Smart Grids Colombia VISIÓN 2030

Parte III

Política y Regulación

Abril de 2016

Equipo de Trabajo

Editores:
Grupo Técnico Proyecto BID integrado por Representantes de:

Banco Interamericano de Desarrollo (Cooperación Técnica)
José Ramón Gómez Guerrero
Jorge Luis Rodríguez Sanabria
Juan Eduardo Afanador Restrepo

Ministerio de Minas y Energía
Marie Paz Rodríguez Mier
Oficina de Asuntos Ambientales y Sociales

Carlos Arturo Rodriguez Castrillón
Profesional Especializado
Oficina Dirección de Energía

Ministerio de Tecnologías de la Información y las Comunicaciones
Liliana Jaimes Carrillo
Despacho Viceministerio TI

Unidad de Planeación Minero-Energética
Camilo Táutiva Mancera
Asesor de Energía

Iniciativa Colombia Inteligente
Alberto Olarte Aguirre
Secretario Técnico C N O – Presidente Colombia Inteligente

Renato Humberto Céspedes Gandarillas
Coordinador Técnico

Firmas Consultoras

Experto en Regulación TIC

Julián Gómez Pineda

Bogotá D.C., Abril de 2016

NOTA ACLARATORIA - *DISCLAIMER*

1. Los planteamientos y propuestas presentados en este documento son los resultados del análisis y elaboración del Estudio desarrollado por el Equipo de Trabajo en el marco de la Cooperación Técnica ATN-KK-14254-CO (CO-T1337) con el aporte de fondos provenientes del Fondo Coreano para Tecnología e Innovación a través del Banco Interamericano de Desarrollo –BID–. Estos planteamientos y propuestas no representan ni comprometen la posición y planteamientos de las entidades oficiales del Gobierno Colombiano participantes.

2. Los análisis realizados en el desarrollo de la Cooperación Técnica consideraron la información disponible hasta el mes de diciembre del año 2015, fecha en la cual finalizó de manera oficial el trabajo realizado durante esta cooperación.

Tabla de Contenido

Índice de figuras

Índice de Tablas

Parte 3B. Estudio a Nivel Regulatorio y de Política relacionado con las TIC para el desarrollo de la Smart Grid Visión 2030

1. Introducción

Los tópicos cubiertos en este entregable desarrollan los siguientes objetivos específicos del proyecto:

a) Efectuar una revisión de experiencias a nivel internacional de aspectos de política y regulación de telecomunicaciones y TIC involucradas en la implementación de Redes Inteligentes[1]
b) Realizar un diagnóstico del esquema regulatorio colombiano en cuanto al desarrollo de las TIC asociadas al sector eléctrico y en particular al despliegue de las RI para identificar barreras y oportunidades, teniendo en cuenta la revisión de experiencias a nivel internacional. Las tecnologías e implementaciones de RI más relevantes para el estudio son identificadas como parte del Componente I de la Cooperación Técnica (CT).
c) Analizar los segmentos, actores y/o componentes del sector de las telecomunicaciones relacionados con el sector eléctrico y en concreto con el desarrollo de las Redes Inteligentes para establecer su situación actual, grado de interacción, coordinación y sus necesidades a nivel de instrumentos regulatorios
d) Identificar y priorizar las medidas regulatorias a implementar en el sector de telecomunicaciones en Colombia que brinden soporte para el desarrollo de las Redes Inteligentes.
e) Detallar el conjunto de recomendaciones para la modificación y/o adecuación de normatividad en aspectos de telecomunicaciones tendientes a la implementación de las RI en el sector eléctrico colombiano.
f) Los resultados de la presente consultoría serán coordinados en conjunto por el consultor encargado de elaborar recomendaciones a nivel regulatorio y de política en el sector eléctrico, para el desarrollo de las redes inteligentes en Colombia

Inicialmente se identificó para el análisis comparativo internacional a Brasil, Chile, Reino Unido y la Unión Europea con énfasis en España y Suecia. Sin embargo, durante la ejecución detallada del análisis y búsqueda de referencias internacionales se encontraron otras experiencias relevantes de acuerdo con el tema bajo análisis, de manera que se procedió con libertad y se incluyeron en algunos casos experiencias de la Agencia Internacional de Energía (AIE), la Organización de Estados Americanos (OEA), los Estados Unidos de América y Holanda. En general, se adoptó el criterio de

[1] Los términos Redes Inteligentes y Smart Grid, sus respectivas siglas RI - SG y Hoja de Ruta y Mapa de Ruta son utilizados indistintamente en estos documentos.

incluir para cada tema bajo comparación aquellos países u organismos internacionales que podían resultar más valiosos.

2. Arquitectura de Redes Inteligentes y su Relación con los Aspectos de Política y Regulación de TIC

Recapitulando sobre los temas ya expuestos encontramos que:

La arquitectura propuesta y presentada en esta sección 2 ha sido construida considerando los principales objetivos energéticos de Colombia enunciados en la Parte I Sección 2 a saber:

1. Objetivo Estratégico - Acceso Universal / Un País Formal
2. Objetivo Estratégico - Seguridad y Calidad / Un País Productivo y Eficiente
3. Objetivo estratégico – Competitividad / Un País Competitivo
4. Objetivo estratégico – Sostenibilidad / Un País Eficiente
5. Objetivo estratégico – Progreso Social / Un País de Oportunidades

Para el cumplimiento de esos objetivos se han considerado diferentes herramientas tecnológicas:

1. Contadores Inteligentes (CI) y *Advanced Metering Infrastructure* (AMI).
2. *Advanced Distribution Automatization* (ADA)
3. *Distributed Energy Resources* (DER)
4. Sistemas energéticos distribuidos - vehículos eléctricos
5. Gestión de activos

La forma como cada una de estas tecnologías y sus funcionalidades asociadas apoya el cumplimiento de los objetivos estratégicos se presenta en la Tabla 1.

Tabla 1. Mejoras obtenidas por la implementación de cada tecnología de RI

TECNOLOGÍA	FUNCIONALIDAD	Reducción de pérdidas técnicas	Reducción de pérdidas no técnicas	Aplanamiento de la curva de demanda	Reducción de costes de comercialización (y operación remota)	Mejora de la continuidad de suministro	Reducción de emisiones de CO_2	Aumento de la independencia energética ante fenómenos naturales	Aumento de vida útil y ahorro de inversiones para aumentar la capacidad de la red de distribución	Mejora del factor de potencia
CIs y monitorización (AMI)	Limitación de potencia				✓					
	Información al usuario			✓						
	Detección de manipulación y aviso a compañía		✓							
	Lectura y operación remota		✓		✓					
	Gestión activa de cargas			✓						
	Tarificación horaria			✓						
	Medida de generación distribuida		✓		✓					
Automatización de la red de distribución (ADA)	Telemando (control remoto)					✓				
	Localización de faltas					✓				
	Self-healing					✓				
	Reconfiguración automática	✓							✓	
Recursos distribuidos (DER)	Generación distribuida en BT (FV)	✓		✓			✓	✓		✓
	Almacenamiento			✓						
Vehículo eléctrico	Movilidad pública						✓			
	V2G			✓			✓			
Gestión de activos									✓	

Fuente: CIRCE

Se establecieron un conjunto de indicadores claves de desempeño (KPIs) y establecieron las metas para cada uno de ellos. La viabilidad de la implementación de cada una de las funcionalidades fue construida considerando 4 variables: coste de implementación, madurez tecnológica, barreras regulatorias y barreras sociales.

Con base en el análisis de estas variables se elaboró una matriz de viabilidad para cada una de las funcionalidades y se realizó una valoración de la influencia de cada funcionalidad de RI sobre los KPIs y se ponderaron la contribución de los KPIs al objetivo global de Colombia la cual se presenta en la siguiente tabla.

Tabla 2 . Importancia de cada funcionalidad en la consecución de los objetivos de Colombia

Funcionalidad	Importancia relativa (%)
Generación distribuida en BT (FV)	23,71
Telemando	15,47
Detección manipulación	14,10
Localización de faltas	9,17
Lectura y operación remota	8,69
Medida Generación Distribuida	6,04
Gestión de activos	4,15
Almacenamiento	3,32
Información del usuario	2,84
Self-Healing	2,29
Tarificación horaria	2,21
Reconfiguración Automática	2,14
Gestión de cargas	1,90
V2G	1,39
Limitación de potencia CI	1,38
Movilidad Eléctrica	1,19

Fuente: CIRCE

Como parte el análisis de TIC de la Parte II se escogió como referencia para el análisis del conjunto de funcionalidades previstas, el modelo CEN-CENELEC-ETSI *Smart Grid Architecture Module* (SGAM) del *Smart Grid Coordination Group* (CEN-CENELEC-ETSI Smart Grid Working Group , 2012). Dicho modelo ha sido conformado por las tres organizaciones de estandarización oficialmente reconocidas por la Unión Europea (UE) como las responsables de la definición de estándares voluntarios a nivel Europeo[2]: el *Comité Européen de Normalisation*, el *Comité Européen de*

[2] Al respecto, ver por ejemplo:
https://www.cen.eu/about/Pages/default.aspx
http://www.cenelec.eu/aboutcenelec/whoweare/index.html

Normalisation Electrotechnique y el *European Telecommunications Standard Institute* (CEN-CENELEC-ETSI).

Debe destacarse entonces que como resultado consignado en la Parte II de este compendio se han considerado la elección de este modelo Europeo para usarlo como referencia sobre otros puntos de vista como el del *National Institute of Standards and Technology* (NIST) del Departamento de Comercio de los Estados Unidos.

La arquitectura SGAM considera tres dimensiones: (i) dominios los cuales están físicamente relacionados con la red eléctrica[3], (ii) capas de interoperabilidad que permiten la representación de entidades y sus relaciones en el contexto de los dominios *Smart Grid* (SG), jerarquías de sistemas de información y en consideración a aspectos de interoperabilidad[4] y (iii) zonas jerárquicas las cuales representan los niveles jerárquicos de gestión de un sistema de potencia de conformidad con estándares de la Inter*national Electrotechnical Commission* IEC (IEC, 2011)[5].

Los estándares de comunicaciones disponibles en la actualidad y que son considerados por el modelo SGAM, están especificados en uno de estos reportes: el documento SGCG/M490/G *Smart Grid Set of Standards* (CEN-CENELEC-ETSI, 2014) ver Tabla 3. La lista de estándares se incluye en el Anexo 2 de la PARTE IV.

Tales estándares involucran algunos de los cuerpos de normalización más importantes de la industria de telecomunicaciones a nivel global: el *3rd Generation Partnership Project* (3GPP), el *Internet Engineering Task Force* (IETF), la *European Standards*[6] (CEN) (Unión Europea, 2012), *European Telecommunications Standard Institute* (ETSI), la *International Electrotechnical commission* (IEC), el *Institute of Electrical and Electronics Engineers* (IEEE), la *International Organization for Standardization* (ISO) y la *International Telecommunications Union* (ITU).

http://www.etsi.org/about/what-we-are

3 Estos son: Generación, transmisión, distribución, recursos de energía distribuidos (DER), e instalaciones del cliente.

4 Conformadas por: Capa de negocios, capa funcional, capa de información, capa de comunicaciones y capa de componentes

5 Las cuales son: Procesos, campo, estación, operación, empresa y mercado.

6 Estándares que han sido ratificados por uno de los tres organismos europeos de normalización: CEN, CENELEC o por el ETSI; que son reconocidos como competentes en el ámbito de la normalización técnica voluntaria de acuerdo con el Reglamento de la UE 1025/2012.

Tabla 3. Desarrollos de estandarización para la arquitectura de referencia SGAM de CEN-CENELEC-ETSI

Nombre del Estándar	Título del documento
SG-CG/ M490/F	Overview of SG-CG Methodologies. Version 3.0 (11/2014)
SGCG/M490/G	Smart Grid Set of Standards. Version 3.1 (10/2014)
SG-CG/M490/H	Smart Grid Information Security. Version 1.0 (12/2014)
SG-CG/M490/I	Smart Grid Interoperability: Methodologies to facilitate Smart Grid system interoperability through standardization, system design and testing. (10/2014)
SG-CG/M490/J	General Market Model Development: The conceptual model and its relation to market models for Smart Grids. Version 3.0 (11/2014)
SG-CG/M490/K	SGAM usage and examples: SGAM User Manual - Applying, testing & refining the Smart Grid Architecture Model (SGAM). Version 3.0 (11/2014)
SG-CG/M490/L	Flexibility Management: Overview of the main concepts of flexibility management. Version 3.0 (11/2014)

Fuente: Consultor Julián Gómez (con base en información pública de CEN, CENELEC y ETSI.)

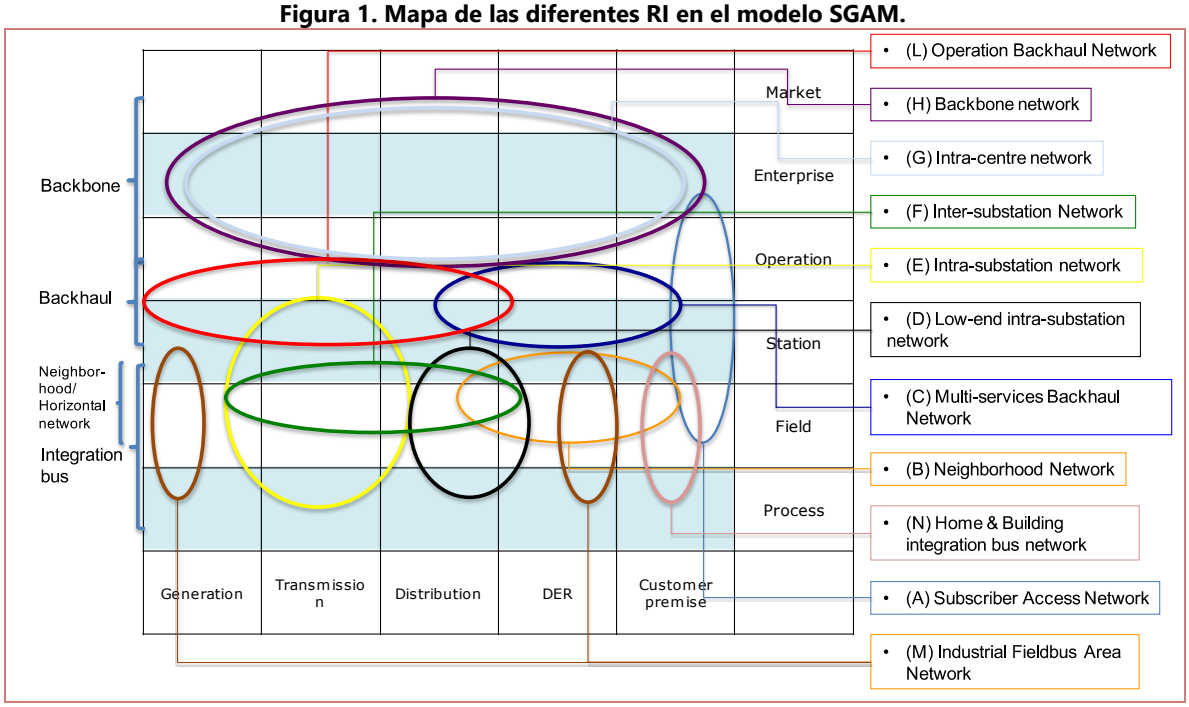
El modelo SGAM permite que dependiendo del tipo de aplicación de RI, se puedan generar diferentes tipos de redes de comunicaciones soportados en diversas tecnologías de transmisión. De esta forma, los siguientes tipos de redes podrían ser definidas para una RI bajo arquitectura SGAM (CEN-CENELEC-ETSI, 2014):

(A) *Subscriber access network*: redes que proveen accesos de banda ancha hasta las instalaciones del cliente.
(B) *Neigborhood Network*: Redes entre las subestaciones de distribución y los usuarios finales.
(C) *Multiservices Backhaul Network:* Redes en la capa superior del nivel de distribución que provee conectividad de backhaul en dos direcciones: hacía los centros de control o hacía las subestaciones primarias y conectividad peer-to-peer en el nivel de distribución.
(D) *Low-end intra-substation network*: Redes dentro de subestaciones secundarias o dentro de una subestación de transmisión.

(E) *Intrasubstation Network*: Redes dentro de las subestaciones de distribución primarias o dentro de las subestaciones de transmisión.
(F) *Intersubstation Network*: Redes que interconectan subestaciones entre sí y con centros de control.
(G) *Intra-control Centre/Intra-Data Centre Network*: redes dentro de dos tipos de facilidades: centros de control y centros de datos. Son redes al mismo nivel lógico pero físicamente son distintas.
(H) *Backbone Network*: Redes interempresas o intercentros de control.
(L) *Operation Backhaul Network*: Redes que permiten soportar operación remota.
(N) *Home and Building integration bus network*: redes que conectan componentes o subsistemas dentro de una casa o edificio.
(M) *Industrial Fieldbus Area Network*: Redes que interconectan equipos de procesamiento de control principalmente en generación de potencia.

Estas redes permiten establecer una correspondencia de las diferentes RI en el modelo SGAM, que relaciona los dominios y zonas (ver Figura 1) con el tipo de red. Estas relaciones son discutidas en el documento de estándares de RI de CEN-CENELEC-ETSI (CEN-CENELEC-ETSI, 2014) y se reproducen en el mapa de la Figura 1.

Figura 1. Mapa de las diferentes RI en el modelo SGAM.



Fuente: CEN-CENELEC-ETSI Smart Grid Coordination Group

Existe además una relación entre los estándares que se presentaron en el *Anexo 2* y su aplicabilidad en los diferentes tipos de redes presentados en la Figura 1[7], mismo que se reproduce en la Tabla 4.

7 Al respecto puede verse la tabla 81 del documento de estándares de RI de CEN-CENELEC-ETSI [8]

Al respecto la Parte II Sección 5 y *Anexos 2, 5 y 8* presentan las tecnologías de comunicaciones disponibles las cuales en principio tienen algunas diferencias con la tabla 81 del documento de estándares de RI de CEN-CENELEC-ETSI (CEN-CENELEC-ETSI, 2014).

Tabla 4. Abanico de tecnologías de comunicaciones disponibles para los diferentes tipos de subredes de la Red Inteligente

		Subscriber Access Network	Neighborhood network	Multi-services backhaul Network	Low-end intra-substation network	Intra-substation network	Inter substation network	Intra-Control Centre / Intra-Data Centre network	Backbone Network	Operation Backhaul Network	Home and Building integration bus Network	Industrial Fieldbus Area Network
		A	B	C	D	E	F	G	H	L	N	M
IEEE protocols (MAC-PHY)												
	IEEE 1901.2 Narrow band PLC											
	IEEE 1901 Broad band PLC											
	IEEE 802.15.4 wireless Low Power											
	IEEE 802.11 (WIFI)											
	IEEE 802.3/1 (Ethernet)											
	IEEE 802.16 (Wimax)											
IETF protocols (Layer 3, 4 and above)												
	IPv4											
	IPv6											
	RPL / 6LowPan / 6TiSCH											
	IP MPLS / MPLS TP											
	XMPP											
ITU Protocols												
	SDH/OTN											
	DSL/PON											
	DWDM											
	Narrow band PLC (Medium & Low voltage)											
	Narrow band PLC (High & very High voltage)											
	Broadband PLC											
ANSI standards												
	SONET / SONET NG											
ETSI / 3GPP Protocols												
	ETSI TS 102 887 Wireless (IEEE 802.15.4g)											
	GSM / GPRS / EDGE											
	3G / WCDMA / UMTS / HSPA											
	ETSI TS 103 908											
	4G LTE/LTE-A											
EN standards												
	EN 61334											
	EN 14908											
	EN 50090											
	EN 13757											
IEC standards												
	IEC 61158											
	IEC 61850											
	IEC 60870-5											
Higher layer comm protocol *												
Legend		Mostly used										
		May be used										

Fuente: CEN-CENELEC-ETSI Smart Grid Coordination Group

Como es de esperarse, las complejidades inherentes al establecimiento de una RI generan importantes desafíos en dos aspectos relacionados con las TIC: la interoperabilidad y la ciberseguridad.

