ambos se presentan a continuación [14]. También se presentan las amenazas en IoT en base a la taxonomía de ENISA.

2.2.1. Vectores de ataque IoT de OWASP

Una colección no exhaustiva de potenciales vectores de ataques para sistemas IoT fue compilada de varias fuentes por el proyecto IoT de OWASP, que también compila vectores de ataque para las aplicaciones web. Cada organización, dependiendo de su tolerancia a riesgos, necesita evaluar la siguiente lista para entender cuáles vectores aplican a su caso. Las contramedidas y técnicas de mitigación que abordan estos ataques necesitan ser confirmados por evaluaciones formales. [14]

La lista Top 10 de OWASP en el contexto IoT incluye:

1. Interfaz web insegura
2. Autenticación y autorización insuficiente
3. Servicios de red inseguros
4. Falta de cifrado de transporte
5. Problemas de privacidad
6. Interfaz en la nube insegura
7. Interfaz móvil insegura
8. Configurabilidad de seguridad insuficiente
9. Software o firmware inseguro
10. Seguridad física débil

Esta lista es un buen punto de partida para generar preguntas y análisis, y para entender los tipos de ataques relevantes.

2.2.2. Modelo de amenazas STRIDE

Un adversario es una entidad maliciosa que tiene como objetivo prevenir que un recurso se comporte de la forma esperada para comprometer la integridad, dispo-

nibilidad o confidencialidad del sistema o sus datos. Los adversarios explotan las vulnerabilidades en los recursos. Estas amenazas son entonces clasificadas basadas en las severidad, y así las potenciales contramedidas pueden ser evaluadas. [14]

STRIDE, desarrollado por Microsoft, modela los riesgos y evalúa las amenazas de los ambientes IT. El modelo STRIDE ha sido también extendido para incorporar amenazas en el contexto IoT. El modelo STRIDE comprende varias categorías de amenazas [14]:

- *Spoofing identity*
  Este es el tipo de amenazas donde una persona o dispositivo utiliza las credenciales de otra persona como su nombre de usuario y contraseña, con el objetivo de ganar acceso a datos y acciones a las que no está realmente autorizado.
- *Tampering*
  Se trata de alterar datos relacionados al dispositivo o los que se encuentran atravesando la red.
- *Repudiation*
  Se trata de la capacidad de negar que una persona o dispositivo estuvo involucrado en una transacción específica o evento. Esto difiere de la capacidad de rastrear qué persona o dispositivo fue responsable por un evento.
- *Information disclosure*
  Es la exposición de información a individuos que se suponen no deberían tener acceso a ésta.
- *Denial of service*
  Refiere a la capacidad de hacer que un servicio particular deje de estar disponible, usualmente a través del consumo de recursos o a través de ejecuciones no confiables.
- *Elevation of privilege*
  Se trata de la capacidad de que un usuario sin privilegios gane suficiente acceso para comprometer o destruir un sistema entero. En las amenazas de elevación de privilegio, un atacante puede penetrar todas las defensas de un sistema y transformarse en alguien confiable para éste, una situación peligrosa en sí misma.

  Es fácil ver que combinando los últimos seis elementos descritos se llega al acrónimo STRIDE.

2.2.3. Taxonomía de amenazas de ENISA

Siendo consistentes con la taxonomía de amenazas propuesta por ENISA en [16], la figura 2.2 muestra la taxonomía aplicada a IoT con algunos ejemplos de ataques listados. [2]

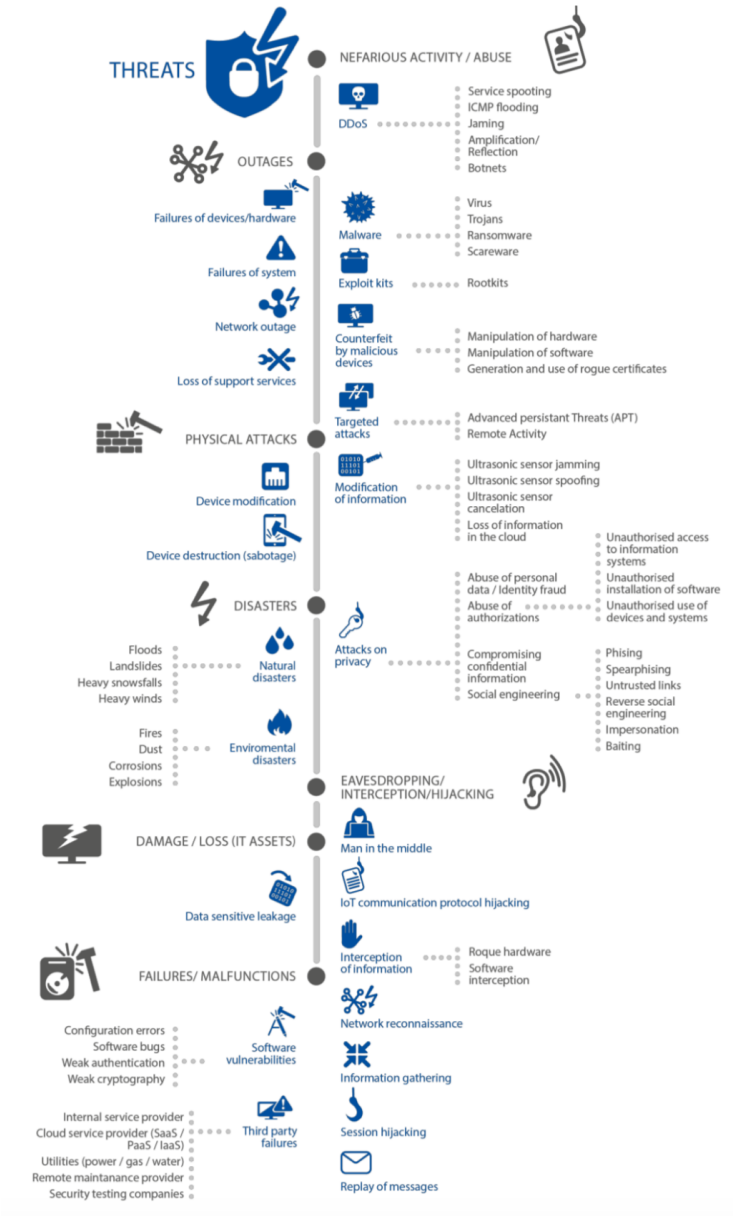

Figura 2.2: Taxonomía de amenazas en IoT [2]

A continuación, también se listan y describen las distintas amenazas presentadas en dicha taxonomía en términos de IoT, clasificadas en distintas categorías en función del tipo de actividad que las origina [2]:

- Actividad maligna / Abusos

- *Malware*
  Son programas de software diseñados para llevar a cabo acciones no deseadas o autorizadas en un sistema, sin el consentimiento del usuario, resultando en daño, corrupción o robo de información. Su impacto puede ser alto, y puede afectar tanto a los dispositivos como a la plataforma IoT.
- *Kits de exploits*
  Es código diseñado para tomar ventaja de una vulnerabilidad con el fin de ganar acceso al sistema. Esta amenaza es difícil de detectar y en los ambientes IoT su impacto oscila entre alto y crítico, dependiendo de los recursos afectados. Tanto la infraestructura como los dispositivos IoT pueden ser blanco de esta amenaza.
- *Ataques dirigidos*
  Son ataques diseñados para un objetivo específico, ejecutados durante un período largo de tiempo, y llevados a cabo en múltiples etapas. El principal objetivo es mantenerse oculto y obtener la mayor cantidad de datos e información sensible o control que sea posible. Mientras que el impacto de esta amenaza es mediano, detectar este tipo de ataques es usualmente muy difícil y lleva tiempo.
- *DDoS*
  Se trata de un ataque donde múltiples sistemas atacan un objetivo único con el fin de saturarlo y hacer que no quede disponible. Esto puede ser realizado creando muchas conexiones, saturando los canales de comunicación o reenviando las mismas comunicaciones una y otra vez. Se pueden realizar este tipo de ataques sobre los dispositivos IoT, la infraestructura o la plataforma del sistema.
- *Suplantación de identidad*
  Esta amenaza puede ser difícil de descubrir, dado que los dispositivos falsos no pueden ser fácilmente distinguidos de los originales. Estos dispositivos usualmente tienen backdoors y pueden ser usados para conducir ataques en otros sistemas ICT en el ambiente.
- *Ataques a la privacidad*
  Esta amenaza afecta tanto la privacidad de los usuarios como la exposición de los elementos de la red a personas no autorizadas. Los dispositivos IoT, la información del sistema en sí misma, y la plataforma pueden ser afectados.
- *Modificación a la información*

En este caso, el objetivo no es dañar el dispositivo, pero sí manipular la información con el fin de causar caos, o adquirir ganancias monetarias.

- Eavesdropping / Interceptación / Hijacking
  - *Man in the middle*
    Es un ataque de eavesdropping, donde se intercepta una comunicación y se lee el contenido. El atacante recibe los mensajes de una de las víctimas y se lo reenvía a la otra, con el fin de hacerles creer que están hablando directamente entre ellas sin nadie de por medio. Todas las comunicaciones dentro de un sistema IoT pueden ser afectadas por esta amenaza.
  - *Hijacking del protocolo de comunicación IoT*
    En este ataque se toma control sobre una sesión de comunicación ya existente entre dos elementos de la red. El intruso es capaz de acceder a información sensible, incluyendo contraseñas. El hijacking puede llegar a usar técnicas agresivas como forzar la desconexión o la denegación de servicio.
  - *Interceptar información*
    Se trata de interceptar de forma no autorizada una comunicación privada, tales como una llamada telefónica, sms, emails, entre otros.
  - *Reconocimiento de la red*
    Se obtiene pasivamente información interna sobre la red: dispositivos conectados, protocolos usados, puertos abiertos, servicios en uso, etc.
  - *Hijacking de sesiones*
    Se roban los datos de conexiones actuando como un host legítimo, con el fin de robar, modificar o borrar los datos transmitidos.
  - *Replay de mensajes*
    Este ataque usa una transmisión de datos válida de forma maligna al enviarla repetidamente o demorarla, con el objetivo de manipular o dar de baja el dispositivo objetivo.
- Outages
  - *Outage de la red*
    Se trata de la interrupción o falla en el suministro de la red, ya sea intencional o accidental. Dependiendo del segmento de la red afectado, y en el tiempo requerido para recuperarlo, la importancia de esta amenaza varía entre alta a crítica.
  - *Fallas en los dispositivos*

Es la amenaza de que los dispositivos hardware fallen o se comporten de forma incorrecta.

- *Falla del sistema*
  Es la amenaza de que los servicios de software o las aplicaciones con las que se tiene contacto fallen.
- *Pérdida de servicios de soporte*
  Se trata de la pérdida de servicios de soporte que son requeridos para que los sistemas de información operen de la forma esperada.

- Daños / Pérdidas
  - *Fuga de información sensible (leakage)*
    En esta amenaza datos sensibles son revelados, intencionalmente o no, a partes no autorizadas. La importancia de esta amenaza puede variar ampliamente, dependiendo del tipo de información.

- Fallas / Mal funcionamiento
  - *Vulnerabilidades del software*
    Los sistemas IoT más comunes son generalmente vulnerables debido a contraseñas débiles, bugs en el software y errores de configuración, poniendo en riesgo a la red. Esta amenaza se encuentra usualmente conectada a otras, como los kits de exploits, y es considerada crítica.
  - *Fallas en terceros*
    Se trata de la existencia de errores en elementos activos de la red causados por la mala configuración de otro elemento de la red que tiene relación directa con ellos.

- Desastres
  - *Desastres naturales*
    Estos incluyen eventos tales como inundaciones, vientos fuertes, nieve intensa, derrumbes, entre otros desastres naturales que pueden dañar físicamente a los dispositivos.
  - *Desastres en el ambiente del sistema*
    Es la amenaza de que ocurran problemas en el ambiente donde se encuentra desplegado el equipamiento IoT y que pueden causar su inoperabilidad.

- Ataques físicos
  - *Modificación en el dispositivo*
    Es la manipulación o alteración de un dispositivo al, por ejemplo, tomar

ventaja de puertos mal configurados y explotarlos.

- *Destrucción del dispositivo*
  Se trata de incidentes tales como el robo, bombas, vandalismo o sabotaje que pueden dañar a los dispositivos.

2.3. Situación actual y desafíos

Es importante analizar la situación actual en la que se encuentra el paradigma IoT con respecto a sus aspectos de seguridad, es decir, se necesita evaluar si los requerimientos se están satisfaciendo, si las amenazas y riesgos están siendo adecuadamente prevenidas y mitigadas, y si las contramedidas y acciones definidas son eficaces y suficientes.

Los autores de [2] realizan este análisis en base a lo que definen como "brechas" o "gaps" de seguridad. Los autores consideran la identificación y definición de estas brechas como parte crítica al abordar la ciberseguridad en IoT, y las definen como la diferencia entre el estado presente y el estado deseado. A partir de dicha identificación, se determinarán los pasos necesarios que necesitan ser tomados con el fin de cerrar dichas brechas y movernos al estado deseado. A continuación, se presentan las brechas identificadas por los autores:

- *Fragmentación en los enfoques y regulaciones de seguridad existentes*
  Actualmente no existe un enfoque común de ciberseguridad en IoT ni a nivel mundial, ni a niveles regionales. En el contexto del estudio presentado en [2], los autores realizaron entrevistas a expertos en seguridad y la mayoría de ellos consideraron tanto la falta de frameworks de seguridad maduros, como la amplitud de los problemas de seguridad a ser considerados, grandes barreras para la mejora de la seguridad. Es común ver que la mayoría de las compañías y fabricantes toman sus propios enfoques cuando implementan seguridad en IoT, resultando en una nula o lenta aceptación de estándares que guíen la adopción de medidas de seguridad y buenas prácticas en IoT.
  Es así que estamos ante una fragmentación en las regulaciones, donde no existen imposiciones claras sobre medidas de seguridad y protocolos en todos los niveles del ecosistema IoT, incluyendo los dispositivos, la red, etc. Por el contrario, la aplicación de estándares únicos a lo largo del ecosistema IoT puede ser vista como un estorbo a la innovación e investigación en el área. Diferentes áreas de aplicación tienen diferentes requerimientos de seguridad, lo que

dificulta aún más la definición de regulaciones comunes.
A la falta de unificación de las reglas a seguir, se le suman la falta de claridad sobre las responsabilidades, tanto morales como legales, de cada actor del ecosistema. Será necesario clarificar dichas responsabilidades, sobre todo ante eventos de seguridad. La heterogeneidad de elementos y actores involucrados hacen de esto un desafío.
Será necesario entender a la ciberseguridad como una responsabilidad compartida entre todos los involucrados. La seguridad no solo le concierne a un solo fabricante, cliente o profesional IT, o solo al sector público o privado. Todos las partes deberán trabajar para lograr progresos en ésta área.

