UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

PROYECTO FIN DE CARRERA

Análisis de las normas de seguridad para los controles, las comunicaciones y otros equipos críticos de la red de energía

Fernando García Gutiérrez

MAYO 2014

Análisis de las normas de seguridad para los controles, las comunicaciones y otros equipos críticos de la red de energía

AUTOR: Fernando García Gutiérrez

TUTOR: Jorge Enrique López De Vergara Méndez

Ingeniería de Telecomunicación

Dpto. de Tecnología Electrónica y de las Comunicaciones

Escuela Politécnica Superior

Universidad Autónoma de Madrid

Mayo de 2014

Preámbulo

Hace tiempo escuché una frase que me llamó la atención y que posteriormente pude comprobar que era de Baltasar Gracián[1], escritor y filósofo español del siglo XVII, y que exponía lo siguiente: "*La libertad consiste en poder hacer lo que se debe hacer*"[2].

Si bien, aun considerándome haber podido ser libre durante toda mi vida, y más si tengo en cuenta esta definición, han existido momentos a lo largo de la misma en los que no he sabido aprovechar y disfrutar de esta libertad. Por fin, y gracias a ciertas personas que existen dentro de mi entorno, he llevado a cabo el esfuerzo necesario para materializar este trabajo, hecho que me permite cerrar un ciclo de estudios que ha permanecido abierto durante más tiempo del esperado. Esto es algo que debía hacer.

[1] http://www.biografiasyvidas.com/biografia/g/gracian.htm

[2] http://es.wikiquote.org/wiki/Baltasar_Graci%C3%A1n

Agradecimientos

En primer lugar, quiero dar las gracias a Jorge, tutor de este Proyecto Fin de Carrera, por el tiempo dedicado durante el mismo. La atención mostrada por él a lo largo de todo el proceso, con tutorías y atención personalizada, con la aportación que han significado sus opiniones, y las pautas que ha marcado a lo largo de este último año han sido fundamentales para aterrizar conceptos, encontrar soluciones y poder materializar gran parte del contenido aquí expuesto.

De manera especial, a Marta quiero agradecer de todo corazón el tiempo pasado junto a mí y dedicarle los resultados del esfuerzo realizado durante el último año. Ella ha sido la persona que me ha aportado la ilusión y el ánimo por trabajar duro en los momentos necesarios y quien me ha inspirado en las situaciones más difíciles.

Quiero también agradecer a familiares y amigos el haber estado apoyándome durante toda mi vida y en particular los últimos años. Mi madre Conchi y mi hermana Ana han sido los pilares en los que sustentarme y las responsables a las que agradecer el ser quien soy, esa persona que ha podido completar este trabajo. De manera directa o indirecta me han aportado también Pedro, Arri, Dani, Juanjo, Rafa, Ángel, Arenas, primo José, primo Dani y muchos otros, que ya sea por una sonrisa en momentos malos o por ayuda en situaciones particulares, me han enseñado a cómo afrontar la dureza de la vida y a mirar para atrás y hacia adelante con el fin de que con perspectiva pudiera sacar lo mejor de mí en las distintas facetas de la vida.

No puedo olvidarme de los compañeros de la carrera y sobre todo del trabajo. Andrés, Fer Alonso, Juanma, Ismael, Iwan, Toni, Abe, David y todos los demás, que con vuestros ánimos, ayuda y consejos he podido avanzar en el trabajo cumplido.

A todos, y también a todos aquellos que sin estar aquí mentados habéis aportado granos de arena en la montaña de mi vida, **GRACIAS**.

INDICE DE CONTENIDOS

1 Introducción **7**

1.1 Motivación y justificación del trabajo realizado *7*

1.2 Objetivos *11*

1.3 Fases de realización *12*

1.4 Organización de la memoria *14*

2 Sistemas de control y comunicación en la infraestructura eléctrica **17**

2.1 La infraestructura eléctrica *18*

2.2 Sistemas de información y comunicación para controlar la infraestructura eléctrica *20*

2.3 Red de comunicaciones de la infraestructura eléctrica *21*

2.3.1 Ejemplo de red de comunicaciones en el sistema eléctrico: Red Eléctrica de España 25

2.4 Sistemas SCADA en el sector eléctrico: estado del arte *25*

2.4.1 Ejemplo SCADA: centro de control de Red Eléctrica de España 28

2.5 Líneas de trabajo existentes en el ámbito de la seguridad cibernética *29*

2.6 Conclusiones *31*

3 Normativa europea y estándares de seguridad **33**

3.1 Directiva 2008/114/EC de infraestructuras críticas *33*

3.1.1 Estrategia de Seguridad Cibernética de la Unión Europea 35

3.2 Estándares de seguridad *37*

3.2.1 ISO 27002, 27032 y 27033 38

3.2.2 NIST 800-53 41

3.2.1 NERC CIP 43

3.2.1 ANSI/ISA 99 and IEC 62443 44

3.2.2 IEC 62351 - Datos y Seguridad de comunicación 46

3.3 Conclusiones *47*

4 Estandarización y regulación **49**

4.1 Estudios regulatorios análogos en Europa: Smart Grid Task Force (SGTF) *50*

4.2 Recomendaciones generales sobre regulación *52*

4.3 ENISA: European Network and Information Security Agency *54*

4.4 Conclusiones sobre la estandarización y regulación *55*

5 Introducción al caso de estudio: relación entre la normativa y los distintos agentes y selección de los parámetros a analizar **57**

5.1 Relación entre las normativas de seguridad y su aplicación en los centros de control y los sistemas de información y comunicación *58*
5.1.1 Operador de distribución eléctrica 61

5.2 Selección de los parámetros a estudiar en el caso de estudio *65*
5.2.1 Gestión de procesos con terceros 66
5.2.2 Seguridad específica de los sistemas de información 67
5.2.3 Seguridad de la infraestructura de red y tratamiento derivado de los datos 68
5.2.4 Auditoría de datos (tanto interna como externa) 69

5.3 Conclusiones *70*

6 Caso de estudio: aplicación de la normativa de seguridad en los centros de control del sistema eléctrico **71**

6.1 Definición de requerimientos técnicos *75*
6.1.1 Gestión de procesos de terceros 79
6.1.2 Seguridad específica de los sistemas de información 81
6.1.3 Seguridad de la infraestructura de red y tratamiento derivado de los datos 83
6.1.4 Auditoría de datos 85

6.2 Arquitectura de los sistemas de información, comunicación y otros equipos críticos de la red de energía para el caso planteado *87*
6.2.1 Arquitectura general 87
6.2.2 Equipos contadores 89
6.2.3 Concentradores de datos 90
6.2.4 Equipos centrales para el procesado de datos 93
6.2.5 Infraestructura de red de comunicaciones 95
6.2.6 Procedimientos de gestión (datos y mantenimiento) 99

6.3 Soluciones propuestas para cada medida de seguridad *101*
6.3.1 Gestión de procesos con terceros 101
6.3.2 Seguridad específica de los sistemas de información 104
6.3.3 Seguridad de la infraestructura de red y tratamiento derivado de los datos 106
6.3.4 Auditoría de datos 107

6.4 Conclusiones *109*

7 Conclusiones del proyecto y trabajo futuro **121**

7.1 Resumen del análisis realizado *121*

7.2 Conclusiones *121*

7.3 Propuestas de trabajo futuro *121*

8 Glosario de acrónimos **121**

9 Referencias bibliográficas **125**

Anexo A: Pliego de condiciones **131**

Entregables *131*

Condiciones de desarrollo – recursos *131*

Anexo B: Presupuesto **133**

Presupuesto de ejecución material. *133*

Desglose por tareas ejecutadas 133

Costes de la mano de obra 137

Coste de los recursos materiales 139

Coste total de los recursos 139

Gastos generales. *139*

Honorarios por la redacción y dirección del proyecto. *140*

Presupuesto total *140*

INDICE DE FIGURAS

FIGURA 1: ARTÍCULO PERIODÍSTICO SOBRE EL PIRATEO DE LOS PROTOCOLOS SEGUROS 7

FIGURA 2: ARTÍCULO PERIODÍSTICO SOBRE LA INSEGURIDAD DE LA UTILIZACIÓN DE LOS NUEVOS SISTEMAS DE MEDICIÓN DE CONSUMO ELÉCTRICO 8

FIGURA 3: DESIGNACIÓN DE INFRAESTRUCTURAS CRÍTICAS EUROPEAS A NIVEL DE SECTOR 9

FIGURA 4: EJEMPLO DE DEPENDENCIAS EN LA INFRAESTRUCTURA ELÉCTRICA. 10

FIGURA 5. DIAGRAMA DE SISTEMA ELÉCTRICO TIPO. 18

FIGURA 6. ESQUEMA DE UNA RED DE COMUNICACIONES PARA UN SCADA 23

FIGURA 7. EJEMPLO DE SCADA PARA EL CONTROL DE UNA PLANTA DE GENERACIÓN ELÉCTRICA. 27

FIGURA 8: EJEMPLO DE ARQUITECTURA SCADA COMERCIAL MONITOR PRO 27

FIGURA 9. CENTRO DE CONTROL DE RED ELÉCTRICA DE ESPAÑA 28

FIGURA 10: SMART GRID CONCEPTUAL MODEL 29

FIGURA 11: EVIDENCIAS Y COMUNICADOS EN RELACIÓN A LA PREOCUPACIÓN MOSTRADA EN EL ENTORNO DE LA CIBERSEGURIDAD 36

FIGURA 12: CAPTURA DE LA PÁGINA WEB DE SMAR GRIDS TASK FORCE 50

FIGURA 13: EJEMPLOS DE ENTIDADES CERTIFICADORAS 58

FIGURA 14: ENTIDADES QUE PARTICIPAN EN EL NEGOCIO Y LA OPERACIÓN DEL SISTEMA ELÉCTRICO 60

FIGURA 15: DISEÑO CONCEPTUAL DE LAS REDES DE DISTRIBUCIÓN MODERNAS. 62

FIGURA 16: FLUJOS DE INFORMACIÓN DE LAS EMPRESAS DE DISTRIBUCIÓN ELÉCTRICA. 64

FIGURA 17: CONTADOR ELECTROMECÁNICO CON SISTEMA FERAIS 72

FIGURA 18: ARQUITECTURA GENERAL DE LA SOLUCIÓN NECESARIA PARA LA IMPLANTACIÓN DE LOS EQUIPOS DE MEDIDA. 88

FIGURA 19: CONTADOR RESIDENCIAL PARA COMPAÑÍAS DE DISTRIBUCIÓN. 90

FIGURA 20: CONCENTRADOR DE DATOS. 91

FIGURA 21: ARQUITECTURAS POSIBLES PARA LA CONEXIÓN DEL CONCENTRADOR DE DATOS 92

FIGURA 22: ARQUITECTURA DE UN CENTRO DE OPERACIONES TOTALMENTE INTEGRADO DE UNA RED DE DISTRIBUCIÓN ELÉCTRICA 94

FIGURA 23: ARQUITECTURA DE LA INFRAESTRUCTURA DE COMUNICACIONES 96

FIGURA 24: MODELO DE REFERENCIA PARA EL CONTROL DE OFDM EN LA ESPECIFICACIÓN PRIME 97

FIGURA 25: MODELO DE ARQUITECTURA PROPIETARIA PARA SMART METERING DE LA INICIATIVA "METERS AND MORE" 98

FIGURA 26. DIAGRAMA DE GANTT DEL PROYECTO 136

FIGURA 27. BASES DE COTIZACIÓN RÉGIMEN GENERAL EJERCICIO 13 - ORDEN ESS/56/2013, DE 28/12 (BOE DEL 29) 138

INDICE DE TABLAS

TABLA 1: NORMAS DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS NERC CIP 43
TABLA 2: NORMAS DE SEGURIDAD PARA LA AUTOMATIZACIÓN INDUSTRIAL ISA 99 –IEC62443 45
TABLA 3: GESTIÓN DE PROCESOS CON TERCEROS 79
TABLA 4: SEGURIDAD ESPECÍFICA DE LOS SISTEMAS DE INFORMACIÓN 81
TABLA 5: SEGURIDAD DE LA INFRAESTRUCTURA DE RED Y TRATAMIENTO DERIVADO DE LOS DATOS 83
TABLA 6: AUDITORÍA DE DATOS 85
TABLA 7: TRAZABILIDAD DE LAS MEDIDAS DE SEGURIDAD SELECCIONADAS, SOLUCIONES Y ESTÁNDARES/NORMAS DE SEGURIDAD EXISTENTES 110
TABLA 8: COSTES SALARIALES DEL PROYECTO 138
TABLA 9: COSTES DE MATERIALES DEL PROYECTO 139
TABLA 10: COSTES PRESUPUESTO DE EJECUCIÓN MATERIAL 139
TABLA 11: COSTES PRESUPUESTO DE EJECUCIÓN POR CONTRATA 140
TABLA 12: PRESUPUESTO TOTAL 140

1 Introducción

1.1 Motivación y justificación del trabajo realizado

En la actualidad en el corazón de los sistemas eléctricos y otras infraestructuras como las instalaciones de petróleo y gas, las plantas de procesos químicos y los centros de gran maquinaria industrial se encuentran controlados por dispositivos electrónicos, ordenadores y sistemas de control interconectados a través de redes de comunicaciones en los que tantos los agentes del mercado, los clientes y los usuarios confían y dan por sentado un buen funcionamiento continuo.

Hoy en día, muchos de estos sistemas son vulnerables a los ataques cibernéticos que pueden inhibir su funcionamiento, dañar datos valiosos o exponer información privada. En el caso de la infraestructura eléctrica, estos ataques pueden afectar grandes extensiones del sistema eléctrico europeo y causar un impacto social enorme. **La exposición ante amenazas es creciente, y por lo tanto, la presión para garantizar la seguridad cibernética de los sistemas de control y comunicación es muy alta en todo el mundo.**

Esta exposición afecta a todos los niveles de seguridad. Una y otra vez, los estándares de seguridad en internet han quedado en evidencia, por ejemplo, después de que el pasado mes de junio se publicara que la Agencia Nacional de Inteligencia (NSA) de EEUU los corrompió para hacerlos vulnerables a su tecnología con el fin de facilitar el espionaje [1]. Estos tipos de fallos en la seguridad, provocan inseguridad en el uso de los sistemas de información y comunicación más modernos.

Figura 1: Artículo periodístico sobre el pirateo de los protocolos seguros
Fuente: www.elmundo.es

Así pues, por un lado, la actual necesidad de llevar a cabo la sustitución de todos los contadores de electricidad situados de los clientes localizados en su red de distribución, tal y como se estipula en el REAL DECRETO 1110/2007, de 24 de agosto, por el que se aprueba el Reglamento unificado de puntos de medida del sistema eléctrico [2] cumpliendo con lo dictado en la ORDEN ITC/3022/2007, de 10 de octubre, por la que se regula el control metrológico del Estado sobre los contadores de energía eléctrica [3][3], se ve reflejado tanto en un potencial problema de seguridad de suministro eléctrico como en un existente problema con la seguridad de los datos que se transmiten y manipulan a través de la infraestructura de información y comunicaciones desplegada para dar soporte a estos dispositivos.

Actualmente, antes y durante la realización de este proyecto, varios medios de comunicación se han hecho eco de los problemas que se plantean. Por ejemplo, recientemente ha sido publicada a través de un conocido medio de comunicación digital una noticia que dice lo siguiente: "*A través de los contadores eléctricos inteligentes se podrán, por tanto, identificar hábitos y datos privados de los miembros que componen una vivienda (la hora de acostarse, comer, marca de electrodomésticos que utilizan…)*"[4].

Figura 2: Artículo periodístico sobre la inseguridad de la utilización de los nuevos sistemas de medición de consumo eléctrico
Fuente: www.elconfidencialdigital.com

[3] La descripción más en detalle tanto del REAL DECRETO 1110/2007 [2], de 24 de agosto, como de la ORDEN ITC/3022/2007 [3], de 10 de octubre, por la que se regula el control metrológico del Estado sobre los contadores de energía eléctrica se realizará dentro del presente capítulo, en el apartado 6.1Definición de requerimientos técnicos.

Por otro lado, y a un nivel paneuropeo, sobre el sistema eléctrico europeo en su conjunto (y por inclusión en el español en particular), existe una condición para la adopción de las normas de la seguridad que han de aplicarse en muchas de las infraestructuras identificadas como críticas (entre las que se encuentra por supuesto los sistemas de control de las redes eléctricas): la Directiva 2008/114/CE [5].

A raíz de los primeros trabajos realizados por la Comisión Europea, se presentó el documento de trabajo sobre la revisión del Programa europeo de protección de infraestructuras críticas (PEPIC) [6]. En el alcance de este documento se concluyó que la Estrategia de Seguridad Interior de la UE pone de manifiesto que las *infraestructuras críticas debe ser mejor protegida de las posibles amenazas que se aprovechan de las nuevas tecnologías y que la UE debe seguir trabajando para designar a la infraestructuras crítica y poner en marcha los planes para proteger los activos incluidos como tales, ya que son esenciales para el funcionamiento de la sociedad y la economía.*

La importancia de las infraestructuras eléctricas a nivel internacional, se puede ver reflejada a través del hecho de que tras el trabajo desarrollado tras la aplicación de la Directiva 2008/114/CE en relación a la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, ha sido en el sector eléctrico donde más designaciones se han realizado, tal y como presenta la Figura 3.

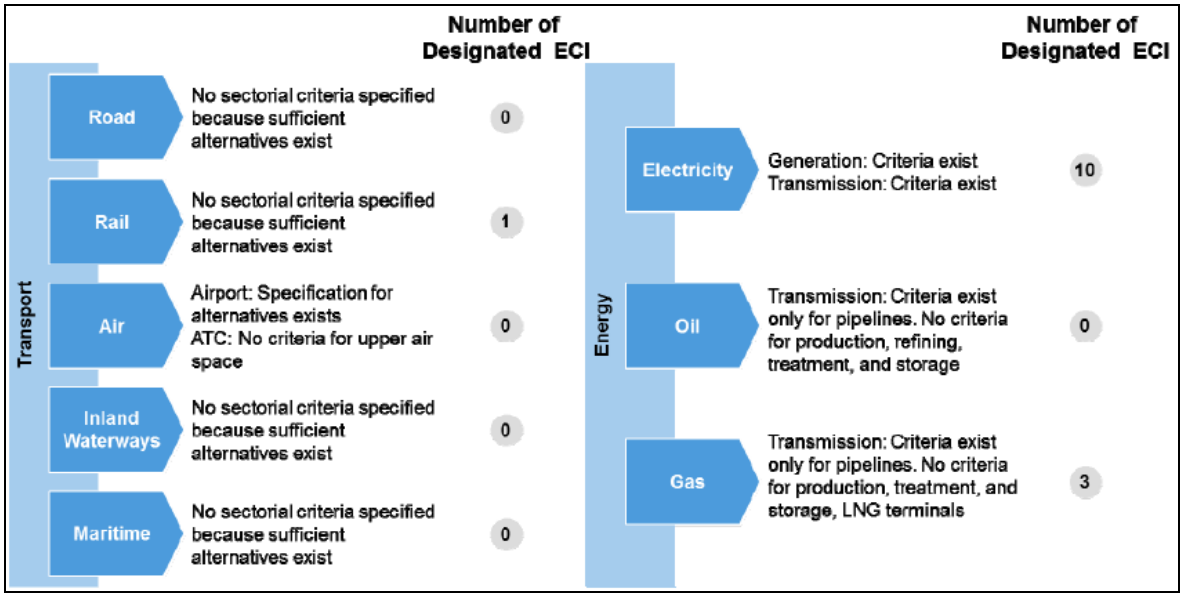

Figura 3: Designación de infraestructuras críticas europeas a nivel de sector
Fuente: Documento [6]

Como continuación de estos trabajos, y como señal de acierto en el trabajo seleccionado, el pasado 28 de agosto de 2013, la Comisión Europea publicó el documento de trabajo sobre el nuevo enfoque del Programa Europeo para la Protección de Infraestructuras Críticas [7]. En este documento, se propone un enfoque reformado CIP de la UE, basado en la aplicación práctica de las actividades realizadas dentro del marco de colaboración llamado “prevención, preparación y respuesta de trabajo”.

Dentro del nuevo enfoque se incluyen las interdependencias entre las infraestructuras críticas, la industria y los agentes reguladores. Las amenazas existentes a una infraestructura como la eléctrica puede tener un impacto muy significativo en otras infraestructuras y para su correcta gestión y desarrollo normativo debe involucrarse a agentes implicados en muy distintos niveles. Como ejemplo de la complejidad, este mismo informe ilustra (Figura 4) relaciones entre el sistema eléctrico y otros sectores que se encuentran afectados por el mismo.

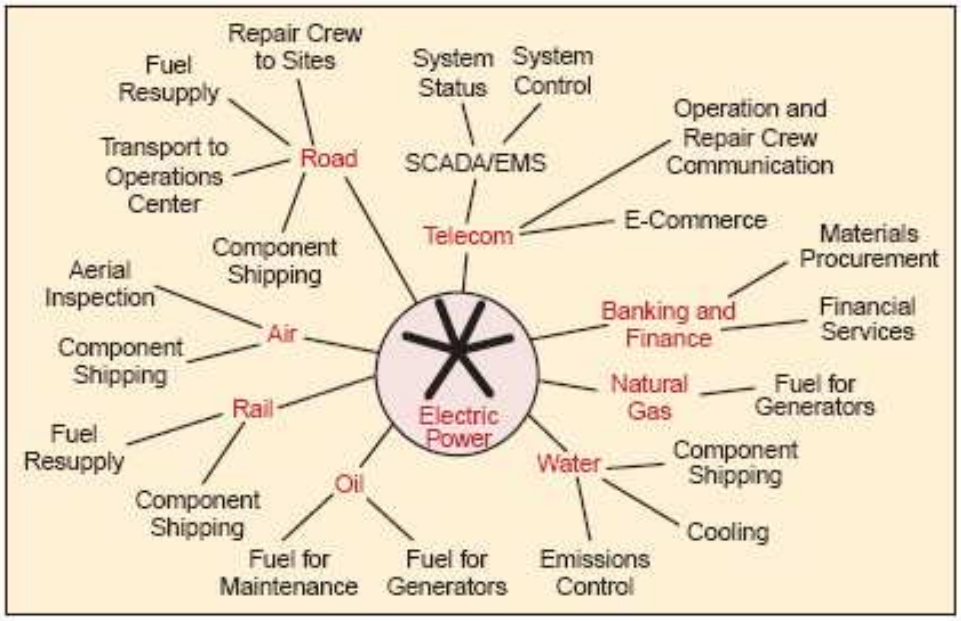

Figura 4: Ejemplo de dependencias en la infraestructura eléctrica
Fuente: Documento[7]

Como consecuencia de lo arriba explicado, si bien, las redes de distribución eléctrica no son el foco de los trabajos desarrollados en cuanto a infraestructuras críticas, el hecho de la importancia que tiene la infraestructura eléctrica en su conjunto, hace plantearse el presente trabajo como uno de los pasos a dar para poder garantizar la seguridad de su funcionamiento.

La inquietud principal que lleva asociada la realización del proyecto que se presenta se debe a la existencia de la necesidad de establecer una estructura organizativa de la seguridad y su aplicación (implementación de una serie de normas de seguridad) en marcos como el de la seguridad cibernética.

Esta estructura permitiría establecer unos niveles más robustos de resistencia ante las carencias que pueden aparecer en el despliegue de la infraestructura de sistemas de información y comunicación asociados a una nueva necesidad que se está implementando en estos momentos.

1.2 Objetivos

El proyecto se centra en la elaboración de un informe sobre la normalización de los requerimientos que tiene que haber para garantizar unos niveles de seguridad 'aceptables' dentro de los sistemas de información y centros de control que gobiernan y dan soporte a la infraestructura eléctrica.

Partiendo de la Directiva 2008/114/CE de infraestructuras críticas y otras normas tales como la ISA99[4], las NERC[5] y/o ISO[6] y/o NIST[7] que son de aplicación, el enfoque del proyecto trata de establecer un análisis regulatorio de las mismas.

Además, en fases posteriores se profundizará en los requerimientos técnicos que implican las distintas normativas dentro de un caso práctico: Caso de estudio: aplicación de la normativa de seguridad en los centros de control del sistema eléctrico, donde se podrá relacionar esta lista de "*requerimientos que tiene que haber para garantizar unos niveles de seguridad 'aceptables'*" con un en ejemplo posible en la actualidad: la implementación de los sistemas de información y comunicación asociados a la infraestructura de telegestión de contadores para una empresa de distribución de electricidad.

En este contexto, durante el texto ve reflejado cuáles son las líneas de trabajo existentes y cuáles deberían ser los requisitos que han de desarrollarse para la implantación de los nuevos estándares.

El objetivo del proyecto es identificar los beneficios de las distintas normas y estándares industriales desde un punto de vista objetivo, e identificar dónde estas normas y estándares pueden ser beneficiosos dentro de un caso de estudio particular. Los resultados finales del proyecto son:

- La elaboración de un documento que recoja cuáles son las necesidades industriales y los requisitos con respecto a la seguridad de los sistemas de control que tienen que realizarse.

---

[4] Comité para desarrollar y establecer normas, prácticas recomendadas, informes técnicos e información relacionada, que definirá las modalidades de los sistemas y mejores prácticas de la automatización industrial y control y evaluación de la seguridad electrónica.

[5] Entidad sin ánimo de entidad lucro cuya misión es asegurar la fiabilidad de la red eléctrica de transporte en Estados Unidos.

[6] Organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

[7] Agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.- http://www.nist.gov/

- La identificación de un elenco de vulnerabilidades del sistema eléctrico inducidos por los sistemas de control y comunicación que llevan asociados.

- La evaluación de los distintos marcos normativos que existen para garantizar la seguridad de los sistemas de control industrial.

- Y por último confeccionar una serie de recomendaciones para la adopción de uno o más de los marcos anteriores a la infraestructura de energía, con especial referencia al cumplimiento de la Directiva 2008/114/CE.

1.3 Fases de realización

Las seis fases de trabajo en las cuales se ha dividido el presente proyecto han sido:

1. Comprensión del problema

   Asimilación de los conceptos básicos del de los sistemas de control y comunicación que gobiernan la infraestructura eléctrica. Esto ha permitido elaborar un diagnóstico de las necesidades de caso, construirlo y trabajar para su solución.

2. Recolección de información

   Búsqueda en libros, artículos y otras publicaciones de la información necesaria a lo largo del proyecto. Ha sido necesario recopilar información acerca de:

   - cómo funcionan los sistemas de control y comunicación dentro de la infraestructura del sistema eléctrico,

   - cuáles son las normativas y estándares existentes acerca de la seguridad en los sistemas de control y comunicación,

   - qué tecnologías existen y están disponibles de manera factible para plantear soluciones factibles al problema planteado.

   Si bien la recopilación de información ha sido realizada de distintas maneras durante la totalidad del proyecto, esto se ha realizado de manera más activa durante la recogida de la información normativa necesaria para el análisis y durante la recogida de información sobre las distintas tecnologías que permitan diseñar la serie de soluciones a adoptarse.

3. Estudio y evaluación de la normativa existente

   Revisión de la documentación encontrada sobre la normativa europea acerca de seguridad de infraestructuras críticas y varios de los principales estándares de seguridad existentes.

   A su vez se realiza un análisis regulatorio en relación a la Directiva 2008/114/EC de infraestructuras críticas, ISA99, las NERC y/o ISO y/o NIST que apliquen, etc.

   Posteriormente se muestra una síntesis que permita reflejar una serie de prácticas a aplicar en materia de seguridad para los distintos entornos relacionados con el funcionamiento de la infraestructura eléctrica y que recomendaciones se realizan al respecto.

4. Definición del caso de estudio

   Para definir el caso de estudio se han tenido en cuenta la relación entre las normativas de seguridad y su aplicación en los centros de control y los sistemas de información y comunicación. Posteriormente se han seleccionado los parámetros a estudiar en el mismo.

5. Realización del análisis para la aplicación de la normativa de seguridad en el caso de estudio seleccionado

   Desarrollo del caso de estudio en el que se definirán los requerimientos técnicos y se diseñarán una serie de sistemas y procedimientos para una empresa de distribución de electricidad que le permitirán tener unas bases con las que cumplir con los parámetros seleccionados en la definición del caso y de esta manera poder llevar a cabo parte de sus procesos de negocio de una manera segura de acuerdo a la aplicación de la normativa existente.

6. Elaboración de conclusiones y escritura de la memoria

   Se han extraído las conclusiones obtenidas como resultado del proyecto y planteamiento de posibles trabajos o estudios como consecuencia del presente proyecto y escrito la presente memoria.

1.4 Organización de la memoria

La memoria del presente proyecto queda estructurada en los siguientes nueve capítulos entre los que se encuentran siete para el análisis elaborado, un glosario de acrónimos y un resumen de referencias bibliográficas.

Además hay dos anexos: un pliego de condiciones y el presupuesto del proyecto. La descripción específica del contenido de cada uno de los apartados de la presente memoria se describe a continuación:

- Capítulo 1: Introducción

  Sección inicial en la que se contextualiza el proyecto y que presenta la motivación, objetivos, fases del proyecto y organigrama de la memoria. Dentro de los objetivos se reseñan las conclusiones del proyecto.

- Capítulo 2: Sistemas de control y comunicación en la infraestructura eléctrica

  Descripción de la infraestructura eléctrica, haciendo referencia a la problemática que existe en este sector sobre la necesidad de generar electricidad en el mismo momento de su consumo y las necesidades de ser soportada por unos complejos sistemas de control y comunicación.

- Capítulo 3: Normativa europea y estándares de seguridad

  Presentación de la normativa europea en materia de infraestructuras críticas y la estrategia de seguridad cibernética definida a nivel paneuropeo.

  También se hace un recorrido por los principales estándares en materia de seguridad para los sistemas de información y comunicación se recogen sus características.

- Capítulo 4: Estandarización y regulación

  Síntesis de varios estudios sobre cómo se están abordando estos temas en ámbitos de referencia internacional desde el punto de vista de la aplicación de distintos procesos de estandarización, que a su vez pueden desembocar en futuros marcos regulatorios.

- Capítulo 5: Introducción al caso de estudio: análisis de la normativa

  Descripción del caso de estudio que se ha elaborado, recogiendo las limitaciones y definiendo el marco de trabajo del análisis elaborado.

- Capítulo 6: Caso de estudio: aplicación de la normativa de seguridad en los centros de control del sistema eléctrico

  Desarrollo del caso de estudio presentado en el capítulo anterior en el que se hace una definición de los requerimientos técnicos de los sistemas y procedimientos a implementarse de manera teórica. Posteriormente se describen las soluciones propuestas para cada una de las medidas de seguridad escogidas en el marco de trabajo para el estudio.

- Capítulo 7: Conclusiones y trabajo futuro

  Recapitulación de las conclusiones obtenidas como resultado del proyecto y planteamiento de posibles trabajos o estudios como consecuencia del presente proyecto.

- Capítulo 8: Glosario de acrónimos

  Conjunto de acrónimos utilizados durante la memoria del proyecto junto con sus nombres completos.

- Capítulo 9: Referencias bibliográficas

  Catálogo de publicaciones que permiten la identificación del soporte de información para parte del contenido del presente proyecto.

- Anexo A: Pliego de condiciones

  Apartado en el que se establecen las condiciones bajo las cuales se ha ejecutado el presente proyecto y en el que se describen los entregables a realizar en el proyecto y las condiciones de desarrollo y recursos a utilizar.

- Anexo B: Presupuesto

  Valoración económica del esfuerzo empleado en la elaboración presente proyecto, se detalla el presupuesto del mismo.

Con el fin de poder establecer un claro hilo conductor a lo largo de todo el proyecto, cada uno de los seis capítulos de análisis (desde el dos hasta el siete) consta de una introducción que permite en primer lugar presentar el contenido del capítulo al lector y después poder enlazarlo con las distintas hipótesis propuestas, el estado del arte o la situación de negocio y con los tratado anteriormente.

Al final de cada uno de estos capítulos del dos al seis se presentan las conclusiones parciales de lo tratado en los mismos.

2 Sistemas de control y comunicación en la infraestructura eléctrica

Para entender la naturaleza y posibles problemas a los que se enfrenta la industria de la seguridad dentro de los sistemas eléctricos es necesario conocer una serie de fundamentos básicos.

En el presente capítulo se introduce brevemente y a grandes rasgos en qué consiste la infraestructura eléctrica, desde la generación de la misma hasta su consumo y se hace referencia específicamente a la problemática que existe en este sector sobre la necesidad de generar electricidad en el mismo momento de su consumo. Este concepto no se desarrolla en detalle.

A continuación se hace una descripción de alto nivel de los sistemas de información y comunicación que tiene asociada la infraestructura eléctrica que permiten su funcionamiento. Éstos son una red de comunicaciones que da soporte a los distintos procesos de negocio (generación, comercialización, etc.) y los sistemas SCADA, que permiten la monitorización y control de los distintos parámetros de funcionamiento del sistema.

Por último y como introducción a la seguridad dentro de las tecnologías de información y comunicación (TIC) dentro de la infraestructura eléctrica, se presentan las líneas de trabajo existentes dentro del ámbito de la seguridad cibernética para el sector energético. El lector encontrará la definición de red inteligente, por qué es importante la seguridad cibernética dentro de la misma y se revisarán las tendencias en Europa y en Estados Unidos en este aspecto.

2.1 La infraestructura eléctrica

Una red eléctrica es una infraestructura interconectada diseñada con el fin de entregar electricidad desde los puntos de producción (centrales de generación) de energía eléctrica hasta los puntos de consumo de la misma.