En cuanto a la Interoperabilidad, existe un documento completo de recomendaciones del CEN-CENELC-ETSI que define un conjunto de metodologías para facilitar la interoperabilidad de los sistemas de una RI o SG mediante la estandarización, el diseño de los sistemas y las pruebas de funcionamiento de los mismos (CEN-CENELEC-ETSI, 2014).

La definición de interoperabilidad adoptada por el modelo CEN-CENELEC-ETSI (CEN-CENELEC-ETSI, 2014), es la misma que se utiliza por parte de la IEEE (IEEE), es decir: "La capacidad de dos o más redes, sistemas, dispositivos, aplicaciones o componentes de interfuncionar, intercambiar y utilizar la información con el fin de realizar las funciones requeridas."

Está claro que la RI concebida como sistema exhibe una alta complejidad en relación con aspectos organizativos y tecnológicos. Su planificación y construcción implica actores diversos de varias organizaciones y dominios de ingeniería. Por lo tanto, un desafío clave de la red inteligente es la integración de generación, transporte, distribución, almacenamiento y consumo de energía eléctrica con los sistemas TIC de apoyo. Por tanto, para crear la RI como un "sistema de sistemas", las funcionalidades e interfaces de sus componentes se deben especificar de antemano. Para que esto funcione, resulta esencial contar con una metodología adecuada para la especificación y gestión de requisitos. Esto asegura la trazabilidad entre las decisiones de diseño y requisitos del sistema, apoya la colaboración entre las partes interesadas mediante la asignación de responsabilidades, permite la construcción del sistema en materia de software y hardware y facilita que el mismo sea probado contra la especificación (CEN-CENELEC-ETSI, 2014).

Aunque el uso de estándares facilita la interoperabilidad a través del diseño y la aplicación de una metodología correcta, estos por si solos no permiten alcanzar un sistema interoperable. Hay otros factores que deben ser tenidos en cuenta para alcanzar la interoperabilidad (CEN-CENELEC-ETSI, 2014):

1. No es lo mismo el diseño de un sistema de red inteligente nuevo que la transformación de un sistema heredado en un sistema interoperable.
2. Se deben recopilar los requisitos de interoperabilidad mediante la identificación de casos de uso en cada una de sus fases (generación, transporte, distribución, almacenamiento y consumo).
3. Finalmente, la validación de la interoperabilidad de los sistemas se realiza a través de pruebas.

En cuanto a la Ciberseguridad existe también un documento completo de recomendaciones del CEN-CENELC-ETSI que aborda el tema de la Seguridad de la Información en las RI o SG, mediante un análisis de los elementos clave de ciberseguridad a nivel de las RI, una revisión de los estándares de seguridad y de la aplicación de casos de uso de seguridad de información en las RI (CEN-CENELEC-ETSI, 2014).

La seguridad de la información de la RI se refiere entonces a las necesidades técnicas y organizacionales para mantener condiciones de seguridad de la información en las redes inteligentes (SGIS) y Protección de Datos y Privacidad (DPP) sostenible y conforme al "estado del arte", permitiendo la recolección, utilización, procesamiento, almacenamiento, transmisión y borrado de toda la información de los actores participantes a ser protegida (CEN-CENELEC-ETSI, 2014).

Finalmente, hay un tercer tema que se ha identificado como muy importante desde la perspectiva de las TIC y es el relacionado con la protección de la privacidad de los usuarios. Efectivamente, la privacidad es una de las principales preocupaciones que han surgido en relación con el despliegue de RI o SG, motivadas en especial por las posibilidades que brindan los contadores inteligentes para establecer detalles sobre los hábitos de vida de los consumidores. Por ejemplo, en el informe de Consultores de la Componente I *(Llombart Estopiñán , et al., "Estudio de factibilidad técnica y económica de soluciones de redes inteligentes para el sector eléctrico colombiano" - Informe 2, 2015*), se explica cómo la información detallada sobre el uso de energía podría poner al descubierto los patrones de uso de energía diarios de una casa y permitir la deducción de qué tipo de dispositivo o

aparato estaba en uso en un momento dado, así como también, revelar las tendencias del comportamiento personal del usuario e inferir información relativa a la vida del consumidor que puede afectar su seguridad e integridad, ya que se aumenta la vulnerabilidad de la persona frente a posibles ataques terroristas o de grupos de cualquier índole que tengan interés en influir en las acciones de las personas. Por tanto es un tema de interés creciente para los usuarios en particular pero también para la sociedad en general, dado que es necesario proteger a los consumidores contra cualquier infracción a la protección de sus datos. Este asunto también es discutido por CEN-CENELEC ETSI en el documento de Seguridad de la Información en las RI *(CEN-CENELEC-ETSI, 2014)*.

Con base en lo anterior, las secciones siguientes abordan una comparación internacional sobre el manejo de política pública y regulación de los temas de ciberseguridad, interoperabilidad y protección de la privacidad de los usuarios, desde la perspectiva de la implementación de RI.

3. Aspectos Claves de TIC relacionados con Redes Inteligentes: Comparación internacional - Ciberseguridad

La ciberseguridad es uno de los temas de mayor importancia en relación con RI desde la perspectiva de las TIC y ha sido el sujeto de numerosos análisis por parte de organismos internacionales, instituciones nacionales y publicaciones especializadas.

El tema es extenso y se ha convertido en un importante tópico de estudio. Por ejemplo, un libro de reciente publicación está dedicado exclusivamente a la Ciberseguridad Aplicada a Redes Inteligentes (Knapp, Samani, & Langill, 2013). Es además un tema en permanente construcción considerando la velocidad de la evolución tecnológica en el área de las TIC y respecto del cual nunca es posible alcanzar un 100% de seguridad (CEN-CENELEC-ETSI, 2014).

A continuación se presentan los puntos más importantes de la comparación internacional, la cual incluye a la (i) Organización de Estados Americanos que presenta un panorama de la situación en las Américas, a los (ii) Estados Unidos de América porque las Normas NERC (*North American Electric Reliability Corporation*) han sido referenciadas en Colombia por el Consejo Nacional de Operación (CNO) en su Guía sobre Ciberseguridad (CNO, 2015), a (iii) Brasil y (iv) Chile que se utilizan como referentes de países Latinoamericanos, al (v) Reino Unido que ha venido construyendo una institucionalidad en torno a la protección cibernética de la infraestructura nacional y a la (vi) Unión Europea que está dando pasos en la adopción de políticas y prácticas de seguridad de redes inteligentes por medio de los trabajos de la la Agencia Europea de Seguridad de Información y Redes (ENISA - *European Network and Information Security Agency*) que recogen las recomendaciones basadas en la arquitectura SGAM propuesta por CEN-CENELEC-ETSI, así como el uso de certificaciones sobre la implementación de RI. Adicionalmente en la UE se revisa con mayor detalle el caso de España.

3.1 Organización de Estados Americanos

Como respuesta a las crecientes amenazas cibernéticas, los delegados de los países del continente americano se han reunido en varias ocasiones durante los últimos diez años para buscar estrategias y acciones en común que detengan estas amenazas.

En el 2004 la Asamblea General de la Organización de Estados Americanos (OEA) aprobó por unanimidad la "Estrategia Interamericana Integral de Seguridad Cibernética" para Combatir las Amenazas a la seguridad cibernética en la resolución AG/RES. 2004 (XXXIV-O/04) (Organización de los Estados Americanos, 2015). En el 2012 los gobiernos de los países americanos firmaron la declaración de "Fortalecimiento de la Seguridad Cibernética de las Américas" (CICTE & OEA, 2015) y para el presente año 2015 el Comité Interamericano contra el Terrorismo (CICTE) de la OEA adoptó[8] la "Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes" (OEA - CICTE, 2015), con lo que se desarrolló un programa regional de seguridad cibernética que busca mejorar la protección de la infraestructura de información crítica en todo el continente.

[8] Aprobado durante la quinta sesión plenaria, celebrada el 20 de marzo de 2015.

Entre los principales objetivos de la Secretaría del CICTE (OEA - CICTE, 2015), se encuentran: (i) el establecimiento de grupos nacionales de "alerta, vigilancia y prevención", también conocidos como Equipos de Respuesta a Incidentes (*CSIRT*) en cada país; (ii) crear una red de alerta Hemisférica que proporciona la formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; (iii) promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y (iv) fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio. El Programa de Seguridad Cibernética de la OEA gira en torno a la implementación del siguiente plan de siete puntos (OEA - CICTE, 2015).

- **Participación de la sociedad civil y del sector privado,** ya que más de 80% de la infraestructura que potencia el Internet y administra los servicios esenciales es propiedad del sector privado y es operada por éste.
- **Crear conciencia** entre los usuarios finales de Internet (incluido internet de las cosas) acerca de las medidas de seguridad cibernética, para asegurar que los individuos entienden los riesgos y la necesidad de adoptar medidas adecuadas para su propia seguridad cibernética.
- **Desarrollo de estrategias nacionales** de seguridad cibernética que permita que los países definan una visión completa de la seguridad cibernética y establezca responsabilidades claras, coordinando acciones entre los gobiernos y los interesados relevantes.
- **Brindar capacitación** para que los funcionarios permanezcan actualizados en el entorno de seguridad cibernética que está en constante evolución.
- **Ejercicios de Gestión de Crisis**. Esto le permite a los Estados Miembros diseñar ejercicios de manejo de crisis de acuerdo con sus necesidades, al tiempo de fortalecer la colaboración a nivel técnico con otros países para responder a las amenazas.
- **Misiones de asistencia técnica**, diseñadas para atender las preocupaciones cibernéticas. Esto involucra visitas, revisiones de las políticas y presentaciones de las autoridades locales, culminando en una serie de recomendaciones de expertos.
- **Compartir información y experiencia**, a través de una red de CSIRTs nacionales y otras autoridades relacionadas con la seguridad cibernética para facilitar la comunicación en tiempo real.

Los estudios más recientes para América relacionados con las amenazas cibernéticas se centran en determinar las actuales tendencias de los ataques a la infraestructura crítica[9]. Es así como en abril de 2015, la OEA en asocio con la compañía privada Trend Micro emitió un informe denominado "Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas" (OEA - TREND MICRO, 2015) con el fin de ayudar a los Estados Miembros a establecer sus capacidades de seguridad cibernética y entender mejor las principales amenazas cibernéticas que afectan esta infraestructura en el continente americano. La información recopilada en el reporte de la OEA ofrece una importante perspectiva de las medidas y políticas de seguridad cibernética de las organizaciones.

[9] La infraestructura crítica consiste, entre otras, en aquellas instalaciones, sistemas y redes, así como servicios y equipos físicos y de tecnología de la información, cuya inhabilitación o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad, la actividad económica, el medio ambiente, servicios de gobierno, o el eficaz funcionamiento de un Estado.

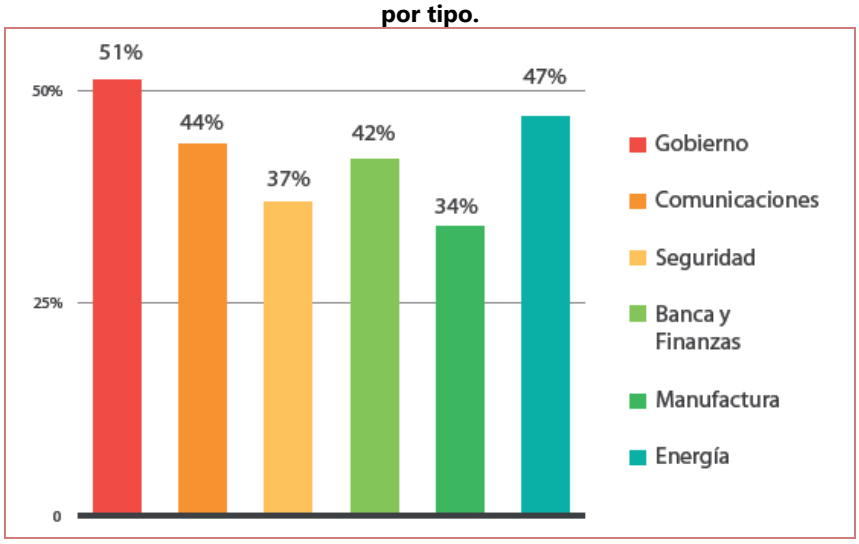
Según este reporte, el gran problema que está reuniendo a los operadores de Protección de Infraestructura Crítica y al gobierno para encontrar una solución, es la seguridad de los Sistemas de Control de Supervisión y Adquisición de Datos (SCADA) así como la seguridad de los Sistemas de Control Industrial. Estos incluyen, entre otros, sistemas que controlan las instalaciones de generación de electricidad. Estos sistemas se han visto comprometidos por ataques utilizando malware, en donde las intrusiones se han manifestado de dos maneras, en una de ellas, el malware se hace pasar por aplicaciones SCADA válidas, en la segunda forma, el malware se utiliza para analizar e identificar protocolos SCADA específicos. El propósito de estos ataques puede ser espionaje industrial o realizar un ataque futuro. Se espera que esta tendencia continúe y aumente en los próximos años, según afirma Trend Micro.

Una de las investigaciones para mitigar los problemas de ciberataques en las futuras redes eléctricas inteligentes que involucran una enorme cantidad de Recursos de Energía Distribuidos (DER , por sus siglas en inglés), es liderada por Steven Low, profesor del Instituto de Tecnología de California, quien presenta algunas conclusiones de los resultados de la investigación sobre la integración de redes informáticas y físicas para optimizar las redes eléctricas desde la generación y transmisión hasta la distribución y el consumo, y afirma lo siguiente: "Al entender los desafíos de ingeniería y los riesgos que traen consigo las oportunidades generadas por los recursos de energía distribuidos (DER), es posible reducir las amenazas potenciales a la seguridad cibernética. Las propiedades de monotonicidad de las fallas de la red provocadas por posibles ataques cibernéticos pueden utilizarse para desarrollar estrategias de desbordamiento de cargas. Las limitaciones de seguridad pueden incluirse en las fórmulas del Flujo de Energía Óptimo (OPF) para mantener la eficiencia de la red. Además, el control ubicuo de frecuencias en el lado de las cargas puede utilizarse para conservar la estabilidad de la red a través de algoritmos distribuidos que se ajusten a los ciberataques potenciales" (OEA - TREND MICRO, 2015).

Con el fin de mostrar un mapa general de la situación de ciberseguridad para infraestructura crítica en países de América, se presentan a continuación los resultados de una encuesta realizada a los Jefes de Seguridad de las principales infraestructuras críticas en los países miembros de la OEA, (OEA - TREND MICRO, 2015).

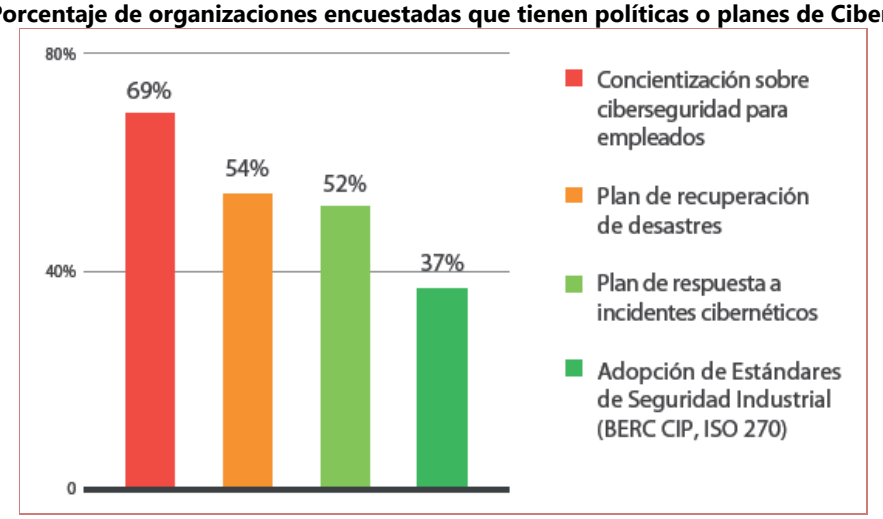
La Figura 2 muestra que los sectores de gobierno y energía son los que más han recibido ciberataques. En la Figura 3 se muestra que únicamente el 37% de las organizaciones encuestadas han adoptado estándares de seguridad industrial como el BERC CIP e ISO 2700x. Trece países miembros de la OEA han experimentado intentos de manipulación a equipos de sus instituciones gubernamentales a través de una red o sistema de control, incluyendo a Colombia. En el reporte se afirma que es necesario un presupuesto adicional para implementar los sistemas de seguridad adecuados pues la mayoría de los ataques presentes y futuros no pueden descubrirse utilizando las medidas de seguridad tradicionales.

Figura 2. Porcentaje de Organizaciones que experimentaron intentos de eliminar o destruir información por tipo.



Fuente: Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas – OEA y Trend Micro (OEA - TREND MICRO, 2015).

Figura 3. Porcentaje de organizaciones encuestadas que tienen políticas o planes de Ciberseguridad



Fuente: Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas – OEA y Trend Micro (OEA - TREND MICRO, 2015).

3.2 Estados Unidos

El papel fundamental de la ciberseguridad para garantizar el funcionamiento eficaz del Smart Grid, se encuentra expresado en el documento del Departamento de Energía (DOE) titulado "*Roadmap to Achieve Energy Delivery Systems Cybersecurity*" (ESCSWG - Energy Sector Control System Working Group, 2011) publicado en septiembre de 2011, donde se afirma que, desde el 2006, la ciberseguridad ha ganado alto interés por parte de varios organismos, tales como la Presidencia, el Congreso y la industria de los Estados Unidos.

Los legisladores estadounidenses han propuesto una serie de proyectos de ley para mejorar la ciberseguridad. A su vez, la Administración determinó que la ciberseguridad tenía el carácter de alta prioridad nacional. Adicionalmente, la Corporación NERC incluye a la ciberseguridad en la lista de los principales problemas emergentes de confiabilidad que enfrenta actualmente la industria eléctrica.

En cuanto a la legislación estadounidense, la importancia de la ciberseguridad para la modernización de la red eléctrica nacional se encuentra documentada en la Sección 1301 de la Ley de independencia energética y seguridad de 2007 (U.S. Government - 110th United States Congress, 2007). Algunos de los apartes relacionados con la Política de modernización de la red eléctrica se reproducen a continuación (traducción libre del original en inglés).

- "Esta es la política de los Estados Unidos para apoyar la modernización del sistema de distribución y transmisión eléctrica de la Nación para mantener una infraestructura eléctrica confiable y segura que pueda satisfacer el crecimiento futuro de la demanda y para lograr cada uno de los siguientes enunciados, que en conjunto caracterizan a un Smart Grid:
    1. Aumento del uso de tecnología de información digital y de control para mejorar la confiabilidad, seguridad y eficiencia de la red eléctrica
    2. Optimización dinámica de las operaciones de red y recursos con una ciberseguridad completa.
    3. Despliegue e integración de recursos distribuidos y generación, incluyendo los recursos renovables.
    4. Desarrollo e incorporación de respuesta de la demanda, recursos del lado de la demanda y recursos de eficiencia energética.
    5. Despliegue de tecnologías "Smart" (tiempo real, automatizado, con tecnologías interactivas que optimicen el funcionamiento físico de aparatos y dispositivos de consumo) para la medición, comunicaciones concernientes al estado y operaciones de la red, y automatización de la distribución.
    6. Integración entre aparatos "inteligentes" ("Smart") y dispositivos de consumo.
    7. Despliegue e integración de tecnologías avanzadas de almacenamiento de electricidad y de recortes de picos (peak-shaving).
    8. Suministro a los consumidores de información oportuna y opciones de control.
    9. Desarrollo de estándares para la comunicación e interoperabilidad.
    10. Identificación y reducción de las barreras injustificadas o innecesarias para la adopción de tecnologías, prácticas y servicios de Smart Grid."