- *Falta de conciencia y conocimiento*
  Si bien como sociedad somos testigos y partícipes de un uso creciente de sistemas y dispositivos cada vez más conectados e interdependientes, los autores concluyen que el conocimiento que tenemos sobre ellos dista de ser el necesario. Esta falta de conocimiento no solo se encuentra en los consumidores, que muchas veces no tienen ni siquiera una comprensión básica de sus dispositivos IoT ni de su impacto. En las entrevistas llevadas a cabo con los expertos, fueron encontradas diferencias en terminologías fundamentales y falta de conocimiento sobre aspectos de seguridad en el contexto de IoT.
  La experticia en tecnología no necesariamente equivale con experticia en seguridad. En general, existe la necesidad de educar apropiadamente a una nueva generación de consumidores, desarrolladores, fabricantes, etc, sobre el uso y riesgos de seguridad generados por IoT, y cómo estar preparados. Es necesario también el entrenamiento tanto en seguridad física (safety) como en ciberseguridad para incrementar la conciencia sobre la problemática.
  Muchos incidentes de seguridad podrían ser evitados si los desarrolladores y fabricantes fueran conscientes de los riesgos con los cuales se enfrentan de forma diaria. Esto se está transformando en una necesidad común con el fin de aumentar la conciencia sobre las amenazas y riesgos actuales y para proveer conocimiento sobre cómo prevenir, proteger y actuar en caso de un incidente de seguridad.

- *Diseño y/o desarrollo inseguro*
  El diseño mismo de un sistema IoT puede hacer de este un sistema inseguro por naturaleza, donde debido a cómo fue diseñado e implementado existen desde el principio vulnerabilidades de seguridad, que usualmente son solucionadas con un enfoque reactivo a medida que se presentan.

Los autores presentan una lista de problemas conocidos y significativos en el contexto de diseño y desarrollo en IoT. Dentro de dicha lista, se menciona la falta de haber seguido un enfoque de "security by design". Esto se trata de un enfoque de diseño y desarrollo de sistemas donde la seguridad es un requerimiento en sí mismo, y donde desde el comienzo se toman medidas para que el sistema tenga la menor cantidad de vulnerabilidades posibles. La falta de protección de la comunicación como la falta de mecanismos fuertes de autenticación, autorización y prevención de hardening son también mencionadas.

- *Falta de interoperabilidad a lo largo de los diferentes dispositivos IoT, plataformas y frameworks*
  La mayoría de los dispositivos IoT usan protocolos patentados, diseñados por sus propios fabricantes, a la hora de interconectarse. Mientras que esto no es un problema para los dispositivos del mismo fabricante, sí se vuelve un problema cuando se quiere interconectar dispositivos de diferente fabricante. Nos encontramos ante distintos modelos de seguridad, conceptos y taxonomías incompatibles. Esto requiere el desarrollo y uso de protocolos estandarizados que necesitan ser soportados por todos los fabricantes para asegurar un buen nivel de interoperabilidad con la mínima pérdida en eficiencia y seguridad.
  Una buena práctica con respecto a esto es evitar el uso de protocolos patentados y de código cerrado, dado que su seguridad no puede ser verificada, y muchos incidentes ya han demostrado que la seguridad basada en la confidencialidad de los mecanismos no implica una cobertura de seguridad adecuada. El uso de frameworks comunes puede también ayudar a mejorar la eficiencia y la seguridad de los dispositivos cuando se interconectan varios de distintos fabricantes.

- *Falta de incentivos económicos*
  Los principales fabricantes y comerciantes de IoT usualmente consideran a la funcionalidad y usabilidad como mucho más importante que implementar y diseñar seguridad. Por lo general los intereses económicos no están alineados con gastar en seguridad. El mayor motivo es la percepción general de que no hay un retorno directo de inversión, que puede ser atribuído al costo económico y a la dificultad de evaluar el impacto financiero de debilidades de seguridad hipotéticas.
  En general, los expertos en IoT entrevistados coinciden que los diferentes riesgos, amenazas y peligros son usualmente subestimados y dejados afuera por motivos de presupuesto. Hay una tendencia a abordar los problemas de segu-

ridad luego de que ocurren los incidentes.

- *Falta de manejo adecuado del ciclo de vida de los productos*
  Existe la necesidad por una manejo adecuado del ciclo de vida de los diferentes recursos que componen un ambiente IoT dado, ya que los dispositivos y redes son interconectados y, en la mayoría de los casos, expuestos en internet, donde pueden ser el objetivo de muchas y diversas amenazas.
  IoT comprende tal variedad de productos que, si se los deja sin atención, hace más vulnerable a toda la cadena de suministro tradicional. IoT expande la superficie de ataque y los diferentes dispositivos y productos tendrán que evolucionar de forma segura para poder cumplir consistentemente con su cometido a través de todo su ciclo de vida.
  A través de su ciclo de vida, los dispositivos IoT deben ser capaces de ser reparados y actualizados rápidamente para asegurar su correcto comportamiento y solucionar todas las vulnerabilidades que son descubiertas constantemente. Como fue mencionado anteriormente, en los ambientes de consumo los usuarios IoT no tienen un entendimiento básico de sus dispositivos y su impacto en el ambiente, lo que puede resultar en los dispositivos no siendo actualizados con subsecuentes brechas de seguridad.

2.4. Buenas prácticas, medidas y recomendaciones

La multiplicidad de requerimientos y desafíos de seguridad que se han desarrollado hasta ahora presentan la necesidad de tomar distintas medidas, tanto a alto nivel en términos del desarrollo del conocimiento sobre seguridad en IoT, como a bajo nivel a la hora de atacar las problemáticas de seguridad en los componentes de los sistemas aplicando variadas técnicas específicas.

En esta sección se presentan recomendaciones de alto nivel con el objetivo de continuar mejorando la seguridad de los sistemas y dispositivos IoT, dirigidas a la comunidad de expertos, fabricantes, desarrolladores, y otros, responsables del desarrollo del paradigma IoT. Estas recomendaciones son presentadas por los autores de [2] en respuesta a los desafíos que éstos mismos presentan y que fueron detallados en la sección anterior.

Luego, se presentan medidas y técnicas de bajo nivel como forma de introduc-

ción a la gran cantidad de aspectos a considerar en cuanto a la seguridad de los componentes y del sistema se refiere. Los autores de [14] presentan un framework de seguridad que se compone de los varios bloques funcionales, y del cual se presentan las consideraciones y técnicas de seguridad principales.

2.4.1. Recomendaciones de alto nivel

- *Promover la armonización de las iniciativas y regulaciones de seguridad en IoT*
  Es necesario resolver la fragmentación existente en cuanto a pautas, iniciativas, estándares y otros esquemas sobre la seguridad en IoT. Un enfoque posible es lograr definir, al menos a niveles regionales, una lista de buenas prácticas y pautas para obtener mayor seguridad y privacidad en los sistemas IoT. A partir de ésta, los distintos sectores de aplicación de los sistemas se deberán enfocar en definir las prácticas y pautas de forma específica para satisfacer sus necesidades, basadas así en su contexto particular y en los riesgos inherentes a su sector.

- *Crear conciencia sobre la necesidad de ciberseguridad en IoT*
  Existe una gran falta de conocimiento sobre seguridad entre los desarrolladores, las industrias, así como los usuarios y consumidores finales. Es esencial que todas las partes interesadas tengan un entendimiento completo sobre los riesgos y amenazas, así como conocimiento suficiente sobre maneras para protegerse contra ellos. Se vuelve de vital importancia crear conciencia en esta área.

- *Definir pautas seguras sobre el ciclo de vida del software y hardware*
  Es recomendable que los desarrolladores, fabricantes y proveedores de productos y soluciones IoT integren y adopten un ciclo de vida del desarrollo del software seguro (SSDLC) en ellos e incorporen procesos relevantes en sus operaciones. La seguridad como requerimiento deberá ser implementada como un todo, en la capa de aplicación, y en cada una de las fases del ciclo de vida.

- *Lograr consensos sobre la interoperabilidad a lo largo del ecosistema IoT*
  Un aspecto esencial será avanzar en la interoperabilidad de los dispositivos IoT, plataformas y frameworks, así como de las prácticas de seguridad. El problema de la interoperabilidad es muy pertinente para el ecosistema IoT debido a la gran escala del mismo, a su penetración en el mundo actual, a la compleja cadena de suministro y a las numerosas partes interesadas. Se recomienda el uso de frameworks de interoperabilidad abiertos y hacerlos más transparentes.

- *Promover incentivos económicos y administrativos*
  La seguridad en los sistemas IoT deberá ser promovida a través de distintas regulaciones e incentivos. La "continuidad del negocio" puede servir como uno de los motivadores de los fabricantes para agregar más seguridad, debido a que usualmente su falta impacta directamente en dicha continuidad. En cambio, la falta de percepción por parte de los usuarios sobre el valor de la seguridad hacen que su demanda sea baja. En IoT, las ventajas competitivas entre fabricantes se enfocan en lanzar el producto lo antes posible. Se deberá incentivar que determinados niveles de seguridad se hayan alcanzado antes de que los dispositivos lleguen al mercado.

- *Establecer una gestión segura del ciclo de vida de los productos y servicios*
  Se recomienda que se definan procesos específicos y enfocados en seguridad en cada una de las etapas del ciclo de vida de los productos y servicios. Algo importante es la necesidad de poder realizar actualizaciones de seguridad en los dispositivos luego de que éstos fueron desplegados.

- *Clarificar las responsabilidades de cada parte interesada*
  Debido a la interrelación de IoT, su seguridad informática y la seguridad física de los usuarios y el ambiente, es necesario clarificar las distintas responsabilidades de las partes interesadas. Se recomienda legislar en este sentido, intentando cubrir los huecos legales que se detecten.

2.4.2. Medidas y técnicas

El framework de seguridad presentado por los autores de [14] consta de la definición de distintos bloques funcionales que tienen determinados objetivos en cuanto a la seguridad del sistema se refiere. En cada uno de ellos se presentan consideraciones y técnicas a tener en cuenta, a continuación se presentan las principales.

Protección de endpoints

Se considera como endpoint a cualquier elemento del sistema IoT que tiene capacidad de computación y comunicación y que expone capacidades funcionales. Cubren un amplio espectro de posibilidades, desde dispositivos del borde del sistema, infraestructuras de comunicación, sensores, controladores, hasta servidores masivos en la nube.

En función del rol funcional de los endpoints y sus requerimientos de seguridad, se utilizan distintos mecanismos y técnicas para implementar capacidades defensivas en ellos. Las consideraciones de seguridad sugeridas por el framework son:

- *Arquitectura*

  Cada endpoint tiene distintas capacidades computacionales y de comunicación. A la hora de implementar seguridad en los mismos, dichas capacidades afectan las posibles técnicas y medidas a seguir. Por ejemplo, los dispositivos del borde del sistema usualmente tienen recursos limitados, donde su poder de computación es bajo y las configuraciones suelen ser estáticas. En cambio, la nube probé capacidades ampliamente superiores a los endpoints que se encuentran en ella.

  Las decisiones tomadas por los fabricantes a la hora de implementar los endpoints determinan y tienen un efecto a largo plazo en la capacidad de seguridad de éstos. Es así que la arquitectura como tal incide en la seguridad. Los responsables de integrar los distintos productos que proveen los fabricantes se encontrarán limitados por éstos a la hora de garantizar la seguridad del sistema IoT y sus endpoints.

  La seguridad de los endpoints puede implementarse tanto en el hardware como en el software. La primera opción ofrece la ventaja de disponer de hardware especializado y resistente a alteraciones que genera mayores niveles de confianza, sobre todo en las operaciones y en las claves criptográficas. Sin embargo, esta opción usualmente implica mayores costos, ya sea económicos o en la complejidad de la gestión. El hardware además no es fácilmente mejorable ni modificable luego de fabricado, por lo que sus funcionalidades de seguridad se mantendrán probablemente estáticas y será difícil solucionar vulnerabilidades cuando son detectadas. Los arquitectos deberán tener en cuenta estos requerimientos en conflicto a la hora de determinar el balance entre hardware y software en la solución de seguridad.

  Al considerar grandes despliegues de infraestructura industrial, se observa que los endpoints son desplegados y utilizados por largos períodos de tiempo. Sus niveles de seguridad deberán ser mejorados en este contexto. Se deberá considerar prioritario no afectar los procesos de negocio existentes al agregar controles de seguridad, estos deberán ser acoplados a los procesos industriales intentando minimizar las interdependencias que se encuentran entre ellos.

- *Seguridad física*

  Los ambientes donde se despliegan los endpoints conforman un amplio rango de

posibilidades, que implican diferentes requerimientos de seguridad a la hora de proteger los recursos contra robo, alteraciones, vandalismo o condiciones climáticas.