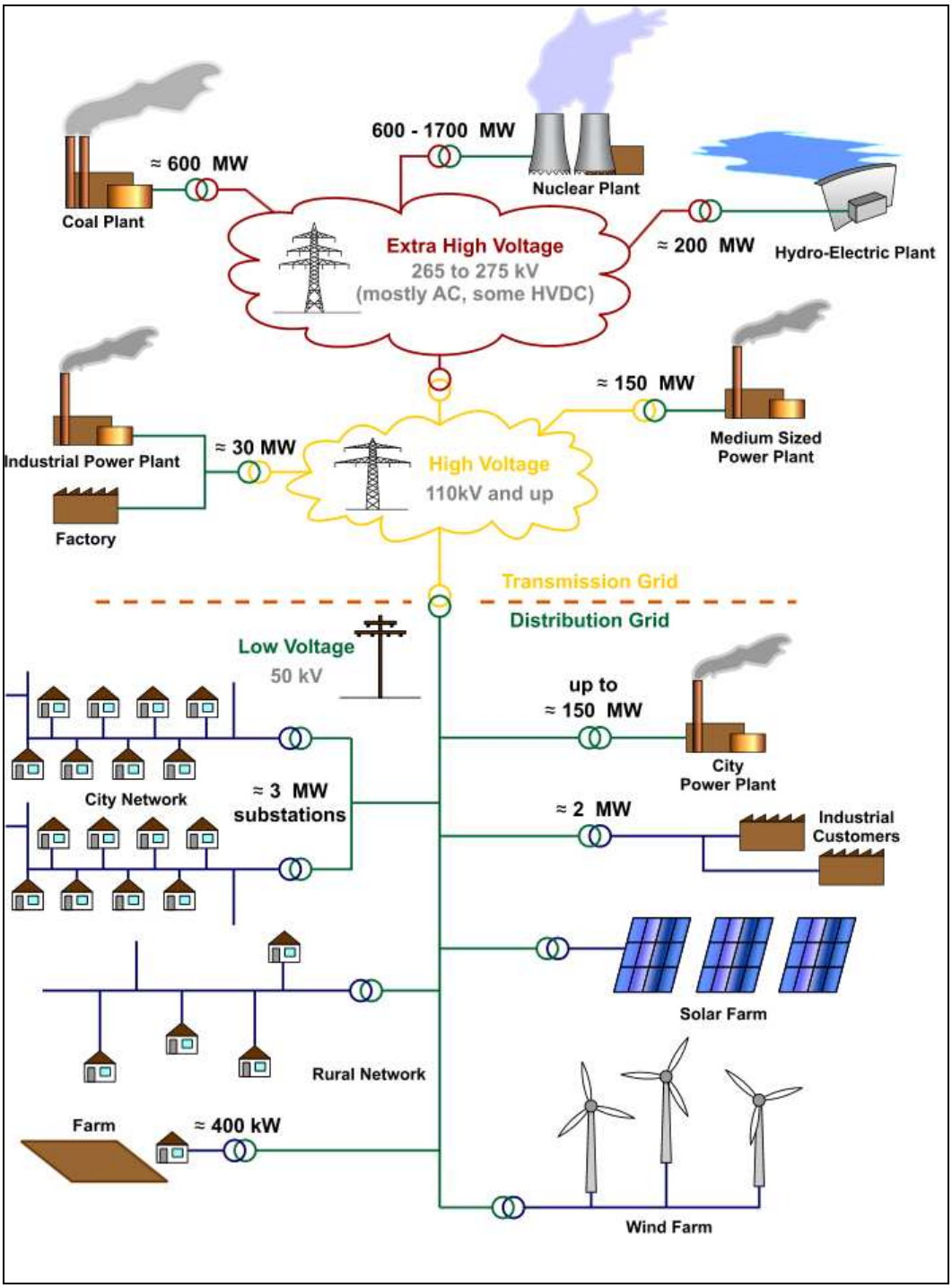

Figura 5. Diagrama de sistema eléctrico tipo

Fuente:

http://upload.wikimedia.org/wikipedia/commons/9/90/Electricity_Grid_Schematic_English.svg

El paradigma clásico, y más generalizado desde el comienzo de la electrificación de la sociedad, consiste en tener un sistema de centrales de generación que producen energía eléctrica, líneas de transmisión de alto voltaje que transportan la electricidad desde los puntos de generación hasta las áreas de consumo y líneas de distribución con niveles de tensión eléctrica menores que permiten entregar la energía a los consumidores finales.

Este esquema de funcionamiento no es cerrado puesto que existen consumidores conectados en la red de alta tensión para consumo de electricidad directamente en los puntos de la red transporte y cada vez más también hay centrales de generación de energía eléctrica distribuidas a lo largo de todo el sistema.

Tanto para el esquema clásico como para las nuevas topologías de infraestructura eléctrica son necesarias una serie de instalaciones (subestaciones de transformación donde se cambian los niveles de tensión de corriente eléctrica, centros de control,…) que permiten controlar y gestionar los flujos de energía eléctrica de la manera más eficiente posible.

Las centrales de generación suelen estar ubicadas cerca de las fuentes de energía o en localizaciones específicas para su adecuado tratamiento. Muchas de las plantas de generación son de grandes dimensiones para poder aprovechar ciertas economías de escala. Esta configuración de grandes centrales necesita de las ya mencionadas líneas de transporte para llevar la energía a los centros de consumo. Estos movimientos de energía se realizan incluso de manera transfronteriza.

En su llegada a las subestaciones, la energía se transforma a niveles de tensión inferiores para adaptar su flujo desde las líneas de transmisión a las líneas de distribución. Por último, para llevar la energía hasta los usuarios finales, la energía es entregada en los niveles de tensión y corriente requeridos por los usuarios finales.

Debido a las características físicas de la electricidad, ésta no es almacenable en su forma de onda electromagnética, y por lo tanto, ha de ser generada y consumida en el mismo tiempo, añadiendo un alto grado de complejidad al proceso explicado anteriormente de generación, trasmisión y distribución de la misma. Así pues, en un sistema eléctrico la generación y la demanda han de estar balanceadas cumpliendo una serie de restricciones técnicas dentro del sistema.

Un desajuste en el proceso de balanceo entre generación y consumo eléctrico provoca ineficiencias en el sistema e incluso situaciones críticas del mismo, como pueden ser cortes en el suministro del mismo.

Debido al grado de dependencia que existe en la actualidad (cadena de frío en alimentos y medicinas, hospitales, sistemas bancarios, etc.), es necesario garantizar el suministro eléctrico con un alto grado de fiabilidad.

Para que esto pueda ocurrir es necesario un completo control del sistema en cada una de sus etapas, y este control no puede ser llevado a cabo sin una serie de sistemas de información y comunicación asociados a la infraestructura eléctrica.

2.2 Sistemas de información y comunicación para controlar la infraestructura eléctrica

Las sucesivas revoluciones industriales han tenido su origen gracias a los hitos energéticos conseguidos por las sociedades modernas. Esto significa que las principales revoluciones pueden ser resumidas de la siguiente manera:

- Uso del carbón: 1ª revolución industrial
- Producción de electricidad: 2ª revolución industrial
- Dependiendo de los distintos sistemas energéticos: derivados del petróleo, energía nuclear, energías renovables: 3ª, 4ª y otras revoluciones industriales

Estas revoluciones han sido los principales catalizadores de muchos de los avances de la sociedad moderna: en tecnología, medicina, comunicación,… Sin embargo, han generado un problema derivado: la dependencia energética.

La sociedad en general necesita grandes cantidades de energía para dar soporte a las necesidades actuales existentes. Para soportar estos consumos eléctricos es necesario el despliegue de una robusta infraestructura energética que viene soportada entre otras por unos complejos sistemas de tecnologías de información y comunicación (TIC).

Los sistemas TIC permiten la comunicación entre los centros de control y los distintos elementos de la infraestructura eléctrica. La información sobre la red eléctrica debe estar disponible en tiempo real para los operadores y los distintos agentes que intervienen en el sistema (productores, comercializadores, clientes y autoridades) y esta información en tiempo real debe contener características técnicas y económicas de la electricidad.

Desde una perspectiva global, hay dos hechos de gran importancia para garantizar la seguridad del sistema eléctrico:

- La importancia de los sistemas TIC es fundamental para la monitorización y operación del sistema eléctrico.
- La mayoría de las instalaciones críticas de la infraestructura eléctrica están desatendidas y permiten un acceso físico a los sistemas TIC.

En los siguientes apartados se van a tratar ciertos aspectos de los sistemas TIC de la infraestructura eléctrica, incluyendo su funcionalidad.

Durante todo el proceso de funcionamiento de la infraestructura eléctrica, para una adecuada operación es inherentemente necesario que los sistemas de información y comunicación sean capaces de realizar con éxito las siguientes tareas:

- controlar el tráfico y detectar intrusiones y conductas erróneas de los componentes y el personal,

- elaborar una base registros fiables y coherentes a lo largo del tiempo,
- cifrar de manera adecuada en términos de seguridad y de manera periódica la información fundamental del sistema,
- gestionar la disponibilidad de los distintos elementos del sistema,
- priorizar los despachos y flujos de energía en función de criterios técnicos, económicos y regulatorios,
- gestionar una correcta configuración del sistema y el mantenimiento del mismo,
- ser capaces de tolerar unos umbrales de fallo,
- identificar y autenticar a los usuarios y los datos,
- eliminar / desactivar las interfaces y funcionalidades innecesarias y
- administrar la seguridad de terceros agentes (usuarios, proveedores, empresas de servicios externas,…)

2.3 Red de comunicaciones de la infraestructura eléctrica

Para de poder establecer un riguroso control de los distintos puntos de la infraestructura eléctrica, las compañías operadoras del sector tienen desplegada una red de comunicaciones que cubre un amplio área y que se utiliza para las siguientes funciones:

- Como red de red de operación y control (para nutrir de datos a los sistemas SCADA), tanto en la redes de transmisión de energía como en las de distribución (basada en protocolos como el IEC 61850[8]).
- El control de la comunicación entre los centros de control de transmisión y las principales instalaciones de su infraestructura (generación de energía, cargas controlables y centros de distribución de control).
- Comunicación directa con las subestaciones eléctricas de otros agentes del mercado.
- La comunicación entre los centros de control y los equipos de campo.
- La comunicación entre los centros de control y los retenes de personal que operan a distancia.

[8] La norma IEC 61850 describe la comunicación entre dispositivos dentro de las subestaciones[70]

- Comunicación para el seguimiento y mantenimiento del sistema de control y equipos de comunicación y su software.

Existen sistemas de control industrial y especialmente ciertas aplicaciones de éstos fundamentados en protocolos de comunicación contrastados y otros que se desarrollan en base a los nuevos avances tecnológicos, y en muchos casos esto provoca que las redes de comunicación asociadas a la infraestructura eléctrica tengan características heterogéneas entre sí y el enfoque de seguridad sea difícil de definir, no siendo sencillo hacer una descripción genérica sobre los mismos.

Como ya se ha explicado, la actividad de operación de la infraestructura eléctrica ha pasado de ser centralizada (que garantizaba las economías de escala y no requería de centros de control excesivamente sofisticados para su operación), a tener muchos puntos de generación distribuidos con el hecho de la entrada en funcionamiento de las plantas de producción de energía renovable, que necesitan de una gestión distinta por parte del operador, produciendo una nueva dinámica de los flujos de electricidad y una necesidad de equilibrios para garantizar el servicio eléctrico. Todo esto implica que las TIC se han convertido en un eslabón cada vez más crítico para la operación.

Esta operación no puede ser posible sin un control de red y una infraestructura de comunicación que preste unos servicios. El concepto de las denominadas redes inteligentes (Smart Grids)[9] comprende el aumento de la automatización y el control de las redes de distribución y las infraestructuras de comunicación que lo permitan.

Sin embargo, la arquitectura de las redes de comunicación para sistemas de automatización eléctricos que cumplan los requisitos de seguridad necesarios para su operación y gestión, depende muchas veces del tamaño del sistema y de la cantidad de tráfico de datos.

Estos datos y sus flujos de información están construidos de manera jerárquica, donde los niveles suelen estar separados por puertas de enlace, DMZ[10], o cortafuegos, como se muestra en la siguiente figura. En la parte inferior de esta estructura se ubican los equipos de campo, que están conectados a un bus de comunicaciones, y su consecuente control se realiza a través de redes de área local más o menos extensas (LAN o WAN).

[9] Red eléctrica con gestión eficiente la electricidad utilizando tecnologías de información y comunicación para optimizar la producción y la distribución de electricidad con el fin de equilibrar mejor la oferta y la demanda entre productores y consumidores.

[10] En seguridad informática, una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red que se ubica entre la red interna de una organización y una red externa, como por ejemplo Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de sus equipos.

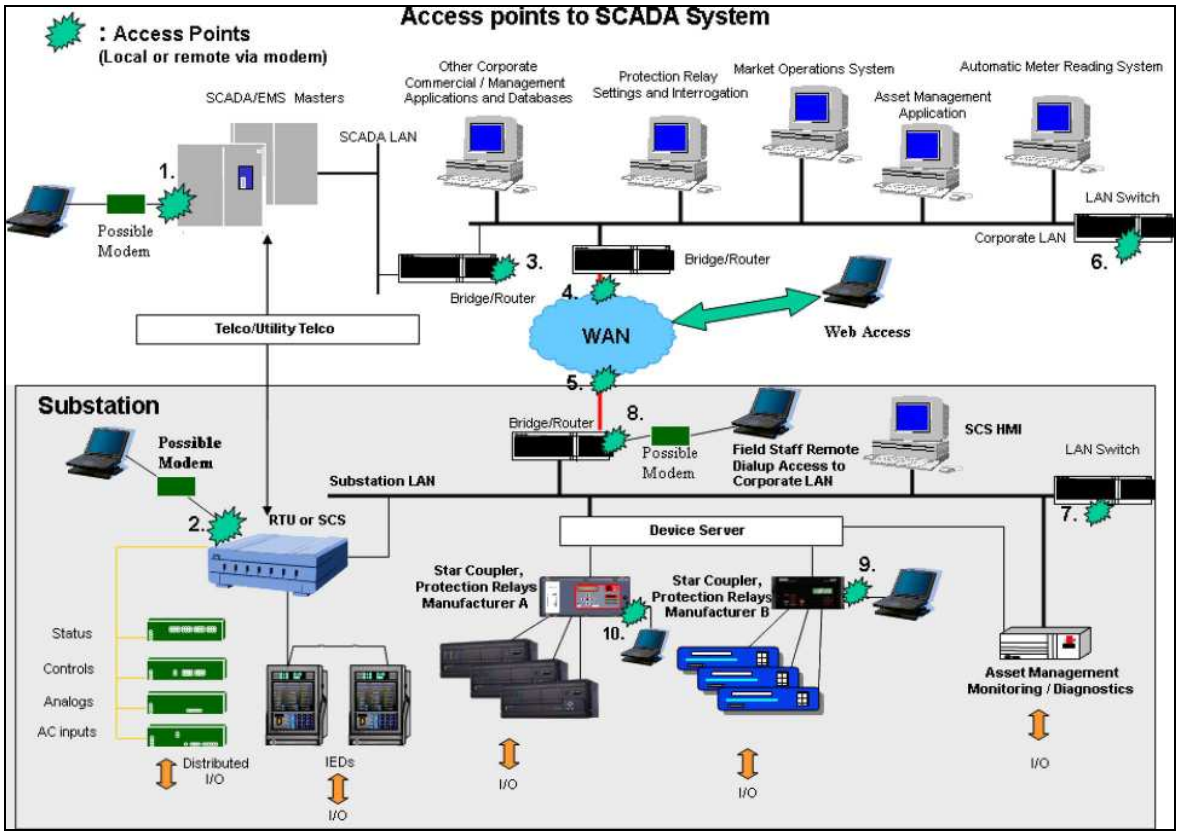

Figura 6. Esquema de una red de comunicaciones para un SCADA
Fuente: Documento [11]

En la infraestructura de redes eléctricas, los sistemas de comunicación asociados a la misma permiten que los controladores de campo se comuniquen con los otros componentes de campo como son sensores, impedancias, etc., a través de buses de comunicación.

Para llevar a cabo esta comunicación existe una la variedad de protocolos, a veces públicos y a veces con soluciones propietarias para casos específicos. Los protocolos se han optimizado para proporcionar un rápido acceso a un gran número de dispositivos, pero no ofrecen suficiente seguridad contra los ataques.

En la red europea, muchas de las comunicaciones se realizan a través de la norma IEC 60870-5-103 o a través de protocolos propietarios, pero cada vez más se implementan redes basadas en la norma IEC 61850, basado en MMS que se ejecutan a través de comunicaciones TCP / IP. IEC 61850-9-1 / 2 proporciona interoperabilidad entre equipos de diferentes fabricantes. La norma propone que las salidas cableadas a los diferentes dispositivos puedan ser digitalizadas en la fuente y luego comunicadas a aquellos dispositivos que utilizan Ethernet.

Por otro lado, algunos de los dispositivos de campo pueden utilizar la radio privada, o las redes públicas de telefonía móvil celular. Además, las subestaciones pueden dar acceso a la infraestructura de comunicaciones a los operarios de campo a través de ordenadores u otros dispositivos portátiles para realizar diagnósticos y operaciones de mantenimiento.

Las subestaciones eléctricas se conectan a través de redes de área local con los sistemas SCADA que se encuentran en los centros de control utilizando distintos protocolos de comunicación. En las redes de comunicación más antiguas se utilizan protocolos estándar tales como IEC 60870-5-102, IEC 60870-5-101/104, IEC 61334, IEC 60870-6-TASE.2 combinados con protocolos particulares desarrollado ad hoc para cada empresa operadora.

En las redes más modernas, los protocolos de comunicación con las subestaciones se tienden a sustituir por IEC 61850 que se basa en el envío de MMS (Manufacturing Message Specification), Especificación de Mensajes de Fabricación que sirven para el intercambio de datos estructurándose de manera reducida del modelo OSI con el protocolo TCP/IP en la capa de transporte/red. Algunas unidades remotas utilizan redes WAN y/o PLC[13] para conectarse directamente con los SCADA.

Como se acaba de mencionar, en muchos de los sistemas eléctricos se utilizan distintas redes de comunicaciones dependiendo de su uso final (control, negocios, administración y gestión de las aplicaciones de empresa), combinando los distintos protocolos. Hoy en día la mayoría de las LAN, el control y administración, se basan en Ethernet y protocolo TCP / IP. Los datos en tiempo real son utilizados por las empresas operadoras de red para la gestión del sistema eléctrico.

En ciertas ocasiones, independientemente de si se configuran redes de tipo público o privado, el centro de control necesita conectarse con las subestaciones de manera remota. En los últimos años, estas conexiones se realizan a través de internet. Para ello se establece una red privada virtual (VPN, Virtual Private Network) que conecta con los equipos remotos, y en muchas ocasiones se utilizan servicios web. Un ejemplo de esto es una WAN de datos que conecta a los operadores en los distintos países de Europa, utilizando su propia red de fibra óptica que ejecuta el protocolo ICCP, Inter-Control Center Communications. Los distintos centros de control (SCADA LAN de cada una de las empresas operadoras y WAN que comunica a las distintas empresas) están separados por cortafuegos.

Los cortafuegos utilizados en las diferentes redes pueden ser configurados para restringir la conectividad hacia o desde las redes para evitar el acceso al sistema. Se puede aplicar la autenticación de todos los usuarios que intentan acceder a la red y permitir el acceso sólo a los servicios externos necesarios.

Así pues los cortafuegos pueden registrar el flujo de tráfico entre redes para poder supervisarlo o realizar la detección de intrusiones. Para cumplir ciertos requisitos de seguridad, se utiliza a veces una zona desmilitarizada (DMZ, DeMilitarized Zone) para separar la red de control de la red de la compañía administrativa o de Internet.

La DMZ ofrece una interfaz privada y una pública para seguridad de los servidores y los sistemas de control. Una de las interfaces está conectada a la red que controla la

[13] PLC se refiere a las redes de comunicación a través de las líneas eléctricas. En el apartado 6.2.5 se describe en líneas generales las características de las mismas puesto que parte de la solución propuesta se configura en base a esta tipología.

operación y otra red permite el acceso para las aplicaciones administrativas y de gestión, asegurando un acceso seguro a los distintos elementos del sistema.

2.3.1 Ejemplo de red de comunicaciones en el sistema eléctrico: Red Eléctrica de España

Red Eléctrica de España es el operador del sistema de transporte único en España y garantiza la continuidad y seguridad del suministro eléctrico manteniendo en constante equilibrio la generación y el consumo. Para desempeñar a cabo esta tarea con éxito, Red Eléctrica de España ha tenido que desplegar una vasta red de telecomunicaciones. A continuación se puede leer una descripción recogida en su página web oficial [25].

> Red Eléctrica dispone en la actualidad de una red de fibra óptica de más de 21.300 km de cable y alrededor de 19.000 equipos, para la prestación de servicios de telemando, telecontrol y teleprotección, con una excelente fiabilidad. Se trata de una extensa red troncal, en la que las fibras ópticas se alojan en el interior de los cables de acero que forman parte del tendido eléctrico de alta tensión, lo que le confiere una robustez y seguridad excepcionales.
>
> Además de su gran extensión, la red de telecomunicaciones de Red Eléctrica tiene como característica distintiva su estructura mallada, lo que permite establecer sistemas de transmisión resistentes a fallos, con unos excepcionales índices de seguridad y disponibilidad.
>
> Actualmente, los servicios prestados por esta red cubren plenamente tanto las necesidades de Red Eléctrica como los requerimientos del sistema eléctrico, al tiempo que por su gran capacidad permite prestar servicios de telecomunicaciones a terceros, con excelentes índices de disponibilidad.

2.4 Sistemas SCADA en el sector eléctrico: estado del arte

SCADA es el acrónimo en inglés de un sistema de Supervisión, Control y Adquisición de Datos del (Supervisory Control And Data Acquisition). Así pues, el término SCADA se utiliza para representar los componentes de comunicación y la arquitectura de control que proporciona las capacidades de control dentro de algunos procesos industriales y de servicios.

Dentro del sector eléctrico, los sistemas SCADA se utilizan especialmente en los centros de control para la monitorización remota de la infraestructura y el control de la gestión de energía que intercambia información sobre cargas, tensiones y otros parámetros. Se puede decir que hoy en día los sistemas SCADA juegan un papel clave en una infraestructura tan crítica como es la energética.

Estos sistemas pueden configurarse para trabajar solos o con otros componentes dentro de la infraestructura. En el sector eléctrico, los sistemas SCADA ayudan a los operadores del sistema en la gestión de una manera fiable y eficiente. Los centros de control donde se instalan SCADA son los EMS y los DMS.

Un EMS es un centro de control para la gestión de energía (Energy Management System) que está asistido por una serie de herramientas las cuales permiten a los operadores de redes eléctricas supervisar, controlar y optimizar el rendimiento de la instalaciones de generación y / o sistema de transmisión. Al igual que el EMS, el DMS es un centro de control para la gestión de energía (Distribution Management System) que está asistido por un conjunto de elementos y diseñado para monitorizar y controlar la red de distribución de manera eficiente y fiable.

Los avances de la tecnología y la evolución del entorno empresarial han impulsado cambios en la arquitectura de la red SCADA. La tendencia actual en el sector eléctrico orienta el mercado hacia la necesidad de una mayor eficiencia, de unas plataformas consolidadas de producción y la creación de grandes empresas con menos personal que utilizan sistemas SCADA. Esto se deriva en:

- una creciente dependencia de las redes públicas de telecomunicaciones para conectar sistemas SCADA separadas;
- un uso cada vez mayor de estándares abiertos y protocolos;
- la interconexión de los sistemas SCADA a las redes de negocio para mejorar la cantidad y el detalle de la información disponible.

Existen además unos sistemas SCADA -BMS (Business Market/Management System) de uso por parte de los comercializadores que optimizan los servicios de negocio para los consumidores de electricidad, tienen mecanismos para dar soporte de equilibrio económico en el sistema, realizar un control de costes, aprovechar sinergias de la infraestructura y proveer de eficiencia económica en el negocio, etc.

Distintas marcas comerciales ofrecen soluciones de sistemas SCADA de acuerdo a las necesidades de los procesos que se necesitan controlar por parte de los operadores. Algunos SCADA comerciales que se pueden encontrar en el mercado son:

- Aimax, Desin Instruments S.A
- CUBE, Orsi España S.A
- FIX, de Intellution
- Lookout, National Instruments
- PLANTSCAPE SCADA and S7 300 PLC, SIEMENS (ejemplo de visualización por pantalla para este tipo de SCADA en Figura 7)
- Monitor Pro, Schneider Electric (ejemplo de architectura para este tipo de SCADA en Figura 8)
- SCADA InTouch, LOGITEK
- Scatt Graph 5000, ABB

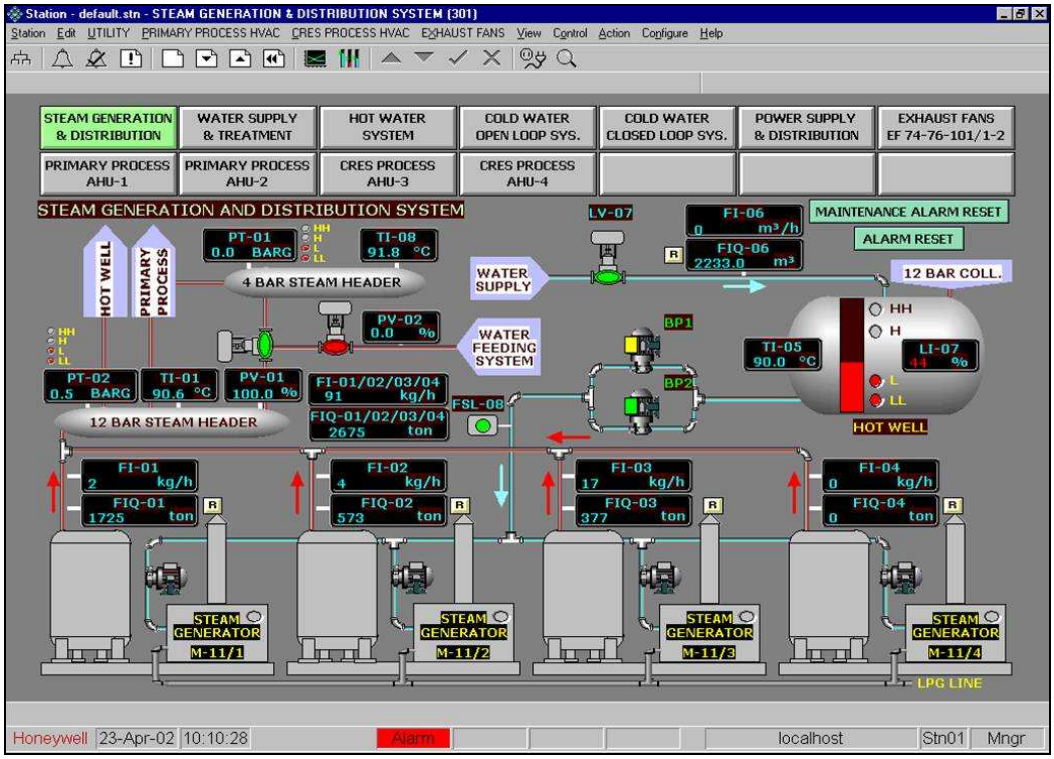

Figura 7. Ejemplo de SCADA para el control de una planta de generación eléctrica
Fuente: Siemens, www.swe.siemens.com/

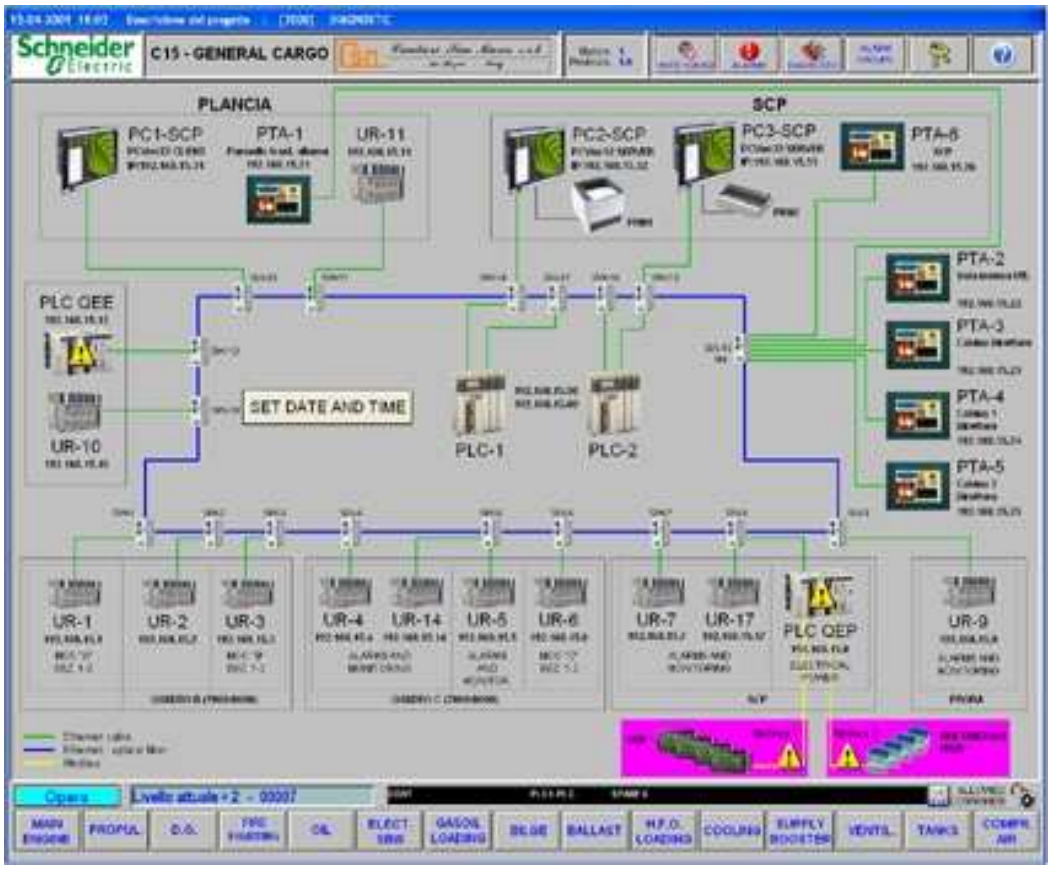

Figura 8: Ejemplo de arquitectura SCADA comercial Monitor Pro
Fuente: Schneider Electric, http://www.schneider-electric.co.uk/

2.4.1 Ejemplo SCADA: centro de control de Red Eléctrica de España

Red Eléctrica de España es el operador del sistema de transporte único en España y garantiza la continuidad y seguridad del suministro eléctrico manteniendo en constante equilibrio la generación y el consumo. Para desempeñar a cabo esta tarea con éxito, cuenta con el Centro de Control Eléctrico (CECOEL).

El CECOEL cuenta entre otros elementos con un SCADA que permite el tratamiento de los datos de la red eléctrica en tiempo real. De acuerdo con la información publicada en su página web [25]

El Centro de Control Eléctrico de Red Eléctrica (CECOEL) emite las instrucciones de operación del sistema de producción y transporte con el fin de garantizar la seguridad y calidad del suministro eléctrico. Para hacer frente a las variaciones de la demanda y a la falta de disponibilidad de los generadores se programa la producción y los intercambios internacionales. Adicionalmente, es preciso emitir consignas de operación de los elementos de la red de transporte para que las variables de control permanezcan dentro de los márgenes establecidos en los procedimientos de operación.

El CECOEL controla de forma permanente el estado de la red y sus parámetros eléctricos, mediante una red de telecomunicaciones, actuando sobre las variables de control para mantener la seguridad y calidad del suministro o para restablecer el servicio en caso de que se haya producido un incidente.

El CECOEL se encuentra soportado por un sistema de control de última generación, cuya misión es gestionar la información que se recibe en tiempo real desde las centrales y las instalaciones de la red para presentarla a los operadores en una forma gráfica fácilmente comprensible y efectuar los estudios que permitan garantizar la seguridad del sistema eléctrico.

Figura 9. Centro de Control de Red Eléctrica de España
Fuente: www.ree.es

2.5 Líneas de trabajo existentes en el ámbito de la seguridad cibernética

Se espera que la demanda de electricidad se aumente en el futuro. Para el crecimiento en muchos sectores emergentes, es necesario un incremente del consumo eléctrico: acondicionamiento de espacios, procesos industriales y transporte (por ejemplo vehículos híbridos, locomotoras de trenes).

Como ya hemos explicado, para poder abordar esta "revolución", la gestión y toda la infraestructura eléctrica es altamente dependiente de los sistemas de información y comunicación. Desde el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés), todas las comunicaciones y los flujos de electricidad que conectan cada nivel (generación, operación de transporte y distribución, clientes, mercados,…) consta en sí mismo de importantes elementos que se integran dentro de las "redes inteligentes" y que están conectados entre sí a través de comunicaciones de dos vías o rutas: flujo energía y canal de comunicaciones. "*Estas conexiones son la base del futuro, red eléctrica inteligente de la energía y dinámica.*" (…) "*Para el IEEE, la Smart Grid es el gran 'Sistema de Sistemas'*".