Por otra parte, el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, en septiembre del 2014 publicó el reporte interinstitucional (IR – *Interagency Report),* **NISTIR 7628** Revisión 1 (NIST (National Institute of Standars and Technology), 2014), donde se presentan los lineamientos para la ciberseguridad en redes inteligentes. Este reporte fue desarrollado por miembros del *Smart Grid Interoperability Panel* (SGIP), *Grid Cybersecurity Committee* (SGCC) y el *Information Technology Laboratory* (ITL) del NIST. El objetivo del documento es suministrar a las organizaciones un marco analítico que les sirva para desarrollar estrategias efectivas de

ciberseguridad adaptadas a sus variantes particulares y relacionadas con las características de redes inteligentes, riesgos y vulnerabilidades.

Adicionalmente, el Presidente de los Estados Unidos, por medio de Orden Ejecutiva 13636, encargó al NIST para que junto con las entidades involucradas, desarrollara un marco para la reducción de riesgos cibernéticos en infraestructura crítica. Como resultado, en febrero de 2014, se emitió el documento titulado "*Framework for Improving Critical Infrastructure Cybersecurity*" (NIST, 2014), el cual proporciona estándares, lineamientos y mejores prácticas para promover la protección de infraestructura crítica, aplicable al subsector eléctrico y las RI; y que junto con otros estándares, lineamientos y prácticas ya existentes para ciberseguridad de RI, pueden ser aprovechados para generar un programa de gestión de riesgo en el contexto de cada empresa u organización.

El *Interagency Report* del NIST, citado arriba, es complemento de un documento anterior llamado "*NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*" (conocido como NIST *Special Publication* 1108R2) (NIST - Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, 2012) publicado en febrero de 2012 y el cual traza un plan para transformar los antiguos sistemas de energía eléctrica en una RI interoperable que permita transferir información y energía en doble vía. Dentro de este plan, el NIST establece ocho áreas prioritarias de trabajo, que son:

- Eficiencia de energía al consumidor y respuesta a la demanda.
- Conocimiento de la situación en tiempo real del desempeño y los componentes del sistema de energía.
- Almacenamiento de energía.
- Transporte eléctrico (Vehículos eléctricos)
- Comunicaciones en redes públicas y privadas.
- Infraestructura de medición avanzada.
- Gestión de red de distribución (Distribution grid)
- Ciberseguridad.

Ambos documentos mencionados anteriormente, están en concordancia con las políticas de *Smart Grid* declaradas por la Comisión Federal para la Regulación de la Energía (FERC - *Federal Energy Regulatory Commission*) publicadas en julio de 2009 bajo el nombre "*Smart Grid Policy*" – 128 FERC 61,060 (FERC (Federal Energy Regulatory Commission), 2009). En el capítulo 1 del mismo documento de políticas (18 CFR Chapter 1), la Comisión adopta su posición de política declarando que la ciberseguridad es esencial para la operación de *Smart Grid* y que el desarrollo de estándares de ciberseguridad es una prioridad fundamental, adicionando además que la ciberseguridad y la seguridad física son los temas de mayor preocupación para la Comisión y la industria eléctrica, por lo que estos dos temas han recibido la mayor atención en el marco de la creación de los últimos estándares federales obligatorios y exigibles.

En mayo de 2012, el Departamento de Energía (DOE) de los Estados Unidos, en colaboración con el Instituto NIST y la Corporación NERC (North American Electric Reliability Corporation) desarrollaron el documento titulado "*Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*" (U.S. Department of energy, 2013), con el objeto de capacitar a las organizaciones del subsector eléctrico para que implementen los procesos de gestión de riesgos de forma efectiva y eficiente, así como la implementación de un programa de ciberseguridad nuevo o construido sobre las políticas o procedimientos en ciberseguridad existentes dentro de la organización. La corporación NERC también cuenta con una normativa compuesta por los denominados estándares CIP (Critical Infrastructure Protection).

Existen algunos proyectos de ley relacionados con ciberseguridad que están siendo debatidos en el Congreso de los Estados Unidos, los cuales se muestran en la Figura 4. El análisis de leyes relacionadas con problemas de ciberseguridad para el sistema eléctrico se presenta en el reporte titulado "*Cybersecurity Issues for the Bulk Power System*" (CRS - Congressional Research Service, 2015), publicado por el *Congressional Research Service* en junio del 2015.

Figura 4. Legislaciones pendientes sobre ciberseguridad, 114° Congreso de los Estados Unidos.

Table 1. Pending Legislation 114th Congress

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 1731	National Cybersecurity Protection Advancement Act of 2015	Homeland Security	April 13, 2015	Referred to the House Committee on Homeland Security	April 13, 2015
H.R. 234	Cyber Intelligence Sharing and Protection Act	Armed Services, Homeland Security, Intelligence (Permanent), Judiciary	January 8, 2015	Referred to the Subcommittee on the Constitution and Civil Justice.	February 2, 2015
H.R. 85	Terrorism Prevention and Critical Infrastructure Protection Act of 2015	Homeland Security	January 6, 2015	Referred to Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.	January 23, 2015
S. 456	Cyber Threat Sharing Act of 2015	Homeland Security and Governmental Affairs	February 11, 2015	Referred to the Committee on Homeland Security and Governmental Affairs.	February 11, 2015

Source: Compiled by the Congressional Research Service from Congress.gov.

Fuente: Congressional Research Service (CRS - Congressional Research Service, 2015).

3.3 Brasil

Desde una perspectiva macro, Brasil viene trabajando en el establecimiento de un marco de políticas y regulación relacionadas con ciberseguridad desde el año 2000 cuando se creó, mediante un Decreto Presidencial (Presidência da República, 2000), el Comité Gestor de Seguridad de la Información conformado por 17 entidades del gobierno Brasileño, con el objetivo de asesorar a la Secretaría Ejecutiva del Consejo de Defensa Nacional.

A partir de esa fecha Brasil ha venido trabajando activamente mediante la elaboración de Leyes, Decretos, Ordenanzas y Normas Complementarias relacionadas con Ciberseguridad.

En el año 2010, el Departamento de Seguridad de la Información y las Comunicaciones, que se encuentra adscrito a la Presidencia de la República, publicó una guía de referencia para la seguridad de infraestructuras críticas de información (Departamento de Segurança da Informação e Comunicações , 2010), el cual establece recomendaciones para (i) el mapeo de activos de infraestructuras críticas de información; (ii) los requisitos mínimos necesarios para la seguridad de la

información en Infraestructuras Críticas; y (iii) el método de identificación de amenazas y generación de alertas de seguridad de infraestructuras críticas de información.

Luego, en el año 2015, el Departamento de Seguridad de la Información y las Comunicaciones publicó su Estrategia de Seguridad de la Información y las Comunicaciones y de Seguridad Cibernética de la Administración Pública Federal para el periodo 2015-2018 (Departamento de Segurança da Informação e Comunicações , 2015).

Por otra parte, el gobierno de Brasil viene trabajando desde el año 2010 para la creación de su hoja de ruta para Redes Inteligentes. En ese año el Ministerio de Minas y Energía emitió una ordenanza para la creación de un grupo de trabajo que analizara e identificara las acciones necesarias para apoyar el establecimiento de políticas públicas para la implementación del "Programa Brasileño de Smart Grid " (Ministério das Minas e Energia, 2010). Luego en el año 2011, la Agencia Brasilera de Desarrollo Industrial (ABDI) articuló un Grupo de Trabajo de Gobierno para elaborar una estrategia para el desarrollo de la industria de proveedores de RI.

Los análisis iniciales de la ABDI en el año 2012 (ABDI, 2012) identificaron los niveles de riesgo asociados con la seguridad de la información en el desarrollo de RI desde cinco perspectivas, como se muestra en la Tabla 5. Mayores niveles de riesgo se identificaban como oportunidades que justificaban asignaciones preferenciales de recursos de I+D, siendo el vector tecnológico de seguridad de información el que presentaba mayores riesgos entre todas las perspectivas analizadas.

Tabla 5. Nivel de riesgo asociado con la I+D de los vectores tecnológicos

Vectores Tecnológicos y actividades relacionadas	Falta de estandarización o en conflicto con otras normas;	Falta de inversiones públicas y / o privadas	desarrollo a largo plazo y de alto riesgo	transformación de la solución de la situación actual, con alto retorno	solución factible de acuerdo con el presupuesto disponible en I + D.
Tecnologías de Información y Comunicación					
Seguridad de la información	Medio	Alto	Alto	Alto	Alto

Fuente: Consultor Julián Gómez (Adaptado de ABDI (ABDI, 2012))

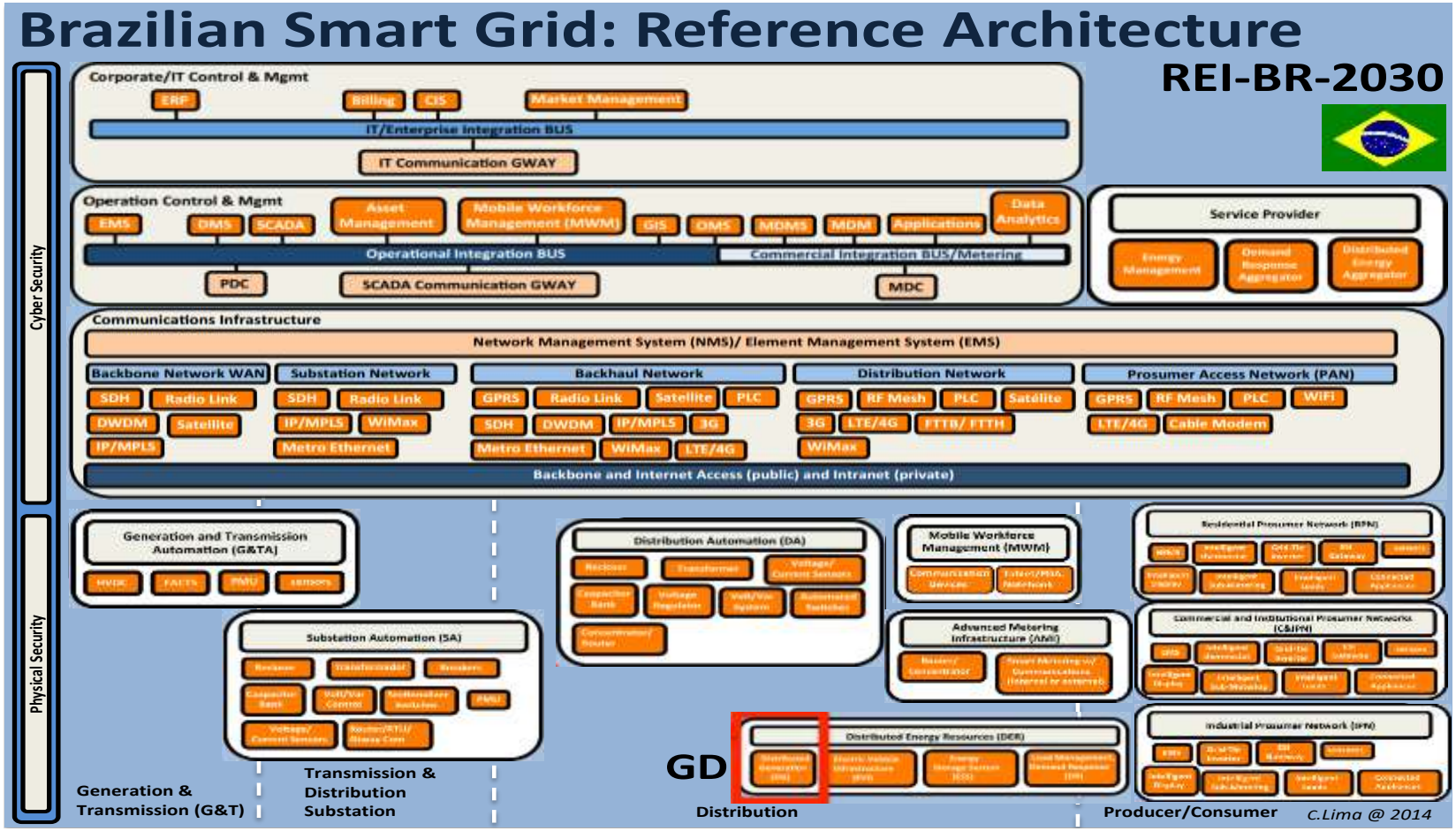
De acuerdo con los análisis de ABDI en el año 2012 (ABDI, 2012) las técnicas de cifrado, autenticación y otras similares, dirigidas a la protección de la información estaban restringidas en ese momento a los componentes críticos de red como los medidores inteligentes. Sin embargo, a medida que el control de la red se descentraliza más, la información se almacena en diferentes puntos de la red, lo que aumenta la necesidad de identificar las amenazas a la integridad de la red y los requisitos de seguridad a ser incorporados en las plataformas de comunicación que soportan las redes inteligentes.

En 2013, el grupo de trabajo gubernamental coordinado por la ABDI definió el "*Programa Brasileiro para desenvolvimento da Indústria fornecedora de Redes Elétricas Inteligentes*" el cual incluía entre

sus áreas estratégicas para desarrollo futuro la necesidad de creación de criterios para Ciber-Seguridad.

A finales de 2013 se creó la primera proposición de la Arquitectura de Referencia de Redes Eléctricas Inteligentes de Brasil, la cual se denominó (REI-BR-2030). Este ha sido considerado como el primer paso en la creación de una "hoja de ruta brasileña" para las Redes Inteligentes. Como puede apreciarse en la Figura 5, la Ciberseguridad ha sido incluida como un elemento transversal dentro de la arquitectura de referencia para Redes Inteligentes definido por Brasil.

Figura 5. Arquitectura de referencia de Red Inteligente para Brasil REI-BR-2030.



Fuente: C. Lima (Lima, 2014)

En el 2014 la ABDI publicó una versión preliminar del mapeo de la cadena de Proveedores TIC y sub productos y servicios de Red Inteligente (ABDI, 2014), la cual, sin embargo, no indica la existencia de políticas o regulación específica para ciberseguridad en Redes Inteligentes en Brasil.

Se considera por tanto que la ciberseguridad en redes inteligentes si bien ha sido ampliamente identificada en Brasil como un tema prioritario que está definido dentro de la arquitectura de red y para el cual se cuenta con recomendaciones de carácter general en la Guía de referencia para la seguridad de infraestructuras críticas de información (Departamento de Segurança da Informação e Comunicações , 2010), todavía es un tema que se encuentra en desarrollo y por tanto no cuenta con recomendaciones específicas.

3.4 Chile

Chile cuenta dentro del Ministerio del Interior y Seguridad Pública con un Departamento de Crimen Organizado, el cual es responsable de elaborar estrategias para el combate de ilícitos como el narcotráfico, terrorismo, ciberseguridad y piratería (propiedad intelectual e industrial), entre otros. Dentro de los principales logros sobre el tema que figuran en el reporte del Ministerio del Interior y Seguridad Pública (Ministerio del Interior y Seguridad Pública de Chile, 2015), se encuentran:

- La creación del Comité Interministerial sobre Ciberseguridad, según Decreto 533 de abril 27 del 2015 (MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA, 2015), el cual está integrado por representantes de las subsecretarías de Interior, Secretaría General de la Presidencia y Relaciones Exteriores. El objetivo principal es crear una política nacional de ciberseguridad y asesorar en la coordinación de acciones, planes y programas de los distintos actores institucionales en la materia, con el propósito de resguardar la imagen, dignidad y honor de las personas, advertir los riesgos de los delitos digitales que puedan afectar gravemente la seguridad pública, los derechos fundamentales e inclusive comprometer la seguridad externa del país mediante actividades de espionaje y ciberataques llevados a cabo por otros países, grupos organizados o, incluso, por sujetos individuales (Ministerio del Interior y Seguridad Pública - Subsecretaría del Interior, 2015)(Ministerio del Interior y Seguridad Pública, abril 20 de 2015).
- Los avances para evaluar la adhesión de Chile a la Convención de Ciber Delitos del Consejo de Europa, llamada Convención de Budapest, cuya misión obliga a sus países asociados a adoptar tipos penales sobre infracción a la propiedad intelectual, fraude informático, pornografía infantil y violaciones a sistemas informáticos. A este convenio ya están adheridos países como Estados Unidos, Japón, Australia, Alemania e Inglaterra. El Convenio de Budapest también insta a la adopción de técnicas intrusivas de investigación y conservación de evidencia para combatir delitos cometidos mediante el uso de sistemas informáticos. Por último, regula la asistencia mutua entre los estados partes durante posibles investigaciones penales y puede operar como tratado de extradición para estas mismas infracciones (Ministerio del Interior y Seguridad Pública - Subsecretaría del Interior, 2015).

Dentro de las acciones programadas para el 2015 y el primer trimestre del 2016, se encuentra el proceso para formular una Política Nacional de Ciberseguridad que proteja la seguridad del país, sus instituciones y los derechos de las personas en este ámbito (Ministerio del Interior y Seguridad Pública de Chile, 2015).

Por tanto, Chile todavía se encuentra en el proceso de creación de una Política Nacional de Ciberseguridad y no se identifican recomendaciones específicas en relación con RI.

3.5 Reino Unido

En el año 2010 el Reino Unido publicó su Estrategia de Ciberseguridad con visión hacía el 2015 (Minister for the Cabinet Office, 2011), la cual reconocía que las redes digitales ya son determinantes en el suministro de electricidad en dicho país. Como parte de la ejecución de la Estrategia Nacional de Ciberseguridad las empresas del Reino Unido han recibido una Guía de Ciberseguridad para negocios que busca reducir el riesgo cibernético en áreas críticas (Cabinet Office, 2013).

Adicionalmente Reino Unido cuenta con un Centro de Protección de la Infraestructura Nacional (CPNI), el cual cubre las áreas de seguridad física, personal y ciberseguridad[10]. La Infraestructura Nacional es definida por el gobierno como "aquellas instalaciones, sistemas, sitios y redes necesarias para el funcionamiento del país y la prestación de los servicios esenciales en los que la vida diaria en el Reino Unido depende". El CPNI categoriza la infraestructura nacional en nueve sectores, incluyendo comunicaciones y energía. La infraestructura se clasifica de acuerdo a su valor o "criticidad" y el impacto de su pérdida. Esta clasificación se realiza mediante una "Escala de criticidad", que asigna categorías para los diferentes grados de severidad de impacto. Dentro de la infraestructura existen activos "críticos" los cuales constituyen la infraestructura nacional crítica de la nación. Estos pueden ser físicos (por ejemplo, sitios, instalaciones, piezas de equipo) o lógicos (por ejemplo, las redes y los sistemas de información). El CNPI da soporte a las compañías eléctricas en comparar sus prácticas de ciberseguridad contra las mejores prácticas, en particular en sistemas SCADA.