En los sistemas industriales, las técnicas de control de acceso físico son comúnmente utilizadas para prevenir el contacto físico entre los endpoints y dispositivos con usuarios no autorizados. De todas formas, algunos endpoints, como es el caso de los medidores inteligentes o el de sensores, no pueden encontrarse dentro de un perímetro de seguridad. Se vuelven necesarias distintas protecciones físicas aplicadas directamente que puedan proporcionar evidencia de alteraciones y que dejen expuestas las modificaciones realizadas, disuadiendo la realización de las mismas y protegiendo al sistema de condiciones climáticas adversas y otros riesgos que puedan generar fallas inesperadas.

- *Identidad*

  La determinación y asignación de una identidad es crucial a la hora generar y establecer confianza. Una gran cantidad de controles de seguridad dependen directamente de la identidad del endpoint y de los otros recursos y entidades con los cuales se comunica, y de la confianza que éstos establecen a través de dicha identidad. Tanto la autenticación como la autorización son ejemplos claros.

  En este contexto, se define a una "entidad" como un elemento con una existencia notoriamente distinta. Un dispositivo es un ejemplo de entidad. A su vez, dicho dispositivo puede estar comprendido por múltiples endpoints, cada uno de los cuales es una entidad, y cada endpoint comprende varios componentes, los que son también una entidad. En este sentido, la "identidad" es una propiedad inherente a una entidad que la distingue del resto de las entidades. Y una "credencial" es una evidencia que soporta una declaración de identidad.

  Aplicando estos conceptos a la hora de garantizar la seguridad de los endpoints se puede afirmar que éstos podrán tener una identidad única, o múltiple, usada para diferentes aplicaciones. Las credenciales son utilizadas para verificar la identidad del endpoint. Existen varios niveles de confianza que pueden aplicar a uno, dependiendo del modelo de amenazas particular del sistema IoT. Cada nivel de confianza determina las capacidades mínimas de seguridad de la credencial, incluyendo su unicidad, almacenamiento y uso.

- *Control de acceso*

  El control de acceso se trata de verificar si una entidad, que solicita acceso a un recurso, se encuentra autorizada a hacerlo. En el caso de los endpoints, el

control de acceso depende de dos conceptos relacionados:

- Autenticación: consta del aseguramiento de que una supuesta característica de una entidad es correcta
- Autorización: es la concesión de derechos

La autorización depende de la verificación del mapeo entre la identidad de la entidad y los derechos y privilegios sobre los servicios y recursos, por lo que la autorización depende sobre la autenticación.

El proceso de establecimiento de confianza a través de la autenticación del endpoint, o el aseguramiento de la identidad de un endpoint remoto, tiene varios pasos donde se comprueba la correctitud, validez, fortaleza e identidad del poseedor de la credencial. No todos los intentos de autenticación resultan en el mismo nivel de confianza en la identidad del endpoint remoto. Existen distintos niveles de aseguramiento de la identidad de las entidades basados en qué tipo de credencial es aplicado a esa autenticación, cómo es almacenada la credencial, y qué técnica de autenticación fue implementada.

En referencia a las comunicaciones en sí mismas, todas deberán estar no solo autenticadas, sino también autorizadas. Cada intento de conexión en un ambiente IoT deberá ser evaluado para determinar si se ajusta a la política de comunicación del endpoint.

Autorizar un intento de conexión implica asegurarse de que el puerto, protocolo, aplicación, librería y el proceso son permitidos por la política definida. La autorización puede ser impuesta tanto en el endpoint como en la red. En el endpoint la disponibilidad de información es mucho mayor, permite determinar la naturaleza de la comunicación y tomar decisiones más informadas.

- *Integridad*

  Es necesario que la información referente a la identidad del endpoint sea apropiadamente asegurada y su integridad mantenida. A su vez, tanto los datos almacenados como aquellos que se encuentran en movimiento y uso, deberán ser monitoreados y mantenidos de forma que la confianza en ellos no se vea aceptada.

  Antes de establecer confianza en cualquier otro software o programa ejecutable, será necesario establecer confianza en los componentes donde se da el proceso de arranque de los sistemas, en el cual se inicia el hardware principal y el sistema operativo. Será crucial que el ambiente "boot" sea verificado y se determine que se encuentra en un estado no comprometido.

  Luego de haber realizado este primer paso de aseguramiento, el sistema operativo puede iniciar y las aplicaciones pueden ejecutarse. Es aquí donde surge

la necesidad de también garantizar la integridad pero en tiempo de ejecución. Se deberán implementar controles que monitoreen, e idealmente impongan, la integridad del endpoint luego de este haberse iniciado. Si bien existe diversidad de técnicas y opciones y no es definitivo cuál es la mejor, sí es importante implementar tantos controles en tiempo de ejecución como sean posibles dentro de las limitaciones del dispositivo.

- *Protección de datos*

  Los datos que son almacenados, utilizados y transferidos por el endpoint deberán ser protegidos utilizando distintas estrategias. La criptografía impone y fortalece la confidencialidad de los datos y además asegura su integridad. Puede ser usada en todos los datos, sólo en las porciones sensibles o en todo el medio de almacenado. En la práctica, múltiples técnicas de protección de datos pueden ser aplicados simultáneamente, proveyendo protección a diferentes tipos de ataque.

  A la hora de proteger los datos, debemos enfocarnos en dos aspectos, la confidencialidad y la integridad de los mismos.

  Por un lado, la confidencialidad refiere a asegurar que la información no sea revelada a partes no autorizadas. Para lograrlo, la criptografía permite renderizar datos de forma ininteligible para entidades no autorizadas que no tienen la clave apropiada para descifrar los datos. A la hora de diseñar e implementar los algoritmos será necesario asegurarse que ninguna parte no autorizada pueda determinar las claves asociadas con el cifrado ni derivar texto plano. Los algoritmos criptográficos deberán ser implementados utilizando prácticas de programación segura, y cuando sea posible, con librerías que estén actualizadas y mantenidas regularmente. Crear algoritmos criptográficos sin una evaluación pública deberá ser evitado. Además, las claves deben ser aleatorias, no predecibles, y del largo suficiente que impida ataques de fuerza bruta o búsquedas exhaustivas en el espacio de claves disponibles.

  Por el otro, la integridad de los datos busca asegurar que cualquier alteración sea detectada. Algunas técnicas comunes de integridad de datos, como los checksums, incrementan la confiabilidad y resiliencia del sistema pero no son efectivas si se quieren prevenir modificaciones maliciosas debido a su falta de fuerza criptográfica. Las firmas digitales como técnica nueva proveen una mayor confianza en las medidas de integridad.

- *Monitoreo y análisis*

  Los mecanismos de monitoreo son de alta importancia y se encargan de la

detección, por lo general en tiempo real, de anomalías en el sistema que podrían implicar ataques o que el sistema se encuentre comprometido. Será necesario entonces también proteger a los mecanismos de monitoreo en sí mismos. La posibilidad de que estos se encuentren comprometidos afecta a todo el sistema al reportar los eventos de forma incorrecta.

- *Configuración y gestión*
  Una buena gestión del endpoint y su configuración es indispensable. El endpoint deberá proveer un control sobre los cambios que se realizan en su componentes, garantizando que éstos son seguros y no lo comprometerán. Todos los cambios y actualizaciones deberán ser firmados, sus payloads cifrados y las acciones registradas en logs para que los endpoints puedan ser subsecuentemente auditados y recuperados.

- *Dispositivos con recursos limitados*
  Algo característico de los sistemas IoT es que, en general, los dispositivos que forman parte del sistema tienen recursos y capacidades limitadas que restringen y dificultan el apropiado cumplimiento de los requerimientos de seguridad (autenticación, protección en tiempo real, gestión de la configuración, entre otros).
  Estos dispositivos deberán ser capaces de ejecutar cripto operaciones. Los dispositivos más nuevos son capaces de ejecutarlas utilizando nuevas técnicas de hardware, como los aceleradores, los coprocesadores y los aceleradores embebidos. Todas estas técnicas incrementan la performance de los dispositivos y la vida de la batería. Actualmente es posible construir endpoints que combinen aceleradores embebidos con nuevos algoritmos y que así sean capaces de brindar el mejor balance entre la capacidad de actualización, la performance y la seguridad.
  En cuanto a la autenticación, desafortunadamente muchos protocolos industriales aún no la soportan de forma adecuada, pero estos protocolos inseguros pueden ser usados a través de TLS y otros protocolos de más bajo nivel para proveer las propiedades de seguridad necesarias.
  Entre otros recursos y capacidades que se pueden encontrar limitados se encuentran las limitaciones inalámbricas, el consumo de batería, la disponibilidad intermitente de la comunicación y la "ventana" de mantenimiento (entiéndase como el período en el cual se tiene acceso para realizar mantenimiento del dispositivo).

Protección de comunicación y conectividad

Este bloque funcional busca proteger el tráfico de datos. Se utilizan las capacidades de autorización de los endpoints para implementar autenticación y autorización en el tráfico. La comunicación y conectividad es protegida por técnicas criptográficas, que garantizan tanto la integridad como la confidencialidad, y por técnicas de control del flujo de información. El nivel de protección necesario depende de las amenazas a las cuales está expuesto el intercambio de los datos. Las consideraciones de seguridad sugeridas por el framework con respecto a esto son:

- *Protección criptográfica*
  Se recomienda que las aplicaciones, en particular las de IoT, utilicen protocolos que ya hayan sido evaluados y verificados, incluyendo su seguridad y su uso de criptografía.
  A la hora del diseño de la seguridad, es importante definir en cuál capa agregar la protección necesaria, y cómo personalizar esa protección para una aplicación dada. Agregar controles de seguridad en todas las capas puede generar problemas en las performance, pero hacerlo solo en una capa puede no ser suficiente.
  Las siguientes son medidas que deberían emplearse:
  - Políticas explícitas de comunicación entre los endpoints
  - Autenticación mutua entre endpoints criptográficamente fuerte
  - Mecanismos de autorización que impongan reglas de control de acceso derivadas de la política definida
  - Mecanismos criptográficos que aseguren la confidencialidad, integridad y novedad de la información intercambiada
- *Flujos de información*
  Se le denomina flujo de información a cualquier información "en movimiento", incluyendo mensajes IP, comunicaciones seriales, flujos de datos, señales de control, y otros. Se pueden prevenir ataques hacia ellos desarrollando medidas específicas.
  Una de las medidas a considerar es separar el flujo de información en varios canales, donde cada uno deberá ser aislado del resto y gestionado y monitoreado de forma independiente. En la misma línea, se recomienda la segmentación de la red, donde cada segmento conecte recursos con políticas de seguridad y requerimientos de comunicación similares.
  La utilización de firewalls también es común y recomendada. Estos se encargan

del filtrado de paquetes a nivel del mensaje que transportan. Pueden ser desplegados tanto como un dispositivo físico como virtual. La función de filtrado de un firewall examina cada mensaje para comprobar que cumpla con la política de tráfico definida. Existen firewalls capaces de aprender automáticamente y crear reglas a partir de la observación del tráfico.

- *Modelos y políticas de seguridad*
  Un modelo de seguridad es aquel que define las relaciones permitidas y prohibidas entre distintos sujetos y objetos del sistema, capturando así, tanto de forma formal como informal, las políticas de seguridad del sistema.
  Las políticas de seguridad en cuanto a la comunicación y conectividad se refiere, deben surgir a partir de un análisis completo de los riesgos. Las políticas especifican cómo filtrar y rutear tráfico, cómo proteger los datos intercambiados y qué reglas de control de acceso deben ser usadas. Estas políticas deberán ser evaluadas constantemente, para garantizar su correctitud y completitud.

Monitoreo y análisis de seguridad

Es necesario que el estado del sistema sea preservado a lo largo del ciclo de vida operacional Este bloque funcional entonces tiene como responsabilidad la recolección de datos sobre el estado general del sistema que permitan la detección de posibles violaciones a la seguridad o amenazas. La política de seguridad del sistema deberá indicar luego las acciones a tomar en cada caso, para las cuales existe un gran rango de posibilidades.

El monitoreo de la seguridad permite, a través del agregado y almacenamiento de los datos, el análisis de eventos pasados y actuales relacionados a la seguridad y la predicción de riesgos futuros. El sistema de monitoreo y análisis deberá también ser asegurado, previniendo fugas de información e inyección de datos falsos.

Los datos a ser monitoreados podrán ser obtenidos tanto de los endpoints como de la red, y deberán ser almacenados de forma segura. Diferentes tipos de análisis serán realizados en búsqueda de indicios de vulnerabilidades y ataques. Este análisis permite ser proactivo en la implementación de controles de seguridad para reducir los riesgos, permite reaccionar a ataques en progreso, y permite entender ataques previos y aprender de ellos para intentar predecir vulnerabilidades que puedan ser explotadas en un futuro.

Las consideraciones de seguridad sugeridas por el framework con respecto al

sistema de monitoreo son:

- *Prevención, detección, análisis y respuesta*
  El monitoreo y análisis de seguridad del sistema generará más valor si es capaz de producir conclusiones que impliquen acciones a incorporar en planes de respuesta automática a incidentes.
  Es deseable que antes de que ocurra un ataque, el sistema sea capaz de detectar indicios de que éste puede ocurrir. Por ejemplo, un atacante puede dejar rastros al realizar actividades de reconocimiento.
  Durante un incidente, es necesario que se registren datos confiables sobre todos los cambios que están ocurriendo en el sistema. Distintas acciones pueden tomarse en el momento, como por ejemplo, elevar los niveles de seguridad de otros sistemas accesibles desde el sistema atacado.
  Por último, luego del incidente, el sistema debe volver a operar normalmente tan pronto como sea seguro y posible. Será deseable que se realice un proceso de análisis y aprendizaje sobre lo sucedido que permita hacer más robusto y efectivo al plan de respuesta a incidentes.