> At IEEE, the smart grid is seen as a large "System of Systems,"

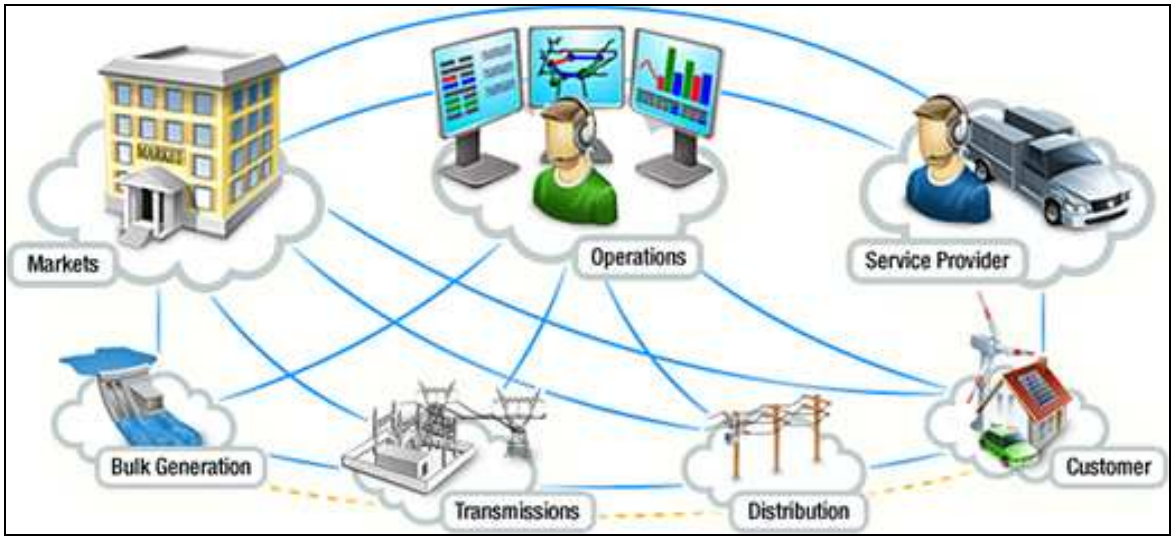

Figura 10: Smart Grid Conceptual Model
Fuente: Documento [9], IEEE

Así pues, se han llevado a cabo muchos los proyectos de investigación para explorar el concepto de redes inteligentes (Smart Grids). De acuerdo con una reciente encuesta sobre redes inteligentes (*Smart Grid - The New and Improved Power Grid: A Survey; IEEE Communications Surveys and Tutorials 2011; X. Fang, S. Misra, G. Xue, and D.*

Yang) [10], la investigación se centra principalmente en tres sistemas en red inteligente: el sistema de infraestructura, el sistema de gestión, y el sistema de protección.

El sistema de gestión es de una red inteligente debe ofrecer una gestión avanzada permitiendo mejorar la eficiencia energética y poder actuar sobre el perfil de la demanda eléctrica, mediante la optimización y el aprendizaje automático.

Los sistemas de protección una red inteligente que deben proporcionar un análisis de fiabilidad de la red, protección de falla, y servicios de seguridad y protección de la privacidad. Para esto, se ha de tener en cuenta la infraestructura utilizada en redes inteligentes, ya que debe proporcionar mecanismos fiables ante ataques y fallos de la propia infraestructura eléctrica. Además aparecen muchas vulnerabilidades asociadas al uso más intenso de los sistemas de comunicación e información.

Por ejemplo, un beneficio proporcionado por la red inteligente, es la capacidad de obtener datos más fiables desde los clientes de contadores inteligentes y otros dispositivos eléctricos, pero a su vez, existe una preocupación por la privacidad de esa información. Esta información puede ser extraída por agentes interesados para que revele información personal de consumidores tales como los hábitos personales.

De acuerdo a lo que comenta Göran N. Ericsson en su pubicación "*Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure*" [11] para garantizar la ciberseguridad de los sistemas es necesaria una acción de coordinación entre las autoridades gubernamentales y agencias centrándose en la seguridad de los sistemas SCADA. Las acciones deberán centrarse en distintos dominios del negocio tales como:

- Proveedores de equipos y servicios (suministradores y mantenedores)
- Control sobre las plantas de generación eléctrica
- Control sobre la gestión de las subestaciones y otras unidades remotas
- Tratamiento de las TIC a nivel corporativo dentro de las empresas
- Garantizar la seguridad de las distintas redes de comunicaciones
- Tratamiento de la información en tiempo real

En Estados unidos existe un amplio desarrollo normativo y de especificaciones de seguridad como veremos en el siguiente capítulo. Además de esto y cabe destacar como novedad con respecto al enfoque que existe en Europa, la realización de un desarrollo normativo desde la agencia nacional de auditoría para poder garantizar un marco común seguro en el desarrollo de las nuevas infraestructuras eléctricas. Los desafíos en curso para asegurar los sistemas de electricidad y redes incluyen:

- Una mejora para vigilar el cumplimiento de la industria con las normas de seguridad cibernética

- Mejorar los aspectos regulatorios, puesto que los actuales hacen difícil garantizar la seguridad cibernética de los sistemas de redes inteligentes de energía

- Un enfoque de cumplimiento de la normativa en lugar de la seguridad integral

- Desarrollo de mejores medidas de seguridad específicas para los sistemas de redes eléctricas

- Desarrollo de un mecanismo eficaz para el intercambio de información sobre seguridad cibernética y otros temas

- Definir indicadores para evaluar la seguridad cibernética

Como veremos en el siguiente capítulo, en Europa la tendencia es la de crear grupos de trabajo que elaboren directrices técnicas y recomendaciones para la adopción de buenas prácticas de los distintos sectores, incluido el sector eléctrico. En concreto para el desarrollo de las nuevas infraestructuras eléctricas, se han configurado distintos paneles de expertos (Smart Grids Task Force (SGTF)[15]), con un grupo centrado en recomendaciones regulatorias para la seguridad de datos, manejo y protección de datos (Grupo 2).

2.6 Conclusiones

En el presente capítulo, se ha realizado una revisión sobre la panorámica general del funcionamiento de la infraestructura eléctrica y un repaso al estado del arte de los sistemas de control y comunicación que se utilizan para dar soporte a su funcionamiento. Los principales puntos a tener en cuenta son:

- El **paradigma clásico de funcionamiento del sistema eléctrico** en el que el flujo de energía va desde los puntos de gran generación hasta los centros de consumo está cambiando **hacia un sistema más distribuido donde el control se realiza a través de sistemas de comunicación e información**.

- Estos **sistemas** de comunicación e información **han de ser robustos con el fin de que puedan tener disponible información fiable en tiempo real** para los operadores y los distintos agentes que intervienen en el sistema (productores, comercializadores, clientes y autoridades).

- Aunque la arquitectura de las redes de comunicación para sistemas de automatización eléctricos que cumplan los requisitos de seguridad necesarios para su operación y gestión depende muchas veces del tamaño del sistema y de la cantidad de tráfico de datos, estos **datos y sus flujos de información sean**

[15] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

manipulados de manera jerárquica, donde los niveles suelen estar separados por puertas de enlace, DMZ, o cortafuegos.

- Los centros de operación y control utilizan **sistemas SCADA**, que tal y como se ha podido ver, **juegan un papel clave en una infraestructura tan crítica como es la energética**. Éstos se instalan en los centros de control (EMS y DMS). La tendencia actual es la necesidad de una mayor eficiencia, produciendo los proveedores de equipos unas plataformas consolidadas.

- Con estas plataformas ya consolidadas, los desafíos en curso para asegurar los sistemas de electricidad y redes incluyen: una **mejora en el cumplimiento de la industria con las normas de seguridad cibernética y los aspectos regulatorios**, que permitan garantizar la seguridad cibernética de los sistemas de redes inteligentes de energía: desarrollar **medidas de seguridad particulares para los sistemas de redes eléctricas**, así como un **mecanismo eficaz para el intercambio de información** cibernéticamente seguro y otros temas y **definir indicadores para evaluar la seguridad cibernética que apliquen a la gestión en el sector eléctrico**.

Se ha visto que el actual desarrollo de la infraestructura necesita de un despliegue asociado de sistemas de información y comunicación seguros y robustos que permitan garantizar una correcta operación y la interacción de los distintos agentes implicados.

Para poder garantizar estos objetivos de seguridad, es necesario que se apliquen una serie de normas, y en muchos casos la existencia de estándares posibilita alcanzar unos niveles de seguridad mínima. Por lo tanto, a continuación se revisará parte de la normativa europea de aplicación sobre seguridad del sector eléctrico y se revisarán varios de los estándares de seguridad con el fin de poder después hablar de los procesos de estandarización y regulación existentes.

Una vez sentadas las bases del estado el arte en el sistema eléctrico y sus aspectos normativos en el ámbito de la seguridad se podrá llevar a cabo de manera adecuada el caso de estudio seleccionado.

3 Normativa europea y estándares de seguridad

En el presente capítulo se va a realizar un estudio y evaluación de la normativa europea y estándares de seguridad que pudieran ser de aplicación al caso que concierne a los controles, las comunicaciones y otros equipos críticos de la red de energía.

En primer lugar se procederá con una revisión de la documentación encontrada sobre la normativa europea acerca de seguridad de infraestructuras críticas y varios de los principales estándares de seguridad existentes.

A nivel europeo se analizará la normativa europea en materia de infraestructuras y la estrategia de seguridad cibernética definida a nivel paneuropeo.

De manera más particular se hace un recorrido por los principales estándares en materia de seguridad para los sistemas de información y comunicación se recogen sus características abordando las normas ISA99, las NERC y/o ISO y/o NIST de aplicación.

Por último se muestra una síntesis que permita reflejar una serie de prácticas a aplicar en materia de seguridad para los distintos entornos que aplican al funcionamiento de la infraestructura eléctrica y que recomendaciones se realizan al respecto.

3.1 Directiva 2008/114/EC de infraestructuras críticas

El 12 de diciembre de 2006, la Comisión Europea comunicó un Programa Europeo para la Protección de Infraestructuras Críticas[12], que establecía un marco general para las actividades de protección de las infraestructuras críticas de la UE (siendo éste, el elemento, sistema o parte de éste situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones).

Las conclusiones del Consejo de Ministros publicada en abril de 2007 reafirmó la responsabilidad de los Estados miembros en la gestión de la protección de las infraestructuras críticas situadas en sus respectivos territorios.

Uno de los principales resultados del Programa fue la publicación de la Directiva 2008/114/EC que establece un procedimiento para la identificación y designación de infraestructuras críticas europeas además de, proporcionar un enfoque común para evaluar estas infraestructuras, con el fin de mejorarlas para proteger mejor las necesidades de los ciudadanos.

Los Estados miembros deben pasar por un proceso de identificación de potenciales infraestructuras críticas. Los criterios deben tener en cuenta las posibles bajas y los efectos económicos, públicos y sectoriales.

En su origen (y por el momento) esta directiva sólo afecta de manera obligatoria a la energía y los transportes. Según la Directiva, la identificación y designación de las infraestructuras críticas que afectasen a varios Estados debía ser completado antes del 12 de enero de 2011 y después se revisarían periódicamente.

Los Estados miembros deben velar por que el Plan de Seguridad (OSP, por sus siglas en inglés) implantado en cada territorio o una medida equivalente está en funcionamiento en cada infraestructura crítica identificada. El OSP deberá ser revisado regularmente para garantizar su buen funcionamiento.

Los Estados miembros deben asegurarse de que existe un oficial de enlace entre los cuerpos de seguridad y un responsable de cada una de sus infraestructuras críticas. El oficial sirve como punto de contacto entre el propietario/operador de la infraestructura y la autoridad del Estado miembro en cuestión. El propósito es permitir el **intercambio de información** sobre los riesgos y peligros relacionados con dicha infraestructura.

Por otro lado, los Estados miembros deberán informar a la Comisión cada dos años sobre los riesgos, amenazas y vulnerabilidades de las diferentes infraestructuras para que la Comisión Europea pueda evaluar las medidas a tomar sobre el conjunto de las instalaciones en base a dicha información recibida.

La Directiva también recoge que como soporte a los propietarios/operadores de las infraestructuras críticas, la Comisión proporcionará acceso a las mejores prácticas y metodologías en materia de protección de estas. Cualquier información sensible será tratada sólo por personas que tengan el nivel adecuado de habilitación de seguridad y sólo para los fines originales.

En cuanto al alcance de esta legislación en el ámbito eléctrico, la directiva considera gran parte de la infraestructura eléctrica como crítica:

> Por **lo que se refiere al sector energético** y, en particular, **a los métodos de generación y transporte de electricidad** (en relación con el suministro de electricidad), se sobreentiende que, toda vez que se estime oportuno, podrán incluirse en la generación de energía eléctrica las partes de transmisión eléctrica de las centrales nucleares, pero se excluirán sus elementos específicamente nucleares regulados por la legislación nuclear pertinente, como los tratados sobre cuestiones nucleares y la legislación comunitaria.
>
> (…)
>
> **Entendiéndose como "infraestructura crítica", el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales** vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.

En España, a nivel nacional, se ha realizado la transposición de la directiva 2008/114/EC a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. En relación a los sistemas de información se contempla lo siguiente:

> Los Planes de Protección Específicos de **las diferentes infraestructuras críticas incluirán todas aquellas medidas que los respectivos operadores críticos consideren necesarias** en función de los análisis de riesgos realizados respecto de las amenazas, en particular, las de origen terrorista, sobre sus activos, **incluyendo los sistemas de información**.
>
> …
>
> **La seguridad de los sistemas de información y comunicaciones previstos en este real decreto será acreditada** y, en su caso, certificada por el Centro Criptológico Nacional del Centro Nacional de Inteligencia, de acuerdo con las competencias establecidas en su normativa específica.

3.1.1 Estrategia de Seguridad Cibernética de la Unión Europea

Para garantiza **transparencia en la operatividad de las empresas**, la Comisión Europea anunció en febrero de 2013 en Bruselas[13] su intención de obligar legalmente a determinadas empresas y administraciones públicas a informar sobre 'ciberataques' u otros incidentes de seguridad digitales.

La norma legal propuesta por la Comisión Europea se **aplicaría a empresas gestoras de infraestructuras importantes, tales como los proveedores de energía**, bancos, empresas que prestan servicios de transporte público, hospitales y administraciones públicas.

La Comisión Europea también considera que los 27 países miembros de la UE deben instalar centros nacionales de seguridad para prevenir ataques desde Internet y reaccionar adecuadamente en caso de que tales ataques se produzcan.

Las líneas generales que propone la Comisión Europea son:

- Que todos los países tenga una estrategia de seguridad Cibernética.
- Se exigirá la regularización y establecimiento de un marco adecuado para un intercambio de información en seguridad Cibernética.
- Para garantizar transparencia, se pedirá que las empresas privadas publiquen la información sobre ‘Ciberataques’.

Figura 11: evidencias y comunicados en relación a la preocupación mostrada en el entorno de la ciberseguridad
Fuente: Elaboración propia

Dentro del comunicado conjunto elaborado por el Parlamento Europeo, el Consejo, el Comité Económico y Social y el Comité de las Regiones como estrategia para el desarrollo de los recursos industriales y tecnológicos para la seguridad cibernética pide a la ENISA[18]:

- Directrices técnicas y recomendaciones para la adopción de normas NIS (Network and Information Security) y buenas prácticas de los distintos sectores.

[18] European Network and Information Security Agency: agencia consultiva de la Unión Europea encargada de mejorar las redes y la seguridad de la información en la Unión Europea. La agencia tiene que contribuir al desarrollo de una cultura de red y seguridad de la información para el beneficio de los ciudadanos, consumidores, empresas y organizaciones del sector público de la Unión Europea, y por tanto contribuirá a mejorar el funcionamiento interno de la EU. Se describirá con mayor detalle en el apartado 4.3.

The Commission asks ENISA to:

- Develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardisation bodies and the European Commission Joint Research Centre, **technical guidelines and recommendations for the adoption of NIS standards and good practices** in the public and private sectors.

3.2 Estándares de seguridad

Los rápidos avances en los sistemas de información y comunicación, han propiciado hardware y software más pequeños y de mejores prestaciones y equipos informáticos menos costosos disponibles para la pequeña empresa y el usuario doméstico. En las últimas décadas, estos equipos han sido interconectados en todo el mundo a través de Internet.

El rápido crecimiento del procesamiento electrónico de datos y comercio electrónico a través de Internet requiere los mejores métodos de protección de los equipos y de la información que éstos almacenan, procesan y transmiten.

Esto ha propiciado que las disciplinas de seguridad informática y seguridad de comunicaciones hayan surgido con numerosas organizaciones profesionales que comparten los objetivos de garantizar la seguridad y fiabilidad de los sistemas de información. Los principios básicos de la seguridad de la información se pueden resumir en los siguientes:

- **Confidencialidad de la información**
- **Integridad de los datos**
- **Disponibilidad**

Con el fin de poder garantizar estos principios básicos, las instituciones y los agentes de mercados involucrados en los diferentes procesos industriales han desarrollado distintos criterios para garantizar que el proceso de especificación, implementación y evaluación de un producto en cuanto a seguridad de la información y las comunicaciones que lleva asociado. Estos criterios vienen definidos de manera rigurosa dentro de estándares.

Los estándares de seguridad aseguran que los usuarios de equipos electrónicos y sistemas puedan especificar sus requisitos funcionales de seguridad y garantía, los proveedores pueden implementar y hacer afirmaciones sobre los atributos de seguridad de sus productos, y los laboratorios de ensayo pueden evaluar los productos para determinar si, efectivamente, estos atributos se cumplen.

El uso generalizado de Internet para la comunicación dentro de la toma de decisiones en tiempo real, el seguimiento de los procesos y el control de sistemas industriales y de negocios (incluidas infraestructuras clave como las redes de electricidad) hace vulnerable sus distintos sistemas ante los ataques de virus y hackers.

La seguridad de los sistemas de control industriales (ICS, por sus siglas en inglés) ha de ser compatibles con los requisitos de tiempo real de los propios sistemas. Desde finales de los noventa muchas organizaciones industriales, han iniciado la publicación de documentos de interés general para la comunidad de seguridad informática.

A lo largo del presente capítulo, se recogen las características de varios de los principales estándares en materia de seguridad para los sistemas de información y comunicación:

- ISO 27000 [14] [15] [16] [17] [18]
- NIST 800-53[19]
- NERC CIP [20]
- ANSI/ISA 99 [21] and IEC 62443 [22]
- IEC 62351 [23]

3.2.1 ISO 27002, 27032 y 27033

La ISO 27002:2005, titulada "Tecnología de la información - Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información" es un código de buenas prácticas de propósito general. En su origen fue desarrollado a partir de la norma británica BS7799, que había sido adoptada como la norma ISO / IEC 17799:2000. Esta norma ha sido revisada en 2007 para alinearse con las otras normas de la serie ISO / IEC 27000.

ISO / IEC 27002 proporciona recomendaciones de mejores prácticas en la gestión de seguridad de la información a ser utilizada por aquellos que tienen la responsabilidad de iniciar, implementar o mantener sistemas de gestión de seguridad de la información (SGSI).

Las ISO 27002 desarrolla una serie de recomendaciones del ciclo de vida completo de los sistemas informáticos:

1. Evaluación y tratamiento del riesgo
2. La política de seguridad
3. Organización de la seguridad de la información
4. Gestión de activos
5. Seguridad de recursos humanos
6. Seguridad física y ambiental
7. Gestión de comunicaciones y operaciones

8. Control de acceso
9. Adquisición, desarrollo y mantenimiento de los sistemas de información
10. Gestión de un incidente en la seguridad de la información
11. Gestión de la continuidad de negocio
12. Cumplimiento de requerimientos legales, políticas y consideraciones de auditoría

Cada sección describe los controles de seguridad de la información y sus objetivos: los primeros son, en general, considerados como la mejor práctica los medios para lograr estos últimos. Sin embargo, a pesar de que la norma ISO 27002 tiene una relevancia general, el proceso de aplicación práctica a menudo no es tan claro.

Gracias a que la temática de esta norma es la seguridad de la información en general, ésta es aplicable a casi todos los sectores y departamentos dentro de una organización (en las redes eléctricas no sólo a los sistemas SCADA, sino también, por ejemplo, a los sistemas administrativos o de ingeniería). La ISO 27002 hace referencia a la seguridad de los activos de información y no sólo a las tecnologías de información y comunicaciones o los sistemas de seguridad en sí mismos. Seguridad de la información se define en el contexto de la norma como: la preservación de la **confidencialidad** (asegurando que la información es accesible sólo aquéllos autorizados a tener acceso), **integridad** de la información (salvaguardando la exactitud e integridad de la información y los métodos de procesamiento) y **disponibilidad** (garantizar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando es necesario). Conceptos que se ajustan a la perfección con los presentados en la introducción del capítulo.

3.2.1.1 Análisis de la ISO 27002

La sección "Evaluación y tratamiento del riesgo" es particularmente débil. La lógica de la norma se basa en un enfoque "planea, haz, revisa y actúa", pero no hace hincapié en el análisis de riesgos como un elemento clave de la etapa de planificación. Por otro lado, no existen métodos de evaluación de riesgos aceptados para los sistemas SCADA. Existen dos problemas generalizados en su aplicación: por un lado una malas prácticas de evaluación de riesgos, y por otro el desarrollo de varios métodos no del todo compatibles que puedan obstaculizar cualquier comparación de resultados.

La sección "política de seguridad" no siempre es muy clara a pesar de ser bastante genérica. Algunos términos, como por ejemplo, "la política general" pueden ser ambiguos cuando existe la necesidad de políticas más detalladas que cubren los requisitos particulares de seguridad y los controles.

Además, en el caso de las infraestructuras energéticas, es recomendable que la política de control de sistemas de seguridad deba estar integrada con la política de seguridad de

la instalación bajo la supervisión del SCADA y de la política de seguridad corporativa en general.

"La propiedad de los activos" presenta un punto conectado a los conceptos clave de la "responsabilidad personal" y "responsabilidad". La aplicación de la responsabilidad (y responsabilidad personal) en cada caso a cada uno de los equipos informáticos y contenido de los datos a lo largo de toda la red debe quedar claro.

Para "el control de acceso" la administración debe evaluar con mayor precisión la autenticación e identificación de los usuarios remotos, gestión de identidad, etc. El sistema SCADA debe interactuar con distintos departamentos dentro de una compañía que no siempre son los empleados de la empresa. Con frecuencia son terceros que participan únicamente de forma temporal en las acciones en los SCADA. Este problema se extiende más allá de la propia instalación.

La sección "continuidad del negocio de gestión" no dice mucho acerca de la especificación y el cumplimiento de los requisitos de disponibilidad. Esto es cierto respecto a la necesidad de examinar y, cuando sea necesario, proporcionar o mejorar la capacidad de recuperación de sistema. La falta de concreción en estos temas puede suponer problemas como la continuidad de las operaciones, algo esencial.

La sección " gestión de incidentes" debería reflejar los regímenes legales y regulatorios que podrían ser diferentes en cada ámbito de aplicación (regional, nacional o en el caso Europeo a nivel UE).

Así, las diferentes normas afectan de forma práctica a la prueba en los registros, los medios y las formas de gestión de documentos, etc. El impacto de este punto está en discusión en el tribunal de las pruebas en los equipos informáticos y los registros.

La sección "Información de auditoría de sistemas" sólo trata sobre cómo obtener las herramientas de auditoría y datos. Sin entrar en grandes detalles, el equipo de control o de auditoria de un sistema podría llegar a tener dificultades en el acceso al mismo. Para cada caso esto debe ser discutido en cualquier aplicación, y, posiblemente, puede requerir interacción, la participación de especialistas en ámbito legal.

3.2.1.2 ISO / IEC 27032 y 27033 - Ciberseguridad y la seguridad de la red.

ISO / IEC 27032 y 27033 son extensiones de la ISO 27002 para atender ciberseguridad de la red en particular, que han sido parcialmente publicados y que en parte se encuentran en fase de desarrollo. En estos momentos se encuentran publicadas:

- ISO / IEC 27032:2012 - Directrices para la ciberseguridad
- ISO / IEC 27033-1:2009 - Seguridad de red - Parte 1: Introducción y conceptos
- ISO / IEC 27033-2:2012 - Seguridad de red - Parte 2: Directrices para el diseño e implementación de la red de seguridad
- ISO / IEC 27033-3:2010 - Seguridad de red - Parte 3: Escenarios de referencia de redes: amenazas, técnicas de diseño y cuestiones de control

3.2.2 NIST 800-53

El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) es la agencia tecnológica estatal de los Estados Unidos que desarrolla y promueve los estándares tecnológicos. NIST es la entidad responsable de la elaboración de normas y directrices de seguridad de información, incluidos los requisitos mínimos para los sistemas de información de sus distintos departamentos nacionales.

Las publicaciones especiales en las series 800 son los documentos actuales de interés general para la comunidad de seguridad informática. La publicación especial de la serie 800 se creó en 1990 para proporcionar una identidad separada de las publicaciones sobre seguridad de la información. El objetivo general de la serie es proporcionar un marco unificado para la seguridad de la información del gobierno de los Estados Unidos y sus proveedores.

La Ley Federal de la Gestión de Seguridad para la Información (FISMA, por sus siglas en inglés) promulgó que:

1. La clasificación de seguridad de la información federal y de los sistemas de información se basaría en proporcionar unos niveles adecuados de seguridad de la información de acuerdo a una serie de niveles de riesgo,

2. Se definirían unos requisitos mínimos de seguridad para la información y sistemas de información para cada categoría.

NIST 800-53 implementa lo anteriormente indicado proporcionando directrices para la selección y especificación de los sistemas de información que soportan las agencias ejecutivas del gobierno federal de los Estados Unidos. Las directrices dadas por 800-53 están bien consolidadas. En agosto de 2009 se publicó su tercera versión, la cual se asemeja a la de la norma ISO 27002, aunque el rango requisitos en su conjunto es algo más amplio:

- Control de acceso
- Sensibilización y capacitación
- Auditoría y justificación de cuentas
- Evaluación de la seguridad y autorización
- Gestión de la configuración
- Planes de contingencia
- Identificación y autenticación
- Respuesta a Incidentes
- Mantenimiento

- Medios de protección
- Protección Física y Ambiental
- Planificación de la Gestión
- Seguridad del personal
- Evaluación de riesgos
- Sistema de adquisición y servicios
- Sistema de protección y comunicaciones
- Sistema de integridad y de la información
- Gestión de programas

3.2.2.1 Análisis de la NIST 800-53

Una característica importante de las directrices que se reflejan dentro de la NIST 800-53 es que proporcionan los puntos de referencia de control de seguridad que representan el punto de partida para determinar los controles de seguridad de bajo, moderado y alto impacto dentro de los sistemas de información.

Además, NIST 800-53 incluye un conjunto de ejemplos prácticos con el fin de dar a conocer las acciones específicas de un evaluador para realizar las pruebas necesarias para determinar las conclusiones señaladas en los procedimientos de evaluación de la seguridad de un sistema.

Los procedimientos de evaluación han sido desarrollados por el NIST para ayudar a las organizaciones a determinar la eficacia en sus sistemas de información. A diferencia de la norma ISO 27002, NIST 800-53 especifica los procedimientos apropiados para la evaluación de su cumplimiento.

Por último, NIST 800-53 facilita una guía orientativa de cómo adaptar sus requisitos a los sistemas de control industriales, y por eso se dispone de manera pública de una guía de alcance y aplicación de controles de seguridad.

3.2.1 NERC CIP

Las normas NERC CIP-001-009 son un estándar de protección de infraestructuras críticas que están estrechamente relacionadas con el apoyo a la operación fiable de los sistemas eléctricos, proporcionando un marco de seguridad cibernética para la identificación y protección de los activos cibernéticos críticos en estos sistemas.

El actual marco NERC reconoce las funciones de cada entidad en la operación del sistema eléctrico, la criticidad y vulnerabilidad de los activos necesarios para administrar la fiabilidad del mismo, y los riesgos a los que están expuestos estos activos.

Las normas NERC CIP son continuamente revisadas. La siguiente tabla contiene los datos sobre las diferentes normas: más actualizada a la fecha de versión, fecha de emisión, título (asunto) de la norma específica.

Tabla 1: Normas de protección de infraestructuras críticas NERC CIP

Norma	Versión	Fecha	Título (dentro de "Ciberseguridad")
CIP-001	2a	16 de febrero de2011	Reporte de sabotajes
CIP-002	4a	9 de mayo de 2012	Identificación de "Ciber-activos" críticos
CIP-003	4	24 de enero de 2011	Controles para la gestión de la seguridad
CIP-004	4a	24 de mayo de 2012	Personal y Capacitación
CIP-005	4a	24 de enero de 2011	Perímetros de seguridad electrónica
CIP-006	4d	9 de febrero de 2012	Seguridad física de los activos cibernéticos críticos
CIP-007	4	24 de enero de 2011	Sistemas de Gestión de la Seguridad
CIP-008	4	24 de enero de 2011	Notificación de incidentes y planificación de la respuesta
CIP-009	4	24 de enero de 2011	Planes de recuperación de activos cibernéticos críticos

La aplicación de las normas NERC debe hacerse a través de las entidades responsables identificadas por el plan de implementación proporcionado por el NERC y asociado al mismo conjunto de normas. Estas entidades se podrían auto-certificar de manera periódica. Las normas buscan siguientes objetivos:

- Aplicabilidad de la misma
- Definición de un propósito de la misma
- Definición de unos requisitos de desempeño
- Capacidad de ser medida
- Especificación de bases técnicas en ingeniería y operaciones
- Completitud de aplicación
- Consecuencias del incumplimiento
- Lenguaje claro
- Sentido práctico
- Terminología coherente

3.2.1.1 Principales críticas a las normas NERC CIP

A pesar de que son normas de obligado cumplimiento dentro de los Estados Unidos, la adopción plena de toda la normativa supone una labor engorrosa y costosa, por lo que las pequeñas empresas prefieren pagar no las desarrollarlas, llegando incluso en muchos casos a pagar las sanciones correspondientes.

Las pruebas prácticas que se han llevado a cabo han podido demostrar cierta insuficiencia de claridad en algunos de los términos y falta de coherencia.

No viene desarrollado un método que especifique su cumplimiento preciso.

Están desarrolladas ad-hoc para el marco normativo estadounidense y seguramente supondrían una revisión sustancial para poder adaptarse a un contexto europeo.

3.2.1 ANSI/ISA 99 and IEC 62443

La norma ANSI / ISA S99, Guía de seguridad y recursos de los usuarios para la automatización industrial y sistemas de control, está, por lo tanto, muy relacionada con el tema de este proyecto y no debería quedarse fuera del análisis normativo.

ISA considera 99 indicadores de cumplimiento y el uso y aplicación de cada uno de ellos puede permitir el aumento de la seguridad. Las normas ISA 99 se presentaron con posterioridad también al IEC para ser aprobadas como normas IEC 62443.

A continuación puede observarse la lista de normas ya publicadas y aprobadas o en fase de desarrollo, y su referencia con respecto a la norma IEC correspondiente.

Tabla 2: Normas de seguridad para la automatización industrial ISA 99 –IEC62443

Referencia ISA	Referencia IEC	Título	Estado
ISA-TR62443-0-3	NA	Comparativa entre ANSI/ISA-99.02.01-2009	Aprobada
ISA-62443-1-1	IEC/TS 62443-1-1	Terminología, conceptos y modelos	Publicada
ISA-TR62443-1-2	IEC/TR 62443-1-2	Glosario de términos y abreviaturas	Propuesta
ISA-62443-1-3	IEC 62443-1-3	Métricas para el cumplimiento de los sistemas de seguridad	En desarrollo
ISA-62443-1-4	IEC/TR 62443-1-4	Seguridad del ciclo de vida y casos de uso	Propuesta
ISA-62443-2-1	IEC 62443-2-1	Requisitos para gestión de la seguridad del sistema	Publicada
ISA-62443-2-2	IEC 62443-2-2	Guías de Implementación del sistema de gestión de seguridad	Propuesta
ISA-TR62443-2-3	IEC/TR 62443-2-3	Gestión de parches en el entorno IACS	Propuesta
ISA-62443-2-4	IEC 62443-2-4	Certificación de las políticas de seguridad de proveedores y prácticas	Propuesta
ISA-TR62443-3-1	IEC/TR 62443-3-1	Tecnologías de seguridad para la IACS	Publicada
ISA-62443-3-2	IEC 62443-3-2	Los niveles de seguridad de aseguramiento de las zonas y conductos	En desarrollo
ISA-62443-3-3	IEC 62443-3-3	Requisitos del sistema de seguridad y niveles de garantía de seguridad	Aprobada
ISA-62443-4-1	IEC 62443-4-1	Requisitos de desarrollo de productos	En desarrollo
ISA-62443-4-2	IEC 62443-4-2	Requisitos técnicos de seguridad para los componentes	En desarrollo

Como sólo una parte del marco ISA aprobado, no es posible evaluar cuánto difiere la norma con respecto a otra más madura como es la NIST 800-53.

3.2.2 IEC 62351 - Datos y Seguridad de comunicación

La norma IEC 62351 ha sido desarrollada por el Grupo de Trabajo 15 (Comunicación de Datos y Seguridad) del Comité Técnico de la Comisión Electrotécnica Internacional 57 (IEC TC 57)[19], que se encarga de la elaboración de normas para el intercambio de información de los sistemas de energía y de otros sistemas (por ejemplo, sistemas de gestión de la energía, SCADA, etc.)

Su ámbito de aplicación es la seguridad de la información para las operaciones de control de potencia del sistema. Su objetivo principal es llevar a cabo la elaboración de normas para la seguridad de los protocolos de comunicación definidos por IEC TC 57. Específicamente estos protocolos son las series IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, el IEC 61968.

Las especificaciones de la norma son las siguientes:

- IEC 62351-1 - Parte 1: Comunicación de seguridad de red y del sistema - Introducción a los problemas de seguridad
- IEC 62351-2 - Parte 2: Glosario de términos
- IEC 62351-3 - Parte 3: Comunicación de seguridad de la red y del sistema - Perfiles incluyendo TCP / IP
- IEC 62351-4 - Parte 4: Perfiles incluyendo la especificación del mensaje de fabricación (MMS, por sus siglas en inglés)
- IEC 62351-5 - Parte 5: La seguridad de IEC 60870-5 y derivados
- IEC 62351-6 - Parte 6: La seguridad de IEC 61850
- IEC 62351-7 - Parte 7: Red y el sistema de gestión (NSM, por sus siglas en inglés)de los modelos de objetos de datos

Además se encuentra todavía en progreso:

- IEC / TS 62351-8 - Parte 8: Control de acceso basado en perfiles

De acuerdo con los resúmenes publicados en la página web del IEC, los contenidos de cada una de estas partes son los siguientes:

- Parte 1: introduce al lector dentro del concepto de seguridad de la información aplicada a las operaciones del sistema.