Por otro lado, el Departamento de Energía y Cambio Climático (DECC) ha establecido la ciberseguridad como una parte importante del programa de implementación de mediciones inteligentes en la red eléctrica mediante el seguimiento de la metodología denominada "Marco de Seguridad Pública", la cual es publicada por el *Cabinet Office*. Dicha metodología incluye una revisión anual de los riesgos de tipo técnico mediante el uso del estándar denominado IS1 (HMG IA Standard No 1), que es un estándar que se alinea bien con estándares internacionales, en particular ISO 27000 (Tristschler & Mackay, 2011).

El tema de ciberseguridad también ha sido considerado en el Mapa de Ruta de Redes Inteligentes definido por el Grupo de Estrategias de Redes Eléctricas (ENSG) (ENSG, 2010).

Además, en Reino Unido se ha constituido el *Smart Grids Forum* con el apoyo de DECC y OfGem[11]. El foro se centra en los temas de desarrollo de la red como una parte clave de la transición a una economía basada en baja emisión de carbono. El Foro tiene entre sus funciones considerar cuestiones estratégicas y los retos futuros de la red (con un enfoque particular después de 2020), incluidas las cuestiones de innovación de redes, estrategias de equilibrio del sistema y despliegue de tecnologías de RI.

De manera específica frente al tema de Ciberseguridad en las Redes Inteligentes en el Reino Unido, la Asociación de Redes de Energía (ENA) comisionó un estudio en el año 2011 (Tristschler & Mackay, 2011) el cual estableció una serie de recomendaciones a nivel nacional, incluyendo:

1) Incorporar consideraciones de seguridad cibernética de redes inteligentes como parte del trabajo del *Smart Grids Forum*, a partir de un reconocimiento explícito de la relación entre la seguridad cibernética de la RI y la seguridad del suministro;

2) Identificar los límites y las interfaces organizacionales y las interfaces entre la Red Nacional y las organizaciones de redes de distribución con respecto a sus roles en las responsabilidades de seguridad cibernética y la colaboración eficaz;

3) Llevar a cabo la evaluación de riesgos de seguridad cibernética en la Red Inteligente:

[10] Ver: http://www.cpni.gov.uk/

[11] Ver: http://uksmartgrid.org/

a) Acordar el uso del estándar IS1 para desarrollar una evaluación del riesgo a nivel nacional sobre las RI;

4) Utilizar los resultados de la evaluación de riesgos para informar/desarrollar actividades específicas a nivel nacional y con los Operadores de la Red de Distribución;

5) Revisar y actualizar las guías y herramientas del CPNI con un enfoque particular sobre los requerimientos de seguridad cibernética de las Redes Inteligentes.

El estudio en mención también identificó el estándar ISO/IEC 27001/27002 como un fuerte candidato a ser complementado con las guías del CPNI para servir como un punto de arranque para el desarrollo de un Sistema de Gestión de Ciberseguridad apropiado para el Reino Unido.

Por otra parte el estudio comisionado por ENA (Tristschler & Mackay, 2011) también indica que los sistemas de vigilancia y control de red necesarios para las redes inteligentes estarán basados en el uso de las TIC para permitir la automatización en un grado significativo. Por lo tanto, el buen funcionamiento de la red inteligente será altamente dependiente de que estos sistemas sean lo suficientemente fiables de tal manera que no tengan un impacto negativo en la seguridad del suministro.

En ese contexto, la fiabilidad de un sistema informático se define como la capacidad de ofrecer un servicio en el que se puede confiar de manera justificada. La fiabilidad debe integrar atributos tales como: disponibilidad, confiabilidad, seguridad, confidencialidad, integridad y mantenibilidad (Tristschler & Mackay, 2011).

Por último en el Reino Unido, la empresa *National Grid* que operan sistemas de transmisión eléctrica en Inglaterra y Gales cuenta con un equipo dedicado de consultoría en riesgos y seguridad, que tiene la responsabilidad de proporcionar experiencia en seguridad en términos de estrategia, arquitectura, protección de datos y asuntos regulatorios. Este equipo utiliza para su trabajo las Normas ISO 27001/27002 como marco de orientación de seguridad cibernética; al igual que la Norma NISTIR 7628 (Tristschler & Mackay, 2011).

3.6 Unión Europea

El Consejo de la Unión Europea expidió una Directiva que puede tener relevancia en la ciberseguridad de las Redes Inteligentes: la Directiva 2008/114/CE13 (Consejo de la Unión Europea, 2008) obliga a los Estados miembros a identificar posibles infraestructuras críticas europeas (ECI), que se definen como activos o sistemas esenciales para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, económicas o sociales del bienestar de las personas, ubicada en los estados miembros, donde la interrupción o destrucción de estos activos o sistemas tendrían un impacto significativo en al menos dos Estados miembros.

Por otra parte, la Directiva obliga a los estados miembros a informar a otros Estados miembros potencialmente afectados acerca de la existencia de las ECI, informar a los propietarios/operadores de la ECI sobre su designación como tales, y desarrollar planes de seguridad para los operadores y nombrar a funcionarios de enlace de seguridad para cada ECI.

Como marco general a nivel de la Unión Europea, ENISA ha establecido una serie de recomendaciones en relación con Estrategias Nacionales de Ciberseguridad (ENISA, 2012).

Algunas de las recomendaciones más relevantes a los países Europeos sobre seguridad en las Redes Inteligentes (RI) también han sido proporcionadas por ENISA y están compiladas en el documento "*Smart Grid Security*" (ENISA (European Network and Information Security Agency), 2012) publicado en el 2012. Como punto de partida, la Agencia Europea luego de evaluar el panorama actual y las pruebas piloto de las Redes Inteligentes, expone los retos más importantes al momento de desarrollar la seguridad en las RI, los cuales se resumen a continuación.

1. Factores que se consideran claves para garantizar el éxito de una Red Inteligente:
    i. Una definición unificada del concepto "Red Inteligente".
    ii. Prevención del fraude y reducción de costos.
    iii. Ciberseguridad de la RI.
    iv. Garantías en la privacidad de los usuarios.
    v. Aceptación por parte del usuario a través de programas educativos, informativos y de concientización.
    vi. Aceptación y despliegue de la medición "inteligente".
2. Falta de un estándar de arquitectura para las RI, ya que los organismos de estandarización reconocen que no existe un estándar que describa claramente la arquitectura de las futuras RI en los componentes de generación, distribución y demás partes que la componen.
3. Abordar una seguridad de extremo a extremo en todos los niveles de comunicación basado en una arquitectura estándar, ya que las compañías involucradas a lo largo de la cadena de valor de la RI están cada vez más interconectadas e interdependientes.
4. Algunos expertos consideran que no se está prestando suficiente atención a la ciberseguridad y privacidad de datos en Europa, para priorizar esto, varios expertos señalaron que antes de enfrentar este reto, se debe primero direccionar correctamente los conceptos básicos de la RI, tales como el modelo de negocio, objetivos, funcionalidades, servicios, etc.
5. La aceptación del consumidor es un factor clave, por esta razón la privacidad se ha considerado más importante que la ciberseguridad y se tratan como dos temas separados, sin embargo varios expertos consideran que estos dos aspectos están íntimamente relacionados.
6. La ciberseguridad y la privacidad deben estar manejadas como parte integral de la fase de diseño.
7. La incorporación de las Redes Inteligentes trae consigo nuevos riesgos cibernéticos debido al uso de internet, redes públicas y nuevas funcionalidades para el usuario final.

Una vez se tienen claros los retos que conlleva el correcto desarrollo de una RI, ENISA propone 10 recomendaciones para los sectores público y privado involucrados en la definición e implementación de las Redes Inteligentes. Esto busca proveer consejos útiles y prácticos que apuntan a mejorar las iniciativas actuales, desarrollar nuevas medidas y buenas prácticas. Para más detalles refiérase al documento "Smart Grid Security" (ENISA (European Network and Information Security Agency), 2012).

- Recomendación 1: Mejorar el marco político y regulatorio, los cuales deben por lo menos apuntar hacia:
    i. Considerar a la privacidad y la ciberseguridad como dos temas intrínsecamente interdependientes.
    ii. Definir medidas de seguridad para ser tenidas en cuenta en los despliegues actuales de Redes Inteligentes (por ejemplo en los contadores inteligentes instalados).
    iii. Exigir a los operadores de red evaluaciones de riesgo obligatorias.
    iv. Exigir a los fabricantes, integradores, proveedores de servicio y operadores de red, el complimiento de certificaciones de seguridad específicas.
    v. Establecer presiones regulatorias (multas) a las empresas por el no cumplimiento.
    vi. Hacer públicos los resultados de cumplimiento.
    vii. Exigir a los operadores reportar a las entidades nacionales o supranacionales sobre los incidentes relacionados con la ciberseguridad.

- Recomendación 2: Promover la creación de una entidad de asociación público-privada para coordinar las iniciativas de ciberseguridad de las RI.
- Recomendación 3: Promover las iniciativas de entrenamiento e incrementar la concientización sobre el tema.
- Recomendación 4: Promover iniciativas de difusión e intercambio de conocimiento.
- Recomendación 5: Desarrollar un conjunto mínimo de estándares y lineamientos de referencia.
- Recomendación 6: Promover el desarrollo de los esquemas de certificación de seguridad para productos y seguridad organizacional.
- Recomendación 7: Promover la creación de bancos de prueba y evaluaciones de seguridad.
- Recomendación 8: Refinar estrategias para coordinar a gran escala los incidentes cibernéticos que afectan los RI.
- Recomendación 9: Involucrar a los Equipos Centrales de Respuesta de Emergencia (CERTS) para que hagan parte activa y realicen asesoramiento al tratar con problemas de seguridad cibernética que afecten las RI.
- Recomendación 10: Promover la investigación en ciberseguridad de RI aprovechando los programas de investigación existentes.

Posteriormente, en el 2014, ENISA publicó un documento sobre certificación de seguridad de las Redes Inteligentes en Europa (ENISA, 2014), el cual describe la necesidad de establecer prácticas armonizadas a nivel Europeo para la certificación de redes inteligentes. Dichas prácticas deben cubrir la cadena de suministro completa de la red eléctrica inteligente y ser compatibles con una plataforma europea basada en la Arquitectura SGAM, en particular en el documento SG-GC/M490_H Seguridad de la Información en Redes Inteligentes (CEN-CENELEC-ETSI, 2014).

En dicho documento, la seguridad de la información de redes inteligentes se refiere a las necesidades técnicas y organizacionales para mantener una SGIS y DPP sostenibles y conformes al "estado del arte", permitiendo la recolección, utilización, procesamiento, almacenamiento, transmisión y borrado de toda la información de los actores participantes a ser protegida. En este sentido el documento SG-GC/M490_H (CEN-CENELEC-ETSI, 2014) provee guía y estándares a los interesados en el tema. Esto incluye la definición de un conjunto de niveles de seguridad de los activos del sistema y establece un conjunto de estándares que soportan la operación confiable de una red inteligente. Dichos estándares se presentan en la Tabla 6.

Tabla 6. Estándares de seguridad seleccionados en Europa

Estándar	Descripción
ISO/IEC 15408	Information technology — Security techniques — Evaluation Criteria for IT Security.
ISO/IEC 18045	Information technology — Security techniques — Methodology for IT Security evaluation.
ISO/IEC 19790	Information technology — Security techniques — Security requirements for cryptographic modules.

ISO/IEC TR 27019	Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.
IEC 62443-2-4	Security for industrial automation and control systems - Network and system security - Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers.
IEC 62443-3-3	Security for industrial automation and control systems, Part 3-3: System security requirements and security levels.
IEC 62443-4-2	Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components.
IEC 62443-2-1	*Security for industrial automation and control systems - Network and system security - Part 2-1: Industrial automation and control system security management system.*
IEEE 1686	Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities.
IEEE C37.240	Cyber Security Requirements for Substation Automation, Protection and Control Systems.
ISO /IEC 15118-2	Road vehicles – Vehicle-to-Grid Communication Interface, Part 2 [22]: Technical protocol description and Open Systems Interconnections (OSI) layer requirements.
IEC 62351-x	Power systems management and associated information exchange – Data and 384 communication security.
IEC 62056-5-3	DLMS/COSEM Security.
IETF RFC 6960	Online Certificate Status Protocol.
IETF RFC 7252	CoAP Constrained Application Protocol.
IETF draft-weis-gdoi-iec62351-9: IEC 62351	Security Protocol support for the Group Domain of Interpretation (GDOI).
IETF RFC 7030	Enrollment over Secure Transport.

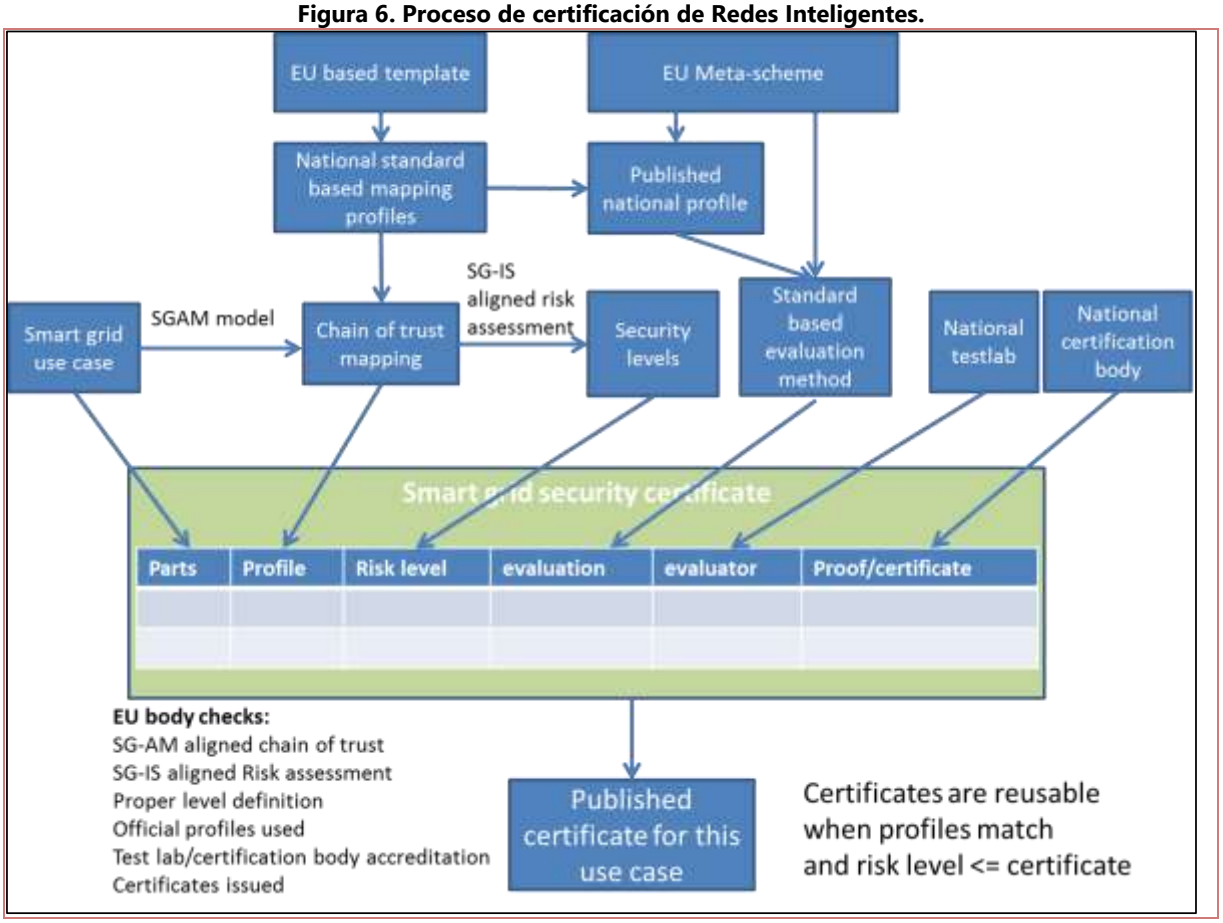
Fuente: CEN -CENELEC-ETSI (CEN-CENELEC-ETSI, 2014)

La aplicación de estos estándares sobre el modelo CEN-CENELEC-ETSI permite establecer un mapeo entre cada estándar con las capas, dominios y zonas del modelo SGAM de CEN-CENELEC-ETSI.

Finalmente, el proceso recomendado por ENISA a los países de la Unión Europea para establecer prácticas armonizadas para la certificación de redes inteligentes (ENISA, 2014), se resumen en la Figura 6

.

Figura 6. Proceso de certificación de Redes Inteligentes.



Fuente: ENISA (ENISA, 2014)

A nivel nacional los países de la Comunidad Europea no han adoptado medidas de ciberseguridad específicas para RI pero varios de ellos sí han establecido estrategias nacionales de ciberseguridad. Por ejemplo en España en el 2013 el Consejo de Ministros aprobó la nueva Estrategia de Ciberseguridad Nacional (Presidencia del Gobierno de España - Departamento de Seguridad Nacional, 2013), la cual se articula en torno a cinco capítulos en los que describe el ciberespacio y su seguridad, detalla el propósito y los principios rectores de la ciberseguridad en España, expone los objetivos de la ciberseguridad, las líneas de actuación, y cómo se articula la ciberseguridad dentro del Sistema de Seguridad Nacional.

En dicho contexto el Consejo de Seguridad Nacional ha impulsado la elaboración de la Estrategia de Ciberseguridad Nacional con el fin de dar respuesta al enorme desafío que supone preservar al ciberespacio de los riesgos y amenazas que se ciernen sobre él. Respecto a la protección de las infraestructuras críticas, en el Ministerio del Interior se creó el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), que entre otros cometidos se encarga de la ciberseguridad en estas infraestructuras. El CNPIC se incluye dentro de la Estrategia Española de Seguridad que aprobó el Consejo de Ministros el 31 de mayo de 2013.

3.7 Resumen de la comparación internacional sobre ciberseguridad en RI

Los aspectos más sobresalientes sobre el tema de ciberseguridad descrito se presentan en la Tabla 7.

Tabla 7. Resumen de las principales características sobre ciberseguridad que presentan las Organizaciones de Estado.