- *Captura y almacenamiento de datos*
  Es importante que los sistemas de monitoreo sean diseñados considerando el riesgo de que un intruso borre toda evidencia de sus actividades. Una forma de mitigar dicho riesgo es a través de la transmisión de los datos a sistemas de monitoreo externos de manera segura y oportuna.
  El sistema deberá ser capaz de monitorear y controlar los endpoints y comunicaciones de forma genérica y consistente.

- *Protección de los datos de seguridad*
  Existen políticas de seguridad y regulaciones para la recolección, comunicación y almacenamiento de datos sensibles usados en el sistema de monitoreo y análisis. Entre ellos se encuentran regulaciones que prohíben ciertos tipos de monitoreos sobre los empleados o requieren que se notifique o se pida autorización al mismo para poder hacerlo. Otras regulaciones prohíben la transmisión de datos personalmente identificables a través de límites geográficos, o el almacenamiento o análisis de esos datos en algunas regiones.

Gestión de la configuración de seguridad

Este bloque funcional colabora con el anterior en la preservación del sistema. Es responsable de controlar los cambios tanto en las funcionalidades operacionales como

en los controles y mecanismos de seguridad que garantizan la protección del sistema en sí misma. Se busca que todo cambio sea realizado de forma segura, controlada y confiable, brindando estabilidad al sistema.

Tanto los cambios en el sistema como el descubrimiento de nuevas vulnerabilidades y amenazas requerirán cambios en las políticas, el firmware y el software. Es así que las funcionalidades de seguridad de los sistemas IoT deberán ser configurables y gestionables, y no estar definidas estáticamente. Además, cada una de las distintas versiones desplegadas deberá ser cuidadosamente controlada, configurada y gestionada.

La gestión de la seguridad se trata de tener la capacidad de ajustar las capacidades de seguridad para que el sistema pueda adaptarse a los cambios. Es necesario contar con una interfaz de usuario que permita la definición, actualización y el monitoreo del estado de la seguridad del sistema.

En cuanto a los endpoints, se deberá contar con capacidad de gestionar y controlar la seguridad de la comunicación dentro de las redes del sistema. Políticas de seguridad deberán ser aplicadas sobre la misma, ya sea en los endpoints o en dispositivos intermedios. Entre los controles de mitigación usados para proteger la comunicación se encuentran los firewalls, el filtrado de paquetes, routers, sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), controles de acceso a la red, entre otros.

Capítulo 3

Smart Grids

Si bien las redes eléctricas actuales cumplen su cometido principal, es decir, el suministro eléctrico seguro, de calidad y sostenible, éstas deben modernizarse para lograr mejoras de eficiencia energética y calidad del suministro, y reducción de emisiones de CO2. Para convertir una red eléctrica en inteligente la solución no consiste en implementar completamente una nueva red, sino en hacer evolucionar la existente. En este sentido se debe tener en cuenta que la red de distribución está constituida por una gran cantidad de activos con una larga vida útil, que se deben monitorizar y automatizar. [17]

Es por esto que en los últimos años las redes eléctricas han ido evolucionando hacia lo que se conocer hoy en día como Smart Grids o redes eléctricas inteligentes. Para responder la pregunta de qué se define como Smart Grid se encuentran disponibles diversas definiciones en la bibliografía estudiada.

3.1. Definiciones

El grupo de organismos reguladores europeos de la electricidad y el gas define Smart Grid como [18]:

"Una red eléctrica que puede integrar el comportamiento y las acciones de todos los usuarios conectados en una forma eficiente en cuanto a costos, incluyendo productores, consumidores y actores que son tanto productores como consumidores, para asegurar una red eléctrica que haga un uso más eficiente de los recursos con un costo inferior, asegurando menores pérdidas y mayor calidad y seguridad de la demanda.".

Basada en una red de comunicación y control de los actores involucrados, la producción de energía eléctrica debe ser coordinada y demandada en una forma más efectiva. En términos generales, una Smart Grid provee una infraestructura de control y comunicación que permite la interacción entre los participantes de la red eléctrica, en particular a los conectados al nivel de distribución. [19]

Las redes inteligentes o smart grids no consisten en la implementación de un paquete definido de tecnologías en la red sino que en realidad se trata de la implantación de una combinación de equipos, tecnologías e infraestructuras de control y comunicaciones para habilitar las mejoras mencionadas con objeto de ofrecer servicios adicionales a todos los agentes de la red.[17]

Para el National Institute of Standards and Technology (NIST) [20]:

"Una smart grid es una red moderna con flujo bidireccional de energía que provee, mediante comunicaciones bidireccionales y capacidades de control, una serie de funcionalidades y aplicaciones a la red".

Esta definición sugiere modernizar las redes de modo que éstas integren sistemas de comunicaciones y control. No menciona expresamente la inteligencia pero sí se refiere a avanzar con nuevas funcionalidades y aplicaciones, lo cual lleva a pensar que realmente son estas funcionalidades, y no los equipos que la componen, las que constituyen la esencia de una Smart Grid. [17]

De hecho, el NIST concibe la smart grid como un complejo sistema de sistemas, cuyo entendimiento exige identificar tanto sus pilares básicos como la interrelación entre los mismos. A tal objeto, el NIST creó un modelo conceptual de arquitectura de referencia, que será visto más adelante. Este modelo proporciona un medio para analizar los casos de uso e identificar interfaces, donde se hacen necesarios estándares de interoperabilidad, y para facilitar el desarrollo de una estrategia para la ciberseguridad. [17]

Según el Massachusetts Institute of Technology (MIT) su definición varía en función de quién lo define; ya sea la industria, el gobierno o la sociedad. [17] No obstante la mejor manera de describirla sería [21]:

"La expansión del uso de nuevos sistemas de comunicaciones, sensores y control en toda la red eléctrica".

El informe del Electric Power Research Institute (EPRI) adopta la siguiente definición, por la cual el concepto de smart grid hace referencia a [22]:

"La modernización del suministro eléctrico para lo cual se debe monitorear, proteger y optimizar automáticamente la operación de los elementos interconectados

a ella, desde la generación (tanto si está centralizada como distribuida), pasando por la red de transporte y distribución hasta los consumidores industriales, sistemas automáticos en edificios, consumidores finales y sus equipos (vehículo eléctrico, electrodomésticos, etc.)".

Por consiguiente, una de las diferencias entre esta definición y la del MIT es que el concepto de smart grid de EPRI considera también a los consumidores finales. Según este informe, el sistema eléctrico del futuro se caracterizará por ser muy flexible, reconfigurable y conectado, y optimizará los recursos energéticos. Se trata entonces de una red en la que no sólo fluye bidireccionalmente electricidad sino también información. [17]

La definición de la Plataforma Tecnológica Europea de Smart Grids, establece que [23]:

"Una smart grid es una red eléctrica que integra inteligentemente las acciones de todos los usuarios conectados a ella (generadores, consumidores y productores-consumidores) para proveer eficientemente un suministro sostenible, económico y seguro".

El informe del EU Commission Task Force for Smart Grids establece que [24]:

"Una smart grid es una red eléctrica que integra de manera económicamente eficiente el comportamiento y las acciones de todos los usuarios conectados al mismo (generadores, consumidores y productores-consumidores) para garantizar un sistema energético sostenible y económicamente eficiente con pocas pérdidas y alto nivel de calidad, protección y seguridad de suministro".

En base a todas estas definiciones podemos sacar algunas características en común de las Smart Grid. Los aspectos que caracterizan en forma general a una Smart Grid son: contadores inteligentes, integración de energías renovables, automatización de la red, movilidad eléctrica, tecnologías de almacenamiento de energía, microrredes, centrales eléctricas virtuales, gestión activa de la demanda y un sistema regulatorio inteligente. Por otro lado, las dos aplicaciones principales de las Smart Grid son el monitoreo y el control avanzado de la red de distribución. [17]

Las redes eléctricas del futuro serán distintas a las actuales, al ofrecer una serie de funcionalidades nuevas. En este sentido, asumiendo que la implantación de las Smart Grids tendrá lugar a largo plazo, es previsible que a mediano plazo coexistan dos generaciones de redes eléctricas: las convencionales o actuales y las redes inteligentes. El grado de avance de las implantaciones dependerá tanto de los aspectos tecnológicos, como del impulso político y de la normativa que incentive su desarrollo.

[17]

A grandes rasgos, según se muestra en [17], las redes eléctricas inteligentes se diferencian de las actuales en los siguientes aspectos:

- Las redes actuales consisten en una mezcla de sistemas electromecánicos y sistemas digitales, mientras que en un futuro se pasará a contar con sistemas en su mayoría digitales.
- La comunicación actualmente es unidireccional, mientras que se está transicionando hacia una comunicación bidireccional.
- También habrá cambios en la generación de energía, pasando de un modelo de generación centralizado a una combinación entre generación centralizada y distribuida.
- Actualmente se cuenta con un número limitado de sensores pero en un futuro se pasará a contar con una gran cantidad de sensores, teniendo una red completamente monitoreada, con mayores niveles de control y supervisión.
- Hoy en día no se cuenta con muchos datos y por lo tanto no hay sistemas de gestión de datos. Con el despliegue de los medidores inteligentes, se contará con una cantidad muy grande de datos, generando la necesidad de contar con sistemas de almacenamiento y de tomar medidas para garantizar la protección de datos sensibles de los clientes. A su vez, mediante el uso de los dispositivos inteligentes, el consumidor pasa a tener un rol más activo en lugar de ser simplemente un consumidor pasivo.
- La facturación pasará a ser más compleja, pudiendo cambiar las tarifas en forma dinámica de acuerdo a la demanda en tiempo real o incluso según la calidad del servicio.
- En las redes eléctricas inteligentes será posible identificar los problemas de calidad de servicio y solucionarlos rápidamente.

Estas diferencias o mejoras que supondrá la implementación de Smart Grids pueden verse en mayor detalle en el apéndice **??**.

3.2. Arquitecturas

Ha habido grandes esfuerzos por lograr la estandarización del concepto de Smart Grid, principalmente en Europa. Para esto se ha trabajado en la definición de estándares, de manera de lograr consenso en cuanto a las funcionalidades a ofre-

cer, interfaces, protocolos y otros estándares a utilizar. La principal motivación para la definición de estos modelos de arquitecturas de referencia es para lograr la interoperabilidad entre los diferentes productos de distintos tipos y fabricantes.

En Estados Unidos la iniciativa U.S. GridWise, que lidera la coordinación de las actividades relacionadas con Smart Grid entre los diferentes participantes, tanto de la industria como del gobierno, publicó en 2007 una serie de pautas para garantizar la interoperabilidad entre las diferentes tecnologías y sistemas. En estas pautas, se definen 8 capas para las cuales se debe garantizar la interoperabilidad. Las mismas se agrupan de la siguiente manera [19]:

- Técnica
  - Conectividad básica
  - Interoperabilidad de las redes
  - Interoperabilidad sintáctica
- Informacional
  - Entendimiento semántico
  - Contexto de negocio
- Organizacional
  - Procedimientos de negocio
  - Objetivos de negocio
  - Políticas económicas y regulatorias

Estas capas forman la base de otros modelos posteriores, como es el caso del modelo NIST y el modelo europeo. [19]

En 2010, el NIST presentó su modelo de referencia para Smart Grids. El mismo divide al concepto de Smart Grid en 7 bloques llamados dominios. Estos son [19]:

- Generación
- Transmisión
- Distribución
- Consumidores
- Proveedores de servicio
- Operaciones
- Mercados

A su vez, identifica las interfaces y relaciones entre los distintos dominios y actores.

El Smart Grid Coordination Group (SGCG), quién es el encargado en Europa

de coordinar los esfuerzos para identificar las funcionalidades más relevantes de los sistemas de Smart Grid y definir los estándares necesarios para su implementación, definió en 2014 un modelo de arquitectura de referencia para el mercado europeo, adaptando el modelo del NIST a la realidad del mismo. El mismo se puede observar en la figura 3.1. Se trata de un modelo tridimensional que se divide en dominios (definidos en forma similar al modelo del NIST), zonas y capas de interoperabilidad. Los dominios se definen como [25]:

- Generación
- Transporte
- Distribución
- Recursos energéticos distribuidos
- Instalaciones del consumidor

Aquí podemos observar que se agrega el dominio "Recursos energéticos distribuidos", lo cual representa la importancia que tienen los pequeños generadores en el mercado europeo. [19]

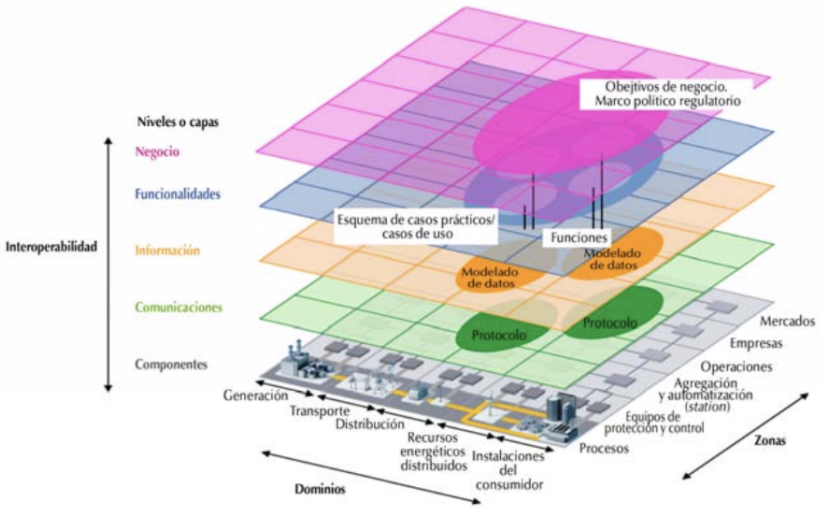

Figura 3.1: Modelo de arquitectura de Smart Grid [17]

Por otro lado, las zonas se derivan de las capas típicas de sistemas de automatización industrial. Las zonas definidas en el modelo son las siguientes [17]:

- *Procesos (Process)*
  Representa todo lo relacionado con la transformación física, química o espacial de la energía así como el equipamiento necesario para ello.
- *Equipos de protección y control (Field)*

Todo el equipamiento utilizado para proteger, controlar y monitorizar los procesos del sistema eléctrico.