[19] http://tc57.iec.ch/index-tc57.html

- Parte 2: abarca los principales puntos abordados en la norma IEC 62351 series. La mayoría de las condiciones de seguridad cibernética se definen formalmente por otras organizaciones de estándares y aquí se proporciona la referencia.

- Parte 3: especifica la forma de garantizar la confidencialidad, la detección de manipulaciones y la autenticación de mensajes para los protocolos SCADA y de telecontrol que hacen uso de TCP / IP como capa de transporte de mensajes.

- Parte 4: especifica los procedimientos, protocolos y algoritmos. Especificaciones para la Fabricación de mensajes (MMS) basados en aplicaciones. Esta especificación técnica debe hacerse referencia como una parte normativa de otras normas IEC TC 57 que tienen la necesidad de utilizar MMS de una forma segura.

- Parte 5: Especifica los mensajes, procedimientos y algoritmos para asegurar el funcionamiento de los protocolos basados en / derivados de la norma IEC 60870-5: Equipos y sistemas de telecontrol - Parte 5: Protocolos de transmisión. Más específicamente, se aplican las normas IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104.

- Parte 6: especifica mensajes, procedimientos y algoritmos para asegurar el funcionamiento de todos los protocolos basados en o derivados de IEC 61850. Esta parte es aplicable al menos a los protocolos de la norma IEC 61850-8-1, IEC 61850-9-2 e IEC 61850-6.

- Parte 7: define las normas de gestión de red y el sistema (NSM) y los modelos de objetos de datos que son específicos de las operaciones del sistema de potencia. Estos objetos de datos NSM se utilizan para supervisar el estado de las redes y sistemas, detectar posibles intrusiones de seguridad, gestionar el rendimiento y la fiabilidad de la infraestructura de información.

3.3 Conclusiones

De la descripción de la directiva 2008/114/EC y de la estrategia de seguridad cibernética de UE se puede concluir que a nivel paneuropeo existe la idea de que:

- **La infraestructura eléctrica es crítica**, puesto que por definición "*"infraestructura crítica", el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones*." **Como toda infraestructura crítica, ha de tener implementados sus mecanismos de seguridad, entre los que se encuentran los de manejo y reporte de información**.

- **Partiendo de los principios básicos de la seguridad de la información se pueden resumir en confidencialidad de la información, integridad de los datos y disponibilidad del sistema, los distintos estándares** (concretamente las organizaciones de estandarización dentro de sus normas) **recogen sus propias definiciones de requerimientos de seguridad para abordarlo.** Estos requerimientos de seguridad siempre han de ser **compatibles con los requisitos de tiempo real de los propios sistemas.**

Después del repaso normativo y de estándares existentes, se van a elaborar en el siguiente capítulo una síntesis que permita reflejar una serie de prácticas a aplicar en materia de seguridad para los distintos entornos que aplican al funcionamiento de la infraestructura eléctrica, viendo cómo es el enfoque desde ciertas organizaciones internacionales como son la Smart Grid Task Force (ver apartado 4.1) o la Agencia Europea de Seguridad de las Redes y de la Información, ENISA (European Network and Information Security Agency) (ver apartado 4.3).

Esta síntesis junto con el trabajo realizado en los capítulos 2 y 3 permitirá cimentar las bases para el posterior caso de estudio.

4 Estandarización y regulación

Después de haber visto a nivel general una descripción de cómo funciona la infraestructura eléctrica y los sistemas de control y comunicación asociados a la misma, y tras haber realizado un repaso a la normativa europea y estándares de seguridad que existen en el marco de las normas que les son de aplicación en distintos entornos, a continuación va a presentarse una serie estudios de cómo se están abordando estos temas en ámbitos de referencia internacional desde el punto de vista de la aplicación de distintos procesos de estandarización, que a su vez pueden desembocar en futuros marcos regulatorios.

Para ello se va a introducir una síntesis que permita reflejar una serie de prácticas (si son las mejores prácticas existentes o no quedaría por determinar en un análisis más a fondo) a aplicar en materia de seguridad para los distintos entornos que aplican al funcionamiento de la infraestructura eléctrica.

Con el fin de poner en contexto al lector, es importante explicar qué son los estándares. De manera explícita según dicta la Real Academia de la Lengua española [24], estandarizar es sinónimo de tipificar[20], que es *ajustar varias cosas semejantes a un tipo o norma común*.

De manera menos rigurosa lingüísticamente hablando, en el mundo industrial se pueden definir los estándares como una serie de normas comunes que se pueden definir como acuerdos documentados, los cuales contienen especificaciones técnicas o criterios precisos que son utilizados consistentemente, como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplen con su propósito.

Por otro lado, regular puede definirse como el acto de medir o realizar ajustes sobre una determinada actividad o al comparar dos o más elementos y así poder establecer orden frente a una situación o cosa específica, para efectuar ajustes con el fin de optimizar el funcionamiento de un dispositivo o sistema (en el objeto de nuestro estudio los sistemas de seguridad para la infraestructura eléctrica) y establecer las normas a las cuales deben adaptarse los individuos que interactúan con estos dispositivos o sistemas.

Así pues, los procesos de regulación, tienen el objeto de establecer un conjunto estructurado de normas que especifican una metodología para definir, describir y transferir representaciones del mundo real. Esto facilita la comprensión y la utilización de las mismas.

Como ejemplo de un proceso regulatorio que afecta a los sistemas de información y comunicación para un amplio abanico de sectores en Europa, se presenta la Directiva 2009/140/CE [26] que modifica la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva

[20] http://lema.rae.es/drae/?val=est%C3%A1ndar , estandarizar. (De estándar). 1. tr. tipificar (‖ ajustar a un tipo o norma).

2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

Esta directiva marca las directrices regulatorias para los Estados miembros en diferentes ámbitos dentro de los sistemas de comunicación e información, entre los que se encuentra la seguridad de los mismos. Al final del presente capítulo se muestran los artículos que desarrollan este ámbito.

La directiva involucra a una agencia consultiva que deberá establecer una senda a seguir para cada uno de los sectores tanto por los reguladores como por los principales agentes del mercado.

4.1 Estudios regulatorios análogos en Europa: Smart Grid Task Force (SGTF)

En estos momentos, el debate que centra el futuro de la red energética habla sobre las redes inteligentes y su desarrollo en el medio-largo plazo. A continuación se van a presentar una serie de estudios que se están realizando dentro de la seguridad para los sistemas de información en distintas infraestructuras eléctricas.

La Comisión Europea ha establecido un grupo de trabajo que está realizando estudios en distintos aspectos en el ámbito de las redes inteligentes: Smart Grid Task Force[21] (SGTF) [27]. En los primeros dos años de trabajo han realizado varios informes en los cuales trataban distintos aspectos de las futuras redes energéticas. Cabe destacar y de alto grado de interés para el presente estudio el documento "Smart Grid Information Security (SGIS)".

Figura 12: Captura de la página web de Smar Grids Task Force
Fuente: http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

[21] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm & http://www.smartgrids.eu/Smart-Grids-Task-Force

Uno de los trabajos realizados por el SGTF y dentro del ámbito del SGIS, ha sido publicado el mandato de la Comisión Europea Red Inteligente, M/490 mandato de normalización la OEN, Organismo Europeo de Normalización, para apoyar el despliegue europeo de Smart Grid [28].

El informe proporciona una descripción de alto nivel sobre cómo las normas pueden ser utilizadas para desarrollar la seguridad dentro de los sistemas de información y comunicación de la futura red eléctrica. También se presentan conceptos útiles a todos los agentes del mercado interesados en las Smart Grid para integrar aspectos necesarios para la seguridad de la información en sus actividades cotidianas.

Cabe destacar que en el propio documento se recoge la idea de que la seguridad dentro de la infraestructura eléctrica requiere de un esfuerzo continuo y que los elementos que se presentan son los primeros pasos hacia una mayor seguridad de las futuras redes energéticas inteligentes. Dentro de esta iniciativa, el grupo de trabajo 2 (Task Force 2) lleva a cabo el estudio sobre recomendaciones en el ámbito de seguridad para el manejo y gestión de la información que se gestionará en las redes de eléctricas "inteligentes". Estos trabajos se centran en:

- Seguridad de los datos
- Manejo de datos
- Privacidad de datos

El SGTF en colaboración con ENISA ha elaborado el informe "*Proposal for a list of security measures for smart grids*" [29], donde estas organizaciones intentan ayudar a los "propietarios de activos de redes inteligentes" para definir buenas prácticas, proporcionándoles un conjunto de medidas de seguridad adecuadas. Estas medidas son agrupadas en dominios.

Los dominios identificados abarcan todos los temas pertinentes señalados por los expertos y por las fuentes de información consultadas (dentro del informe se pueden ver que estas fuentes engloban a gran parte de los agentes del mercado). Los dominios aquí incluidos son:

- Gobernanza de la seguridad y gestión de riesgos
- Gestión de terceras partes
- Proceso de ciclo de vida seguro para componentes de la red / sistemas y de operación inteligentes
- Seguridad, sensibilización y formación del personal
- Respuesta ante incidente e intercambio de información
- Auditoría y contabilidad

- Continuidad de operaciones
- Seguridad física
- Seguridad de los sistemas de información
- Seguridad de la red
- Diseño resistente y robusto de funcionalidades básicas e infraestructuras críticas

4.2 Recomendaciones generales sobre regulación

Independientemente de los resultados analíticos de los casos prácticos a desarrollar, es importante que a la hora de aplicar las normativas que rijan el comportamiento sobre la seguridad en los sistemas de comunicación en la infraestructura eléctrica, éstos sigan una serie de premisas que permitan un adecuado soporte, y puedan contar con el diagnóstico del negocio que se desea soportar y la evaluación de los beneficios y costos de la nueva norma. Es para ello necesario que las normas sean capaces de recoger:

- La actitud y apertura de los agentes involucrados en el proceso regulador; tanto de agentes del mercado como de usuarios, pero en especial del Regulador, que es fundamental para que el proceso consiga unos buenos resultados.
- Evaluación de Impacto Regulatorio, que debería ser implementada y dirigida por la entidad que establezca los mínimos criterios de seguridad siempre y cuando garantice al máximo los siguientes aspectos:
    - Objetividad
    - Transparencia
    - Participación de todos los involucrados en el proceso regulatorio

En la última directiva en materia de regulación Europea en el ámbito de los sistemas de información comunicación, se desarrolla un elenco de recomendaciones para los distintos servicios de comunicaciones electrónicas de la UE para llevar a término el mercado interior de las comunicaciones electrónicas reforzando el mecanismo comunitario de regulación de los operadores en diferentes materias como son la seguridad, la privacidad, la gestión, etc. dentro de los distintos mercados clave (energía, transporte, telecomunicaciones,…).

Concretamente en el ámbito de la seguridad vienen especificados: 4 puntos principales que se recogen a continuación:

1. Los Estados miembros velarán por que las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público adopten las medidas técnicas y organizativas adecuadas para gestionar adecuadamente los riesgos existentes para la seguridad de sus redes y servicios. Considerando el estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado al riesgo presente. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y las redes interconectadas.

2. Los Estados miembros velarán por que las empresas que suministran redes de públicas comunicaciones adopten todas las medidas oportunas para garantizar la integridad de sus redes a fin de asegurar la continuidad de la prestación delos servicios que utilizan esas redes.

3. Los Estados miembros velarán por que las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público notifiquen a la autoridad nacional de reglamentación competente las violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios.

4. La Comisión, teniendo en cuenta en la mayor medida posible el dictamen de la ENISA, podrá adoptar las normas de desarrollo técnicas apropiadas con objeto de armonizar las medidas a que se refieren los apartados 1, 2 y 3, incluidas las medidas que definan las circunstancias, el formato y los procedimientos aplicables a los requisitos de notificación. Estas normas de desarrollo técnicas se basarán en la mayor medida posible en normas europeas e internacionales, y no impedirán que los Estados miembros adopten requisitos adicionales con miras a alcanzar los objetivos de los apartados 1 y 2.

En el siguiente capítulo se desarrollará un caso de estudio que permitirá analizar la normativa actual en materia de seguridad y su aplicación en los centros de control del sistema eléctrico. Para ello es necesario realizar una selección de los parámetros a estudiar, para los cuales la Task Force for Smart Grid es una referencia como punto de partida.

Posteriormente se realizará un contraste de la relación de necesidades que la normativa establece y su implementación en los puntos de gestión de la infraestructura: establecer una relación directa de las normativas y su aplicación en los centros de control.

Una vez se disponga de esta relación es posible establecer una serie de requerimientos técnicos que permitan conocer la morfología del sistema a implantar y por último se realizará una propuesta de solución que satisfaga una serie de prácticas en materia de seguridad para los sistemas de comunicaciones y control dentro de la infraestructura eléctrica.

4.3 ENISA: European Network and Information Security Agency

El Reglamento Europeo 460/2004 del Parlamento Europeo y del Consejo de 10 de Marzo de 2004 [32], crea la Agencia Europea de Seguridad de las Redes y de la Información, ENISA (European Network and Information Security Agency): su misión es garantizar un alto grado de seguridad de las redes y la información en la UE.

ENISA, por tanto, es el organismo a nivel Europeo de realizar las siguientes tareas:

- ofrece asesoramiento experto sobre seguridad de las redes y de la información a las autoridades nacionales e instituciones europeas,
- funciona como foro de intercambio de mejores prácticas,
- facilita el contacto entre las instituciones europeas, las autoridades nacionales y las empresas.

De la mano de las instituciones europeas y las autoridades nacionales, ENISA pretende impulsar en toda la UE una cultura de la seguridad de las redes informáticas.

ENISA ha iniciado el trabajo de la definición de las medidas mínimas de seguridad para distintos aspectos dentro del sector eléctrico con el fin de ayudar a establecer un marco común de medida que pudiera ser utilizado para:

- Establecer unas directrices mínimas dentro de un marco nacional consistente sobre los niveles de seguridad y resistencia de los operadores del mercado de sistemas eléctricos;
- Proporcionar un indicador de umbrales mínimos de seguridad y capacidad de recuperación en los Estados miembros, evitando la creación del "eslabón más débil“;
- Contribuir a lograr un nivel adecuado de transparencia en el mercado interior (en particular para los esfuerzos de seguridad en los que intervienen los distintos stakeholders)

4.4 Conclusiones sobre la estandarización y regulación

Como preámbulo a las conclusiones del capítulo, se quiere matizar que si bien, los dominios aquí incluidos son parecidos a los parámetros indicados en el apartado 5.2, Selección de los parámetros a estudiar en el caso de estudio, éstos (los incluidos dentro del presente trabajo) fueron definidos durante el trabajo con anterioridad a la publicación de este informe de SGT2 y ENISA. La similitud puede deberse a la congruencia de trabajos con ámbitos y objetivos similares. El documento [29] aborda la problemática de manera general para redes inteligentes y el posterior caso de estudio definido en el capítulo 5 y abordado en el capítulo 6 sólo en relación a la problemática de los contadores inteligentes.

Cabe destacar de lo incluido en el presente capítulo que:

- En estos momentos, dentro del debate sobre las redes inteligentes y su desarrollo en el medio-largo plazo, **la Comisión Europea ha establecido un grupo de trabajo** que está realizando estudios en distintos aspectos en el ámbito de las redes inteligentes: **SGTF**.

- El SGTF en colaboración con ENISA ha elaborado el informe "***Proposal for a list of security measures for smart grids***" [29] para definir buenas prácticas en relación al ámbito de las redes inteligentes proporcionándoles un conjunto de medidas de seguridad adecuadas.

- Las normas en materia de seguridad que deben ser implementadas deben cumplir unos criterios mínimos siempre y cuando garantice al máximo **objetividad, transparencia y participación de todos los involucrados en el proceso regulatorio.**

- A nivel Europeo, **ENISA** es la agencia que **ofrece asesoramiento experto sobre seguridad de las redes y de la información a las autoridades nacionales e instituciones europeas**, funciona como **foro de intercambio de mejores prácticas y facilita el contacto entre las instituciones europeas, las autoridades nacionales y las empresas**.

Una vez terminada la síntesis que ha permitido reflejar una serie de prácticas a aplicar en materia de seguridad para los distintos entornos que aplican al funcionamiento de la infraestructura eléctrica, y tras haber adquirido suficiente conocimiento del estado del arte sobre las comunicaciones en el sector eléctrico y la normativa relacionada en materia de seguridad, se dispone de los conocimientos necesarios para plantear y abordar el caso de estudio.

El planteamiento se realizará estableciendo una relación entre la normativa existente y los distintos agentes involucrados en el sector eléctrico, para posteriormente realizar una selección de los parámetros de seguridad específicos a estudiar. El caso de estudio consistirá en la definición de unos elementos que cumplan unas medidas de seguridad mínimas que permitan desarrollar un posible caso de estudio: la infraestructura de información y comunicaciones de los sistemas de los nuevos contadores de electricidad.

5 Introducción al caso de estudio: relación entre la normativa y los distintos agentes y selección de los parámetros a analizar

Como se ha podido ver en los capítulos anteriores, los estándares existentes en materia de seguridad relacionada con los sistemas de información y control que dan soporte a la infraestructura eléctrica, abarcan una amplia gama de ámbitos para los cuales establecen una serie de normas para mantener un cierto nivel de seguridad y unas garantías de operación de los distintos sistemas.

A su vez, en cada país, o conjunto de países, se establecen marcos de regulación comunes para el tratamiento de su propia normativa, y para esto se constituyen una serie de procedimientos reglamentarios para tratar también de garantizar unos niveles de calidad en la operación de gran parte de sus infraestructuras básicas (como en el caso que se va a tratar).

De esta manera, y conociendo las necesidades de negocio y el soporte que necesita, en el presente caso de estudio la red de electricidad y la infraestructura asociada que conforman los sistemas de control y comunicación, es posible identificar una serie de áreas dentro de su proceso de negocio que resultan críticas para su buen funcionamiento y que por lo tanto han de ser protegidas y mantenidas de manera segura.

Así pues, las normativas anteriormente descritas proporcionan, tanto las líneas generales de trabajo a seguir que garanticen una correcta operación de negocio, como las técnicas específicas para la implementación de procedimientos que incorporen seguridad para los controles, las comunicaciones y otros equipos críticos de la red de energía.

En muchos países, ya es incluso posible para ciertas normas específicas obtener la certificación de seguridad cibernética por un organismo acreditado, permitiendo por ejemplo a proveedores ser capaces de garantizar y a usuarios poder esperar garantías de ciertos niveles de calidad (o niveles de sofisticación) en sus equipos y cualificación de personal con respecto a unos parámetros y especificaciones dados.

Figura 13: Ejemplos de entidades certificadoras
Fuente: Elaboración propia

En el presente capítulo, en primer lugar se va a exponer la relación entre las normativas de seguridad anteriormente explicadas y su aplicación en el caso de estudio seleccionado: centros de control de distribución de energía eléctrica y sus sistemas de información y comunicación.

Posteriormente, se argumentará la selección de los parámetros a analizar en el caso de estudio que se desarrollará durante el capítulo 6 y para el cual se presentará una solución aplicada de las normas descritas en los capítulos precedentes. Al final de capítulo se pueden encontrar una serie de conclusiones previas al caso de estudio.

5.1 Relación entre las normativas de seguridad y su aplicación en los centros de control y los sistemas de información y comunicación

- Ya se explicó con anterioridad que la infraestructura de TICs que rodea a los sistemas de energía eléctrica, desde puntos de generación hasta el consumo, pasando por las redes de transmisión y otros aspectos de negocio, necesitan de una red de operación y control, que incluye como ya se vio en el apartado □,

Red de comunicaciones de la infraestructura eléctrica, SCADAs y redes de comunicación entre gran parte de los agentes involucrados en el sector.

Muchos de estos agentes se ven envueltos como responsables en mayor o menor medida en el ámbito de la seguridad que rodea a los sistemas de información y comunicación dentro de la infraestructura eléctrica, que son muchos, y como ya se explicó en el segundo capítulo, no hay un único ente encargado de gestionar toda esta infraestructura, sino que en un sistema liberalizado como el español (y que comparten en muchos otros países de Europa) existen los operadores de las centrales de generación, los de las redes de distribución, los de las redes de transmisión, las empresas comercializadoras de energía y el operador del mercado eléctrico.

A su vez dentro del negocio eléctrico existen también otros agentes que interactúan dentro de su operativa, y que debe tomar las siguientes decisiones:

- Reguladores, responsables políticos y otros legisladores

  Al resultar el servicio de suministro eléctrico básico para la sociedad, éste se regula a través de leyes y Reales Decretos emitidos por el gobierno de España, y se realiza un control regulatorio a través de la Comisión Nacional de Energía[22] (CNE).

  Además, la CNE dicta circulares de desarrollo y ejecución de las normas contenidas en los Reales Decretos y Órdenes del Ministerio de Economía que regulan el desarrollo de la normativa energética, siempre que tales disposiciones le habiliten de modo expreso para ello. Las circulares han de ser publicadas en el "Boletín Oficial del Estado".

  A nivel internacional existe la ACER (Agencia de Cooperación de Reguladores Europeos), que de manera independiente promueve la cooperación entre los reguladores europeos de la energía y asegura que la integración del mercado y la armonización de los marcos normativos se hacen en relación con los objetivos de la política energética de la UE.

- Proveedores de soluciones de seguridad

  Empresas de ingeniería, consultoría y tecnología que acercan y ponen en conocimiento a las empresas del sector energético la oferta de soluciones tecnológicas disponibles en materia de seguridad, de forma que se puedan incorporar los últimos avances tecnológicos a las empresas finales y que se encargan de generar la oferta tecnológicas. En materia de seguridad cibernética, suelen ser empresas que teniendo conocimientos acerca de las TIC, desarrollan productos a medida para las necesidades de los clientes energéticos dentro de esta materia.

- Instituciones académicas y centros de investigación y desarrollo

  Universidades y centros de investigación que se encargan de desarrollar el conocimiento científico para realizar los avances teórico-prácticos de las futuras soluciones tecnológicas e industriales. Normalmente, grupos de investigación no necesariamente energética realizan estudios y avances en el ámbito de la seguridad informática y de las comunicaciones.

- Fabricantes de equipos

[22] En el momento de la realización de esta parte del trabajo, la CNE era el ente regulatorio encargado de esta actividad. En estos momentos es la CNMC, Comisión Nacional de los Mercados y la Competencia, integrando a las distintas comisiones nacionales, la responsable de estas tareas.

Empresas encargadas de desarrollar los componentes industriales para implantar en las empresas de servicios. Como ejemplo, en España se encontraría AFIBEL (Asociación de Fabricantes de Bienes de equipo Eléctrico), que engloba a todas las empresas industriales que fabrican componentes para la generación, transporte y suministro eléctrico. Son empresas de alto calado industrial.

- Operadores de redes y de centros de generación eléctrica

  Empresas que operan las redes de transporte y distribución eléctrica y/o empresas que se encargan de gestionar los puntos de generación eléctrica. Ya explicadas en detalle durante el capítulo 2.1 del presente documento.

- Organismos de normalización y estandarización

  Entidades encargadas de desarrollar las normas y estándares que permiten homogeneizar criterios técnicos o de negocio para los distintos sectores de actividad. Ya explicados y comentados durante los capítulos 3 y 4 del presente documento.

Figura 14: Entidades que participan en el negocio y la operación del sistema eléctrico
Fuente: elaboración propia

Como resulta altamente complicado realizar un análisis que recoja y englobe todas las necesidades de cada una de estas entidades, se va a realizar el caso de estudio para las áreas de seguridad que conciernen a **operadores de las redes de distribución, sus centros de control y los sistemas de información y comunicación con los que interactúan con el resto de agentes**.

5.1.1 Operador de distribución eléctrica

La actividad de las empresas de distribución eléctrica está regulada tal y como establece la Ley 54/97 del Sector Eléctrico y su normativa de desarrollo.

Según la Ley 17/2007, Artículo 39, los distribuidores/gestores de red de distribución son sociedades mercantiles cuya función es explotar, mantener y desarrollar las instalaciones de distribución para garantizar la capacidad de la red de asumir una demanda razonable

En estos momentos la actividad que desarrollan las empresas operadoras de redes de distribución eléctrica es una actividad regulada cuyo objeto principal es la transmisión de energía eléctrica desde la red de transporte hasta los puntos de consumo en condiciones adecuadas de calidad.

Debido a la naturaleza de su negocio, en España, la distribución de electricidad es un monopolio natural (en cada asignación de distribución eléctrica, solo puede existir un único distribuidor con el fin de no incurrir en costes duplicados para el sistema) y cada distribuidor de red está obligado a la construcción de la infraestructura necesaria para suministrar en su zona.

Como se verá en mayor detalle dentro del capítulo 6, Caso de estudio: aplicación de la normativa de seguridad en los centros de control del sistema eléctrico, en la actualidad los distribuidores tienen que llevar a cabo la sustitución de los sistemas de medición de consumo de electricidad de todos los clientes que se encuentren en su zona y que tengan una potencia menor de 15kW.

Así pues, desde la óptica del marco regulatorio las funciones más principales que deben acometer las empresas de distribución eléctrica son:

- Planificar, desarrollar y explotar la red de distribución.
- Ampliar las instalaciones para atender nuevos suministros.
- Prestar el servicio con la calidad de servicio reglamentaria.
- Medir el consumo de los puntos de suministro.
- Facturar las tarifas de acceso.

La mejora de la calidad del suministro es un elemento esencial del servicio eléctrico y uno de los objetivos fundamentales de la actividad de las empresas de distribución de electricidad.

Según refleja una de las principales distribuidoras de electricidad en España, "*La Red Inteligente (Smart Grid) es la evolución tecnológica de la actual red de distribución de energía eléctrica que introduce nuevos conceptos como: telegestión de los contadores, micro - generación distribuida, automatización de las subestaciones, almacenamiento de energía distribuida, gestión de la demanda y suministro eficiente y flexible a vehículos eléctricos. Este*

nuevo concepto permitirá ahorrar energía, reducir costes e incrementar la flexibilidad de la red en sí misma.

La Telegestión es el primer gran paso imprescindible para la implantación de las Smart Grids y sus potenciales aplicaciones:

- *Posibilita la gestión inteligente de las puntas de demanda.*
- *Ofrece información más fiable sobre el comportamiento de la red: mejora la toma de decisiones de explotación.*
- *Permite mayor flexibilidad ante cambios regulatorios, facilita la detección del fraude y otras pérdidas no técnicas y mejora la información para avanzar en la eficiencia global del sistema eléctrico*."

De la misma manera, en el IEEE En la actualidad, existen nuevos paradigmas energéticos en los que define "*las nuevas redes de distribución eléctrica como aquellas que conectan todos los dispositivos de campo inteligentes, y gestionan a través de redes de comunicación por cable e inalámbricas. También puede conectarse a las instalaciones de almacenamiento de energía y recursos energéticos distribuidos alternativas a nivel de distribución*". Definen su paradigma de acuerdo a la siguiente figura:

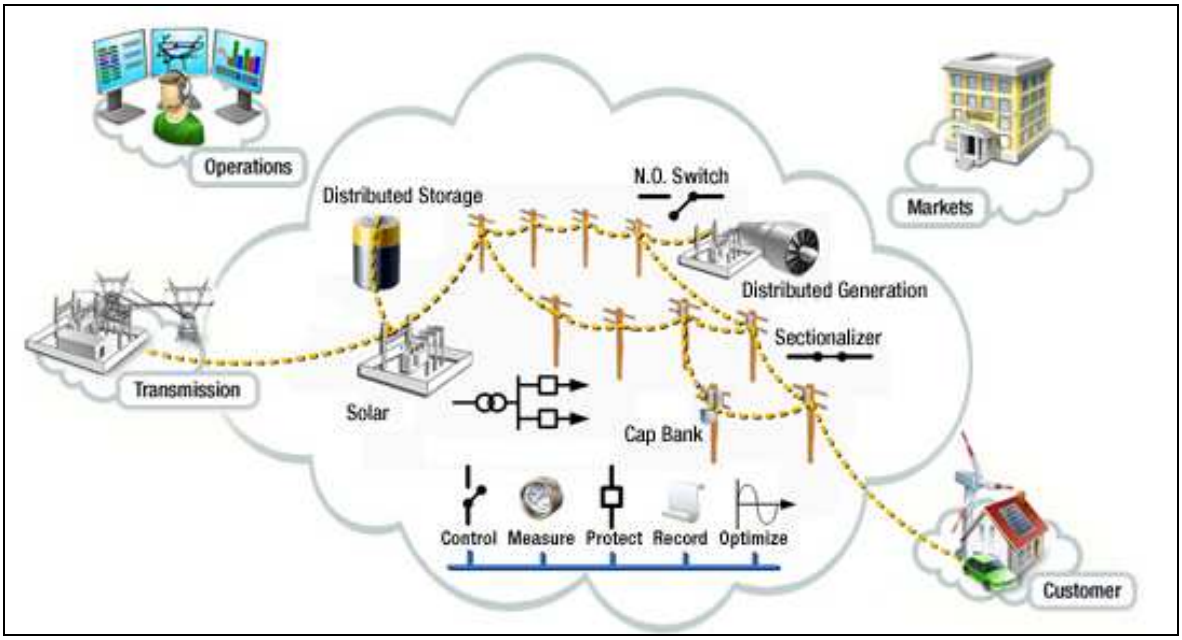

Figura 15: Diseño conceptual de las redes de distribución modernas.
Fuente: Documento [9], IEEE

Para poder ser capaces de llevar a cabo con éxito su operación ante los nuevos desafíos, en relación al tratamiento de la información, es imprescindible que una empresa de distribución eléctrica opere su centro de control y las infraestructuras de comunicación siguiendo las consiguientes tareas:

- Disponibilidad de información muy detallada del cliente con respecto a su consumo de energía y a su comportamiento.

- Disponibilidad de la sensibilidad de los agentes ante señales económicas.
- Prestación de nuevos servicios.
- Gestión de flujos reversibles de energía.
- Control/gestión de un número muy elevado de unidades de generación distribuida con alta volatilidad y problemas de predicción.
- Gestión activa de la demanda.
- Gestión de servicios auxiliares.
- Gestión de señales: sensores y equipos de medida.

En la Figura 16, se muestra de manera esquemática los flujos de información de las empresas de distribución eléctrica, lo que permitirá dar sentido al enfoque planteado para evaluar el marco de seguridad de las redes de distribución de electricidad.

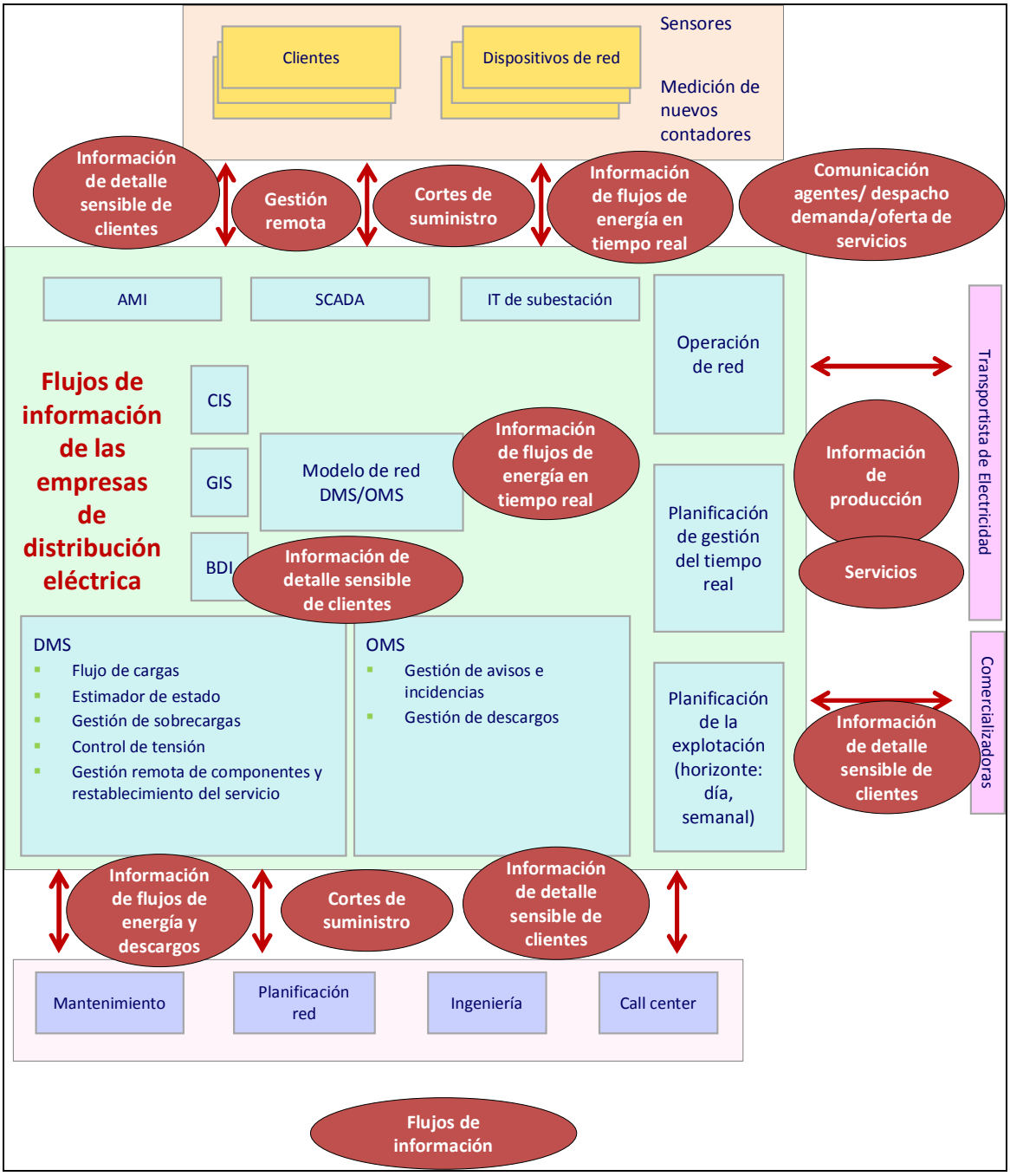

Figura 16: Flujos de información de las empresas de distribución eléctrica.
Fuente: Elaboración propia

Con el fin de poder llevar a cabo todas estas tareas y realizar un tratamiento seguro de la información, es necesario que las empresas de distribución eléctrica mantengan una estricta política en su seguridad en los sistemas TIC y puedan aplicar de manera rigurosa las medidas que consideren oportunas para garantizar una correcta operación.