Administración	Acuerdos, Regulación o Estándares	Observaciones principales
OEA	**Acuerdos:** 2015: "Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes" 2012: "Fortalecimiento de la Seguridad Cibernética de las Américas" - OEA/Ser.L/X.2.12. 2004: "Estrategia Interamericana Integral de Seguridad Cibernética" - AG/RES. 2004 (XXXIV-O/04).	El 37% de las organizaciones encuestadas por la OEA han adoptado estándares de seguridad industrial como el BERC CIP e ISO 2700x. Se espera que los acuerdos declarados por la OEA sea de cumplimiento obligatorio para los países que decidan adoptar las estrategias recomendadas.
EE.UU.	**Estándar:** 2014: "Framework for Improving Critical Infrastructure Cybersecurity". NIST.	El marco de ciberseguridad del NIST, incorpora normas de consenso voluntario y mejores prácticas en la industria, fue elaborado por Orden Ejecutiva para ser usado como guía en las organizaciones individuales con el propósito de mejorar la ciberseguridad de la infraestructura crítica en la nación. El Secretariado de Seguridad Nacional, en coordinación con las Agencias específicas del sector, deberá establecer un programa voluntario para apoyar la adopción de este Marco de Ciberseguridad.
	Lineamientos de Seguridad: 2014: NISTIR 7628 Revision 1 – "Guidelines for Smart Grid Cybersecurity" 2012: "Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline"	El objetivo del NISTIR 7628 es suministrar a las organizaciones un marco analítico que les sirva para desarrollar estrategias efectivas de ciberseguridad adaptadas a sus variantes particulares y relacionadas con las características de redes inteligentes, riesgos y vulnerabilidades
	Proyectos de Ley: H.R. 1731: National Cybersecurity Protection Advancement Act of 2015. H.R. 85: Terrorism Prevention and Critical	Estos proyectos de ley fueron presentados por el Departamento de Seguridad Nacional en el primer semestre del 2015. A la fecha presente, están en las primeras etapas de aprobación y aún no han sido evaluados por

	Infrastructure Protection Act of 2015.	el Senado.
Brasil	**Lineamientos de RI y Ciberseguridad:** Arquitectura de Referencia de Redes Eléctricas Inteligentes de Brasil "REI-BR-2030". 2015: "Estratégia de Segurança da Informação e Comunicações e De Segurança Cibernética da Administração Pública Federal 2015 - 2018" - Departamento de Segurança da Informação e Comunicações 2010: "Guia de Referência para a Segurança das Infraestruturas Críticas da Informação". -Departamento de Segurança da Informação e Comunicações.	No se han identificado recomendaciones específicas de ciberseguridad para Redes Inteligentes. El tema de ciberseguridad es un elemento transversal a la arquitectura RI pero el tema se encuentra en desarrollo, con avances realizados por la Agencia Brasilera de Desarrollo Industrial.
Chile	**Acuerdos:** Por Decreto 533 de 2015 se creó el Comité Interministerial sobre Ciberseguridad. Avances para la posible adehsión de Chile a la Convención de Ciber Delitos del Consejo de Europa – Convención de Budapest.	Chile se encuentra en proceso de creación de una Política Nacional de Ciberseguridad y no se identifican recomendaciones específicas en relación con RI.
Reino Unido	**Lineamientos:** 2010: "The UK Cyber Security Strategy Protecting and promoting the UK in a digital world". **Estándar:** IS1 (HMG IA Standard No 1), congruente con estándar internacional ISO 27000.	El Centro de Protección de la Infraestrucutra Nacional (CPNI), del Reino Unido, da soporte a las compañías eléctricas en comparar sus prácticas de ciberseguridad contra las mejores prácticas, especialmente en sistemas SCADA. La Asociación de Redes de Energía (ENA), recomienda el uso del estándar IS1 para desarrollar una evaluación del riesgo a nivel nacional sobre las Redes Inteligentes.
Unión Europea	**Estándar:** SG-GC/M490_H Seguridad de la Información en Redes Inteligentes. CEN-CENELEC-ETSI. **Directrices:** 2008: Directiva 2008/114/CE13. Consejo de la Unión Europea. **Recomendaciones:**	Reconocen la necesidad de establecer prácticas armonizadas a nivel Europeo para la certificación de redes inteligentes. Debe basarse en la arquitectura SGAM (SG-GC/M490_H). El Consejo de la Unión Europea ordenó a los Estados miembros a identificar posibles infraestructuras críticas europea (ECI), informar a los otros Estados miembros acerca de la existencia de las ECI y desarrollar planes de seguridad para los operadores.

	2012: "*Smart Grid Security*", *ENISA*. 2012: "National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace" – ENISA. 2014: Smart grid security certification in Europe, Challenges and recommendations – ENISA.	Los organismos de estandarización reconocen que no existe un estándar que describa claramente la arquitectura de las futuras RI en los componentes de generación, distribución y demás partes que la componen. ENISA declara la necesidad de establecer prácticas armonizadas a nivel Europeo para la certificación de redes inteligentes. Deben ser compatibles con arquitectura SGAM, descrita en el documento SG-GC/M490_H. A nivel nacional los países de la Comunidad Europea no han adoptado medidas de ciberseguridad específicas para RI pero varios de ellos sí han establecido estrategias nacionales de ciberseguridad

4. Aspectos Claves de TIC relacionados con Redes Inteligentes: Comparación internacional - Interoperabilidad

La interoperabilidad es otro de los temas que se ha considerado crítico desde la perspectiva de las TIC en la implementación de RI.

A continuación se presenta una comparación internacional de los casos más interesantes para el análisis de Colombia, que corresponden a (i) Brasil y (ii) la Unión Europea. Brasil es un referente importante desde el punto de vista Latinoamericano y ha desarrollado varios esfuerzos de estandarización de carácter nacional con aplicación directa sobre RI. La Unión Europea por su parte se encuentra desarrollando el modelo CEN-CENELEC-ETSI *Smart Grid Architecture Module* (SGAM) del *Smart Grid Coordination Group,* que ha sido recomendado como marco de referencia para Colombia por los Consultores de la Componente I (Llombart Estopiñán , et al., "Estudio de factibilidad técnica y económica de soluciones de redes inteligentes para el sector eléctrico colombiano" - Informe 2, 2015). Adicionalmente, se presenta el caso de (iii) Chile, que si bien no ha realizado esfuerzos de estandarización específicos para la implementación de RI, sí permite exponer un punto importante desde la regulación de las TIC y es que los criterios regulados de interconexión se aplican exclusivamente sobre redes públicas de telecomunicaciones.

4.1 Brasil

En el 2014 la ABDI publicó una versión preliminar del mapeo de la cadena de Proveedores TIC y sub productos y servicios de Red Inteligente (ABDI, 2014), en la cual indicó que el término **interoperabilidad** puede ser definido como la capacidad de dos o más sistemas para comunicarse de forma transparente, logrando plenamente sus propósitos. Por lo tanto, la ABDI consideró esencial que los fabricantes y distribuidores de electricidad adopten las mismas reglas o Normas o simplemente adopten un estándar abierto, asegurando de esta forma menores inversiones en los despliegues y costos de operación más bajos durante la vida de servicio de las aplicaciones.

En dicho contexto, la ABDI ha considerado importante adoptar un conjunto de interfaces entre elementos basados en una "arquitectura unificadora" y en protocolos definidos en estándares o normas de consenso. Por lo tanto, de acuerdo con la ABDI, se debe establecer una arquitectura de referencia para el intercambio de información entre dispositivos y sistemas eléctricos para describir todos los modelos de objetos, servicios, protocolos e interfaces y su relación con los demás. A este "marco" se le da el nombre en Brasil de "hoja de ruta".

En el 2014 la ABDI en su versión preliminar del mapeo de la cadena de Proveedores TIC y sub productos y servicios de Red Inteligente (ABDI, 2014), identificó las principales organizaciones internacionales de estandarización y entidades relacionadas con el desarrollo de redes inteligentes para el sector eléctrico. Las entidades identificadas a nivel internacional incluyeron la Comisión Electrotécnica Internacional (IEC), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), el Instituto Nacional de Estándares y Tecnología (NIST), la Unión Internacional de Telecomunicaciones (UIT) y la Fuerza de Tarea de Ingeniería de Internet (IETF). A nivel nacional la ABDI identificó a la Asociación Brasilera de Normas Técnicas (ABNT), la Agencia Nacional de Energía Eléctrica (ANEEL) y el Instituto Nacional de Metrología, Calidad y Tecnología (INMETRO).

La ABDI también estableció las Normas y Estándares más utilizados a nivel mundial en Redes Inteligentes y su grado de utilización en Brasil por tipo de áreas de aplicación tecnológica (ABDI, 2014).

La Tabla 8 presenta la adopción de estándares en Brasil relacionados con medición inteligente. Puede apreciarse que se adoptan Normas Internacionales y también existe una serie de Normas Nacionales: ABNT 14522, ANEEL REN No 502 y ANEEL REN No 610.

Tabla 8. Estándares utilizados en Brasil para medición inteligente

Área de Aplicação Tecnológica	Nome do Padrão	Elaborado Por	Ano de Publicação mais Recente	Usado no Brasil?	Citado em Roadmap? Qual?	Padrão "core"?
INTERNACIONAL						
Medição Inteligente (MI)	ANSI C12.19	ANSI	2009	sim		
	ANSI C12.19	ANSI	2009	sim		
	IEC 62056	IEC	2014	sim	IEC	sim
	NEMA SG-AMI-1	NEMA	2009	não		
	ASAP-SG	EPRI	2011	não		
	EURIDIS	EURIDIS	2006	não		
	ABNT 14522	ABNT	2008	sim		
	REN Nº 502	ANEEL	2012	sim		
	REN Nº 610	ANEEL	2014	sim		

Fuente: ABDI (ABDI, 2014)

Por tanto, desde una perspectiva nacional y en relación con medición inteligente, Brasil ha establecido una Norma Técnica para el intercambio de información para sistemas de medición de energía eléctrica mediante la ABNT 14522 (ABNT, 2008) y dos Resoluciones Normativas que reglamentan los sistemas de medición de energía eléctrica de baja tensión (Resolución ANEEL No 502 (ANEEL, 2012)) y las modalidades de prepago y pospago electrónico de energía eléctrica (Resolución ANEEL No 610 (ANEEL, 2014)).

Desde el año 2010 Brasil ha venido trabajando en una propuesta de protocolo abierto para sistemas de medición, denominada Sistema Brasileño de Multimedición Avanzada (SIBMA) cuyo objetivo es permitir la integración de los contadores inteligentes para la medición remota con la central de distribución de energía. Los esfuerzos de estandarización Brasileños han permitido la definición de Normas técnicas para la especificación de medidores electrónicos de energía eléctrica (Norma ABNT NBR 14519 (ABNT, 2011) y los procedimientos de acreditación de los medidores (Norma ABNT NBR 14521 (ABNT, 2011)).

Adicionalmente, el Instituto Nacional de Metrología (INMETRO) ha establecido ordenanzas que establecen los requisitos metrológicos de los medidores electrónicos (INMETRO, 2013) y del software de captura (INMETRO, 2012).

En cuanto a los estándares utilizados en Brasil en relación con RI para tecnologías de información (ver Tabla 9) y telecomunicaciones (ver Tabla 10) en general se adoptan Normas internacionales. Sin embargo, a nivel de Telecomunicaciones se encuentra además una Resolución Normativa de carácter nacional que regula el uso de las instalaciones de distribución de energía eléctrica como medio de transporte para comunicaciones analógicas o digitales (Resolución ANEEL No 375 (ANEEL, 2009)).

Tabla 9. Estándares de tecnologías de información utilizados en Brasil en relación a Redes Inteligentes

Área de Aplicação Tecnológica	Nome do Padrão	Elaborado Por	Ano de Publicação mais Recente	Usado no Brasil?	Citado em Roadmap? Qual?	Padrão "core"?
INTERNACIONAL						
Tecnologia da Informação (TI)	IEC 61968	IEC	2006	Sim (ELETROPAULO, CEMIG, LIGHT)	IEC, NIST	sim
	IEC 61970	IEC	2006	sim	IEC, NIST	sim
	MULTISPEAK	MULTISPEAK	2013	sim		
	SCL	IEC	2004	sim		
	WSDL	W3C	2007	sim		
	IPV4 (RFC 791)	IETF	1981	sim		
	IPV6	IETF	1998	sim		
	IEC 62325	IEC	2005	sim		

Fuente: ABDI (ABDI, 2014)

Tabla 10. Estándares de telecomunicaciones utilizados en Brasil en relación a Redes Inteligentes

Área de Aplicação Tecnológica	Nome do Padrão	Elaborado Por	Ano de Publicação mais Recente	Usado no Brasil?	Citado em Roadmap? Qual?	Padrão "core"?
INTERNACIONAL						
Telecomunicações (TELECOM)	IEC 62488	IEC	2012	não		
	IEEE 1888	IEEE	2014	não		
	IEEE 802.16	IEEE	2013	sim		
	3GPP	3GPP	2009	sim		
	SDH (G.707, G.783, G.784, G.803)	ITU-T	2006	sim		

	IMT-ADVANCED	ITU-R	2008	sim		
	IEC 61400-25	IEC	2006	não		
	IEEE 1701	IEEE	2012	não		
	IEEE 1703	IEEE	2012	não		
	IEEE 1901	IEEE	2010	não		
	IEEE 802.11	IEEE	2013	sim		
	IEEE 802.15.4g	IEEE	2012	sim		
	IEEE 802.15.5	IEEE	2005	sim		
	IEEE 1588	IEEE	2008	sim		
	IEEE 1615	IEEE	2007	sim		
	IEEE 1777	IEEE	2007	sim		
	6lowPAN	IETF	2009	sim		
	PRIME	PRIME ALLIANCE	2006	sim		
	REN 375	ANEEL	2010	sim		
	IEC 61334	IEC	2001	sim		
	OPENADR	OPENADR	2009	não		
	ZIGBEE	ZIGBEE ALLIANCE	2012	sim		
	TIA-4957.000	TIA / ANSI	2013	não		
	LONWORKS	ECHELON	2005	não		
	HOMEPLUG	HOMEPLUG ALLIANCE	2010	sim		
	SEP 2.0	ZIGBEE ALLIANCE	2010	sim		

Fuente: ABDI (ABDI, 2014)

4.2 Chile

En la Estrategia Nacional de Energía 2012-2030 del Ministerio de Energía de Chile (Ministerio de Energía) se menciona que se analizará la viabilidad técnica y económica de las Redes Inteligentes, tomando en cuenta los desarrollos, las implementaciones y experiencia local e internacional en proyectos pilotos, y sobre todo tratando de valorizar las ventajas de implementar este desarrollo tecnológico en el mercado chileno, para contribuir, entre otras cosas, a la introducción de la generación distribuida.

Sin embargo el desarrollo de Redes Inteligentes en Chile es incipiente a nivel de políticas, regulación e implementación. No existen, por ejemplo, definiciones de arquitectura de Redes Inteligentes a nivel Nacional, ni se han adoptado mecanismos de estandarización o normas técnicas específicas que favorezcan la interoperabilidad.

De hecho, en el caso de Chile no se encontró una definición para "interoperabilidad" que pueda aplicarse al caso de Redes Inteligentes. Tampoco se hace mención a dicho concepto en la Ley General de Telecomunicaciones (MINISTERIO DE TRANSPORTES Y TELECOMUNICACIONES, 1982). En cuanto al término "interconexión", este sí es utilizado, pero como obligación legal con sus reglas asociadas la interconexión existe únicamente entre Concesionarios de servicios públicos de Telecomunicaciones.

En el tema de medidores, existen Normas Técnicas expedidas en 1925 por el entonces Ministerio de Economía, Fomento y Reconstrucción (Ministerio de Economía, Fomento y Reconstrucción, 1925) y todavía vigentes, las cuales indican que los instrumentos de medida deberán ser calibrados individualmente en los Laboratorios de la Dirección de Servicios Eléctricos (que corresponde hoy en día a la Superintendencia de Electricidad y Combustibles).

En el tema de medidores, se han dado algunos planes piloto como Smart City Santiago[12], el cual ha realizado la instalación de medidores inteligentes por parte de Chilectra mediante el uso del modelo CERM1 de tecnología ENEL[13]. Este tipo de medidores eléctricos cuentan con certificación expedida por la Superintendencia de Electricidad y Combustibles en Chile.

Por otra parte, existe en Chile un Instituto Nacional de Normalización cuya función es fomentar la elaboración y uso de normas chilenas, coordinando la Red Nacional de Metrología y acreditando organismos de evaluación de la conformidad. Sin embargo, no se identificaron Normas técnicas nacionales que promocionen el uso de protocolos abiertos para sistemas de medición.

4.3 Unión Europea

El Reglamento (UE) No 1025/2012 del Parlamento Europeo y del Consejo (Parlamento Europeo y Consejo Europe, 2012) estableció los lineamientos para la normalización en Europa. Dicho reglamento indica en sus considerandos que: "(...) el principal objetivo de la normalización es la definición de especificaciones técnicas o cualitativas voluntarias con las que pueden ser conformes actuales o futuros productos, procesos de producción o servicios. La normalización puede abarcar distintos ámbitos, como la normalización de diferentes calidades o tamaños de un producto determinado o las especificaciones técnicas en mercados de productos o servicios en los que resulta esencial la compatibilidad y la interoperabilidad con otros productos o sistemas."

El reglamento también indica en sus considerandos que: "(...) la normalización europea se organiza por y para las partes interesadas sobre la base de la representación nacional [el Comité Europeo de Normalización (CEN) y el Comité Europeo de Normalización electrotécnica (CENELEC)] y la participación directa [Instituto Europeo de Normas de Comunicación (ETSI)] (...)" y que: "Las normas europeas son adoptadas por las organizaciones europeas de normalización, a saber, el CEN, el Cenelec y el ETSI."

El mismo reglamento en sus disposiciones generales establece que una «norma armonizada» es una norma europea adoptada a raíz de una petición de la Comisión para la aplicación de la legislación de armonización de la Unión.

En 2011 la Comisión Europea expidió el mandato[14] de estandarización denominado M/490 *Smart Grid Mandate* (European Commission, 2011) por medio del cual solicitó a las Organizaciones de Estandarización Europeas (ESO) el desarrollo o actualización de un conjunto de normas coherentes dentro de un marco europeo común que integren una variedad de tecnologías de computación de comunicación digitales y arquitecturas eléctricas con los procesos y servicio asociados, que permitan lograr la interoperabilidad y habiliten o faciliten la aplicación en Europa de los diferentes servicios y funcionalidades de las RI según la definición del *Smart Grid Task Force*, que sean lo suficientemente flexibles para dar cabida a la evolución futura. Los aspectos de Construcción, Industria, Electrodomésticos y domótica fueron considerados por fuera del alcance del mandato; sin embargo, sus interfaces con la red inteligente y sus servicios relacionados sí se definieron bajo el alcance del mandato.

El mandato M/490 también indica que una red de energía segura y robusta resulta esencial para la mejora continua de los mercados energéticos europeos, pero esto sólo será posible si las redes TIC asociadas son

[12] http://www.smartcitysantiago.cl/medicion-inteligente

[13] Este tipo de medidores también se encuentran implementados de manera masiva en Italia y España

[14] De acuerdo con el Comité Europeo para la Estandarización (CEN), los mandatos son el mecanismo por el que la Comisión Europea (CE) y la secretaría de la Asociación Europea de Libre Comercio (EFTA) solicitan a los organismos europeos de normalización (ESO) el desarrollo y adopción de Normas europeas en apoyo de las políticas y la legislación europea.
Ver: https://www.cen.eu/work/supportLegislation/Mandates/Pages/default.aspx Consulta realizada el 12 de septiembre de 2015.

seguras y robustas. También dice que son temas esenciales: mantener la seguridad de los datos y del sistema así como respetar los derechos y las libertades de los consumidores finales.

El mandato M/490 incluye además las siguientes consideraciones, que son de resaltar:

1. El alcance de las redes inteligentes es grande; por tanto, el riesgo es que demasiados organismos de normalización trabajen en este tema, proporcionando conjuntos inconsistentes de especificaciones técnicas, causando la no interoperabilidad de equipos y aplicaciones y que las prioridades no sean definidas con precisión.
2. El reto de la implementación de redes inteligentes requerirá cambios en los estándares existentes, las Normas y procesos de la industria.
3. Las RI requieren por tanto de un marco que reúna las siguientes características:
    a. Los suficientemente comprensivo e integrado para incluir a toda la variedad de actores de las RI y garantizar las comunicaciones entre ellos.
    b. Con la profundidad suficiente para garantizar desde la interoperabilidad de las RI de conectividad básica hasta las aplicaciones empresariales distribuidas complejas, incluyendo un conjunto unificado de definiciones de modo que todos los Estados Miembros tengan una comprensión común de los diversos componentes de la red inteligente.
    c. Flexible y lo suficientemente rápido para tomar ventaja de la infraestructura y servicios de telecomunicaciones existente, así como la aparición de nuevas tecnologías, mientras que mejora la competitividad de los mercados
    d. Lo suficientemente flexible para dar cabida a algunas diferencias entre los enfoques de los Estados miembros de la UE para la implementación de las RI.