- *Agregación y automatización (Station)*
  Tiene el objetivo de "agrupar" los datos a comunicar y procesar en la zona de operaciones.
- *Operaciones (Operation)*
  Representa a los sistemas para controlar la operación.
- *Empresas (Enterprise)*
  Incluye tanto los procedimientos organizacionales y comerciales como aquellos relativos a los servicios e infraestructuras para empresas del rubro.
- *Mercados (Market)*
  Refleja todas las posibles operaciones mercantiles relacionadas con el suministro de energía, como por ejemplo el mercado mayorista y el minorista.

Por último, las cinco capas de interoperabilidad que define el modelo son [17]:

- *Componentes*
  Representa el nivel físico del sistema eléctrico.
- *Comunicaciones*
  Corresponde a la infraestructura y protocolos de comunicación necesarios para intercambiar la información entre las cinco capas.
- *Información*
  Refiere a los modelos de datos, es decir, al registro, almacenamiento y elaboración de información a partir de los datos intercambiados.
- *Funcionalidades*
  Representa la actividad de las compañías eléctricas.
- *Negocio*
  Representa los objetivos y procesos de negocio.

Estos modelos de arquitectura de referencia permiten identificar las diferentes áreas a abordar y los estándares, protocolos y sistemas disponibles en cada una. De esta manera, resulta más fácil identificar en qué áreas hace falta establecer estándares o desarrollar nuevos componentes para permitir el funcionamiento esperado y cumplir con los objetivos de este tipo de sistemas. [17]

3.3. AMI (Advanced Metering Infrastructure)

Las AMI son un componente crucial de las Smart Grids, se trata de la infraestructura de medición. Maneja la comunicación bidireccional entre los medidores inteligentes y los sistemas, permitiendo enviar, recibir y procesar los datos de consumo de los clientes, además de operaciones adicionales sobre la red.

Según [26] las arquitecturas más comunes para este tipo de sistemas incluyen los siguientes componentes:

- *Medidores inteligentes (Smart Meters)*
  Dispositivos encargados de medir y reportar el consumo de energía.
- *Concentradores (Data Concentrators)*
  Dispositivos que procesan datos de varios medidores.
- *Head End System (HES)*
  Sistema encargado de recolectar los datos, procesarlos y tomar acciones en base a los mismos.
- *Redes de area local (Home Area Network, Neighborhood Area Network)*
  Permiten la comunicación bidireccional entre los medidores y los concentrados.
- *Wide Area Network (WAN)*
  Permite la comunicación bidireccional entre los concentradores y el HES o entre medidores y HES en algunos casos.

Los medidores inteligentes son una evolución de los medidores electromecánicos tradicionales, estos cuentan con la habilidad de medir el consumo de energía en tiempo real y de comunicarse sobre una o más redes, tanto cableadas como inalámbricas, para transmitir las mediciones a la empresa proveedora del servicio.[26]

Estos dispositivos son una pieza central dentro de las AMI. Ellos son los encargados de medir el consumo de energía de los consumidores finales y de transmitir esta información al proveedor del servicio para que pueda facturar al consumidor en forma automática. Además, se encargan de la medición de otros parámetros técnicos de interés para el proveedor para balancear la carga en la red de energía eléctrica, y también permiten la desconexión o reconexión en forma automática de clientes, tanto por razones contractuales, como por ejemplo que no se encuentren al día con el pago del servicio, como por razones técnicas o de seguridad debido a problemas en la red. [26]

La información recabada por los medidores inteligentes permite que el proveedor

del servicio tenga una visión en tiempo real, o al menos casi en tiempo real, del estado de la red. De esta forma, es posible manejar la red de mejor manera con el fin de prevenir o manejar emergencias, evitando así daños en la red o incluso daños o perjuicios a los consumidores. Con esta información se pueden generar reportes y estadísticas de utilidad para la empresa proveedora que le permitan realizar una mejor planificación de las tareas de generación y distribución.[26]

Por otro lado, el uso de este tipo de medidores facilita la comunicación con los clientes, generando así una comunicación de dos vías, lo cual es uno de los objetivos de las Smart Grids. En esta línea, una de las funciones más útiles para los clientes es la comunicación de los cambios en los precios del servicio, permitiendo que sea posible adaptar el consumo realizando las tareas que requieran un mayor consumo energético en las horas donde el precio de la energía sea menor.[26]

Según [27], los sistemas de Smart Meters deben al menos soportar las siguientes funciones:

- Adquisición de información sobre la red local doméstica (HAN, Home Area Network), y procesamiento y comunicación de la misma sobre una Wide Area Network (WAN) a la empresa.
- Almacenamiento de la información de consumo y demanda. Comunicación del consumo en tiempo real a la empresa para su facturación y contabilidad.
- Comunicación al usuario del consumo en tiempo real, por ejemplo a través de un display en el dispositivo o a través de una aplicación móvil.
- Comunicación bidireccional con el HES, permitiendo:
  - Control del medidor sin requerir acceso físico al mismo.
  - Descarga/Actualización del software en el medidor de manera remota.
- Escalabilidad e interoperabilidad, con el objetivo de soportar varios proveedores de servicio. Esto resulta de importancia en mercados como el europeo, donde la comercialización de energía eléctrica no está restringida a un único proveedor.
- Construcción de perfiles de carga.
- La privacidad y seguridad de los datos de los consumidores debe estar garantizada mediante la utilización de servicios y mecanismos de seguridad apropiados.

Los medidores inteligentes se instalan comúnmente en los hogares de los consumidores, y típicamente se conectan a un concentrador, en donde se agrupa la

información de todos los medidores conectados a él. Estos concentradores pueden ser a nivel de edificio, de cuadra o grupo de hogares o a nivel de barrio incluso. Otra solución posible es que los medidores se comuniquen directamente en forma individual con el sistema de la empresa proveedora del servicio (HES, Head End System). [28]

Las comunicaciones entre medidores y concentradores, y entre concentradores o medidores y el HES, se puede realizar sobre distintos tipos de red, siendo muy común que se utilice la tecnología PLC (Power Line Communication) utilizando la misma red eléctrica para conectar medidores y concentradores, y tecnologías wireless como por ejemplo GPRS/UMTS para la conexión con el HES. [28]

Un ejemplo de arquitectura posible puede observarse en la figura 3.2.

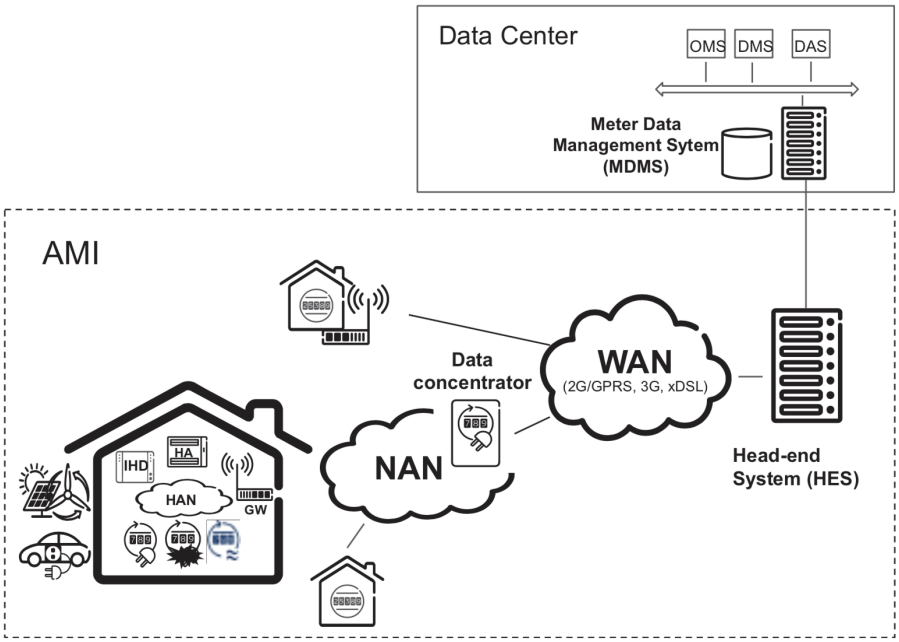

Figura 3.2: Red de medidas inteligentes [26]

El despliegue de medidores inteligentes está teniendo mucha inversión en los últimos años, por ejemplo en Europa, para 2022 todos los estados miembros de la unión europea deberán contar con medidores inteligentes para electricidad. Es por esto que resulta de mucha importancia el estudio de las consecuencias que esto puede conllevar, de sus riesgos y problemáticas asociadas, y de posibles soluciones a las mismas. [27]

3.4. Desafíos de seguridad y privacidad

El desarrollo de las Smart Grids genera varios desafíos de seguridad agravados por la escala y la complejidad que toman estos sistemas. Muchos subsistemas que se encontraban previamente aislados ahora requieren interoperabilidad y comunicación constante entre ellos.

La creciente adopción de estos sistemas, genera muchas preguntas y preocupaciones acerca de su seguridad y de la privacidad de los clientes.

Del lado de los proveedores, preocupa la presencia de vulnerabilidades de seguridad en los dispositivos disponibles en el mercado que permita que potencialmente un atacante pueda modificar las lecturas de los medidores, provocando grandes pérdidas económicas, tanto a los consumidores como a los proveedores. Además, muchos de estos dispositivos cuentan con la capacidad de ser apagados en forma remota, pudiendo resultar en graves problemas de disponibilidad del servicio de ser atacados con malas intenciones. [19]

Por otra parte, del lado de los consumidores, preocupa que la información sobre el consumo de los hogares caiga en manos equivocadas o incluso que se haga un mal uso de la misma por las empresas proveedoras del servicio. Esta información es de carácter sensible ya que al tener datos del consumo en tiempo real se puede hacer un análisis de los hábitos de los consumidores, incluso llegando al detalle de saber si se encuentran personas o no en el hogar, y qué actividades realizan y en qué horarios. Esta información inferida puede ser utilizada con varios fines, como por ejemplo publicidad dirigida, estudio de comportamiento de consumidores, robo, etc. En [29] se muestra cómo a través de la información recolectada se puede extrapolar un perfil de usuario muy preciso.

Los problemas de seguridad y privacidad son la principal barrera en la aceptación de este tipo de sistemas. En algunos países incluso hay leyes que regulan su uso, siendo Alemania un ejemplo de esto, donde las medidas de consumo de energía están sujetas a regulaciones de privacidad y se requiere la utilización de mecanismos de cifrado para su transferencia, proponiendo el uso de doble cifrado para evitar ataques man-in-the-middle. Debido a esto las empresas se arriesgan a sufrir no solo pérdida de reputación y clientes, sino también a enfrentar consecuencias legales, por lo que resulta de suma importancia para ellas encontrar soluciones a estos problemas. [19]

Las amenazas cambian constantemente y cada día se desarrollan nuevos méto-

dos de ciberataques que requieren nuevas medidas de seguridad. Las soluciones de seguridad existentes no siempre pueden ser aplicadas directamente, debido a que las Smart Grid son sistemas ciberfisicos con problemáticas particulares distintas a los de los sistemas puramente computacionales. [19]

Además, se requiere un cambio en la forma de pensar en la seguridad en este tipo de sistemas. El enfoque actual se centra principalmente en la seguridad física y en la resistencia a fallos pero es necesario tener en cuenta las nuevas funciones y características que tendrán estos sistemas. [19] En la realidad de las redes eléctricas, las medidas adicionales de seguridad pueden llegar a ser contraproductivas, generando que una señal de vital importancia no llegue a destino a tiempo debido a medidas como chequeos de integridad y autenticación. Las medidas que se tomen para garantizar la seguridad tienen que estar bien justificadas y enfocadas correctamente. Esto no resulta nada fácil de lograr, especialmente en un mundo donde hay tantos estándares de seguridad disponibles, lo cual hace que no resulte trivial elegir qué camino seguir. [19]

Como un desafío adicional se debe tener en cuenta que realizar pruebas de seguridad en los sistemas de Smart Grid no es una tarea sencilla, dado que no se puede trabajar sobre una copia completa del sistema aislada completamente del ambiente de producción. [19]

Otro desafío a tener en cuenta es que los dispositivos que componen una Smart Grid tienen una expectativa de vida mucho mayor a los sistemas computacionales convencionales. Mucho puede cambiar en este tiempo, lo cual requiere que los sistemas estén en continua actualización, elevando así los costos de mantenimiento. [19]

Según [19] existen varias preguntas por responder. La primera es decidir qué sistemas dentro de la Smart Grid se deben asegurar. Esta pregunta es difícil de responder, ya que el objetivo cambia constantemente, todavía no se sabe con certeza cómo van a lucir los sistemas futuros, además de que las soluciones serán distintas para diferentes proveedores del servicio. Para esto es útil basarse en las arquitecturas estándar ya analizadas por distintos grupos de investigación.

La segunda pregunta es contra qué tipo de ataques se debe asegurar el sistema. Esto se puede derivar de la experiencia de otros campos de las tecnologías de la información y de otros tipos de sistemas. Sin embargo, el desarrollo de nuevos métodos de ataque y el entendimiento de los mismos continúa siendo una carrera entre atacantes y quienes se dedican a garantizar la seguridad del sistema.

Por último, se debe considerar cuál sería el efecto de un ataque. Para evaluar qué áreas o partes del sistema es prioritario asegurar, resulta necesario evaluar los posibles riesgos y sus probabilidades e impacto, de forma de mitigar los riesgos con mayor probabilidad de ocurrencia y con impacto más crítico. Esto resulta en un esfuerzo interdisciplinario para nada trivial.