5.2 Selección de los parámetros a estudiar en el caso de estudio

De entre las especificaciones que conciernen a la seguridad en general, se van a seleccionar una serie de parámetros para poder elaborar un análisis adecuado dentro del caso de estudio que centre el objeto del proyecto a los sistemas de control y comunicación, permita establecer una comparativa dentro de las exigencias de cada conjunto normativo y elaborar la definición de requerimientos técnicos para los equipos que conforman estos sistemas.

Recorriendo todos estos estándares y especificaciones normativas, se pueden identificar un conjunto de áreas globales a abordar por la seguridad:

- Gobernanza de la seguridad y la gestión de riesgos
- Gestión de procesos con terceros
- Componentes de las infraestructuras, sus sistemas y procedimientos operativos
- Respuesta ante incidentes e intercambio de conocimiento
- Continuidad de operaciones
- Seguridad específica de los sistemas de información
- Seguridad de la infraestructura de red y tratamiento derivado de los datos
- Auditoría de datos

Con el fin de entrar en profundidad en las áreas que conciernen al ámbito de las comunicaciones y la parte que tiene una componente TIC dentro de los sistemas de control, se considerarán para el estudio la **gestión de procesos con terceros,** la **seguridad específica de los sistemas de información,** la **seguridad de la infraestructura de red y** el **tratamiento derivado de los datos y auditoría de datos**.

Dentro de cada una de estas áreas recientemente explicadas, es posible identificar una serie de medidas de seguridad que aplican a cada uno de ellos, por ejemplo para la gestión de procesos con terceros se podrían definir los siguientes medidas de seguridad a considerar: acuerdos de confidencialidad con terceros, seguimiento de los servicios de terceros, garantía de continuidad de servicio,…

5.2.1 Gestión de procesos con terceros

Las empresas gestoras deben establecer un programa o conjunto de reglas a través del cual se tramiten de manera ordenada las gestiones con entidades proveedoras externas y en el cual queden definidos los procedimientos para elaborar acuerdos sobre temas relacionados con la seguridad de la infraestructura, sus comunicaciones y el acceso a datos. En el caso de que fuese necesario, estos acuerdos también deben tener en cuenta la cadena de suministro de equipos y las vinculaciones de personal relacionados con el trabajo o las operaciones que se incluyen en los servicios provistos.

Como ya se ha comentado, para el caso de la gestión de terceros, los parámetros que se considerarán son los siguientes:

- Acuerdos de confidencialidad con terceros

  Los gestores de las redes energéticas que contraten a proveedores de equipos deben establecer y mantener acuerdos de terceros apropiados para preservar la integridad, confidencialidad y disponibilidad de la información, al mismo nivel que los servicios internos cuando se trata con clientes y terceros.

- Seguimiento de los servicios de terceros

  Los gestores de las redes energéticas deben ser capaces de establecer y mantener con clientes y proveedores mecanismos para vigilar el cumplimiento de las obligaciones contractuales que se hayan adquirido con terceros en materia de gestión de las TIC y los servicios relacionados con las mismas, y, además, se deben poder validar soluciones para aplicar a los criterios de acuerdo con los requerimientos predefinidos. Los gestores de los centros de control y las infraestructuras de comunicación deben ser capaces de revisar estos servicios según los acuerdos establecidos, vigilar el cumplimiento de los mismos y gestionar los cambios para asegurarse de que los servicios prestados cumplen con todos los requisitos concertados con el tercero.

- Existencia de procedimientos de gestión de la información y la infraestructura de soporte (disponibilidad): garantía de continuidad de servicio

  Es necesario que los equipos soporten continuidad en el servicio y que además existan procedimientos que admitan una continuidad de operaciones que permita reanudar y mantener las operaciones de los sistemas de información en los centros de control para un funcionamiento normal en la operación de distribución eléctrica. Se deben habilitar todos los medios posibles para asegurar las funciones esenciales después de eventos inesperados que interrumpan la operación normal del centro de control.

5.2.2 Seguridad específica de los sistemas de información

En este área se deben establecer y mantener los sistemas de control de que aseguren que los sistemas de información y comunicación y sus componentes sean accesibles de manera lógica por entidades autorizadas y que su información esté bien protegida.

Para el área de seguridad específica de los sistemas de información, los parámetros que se considerarán son los siguientes:

- Seguridad de los datos y la información: procedimientos y niveles de cifrado

  Se deben implementar los requisitos de seguridad para proteger la información en el sistema de información y comunicación. Por ejemplo, se deben cifrar los datos de manera confidencial tanto en los lugares donde estén almacenados como en los canales de comunicación. Asimismo, se deben establecer los procedimientos para el manejo y almacenamiento de la información para proteger esta última contra su divulgación o uso no autorizado.

- Gestión de usuarios

  Se deben establecer y mantener cuentas de usuario para las aplicaciones utilizadas en los centros de control, que permitan una correcta identificación de todos los usuarios, haciendo diferenciación en los permisos y la accesibilidad y privilegios de los mismos. Los procedimientos para implantar políticas de accesibilidad deben abarcar todas las fases del ciclo de vida del acceso de los usuarios, desde el registro inicial de nuevos usuarios a la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Además, es necesario que la organización de gestión de cuentas de los centros de control incluya las siguientes funcionalidades: autorización de privilegios, activar, modificar, desactivar y eliminar cuentas.

- Control de acceso y Control de acceso remoto

  Se debe cumplir el acceso lógico a las entidades autorizadas en los sistemas de información de los centros de control y en su perímetro de seguridad. Esto quiere decir que se deben documentar e implementar procedimientos para la gestión del acceso a la información donde la información esté protegida. Deberán existir reglas que permitan el acceso a los sistemas según los roles establecidos para cada uno de los usuarios. De la misma manera, se establecerán y mantendrán procedimientos similares para los accesos remotos. En estos casos, los gestores de las redes de distribución podrían utilizar distintos métodos de acceso remoto a los sistemas. Se deben desarrollar políticas para evitar múltiples sesiones por un usuario y/o conexiones remotas, hacer una correcta gestión de sesiones inactivas e intentar reducir lo máximo posible los fallos de conexión.

5.2.3 Seguridad de la infraestructura de red y tratamiento derivado de los datos

Dentro de este área de seguridad se debe establecer y mantener un programa de ingeniería de red segura que evite los controles de seguridad.

Para el área de seguridad de la infraestructura de red y tratamiento derivado de los datos, los parámetros que se considerarán son los siguientes:

- Necesidad de segregación de redes

  Una correcta infraestructura de red puede establecer una red separada para ciertos sistemas y no integrarlos de manera única. Por ejemplo, grupos de servicios de información, los usuarios y los sistemas de información podrían estar separados dependiendo de las necesidades de operación y el negocio. Cuando proceda y sea técnicamente posible, la infraestructura de red de los sistemas de control de procesos se debe dividir en varias zonas con diferentes funciones y los requisitos de protección. En particular, los diferentes ámbitos técnicos y operativos deben estar separados unos de otros.

- Nivel de aseguramiento de la comunicación con la infraestructura de red

  Se deben establecer y mantener comunicaciones seguras a través de la red segregada. En los sistemas de información y comunicación se debe proteger la confidencialidad de la información transmitida. La gestión segura de las redes, que puede llegar a abarcar los límites organizativos, debe tratar de manera cuidadosa los distintos flujos de datos, teniendo en cuenta todas las implicaciones legales que podría implicar una inadecuada gestión de la gestión de red, monitorizar las comunicaciones y realizar una protección de datos adecuada. Se debe realizar un control que permita asegurar que las conexiones informáticas y los flujos de información no violen las políticas de control de acceso de las aplicaciones de negocio.

5.2.4 Auditoría de datos (tanto interna como externa)

Se deberían establecer y mantener un proceso de auditoría y rendición de cuentas que permita tener un de registro adecuado en los sistemas de información y comunicación de los centros de control y sus componentes que proporcione un conjunto de datos los que queden registrados y sean válidos para posteriores análisis y test.

Para el área de auditoría de datos, los parámetros que se considerarán son los siguientes: seguridad de los datos y la información:

- Agregación de los procedimientos de auditoría interna a la función de seguridad

  Se deben establecer y mantener los programas software, los dispositivos, y que los distintos componentes sean capaces de poder soportar auditorias de seguridad. Los sistema de información y comunicación deben ser capaces de generar registros para que los distintos eventos que sucedan puedan ser auditables.

- Trazabilidad de la información de los sistemas que soportan las infraestructuras eléctricas

  Se deben establecer y mantener actividades de vigilancia de los sistemas que soportan las infraestructuras eléctricas. El operador de las redes de distribución y el gestor de los centros de control deben implementar y documentar un proceso electrónico o manual de seguimiento y registro de acceso a los puntos de las redes de manera continua. Los sistemas deben ser monitorizados y los distintos eventos que se produzcan han de ser registrados para poder trazarlos. Los registros tienen que poder manejarse en caso de fallos para identificar posibles problemas en los sistemas de información y comunicación.

- Protección de la información de las auditorías internas de seguridad

  Se debe proteger la información de auditoría generada. Deben existir bases de datos y otras instalaciones de registro de información, que deben ser protegidos contra posibles alteraciones, borrados o pérdida de cualquier tipo y también de accesos no autorizados.

5.3 Conclusiones

Un análisis en detalle de toda la normativa aplicable a la seguridad en los sistemas TIC que se encuentran asociados a la infraestructura eléctrica es relativamente complejo, y con el fin de poder entrar en profundidad se han seleccionado el análisis de la normativa a los **centros de control de las redes de distribución de electricidad**.

Si bien, se encuentra involucrados en la aplicación de la normativa distintas áreas de la actividad de distribución, para el caso de estudio se van a considerar las siguientes como parámetros del análisis, por haber sido identificados como los que tienen mayor relación con el ámbito de las telecomunicaciones: **gestión de procesos con terceros, seguridad específica de los sistemas de información, seguridad de la infraestructura de red y tratamiento derivado de los datos y auditoría de datos**.

En cada una de estas áreas se aplicarán una serie de **medidas de seguridad** sobre las que las empresas responsables de los centros de control deberán aplicar los estándares y las normativas relativas a la seguridad cibernética.

6 Caso de estudio: aplicación de la normativa de seguridad en los centros de control del sistema eléctrico

En el presente capítulo se va a desarrollar el caso de estudio en el que se diseñarán para una empresa de distribución de electricidad una serie de sistemas, procedimientos y documentos que le permitirán cumplir con los parámetros seleccionados en capítulo 5 del presente documento, y de este modo poder llevar a cabo parte de sus procesos de negocio de una manera segura de acuerdo a la aplicación de la normativa existente.

En el caso de estudio se trata la situación de una empresa que no existe en una localidad inexistente, pero que plantea una serie de características perfectamente razonables dentro del negocio de distribución eléctrica.

Por tanto, sea la empresa de distribución de electricidad Iberfende Distribución de Electricidad, S.A.[23], en adelante IDESA, que se encarga de la distribución de electricidad de Fuentesur[24], en la provincia de Madrid, y que va a realizar la sustitución de todos los puntos de medida para los clientes localizados en su red de distribución de acuerdo al REAL DECRETO 1110/2007, de 24 de agosto, por el que se aprueba el Reglamento unificado de puntos de medida del sistema eléctrico [2] cumpliendo con lo dictado en la ORDEN ITC/3022/2007, de 10 de octubre, por la que se regula el control metrológico del Estado sobre los contadores de energía eléctrica [3][25].

IDESA, realiza la distribución de energía dentro de Fuentesur para 10.000 puntos de suministro del total de los 95.000 puntos de suministro a los que da servicio dentro de la provincia de Madrid. Todos estos clientes son hogares particulares localizados en viviendas de edificios y locales comerciales donde se encuentran negocios pertenecientes a distintas empresas.

Hasta la fecha, IDESA tiene instalados contadores para medir la cantidad de electricidad consumida en todos los puntos de suministro donde da servicio un contador electromecánico analógico[26] para cada uno de los clientes bien sean hogares particulares o en los locales de las empresas.

---

[23] No existe tal empresa. Empresa ficticia para el presente caso de estudio.

[24] No existe tal localidad. Es una población ficticia para el presente caso de estudio.

[25] La descripción más en detalle tanto del de REAL DECRETO 1110/2007 [2], de 24 de agosto, como de la ORDEN ITC/3022/2007 [3], de 10 de octubre, por la que se regula el control metrológico del Estado sobre los contadores de energía eléctrica se realizará dentro del presente capítulo, en el apartado 6.2. Definición de requerimientos técnicos.

[26] Estos contadores electromecánicos (Sistema Ferais) también conocidos como contador de inducción, son los que tiene el disco horizontal que gira con una velocidad proporcional a la potencia conectada por el usuario.

Estos contadores calculan la energía consumida de manera electromecánica a través de una bobina engranada en un disco horizontal que gira cuando se le aplica una corriente para una determinada diferencia de potencial configurada. Esto hace que dependiendo de la potencia instantánea que se aplica, el giro que sufre el disco a lo largo del tiempo da un valor de energía que es fácil de medir. Los resultados de estas mediciones se presentan a través de un display analógico que muestra el valor de energía que se ha consumido desde la puesta en marcha del contador y el tiempo que este ha estado conectado a la aplicación de potencia entre su paso de circuitos eléctricos.

Figura 17: Contador electromecánico con sistema Ferais
Fuente: http://en.wikipedia.org/wiki/Electricity_meter

Todos los contadores que IDESA tiene instalados para la medición del consumo eléctrico de sus clientes se encuentran dentro de las salas de contadores de 230 edificios distintos y urbanizaciones, sumando un total de 10.000 unidades. Los contadores se distribuyen de manera que 60 de ellos están en bloques de 25 puntos de suministro y los otros 170 en boques de 50 puntos de suministro, en ambos casos entre viviendas y locales comerciales para cada urbanización o edificio.

La disposición urbanística de Fuentesur permite que IDESA sea capaz de realizar las tareas de recolectar los datos que muestran los displays de todos sus contadores con un equipo de dos personas dedicadas a tiempo completo que se encargan de realizar esta tarea 6 veces al año (cada dos meses) para emitir las facturas correspondientes.

Los datos recogidos se almacenan en una agenda electrónica de bolsillo PDA (siglas en inglés, Personal Digital Assistant). Estos datos son volcados a un PC, donde la empresa tiene ubicado el sistema de facturación a sus clientes, después de cada jornada de trabajo a lo largo de los dos meses que dura el proceso de recogida de datos.

La sustitución de todos los puntos de medición para los clientes localizados en su red de distribución de acuerdo al REAL DECRETO 1110/2007, de 24 de agosto[2], por el que se aprueba el Reglamento unificado de puntos de medida del sistema eléctrico

cumpliendo con lo dictado en la ORDEN ITC/3022/2007, de 10 de octubre [3], por la que se regula el control metrológico del Estado sobre los contadores de energía eléctrica le permitirá a IDESA realizar de manera telemática la tarea de recolección de datos de todos sus puntos de suministro y además poder ofrecer a sus clientes una serie de tarifas y servicios gracias a las nuevas capacidades de los dispositivos de medición a instalar.

El objetivo de IDESA es realizar la sustitución de los contadores eléctricos de tal manera que le permita:

- Cumplir con el normativa de acuerdo al RD 1110/2007 [2], y a la ORDEN ITC/3022/2007 [3].
- Poder ejecutar la práctica de nuevos servicios asociados a la instalación de los contadores, tales como la telemedida y la oferta diferenciada de productos
- Implementar sistemas y procedimientos que le permitan cumplir de manera correcta con la normativa de seguridad existente.

Llevar a cabo esta actuación le requiere, además de la propia sustitución de los puntos de medida en los clientes, una serie de adaptaciones dentro de su centro de control para de la actividad de gestión en la distribución de energía eléctrica, una modificación de procedimientos y la implantación de una serie de políticas por parte de la empresa entre las cuales se encuentran la formación, la gestión con terceros, etc.

En el presente caso de estudio se definirán los requerimientos técnicos necesarios para cumplir con la normativa existente y poder realizar de manera segura la implantación de las nuevas soluciones desde los siguientes puntos de vista:

- Gestión de procesos con terceros
- Seguridad específica de los sistemas de información
- Seguridad de la infraestructura de red y tratamiento derivado de los datos
- Auditoría de datos

Antes de la definición de los requerimientos técnicos, se realiza una descripción de la arquitectura de los sistemas de información y comunicación que soporta los centros de control del caso planteado. Los puntos que se van a tratar en ese momento y los componentes de esta arquitectura son:

- Descripción general de la arquitectura
- Dispositivos contadores que se instalarían
- Concentradores de datos
- Equipos centrales para el procesado de datos

- Infraestructura de la red de comunicaciones
- Y una definición de algunos procedimientos de gestión que se deberían implantar para garantizar un servicio seguro

En los siguientes puntos se van a definir los requerimientos técnicos que son necesarios para cumplir cada una de las medidas de seguridad comprendidas en las áreas presentadas dentro de los parámetros seleccionados en el caso de estudio, y la descripción de las soluciones para cumplir con el objetivo de la empresa, que serán:

- Contratos con empresas proveedoras de servicios y con usuarios para el uso de los dispositivos y accesos a los datos
- Procedimientos para el seguimiento de actividades de empresas proveedoras
- Tratamiento de los datos y la información: procedimientos y niveles de cifrado
- Gestión de usuarios, control de acceso y control de acceso remoto
- Segregación de redes
- Aseguramiento de la comunicación con la infraestructura de red
- Procedimientos y definición de las auditorias de los sistemas definidos en la arquitectura: dispositivos, redes
- Procedimientos de auditoría interna de la función de seguridad
- Trazabilidad de la información de los sistemas que soportan las infraestructuras eléctricas

Estas soluciones son descritas con mayor detalle en el apartado 6.3, Soluciones propuestas para cada medida de seguridad. Conviene informar que dentro del caso de estudio no se analiza el hecho de que seguramente todos los contadores no puedan ser sustituidos en un ciclo de lectura y poner en marcha los nuevos sistemas. Se presupone que ambas formas de operar se mantendrán de manera conjunta durante un periodo indeterminado de tiempo.

6.1 Definición de requerimientos técnicos

Según el Real Decreto 111/2007 [2], "*El sistema de medidas previsto en el presente reglamento, constituye un elemento básico necesario para el funcionamiento de un mercado abierto y para efectuar la liquidación de la energía, dado que es necesaria la existencia de un sistema que permita la medición de los consumos y de los tránsitos de energía entre los diferentes sujetos y actividades eléctricas*".

Esto implica la necesidad de dotar a los puntos de suministro de unos equipos de medida que cumplan con dichas tareas. Además, como consecuencia de esto, las empresas de distribución eléctrica necesitan desplegar una serie de infraestructuras, software y procedimientos para la correcta utilización de estos equipos.

De acuerdo al ámbito de aplicación y a las definiciones aportadas por el RD 111/2007, el sistema de medidas del sistema eléctrico nacional estará compuesto por los equipos de medida situados en, entre otros lugares, los puntos de conexión de los clientes y los equipos del sistema de comunicaciones, y por los sistemas informáticos que permitan la obtención y tratamiento de la información de medidas eléctricas, incluyendo tanto los dispositivos físicos como los programas que los controlen.

Según las responsabilidades asignadas por el RD 111/2007, "*El operador del sistema es el responsable del sistema de medidas del sistema eléctrico nacional, debiendo velar por su buen funcionamiento y correcta gestión*".

En relación a la empresa IDESA, como operador de la red de distribución en Fuentesur, ésta debe acatar lo dictado en el RD 111/2007, según la Ley del Sector Eléctrico [34] y sus posteriores modificaciones. Por lo tanto, deberá ejecutar la implantación de los siguientes sistemas con sus correspondientes especificaciones técnicas (a parte de los equipos eléctricos):

- Equipo de medida que estará constituido por un contador de energía activa, un contador de reactiva, transformadores de medida y otros dispositivos complementarios que pudieran requerirse, como registradores, elementos de control de potencia, módem y relojes conmutadores horarios.

- Dispositivos de comunicación para la lectura remota de todos los equipos de medida.

- Un canal de comunicaciones apropiado, ya sea a través de un puerto serie RS-232 o un opto-acoplador[27], con las características que establezcan las instrucciones técnicas complementarias.

[27] dispositivo de emisión y recepción que funciona como un interruptor activado mediante la luz emitida por un diodo LED que satura un componente optoelectrónico (Malvino, Albert Paul (2000). Principios de Electrónica. McGraw-Hill/Interamericana de España S. A. U)

- Los equipos de medida deberán disponer de al menos un integrador totalizador o elemento visualizador de la energía circulada que garantice su lectura tras ausencia de tensión de red.

- Se instalarán registradores con carácter general, los cuales podrán estar integrados en un contador combinado o constituir un dispositivo independiente de los contadores. Cada registrador podrá almacenar información de uno o más equipos de medida, con las condiciones que establezcan las instrucciones técnicas complementarias.

- Los equipos básicos tipo 5[28] deberán permitir la discriminación horaria de las medidas, con capacidad para gestionar al menos seis periodos programables.

- Los sistemas de telecontrol y telemedida estarán constituidos por los siguientes elementos:

    - Los equipos de medida y de control (contador, elementos con función de control de potencia, interruptores, displays, etc.), ubicados en el punto de medida

    - El sistema informático de gestión, que gestiona los flujos de información y el funcionamiento de los equipos de medida y control, y el sistema de comunicación entre ambos.

    - Podrán instalarse concentradores intermedios que actúen de enlace entre los equipos de medida y control y el sistema informático de gestión.

Las especificaciones funcionales mínimas de los sistemas de telegestión deberán ser al menos (sin perjuicio de que el encargado de la lectura pueda implementar en el sistema funcionalidades adicionales, y sin entrar en detalle sobre otros sistemas complementarios como puedan ser el acoplamiento de máquinas de cobro con monedas o tarjetas):

- Lectura remota de los registros de energía activa y reactiva, así como de potencia, necesarios para la facturación de las energías y las tarifas, u otros usos que le fueran requeridos, tales como la inclusión en un panel representativo de consumidores.

- Lectura remota de los registros de los parámetros de calidad.

[28] Equipos situados en los puntos de medida tipo 5 según la Ley, siendo estos:

a) Puntos situados en las fronteras de clientes cuya potencia contratada en cualquier periodo sea igual o inferior a 15 kW.

b) Puntos situados en las fronteras de instalaciones de generación cuya potencia nominal sea igual o inferior a 15 kVA.

- Parametrización del equipo de medida de forma remota, incluyendo la configuración de los períodos de discriminación horaria y la potencia contratada.

- Activación del modo de control de la potencia demandada, maxímetro o dispositivo de control de potencia.

- Sincronización periódica remota con los concentradores.

- Control remoto de la potencia: corte y reconexión del suministro, tanto para la gestión de altas y bajas de suministros como para la ejecución de planes de gestión de la demanda.

- Capacidad de gestión de cargas, con el objeto de reducir la demanda en momentos críticos (control remoto del control de la carga).

Tal como se relata en el artículo 5 del RD 111/2007, existirían una serie de exigencias para los sistemas y protocolos de comunicaciones tales como los modos de conexión y los protocolos de información a utilizarse. No existe un amplio detalle definido en cuanto a los requerimientos salvo que "*las propuestas cumplan con los criterios de calidad mínimos para garantizar la funcionalidad y seguridad*" pudiéndose "*utilizar distintos medios físicos de comunicación, tales como RTC, GSM, GPRS, PLC, etc*", siendo los protocolos de comunicación preferentemente públicos.

Queda además declarado que "*El operador del sistema será responsable de definir la red troncal y disponer los medios necesarios para la conexión del concentrador principal a la* misma", y "*El responsable de un equipo de medida lo será también de la instalación, mantenimiento y operación de los equipos de comunicaciones necesarios hasta su conexión a la red troncal o red de acceso según corresponda*".

Cabe destacar, que en el RD 111/2007 también se mencionan el equipamiento y funciones de los concentradores. Se definen para estos un contador principal por operador de red de distribución y concentradores secundarios. En el texto normativo se recogen descripciones acerca de:

- El operador del sistema

  "El operador del sistema será el propietario del concentrador principal y de los concentradores secundarios en caso de existir y de las medidas eléctricas y será responsable de su instalación, mantenimiento y administración"

- La información que han de contener los concentradores

  "El concentrador principal actuará como servidor de datos para todos los puntos de medida cuyo encargado de la lectura sea el operador del sistema. Las instrucciones técnicas complementarias detallarán la información y grado de desagregación que deberá contener.

  …

Los concentradores secundarios del encargado de la lectura actuarán igualmente como servidores de datos en relación con los puntos de medida a él asociados, debiendo recibir la información que se determine en las instrucciones técnicas complementarias."

- Acceso a la información contenida

  "La información relativa a la medida de clientes obtenida por la aplicación de este reglamento tiene carácter confidencial.

  …

  El operador del sistema gestionará el acceso a la información del concentrador principal, de forma que se garantice su confidencialidad

  …

  Los titulares de concentradores secundarios serán plenamente responsables de garantizar la confidencialidad de la información y datos de clientes de que dispongan."

- Canales de comunicación con los usuarios

  "*El acceso de los usuarios a los concentradores principal y secundarios para consulta de datos se realizará mediante los canales de comunicación y procedimientos que establezcan los procedimientos de operación del sistema con objeto de garantizar su seguridad*"

- Periodicidad de las lecturas

  Que será fijada en las especificaciones complementarias.

Si bien en la redacción del RD 111/2007 no se hace referencia a la aplicación de ninguna norma o estándar específicos para la aplicación de criterios de seguridad, en repetidas ocasiones se hace mención a garantizar la operatividad y la seguridad tanto de los sistemas implantados como de los datos que se verán involucrados durante el proceso. Esto, sumado a la necesidad intrínseca de transmitir seguridad a los clientes de cada compañía, hace necesario la aplicación de las mejores prácticas en materia de seguridad para cada una de las soluciones y procedimientos adoptados.

A continuación, para cada parámetro definido en el capítulo sobre la introducción del caso de estudio, con los que justifican una operación segura y para los cuales es necesario aplicar criterios de seguridad, se van a definir una serie de medidas de seguridad relacionadas con cada parámetro. Para cada medida se va a listar la normativa existente en materia de seguridad que le aplica y por último se va a proceder a una definición de los requerimientos técnicos necesarios para desarrollar una solución práctica.

6.1.1 Gestión de procesos con terceros

IDESA necesitaría establecer y mantener unos procedimientos y normas de gestión con terceras partes que se vean involucradas en la provisión de equipos y servicios sea cual sea el grado de éstos, que incluyan acuerdos sobre temas relacionados con la seguridad de los servicios, equipos y sistemas con los que vayan a interactuar dentro de la gestión de la infraestructura de la red de distribución. El alcance para los contratos y acuerdos a establecer también ha de tener en cuenta todos los agentes involucrados en la cadena de suministro tanto de equipos como de servicios.

Tabla 3: Gestión de procesos con terceros

Medida de seguridad	Normativa(s)	Requerimientos técnicos
Acuerdos de confidencialidad con terceros	• NISTIR 7628 - SG.SA-2 • ISO/IEC 27036 - 6.1.1 Acquisition process • ISO/IEC 27002 - 6.2.1 Identification of risks related to external parties	Se deberán tener establecidas una serie de condiciones para los acuerdos de confidencialidad firmados con terceras empresas de proveedoras externas y contratistas. Éstas deberán cumplir con las políticas de organización de IDESA y sus procedimientos de seguridad. IDESA deberá establecer una estrategia de relaciones con los proveedores. Es conveniente antes de firmar un contrato, identificar correctamente los posibles riesgos y establecer controles apropiados antes de conceder accesos.

Medida de seguridad	Normativa(s)	Requerimientos técnicos
Seguimiento de los servicios de terceros	• ISO/IEC 27002 - 10.2 Third party service delivery management • NISTIR 7628 - SG.AU-1 Audit and Accountability Policy and Procedures	IDESA debe revisar la aplicación de los acuerdos, vigilar el cumplimiento de los mismos y gestionar los cambios para asegurarse de que los servicios prestados cumplen con todos los requisitos acordados con los otros agentes implicados. Se deberán además establecer procedimientos y políticas de auditoría y contabilidad seguras y robustas, ya que por los resultados de las mismas se pueden ver implicados personal de la empresa, contratistas y otros agentes.
Existencia de procedimientos de gestión de la información y la infraestructura de soporte (disponibilidad): garantía de continuidad de servicio	• NISTIR 7628 - SG.CP-2 Continuity of Operations Plan • NISTIR 7628 - SG.CP-11 Fail-Safe Response - General Requirement • ISO/IEC TR 27019 - 14.1.1 Including information security in the business continuity management process • ISO/IEC TR 27019 - 14.2.1 Emergency communication	IDESA debería contar con un plan de continuidad de las operaciones en caso de una interrupción en los sistemas de información, además de tener preestablecido un procedimiento de prueba de fallos apropiado en caso de pérdida de comunicación con otros sistemas de información o pérdida del sistema de información de su propia red. Se debe además tener en cuenta el poder garantizar la continuidad del suministro de electricidad (negocio de IDESA) en caso de fallo en los sistemas TIC.

6.1.2 Seguridad específica de los sistemas de información

IDESA deberá establecer de manera regular controles de seguridad y realizar el mantenimiento de los sistemas de información que garantice que estos pueden gestionar los flujos de información de redes de distribución según los nuevos requisitos normativos y deberá asegurarse de que los componentes que las empresas proveedoras le suministren deben tener acceso lógico sólo por entidades autorizadas. De esta manera su información quedará protegida adecuadamente.

Tabla 4: Seguridad específica de los sistemas de información

Medida de seguridad	Normativa	Requerimientos técnicos
Seguridad de los datos y la información: procedimientos y niveles de cifrado	• ISO/IEC TR 27019 - B.1.1.1.6 Encryption of Sensitive Data during Storage and Transmission • ISO/IEC 27002 - 10.7.3 Information handling procedures	Es necesario que IDESA identifique cuáles deben ser los datos sensibles y/o confidenciales. Éstos deberían ser almacenados y transmitidos sólo de forma cifrada. A su vez, los procedimientos para el uso y almacenamiento de la información se deben establecer para proteger la información contra su uso no autorizado.

Medida de seguridad	Normativa	Requerimientos técnicos
Gestión de usuarios	• ISO/IEC 27002 - 11.2 User access management • NISTIR 7628 - SG.AC-3 Account Management - Requirement 1	IDESA cubrirá todas las fases del ciclo de vida del acceso de los usuarios, desde el registro inicial de nuevos usuarios hasta la eliminación de los que ya no requieren acceso a los sistemas y servicios de información. Debe prestarse especial atención, a la asignación de perfiles de acceso y sus privilegios, en especial a aquellos que permiten a los usuarios acceder a los sistemas de control. Las funcionalidades mínimas deberían ser autorizar accesos, activar cuentas a otros usuarios, editar, desactivar y eliminar cuentas.
Control de acceso y Control de acceso remoto	• NERC CIP-003-4 - Requirement 5. Access Control • IEC 62443 - 4.3.3.7.2 Establish appropriate logical and physical permission methods to access IACS devices • NISTIR 7628 - SG.AC-2 Remote Access Policy and Procedures - Requirement 1 • IEC 62443 - 4.3.3.6.6 Develop a policy for remote login and connections	IDESA debe documentar e implementar un programa para la gestión del acceso a la información crítica. El permiso de acceso y el control de los dispositivos del sistema debería ser lógicos (reglas que otorgan o niegan el acceso a los usuarios conocidos basados en sus roles). Se deberán implementar tanto los procedimientos que definan el acceso remoto a los sistemas de información y comunicación como las respuestas del sistema correspondientes a los intentos y los períodos de inactividad de conexión fallidos.

6.1.3 Seguridad de la infraestructura de red y tratamiento derivado de los datos

IDESA deberá establecer y mantener un programa de ingeniería de red segura y una política de gestión de datos que evite que las posibles amenazas eludan los controles de seguridad de que se hayan fijado.

Tabla 5: Seguridad de la infraestructura de red y tratamiento derivado de los datos

Medida de seguridad	Normativa	Requerimientos técnicos
Necesidad de segregación de redes	• ISO/IEC 27002 - 11.4.5 Segregation in networks	IDESA debería mantener una red separada para el sistema de información que gestionan el negocio y con los que establece otras comunicaciones. Deberían quedar claramente definidos los grupos de servicios de información, los usuarios y los sistemas de información deben ser segregados en las redes. Cuando sea técnicamente viable, la infraestructura de red de los sistemas de control de procesos se debe dividir en varias zonas con diferentes funciones.