A partir de dicho mandato los ESO combinaron sus aproximaciones estratégicas y establecieron desde julio de 2011, junto con las partes interesadas relevantes el Grupo de Coordinación de RI del CEN CNELEC-ETSI (denominado SG-CG). Para 2014 el SG-CG había dado respuesta al mandato M/490 mediante la finalización de los reportes que se detallaron previamente en la Tabla 3. Estos reportes fueron aprobados por las Juntas Técnicas de CEN, CENELEC y ETSI en diciembre de 2014.

Los reportes constituyen el cuerpo de la Arquitectura SGAM que se discutió brevemente en la sección 2 de este documento.

4.6 Resumen de la comparación internacional sobre Interoperabilidad en RI

Los aspectos más sobresalientes sobre el tema de privacidad de los consumidores descrito a lo largo de la Sección 4, se presenta en la Tabla 11.

Tabla 11. Resumen de las principales características sobre interoperabilidad en Redes Inteligentes.

Administración	Acuerdos, Regulación o Estándares	Observaciones principales
Brasil	**Estándares:** 2014: "Mapeamento da Cadeia Fornecedora de TIC e de seus Produtos e Serviços para Redes Elétricas Inteligentes (REI). Normas Técnicas, Padrões e Regulamentos Aplicados à Cadeia de	La ABDI estableció las Normas y Estándares más utilizados a nivel mundial en Redes Inteligentes y su grado de utilización en Brasil por tipo de áreas de aplicación tecnológica. Brasil cuenta con algunas normas técnicas

	Produtos e Serviços de TIC para REI". **Normas nacionales:** • ABNT 14522. • ANEEL REN No 502. • ANEEL REN No 610. **Estándares internacionales usados en Brasil:** 2009: ANSI C12.19. 2014: IEC62056. 2006: IEC61968, IEC61970. **Ordenanzas:** 2013: Portaria no 401, de 15 de agosto de 2013. Estabelecer requisitos adicionais aos já fixados no Regulamento Técnico Metrológico de medidores eletrônicos de energia elétrica multitarifação. 2012: Portraia No. 586 - Establecer os requisitos técnicos de software; Garantir que o software proporcione medidas corretas e dentro dos erros admissíveis: Garantir que o software nao seja afetado por outros softwares. **Resolución Normativa:** 2009: RESOLUÇÃO NORMATIVA No 375, DE 25 DE AGOSTO DE 2009 Regulamenta a utilização das instalações de distribuição de energia elétrica como meio de transporte para a comunicação digital ou analógica de sinais.	propias, destacándose su propuesta de protocolo abierto para sistemas de medición, denominada Sistema Brasileño de Multimedición Avanzada (SIBMA), cuyo objetivo es permitir la integración de los contadores inteligentes para la medición remota con la central de distribución de energía. El Instituto Nacional de Metrología (INMETRO) ha establecido ordenanzas que establecen los requisitos metrológicos de los medidores electrónicos
Chile	**Normas Técnicas:** 1925: NSEG 3 E.n71. Normas Técnicas sobre Medidores. **Estándares:** Modelo CERM1 de tecnología ENEL.	El desarrollo de Redes Inteligentes en Chile es incipiente a nivel de políticas, regulación e implementación. No existen, por ejemplo, definiciones de arquitectura de Redes Inteligentes a nivel Nacional, ni se han adoptado mecanismos de estandarización o normas técnicas específicas que favorezcan la interoperabilidad. Cabe enfatizar que los criterios regulados de interconexión se aplican exclusivamente sobre redes públicas de telecomunicaciones. En el tema de medidores, se han dado

		algunos planes piloto como Smart City Santiago, el cual ha realizado la instalación de medidores inteligentes por parte de Chilectra mediante el uso del modelo certificado CERM1 de tecnología ENEL.
Unión Europea	**Reglamento:** 2012: REGLAMENTO (UE) No 1025/2012 DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión no 1673/20 **Mandato:** 2011: M/490 Smart Grid Mandate. Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment.	En el 2014 el Grupo de Coordinación de Redes Inteligentes del CEN CNELEC-ETSI (SG-CG), dio respuesta al mandato de estandarización denominado M/490 Smart Grid Mandate, mediante un conjunto de reportes que constituyen el cuerpo de la Arquitectura SGAM. Las normas europeas son adoptadas por las organizaciones europeas de normalización, a saber, el CEN, el Cenelec y el ETSI.

5. Aspectos Claves de TIC relacionados con Redes Inteligentes: Comparación internacional - Privacidad de los consumidores

La posibilidad de utilizar infraestructura de medición avanzada directamente en las casas de los usuarios ha generado preocupaciones sobre los derechos de los consumidores, especialmente en relación con su privacidad.

En esta sección se exponen en primer lugar las consideraciones sobre el tema de privacidad y derechos de los consumidores que han sido realizadas por la Agencia Internacional de Energía, en especial en relación a preocupaciones sobre temas de política y seguridad.

También se incluye en la comparación a los Estados Unidos, revisando en particular las medidas de protección de derechos de los usuarios establecidas por el estado de California, específicamente sobre dispositivos de medición avanzada.

De Europa se incluye la regulación específica existente a nivel de la Unión Europea así como los planes futuros y se analizan con más detalle los casos de Suecia y en especial de Holanda, donde se han tomado medidas de protección de los usuarios que les permiten a estos incluso rechazar la instalación de contadores remotos inteligentes.

5.1 Agencia Internacional de Energía

La Agencia Internacional de Energía (AIE), a través del Acuerdo de Implementación para un Programa Cooperativo en RI (ISGAN), publicó en abril del 2012 un reporte titulado "*Smart Grid Cyber Security*" (IEA (International Energy Agency), 2012), en donde se identifican asuntos claves en el diseño de políticas de ciberseguridad. Entre los temas presentados, se destacan una guía para el desarrollo de un marco de trabajo con el objeto de proteger la privacidad de los datos del usuario.

Indica la AIE que es importante enfrentar dos retos relevantes, que son, los problemas de rentabilidad económica en la inversión que esto implica y los cambios organizacionales requeridos para alcanzar una seguridad robusta. Además, al momento de formular las políticas, el objetivo debe apuntar hacia maximizar la evolución de los sistemas y simultáneamente reducir el riesgo de seguridad, es decir, se debe calcular un balance entre innovación y privacidad.

Los requerimientos para la protección de los datos de consumidor se implementan principalmente en la Infraestructura de Medición Avanzada (AMI) y deben enfocarse en cuatro propiedades que son: integridad[15] de los datos, autenticación[16], confidencialidad[17] y no-repudio[18].

En el reporte (IEA (International Energy Agency), 2012) se citan algunas preocupaciones en temas de políticas y seguridad planteadas por analistas del Reino Unido, por cuanto a la medición en las RI y que reflejan las complejas interacciones de las políticas en el ámbito de la privacidad de los consumidores. Algunos de estos aspectos son:

- La gran cantidad de datos incrementa los problemas de privacidad. Esto se vio reflejado en una decisión del alta Corte Holandesa cuando en 2009 anuló una ley que obligaría a todos los ciudadanos a instalar un "medidor inteligente" en sus casas, basándose en que esta es contraria a

[15] Integridad significa que los sistemas y la información están protegidos de modificación no autorizada.

[16] Autenticación significa que el acceso al sistema se encuentra restringido exclusivamente a individuos autorizados.

[17] Confidencialidad significa que la información es protegida de divulgación no autorizada.

[18] No-repudio significa que se evita la capacidad de los usuarios o sistemas para negar la responsabilidad de las acciones.

los principios de la Convención Europea de Derechos Humanos (este aspecto se amplía en la sección 0).

- La disponibilidad de datos sobre consumo detallado en servicios públicos plantea inquietudes en torno a la fijación de precios selectivos o predatorios y el potencial incremento del rechazo por parte de los usuarios.
- La existencia de interruptores que permiten la desconexión remota y que estén ampliamente distribuidos incrementa la vulnerabilidad a los apagones por sabotaje o ataques de grupos criminales.
- La posibilidad de desconexión remota también genera preocupaciones acerca de los cortes de energía como una acción coercitiva por parte del gobierno para cumplir con los ahorros de energía u otros objetivos políticos como por ejemplo castigar la disidencia.
- La selección de un protocolo específico tiene implicaciones en los costos y en la propiedad intelectual, ya que la obligatoriedad de ciertos protocolos de cifrado implicaría costos de regalías por cada dispositivo que lo utilice (por ejemplo la criptografía de curva elíptica).

5.2 Estados Unidos de América

Uno de los ejemplos de implementación de políticas para la protección a los derechos del usuario se vio reflejado en las acciones del Estado de California en los Estados Unidos, donde se tomó la decisión de adoptar reglas para proteger la privacidad y seguridad de los datos del consumo en los usuarios, que son generados por los "*Smart Meters*" de las compañías de energía eléctrica y de gas, bajo la "*Decision 11-07-056, July 28, 2011*" (PUC (Public Untilities Commission), 2011). En el documento se detallan las discusiones de las propuestas presentadas para tomar la decisión final y se concluye con la aprobación e implementación de la propuesta "*Senate Bill (SB) 1476*"[19] (California Government, 2010), así mismo se analiza la comparación y pertinencia de esta decisión con las políticas precedentes sobre privacidad y seguridad, como por ejemplo la compatibilidad con la Decision 10-06-047 donde se aprueban los Principios de Prácticas de Información Justa (FIPPs)[20].

Basados en estos principios, la Comisión de Servicios Públicos adoptó un conjunto de Reglas de Privacidad (en el "*Attachment D - Rules Regarding Privacy and Security Protections for Energy Usage Data*" de la misma Decisión (PUC (Public Untilities Commission), 2011)), que rige el tratamiento de la información del usuario generada por los medidores avanzados (*Advanced Meters*); las especificaciones reglamentarias se agrupan en los siguientes temas:

- Transparencia por parte de las Entidades hacía los usuarios, mediante notificación clara y completa sobre el acceso, recolección, almacenamiento, uso y divulgación de la los datos de consumo del usuario.
- Especificación del propósito de uso de la información recolectada, así como del tiempo aproximado de retención de la información. Se establece que esto se debe detallar en la notificación.

[19] El 29 de septiembre de 2010, la propuesta SB 1476 se convirtió en ley y capitulada por el Secretario de Estado. SB 1476 añadió secciones 8380 y 8381 del Código de Servicios Públicos, estas nuevas secciones abordan temas de privacidad derivados de la utilización de contadores inteligentes ("Section 8380 - Privacy protections for customer energy consumption data collected by California energy utilities using advanced metering infrastructure").

[20] Estos principios son la base de la Ley de Privacidad de 1974 "Privacy Act of 1974" (USA) y han sido ampliamente adoptadas como marco de referencia para las leyes de cada Estado, países extranjeros y organizaciones internacionales, que involucren la privacidad del individuo.

- Participación del usuario, que la Entidad debe proveerle al usuario como derecho para tener cierto acceso y control de su información de consumo. Se describen también las restricciones de divulgación.
- Minimización de la cantidad de datos, tanto la de los recolectados como los retenidos o divulgados.
- Restricciones de divulgación y uso de los datos, para los cuales se debe tener un propósito definido tanto para su recolección como para su uso o divulgación.
- La calidad e integridad de los datos recolectados, almacenados, utilizados o utilizados, debe ser asegurada por la Entidad.
- La protección de los datos, frente a destrucción, uso, modificación, divulgación o acceso no autorizado, debe asegurarse tomando medidas razonables de seguridad técnica, física y administrativa.
- Rendición de cuentas y auditoría de la Entidad a solicitud de la Comisión de Servicios Públicos.

Cabe resaltar la implementación de uno de estos temas a través de una iniciativa del Gobierno de los Estados Unidos llamada "Green Button", con la cual se fortalece el derecho a la participación del usuario. Consiste en una plataforma tecnológica que le provee al ciudadano acceso y control de sus datos de consumo eléctrico, de forma simple y segura en un formato estandarizado (U.S. Department of Energy, 2015), fue lanzada en el 2012 por un grupo conformado por el Departamento de Energía (DOE), la Presidencia de los Estados Unidos y el Instituto Nacional de Estándares y Tecnología (NIST). Posteriormente, en el 2015, se creó la Alianza "Green Button Alliance", con el fin de acelerar el desarrollo de aplicaciones, despliegue del estándar y certificaciones que promuevan la adopción de la iniciativa en la industria. Esta alianza utilizará estándares y tecnología existente proveniente de NAESB (North American Energy Standards Board) y UCAIug (UCA International Users Group), para enfocar los esfuerzos en desarrollar un ecosistema de industria compuesta por empresas eléctricas, organismos reguladores, responsables de las políticas, operadores de sistemas de control y automatización, entre otros.

5.3 Brasil

Los análisis iniciales de la Agencia Brasilera de Desarrollo Industrial (ABDI) (ABDI, 2012) identificaron entre los principales desafíos regulatorios de las *Smart Grids* los temas relacionados con la seguridad cibernética y la privacidad de los consumidores. En particular se indicó que la manipulación de la información de los hábitos de consumo de energía pueden exponer los comportamientos de los consumidores dado que una red inteligente hace posible identificar cada aparato eléctrico presente en una residencia. De acuerdo con ABDI esta posibilidad requiere por tanto de regulaciones específicas en relación con la seguridad y la integridad de la información transmitida a través de la red.

Sin embargo, no se identificó que Brasil a la fecha de entrega de este reporte haya tomado medidas específicas sobre este punto.

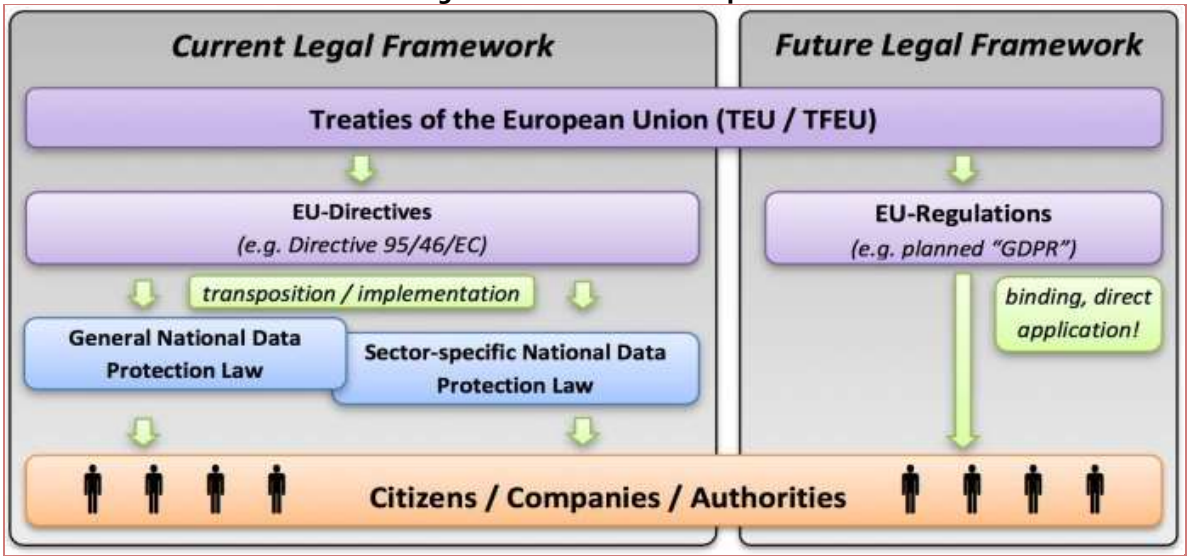
5.4 Unión Europea con énfasis en los casos de Holanda y Suecia

En el 2012 la Comisión Europea emitió la propuesta de marco legal para la protección de datos personales en Europa (*General Data Protection Regulation*) (European Commission, 2012). Esta propuesta apunta a actualizar las Directrices para Protección de Datos vigente desde 1995 "*Directive 95/46/EC*" (European Parliament, 1995). Un cambio importante que se busca alcanzar con la propuesta es el tipo de instrumento legal, que pasa de ser un documento de directrices que adopta cada país para generar sus propias leyes, a

convertirse en un reglamento cuya obligación recae directamente en todos los ciudadanos, Autoridades y Compañías de los países pertenecientes a la Unión Europea. Por consiguiente, el nuevo reglamento propuesto contendrá más detalles y especificaciones que la directriz existente, no obstante, se basa en los mismos principios generales de protección de datos que opera actualmente. Este nuevo enfoque se ilustra en la

Figura 7.

Figura 7. Comparación de estructura lógica de la Legislación en Protección de Datos entre la actual y la futura regulación en la Unión Europea.



Fuente: Smart Grid Coordination Group, 2014 (CEN-CENELEC-ETSI, 2014).

En el presente año todos los 28 Estados miembros del Consejo de la Unión Europea han declarado estar de acuerdo en emitir una nueva ley de protección de datos unificada para los países europeos (the guardian, 2015) basados en los trabajos que la Comisión Europea viene realizando desde el 2012.

Paralelamente a las propuestas de ley, también se han propuesto algunas tecnologías para mejorar la privacidad en las mediciones de los *Smart Meter*. Según el Grupo de Coordinación de *Smart Grid* (CEN-CENELEC-ETSI, 2014), el único enfoque que es ampliamente implementado es la técnica denominada "Forma anónima o seudo-anónima de los datos medidos", el cual consiste en un protocolo seguro para anonimizar la identificación de los datos. El funcionamiento se basa en que la información puede separarse en dos tipos de datos: por un lado los datos de consumo y por otro los datos personales, los cuales son almacenados en forma separada. Mientras que los datos de consumo son mediciones que se realizan con menos frecuencia, ya que son los que se utilizan para facturación, los datos personales son los que se anonimizan por lo que corresponden a mediciones que se realizan con más frecuencia y sirven para determinar comportamientos de consumo o para gestionar la demanda.

Suecia

Hasta el momento, en Suecia no existe una regulación específica para la protección de datos generados por un *Smart Meter* y por tal motivo no está explícitamente regulada la definición sobre la propiedad de los datos. A pesar de esto, el despliegue de los *Smart Meter* se completó en Suecia desde el 2009.

Existe sin embargo una reglamentación general para protección de datos personales, la cual fue establecida en 1998 por la Autoridad Sueca de Protección de Datos (*Swedish Data Protection Authority*). En ella el usuario tiene la opción de ver los datos de su propio consumo, pero no siempre es así, ya que no es obligación de los proveedores de servicio presentar al usuario esta información. Esta misma

reglamentación general advierte que el usuario tiene derecho de conocer sus datos por lo menos una vez al año a través de la empresa proveedora.

Holanda

El reglamento más importante en el Reino Holandés en cuanto a recopilación y uso de datos personales ha sido establecido en la Ley de Protección de Datos Personales (*Wet bescherming persoonsgegevens*), aprobada por el Congreso Holandés en Julio de 2000. Allí se establece que El usuario es dueño de los datos medidos por el *Smart Meter*.

El Senado Holandés, ordenó detener la instalación de los "*Smart Meters*", por el hecho de que leer remotamente los datos de consumo de cada hogar a intervalos cortos de tiempo (cada 15 minutos) vulnera del derecho a la intimidad. El Senado holandés volvió a autorizar más tarde la instalación de los contadores, pero bajo la condición de que cada contador debía tener la posibilidad de ajustar los intervalos de tiempo de medición incluyendo la posibilidad de no transmitir automáticamente ninguna lectura de forma remota. Para marzo de 2014, el gobierno holandés en documento oficial referente al Programa de *Smart Meter*, resaltó lo siguiente: "Los usuarios residenciales y de negocios pequeños en los Países Bajos, no están obligados a aceptar la instalación de los *Smart Meter*", y aclaró que en caso de que el usuario acepte su instalación, podrá escoger entre la opción de tener mediciones remotas ya sea constantemente o en situaciones específicas de tiempo (reporte bimensual, cuando cambie de operador o por mudanza).