3.5. Tipos de amenazas

En 2013, la European Union Agency for Network and Information Security (ENISA) estudió las amenazas más importantes dentro del contexto de Smart Grid, sugiriendo los siguientes grupos de amenazas [30]:

- Desastres naturales
- Daño o pérdida de componentes
- Cortes de suministro
- Actividad criminal y abuso
- Ataques físicos a la infraestructura
- Pérdida o daño de información involuntaria
- Fallas o mal funcionamiento
- Escuchas, intercepción o secuestro de las comunicaciones
- Problemas legales

Además, la organización U.S. National Electric Sector Cybersecurity Organization Resource (NESCOR) se enfocó en la identificación de escenarios de falla, los cuales los define como eventos ocurridos sobre componentes de una Smart Grid que tienen un impacto negativo en la red eléctrica. Estos eventos se deben a vulnerabilidades que son explotadas por amenazas, siendo tanto ataques deliberados, fallas involuntarias o desastres naturales. Estos escenarios se categorizan según dónde pueden ocurrir, utilizando como guía los dominios definidos en los modelos de arquitectura de referencia. Los componentes donde pueden ocurrir estos escenarios son [31]:

- *Red de medidas (AMI)*
  Sistemas que permiten obtener información de la carga y demanda en la red eléctrica y la facturación casi en tiempo real.
- *Recursos de energía distribuidos*
  Sistemas descentralizados que proveen energía a la red o almacenan energía sobrante.

- *Sistemas de monitoreo, protección y control*
- *Transporte eléctrico*
  Todos los sistemas relacionados a los vehículos eléctricos.
- *Respuesta a la demanda*
  Sistemas relacionados a la administración del consumo de energía por parte de los consumidores para responder a variaciones en las capacidades de generación, como balance de la red eléctrica y fijación de precios.
- *Administración de la distribución*
  Componentes para administrar y optimizar el funcionamiento de los sistemas de distribución.

Por otra parte, los agentes que lleven a cabo estas amenazas pueden ser muy variados, incluyendo incluso errores involuntarios o desastres naturales. Resulta importante estudiarlos y clasificarlos, ya que la urgencia con la que deben ser tratados los distintos tipos de amenaza depende en gran medida de las capacidades, recursos y motivación con las que cuente el agente, o con la probabilidad de ocurrencia en el caso de los agentes involuntarios. Tanto ENISA como NESCOR clasifican a estos agentes de manera muy similar, en las siguientes categorías [30, 31]:

- Otros países que busquen obtener información o causar daño por motivos políticos.
- Organizaciones terroristas o individuos que busquen causar daño por motivos religiosos, ideológicos o por razones políticas.
- Organizaciones o individuos motivados por la ganancia económica o por ganar una ventaja competitiva.
- Organizaciones o individuos que busquen causar daño.
- Grupos de activistas o individuos movidos por motivos sociales o políticos.
- Individuos o grupos que busquen reconocimiento o simplemente por entretenimiento.
- Desastres naturales, accidentes, errores humanos, degradación de los sistemas.

3.6. Ataques posibles

La transformación de las redes eléctricas convencionales a Smart Grids trae consigo muchos nuevos ataques posibles, agrandando así la superficie de ataque. En

el pasado la principal preocupación eran los ataques a los diferentes componentes físicos de la red. Hoy en día estos ataques siguen siendo una preocupación, incluso en mayor medida, ya que ahora no alcanza con proteger las instalaciones donde se encuentran estos componentes, debido a que algunos de ellos se encontrarán en los domicilios de los consumidores como es el caso de los medidores inteligentes. [19]

Con el desarrollo de Smart Grids se suman ataques a las redes de comunicación o a los sistemas informáticos de control, los cuales pueden tener un impacto negativo sobre la red eléctrica, tanto intencionalmente o como efecto secundario. [19]

Los ataques posibles pueden ser pequeños, como lo son los ataques de tampering a los medidores inteligentes que tienen como objetivo reducir el costo del servicio o enviar medidas fraudulentas, causando que no pueda ser interpretado correctamente el estado del sistema y generando errores en los comandos de control. O también pueden ser ataques de mayor envergadura, donde varios subsistemas son atacados para causar pérdidas de suministro eléctrico a gran escala. [19]

Los ataques pueden tener consecuencias tanto para los consumidores como para los proveedores del servicio, generando la no disponibilidad de energía eléctrica, pérdida de reputación o pérdidas financieras para el proveedor. Incluso a mayor escala se puede provocar la pérdida del suministro en barrios o ciudades enteras, generando consecuencias aún más graves como lesiones serias, muertes o daños a servicios críticos como el transporte y la asistencia de salud. [19]

Los ataques son posibles debido a la existencia de vulnerabilidades y, debido a la inexperiencia con este tipo de tecnologías, en este campo es muy probable que se lancen al mercado productos que no han pasado por controles estrictos de aseguramiento de calidad. Además, se está intentando avanzar muy rápidamente con la implantación de medidores inteligentes y no todos los países cuentan con leyes regulando requerimientos de seguridad mínimos. Nos encontramos así ante la situación de que potencialmente se esté instalando un gran número de medidores con potencial de ser vulnerables debido a la no definición de requerimientos de seguridad para los mismos. [19]

Para encontrar soluciones a estos problemas se requiere analizar cuáles son los distintos atacantes posibles y sus motivaciones. En [27] se identifican los siguientes tipos de atacantes:

- *Eavesdroppers (espías pasivos)*
  Cualquier tipo de individuo u organización interesada en saber lo que se está transmitiendo en la red. Puede ser solo por curiosidad o con intencio-

nes maliciosas, como por ejemplo para saber cuándo hay personas en el hogar para decidir el mejor momento para llevar a cabo un robo. Este tipo de ataques pasivos no tienen impacto en el suministro eléctrico.

- *Agencias de publicidad y periodistas*
  A través de escuchas pasivas en la red, las agencias de publicidad pueden recabar información valiosa para, por ejemplo, saber cuándo son los mejores momentos en el día para publicitar un producto o cuáles son los hábitos de los consumidores para poder dirigir la publicidad de forma más efectiva. Además, periodistas investigando a personalidades importantes, como políticos o celebridades, pueden utilizar este tipo de escuchas y análisis del tráfico para averiguar sus hábitos y estilo de vida.

- *Consumidores*
  Los mismos consumidores del servicio pueden ser atacantes, reportando medidas de consumo de energía inferiores o reportando una mayor generación de energía de lo real. Este tipo de ataques tienen un impacto económico para las empresas.

- *Nuevos atacantes*
  Se trata de atacantes que no buscan un beneficio económico pero buscan atacar los sistemas con el objetivo de demostrar su habilidad. Aunque no obtengan un beneficio económico directo, igualmente causan perjuicios para los consumidores y empresas.

- *Atacantes activos*
  Individuos o grupos de atacantes, potencialmente financiados por otras naciones enemigas, que buscan cortar el suministro de energía en partes de la red o incluso en la totalidad de la red. Estos atacantes muchas veces buscan poner en riesgo la seguridad nacional.

Una vez estudiado el modelo de atacantes y habiendo identificado posibles atacantes y sus motivaciones, se puede pasar a estudiar los ataques posibles sobre el sistema, como se muestra en [27]:

- *Eavesdropping (Escuchas Pasivas)*
  Se trata de un ataque pasivo en el que el atacante escucha en la WAN la información en tránsito desde el medidor hasta el HES. Estos ataques afectan la privacidad de los consumidores y tienen distintas posibles consecuencias que ya fueron discutidas previamente.

- *Ataques de denegación de servicio (DoS)*
  Estos ataques pueden tener como objetivo la red eléctrica en su totalidad o partes de la misma, buscando dejar no disponible el servicio. Se pueden realizar enviando una cantidad de mensajes mucho mayor a la normal tanto a los medidores como al HES, de forma de evitar que se procesen mensajes válidos, evitando así el funcionamiento de la Smart Grid.

- *Inyección de paquetes*
  Al inyectar mensajes falsos en la comunicación, se puede enviar información de facturación falsa, generando costos económicos a los consumidores y/o a los proveedores, o incluso se puede enviar mensajes para desconectar a un hogar de la red.

- *Inyección de malware*
  Mediante la inyección de malware en la red, se puede afectar la comunicación entre los dispositivos y comprometer los procesos de facturación y reporte. Al afectar estos procesos se puede desestabilizar la carga en la red, ya que el balance de la misma depende del reporte del estado de la oferta y la demanda. En las redes eléctricas esto puede provocar el mal funcionamiento de la infraestructura de distribución.

- *Conectar o desconectar dispositivos en forma remota*
  Al enviar mensajes de desconexión a los medidores se puede lograr la desconexión de uno, varios o incluso de toda la red de medidores.

- *Manipulación del firmware*
  Las manipulaciones al firmware pueden ser tanto a la parte encargada de medir el consumo como a otras partes del mismo. En el primer caso, las manipulaciones pueden servir para enviar medidas de consumo falsas, provocando el mal funcionamiento de las funciones de facturación y reporte. Este ataque puede ser realizado teniendo acceso físico al medidor pero también si está habilitada la actualización del firmware de forma remota. Normalmente un único medidor será afectado pero puede realizarse un ataque masivo si la actualización remota es una posibilidad.

- *Ataques Man-in-the-Middle (MitM)*
  Pueden ser realizados tanto en las redes locales de medidores, es decir, entre medidores y concentrador, o en la WAN pudiendo manipular todo el tráfico en tránsito hacia y desde el HES. Estos ataques pueden tener consecuencias muy graves, incluso comprometiendo la seguridad nacional.

Como se puede observar, las consecuencias de estos ataques van desde la divulgación de información de los consumidores, afectando su privacidad, lo cual puede traer consecuencias legales para las empresas, hasta problemas de seguridad nacional.

Frente a este escenario resulta apremiante tomar medidas para evitar o mitigar el riesgo de sufrir estos ataques. Diferentes contramedidas pueden ser aplicadas, algunas son familiares porque se tratan de las mismas aplicadas a las redes de propósito general, como por ejemplo [27]:

- *Comunicaciones cifradas*
  Se recomienda doble cifrado, tanto en la capa de aplicación, asegurando cifrado end-to-end, como en la capa de transporte, utilizando protocolos ya existentes como por ejemplo TLS.

- *Protección de integridad*
  Es de vital importancia garantizar la integridad de los mensajes, utilizando por ejemplo Message Authentication Codes (MAC) para asegurar la integridad de la información de consumo energético.

- *Verificación de autenticidad*
  Tanto los participantes en la comunicación como la información transmitida deben ser autenticados. Es deseable la implementación de autenticación mutua. Se puede usar cualquiera de las soluciones estándares ya conocidas.

- *Utilización de Gateways*
  Esta es una solución propuesta por algunos países europeos, como por ejemplo Alemania y el Reino Unido. Consiste en la utilización de un dispositivo que actúe como gateway entre los dispositivos de medición y el HES. El gateway recibe los datos de consumo directamente de los medidores y concentradores y comunica esta información al HES en forma periódica, cada cierto intervalo de tiempo. Este nuevo dispositivo es el responsable de garantizar la privacidad de los consumidores. Además, el gateway recibe los comandos que envía el HES y los transmite a los medidores.

- *Sistemas de detección y prevención de intrusiones*
  Este tipo de sistemas ayudan en la identificación de intrusiones, detectando nodos que estén actuando como fuentes de ataques y excluyéndolos de la red.

Además de estas contramedidas, es recomendable tener en cuenta los requerimientos de seguridad de los sistemas de AMI lo más temprano posible en el diseño de la solución. [27]

Capítulo 4

DLMS/COSEM

DLMS/COSEM es un protocolo de capa de aplicación para intercambio de medidas de energía desde y hacia medidores inteligentes, soportando aplicaciones como lectura de medidas en forma remota, control remoto de dispositivos de medida y servicios de valor agregado de medición de cualquier tipo de energía. Este protocolo se describe en una serie de estándares que fue adoptado por la International Electrotechnical Commission (IEC) como la serie de estándares IEC 62056. Estos estándares han sido adoptados por un gran número de fabricantes y proveedores de servicio, convirtiéndolo en uno de los más implementados en los medidores inteligentes y en particular, el estándar utilizado en la solución de UTE.

A continuación, describiremos brevemente el protocolo y pasaremos a presentar sus vulnerabilidades conocidas estudiadas, tanto del protocolo en sí como posibles vulnerabilidades de implementación.

4.1. Descripción del protocolo

El protocolo DLMS/COSEM, utilizando un enfoque basado en objetos, provee distintas clases de interfaz para representar objetos de la realidad de las AMI y sus funcionalidades. Mediante la instanciación de estas clases, se representa el estado y la funcionalidad del equipamiento de medición, de forma de exponerlo a través de la red de comunicación.

Los dispositivos de la AMI se modelan en el protocolo como dispositivos físicos, los cuales a su vez contienen uno o varios dispositivos lógicos que se encargan de modelar funcionalidades específicas de cada equipo. Es en estos últimos donde se

encuentran los objetos que modelan la funcionalidad ofrecida por los dispositivos. Estos objetos, al igual que en el paradigma de programación orientada a objetos, no son más que una agrupación de atributos y métodos. [32]

Los medidores actúan como servidores, los cuales son consultados por aplicaciones cliente que obtienen datos, proveen información de control o ejecutan acciones en el medidor a través de los atributos y métodos expuestos en los objetos definidos en el medidor.