Medida de seguridad	Normativa	Requerimientos técnicos
Nivel de aseguramiento de la comunicación con la infraestructura de red	• NISTIR 7628 - SG.SC-9 Communication Confidentiality • ISO/IEC 27011 – A.10.6 Network security management • ISO/IEC 27002 - 11.4.7 Network routing control	El sistema de información que se implemente en IDESA debe proteger la confidencialidad de la información transmitida. Además se deberá garantizar la gestión segura de las redes de comunicación, abarcando incluso los ámbitos organizativos, estableciendo un procedimiento de flujo de datos cuidadoso, que cubra aspectos legales, de seguimiento y protección. Se aplicará un control del enrutamiento para garantizar que las conexiones desde el centro de control y los flujos de información no infringen la política de control de acceso de las aplicaciones de negocio.

6.1.4 Auditoría de datos

IDESA debería establecer y mantener un proceso continuo de auditoría que permita el registro en los sistemas de redes inteligentes y que garantice de manera suficiente la validación y veracidad de los datos. Deberá tener asimismo definidos procedimientos que permitan el manejo tanto de los datos como del funcionamiento de los sistemas para posteriores revisiones y evaluaciones.

Tabla 6: Auditoría de datos

Medida de seguridad	Normativa	Requerimientos técnicos
Agregación de los procedimientos de auditoría interna la función de seguridad	• NISTIR 7628 - SG.AU-15 Audit Generation - Requirement 1 • ISO/IEC TR 27019 - 10.10.1 Audit logging	Los sistemas de información deberán proporcionar a IDESA la capacidad de generar registros de auditoría para que esta información pueda ser seleccionada dentro de una la lista de eventos auditables. Los eventos de auditoría pertinentes también pueden incluir algunas acciones no sólo en términos económicos, sino también poder llevarlas a cabo por el personal de operación, tales como los controles sobre los accesos o las operaciones en las infraestructuras.

Medida de seguridad	Normativa	Requerimientos técnicos
Trazabilidad de la información de los sistemas que soportan las infraestructuras eléctricas	• NERC CIP-005-4a - Requirement 3. Monitoring Electronic Access • ISO/IEC 27002 - 10.10 Monitoring	El administrador de sistemas debe implementar y documentar un(os) proceso(s) automático(s) o manual(es) para el seguimiento y registro de accesos a puntos de acceso en el Perímetro de Seguridad de los sistemas que funcione de manera ininterrumpida. Los sistemas deben ser monitorizados y los eventos deben ser registrados. Estos registros deben gestionarse de manera segura y poderse utilizar para identificar posibles problemas en los sistemas.
Protección de la información de las auditorías internas de seguridad	• ISO/IEC 27002 - 10.10.3 Protection of log information • NISTIR 7628 - SG.AU-9 Protection of Audit Information - General Requirement	Los servidores y dispositivos de almacenamiento de la información registrada deben ser protegidos contra la alteración y el acceso no autorizado. Esta información debería estar disponible de manera ininterrumpida para la posible ejecución de auditorías y las herramientas de auditoría deberían permitir la identificación de accesos no autorizados, modificaciones y/o eliminaciones de registros.

6.2 Arquitectura de los sistemas de información, comunicación y otros equipos críticos de la red de energía para el caso planteado

A continuación se va a explicar la composición y arquitectura de los sistemas de información, comunicación y otros equipos críticos de la red de energía para realizar la sustitución de todos los puntos de medición para los clientes localizados en su red de distribución.

En primer lugar se presentará la arquitectura general que se debería desplegar para cumplir con la normativa existente, y posteriormente se describirá cada uno de los elementos y procedimientos de gestión que se implementarán.

Sin entrar en detalle de cuáles son los motivos de la configuración de la red eléctrica de IDESA, y asumiendo que la compañía cumple con la Legislación Nacional y los distintos reglamentos sobre condiciones técnicas y garantías de seguridad en líneas eléctricas de alta tensión, se considera que dentro de su red de distribución eléctrica cuenta con una subestación eléctrica, que permite conectar su red de distribución a la red de transporte de electricidad. Esta subestación eléctrica transforma la tensión eléctrica de las líneas de transporte a una tensión útil para su distribución en la localidad de Fuentesur. Dicha subestación se encuentra a las afueras del municipio dentro un edificio.

Para completar la distribución de electricidad en Fuentesur, IDESA cuenta con otras tres subestaciones secundarias, que permiten reducir los niveles de tensión hasta los adecuados para su distribución final a los hogares del municipio. Todos los clientes con los que cuenta IDESA dentro del municipio se encuentran a menos de un kilómetro de distancia de alguna de estas tres subestaciones. Como se podrá ver más adelante, dentro de las mismas se ubicarán los concentradores de datos.

6.2.1 Arquitectura general

Muchas son las empresas que ya están desarrollando soluciones para el cumplimiento de la normativa relativa al Reglamento unificado de puntos de medida del sistema eléctrico, cumpliendo con lo dictado en la ORDEN ITC/3022/2007 [3], y están realizando los despliegues necesarios.

Según dicha orden, en relación al punto 3 de su artículo 2, "*se denomina sistema de telegestión a un sistema de medida y comunicación bidireccional entre los contadores y suministradores eléctricos que, con las máximas garantías de integridad y seguridad, permite acceso remoto a los contadores de energía eléctrica, con disponibilidad de lectura, gestión de la energía, control de la potencia demandada y contratada, gestión de la conexión/desconexión de suministros y mecanismos antifraude avanzados, posibilitando el intercambio de información y actuaciones entre los sistemas de las empresas distribuidoras eléctricas y contadores.*"

Realizando un desglose a alto nivel de los componentes que estos despliegues tienen, y que también el despliegue que realice IDESA debe tener, se identifica que es necesario:

- dotar a los puntos finales de los equipos de medida adecuados y que éstos tengan las especificaciones técnicas requeridas por la legislación,
- desplegar una red de comunicaciones que permita tanto la transmisión de los datos recogidos en los equipos de medida como el control sobre los mismos por parte de los operadores, e,
- incluir dentro del centro de control los sistemas que permitan la gestión de toda la infraestructura.

La Figura 18 muestra como ejemplo de arquitectura general necesaria a desplegar para la implantación de los equipos de medida planteada por la iniciativa "Meters & More"[29]. El sistema planteado en esa figura podría dar soporte tanto al despliegue de todos estos equipos de medida como para que IDESA pueda tratar la información recogida a través de la lectura sobre los mismos y realizar la operación requerida según la normativa vigente.

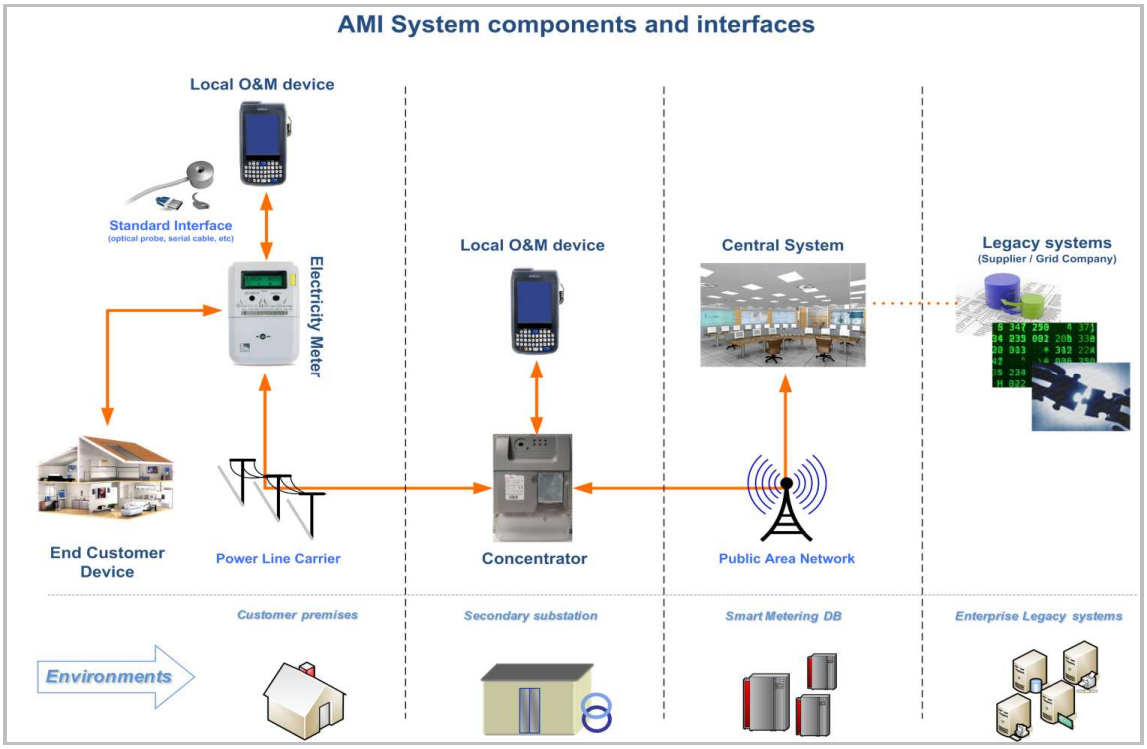

Figura 18: Arquitectura general de la solución necesaria para la implantación de los equipos de medida.
Fuente: http://www.metersandmore.com/technology/ [35]

[29] "Meters & More" es una tecnología desarrollada por Enel para los despliegues de Smart Grids, abierta, interoperable, en proceso de estandarización a nivel europeo puesta a disposición de las empresas del sector sin ánimo de lucro.

Pero la solución escogida para IDESA se aproximaría más a los estándares de tecnología PRIME [36][30], en la cual se especifica una arquitectura de última milla soportada mediante tecnología PLC. Esta elección evitaría desplegar una red de comunicaciones de manera paralela desde el centro de control o los concentradores de datos hasta los equipos de medición situados en la localización de cada uno de los clientes, puesto que las comunicaciones se realizarían a través de la propia infraestructura eléctrica desde los clientes finales hasta un punto de concentración de datos donde se canalizaría la comunicación con el centro de control a través de líneas de ADSL.

Así pues, los siguientes elementos que configuran la solución se desarrollarán durante las siguientes subsecciones:

- Equipos contadores
- Concentradores de datos
- Equipos centrales para el procesado de datos
- Infraestructura de red de comunicaciones
- Procedimientos de gestión y mantenimiento de datos

6.2.2 Equipos contadores

Los equipos de medida para el consumo de electricidad, han de cumplir con la normativa establecida en la ORDEN ITC/3022/2007 [3].

Estos equipos, según las especificaciones técnicas, deberán incorporar las siguientes funciones: "*con disponibilidad de lectura, gestión de la energía, control de la potencia demandada y contratada y gestión de la conexión/desconexión de suministros y mecanismos antifraude avanzados, posibilitando el intercambio de información y actuaciones entre los sistemas de las empresas distribuidoras eléctricas*".

Además de esta normativa, estos dispositivos, junto a la infraestructura de telegestión, en relación a la información entre usuarios y empresa suministradora de electricidad *deben garantizar una mayor rapidez, eficiencia y facilidad de relación entre el proveedor de electricidad y los cliente[55]*.

En la actualidad existen distintos dispositivos comerciales. En la Figura 19, se muestra un contador de electricidad para hogares, que podría ser perfectamente instalado en los puntos de suministro de IDESA y que ha sido desarrollado por un fabricante industrial de componentes eléctricos.

[30] PoweRline Intelligent Metering Evolution, tecnología utilizada por varias compañías de distribución, como Iberdrola, con la intención de desarrollar una infraestructura AMI de telegestión de contadores de carácter pública, abierta y estándar.

Figura 19: Contador residencial para compañías de distribución.
Fuente: Documento [38]. Soluciones para la gestión PRIME, Circuitor

Según sus especificaciones técnicas, el nivel de seguridad de datos se corresponde con Categoría III (110 V) según EN-61010. Esto quiere decir que según la Comisión Electrotécnica Internacional cumple con las necesidades para la adquisición de datos en distribución eléctrica. Sin entrar en mayor detalle, se considera por tanto, que los datos obtenidos son fiables.

Debe contar con un puerto que permita la conexión a la red de comunicaciones. Según especificaciones técnicas este modelo permitiría tanto la conexión a través de PLC como a través de un puerto óptico, pudiendo configurarse los protocolo de comunicación DLMS (IEC 62056 - Device Language Message Specification) / OFDM (Orthogonal Frequency Division Multiplexing), ambos de forma bidireccional, lo cual permite transmitir los datos desde el dispositivo hasta localizaciones externas, y también recibir comunicación para su telecontrol. Por otra parte, también cuenta con una memoria interna que permite almacenar hasta tres meses los registros horarios obtenidos.

Para poder garantizar un comportamiento seguro de acuerdo al caso de estudio planteado, los equipos de medidas eléctricas deberían cumplir con los requerimientos técnicos de:

- Existencia de procedimientos de gestión de la información y la infraestructura de soporte (disponibilidad): garantía de continuidad de servicio
- Seguridad de los datos y la información: procedimientos y niveles de cifrado
- Control de acceso y control de acceso remoto

6.2.3 Concentradores de datos

En comunicaciones, un concentrador de datos es un equipo de la red de comunicaciones que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás.

Dentro de la orden ORDEN ITC/3022/2007 [3], se diferencian dos tipos de concentradores: los Concentradores CT, y los concentradores secundarios. Según la definición recogida en la estructura del sistema de telegestión establecida en la orden se especifica:

"Concentradores CT: se comunicarán remotamente con los concentradores secundarios por la red de acceso, utilizando distintos medios de comunicación; y con los contadores, fundamentalmente mediante PLC. Su ubicación topológica natural es el centro de transformación.

Concentradores secundarios: se comunicarán con el concentrador principal por la red troncal."

Debido a la topología de los clientes y de la estructura de negocio, se va a considerar que IDESA se conecta directamente a los contadores que desplegará con concentradores de datos a través de PLC, aprovechando la infraestructura de cables eléctricos con los que cuenta la compañía desde los puntos de suministro eléctrico de los clientes hasta las subestaciones de electricidad que disponen. Por lo tanto, a efectos de normativa son "Concentradores CT". A su vez, éstos serán conectados directamente con el centro de control de la compañía a través de líneas ADSL, no siendo necesaria la conexión de "Concentradores secundarios".

En el mercado existen varios equipos que se comercializan con el fin de dar este servicio de concentrador de datos. Por ejemplo, el que aparece en la Figura 20, de la marca Circuitor, permite la conexión de datos de 2.000 equipos de medida distintos mediante PLC y su comunicación con el centro de control a través de distintos canales de comunicación: ADSL, GPRS/UMTS o PLC de banda ancha. Otros equipos también pueden soportar la conexión a través de WIMAX.

Figura 20: Concentrador de datos
Fuente: Documento[37]. Circuitor

De acuerdo a la conexión para la comunicación de estos equipos con el centro de control, cada una de las posibles opciones tendría sus particularidades. En la Figura 21, se pueden observar las distintas opciones tecnológicas que podrían utilizarse con el concentrador de datos presentado anteriormente.

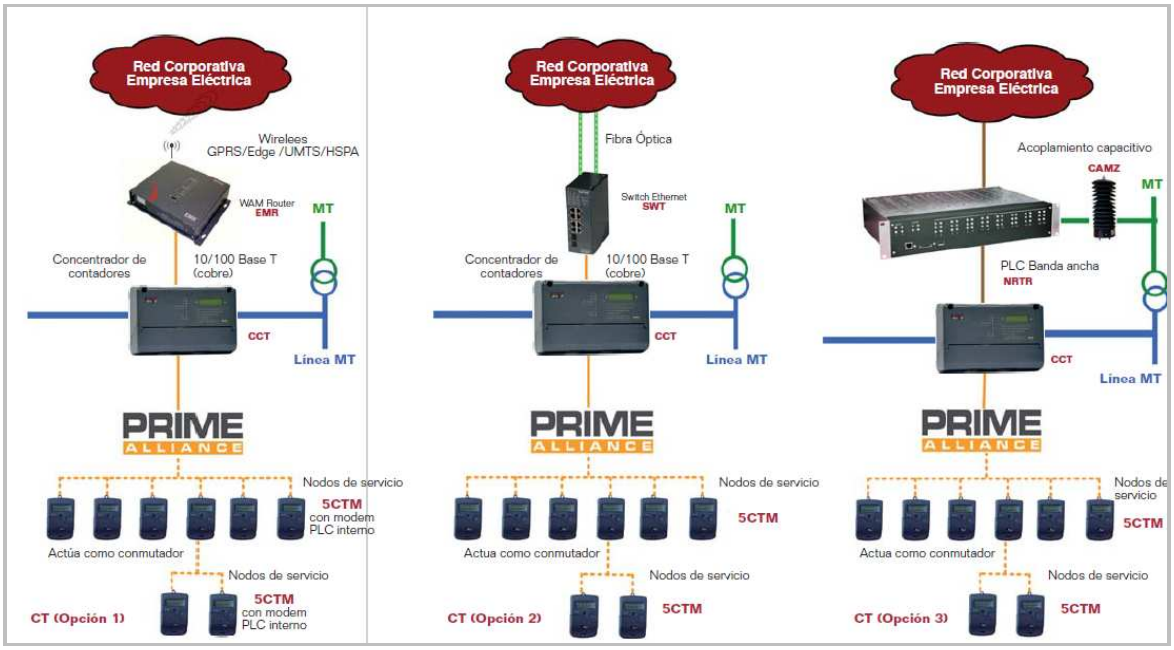

Figura 21: Arquitecturas posibles para la conexión del concentrador de datos
Fuente: Documento[37]. Circuitor

De acuerdo a lo indicado en el comienzo del presente apartado, IDESA podría llegar a cubrir los contadores colocados en todos sus clientes (10.000), con tan sólo cinco de estos dispositivos, y de esta manera podría transmitir desde los mismos la información de las medidas al centro de control.

Esta configuración se podría llevar a cabo siempre y cuando la distancia desde cada uno de los clientes esté dentro de la zona de recepción de información de estos equipos. En caso de que por problemas de topología en la distribución de sus clientes no pudieran llegar a conectarse 2.000 en cada uno de los concentradores de datos, sería necesario incorporar alguno de manera adicional.

Estos equipos estarían colocados dentro de los edificios e instalaciones donde se encuentren las subestaciones eléctricas de que dispone la compañía dentro de su red de distribución.

Para poder garantizar un comportamiento seguro de acuerdo al caso de estudio planteado, el dispositivo concentrador de datos debería cumplir con los requerimientos técnicos de:

- Existencia de procedimientos de gestión de la información y la infraestructura de soporte (disponibilidad): garantía de continuidad de servicio
- Seguridad de los datos y la información: procedimientos y niveles de cifrado
- Control de acceso y control de acceso remoto
- Necesidad de segregación de redes
- Nivel de aseguramiento de la comunicación con la infraestructura de red

6.2.4 Equipos centrales para el procesado de datos

El centro de control de IDESA debe ser capaz de procesar los datos que le llegan desde todos sus clientes. Para ello, se deben emplear sistemas SCADA para redes de distribución y que permitan recepción de datos, acceso a redes de información bidireccionales y control sobre equipos remotos.

ABB, una de las principales empresas de fabricación de equipos industriales incluyó dentro de su publicación sectorial Revista ABB 3/2009 [40], un artículo sobre "Gestión de redes para la red de distribución". En la introducción de este artículo se incluían el siguiente párrafo:

"A medida que los sistemas de distribución evolucionan y se convierten en sistemas de distribución inteligentes, los centros de operaciones que los controlan están evolucionando para adoptar funciones nuevas para gestionar dichas redes. Los distintos sistemas de TI (Tecnologías de Información) utilizados en esos centros de control se están simplificando y se comunican con fluidez para proporcionar un sistema integrado de vigilancia y gestión. Las aplicaciones y el software analítico más avanzados están proporcionando análisis más sofisticados y operaciones automatizadas. Los sistemas de control de los centros de operaciones ayudan no sólo a que la red sea más inteligente sino también a mejorar el apoyo a los decisores responsables de las operaciones, el mantenimiento y la planificación. Dichos centros de operaciones integrados ayudan a las organizaciones de distribución a alcanzar sus objetivos a pesar de las dificultades crecientes."

En este caso, los objetivos que debe buscar IDESA, son poder llevar a cabo la telegestión de manera correcta según lo indicado en la ORDEN ITC/3022/2007 [3], y poder realizarla de manera segura.

El centro de control deberá por lo tanto incluir sistemas que permitan la recepción de los datos, su almacenamiento y disposición para ser utilizados por otras unidades de la red empresarial, tales como contabilidad (para facturación), disposición de datos a entidades externas (a disposición de las comercializadoras de electricidad), trazabilidad de los datos para posibles controles y auditorias, etc.

Por otro lado, debe existir una aplicación que permita las funciones de control sobre los dispositivos distribuidos, tanto de los equipos contadores, como de los equipos de comunicaciones. Este control se hace a través de sistemas SCADA. Ya se presentó en el apartado 2.4 la descripción de un ejemplo de cómo son los SCADA dentro del sector eléctrico. La operativa del centro de control que tendría que incluir IDESA dentro de sus instalaciones deberá pues garantizar una operativa de telegestión sobre los contadores.

Para esta operativa deben disponer o incorporar en caso de ser necesario equipos de almacenamiento de datos, aplicaciones que dispongan de una interfaz gráfica adecuada, permitan el acceso a la información de los equipos de medida en tiempo real, y la configuración de unos sistemas de alarmas que indiquen situaciones de funcionamiento incorrecto.

Además, el SCADA deberá comunicarse con otros sistemas de negocio dentro de la empresa. En la Figura 22 se muestra un ejemplo de arquitectura de un centro de operaciones totalmente integrado de una red de distribución eléctrica.

También, dentro del centro de control de IDESA se debe disponer de una serie de sistemas que aparte de la telegestión de los equipos de medida tal y como indica la ORDEN ITC/3022/2007 [3], permitan tener estos datos a disposición para:

1. por un lado su gestión interna dentro de otros posibles departamentos de la empresa aparte del de operación: contabilidad, marketing y estrategia, etc, y,
2. por otro facilitárselo a terceros agentes tales como los consumidores, empresas de comercialización de electricidad, empresas proveedoras de servicios, entidad reguladora del mercado, etc.

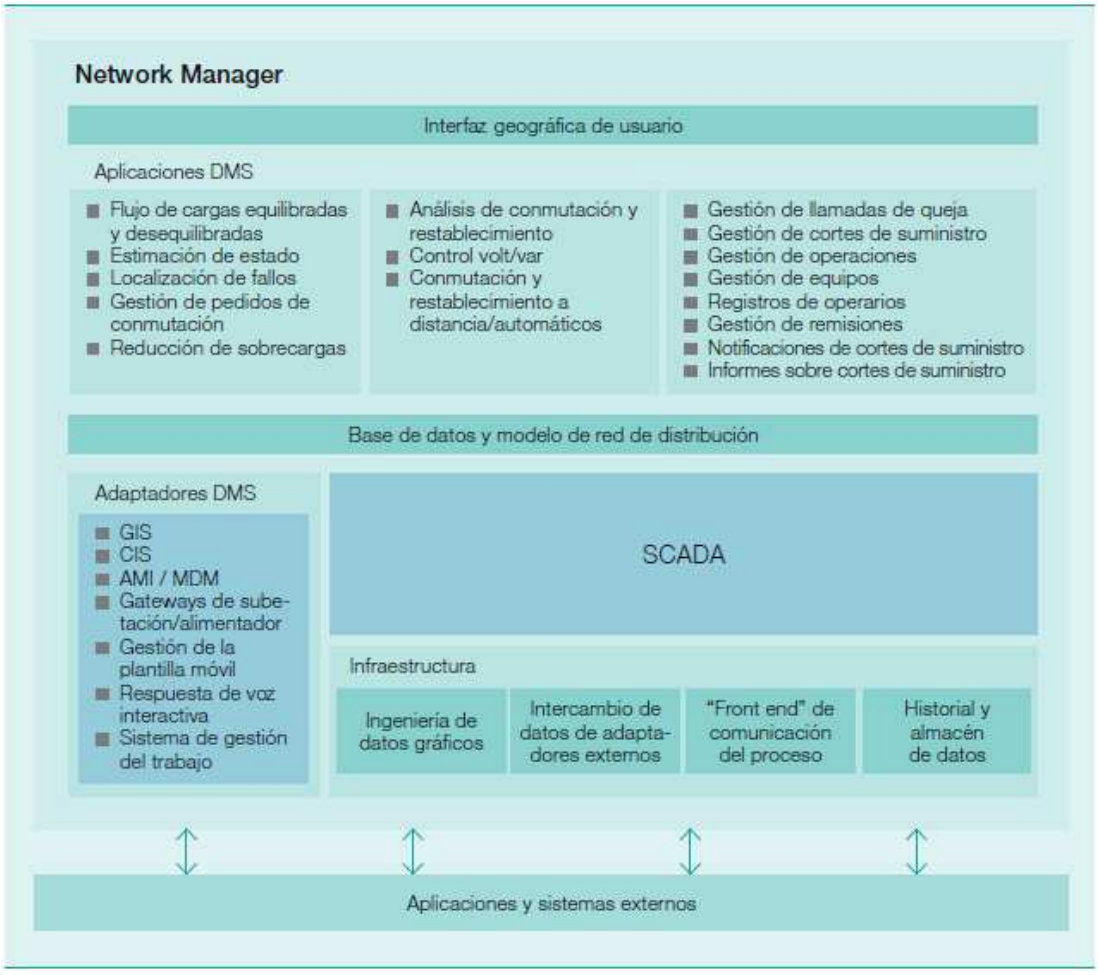

Figura 22: Arquitectura de un centro de operaciones totalmente integrado de una red de distribución eléctrica
Fuente: Documento[40]. Revista ABB 3/2009

Para su correcta operación, IDESA deberá contar con personal cualificado capaz de operar la funcionalidad que se implemente dentro de SCADA. Las principales soluciones tecnológicas de SCADA para la telegestión de equipos de medida ofrecen estas prestaciones.

Para poder garantizar un comportamiento seguro de acuerdo al caso de estudio planteado, los equipos para el procesado de datos con los que IDESA tendría que contar dentro de su centro de control y que posteriormente conecten con la red corporativa, deberían cumplir con los requerimientos técnicos de:

- Existencia de procedimientos de gestión de la información y la infraestructura de soporte (disponibilidad): garantía de continuidad de servicio
- Seguridad de los datos y la información: procedimientos y niveles de cifrado
- Gestión de usuarios
- Control de acceso y Control de acceso remoto
- Necesidad de segregación de redes
- Nivel de aseguramiento de la comunicación con la infraestructura de red
- Agregación de los procedimientos de auditoría interna la función de seguridad
- Trazabilidad de la información de los sistemas que soportan las infraestructuras eléctricas
- Protección de la información de las auditorías internas de seguridad

6.2.5 Infraestructura de red de comunicaciones

Como ya se ha descrito anteriormente, para la transmisión de la información necesaria para enviar las mediciones de los equipos contadores y su telegestión, es necesario un canal de la comunicación entre los contadores y el centro de control. Para poder satisfacer una comunicación segura, ésta se realizaría en dos segmentos:

1. El primero, desde los equipos de medida hasta los concentradores de datos, que se realizaría por tecnología PLC, usando como medio físico la propia red de distribución de cableado eléctrico de la empresa.
2. El segundo, desde los concentradores de datos hasta el centro de control, a través de conexiones ADSL. Para esto, se espera que desde cada concentrador de comunicaciones existirá una línea de conexión a internet que permitirá la comunicación de los datos llegados a los concentradores desde éstos hasta el centro de control.

En la Figura 23 se muestra una posible arquitectura de la infraestructura de comunicaciones comparada con la arquitectura OSI[33].

[33] El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), también llamado OSI (en inglés, Open System Interconnection 'sistemas de interconexión abiertos') es el modelo de red descriptivo, que fue creado por la Organización Internacional para la Estandarización (ISO).

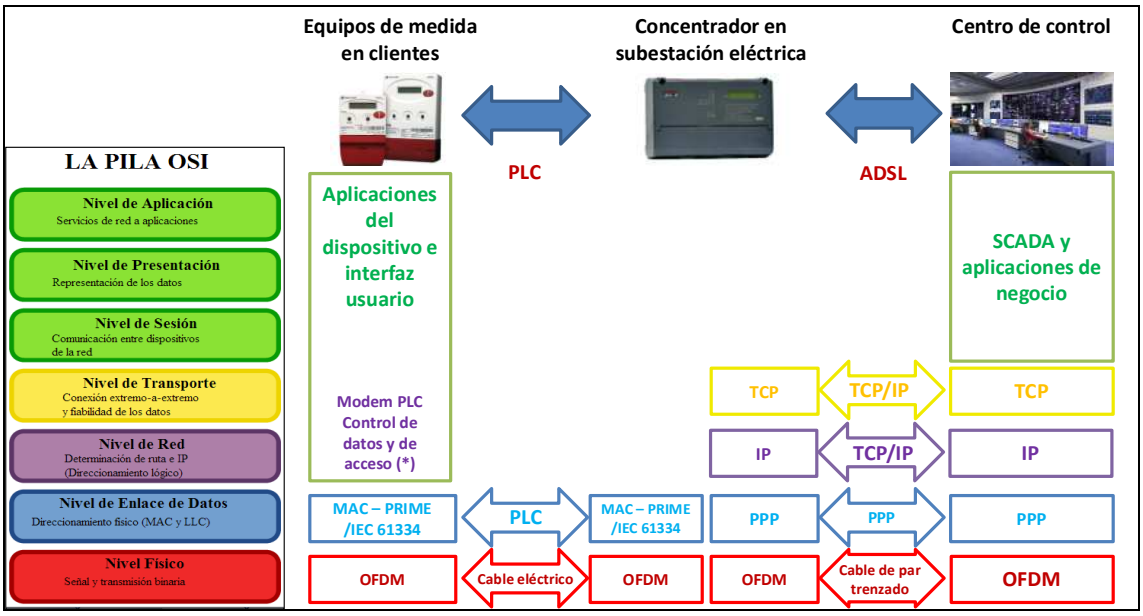

Figura 23: Arquitectura de la infraestructura de comunicaciones
Fuente: Elaboración propia

A continuación se describen en líneas generales las características de cada una de estas tecnologías para redes de comunicaciones y cómo se implementarían de manera específica con el fin de poder satisfacer las necesidades de una empresa como IDESA.

PLC, tal y como se indicó en el apartado 2.3, se refiere a tecnologías diferentes que utilizan las líneas de energía eléctrica convencionales para transmitir señales de radio para propósitos de comunicación.

La tecnología PLC aprovecha la red eléctrica para convertirla en una línea digital de alta velocidad de transmisión de datos, permitiendo, entre otras cosas, el acceso a Internet mediante banda ancha.

Actualmente, los dispositivos comerciales para la comunicación a través de PLC utilizan multiplexación en frecuencia (OFDM[34]) y aprovechar mejor el ancho de banda disponible. Con esta tecnología, la capacidad de transmisión de las líneas de PLC de 2ª generación es de más de 130 Mb/s totales, que pueden programarse para ser distribuidos de manera bidireccional[35].

---

http://en.wikipedia.org/wiki/OSI_model

[34] La Multiplexación por División de Frecuencias Ortogonales, en inglés Orthogonal Frequency Division Multiplexing (OFDM), o Discrete Multi-tone Modulation (DMT) es una multiplexación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o en PSK.

[35] La tecnología PLC en los Programas de Fomento de la Sociedad de la Información de Red.es (Power Line Communication Technology in the Information Society Promotion Programs Managed by Red.es) J. R. González Puyol y F. J. García Vieira

Esta solución permitiría la comunicación desde los equipos de medida hasta los concentradores de datos mediante tecnología PLC, usando como medio físico la propia red de distribución de cableado eléctrico de la empresa utilizando bien el protocolo de comunicación IEC 61334 o bien soluciones propietarias de los equipos seleccionados para su instalación.

En ambos casos hay que tener en cuenta que los equipos de medida como el concentrador de datos deben ser capaces de transmitir a través de estos protocolos.

En la Figura 24 se muestra un ejemplo de cómo implementar la arquitectura para acceder a la red de comunicación desde la zona de control de datos y como realizar una gestión de los mismos. Es la solución propuesta por la tecnología PRIME. En el documento Draft Specification for PoweRline Intelligent Metering Evolution, además de este modelo, se desarrolla un algoritmo para optimizar el acceso al medio de los dispositivos a las líneas de PLC. Éste queda descrito en su capítulo "4.3.3.3.2 CSMA-CA algorithm".

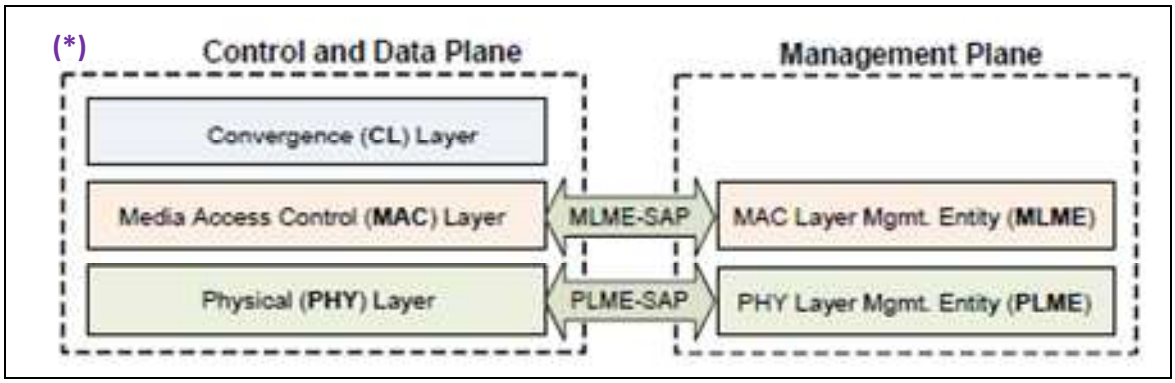

Figura 24: Modelo de referencia para el control de OFDM en la especificación PRIME
Fuente: Draft Specification for PoweRline Intelligent Metering Evolution

Para la comunicación de los equipos concentradores de datos hasta el centro de control que tiene IDESA, según la hipótesis planteada en el capítulo 1, en la que el centro de control no se encuentra en una ubicación cercana, una solución adecuada sería la utilización de líneas ADSL. Estas líneas ADSL sería contratadas a un proveedor de servicios de comunicaciones.