5.5 Reino Unido

El Departamento de Energía y Cambio Climático (DECC) del Gobierno del Reino Unido, junto con la empresa Ofgem, han publicado un Programa para Implementación de *Smart Metering* y dentro de los documentos que lo componen se encuentra el reporte dedicado a seguridad y privacidad de datos "*Data Privacy and Security*" (Ofgem, 2010) publicado en julio de 2010. En el mismo se presentan los principios de los derechos del consumidor los cuales están en concordancia con la ley de 1998 denominada *Data Protection Act*, la cual implementa a su vez la *EU Data Protection Directive* "Directive 95/46/EC" (European Parliament, 1995).

Los trabajos de actualización del presente año por parte del gobierno del Reino Unido han estado a la par con los acuerdo de la Unión Europea, ya que en Mayo del 2015 publicaron una actualización del *Policy Paper* titulado "*2010 to 2015 government policy: consumer protection*" (Department for Business, Innovation & Skills , 2015) en donde anuncian que para Octubre del presente año entrará en vigor la nueva ley de los derechos del consumidor: "*Consumer Rights Act*" (Department for Business, Innovation & Skills, 2015) (UK Government, 2015).

5.6 Resumen de la comparación internacional sobre Privacidad de los consumidores en RI

Los aspectos más sobresalientes sobre el tema de privacidad de los consumidores se presentan en la Tabla 12.

Tabla 12. Resumen de las principales características sobre privacidad de los consumidores que presentan las Organizaciones de Estado.

Administración	Acuerdos, Regulación o Estándares	Observaciones principales
Agencia Internacional de Energía.	**Lineamientos:** 2012: ISGAN White paper - "Smart Grid Cyber Security"	La AIE presentó una guía para el desarrollo de un marco de trabajo con el objeto de proteger la privacidad de los datos del usuario y diseñar políticas de seguridad. Presenta especial atención en la Infraestructura de Medición Avanzada.
Estados Unidos	**Normatividad:** 2011: "Decision 11-07-056, July 28, 2011". "Attachment D - Rules Regarding Privacy and Security Protections for Energy Usage Data". 2010: Propuesta regulatoria "Senate Bill (SB) 1476". Se convirtió en ley el 29 de septiembre de 2010. ("Section 8380 - Privacy protections for customer energy consumption data collected by California energy utilities using advanced metering infrastructure"). Decisión 10-06-047 donde se aprueban los Principios de Prácticas de Información Justa (FIPPs). Ley de Privacidad de 1974 "Privacy Act of 1974". **Proyecto de implementación:** 2015: Green Button Alliance.	El Estado de California adoptó reglas para proteger la privacidad y seguridad de los datos del consumo de los usuarios, entre ellas la "Decision 11-07-056 - Attachment D", que rige el tratamiento de la información del usuario generada por los medidores avanzados (Advanced Meters), las cuales incluyen aspectos como transparencia, especificación del propósito, participación del usuario, minimización de la cantidad de datos, restricciones de divulgación y uso, calidad e integridad de datos, protección de los datos, rendición de cuentas y auditoría. En el 2015, se creó la Alianza "Green Button Alliance", con el fin de acelerar el desarrollo de aplicaciones, despliegue de estaandarización y certificaciones que promuevan la adopción de la iniciativa en la industria. Esta alianza utilizará estándares y tecnología existente proveniente de NAESB (North American Energy Standards Board) y UCAIug (UCA International Users Group), para enfocar los esfuerzos en desarrollar un ecosistema de industria compuesta por empresas eléctricas, organismos reguladores, responsables de las políticas, operadores de sistemas de control y automatización, entre otros.
Brasil	**Reportes de estudios:** 2012: "Relatório de acompanhamento setorial Smart Grid. Tendênciasno mundo e no Brasil e possibilidades de desenvolvimento produtivo e tecnológico". – Agencia Brasilera de Desarrollo Industrial (ABDI).	No se identificó que Brasil a la fecha de entrega de este reporte haya tomado medidas específicas sobre este punto
Unión Europea	**Propuesta:** 2012: "General Data Protection	La Unión Europea cuenta con un marco legal para la protección de datos personales en Europa, el cual se encuentra en proceso de actualización para

	Regulation - Regulation of the European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data". Por la Comisión Europea. 1995: "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. By the European Parliament"	convertirse en un reglamento cuya obligación recae directamente en todos los ciudadanos, Autoridades y Compañías de los países pertenecientes a la Unión Europea
Suecia	**Normatividad:** 1998: Swedish Data Protection Authority Rules.	Hasta el momento, en Suecia no existe una regulación específica para la protección de datos generados por un Smart Meter y por tal motivo no está explícitamente regulada la definición sobre la propiedad de los datos. A pesar de esto, el despliegue de los Smart Meter se completó en Suecia desde el 2009.
Holanda	**Normatividad:** 2000: "Wet bescherming persoonsgegevens" (Ley de protección de datos personales, por el Congreso Holandés)	El reglamento establece que el usuario es dueño de los datos medidos por el Smart Meter. El Gobierno Holandés declaró en marzo del 2014 que los usuarios residenciales y de negocios pequeños en los Países Bajos, no están obligados a aceptar la instalación de los Smart Meter. En caso de que el usuario acepte su instalación, podrá escoger entre la opción de tener mediciones remotas ya sea constantemente o en situaciones específicas de tiempo (reporte bimensual, cuando cambie de operador o por mudanza).
Reino Unido	**Normatividad:** 1998: Data Protection Act. Que implementa la "EU Data Protection Directive 95/46/EC". **Políticas:** 2015: "2010 to 2015 government policy: consumer protection".	Los trabajos de actualización de políticas para el presente año 2015 por parte del gobierno del Reino Unido han estado a la par con los acuerdo de la Unión Europea. Para finales de Octubre del presente año entrará en vigor la nueva ley de los derechos del consumidor: "Consumer Rights Act"

6. Conclusiones de la comparación internacional

A continuación se presentan las principales conclusiones que surgen de la comparación internacional presentada en este documento:

1) Desde la perspectiva regulatoria y de política en el sector de las Tecnologías de Información y Comunicación (TIC) se han identificado tres temas principales para el desarrollo de las redes inteligentes en el sector eléctrico colombiano: ciberseguridad, interoperabilidad y protección de la privacidad de los usuarios.

2) En relación a la ciberseguridad, la comparación internacional ha permitido relevar los siguientes aspectos:

   a) Existe un amplio consenso donde se indica que, al introducir la nueva tecnología de Redes Inteligentes, la seguridad del suministro eléctrico está directamente relacionado con la seguridad cibernética, por tanto, el éxito del correcto funcionamiento del suministro eléctrico a través de Redes Inteligentes depende, entre otros, de la protección que se tenga contra ataques cibernéticos.

   b) La totalidad de los países analizados cuenta con una Estrategia Nacional de Ciberseguridad o está en proceso de construcción de la misma.

   c) Existe una importante actividad legislativa en torno al tema de Ciberseguridad, particularmente en los Estados Unidos.

   d) En varios países se hacen esfuerzos específicos para identificar y proteger infraestructuras críticas, incluyendo las asociadas a los sectores eléctrico y de comunicaciones:

      i) En los Estados Unidos el Presidente encargó al NIST para que junto con las entidades involucradas, desarrollara un marco para la reducción de riesgos cibernéticos en infraestructura crítica. Como resultado, en 2014, se emitió el documento titulado "*Framework for Improving Critical Infrastructure Cybersecurity*".

      ii) La Unión Europea requiere a los Estados miembros para que identifiquen posibles infraestructuras críticas europeas, que se definen como activos o sistemas esenciales para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, económicas o sociales del bienestar de las personas, ubicada en los estados miembros, donde la interrupción o destrucción de estos activos o sistemas tendrían un impacto significativo.

      iii) A nivel institucional el Reino Unido cuenta con un Centro de Protección de la Infraestructura Nacional, el cual cubre las áreas de seguridad física, personal y ciberseguridad. A su vez, España creó el Centro Nacional de Protección de Infraestructuras Críticas, que entre otros cometidos se encarga de la ciberseguridad de las mismas.

   e) Se han establecido lineamientos de seguridad específicos para redes inteligentes:

      i) En Estados Unidos el NIST publicó el Reporte Institucional NISTIR 7628. Existe además una guía publicada por el DOE y la corporación NERC: "*Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*" y una normativa compuesta por los estándares CIP (*Critical Infrastructure Protection*) de la corporación NERC.

      ii) En la Unión Europea el documento SG-GC/M490_H Seguridad de la Información en Redes Inteligentes, establece recomendaciones y estándares para soportar las Redes Inteligentes bajo arquitectura SGAM. A su vez ENISA estableció recomendaciones para los sectores

público y privado involucrados en la definición e implementación de las Redes Inteligentes en su documento: "*Smart Grid Security*".

iii) Brasil definió una arquitectura propia de Red Inteligente (REI-BR-2030) en la cual identificó la ciberseguridad como un elemento transversal a la arquitectura de referencia. Sin embargo, el tema se considera en desarrollo y no se han identificado recomendaciones específicas de ciberseguridad para Redes Inteligentes.

f) En Europa ENISA publicó el documento "*Smart grid security certification in Europe Challenges and recommendations*" que describe la necesidad de establecer prácticas armonizadas a nivel Europeo para la certificación de redes inteligentes. Dichas prácticas deben cubrir la cadena de suministro completa de la red eléctrica inteligente y ser compatibles con una plataforma europea basada en la Arquitectura SGAM, en particular en el documento SG-GC/M490_H Seguridad de la Información en Redes Inteligentes.

3) En cuanto a la interoperabilidad, la comparación internacional evidenció lo siguiente:

a) A nivel Latinoamericano, los mayores avances en la definición de estándares de interoperabilidad fueron identificados en Brasil donde la ABDI en su versión preliminar del mapeo de la cadena de Proveedores TIC y sub productos y servicios de Red Inteligente estableció las Normas y Estándares más utilizados a nivel mundial en Redes Inteligentes y su grado de utilización en Brasil por tipo de áreas de aplicación tecnológica.

i) Brasil cuenta además con algunas normas técnicas propias con aplicación a Redes Inteligentes, destacándose su propuesta de protocolo abierto para sistemas de medición, denominada Sistema Brasileño de Multimedición Avanzada (SIBMA) cuyo objetivo es permitir la integración de los contadores inteligentes para la medición remota con la central de distribución de energía.

b) Pero el esfuerzo de normalización más importante para el caso Colombiano es el emprendido por la Unión Europea, dada la recomendación de los Consultores de la Componente I de utilizar la arquitectura SGAM definida por CEN-CENELEC-ETSI como referencia para el caso Colombiano

i) En 2011 la Comisión Europea expidió el mandato de estandarización denominado M/490 *Smart Grid Mandate* por medio del cual solicitó a las Organizaciones de Estandarización Europeas (ESO) el desarrollo o actualización de un conjunto de normas coherentes dentro de un marco europeo común que integren una variedad de tecnologías de computación de comunicación digitales y arquitecturas eléctricas con los procesos y servicio asociados, que permitan lograr la interoperabilidad y habiliten o faciliten la aplicación en Europa de los diferentes servicios y funcionalidades de las RI según la definición del *Smart Grid Task Force*.

ii) En respuesta a dicho mandato las ESO combinaron sus aproximaciones estratégicas por medio del Grupo de Coordinación de Redes Inteligentes del CEN-CNELEC-ETSI (denominado SG-CG). Para 2014 el SG-CG había dado respuesta al mandato M/490 mediante la finalización de un conjunto de reportes que constituyen el cuerpo de la Arquitectura SGAM.

4) Finalmente, en el aspecto de protección de la privacidad de los usuarios, la comparación internacional permitió establecer los siguientes aspectos:

a) Existe amplio consenso en que la posibilidad de utilizar infraestructura de medición avanzada genera preocupaciones sobre los derechos de los consumidores, especialmente en relación con su privacidad.

b) En Estados Unidos, el Estado de California adoptó reglas para proteger la privacidad y seguridad de los datos del consumo de los usuarios las cuales incluyen aspectos como transparencia, especificación del propósito, participación del usuario, minimización de la cantidad de datos,

restricciones de divulgación y uso, calidad e integridad de datos, protección de los datos, rendición de cuentas y auditoría.

c) La Unión Europea cuenta con un marco legal para la protección de datos personales en Europa, el cual se encuentra en proceso de actualización para convertirse en un reglamento cuya obligación recae directamente en todos los ciudadanos, Autoridades y Compañías de los países pertenecientes a la Unión Europea.

   i. Dentro de la Unión Europea es significativo el caso de Holanda donde los usuarios residenciales y de negocios pequeños no están obligados a aceptar la instalación de los *Smart Meter* y en caso de que el usuario acepte su instalación, podrá escoger entre la opción de tener mediciones remotas ya sea constantemente o en situaciones específicas de tiempo.

7. Diagnóstico del esquema regulatorio Colombiano de TIC con aplicación a Redes Inteligentes

7.1 Segmentos, actores y/o componentes del sector de telecomunicaciones relacionados con el sector eléctrico

Si bien algunas empresas que están en el sector de energía se encuentran integradas o participan de un grupo que tiene intereses en el sector de las Telecomunicaciones, tales como ISA y EMCALI, en general no se encontró evidencia de interacción directa entre las empresas de energía y las instituciones a nivel del gobierno relacionadas con el sector TIC tales como MinTIC, CRC ó ANE[21].

En cambio, sí existe una interacción entre las empresas de energía y las empresas prestadoras de servicios de Telecomunicaciones, la cual es, esencialmente, del tipo proveedor-cliente.

En este tipo de relación, las empresas de energía contratan los servicios de las empresas de telecomunicaciones, esencialmente para la provisión de sus redes de datos corporativas, que son redes de área amplia (redes WAN) a nivel nacional y en algunos casos, también contratan soluciones de último kilómetro para la conexión con usuarios finales.

Las redes WAN que contratan las empresas del sector eléctrico se utilizan para la conexión de las redes de área local (redes LAN) corporativas ubicadas tanto en las áreas administrativas como en las áreas operativas y centros de gestión de las empresas del sector eléctrico. Típicamente son redes IP soportadas en tecnologías de transporte basadas en fibra óptica. Los contratos para este tipo de redes están respaldados mediante acuerdos de nivel de servicio (SLA) que garantizan la disponibilidad mediante un porcentaje de tiempo de funcionamiento, típicamente igual o superior a 99,6%.

En cuanto a las redes de último kilómetro se encontró evidencia del uso de conexiones basadas en tecnologías celulares tales (GPRS, 3G y LTE), pero algunas empresas indicaron su aspiración futura de utilizar conexiones de fibra óptica.

De hecho, en relación con el tema de la red de último kilómetro, una empresa indicó su aspiración de llevar los AMI hasta los usuarios por medio de su propia unidad de telecomunicaciones o mediante combinación de soluciones (unas tercerizadas y otras construidas directamente) y dio como ejemplo la implementación del AMI para prepago que en su opinión debe hacerse por fibra óptica. Sin embargo expresó sus inquietudes respecto a cómo hacer inversiones en equipos de telecomunicaciones considerando la regulación del sector eléctrico, que en su concepto, no motiva ni incentiva hacer grandes inversiones porque no está claro cómo se van a remunerar. Mencionó que previamente las inversiones se han pagado contra reducción de pérdidas o incremento en el recaudo, pero hay nuevos espacios de inversión donde la reducción de pérdidas no genera el retorno esperado.

Otra empresa indicó que si se toma el caso de los medidores inteligentes la mejor solución es apoyarse en proveedores de red celular, pero la gran incertidumbre es el acuerdo de nivel de servicio porque los Operadores móviles son renuentes a firmarlo. También indicó que para una empresa de energía no es rentable tener una infraestructura de telecomunicaciones porque la obsolescencia es muy rápida y porque

[21] Con el propósito de establecer los tipos de relaciones, interacción y coordinación entre los actores del sector eléctrico y del sector de las telecomunicaciones y en concreto con el desarrollo de las Redes Inteligentes (RI) se realizó una teleconferencia el 22 de septiembre de 2015 en la cual participaron las empresas CODENSA (Ing César Rincón e Ing Héctor A Díaz), EPSA (Ing Carlos Andrés Becerra e Jaime Sánchez) y EMCALI (Ing Omar Arango e Ing Gerardo Rojas). Se discutieron además temas relacionados con Ciberseguridad e Interoperación para RI.

además coincide con la primera empresa en que es necesario saber cómo se remunerarían nuevas inversiones, si fueran en telecomunicaciones.

Otra empresa consultada sobre si el acceso a los clientes debe hacerse mediante tecnologías PLC o el uso de redes de acceso de telecomunicaciones de un tercero, indicó que PLC es una alternativa importante hasta cierto punto, por ejemplo hasta concentradores y luego desde ahí se utiliza, por ejemplo GPRS. Sin embargo siguen explorando posibilidades. Indicaron que en caso de expandir los sistemas por ejemplo hacía un *Smart Metering,* eventualmente puede valer la pena una red propia. Sin embargo, mencionaron que hoy en día, dados los costos de GPRS y planes de datos las iniciativas de medición remota se hacen inviables. Por último coincidió en que el aspecto regulatorio de inversiones en nuevas tecnologías todavía tiene un el panorama que no está claro.

Por tanto, entre los aspectos mencionados por las empresas del sector eléctrico en su relación con el sector de telecomunicaciones y que pueden guardar relación con aspectos de política sectorial o regulación, es importante resaltar lo siguiente: la calidad de servicio y los costos de la conexión de último kilómetro, han sido identificados por los actores del sector eléctrico como posibles barreras para el despliegue de RI.

1) En relación con los precios minoristas del mercado de datos móviles, mencionados como una barrera en el desarrollo del *Smart Metering*, es importante mencionar que la Ley 1341 de 2009 (Congreso - Ley 1341, 2009) establece que los PRST podrán fijar libremente los precios al usuario y la CRC sólo podrá regular estos precios cuando no haya suficiente competencia, se presente una falla de mercado o cuando la calidad de los servicios ofrecidos no se ajuste a los niveles exigidos, indicándose además que la CRC hará énfasis en la regulación de mercados mayoristas.
2) En cuanto al tema de la no disponibilidad de acuerdos de nivel de servicio y los problemas de calidad de servicio (QoS) de las redes móviles, la Resolución CRC 4734 de 2015 (CRC, 2015) adoptó medidas regulatorias que amplían las obligaciones de los Operadores Móviles en QoS, incluyendo entre otros, la publicación de mapas de cobertura por tipo de tecnología y la medición de parámetros de acceso a internet a través de redes móviles.
    a) Sin embargo, es difícil que se puedan establecer acuerdos de nivel de servicio en redes móviles porque los recursos de acceso radioeléctricos no son dedicados por usuario sino compartidos entre múltiples usuarios que tienen patrones de tráfico variables en el tiempo.

Se identifica además otra posible barrera, para el despliegue de RI pero relacionada con la regulación del sector eléctrico y es que no se ha definido el reconocimiento que se le hace a las empresas del sector por sus inversiones en activos de telecomunicaciones.

Entonces, como ya se mostró, las empresas del sector eléctrico describen su relación con el sector de telecomunicaciones en términos cliente - proveedor, pero tienen una clara percepción que la situación está cambiando y que los desarrollos tecnológicos del sector eléctrico pueden implicar una convergencia entre estas industrias hacia el futuro.

Al respecto una empresa indicó la necesidad de establecer mecanismos y herramientas de comunicación formales entre los sectores de energía y telecomunicaciones. La empresa sugirió que puede haber proyectos especiales enfocados en RI para pagar las inversiones así como regulación que apoye las redes inteligentes, tanto en el sector eléctrico como el de telecomunicaciones: algún tipo de convergencia.