Para definir un medidor basta con definir un dispositivo físico con sus dispositivos lógicos e instanciar las clases de interfaz deseadas. El estándar define 70 clases de interfaz que pueden ser utilizadas, cada una con distintos atributos y métodos disponibles. Por ejemplo, para definir una medida de energía se provee una clase Register, la cual será instanciada por cada uno de los tipos de medidas que mantenga el medidor. Tomando como ejemplo un medidor que se encargue de medir el consumo de energía eléctrica, de gas y de agua, se definirán tres dispositivos lógicos, uno por cada tipo de energía, y dentro de cada uno de ellos se tendrá una instancia de la clase Register, la cuál contendrá un atributo con el valor de la medida del consumo de energía. [32]

4.2. Acceso a los objetos

Para poder acceder a los objetos en un servidor DLMS/COSEM, es necesario establecer una Application Association (AA) con el cliente, de manera de identificar a los participantes y establecer el contexto en el cual se llevará a cabo la comunicación, proveyendo por ejemplo cuál mecanismo de autenticación debe ser utilizado. Los servidores siempre poseen una instancia de un tipo especial de clase llamada Association, que contiene esta información y además contiene una lista de todos los objetos que son accesibles en ese servidor en particular para que una aplicación cliente pueda saber a qué información puede acceder y cómo hacerlo. [32]

El protocolo provee dos formas de acceder a los objetos, por Logical Name (LN) o por Short Name (SN).

Cada objeto tiene siempre un LN, en general los fabricantes usan los mismos valores en sus dispositivos, de forma que una misma aplicación encargada de recolectar datos de medidores pueda hacerlo sin importar el fabricante. El LN es el primer atributo de un objeto COSEM y junto con el id de la clase de interfaz define el significado del objeto. El LN se define como un código OBIS (Object Identifica-

tion System), de 6 bytes, por ejemplo el código del objeto Association es siempre 0.0.40.0.0.255, y dentro de cada objeto los atributos y métodos se identifican con un id numérico. [32]

En la forma de acceso por LN, los métodos y atributos se acceden mediante el id de la clase de interfaz, el valor del LN y el índice del atributo o del método al que se quiere acceder. De la siguiente manera: id de la clase | logical name | id atributo o método. [32]

En cambio en la forma de acceso por SN, cada objeto es mapeado a un SN. Esta es una forma de acceso simplificada, indicada para ser utilizada por dispositivos simples. En este caso, cada atributo y método de los objetos es identificado con un entero de 13 bits. [32]

Mediante estas dos formas el cliente puede acceder a los objetos, pudiendo leer o modificar los valores de sus atributos o invocando acciones mediante sus métodos.

4.3. Autenticación y control de acceso

Se definen tres niveles de autenticación en el protocolo [32]:

- *Lowest Level Security*
  Ni el cliente ni el servidor son autenticados.
- *Low Level Security (LLS)*
  Solo el cliente se autentica presentando un password al servidor. Este tipo de autenticación solo debe ser utilizado cuando la comunicación se lleva a cabo sobre un canal seguro, de manera de evitar escuchas y replay de mensajes.
- *High Level Security (HLS)*
  Se utiliza autenticación mutua, tanto el cliente como el servidor se autentican contra su contraparte. Este es el método de autenticación recomendado ya que en general no se puede garantizar la seguridad del canal de comunicación. Se puede optar por HLS-MD5 (Message Digest 5), HLS-SHA1 (Secure Hash Algorithm 1) o HLS GMAC (Galois Message Authentication Code). [33]

Hay muchos mecanismos posibles para controlar el acceso a los objetos COSEM, el más simple es utilizando la dirección de los clientes para definir a qué objetos ese cliente en particular puede tener acceso y de qué tipo (lectura o escritura). [32]

4.4. Establecimiento de la conexión

Para el manejo de la conexión entre un cliente y un servidor DLMS/COSEM, se utilizan los servicios provistos por Association Control Service Element (ACSE). Se cuenta con 4 tipos de mensajes para establecer y terminar una conexión, estos son [32]:

- AARQ (Association Request)
- AARE (Association Response)
- RLRQ (Release Request)
- RLRE (Release Response)

El formato de estos mensajes se encuentra definido en el estándar OSI/IEC 8650-1 y se puede consultar en el apéndice 1.

Al comenzar una conexión, el cliente envía un mensaje AARQ al servidor, indicando algunos de sus datos y qué método de cifrado y autenticación desea utilizar, además se envía información adicional como qué versión del protocolo utilizar. Como respuesta a este mensaje, el servidor envía un mensaje AARE, aceptando o rechazando el intento de conexión, o si se utiliza HLS como método de autenticación, aceptando parcialmente la conexión, esperando a que se complete el paso extra de autenticación mutua. Este paso extra consiste en la respuesta a un desafío presentado por la contraparte, el servidor le envía al cliente un nonce y el cliente le envía al servidor su respuesta en base a este nonce, y viceversa. En el caso de utilizar MD5 o SHA1, las respuestas HLS se calculan como f(nonce | secreto compartido). Al utilizar GMAC para calcular la respuesta al desafío, se aplica GMAC a la concatenación de un byte de control 0x10, la clave de autenticación y el nonce. [33]

Luego de establecida la conexión el cliente puede enviarle al servidor requests, tanto para obtener datos como para invocar métodos, para las cuáles recibirá respuestas del servidor. Los mensajes cuentan con un header que indica el tipo de mensaje que es y el tipo de comunicación, los valores posibles pueden verse en la figura 4.1:

Finalmente, al querer terminar una conexión, el cliente le envía al servidor un mensaje RLRQ solicitando la finalización y luego el servidor responde con un mensaje RLRE confirmando la conclusión de la comunicación entre ambos. Este intercambio, desde comienzo a fin de la conexión, puede verse en la figura 4.2.

Message	Plaintext	Global	Dedicated
Get Request	192	200	208
Set Request	193	201	209
Event Notification Request	194	202	210
Action Request	195	203	211
Get Response	196	204	212
Set Response	197	205	213
Action Response	198	206	214

Figura 4.1: Tipos de mensaje DLMS/COSEM [33]

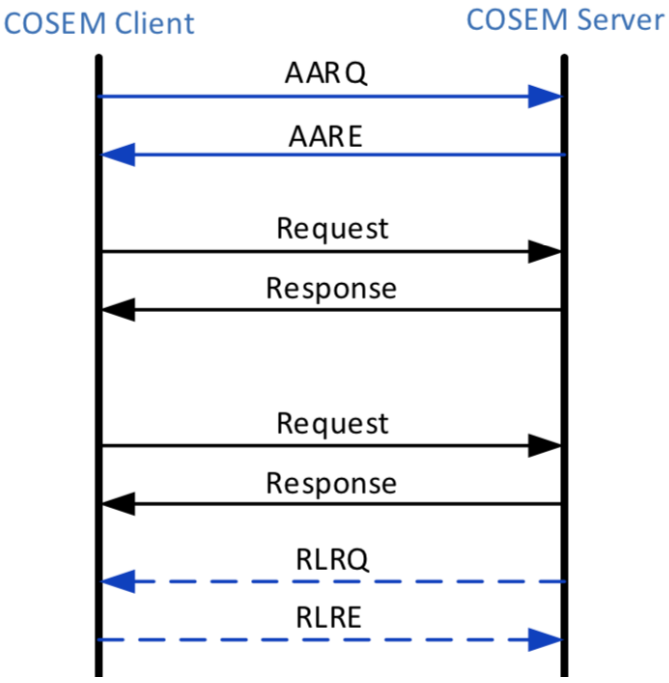

Figura 4.2: Flujo de comunicación entre cliente y servidor [32]

4.5. Perfiles de comunicación

El protocolo DLMS/COSEM permite la comunicación tanto sobre redes TCP-UDP/IP como HDLC. En el caso de las redes TCP-UDP/IP, los servicios de COSEM son soportados por la capa de transporte COSEM, que consiste en un wrapper sobre el protocolo TCP o UDP que agrega un header de 8 bytes antes del mensaje, indicando la versión del protocolo utilizada, los puertos de origen y destino, y el largo del mensaje enviado. De esta forma, se asegura que se reciba todo el mensaje antes de ser procesado. [32]

4.6. Uso de criptografía

Cada dispositivo cuenta con tres claves [33]:

- *Clave maestra*
  Se trata de una clave AES, programada en el firmware del medidor al momento de fabricación. Es requerida para cambiar el método de cifrado y las claves de cifrado y autenticación.
- *Clave de cifrado*
  Clave de 128 o 256 bits, utilizada para el cifrado de los mensajes DLMS/COSEM.
- *Clave de autenticación*
  Es una clave del mismo largo que la clave de cifrado. Se utiliza para calcular el tag de autenticación de los mensajes enviados, este tag de autenticación sirve como prueba de la integridad del mensaje y demuestra el conocimiento de la clave de autenticación por parte del emisor del mensaje.

Hay tres modos de comunicación posible: en texto plano, es decir, sin cifrar, cifrada utilizando la clave de cifrado global o cifrada utilizando una clave dedicada para la sesión en curso. [33]

Para el cifrado de los mensajes el protocolo utiliza el modo de cifrado en bloque Galois Counter Mode (GCM) y AES-128. Cada bloque del keystream se calcula usando AES-128 en base a la clave de AES de 128 bits, un vector de inicialización (IV) único y el contador de bloque, el cual se expresa como un entero sin signo de 32 bits que comienza con el valor 1. Es muy importante que el IV sea único,

ya que repetir el keystream puede tener consecuencias graves, comprometiendo la confidencialidad de la comunicación. El IV en teoría puede ser de cualquier largo, pero IVs de largo menor a 96 bits se consideran inseguros. DLMS/COSEM sigue esta recomendación y utiliza como IV la concatenación del AP Title, valor que identifica a cada dispositivo y es intercambiado durante el establecimiento de la conexión, de 64 bits, seguido del frame counter, de 32 bits. [33]

Sea Kn el bloque n del keystream, tenemos que Kn = EncryptAES(IV | Contador). El primer bloque se reserva para cifrar el tag de autenticación y el resto de los bloques para el payload. Si el número de bytes en el payload a cifrar no es divisible por el tamaño del bloque, que en este caso es 128 bits, entonces se agregan bits de padding al último bloque del mismo. [33]

En las figura 4.3 y 4.4 se puede observar un diagrama del funcionamiento del algoritmo de cifrado y descifrado, respectivamente.

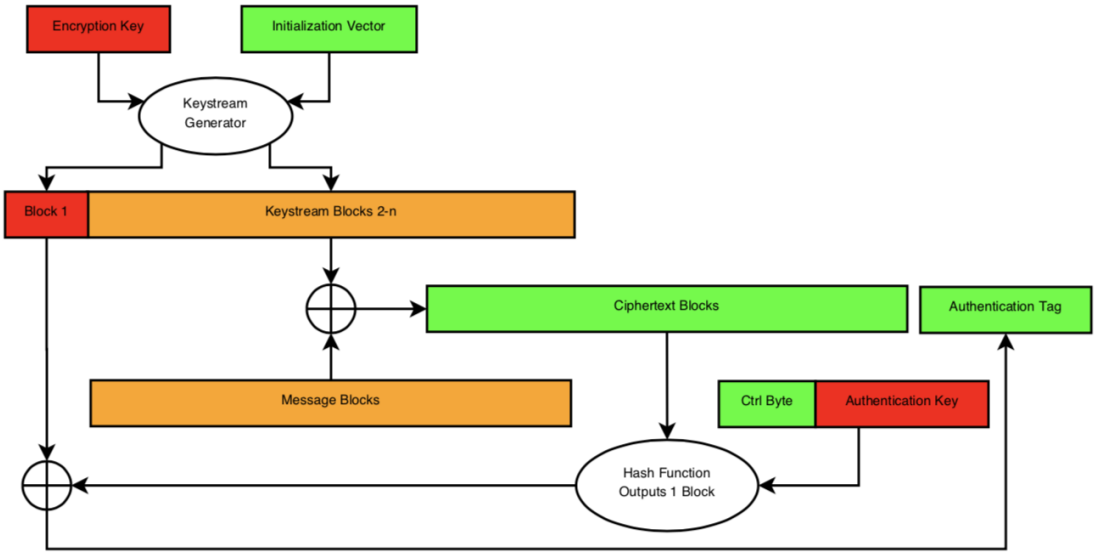

Figura 4.3: Algoritmo de cifrado [32]

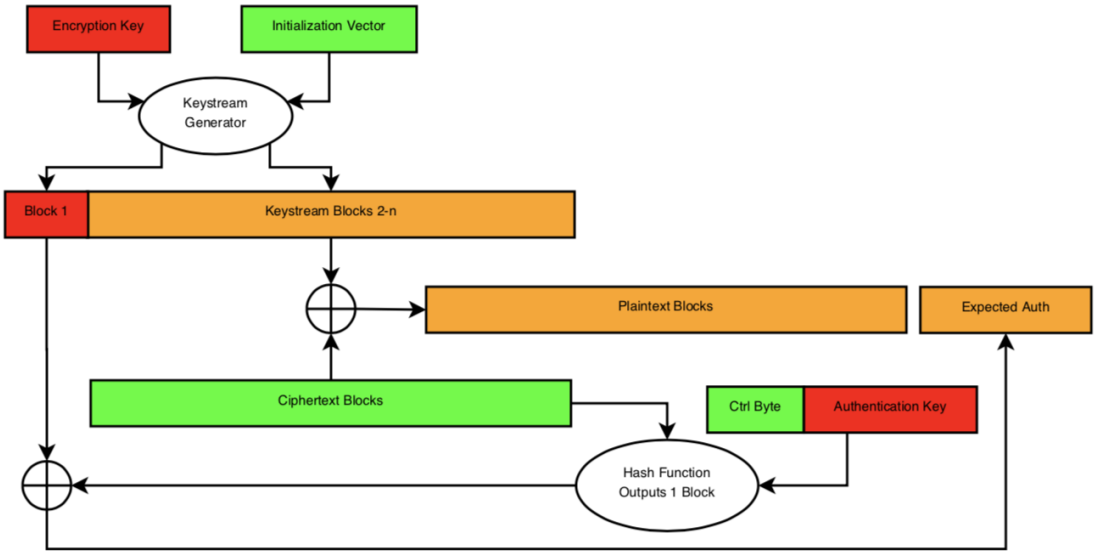

Figura 4.4: Algoritmo de descifrado [32]

4.7. Vulnerabilidades

El protocolo DLMS/COSEM no está libre de vulnerabilidades, tanto del protocolo en sí como particulares a sus diferentes implementaciones. A continuación mostraremos algunas de las vulnerabilidades conocidas estudiadas en [33].