En la arquitectura presentada, se plantea la transmisión a través cable de par trenzado utilizando Ethernet o cualquiera de sus versiones como protocolo de acceso al medio. Esta configuración podría variarse en función de la que pudiese establecer la compañía proveedora de servicios de comunicaciones.

Como alternativa a la arquitectura que se plantea, podría definirse otra a partir de tecnologías propietarias, tal y como realizan otras compañías de distribución eléctrica en la plataforma "Meters and More" (ver Figura 25).

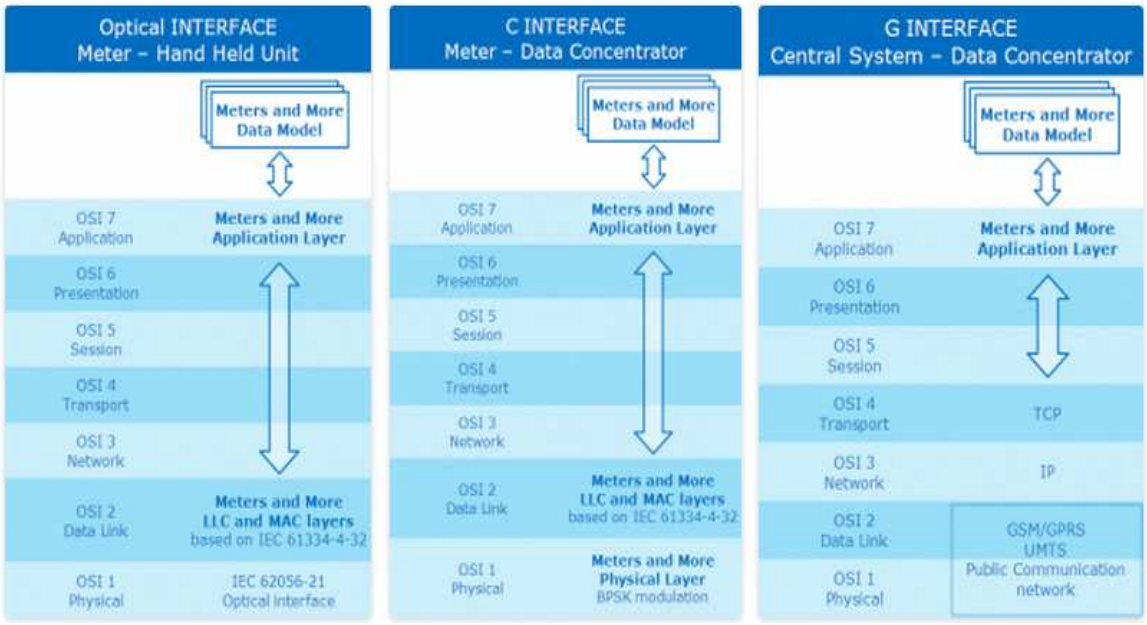

Figura 25: Modelo de arquitectura propietaria para Smart Metering de la iniciativa "Meters and More"
Fuente: http://www.metersandmore.com/technology/

En cualquier caso, para poder garantizar un comportamiento seguro de acuerdo al caso de estudio planteado, la infraestructura de red de comunicaciones que IDESA tendría que desplegar para la comunicación con los dispositivos distribuidos deberían cumplir con los requerimientos técnicos de:

- Existencia de procedimientos de gestión de la información y la infraestructura de soporte (disponibilidad): garantía de continuidad de servicio
- Seguridad de los datos y la información: procedimientos y niveles de cifrado
- Necesidad de segregación de redes
- Nivel de aseguramiento de la comunicación con la infraestructura de red

6.2.6 Procedimientos de gestión (datos y mantenimiento)

Los procedimientos de gestión que van asociados a la arquitectura de los sistemas de información, comunicación y otros equipos pueden referirse a los accesos a equipos de medida y concentradores de datos, mantenimiento de la infraestructura eléctrica, acceso a los sistemas de control y los datos generados, revisión de tareas a través de auditorías, etc.

Con el fin de establecer criterios comunes a la normativa analizada y poder estudiar de manera específica el caso de estudio planteado, los procedimientos de gestión que se van a considerar dentro de la arquitectura son:

- Estrategia de relaciones con los proveedores y contenido específico de los contratos con terceras empresas, proveedoras externas y contratistas.

  Es necesario que todas las unidades de negocio tenga en cuenta que a la hora de realizar una subcontratación es necesario incluir en los contratos las cláusulas de confidencialidad e indemnidad que permitan garantizar el cumplimiento de las especificaciones de seguridad mínimas que aseguren integridad de la información, confidencialidad de los datos y trazabilidad de las operaciones realizadas sobre los dispositivos y la información contenida.

- Plan de seguimiento de servicios prestados: ya sea con los proveedores, o los servicios que IDESA ofrece a sus clientes.

  Por un lado, una vez contratados los servicios de empresas de proveedores de servicios, es necesario que en IDESA se establezcan las personas encargadas del seguimiento de los trabajos por parte de terceros y una serie de procedimientos de control y registro de las tareas realizadas.

  Los equipos de medida instalados en los clientes deben ofrecer tanto una garantía de funcionamiento suficiente como un cierto nivel de seguridad en el acceso ante posibles manipulaciones, bien sea por los propios clientes o bien por otros agentes, pudiendo evitar manipulaciones no deseadas, provocando distorsión de la información, robo de la misma siendo ésta sensible, o fraudes.

- Procedimientos y políticas de auditoría y contabilidad seguras y robustas, ya que por los resultados de las mismas se pueden ver implicados personal de la empresa, contratistas y otros agentes.

  Es necesario que esté documentado todo el flujo de información así como la localización de la misma para eventuales procedimientos de auditoria, ya sea de funcionamiento/técnica, de revisión de datos o contable

- Plan de continuidad de las operaciones: en caso de una interrupción en los sistemas de información, además de tener preestablecido un procedimiento de prueba de fallos apropiado en caso de pérdida de comunicación con otros sistemas de información o pérdida del sistema de información de su propia red.

IDESA debe garantizar cierto grado de resiliencia de su red de comunicaciones.

- Plan de continuidad del suministro de electricidad.

  Independientemente del funcionamiento de la infraestructura de comunicación, es imprescindible garantizar con la máxima fiabilidad y continuidad el suministro de energía eléctrica, puesto que es el negocio de IDESA. Los niveles de calidad en su operación se miden en tiempos de energía no suministrada[36].

Para poder garantizar un comportamiento seguro de acuerdo al caso de estudio planteado, los procedimientos de gestión seleccionados que IDESA deberían implementar dentro de las funciones de su compañía con el fin de poder dar soporte desde los centros de control a la nueva infraestructura desplegada deberían cumplir con los requerimientos técnicos de:

- Acuerdos de confidencialidad con terceros
- Seguimiento de los servicios de terceros
- Existencia de procedimientos de gestión de la información y la infraestructura de soporte (disponibilidad): garantía de continuidad de servicio
- Gestión de usuarios
- Agregación de los procedimientos de auditoría interna la función de seguridad
- Trazabilidad de la información de los sistemas que soportan las infraestructuras eléctricas
- Protección de la información de las auditorías internas de seguridad

[36] La calidad de servicio viene configurada por el siguiente contenido[64]:

- Continuidad del suministro, relativa al número y duración de las interrupciones del suministro.
- Calidad del producto, relativa a las características de la onda de tensión.
- Calidad en la atención y relación con el cliente, relativa al conjunto de actuaciones de información asesoramiento, contratación, comunicación y reclamación.

6.3 Soluciones propuestas para cada medida de seguridad

A continuación se presentarán las soluciones necesarias para que la empresa IDESA pueda instalar y poner en marcha los equipos de medida de acuerdo a la legislación existente. Las soluciones a implementar están orientadas al cumplimiento de la mayor parte posible de los requerimientos de seguridad definidos en el apartado 6.1 implementando la arquitectura descrita en el apartado 6.2.

6.3.1 Gestión de procesos con terceros

Para una empresa como IDESA, los terceros serían todos aquellos agentes que tienen relación con alguna de las partes de su negocio. De acuerdo a las particularidades del negocio de distribución de electricidad y todo lo relacionado con la implantación de la nueva infraestructura, éstos serían:

1. Empresas que pudieran dar el servicio de mantenimiento de los contadores, concentradores y la infraestructura de red de comunicaciones.

   La realización de estas tareas puede llevarse a cabo de dos maneras, desde dentro de IDESA, siempre y cuando cuenten con personal especializado, o a través de empresas proveedoras de servicios.

2. Clientes. Desde la instalación de los nuevos contadores, los usuarios tienen que ser capaces de ver en tiempo real los consumos que están teniendo y esto sólo se puede hacer a través de acceso a la información que provee el contador.

   IDESA puede facilitar el acceso y la disponibilidad de estos datos a los usuarios a través de una plataforma web sin acceder directamente a los datos y al control del contador. La información recogida en las lecturas y guardada dentro de bases de datos en los servidores de información (de la compañía o externos) podría estar disponible para los clientes a través de consultas. En la actualidad otras empresas de distribución eléctrica ya ofrecen este servicio.

3. Empresas comercializadoras. Los clientes no realizan la contratación de la compra de electricidad a la empresa distribuidora de su zona, sino que lo hacen de manera liberalizada a través de empresas de comercialización eléctrica[37], que son quienes compran y venden la energía a los clientes finales, utilizando las redes de transporte y distribución para su suministro.

[37]Comercializador eléctrico: Tal como indica la legislación vigente, [64] se entiende por comercializadores de energía eléctrica a toda sociedad mercantil debidamente inscrita en el registro correspondiente o equivalente en su país de origen que accediendo a las redes de transporte o distribución tiene como función la venta de energía eléctrica a los consumidores o a otros sujetos del sistema. Esta actividad se encuentra regulada en los artículos 70 a 74 del Real Decreto 1955/2000 [63], por el que se regulan las actividades de transporte, distribución, comercialización, suministro y procedimientos de autorización de energía eléctrica, modificado por el Real Decreto 198/2010, de 26 de febrero.

Estas empresas han de conocer toda la información de consumo de cada uno de sus clientes para poder realizar correctamente la facturación de este consumo a los mismos. La información de cada cliente ha de ser suministrada a cada comercializador de manera adecuada.

4. REE, empresa de Transmisión de energía eléctrica. Si bien REE es una empresa involucrada en las actividades de negocio de IDESA puesto que tiene que suministrar la electricidad desde los generadores en alta tensión hasta la red de IDESA, su relación se ve directamente afectada por los nuevos contadores.

Con el fin de poder llevar a cabo una gestión segura de procesos con terceros es necesario que se desarrollen una serie de soluciones que permitan cumplir con las medidas de seguridad mencionadas en el apartado 0 . Estas medidas de seguridad son:

- Acuerdos de confidencialidad con terceros
- Seguimiento de los servicios de terceros
- Garantía de continuidad de servicio

6.3.1.1 Acuerdos de confidencialidad con terceros

Con todos los agentes descritos anteriormente, bien sea desde una posición de provisión del servicio de distribución de electricidad, como empresa contratante de servicios a terceros, o como de relación de negocio con REE o las comercializadoras, IDESA debe firmar acuerdos de confidencialidad que garanticen que la información que se encuentre en su bases de datos, sea leída de los contadores o se encuentre en tránsito por las redes de comunicaciones no será utilizada de manera indebida.

Según la web modelodecontrato.net [65], los acuerdos de confidencialidad incluirán:

- ***Consideraciones****. Las consideraciones son todo aquello a lo que hace relación el contrato de confidencialidad. Es decir, la información, negocio, proyecto o desarrollo tecnológico, entre otros aspectos.*
- ***Cláusulas****. Son todas las especificaciones que queramos incluir dentro del contrato y que definen sus condiciones. Normalmente se suelen tratar aquí las partes, definiciones, excepciones, posibles sanciones y los plazos. Leer más sobre las cláusulas del contrato de confidencialidad.*

Las cláusulas que IDESA debería incluir son las siguientes::

- **Partes afectadas**: descripción legal de IDESA y terceros.
- **Definición de confidencial**: desarrollando al máximo los contenidos que queremos que queden sujetos a confidencialidad.
- **Excepciones**: aludiendo a aquellos casos en los que es posible romper la confidencialidad.

- **Sanciones**: debe incluirse las normas legales o la jurisdicción a la que se someten ambas partes en caso de conflicto.

- **Plazo**: tiempo a partir del cual ambas partes quedan exonerados del cumplimiento de la confidencialidad.

6.3.1.2 Seguimiento de los servicios de terceros

Las actividades que garanticen la seguridad y la confidencialidad del tratamiento de los datos requerirán por parte de IDESA un procedimiento de seguimiento y control de los servicios provistos a través de un conjunto de acciones que se llevarán a cabo para la comprobación de la correcta ejecución de las actividades de los servicios provistos.

El instrumento fundamental para ejecutar esta medida con éxito es el **Informe de Seguimiento.** Este informe será una fuente de información básica para el conocimiento del progreso de los servicios por parte del Comité de Seguimiento o de la persona encargada del mismo y una herramienta para la supervisión y monitorización de los servicios. Se elaborará según una plantilla y con suficiente frecuencia para garantizar una adecuada operativa.

El propósito final que debe guiar este seguimiento es proporcionar un entendimiento del progreso del proyecto, de forma que se puedan tomar las acciones correctivas apropiadas cuando la ejecución del proyecto se desvíe significativamente de su planificación.

Este seguimiento deberá incluir una serie de actividades tales como:

- Elaboración del Informe de Seguimiento

- Convocatoria de la reunión de seguimiento

- **Reunión de seguimiento**

- Elaboración del **Acta** de Reunión y/o actualización del Informe de Seguimiento

- Envío del Acta de Reunión e Informe de Seguimiento

- Revisión y validación del Acta de Reunión e Informe de Seguimiento

- Actualización del Informe de Seguimiento y/o Acta de Reunión

- Aprobación del Acta de Reunión e Informe de Seguimiento

6.3.1.3 Garantía de continuidad de servicio

La continuidad del servicio se preocupa de impedir que una imprevista y grave interrupción de los servicios, debido a desastres naturales u otras fuerzas de causa mayor, tengan consecuencias catastróficas para el negocio.

La estrategia de la Gestión de la Continuidad del Servicio debe contar con procedimientos[38]:

- **Proactivos**: que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- **Reactivos**: cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

De manera proactiva, se deberían poder tener para los Sistema de comunicación de emergencia: líneas de telefonía móvil dentro del centro de control.

Como procedimiento de recuperación, sería necesario que para equipos de medida, infraestructura de comunicaciones y del propio centro de control se configurasen sistemas "*Cold standby*"[39] de manera que IDESA en caso de fallo grave, pudiese sustituir los equipos para que se pueda reproducir en un corto espacio de tiempo su producción y el servicio.

6.3.2 Seguridad específica de los sistemas de información

Los sistemas de información que se desplieguen han de contener una seguridad específica. Con el fin de poder garantizar una seguridad mínima de los sistemas de información existentes en la configuración planteada en el apartado 6.2 Arquitectura de los sistemas de información, comunicación y otros equipos críticos de la red de energía para el caso planteado, es necesario que se desarrollen una serie de soluciones que permitan cumplir con las medidas de seguridad mencionadas en el apartado 6.1.2 Seguridad específica de los sistemas de información. Estas medidas de seguridad son:

- Seguridad de los datos y la información
- Gestión de usuarios
- Control de acceso y control de acceso remoto

[38] OSIATIS S.A. – Gestión de la Continuidad de Servicio - www.osiatis.es [66]

[39] Se refiere a sistema "Cold standby" todo aquel que se encuentra parado y sin uso hasta que debido a una incidencia son activados y utilizados.

6.3.2.1 Seguridad de los datos y la información

Si bien durante la transmisión de la información desde los contadores al centro de control y viceversa, no se envía información de carácter personal, sí que se producen dos situaciones que exigen cierto nivel de seguridad.

La primera es que al enviar la información de consumos desde los clientes al centro de control de IDESA, estos consumos pueden revelar información sobre hábitos, si hay actividad (y por tanto si hay o no personas) en una ubicación, etc.

Esta información, que podría ser interesante compartir desde el punto de vista de los clientes a las compañías de comercialización de electricidad y viceversa (con el fin de que les hagan unos o puedan hacer las otras ofertas), pero también podría ser utilizada por eventuales ladrones que quisieran acceder a un hogar o una empresa que supiesen que está vacía durante un periodo de tiempo.

Por otro lado, desde el centro de control, tal y como dice la ORDEN ITC/3022/2007, [3], al poder realizar la telegestión, esta operación podría ser sustituida a través de un intruso que accediese al medio de la red y operase la misma de forma remota.

No todas las soluciones presentadas en el apartado 6.2 proveen a la comunicación establecida la **capacidad de cifrado de la información transmitida.** Las empresas deben establecer una comunicación a través de protocolos seguros seleccionando proveedores de equipos que así lo garanticen. Para evitar estos casos, es necesario que los datos sean transmitidos de forma cifrada. Por ejemplo, la tecnología ZigBee [68], distinta (y para redes inalámbricas) a las mencionadas en el apartado 6.2.

Tal y como indica la revista "Anales de mecánica y electricidad" en su edición web [69], "*El estándar permite conectar a la red ZigBee Smart Energy contadores de electricidad, agua y gas. Para alargar la vida de las baterías de los contadores no conectados al suministro eléctrico, éstos envían periódicamente las medidas, estando el resto del tiempo en reposo y con la radio apagada. En el caso de los contadores eléctricos también es posible leer en cualquier momento las medidas, ya que suelen estar conectados permanentemente a alimentación. Por último destacar que junto con la medida, estos contadores pueden enviar información del estado del contador, como por ejemplo que la batería está baja o que lo han intentado abrir para manipularlo*".

Esta cifrado de datos en itinerantica se realiza mediante cifrado AES-CCM (Advanced Encryption Standard – CCM Star), con clave simétrica de 128 bits. También serían válidas otras soluciones que garantizasen un mínimo nivel de seguridad en la comunicación.

De la misma manera, en **los servidores donde se encuentre la información recogida, ésta debe estar almacenada de forma cifrada**. A su vez, IDESA establecerá una serie de **procedimientos para el acceso a la misma**, evitando su uso no autorizado.

6.3.2.2 Gestión de usuarios

En muchas ocasiones se agrupa la propia gestión de los usuarios con el control de acceso, asunto que se tratará en el próximo apartado.

La gestión de usuarios que debe realizar una empresa como IDESA, en la cual existen distintos perfiles de acceso, con distintos grados de formación y conocimiento debe cubrir todas las fases del ciclo de vida del acceso de los usuarios, desde el registro inicial de nuevos usuarios hasta la eliminación de los que ya no requieren acceso a los sistemas y servicios de información.

Tal y como se explicó en el apartado 6.1.3, Seguridad de la infraestructura de red y tratamiento derivado de los datos, el gestor del sistema debe prestar especial atención, a la asignación de perfiles de acceso y sus privilegios, en especial a aquéllos que permiten a los usuarios acceder a los sistemas de control. Las funcionalidades mínimas deberían ser capaces de ser soportadas tanto por los dispositivos como por el software que tengan implementando, es decir: autorizar accesos, activar cuentas a otros usuarios, editar, desactivar y eliminar cuentas.

6.3.2.3 Control de acceso y control de acceso remoto

Entre otros, deberá implantarse un modo de conexión de acceso seguro. Esto se consigue mediante la definición de perfiles de acceso, y en función del grado de los mismos se concederán privilegios. Ejemplo: los usuarios que quieran acceder desde internet a los datos de su contador, tendrán un perfil, llamémosle de “cliente” y podrán visualizar sus datos de consumo (en cumplimiento de la normativa).

Por otro lado, los operarios de mantenimiento (ya sean en remoto o con acceso in situ) tendrían un perfil llámese “operario”, que permitiría la manipulación de los parámetros del contador en función de las necesidades del cliente y la empresa.

Por último se crearía un perfil “administrador”, que tendría control sobre el acceso a la información de los usuarios, el acceso a la operación, kla posibilidad de altas y bajas de usuarios, etc. Además, podrían crearse perfiles temporales para los controles de auditoría y otros en función de las futuras necesidades de IDESA.

Así pues, se establecerán y quedarán reflejados en un manual interno de la compañía implementar los procedimientos que definan el acceso remoto a los sistemas de información y comunicación y las respuestas del sistema correspondientes a los intentos y los períodos de inactividad de conexión fallidos.

6.3.3 Seguridad de la infraestructura de red y tratamiento derivado de los datos

La seguridad de la infraestructura de red y tratamiento derivado de los datos incluye la definición de los procesos de seguridad de la arquitectura de red y de la itinerantica necesarios para la información a tratar. De acuerdo a lo definido en el apartado 6.1.3, las medidas que se deben implementar son:

- Necesidad de segregación de redes
- Nivel de aseguramiento de la comunicación con la infraestructura de red

6.3.3.1 Segregación de redes

Para poder garantizar un nivel de segregación de redes que cumpla con estos requerimientos, habría que implementar la solución que se propone en la Figura 22, de manera que las distintas unidades de negocio no tuviesen acceso a la manipulación de datos fuera de su ámbito de aplicación y que siempre quedase registro específico de los accesos a la misma.

En cuanto a la localización física de los sistemas, como ya se comentó, "cuando sea técnicamente viable, la infraestructura de red de los sistemas de control de procesos se debe dividir en varias zonas con diferentes funciones".

6.3.3.2 Aseguramiento de la comunicación

En el caso del tramo de red correspondiente a la red de PLC, el aseguramiento de la comunicación se realizará proveyendo a la capa de Control de acceso al medio las funcionalidades de autenticación y la integridad de los datos a través de un método de conexión segura y una política de gestión de claves.

Para el tramo de red correspondiente a la red ADSL, se realizará una contratación del servicio, garantizando que el proveedor pueda asegurar los mismos niveles de autenticación e integridad de los datos.

6.3.4 Auditoría de datos

Se diferencian en relación a los sistemas que se han provisto dentro de la soluciones dos tipos de auditorías: auditorías interna y externa.De manera formal y según recoge la Real Academia de la Lengua española, la auditoría es la "*revisión de la contabilidad de una empresa, de una sociedad, etc., realizada por un auditor*".

Tal y como definen varias empresas que dan servicios relacionados con la seguridad de los sistemas de información, "*la auditoría de seguridad, ayuda a las organizaciones a alcanzar su nivel objetivo de seguridad, disponiendo de sistemas de información más robustos y seguros"*. La auditoría interna[40] *"es un proceso cuya responsabilidad parte de la Alta Gerencia de las compañías, y se encuentra diseñado para proporcionar una seguridad razonable sobre el logro de los objetivos de la organización"*. Entre otros objetivos, la auditoria interna de las empresas atiende a:

- La validación de la efectividad y eficiencia de las operaciones.
- La confiabilidad de la información financiera.
- El cumplimiento con las leyes, reglamentos, normas y políticas.

[40] Según definición que publica la empresa de auditoría Deloitte en su página web http://www.deloitte.com/view/es_PE/pe/servicios/enterprise-risk-services/auditoria-interna/index.htm

Con el fin de poder llevar a cabo una auditoría segura de datos es necesario que se sigan una serie de prácticas y se implementen soluciones de manera que permitan cumplir con las medidas de seguridad mencionadas en el apartado 6.1.4Auditoría de datos. Estas medidas de seguridad son:

- Agregación de los procedimientos de auditoría interna la función de seguridad
- Trazabilidad de la información de los sistemas que soportan las infraestructuras eléctricas
- Protección de la información de las auditorías internas de seguridad

6.3.4.1 Agregación de los procedimientos de auditoría interna la función de seguridad

Desde el centro de control de IDESA, o desde el acceso de su unidad de control interno, debe existir una aplicación que permita rescatar los datos de acceso de usuarios, valores de medias, e incluso información de sistema, proporcionando la capacidad de generar registros de auditoría para que esta información pueda ser seleccionada dentro de una la lista de eventos verificables.

Así pues, cada acceso, cambio de configuración u operación realizada sobre la infraestructura, debe quedar registrada para poder ser auditada.

6.3.4.2 Trazabilidad de la información de los sistemas que soportan las infraestructuras eléctricas

De la misma manera que es necesaria la verificación de los accesos para un control de auditoría de seguridad, en los sistemas de información de IDESA el seguimiento y registro de accesos a puntos de acceso en el perímetro de Seguridad a los sistemas comunicación debe estar implementado y documentado.

Los sistemas deben ser monitorizados y cada evento debe ser registrado. Estos registros deben gestionarse de manera segura y poderse utilizar para identificar posibles problemas en los sistemas.

En la actualidad, distintas agencias certificadoras proveen de la información y formación necesaria para abordar este cometido y acreditan a las compañías para poder llevar a cabo este tipo de tareas con éxito.

6.3.4.3 Protección de la información de las auditorías internas de seguridad

Al igual que para el tratamiento de los datos de red, los servidores y dispositivos de almacenamiento de la información de auditoría deben ser protegidos contra la alteración y el acceso no autorizado.

Con el fin de poder realizar la función de auditoría de manera eficaz, esta información debería estar disponible de manera ininterrumpida para la posible ejecución de auditorías. Tal y como se explicó en el apartado 6.1.4, Auditoría de datos, las

herramientas de auditoría deberían permitir la identificación tanto de accesos no autorizados, como de modificaciones y/o eliminaciones de registros.

6.4 Conclusiones

La implantación del conjunto de medidas que satisfagan con todos los requerimientos técnicos para las áreas de seguridad no resulta tarea sencilla.

Como se ha podido observar, la disposición de los nuevos equipos de medida y **garantizar la seguridad de la información** para que sea procesada de manera correcta dentro del centro de control, **no es una única solución, sino que se obtiene tras la aplicación de un conjunto soluciones que tienen que ver con la selección tecnológica escogida, los procedimientos a implementar y el software que dé soporte para el control y la gestión de los dispositivos**.

Más allá de esta reflexión, como conclusión del caso de estudio se va a elaborar una tabla que permita trazar de manera simple el siguiente conjunto de informaciones:

1. la relación entre los dominios que comprenden las funciones de seguridad seleccionadas para el análisis,
2. con las medidas de seguridad que corresponden a cada una de estas funciones y
3. las soluciones que se proponen en el caso,
4. normativa o estándar que refleja lo indicado (si fuese de aplicación)

Tabla 7: Trazabilidad de las medidas de seguridad seleccionadas, soluciones y estándares/normas de seguridad existentes

Dominio	Medida de seguridad	Solución/es	ISO 27002, 27035, 27036,…	NIST	NERC-CIP	IEC 62351, 62443
Gestión de procesos con terceros	Acuerdos de confidencialidad con terceros	Contratos de confidencialidad que incluyan las consideraciones y clausulas necesarias para garantizar un nivel mínimo de seguridad.	ISO 27036 - 6.1.1 Acquisition process ISO 27002 - 6.2.1 Identification of risks related to external parties	NISTIR 7628 - SG.SA-2		
	Seguimiento de los servicios de terceros	Informe de Seguimiento de terceros. Reuniones de seguimiento de los servicios de terceros	ISO 27002 - 10.2 Third party service delivery management	NISTIR 7628 - SG.AU-1 Audit and Accountability Policy and Procedures		
	Garantía de continuidad de servicio	Definición de una estrategia de gestión de la continuidad del servicio que incluya procedimientos proactivos (líneas de emergecia) y reactivos (sistemas Cold standy)	ISO 7019 - 14.1.1 Including information security in the business continuity management process ISO TR 27019 - 14.2.1 Emergency communication	NISTIR 7628 - SG.CP-2 Continuity of Operations Plan NISTIR 7628 - SG.CP-11 Fail-Safe Response - General Requirement	NERC CIP-008 Notificación de incidentes y planificación de la respuesta NERC CIP-009 Planes de recuperación de activos cibernéticos críticos	

Dominio	Medida de seguridad	Solución/es	ISO 27002, 27035, 27036,…	NIST	NERC-CIP	IEC 62351, 62443
Seguridad específica de los sistemas de información	Seguridad de los datos y la información	Capacidad de cifrado tanto de la información transmitida como de la almacenada en los servidos. Procedimientos seguros para el acceso a esta información.	ISO 27019 - B.1.1.1.6 Encryption of Sensitive Data during Storage and Transmission ISO 27002 - 10.7.3 Information handling procedures			
	Gestión de usuarios	Software de gestión que permita una asignación de perfiles y privilegios pudiendo dar accesos, activar/desactivar cuentas de otros usuarios, editar, eliminar,…	ISO 27002 - 11.2 User access management	NISTIR 7628 - SG.AC-3 Account Management - Requirement 1		IEC / TS 62351-8 - Parte 8: Control de acceso basado en perfiles
	Control de acceso y control de acceso remoto	Implantación un modo de conexión de acceso seguro y establecimiento de control de acceso, incluyendo sistemas de respuesta ante intentos de acceso seguros		NISTIR 7628 - SG.AC-2 Remote Access Policy and Procedures - Requirement 1	NERC CIP-003-4 - Requirement 5. Access Control	IEC 62443 - 4.3.3.7.2 Establish appropriate logical and physical permission methods to access IACS devices IEC 62443 - 4.3.3.6.6 Develop a policy for remote login and connections

Dominio	Medida de seguridad	Solución/es	ISO 27002, 27035, 27036,…	NIST	NERC-CIP	IEC 62351, 62443
Seguridad de la infraestructura de red y tratamiento de los datos	Necesidad de segregación de redes	Implementación de redes independientes para las unidades de negocio que no estén directamente vinculadas con el acceso a la nueva infraestructura.	ISO 27002 - 11.4.5 Segregation in networks		NERC CIP-005 4AA– Perímetros de seguridad electrónica	
	Nivel de aseguramiento de la comunicación con la infraestructura de red	Capa de control de acceso al medio las funcionalidades de autenticación y la integridad de los datos a través de un método de conexión segura y una política de gestión de claves	ISO 27011 – A.10.6 Network security management ISO 27002 - 11.4.7 Network routing control	NISTIR 7628 - SG.SC-9 Communication Confidentiality		IEC 62443-2-1 Requisitos para gestión de la seguridad del sistema IEC 62351-1 - Partes 1,2,3 : Comunicación de seguridad de red y del sistema

Dominio	Medida de seguridad	Solución/es	ISO 27002, 27035, 27036,…	NIST	NERC-CIP	IEC 62351, 62443
Auditoría de datos	Agregación de los procedimientos de auditoría interna la función de seguridad	Aplicación que permita rescatar los datos de acceso de usuarios, valores de medias, e incluso información de sistema, proporcionando la capacidad de generar registros de auditoría para que esta información pueda ser seleccionada y verificada.	ISO/IEC TR 27019 - 10.10.1 Audit logging	NISTIR 7628 - SG.AU-15 Audit Generation - Requirement 1		
	Trazabilidad de la información de los sistemas que soportan las infraestructuras eléctricas	Implementación y documentación del seguimiento y registro de accesos a puntos de acceso en el perímetro de seguridad a los sistemas comunicación.	ISO 27002 - 10.10 Monitoring		NERC CIP-005-4a - Requirement 3. Monitoring Electronic Access	
	Protección de la información de las auditorías internas de seguridad	Herramientas de auditoría que permitan la identificación tanto de accesos no autorizados como de modificaciones y/o eliminaciones de registros.	ISOC 27002 - 10.10.3 Protection of log information	NISTIR 7628 - SG.AU-9 Protection of Audit Information - General Requirement		

7 Conclusiones del proyecto y trabajo futuro

Como resultado del proyecto, en el presente capítulo se presenta en primer lugar un resumen del trabajo realizado durante los distintos capítulos de análisis, con el fin de introducir las conclusiones globales de todo el proyecto y presentar de manera enlazada los resultados alcanzados.

Ya que el ámbito en el que se desarrolla el proyecto se trata de un análisis normativo de un sector emergente, antes de poner punto y final al proyecto se presentan también una serie de ideas como propuesta de trabajo futuro en las que se sugieren líneas de actuación para futuros proyectos.

7.1 Resumen del análisis realizado

Con el fin de poder realizar un análisis de las normas de seguridad para los controles, las comunicaciones y otros equipos críticos de la red de energía, ha sido necesario en primer lugar plantear y entender cuál es el conjunto de necesidades en torno al caso de estudio que se iba a plantear. Así pues, en el capítulo 2 se han presentado a alto nivel los conceptos básicos de la infraestructura eléctrica y sistemas de control y comunicación con los que se opera.

Para conseguir este entendimiento y también poder realizar el posterior análisis, se ha llevado a cabo la búsqueda en libros, artículos y otras publicaciones de la información necesaria a lo largo del proyecto. Como ya se explicó en el apartado 1.3, la recopilación de información ha sido realizada de distintas maneras durante la totalidad del proyecto.

En referencia al trabajo de análisis, en primer lugar, se ha revisado de la documentación encontrada sobre la normativa europea acerca de seguridad de infraestructuras críticas y varios de los principales estándares de seguridad existentes.

De manera paralela, se ha realizado tanto un repaso de la Directiva 2008/114/EC de infraestructuras críticas y las implicaciones que tiene a nivel de infraestructura eléctrica, como una síntesis de prácticas a aplicar en materia de seguridad para los distintos entornos que aplican al funcionamiento de la infraestructura eléctrica y qué recomendaciones se realizan al respecto en base a varias normas relativas a seguridad de eléctrica, comunicaciones y control industrial, como son las ISO serie 27000, NIST 800-53, NERC-CIP, ANSI/ISA99, IEC 62443 y IEC 62341.

Finalmente se abordó el caso de estudio sobre las normas de control en la infraestructura eléctrica que afectaban al despliegue de los nuevos equipos de medida que recoge el Decreto 1110/2007 [2]. Para esto se definieron una serie de requerimientos técnicos en concordancia con la reglamentación y los estándares existentes. El objetivo de esta parte del trabajo ha sido que en función de estos requerimientos se pudiera diseñar una serie de soluciones que permitieran implementar estos nuevos equipos garantizando unos niveles mínimos de seguridad.

Por último, durante el caso de estudio se han diseñado una serie de sistemas, procedimientos y documentos que le permitirán cumplir con los parámetros seleccionados en la definición del caso y de esta manera poder llevar a cabo parte de sus procesos de negocio de una manera segura de acuerdo a la aplicación de la normativa existente.

7.2 Conclusiones

Como resultado del trabajo y el análisis realizado a lo largo del proyecto se han alcanzado conclusiones en muy diversos ámbitos. Del capítulo 2, Sistemas de control y comunicación en la infraestructura eléctrica, se puede extraer que:

- El paradigma clásico de funcionamiento del sistema eléctrico está cambiando hacia un sistema más distribuido donde el control se realiza a través de sistemas de comunicación e información.

- Estos sistemas de comunicación e información han de ser robustos con el fin de que puedan tener disponible información fiable en tiempo real.

- En el sector eléctrico, los datos y sus flujos de información deben ser manipulados de manera jerárquica, donde los niveles suelen estar separados por puertas de enlace, DMZ, o cortafuegos.

- Los centros de operación y control utilizan sistemas SCADA, que tal y como se ha podido ver, juegan un papel clave en una infraestructura tan crítica como es la energética. Con estas plataformas ya consolidadas, los desafíos en curso para asegurar los sistemas de electricidad y redes incluyen:

    - una mejora en el cumplimiento de la industria con las normas de seguridad cibernética y los aspectos regulatorios, que permitan garantizar la seguridad cibernética de los sistemas de redes inteligentes de energía,

    - desarrollo de medidas de seguridad particulares para los sistemas de redes eléctricas, así como un mecanismo eficaz para el intercambio de información sobre seguridad cibernética y otros temas, y definir indicadores para evaluar la seguridad cibernética que apliquen a la gestión en el sector eléctrico.

Posteriormente, de la descripción de la directiva 2008/114/EC, texto de referencia en materia de seguridad dentro de la Unión Europea, y de la estrategia de seguridad cibernética de UE se puede concluir que a nivel paneuropeo existe la idea de que:

- La infraestructura eléctrica es crítica, por lo que por definición y como toda infraestructura crítica, ha de tener implementados sus mecanismos de seguridad, entre los que se encuentran los de manejo y reporte de información.
- Partiendo de los principios básicos de la seguridad de la información se pueden resumir en confidencialidad de la información, integridad de los datos y

disponibilidad del sistema, los distintos estándares recogen sus propias definiciones de requerimientos de seguridad para abordarlo. Estos requerimientos de seguridad siempre han de ser compatibles con los requisitos de tiempo real de los propios sistemas.

En relación a la síntesis realizada en el capítulo 4, Estandarización y regulación, que ha permitido reflejar una serie de prácticas a aplicar en materia de seguridad para los distintos entornos que aplican al funcionamiento de la infraestructura eléctrica cabe destacar:

- En estos momentos, dentro del debate sobre las redes inteligentes y su desarrollo en el medio-largo plazo, la Comisión Europea ha establecido un grupo de trabajo que está realizando estudios en distintos aspectos en el ámbito de las redes inteligentes: SGTF.

- El SGTF en colaboración con ENISA (ver apartado 4.3), ha elaborado el informe "*Proposal for a list of security measures for smart grids*" [29] para definir buenas prácticas en relación al ámbito de las redes inteligentes, proporcionándoles un conjunto de medidas de seguridad adecuadas.

- Las normas en materia de seguridad que deben ser implementadas deben cumplir unos criterios mínimos siempre y cuando garantice al máximo objetividad, transparencia y participación de todos los involucrados en el proceso regulatorio.

- A nivel Europeo, ENISA es la agencia que ofrece asesoramiento experto sobre seguridad de las redes y de la información a las autoridades nacionales e instituciones europeas, funciona como foro de intercambio de mejores prácticas y facilita el contacto entre las instituciones europeas, las autoridades nacionales y las empresas.

En el capítulo 1, , gracias al análisis en detalle de toda la normativa aplicable a la seguridad en los sistemas TIC, se identificaron los siguientes parámetros del análisis como los que tienen mayor relación con el ámbito de las telecomunicaciones: gestión de procesos con terceros, seguridad específica de los sistemas de información, seguridad de la infraestructura de red y tratamiento derivado de los datos y auditoría de datos.

En cada una de estas áreas se aplicarán una serie de medidas de seguridad sobre las que las empresas responsables de los centros de control deberán aplicar los estándares y otras normativas.

Como cierre al trabajo realizado, se ha elaborado la que relaciona de manera simple dominios que comprenden de las funciones de seguridad seleccionadas para el análisis, con las medidas de seguridad que corresponden a cada una de estas funciones, las soluciones que se proponen en el caso y la normativa o estándar que refleja de aplicación. Así pues, queda también reflejado el hecho de que la implantación del conjunto de medidas que satisfagan con todos los requerimientos técnicos para las áreas de seguridad no resulta tarea sencilla

La función de seguridad no es una única solución, sino que se obtiene tras la aplicación de un conjunto soluciones que tienen que ver con la selección tecnológica escogida, los procedimientos a implementar y el software que de soporte que se desarrolle para el control y la gestión de los dispositivos.

7.3 Propuestas de trabajo futuro

Debido a la necesidad latente de disponer de unos sistemas información y comunicación más seguros que permitan a las redes de transporte y distribución de electricidad dar servicios cada vez más completos tanto para sus gestores y como los usuarios, los criterios de seguridad bajo los que se deben regir estos sistemas de información y comunicación deben ser robustos, garantizando la integridad y privacidad de los datos que se transmiten y almacenan.

En relación a esto, se plantean a continuación posibles líneas de estudio relacionadas con el trabajo desarrollado y las conclusiones obtenidas:

- En primer lugar, se sugiere a los ingenieros especialistas en desarrollo, el diseño de los equipos (hardware y software) y/o las posibles mejoras sobre los existentes para que cumplan los requerimientos establecidos en este análisis o incrementen los niveles de seguridad dentro de los distintos parámetros.

- Otra línea de trabajo que se puede desarrollar es el análisis de los parámetros de seguridad no incluidos en el presente estudio.

  Cabe recordar que en la sección *5.2 Selección de los parámetros a estudiar en el caso de estudio,* los parámetros escogidos para la elaboración del caso de estudio fueron la gestión de procesos de terceros, la seguridad específica de los sistemas de información, las seguridad de la infraestructura de red y tratamiento derivado de los datos y la auditoría de datos.

  De la misma manera, se podría profundizar para una empresa de similares características a IDESA el análisis, arquitectura necesaria y equipos que permitan dar una solución para la ‘Gobernanza de la seguridad y la gestión de riesgos’, los ‘Componentes de las infraestructuras, sus sistemas y procedimientos operativos’, una ‘Respuesta ante incidentes e intercambio de conocimiento’ y una ‘Continuidad de operaciones’.

- Profundizar en el desarrollo de las soluciones que se puedan dar para los dispositivos que controlan el acceso de usuarios a los nuevos dispositivos de medición que están instalando en los hogares, centrándose en cómo realizar la provisión de información, control de calidad de los datos y garantizando un acceso adecuado los mismos.

- Elaborar propuestas para implementar una correcta relación entre datos de centro de control resultantes de la nueva infraestructura que pudiese desplegar una

empresa similar a IDESA y su interacción con otras líneas de negocio de la misma.

Si bien las empresas de distribución eléctrica en la actualidad se encuentran legalmente separadas, sus datos pueden ser intercambiables con empresas de transporte de electricidad, comercializadoras, clientes (ya se hace), regulador de mercado (obligatorio), centros de investigación… Trabajos futuros podrían elaborar reglas técnicas o normas de uso de toda esta información.

- Elaborar la misma definición de requerimientos y propuesta de soluciones para otra arquitectura dependiendo de la configuración de usuarios.

Por ejemplo, en vez de proponer una conexión de los mismos a través de PLC y desde el concentrador hasta el centro de control por ADSL, o también ver cómo se realizaría esto mismo para usuarios o localizaciones remotas o aisladas. Se podría plantear cómo influirían ahí las obligaciones de servicio público, etc. (en España los servicios posiblemente comprendidos serían el servicio y comercialización de último recurso de electricidad y servicio universal de telecomunicación).

8 Glosario de acrónimos

El glosario de acrónimos aquí contenido incluye las abreviaturas y los acrónimos que se encuentran en el presente proyecto clasificados por orden alfabético y sin atender a lugar en el texto.

Acrónimo	**Correspondencia**
ACER	Agencia de Cooperación de Reguladores Europeos
AES	Advanced Encryption Standard
AFIBEL	Asociación de Fabricantes de Bienes de equipo Eléctrico
ANSI	American National Standards Institute
BBDD	Base(s) de Datos
BMS	Business Market/Management System
BOE	Boletín Oficial del Estado
CE	Comisión Europea
CECOEL	Centro de Control Eléctrico de Red Eléctrica de España
CCM	Computational Continuum Mechanics
CIP	Critical Infrastructure Protection
CNE	Comisión Nacional de Energía
CNMC	Comisión Nacional de los Mercados y la Competencia
DLMS	Device Language Message Specification

Acrónimo	Correspondencia
DMS	Distribution Management System
MDT	Discrete Multi-Tone modulation
DMZ	Demilitarized zone
EMS	Energy Management System
ENISA	European Network and Information Security Agency
FISMA	Federal Information Security Management Act
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
ICCP	Inter-Control Center Communications
ICS	Industrical Control System
IDESA	Iberfende Distribución de Electricidad, S.A.
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISA	International Society of Automation
ISO	International Organization for Standardization
LAN	Local Area Network
MMS	Manufacturing Message Specification

Acrónimo	Correspondencia
NERC	North American Electric Reliability Corporation
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NSM	Network and System Management
OEN	Organismo Europeo de Normalización
OFDM	Orthogonal Frequency Division Multiplexing
OMS	Outage Management System
ORDEN ITC	Orden promulgada por el Ministerio de Industria, Turismo Y Comercio
OSI	Open System Interconnection
OSP	Operator security plan
PEPIC	Programa Europeo de Protección de Infraestructuras Críticas
PDA	Personal Digital Assistant
PLC	Power Line Communications
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
RD	Real Decreto

Acrónimo	Correspondencia
REE	Red Eléctrica de España
RS	Recommended Standard
RTC	Red Telefónica Conmutada
SCADA	Supervisory Control And Data Acquisition
SGIS	Smart Grid Information Security
SGSI	Sistema de gestión de la seguridad de la información
SGTF	Smart Grids Task Force
TCP/IP	Transmission Control Protocol / Internet Protocol
TIC	Tecnologías de Información y Comunicación
UE	Unión Europea
VPN	Virtual Private Network
WAN	Wide Area Network

9 Referencias bibliográficas

Las Referencias bibliográficas se y sitios web utilizados para la adquisición de conocimiento y provisión del contenido de la presente memoria se encuentra detallada a continuación y sin necesidad de atender a lugar en el texto.

La totalidad de los enlaces a páginas web expuestos a continuación estaban habilitados y funcionando a fecha 20 de abril de 2014.

[1] La NSA pirateó protocolos de seguridad en la Red para sus labores de espionaje, Unidad Editorial Información General S.L.U, http://www.elmundo.es/america/2013/09/06/estados_unidos/1378428110.html

[2] REAL DECRETO 1110/2007, de 24 de agosto, por el que se aprueba el Reglamento unificado de puntos de medida del sistema eléctrico.

[3] ORDEN ITC/3022/2007, de 10 de octubre, por la que se regula el control metrológico del Estado sobre los contadores de energía eléctrica.

[4] Atención, consumidores: los contadores eléctricos inteligentes desvelan datos reservados de los usuarios, EL Confidencial Digital S.L., http://www.elconfidencialdigital.com/dinero/Atencion-consumidores-contadores-inteligentes-reservados_0_2246175379.html

[5] "DIRECTIVA 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección" - Diario Oficial de la Unión Europea.

[6] Commission Staff Working Document SWD(2012) 190, on the review of the European Programme for Critical Infrastructure Protection (EPCIP)

[7] Commission Staff Working Document SWD(2013) 318, on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure

[8] SCADA/Business Network Separation: Securing an Integrated SCADA System, http://www.automation.com/library/articles-white-papers/hmi-and-scada-software-technologies/scadabusiness-network-separation-securing-an-integrated-scada-system

[9] Smart Grid Conceptual Model, http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model

[10] Smart Grid - The New and Improved Power Grid: A Survey; IEEE Communications Surveys and Tutorials 2011; X. Fang, S. Misra, G. Xue, and D. Yang

[11] Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure; Author(s): Ericsson, G.N. Svenska Kraftnat (Swedish Nat. Grid), Sundbyberg, Sweden

[12] Communication from the Commission of 12 December 2006, COM (2006) 786 final, on a European Programme for Critical Infrastructure Protection

[13] Joint communication, COM(2013) 1 final, to the European Parliament, the Council, the European economic and social committee and the committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

[14] ISO/IEC 27002:2005, Tecnología de la información - Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información

[15] ISO/IEC 27032:2012, Information technology -- Security techniques -- Guidelines for cybersecurity

[16] ISO/IEC 27033-5:2013, Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

[17] ISO/IEC 27035:2011, Information technology -- Security techniques -- Information security incident management

[18] ISO/IEC 27036 (draft ISO/IEC 27036 — IT Security — Security techniques — Information security for supplier relationships)

[19] NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

[20] NERC – CIP Complete Set of Reliability Standards
http://www.nerc.com/page.php?cid=2%7C20

[21] ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems

[22] IEC 62443: Network and system security for industrial-process measurement and control

[23] IEC 62351: Smart Grid Security

[24] Real Academia Española, Diccionario de la lengua española (DRAE) es la obra de referencia de la Academia. La edición actual —la 22.ª, publicada en 2001, http://www.rae.es/recursos/diccionarios/drae

[25] Red Eléctrica de España, www.ree.es

[26] Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas

[27] European Task Force for the Implementation of Smart Grids into the European internal market, Mission And Work Programme

[28] Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment

[29] Proposal for a list of security measures for smart grids, Konstantinos Moulinos

[30] Energy: Smart Grids Task force - European Commission http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

[31] European technology platform for the electricity networks of the future http://www.smartgrids.eu/Smart-Grids-Task-Force

[32] Reglamento Europeo 460/2004 del Parlamento Europeo y del Consejo de 10 de Marzo de 2004, por la que se establece ENISA

[33] European Union Agency for Network and Information Security https://www.enisa.europa.eu/

[34] Ley 54/1997, de 27 de noviembre, del sector eléctrico (y posteriores modificaciones que aplican al análisis realizado)

[35] Meters&More initiative http://www.metersandmore.com/

[36] PRIME Alliance | Advanced Meter Reading & Smart Grid www.prime-alliance.org

[37] Circuitor, Tecnología para la eficiencia energética (Catálogo)

[38] Circuitor, Contadores multifunción de energía eléctrica (Catálogo)

[39] Haciendo realidad la Red del Futuro, Sistema de Telegestión basado en Tecnología PRIME, ZIV

[40] Revista ABB 3/2009, El suministro eléctrico. Gestión de redes para la red de distribución, Centros de operaciones innovadores gestionarán las redes de distribución futuras, Tim Taylor, Marina Ohrn

[41] PLC (Power Line Communications), José Luis Delgado Q.

[42] Tecnologías y actividades de estandarización para la interconexión de Home Networks, Anexo B, Alcatel para Fundación AUNA

[43] La tecnología PLC en los Programas de Fomento de la Sociedad de la Información, J. R. González Puyol y F. J. García Vieira

[44] Draft Specification for PoweRline Intelligent Metering Evolution, prepared by the PRIME Alliance Technical Working Group

[45] Distributed Generation: The Power Paradigm for the New Millennium. CRC Press, Boca Raton. Borberly, A. and Kreider, J. F. (2001)

[46] Merging SONET and Ethernet Communications for Power System Applications Edmund O. Schweitzer, III, David Whitehead, Ken Fodero, and Paul Robertson, Schweitzer Engineering Laboratories, Inc.

[47] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas

[48] RD 982/1987, de 5 de junio, por el que se da nueva redacción a los artículos 67 y 68 del Reglamento General de Contratación del Estado.

[49] Orden IET/290/2012, de 16 de febrero, por la que se modifica la Orden ITC/3860/2007, de 28 de diciembre, por la que se revisan las tarifas eléctricas a partir del 1 de enero de 2008 en lo relativo al plan de sustitución de contadores. MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

[50] “Cyber security assessment of a power plant” - Igor Nai Fovino, Luca Guidib, Marcelo Masera, Alberto Stefanini

[51] IEC Smart Grid Standardization Roadmap, - Smart Grid Strategic Group, European Commission

[52] Communications Networks: The Enablers of Utility Automation Success By: Charles Plummer

[53] Power Line Communication Applictions Study, by Phil Sutterlin and Walter Downey

[54] Distribución inteligente, Endesa, S.A. 2012 http://www.endesasmartgrids.com/index.php/es/distribucion-inteligente

[55] El Contador Inteligente, Endesa, S.A. 2012 http://www.endesasmartgrids.com/index.php/es/la-casa-inteligente/el-contador-inteligente

[56] Detección de APTs , José Miguel Holguín, Maite Moreno, Borja Merino, Javier Morant, Alberto López

[57] Cyber-security threat characterisation, A rapid comparative analysis Neil Robinson, Luke Gribbon, Veronika Horvath, Kate Robertson A rapid comparative analysis

[58] Ministerio de Empleo y Seguridad Social, BOE, resolución de 9 de octubre de 2013, de la Dirección General de Empleo, por la que se registra y publica el XVII Convenio colectivo nacional de empresas de ingeniería y oficinas de estudios técnicos.

[59] Can we learn from SCADA security incidents?, ENISA

[60] Testimony of Joseph McClelland Director, Office of Electric Reliability Federal Energy Regulatory Commission Before the Committee on Energy and Natural Resources United States Senate, July 17, 2012

[61] CYBERSECURITY Challenges in Securing the Electricity Grid Statement of Gregory C. Wilshusen, Director Information Security Issues

[62] Testimony of Gerry Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation Before the Senate Energy and Natural Resources Committee Hearing on the Status of Actions Taken to Ensure that the Electric Grid is Protected from Cyber Attacks

[63] Real Decreto 1955/2000, por el que se regulan las actividades de transporte, distribución, comercialización, suministro y procedimientos de autorización de energía eléctrica.

[64] Energía Eléctrica, Ministerio de Industria, Energía y Turismo http://www.minetur.gob.es/energia/electricidad/Paginas/Index.aspx

[65] modelodecontrato.net - Contrato de confidencialidad www.modelodecontrato.net

[66] OSIATIS S.A. - Gestión de la Continuidad del Servicio. www.osiatis.es; http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_continuidad_del_servicio/vision_general_gestion_de_la_continuidad_del_servicio/vision_general_gestion_de_la_continuidad_del_servicio.php

[67] Código de Buenas Prácticas para el despliegue de infraestructura de redes de comunicaciones. Comisión de Regulación de Comunicaciones y la Agencia Nacional del Espectro de Colombia, Octubre 2013

[68] ZigBee Smart Energy, http://www.zigbee.org/Standards/ZigBeeSmartEnergy/Overview.aspx

[69] Gestión de redes inteligentes domésticas mediante ZigBee Smart Energy, http://www.revista-anales.es/web/n_16/seccion_3.html

[70] IEC 61850 Communication Protocol Manual, 650 series, ABB

Anexo A: Pliego de condiciones

El presente proyecto presenta un informe sobre la normalización de los requerimientos que tiene que haber para garantizar unos niveles de seguridad 'aceptables' dentro de los sistemas de información y centros de control que gobiernan y dan soporte a la infraestructura eléctrica.

La memoria presentada es un análisis de la normativa existente y un caso de estudio que define las directrices para la aplicación de la misma en parte de estos sistemas.

Entregables

- Memoria del proyecto

  Original y dos copias del Proyecto, encuadernadas de forma normalizada.

  Cesión a la Universidad Autónoma de Madrid, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, para que pueda ser utilizada de forma libre y gratuita por todos los usuarios del repositorio y del portal e-ciencia, los derechos de reproducción, de distribución, de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual

Condiciones de desarrollo – recursos

- Equipo de desarrollo portátil.
- Sistema operativo Windows 7 utilizado en el equipo de elaboración de la documentación.
- Microsoft Office 2010 (paquetes de trabajo Word, Power Point, Excel y Project) utilizado para la elaboración de la documentación.

Anexo B: Presupuesto

Con el fin de poder una valoración económica del esfuerzo empleado en la elaboración presente proyecto, se detalla el presupuesto del mismo, que se desglosa en las siguientes partidas:

- Presupuesto de ejecución material.
- Gastos generales y Beneficio industrial.
- Honorarios por la redacción y dirección del proyecto.
- Presupuesto total.

Todas las cantidades aparecen expresadas en euros.

Presupuesto de ejecución material.

El presupuesto de ejecución material es el importe del coste de los materiales y de la mano de obra, necesarios para la ejecución de una obra o un trabajo contratado..

En el presente proyecto, el "Presupuesto de ejecución material" consta de Costes de mano de obra y Costes de recursos materiales.

Desglose por tareas ejecutadas

Con el fin de poder representar de una manera clara y comprensible los costes de mano de obra del proyecto una división en tareas del trabajo realizado para el desarrollo de este Proyecto Fin de Carrera.

El proyecto consta de las siguientes tareas con sus esfuerzos correspondientes:

1. Entendimiento del problema

   Objetivo: Asimilación de los conceptos básicos del de los sistemas de control y comunicación que gobiernan la infraestructura eléctrica. Esto ha permitido elaborar un diagnóstico de las necesidades de caso, construirlo y trabajar para su solución.

   Duración: 1 semana

   Esfuerzo: Ingeniero superior, 0.25 personas-mes.

2. Recolección de información

   Objetivo: Búsqueda en libros, artículos y otras publicaciones de la información necesaria a lo largo del proyecto. Ha sido necesario recopilar información acerca de cómo funcionan los sistemas de control y comunicación dentro de la infraestructura del sistema eléctrico, cuáles son las normativas y estándares

existentes acerca de la seguridad en los sistemas de control y comunicación y qué tecnologías están disponibles de manera factible para plantear soluciones factibles al problema planteado.

Duración: 7 semanas a tiempo parcial, 4 durante la recogida de la información normativa necesaria para el análisis y 3 más para la recogida de información sobre las distintas tecnologías que permitan diseñar la serie de soluciones a adoptar.

Esfuerzo: Ingeniero superior, 0.875 personas-mes.

3. Estudio y evaluación de la normativa existente

   Objetivo: Revisión de la documentación encontrada sobre la normativa europea acercad e seguridad de infraestructuras críticas y varios de los principales estándares de seguridad existentes; análisis regulatorio en relación a la Directiva 2008/114/EC de infraestructuras críticas, ISA99, las NERC y/o ISO y/o NIST que apliquen, etc., y síntesis que permita reflejar una serie de prácticas a aplicar en materia de seguridad para los distintos entornos que aplican al funcionamiento de la infraestructura eléctrica y que recomendaciones se realizan al respecto

   Duración: 9 semanas de las cuales las cuatro primeras serán a tiempo parcial.

   Esfuerzo: Ingeniero superior, 1.75 personas-mes.

4. Definición del caso de estudio

   Objetivo: Establecer la relación entre de las normativas de seguridad y su aplicación en los centros de control y los sistemas de información y comunicación y posteriormente se han seleccionado los parámetros a estudiar en el mismo.

   Duración: 2 semanas en las cuales la segunda se solapará con la realización del análisis

   Esfuerzo: Ingeniero superior, 0.375 personas-mes.

5. Realización del análisis para la aplicación de la normativa de seguridad en el caso de estudio seleccionado

   Objetivo: Desarrollo del caso de estudio en el que se definirán los requerimientos técnicos y se diseñarán para una empresa de distribución de electricidad una serie de sistemas, procedimientos y documentos que le permitirán cumplir con los parámetros seleccionados en la definición del caso y de esta manera poder llevar a cabo parte de sus procesos de negocio de una manera segura de acuerdo a la aplicación de la normativa existente.

   Duración: 7 semanas, de las cuales, las 4 serían a tiempo parcial y las 3 a tiempo completo

   Esfuerzo: Ingeniero superior, 1.25 personas-mes.

6. Elaboración de conclusiones y escritura de la memoria

   Objetivo: Se han realizado las conclusiones obtenidas como resultadas del proyecto y planteamiento de posibles trabajos o estudios como consecuencia del presente proyecto y escritas la presente memoria.

   Duración: 4 semanas, la primera a tiempo parcial y las 3 últimas a tiempo completo

   Esfuerzo: Ingeniero superior, 0.875 personas-mes.

   La valoración de la escritura del a memoria se realizará más adelante en el punto honorarios por redacción.

A continuación se muestra un diagrama de Gantt con las relaciones de dependencia entre las distintas tareas.

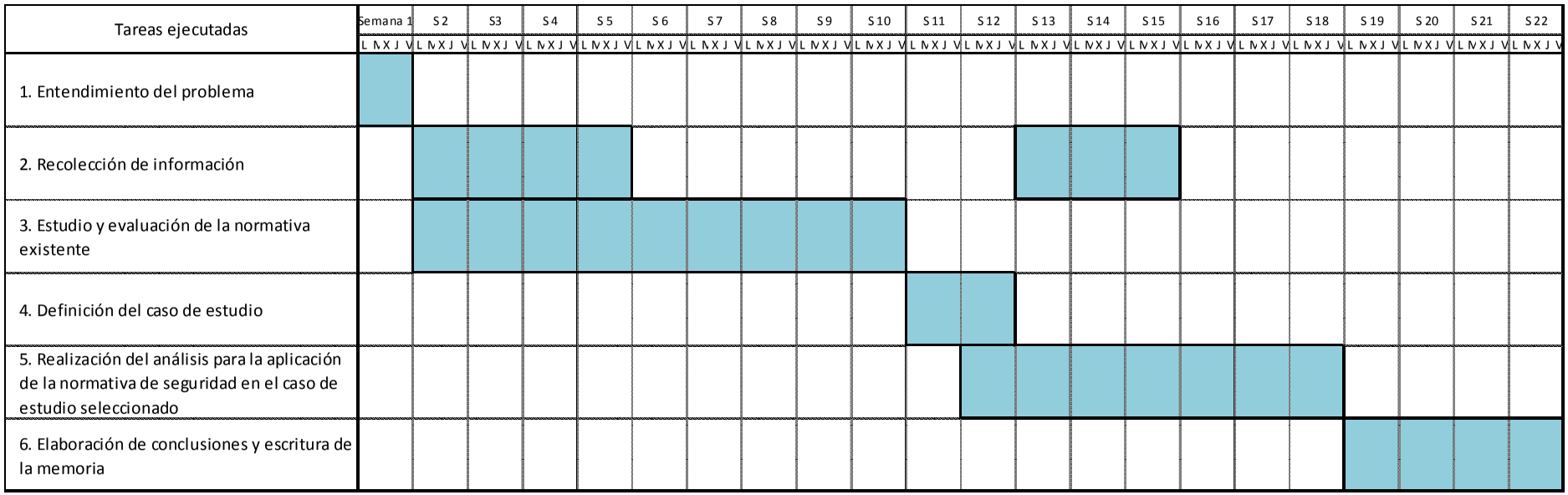

Figura 26. Diagrama de Gantt del proyecto

El tiempo para la ejecución de cada una de las tareas expresadas del trabajo que se incluye en el presente proyecto representa el tiempo equivalente de un ingeniero trabajando de manera continua e ininterrumpida durante la confección del mismo trabajo. Estos tiempos han sido estimados en base a la carga de trabajo realizado durante el las distintas tareas llevadas a cabo para realizar el presente estudio.

La duración total del proyecto hubieran sido cinco meses, en los que se hubiese incurrido en un esfuerzo de cinco personas-mes de un Ingeniero.

Costes de la mano de obra

El coste de la mano de obra considerado para la ejecución del proyecto asciende a 17,078.88 €.

Para la realización del proyecto se ha requerido del trabajo de un profesional con el siguiente perfil profesional:

- Un Ingeniero de Telecomunicación, encargado tanto del planteamiento, desarrollo e implementación del trabajo analítico y técnico, así como de la redacción, presentación y encuadernación del proyecto.

El coste del salario bruto mensual del ingeniero encargado del proyecto para la elaboración del presupuesto corresponde a doce pagas de 3,105.25 €.

La estimación de los costes se realiza en base a los siguientes datos:

- La base cotizable se establece bajo el supuesto en el cual se remunera salarialmente al Ingeniero encargado del proyecto según los salarios pactados en el Convenio colectivo nacional de empresas de ingeniería y oficinas de estudios técnico publicado en Boletín Oficial del Estado (BOE) Resolución de 9 de octubre de 2013, de la Dirección General de Empleo de acuerdo al grupo salarial de Licenciados y titulados 2.º y 3.er ciclo universitario y Analista.

  Esto son 23.618,28 euros anuales y al no realizarse trabajos bajo ninguna condición extraordinaria, no se aplican ningún plus en su remuneración. Prorrateando esta cantidad a 10,5 meses laborables. El coste salarial mensual asciende a 2,249.36 €.

- Para el cálculo del coste de la seguridad social se han tenido en cuenta las siguientes partidas:

  - Contingencias comunes (23.6%)
  - Desempleo. F.G.S y Formación profesional (6.3%)
  - Accidentes de trabajo y enfermedades profesionales (8,33%)

  Las cotizaciones según el Régimen General de la Seguridad Social. El ingeniero pertenece al grupo 1. Por lo tanto,

Grupos de Cotización	Base mínima	Base máxima
	Euros (Mes)	Euros (Mes)
1	1.051,50	3.425,70

Figura 27. BASES DE COTIZACIÓN RÉGIMEN GENERAL EJERCICIO 13 - ORDEN ESS/56/2013, de 28/12 (BOE del 29)

- Teniendo en cuenta la carga de trabajo necesaria para ejecutar el proyecto bajo una jornada laboral de 8 horas/día y 20 días laborales/mes y las tareas especificadas en el apartado 11.1.1, el número de meses a emplear son 5.5

Tabla 8: Costes salariales del proyecto

Costes salariales	
Concepto	**Coste**
Base cotizable máxima anual (valor medio mes)	2,249.36 €
Contingencias comunes (23.6%)	528.31 €
Desempleo. F.G.S y Formación profesional (6.3%)	141.03 €
Accidentes de trabajo y enfermedades profesionales	186.55 €
Coste de la seguridad social	855.89 €
Salario bruto mensual	3,105.25 €
Nº de meses:	5.5
Coste total mano de obra:	17,078.88 €

Coste de los recursos materiales

En la siguiente tabla constan los costes de los recursos materiales empleados, considerando un periodo de amortización para el hardware y el software de 5 años.

En primer lugar se indicarán los costes totales y a continuación se imputarán las cuantías correspondientes a la amortización de los recursos durante su periodo de utilización en el desarrollo del proyecto.

Tabla 9: Costes de materiales del proyecto

Costes presupuesto materiales del proyeto	
Equipo de desarrollo portátil	1,200.00 €
Sistema operativo Windows 7	283.62 €
Microsoft Office Office 2013	269.00 €
Coste total mano de obra:	1,752.62 €

Coste total de los recursos

La suma de los costes por mano de obra y de los costes por recursos materiales es lo que constituye el Presupuesto de ejecución material.

Tabla 10: Costes Presupuesto de ejecución material

Presupuesto de ejecución material	
Concepto	**Coste**
Costes por mano de obra	15,472.45 €
Costes por recursos materiales	1,752.62 €
Coste total:	17,225.07 €

Gastos generales.

Bajo Gastos generales se incluyen todos aquellos gastos derivados de la utilización de instalaciones, gastos fiscales, etc. Prorrateados a los meses de trabajo estimados duranteel trabajo.

Además se incluye en el último apartado un 6% de incremento de coste debido al beneficio industrial de la empresa.

Con esto, el Presupuesto de Ejecución por contrata queda como sigue:

Tabla 11: Costes Presupuesto de Ejecución por contrata

Presupuesto de Ejecución por contrata	
Concepto	**Coste**
Presupuesto de ejecución material	17,225.07 €
Gastos generales	2,756.01 €
Beneficio industrial	1,033.50 €
Coste total:	21,014.59 €

Honorarios por la redacción y dirección del proyecto.

Tanto para la redacción como para la dirección del proyecto son los asociados a Trabajos tarifados por tiempo empleado, con un valor de un 5%.

Presupuesto total

Sumando todas las imputaciones anteriores, y aplicando el 21% de IVA, se obtiene el presupuesto total.

Tabla 12: Presupuesto total

Presupuesto total	
Concepto	**Coste**
Presupuesto de ejecución por contrata	21,014.59 €
Honorarios por dirección	1,176.82 €
Honorarios por redacción	1,176.82 €
Total libre de impuesto del valor añadido	23,368.22 €
IVA (21%)	4,907.33 €
Coste total:	**28,275.54 €**

Madrid, Mayo de 2014

El Ingeniero Jefe de Proyecto

Fdo.: Fernando García Gutiérrez
Ingeniero de Telecomunicación