4.8. Vulnerabilidades del protocolo

- *Autenticación opcional*
  El uso de autenticación es opcional según la definición del protocolo, y el mismo es independiente del cifrado de los mensajes. Un atacante puede manipular el byte de seguridad de los mensajes y truncar el mensaje de modo de eliminar el byte de autenticación, y así mantener una comunicación sin autenticación, sin que el receptor pueda saber si esta era la intención original del emisor.

- *Filtrado de información*
  Como vimos, cada mensaje contiene un header indicando el tipo de mensaje y modo de comunicación utilizado. Esto es innecesario, ya que se revela el tipo de mensaje incluso al tratarse de una comunicación cifrada, haciendo posible que atacantes sepan qué información se está transmitiendo. Esto podría ser sustituido simplemente indicando si se trata de comunicación cifrada utilizando

la clave global o una clave dedicada y el tipo de mensaje indicado cifrado con el resto del mensaje. Los dispositivos no requieren esta información adicional para poder descifrar el mensaje.

- *Métodos de autenticación vulnerables*
  En HLS, el método que se utiliza para autenticar al cliente y al servidor es el mismo. Dadas las circunstancias adecuadas, un atacante podría impersonar a un servidor válido mediante un ataque de replay del AP Title, nonce y la respuesta al desafío de autenticación. Además, ataque de diccionario offline son posibles, dado que se conoce el nonce (enviado en texto plano), la respuesta al desafío y la función de autenticación. Con esta información, dado suficiente tiempo y recursos, la clave utilizada puede ser calculada.

- *Posibilidad de inyección de respuestas al cliente*
  Las respuestas no están ligadas a las requests, es decir, dado una request enviada por el cliente las respuestas pueden ser reemplazadas por otro mensaje y, siempre y cuando contenga el tipo de datos esperado, será tomado como una respuesta válida.

4.9. Vulnerabilidades de implementación

A continuación se listan algunas vulnerabilidades que pueden estar presentes en implementaciones particulares del protocolo [33]:

- *Incumplimiento del uso del frame counter*
  El servidor acepta mensajes cuyo frame counter sea menor o igual al contador del último mensaje cifrado recibido de un dispositivo. Esto resulta en una falta de protección adecuada ante ataques de replay.

- *Uso de nonces predecibles*
  Si se utilizan nonces predecibles un atacante podría calcular las respuestas HLS necesarias para lograr autenticarse con el servidor o cliente.

- *Se permiten AP Titles idénticos*
  Si se permiten comunicaciones entre dos dispositivos con el mismo AP title, un cliente o servidor puede permitir la comunicación con un dispositivo DLMS /COSEM con su mismo AP title. Esto podría permitir ataques de replay.

- *Se permiten mensajes cifrados sin autenticación*
  Los mensajes cifrados sin autenticación son susceptibles a manipulación, por

lo que es deseable que no sean procesados.

- *Se permiten métodos de autenticación inseguros*
  LLS no debería ser utilizado ya que la password se envía en texto plano. Además, métodos de autenticación propietarios, y las versiones MD5 y SHA1 de HLS son vulnerables a ataques man-in-the-middle.

- *Los mensajes son procesados únicamente en base al header que indica el tipo de mensaje, sin verificar el contenido de los mismos*
  Si se procesan mensajes solo teniendo en cuenta el header indicando el tipo de mensaje, un atacante podría enviar un mensaje cuyo tipo indique que se trata de un mensaje cifrado, pero con los bits de cifrado y autenticación desactivados en el byte de seguridad, potencialmente engañando al servidor para que procese un mensaje malicioso enviado en texto plano.

- *Se envían mensajes AARE cifrados en respuesta a AARQ en texto plano*
  Esto puede permitir utilizar esta información para obtener el keystream, ya que los valores de los mensajes AARE son conocidos en base al AARQ enviado.

- *Posibilidad de ataques de diccionario online*
  Se permiten múltiples intentos de autenticación, permitiendo ataques de diccionario online. Luego de N intentos de conexión, los mensajes de error deberían ser los mismos.

- *Se permiten mensajes con un tag de autenticación inválido*
  Si se procesan mensajes sin controlar el tag de autenticación los mensajes son vulnerables a violaciones de integridad.

- *Se permiten AP Titles arbitrarios*
  Si se permiten conexiones desde cualquier cliente, en lugar de permitir conexiones solamente de clientes con ciertos AP Titles esperados, un atacante podría llevar a cabo un ataque de Denial of Service (DoS), iniciando conexiones desde una cantidad suficiente de clientes.

Referencias bibliográficas

[1] Alessandro Bassi, Martin Bauer, Martin Fiedler, Thorsten Kramp, and Rob Kranenburg. Enabling things to talk: designing IoT solutions with the IoT architectural reference model. Springer, 2013.

[2] European Union Agency for Network and Information Security (ENISA). Baseline security recommendations for iot in the context of critical information infrastructures. Technical report, ENISA, Dec 2017.

[3] ISO/IEC JTC 1. Internet of things (iot) preliminary report 2014. Technical report, ISO/IEC JTC 1, 2014.

[4] George Corser. Internet of things (iot) security best practices. Technical report, Institute of Electrical and Electronics Engineers (IEEE), Feb 2017.

[5] International Telecommunication Union (ITU). Global information infrastructure, internet protocol aspects and next-generation networks: Overview of the internet of things. Technical report, International Telecommunication Union (ITU), June 2012.

[6] Stamatis Karnouskos Stephan Haller and Christoph Schroth. The internet of things in an enterprise context. In Future Internet – FIS 2008 Lecture Notes in Computer Science, volume 5468, pages 14–28. Springer, 2009.

[7] Ericsson. Ericsson mobility report june 2019. Technical report, Ericsson, June 2019.

[8] International Electrotechnical Commission (IEC). IoT 2020: smart and secure IoT platform: white paper. International Electrotechnical Commission (IEC), 2016.

[9] Zozo Hassan, Hesham Ali, and Mahmoud Badawy. Internet of things (iot): Definitions, challenges, and recent research directions. International Journal of Computer Applications, 128:975–8887, Oct 2015.

[10] Se-Ra Oh and Young-Gab Kim. Security requirements analysis for the iot. In 2017 International Conference on Platform Technology and Service (PlatCon), Feb 2017.

[11] Cloud Standards Customer Council. Cloud Customer Architecture for IoT. Cloud Standards Customer Council, 2016.

[12] Ravi C Bhaddurgatte and Vijaya Kumar BP. A review: Qos architecture and implementations in iot environment. In Trends in engineering and technological development: Some recent advances. Nov 2015.

[13] Giacomo Tanganelli, Carlo Vallati, and Enzo Mingozzi. Ensuring quality of service in the internet of things. In Studies in Computational Intelligence, pages 139–163. June 2018.

[14] Industrial Internet Consortium. Industrial internet of things volume g4: Security framework. Technical report, Sep 2016.

[15] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76:146 – 164, 2015.

[16] European Union Agency for Network and Information Security (ENISA). Enisa threat landscape report 2016. Technical report, ENISA, Jan 2017.

[17] Unai Castro Legarza and Eloy Álvarez Pelegry. Redes de distribución eléctrica del futuro: Un análisis para su desarrollo. In Cuadernos Orkestra. Nov 2013.

[18] European Regulators' Group for Electricity and Gas (ERGEG). Position paper on smart grids. an ergeg public consultation paper. Technical report, ERGEG, Dec 2009.

[19] Florian Skopik and Paul Smith. Smart grid security innovative solutions for a modernized grid. Elsevier, 2015.

[20] National Institute of Standards and Technolgy (NIST). Framework and roadmap for smart grid interoperability standards, release 1.0. Technical report, NIST, 2009.

[21] Massachusetts Institute of Technology (MIT). The future of the electric grid. an interdisciplinary mit study. Technical report, MIT, 2011.

[22] Electric Power Research Institut (EPRI). Estimating the costs and benefits of the smart grids. a preliminary estimate of the investment requirements and the resulting benefits of a fully functioning smart grid. (technical report no. 1022519). Technical report, EPRI, 2011.

[23] Smart Grids European Technology Platform. Strategic deployment document for europe‘s electricity networks of the future. Technical report, SGETP, 2010.

[24] EU Commission Task Force for Smart Grids. Functionalities of smart grids and smart meters. Technical report, EU Commission Task Force for Smart Grids, 2010.

[25] Smart Grid Coordination Group. Cencenelecetsi. reports in response to smart grid mandate m/490. Technical report, Smart Grid Coordination Group, 2014.

[26] Z. Popovic and V. Cackovic. Advanced metering infrastructure in the context of smart grids. Technical report, IEEE International Energy Conference (ENERGYCON), 2014.

[27] Christoph Ruland Obaid Ur-Rehman, Natasa Zivic. Security issues in smart metering systems. Technical report, Aug 2015.

[28] Mariagrazia Fugini Gerardo Pelosi Alessandro Barenghi, Luca Breveglieri. Computer Security Anchors in Smart Grids: The Smart Metering Scenario and Challenges. Springer, 2015.

[29] Kevin Fu Emmanuel Cecchet David Irwin Andrés Molina-Markham, Prashant Shenoy. Private memoirs of a smart meter. Technical report, 2010.

[30] ENISA. Smart grid threat landscape and good practice guide. Technical report, ENISA, 2013.

[31] NESCOR Technical Working Group 1. lectric sector failure scenarios and impact analyses. Technical report, NESCOR, 2013.

[32] Petr Matousek. Analysis of dlsm protocol. Technical report, Brno University of Technology, 2018.

[33] Loren Weith. Dlms / cosem protocol security evaluation. Thesis, Eindhoven University of Technology, March 2014.

APÉNDICES

Apéndice 1

A continuación se muestran ejemplos de la estructura de algunos mensajes DLMS/COSEM. En las siguientes figuras se podrá observar los campos que componen los mensajes, indicando cuáles son opcionales.

```
AARQ-apdu ::= [APPLICATION 0] IMPLICIT SEQUENCE {          --- APPLICATION 0 = 60H = 96
        protocol-version              [0]     IMPLICIT BITSTRING {version 1(0)} DEFAULT {version 1},
        application-context-name      [1]     Application-context-name,
        called-AP-title               [2]     AP-title OPTIONAL,
        called-AE-qualifier           [3]     AE-qualifier OPTIONAL,
        called-AP-invocation-id       [4]     AP-invocation-identifier OPTIONAL,
        called-AE-invocation-ide      [5]     AE-invocation-identifier OPTIONAL,
        calling-AP-title              [6]     AP-title OPTIONAL,
        calling-AE-quantifier         [7]     AE-qualifier OPTIONAL,
        calling-AP-invocation-id      [8]     AP-invocation-identifier OPTIONAL,
        calling-AE-invocation-id      [9]     AE-invocation-identifier OPTIONAL,
        sender-acse-requirements      [10]    IMPLICIT ACSE-requirements OPTIONAL,
        mechanism-name                [11]    IMPLICIT Mechanism-name OPTIONAL,
        calling-authentication-value  [12]    EXPLICIT Authentication-value OPTIONAL,
        implementation-information    [29]    IMPLICIT  Implementation-data OPTIONAL,
        user-information              [30]    IMPLICIT  Association-information OPTIONAL
}
```

Figura 1.1: Estructura mensaje AARQ [32]

```
AARE-apdu ::= [APPLICATION 1] IMPLICIT SEQUENCE {          --- APPLICATION 1 = 61H = 97
        protocol-version                [0]     IMPLICIT BIT STRING {version 1(0)} DEFAULT {version1},
        application-context-name        [1]     Application-context-name,
        result                          [2]     Association-result,
        result-source-diagnostic        [3]     Associate-source-diagnostic,
        responding-AP-title             [4]     AP-title OPTIONAL,
        responding-AE-qualifier         [5]     AE-qualifier OPTIONAL,
        responding-AP-invocation-id     [6]     AP-invocation-identifier OPTIONAL,
        responding-AE-invocation-id     [7]     AE-invocation-identifier OPTIONAL,
        responder-acse-requirements     [8]     IMPLICIT ACSE-requirement OPTIONAL,
        mechanism-name                  [9]     IMPLICIT Mechanism-name OPTIONAL,
        responding-authentication-value [10]    EXPLICIT Authentication-value OPTIONAL,
        application-context-name-list   [11]    IMPLICIT Application-context-name-list OPTIONAL,
        implementation-information      [29]    IMPLICIT Implementation-data OPTIONAL,
        user-information                [30]    IMPLICIT Association-information OPTIONAL
}
```

Figura 1.2: Estructura mensaje AARE [32]

```
RLRQ-apdu ::= [APPLICATION 2] IMPLICIT SEQUENCE {   --- APPLICATION 2 = 62H = 98
        reason                  [0]     IMPLICIT Release-request-reason OPTIONAL,
        aso-qualifier           [13]    ASO-qualifier OPTIONAL,
        asoi-identifier         [14]    IMPLICIT ASOI-identifier OPTIONAL,
        user-information        [30]    IMPLICIT Association-information OPTIONAL
}
```

Figura 1.3: Estructura mensaje RLRQ [32]

```
RLRE-apdu ::= [APPLICATION 3] IMPLICIT SEQUENCE {   --- APPLICATION 3 = 63H = 99
        reason                  [0]     IMPLICIT Release=response-reason OPTIONAL,
        aso-qualifier           [13]    ASO-qualifier OPTIONAL,
        asoi-identifier         [14]    IMPLICIT ASOI-identifier OPTIONAL,
        user-information        [30]    IMPLICIT Association-information OPTIONAL
}
```

Figura 1.4: Estructura mensaje RLRE [32]