Otra empresa indicó que la discusión se enmarca en el tema convergente de las tecnologías, donde el sector eléctrico ha ido madurando de forma tradicional pero ahora hay una interdependencia entre tecnologías de operación con las TICs. También indicó que a nivel regulatorio telecomunicaciones y energía son mundos muy dispares y se requieren reglas para la red convergente que se tiene de aquí en adelante. Mencionó que la regulación no va a la velocidad que lo requiere el sector e ilustró el caso con las energías renovables.

7.2 Protección de la Privacidad de los consumidores

Constitución Política

La Constitución Política de Colombia (Asamblea Nacional Constituyente, 1991) incluye en su artículo 15, dentro de los derechos fundamentales, el de intimidad personal y familiar y el del buen nombre. De igual modo, dicho artículo incluye el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre las personas en bancos de datos y en archivos de entidades públicas y privadas; y el derecho a que en la recolección, tratamiento y circulación de datos se respeten la libertad y demás garantías consagradas en la Constitución.

Legislación relacionada con habeas data y manejo de información contenida en bases de datos

En el año 2008 la Ley Estatutaria 1266 (Congreso de Colombia, 2008) desarrolló el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

La Ley en mención se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada, con algunas excepciones, por ejemplo, de las bases de datos asociadas con la inteligencia del estado.

La Ley contiene una serie de definiciones que son importantes para este análisis: titular de la información, fuente de información, operador de información, usuario, dato personal, dato semiprivado y dato privado.

El titular de la información es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y es sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la ley.

La fuente de información es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos.

El operador de información es la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente.

El usuario es la persona natural o jurídica que puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos

del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos.

El dato personal es cualquier pieza de información vinculada a una o varias personas determinadas o determinables, o que puedan asociarse con una persona natural o jurídica. Los datos personales pueden ser: públicos, semiprivados o privados.

Un dato semiprivado es el que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general. A su vez un dato privado es el que por su naturaleza íntima o reservada sólo es relevante para el titular.

La Ley establece un conjunto de principios de administración de los datos, los cuales incluyen los de: (i) veracidad o calidad de los registros o datos, (ii) finalidad, (iii) circulación restringida, (iv) temporalidad de la información, (v) interpretación integral de derechos constitucionales como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información; (v) seguridad y (vi) confidencialidad.

La Ley hace explícitos los derechos de los titulares de la información los cuales se pueden ejercer frente a los operadores de los bancos de datos, las fuentes de información y los usuarios, como se explica a continuación:

1. Frente a los operadores de los bancos de datos, entre otros: el derecho fundamental al habeas data[22], la certificación de la existencia de la autorización expedida por la fuente o por el usuario y Solicitar información acerca de los usuarios autorizados para obtener información.
    a. La administración de datos semiprivados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países el cual no requiere autorización del titular.
2. Frente a las fuentes de información, entre otros: Ejercer los derechos fundamentales al hábeas data y de petición, pedir la actualización o rectificación de los datos contenidos en la base de datos y solicitar prueba de la autorización, cuando la misma sea requerida
3. Frente a las fuentes de información, entre otros: solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador y solicitar prueba de la autorización, cuando ella sea requerida.

Existen además un conjunto de deberes de los operadores de los bancos de datos, las fuentes de información y los usuarios, mismos que no van a ser profundizados en este análisis.

Legislación relacionada con la protección de datos personales

En el año 2012 la Ley Estatutaria 1581 (Congreso de Colombia, 2012) dictó un conjunto de disposiciones generales para la protección de datos personales con el objeto de desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

[22] La Corte Constitucional de Colombia definió el derecho Hábeas Data como el derecho que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de su divulgación, publicación o cesión, de conformidad con los principios que regulan el proceso de administración de datos personales. Asimismo, ha señalado que este derecho tiene una naturaleza autónoma que lo diferencia de otras garantías con las que está en permanente relación, como los derechos a la intimidad y a la información.

La Ley en mención se aplica a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada, con algunas excepciones, por ejemplo, de las bases de datos asociadas con seguridad y defensa nacional, monitoreo y control de lavado de activos y financiación del terrorismo, la inteligencia del estado, bases de datos y archivos con información periodística y bases de datos reguladas por la Ley 1266 de 2008 (ver sección 0).

La Ley contiene una serie de definiciones que son importantes para este análisis: autorización, base de datos, dato personal, encargado del tratamiento, responsable del tratamiento, titular y tratamiento.

La Autorización es el consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales; la Base de Datos es el conjunto organizado de datos personales que sea objeto de tratamiento; el Dato Personal es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables; el Encargado del Tratamiento es la Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta del responsable del tratamiento; el Responsable del Tratamiento es la Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos; el Titular es la Persona natural cuyos datos personales sean objeto de Tratamiento; y finalmente el Tratamiento es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

La Ley establece un conjunto de principios de administración de los datos, los cuales incluyen los de: (i) legalidad en materia de tratamiento de datos, (ii) finalidad, (iii) libertad donde se indica que el Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular salvo algunas excepciones[23], (iv) veracidad o calidad, (v) transparencia según la cual debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan, (vi) acceso y circulación restringida, (vii) seguridad y (viii) confidencialidad.

La Ley prohíbe expresamente el tratamiento de datos sensibles (aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación) y de datos personales de niños, niñas y adolescentes.

La Ley hace explícitos los derechos de los titulares, los cuales incluyen los siguientes:

1. Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
2. Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito.
3. Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
4. Presentar ante la Superintendencia de Industria y Comercio (SIC) quejas por infracciones a lo dispuesto en la Ley;
5. Revocar(por determinación de la SIC) la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales;

[23] Por ejemplo: Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, datos de naturaleza pública, casos de urgencia médica o sanitaria, tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos, datos relacionados con el Registro Civil de las Personas.

6. Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Existe además el deber por parte del Responsable del Tratamiento, al momento de solicitar al Titular la autorización, de informarle de manera clara y expresa, entre otros, lo siguiente: El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; los derechos que le asisten como Titular y la identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Decreto Reglamentario de la Ley de protección de datos personales

En el año 2013, el Gobierno Nacional expidió el Decreto 1377 (Presidencia de la República de Colombia, 2013) mediante el cual se reglamentó parcialmente la Ley 1581 de 2012 (ver sección 0). Dicha reglamentación cubre los aspectos de autorización, políticas de Tratamiento de la información, ejercicio de los derechos de los Titulares, transferencias y transmisiones internacionales de datos personales y responsabilidad demostrada frente al tratamiento de datos personales.

En particular resultan de interés los siguientes aspectos del reglamento:

1. En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos
2. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.
3. Los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.
4. Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.
5. Los Titulares podrán en todo momento solicitar al responsable o encargado la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo
6. Los Responsables y Encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento
7. Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas, las cuales deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares
8. En los casos en los que no sea posible poner a disposición del Titular las políticas de tratamiento de la información, los responsables deberán informar por medio de un aviso de privacidad al titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales
9. El Titular podrá consultar de forma gratuita sus datos personales: (i) al menos una vez cada mes calendario, y (ii) cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas.

Regulación de Telecomunicaciones

La Resolución CRC 3066 de 2011 (CRC, 2011) incluye dentro de los derechos de los usuarios de los

servicios de comunicaciones: el de gozar de una protección especial en cuanto al manejo confidencial y privado de los datos personales que ha suministrado al proveedor, así como al derecho a que dichos datos no sean utilizados por el proveedor para fines distintos a los autorizados por el usuario.

Adicionalmente, indica que con el fin de asegurar la protección de los datos personales suministrados por el usuario al momento de la celebración del contrato y, en todo caso, durante la ejecución del mismo, los proveedores garantizarán que dichos datos sean utilizados para la correcta prestación del servicio y el adecuado ejercicio de los derechos de los usuarios y que los datos personales de los usuarios no podrán ser utilizados por los proveedores de servicios de comunicaciones para la elaboración de bases de datos con fines comerciales o publicitarios, distintos a los directamente relacionados con los fines para los que fueron entregados, salvo que el usuario así lo autorice, de manera expresa y escrita.

Adicionalmente, la mencionada resolución establece que los proveedores no podrán entregar a su arbitrio los datos de localización y de tráfico del usuario, salvo autorización expresa y escrita de este.

Regulación del Sector Eléctrico

En el 2014 la Comisión de Regulación de Energía y Gas (CREG) modificó el Código de Medida mediante Resolución 038 de 2014 (CREG, 2014). La Resolución establece las condiciones técnicas y procedimientos que se aplican a la medición de energía de: los intercambios comerciales en el Sistema Interconectado Nacional (SIN), los intercambios con otros países, las transacciones entre agentes y las relaciones entre agentes y usuarios.

La mencionada Resolución establece que los representantes de las fronteras deben asegurar que los medidores, tanto el principal como el de respaldo, de las fronteras comerciales con reporte al ASIC cuenten con un sistema de protección de datos. También indica que el CNO debe definir los requerimientos mínimos de seguridad e integridad para la transmisión de los datos entre el medidor y el Centro de Gestión de Medidas y entre este último y el ASIC. Además establece dos niveles de acceso:

Nivel de acceso 1: Lectura de la identificación de la frontera comercial, las mediciones realizadas y los parámetros configurados en el medidor.

Nivel de acceso 2: Configuración de las funciones de tiempo y/o fecha, calibración, configuración de los parámetros y restauración del equipo, así como el nivel anterior.

También indica que el representante de la frontera debe administrar el acceso al medidor, estableciendo una lista de usuarios, contraseñas y niveles de acceso otorgados, además debe mantener un registro de los accesos al medidor de Nivel de acceso 2 en el cual identificar como mínimo la fecha y hora de acceso, la persona o funcionario, propósito del acceso, actividades realizadas y la constancia de que el medidor quedó operando correctamente.

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

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

Los Representantes de la Frontera (RF) deben adecuar los sistemas de medición, bases de datos y sus procedimientos dentro de los 24 meses siguientes a la entrada en vigencia de la presente resolución, para dar cumplimiento a lo señalado en este artículo.

Adicionalmente se indica que todos los agentes que tengan acceso a las lecturas de las mediciones deben aplicar los requisitos legales vigentes sobre la protección de datos de los usuarios.

La CREG también indica que las condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC deben ser definidas por el CNO considerando: los riesgos potenciales, la flexibilidad, escalabilidad, interoperabilidad, eficiencia y economía para el intercambio de los datos de las mediciones y el acceso a los diferentes sistemas de información

Finalmente, la CREG indica que el ASIC debe implementar y mantener un sistema de gestión de la seguridad de la información para los procesos involucrados en la gestión de las mediciones reportadas por los representantes de las fronteras con base en la norma ISO/IEC 27001 y debe obtener una certificación dentro de los 24 meses siguientes a la entrada en vigencia de la Resolución.

7.3 Identificación de barreras y oportunidades de mejora relacionadas con la protección de la privacidad de los consumidores en Colombia

Como se presentó en las secciones previas, se identifican un conjunto de fortalezas en el tema de protección de privacidad de los consumidores en Colombia con aplicaciones a Redes Inteligentes:

1) La Constitución garantiza entre otros, como un derecho fundamental, el de intimidad personal y familiar y el del buen nombre; así como el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre las personas en bancos de datos y en archivos de entidades públicas y privadas; y el derecho a que en la recolección, tratamiento y circulación de datos se respeten la libertad y demás garantías consagradas en la Constitución.

    a) Existe legislación estatutaria específica relacionada con habeas data, manejo de información contenida en bases de datos y protección de datos personales.
    b) Existen decretos reglamentarios de las leyes de protección de datos personales.
    c) Por tanto, la protección de la privacidad de la información en Colombia tiene un origen constitucional, expresado como un derecho fundamental respecto del cual existen leyes estatutarias que son aplicables y de obligatorio cumplimiento en todos los sectores de la economía y de manera independiente de la tecnología que sea utilizada.
    d) Es de anotar que las empresas del sector eléctrico, tienen que cumplir tanto la Ley Estatutaria 1581 de 2012 como el Decreto Reglamentario 1377 de 2013, en la medida en que sean Encargados o Responsables del Tratamiento de Datos Personales, conforme lo definido por la Ley
        i) En el caso de los datos de consumo eléctrico de las personas naturales dado que se trata de información que puede asociarse a una o varias personas, son datos personales y se requiere de la autorización de su titular para recolectarlos y procesarlos.
        ii) Por tanto, la autorización a solicitar al Titular debe indicarle qué datos personales serán recolectados y cuál será la finalidad específica del tratamiento.
        iii) Además como la Ley prohíbe expresamente el tratamiento de datos sensibles (aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación) el Tratamiento de los datos personales por parte del Sector Eléctrico (por ejemplo el consumo de los usuarios) debe ser lo suficientemente agregado como para que no viole su intimidad, por ejemplo mediante patrones de consumo que no sean demasiado detallados, tal que no puedan revelar sus hábitos de vida.
2) La regulación de telecomunicaciones y del sector eléctrico han dado pasos para asegurar la protección de datos personales.
    a) A nivel del sector eléctrico la CREG estableció que el ASIC debe implementar y mantener un sistema de gestión de la seguridad de la información para los procesos involucrados en la gestión de las mediciones reportadas por los representantes de las fronteras con base en la norma ISO/IEC 27001

Considerando lo anterior se concluye que:

1) El tema de datos personales está adecuadamente cubierto en términos de política
2) A nivel regulatorio se identifican oportunidades de mejora específicas:
    a. Considerando lo establecido por la Ley Estatutaria 1581 de 2012 en relación al tratamiento de datos sensibles de personas naturales, es necesario precisar para el sector eléctrico qué datos se pueden obtener y que tipo de Tratamiento puede hacerse de los mismos, independientemente de la tecnología que se esté considerando. También debe establecerse qué datos deberían ser públicos para no alterar la libre competencia.
        i. También se debe definir que tratamiento se debe dar a los datos de personas jurídicas.

Por otro lado existe una oportunidad de mejora para las empresas del sector eléctrico tiene que asegurar el cumplimiento de los mandatos de la Ley en tanto sean Encargados o Responsables del Tratamiento de Datos Personales.

7.4 Interoperabilidad en Colombia

Legislación de telecomunicaciones e interoperabilidad

La Ley 1341 de 2009 (Congreso - Ley 1341, 2009) por la cual, entre otros, se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC establece que en desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones, entre otros, para garantizar la interconexión y la interoperabilidad de las redes de telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.

La misma Ley también indica que entre las funciones de la CRC está imponer de oficio o a solicitud de parte, las servidumbres de acceso, uso e interconexión y las condiciones de acceso y uso de instalaciones esenciales, recursos físicos y soportes lógicos necesarios para la interconexión, y señalar la parte responsable de cancelar los costos correspondientes, así como fijar de oficio o a solicitud de parte las condiciones de acceso, uso e interconexión. Así mismo, la CRC puede determinar la interoperabilidad de plataformas y el interfuncionamiento de los servicios y/o aplicaciones.

Adicionalmente, uno de los principios orientadores de la Ley que resultan relevantes en este análisis es el de neutralidad tecnológica, de acuerdo con el cual el Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible

Resoluciones del MinTIC asociadas con interoperabilidad

El MinTIC, por solicitud expresa de la Ley 1341 de 2009 (Congreso - Ley 1341, 2009), definió el significado de una Red de Telecomunicaciones mediante la Resolución 202 de 2010 (MinTIC, 2010), indicando que es el "Conjunto de nodos y enlaces alámbricos, radioeléctricos, ópticos u otros sistemas electromagnéticos, incluidos todos sus componentes físicos y lógicos necesarios, que proveen conexiones entre dos (2) o más puntos, fijos o móviles, terrestres o espaciales, para cursar telecomunicaciones. Para su conexión a la red, los terminales deberán ser homologados y no forman parte de la misma."

Adicionalmente definió la interoperabilidad como la aptitud de los sistemas y aplicaciones, basados en Tecnologías de la Información y las Comunicaciones, y los procesos que estos soportan, para intercambiar información y posibilitar mutuamente la información intercambiada. Para el caso de redes de telecomunicaciones, la interoperabilidad es inherente a la interconexión de las mismas.

Finalmente, la misma Resolución bajo análisis definió la interconexión como la vinculación de recursos físicos y soportes lógicos de las redes, incluidas las instalaciones esenciales, necesarias para permitir el interfuncionamiento de los servicios y/o aplicaciones y la interoperabilidad de plataformas.

Regulación de la CRC asociada con la interoperabilidad

El Régimen de acceso, uso e interconexión de redes está regulado por la CRC mediante la Resolución 3101 de 2011 (CRC, 2011). Dicha Resolución amplió la definición de interconexión provista por la Resolución 202 de 2010 (MinTIC, 2010), indicando que la interconexión es la vinculación de recursos físicos y soportes lógicos de las redes de telecomunicaciones, incluidas las instalaciones esenciales, necesarias para permitir el interfuncionamiento de redes y la interoperabilidad de plataformas, servicios y/o aplicaciones que permite que usuarios de diferentes redes se comuniquen entre sí o accedan a servicios prestados por otro proveedor. La interconexión de las redes implica el uso de las mismas y se constituye en un tipo especial de acceso entre proveedores de redes y servicios de telecomunicaciones.

De esta manera el ámbito de la intervención del estado que se mencionó en la sección 8, para garantizar la interconexión y la interoperabilidad, la primera se da entre redes de telecomunicaciones diferentes entre sí.

Adicionalmente la CRC establece una distinción entre el interfuncionamiento el cual se da entre redes y la interoperabilidad la cual se da entre plataformas.

La misma Resolución 3101 indica que el interfuncionamiento es la interacción entre redes, entre sistemas finales o entre partes de los mismos, con el propósito de proporcionar una entidad funcional capaz de soportar comunicaciones extremo a extremo, en total conformidad con la definición contenida en la recomendación UIT-T Y.2261 (UIT, 2007).

En cuanto a la interoperabilidad, la CRC profundizó la definición del MinTIC contenida en la Resolución 202 de 2010 (MinTIC, 2010), indicando que es el correcto funcionamiento de plataformas, servicios y/o aplicaciones que se prestan sobre redes interconectadas, a partir del intercambio mutuo de información y la utilización de la misma

Adicionalmente la CRC indica en relación con la neutralidad tecnológica que los proveedores[24] podrán utilizar cualquier tecnología que elijan para la prestación de sus servicios, siempre que se preserve la interoperabilidad de plataformas, servicios y/o aplicaciones y el interfuncionamiento de redes.

La Resolución 3101 también indica que con el objeto de proveer redes y/o servicios de telecomunicaciones, aplicaciones y/o contenidos, cualquier proveedor[25] tiene derecho al acceso a las instalaciones esenciales de los proveedores de redes y servicios de telecomunicaciones (PRST) y establece que si una relación de acceso involucra el uso de plataformas tecnológicas, los proveedores deberán establecer las condiciones necesarias para garantizar la interoperabilidad con las plataformas de otros proveedores, para lo cual garantizarán, entre otros aspectos, una disponibilidad mínima de interfaces abiertas y la prestación de servicios, aplicaciones y/o contenidos a usuarios de cualquier red.

[24] Entendiéndose en el contexto de la Resolución 3101 que se trata de una persona natural o jurídica que sirviéndose de redes de telecomunicaciones, presta a terceros servicios de telecomunicaciones, provee contenidos y/o aplicaciones, o comercializa redes o servicios de telecomunicaciones y que dicho proveedor puede o no operar una red.
[25] ídem.

El análisis combinado de las secciones 8 y 0 y de las regulaciones discutidas en esta sección, llevan a concluir que aun cuando existe un principio de neutralidad tecnológica aplicable al sector TIC, en su aplicación se debe preservar tanto la interoperabilidad de plataformas como el interfuncionamiento de redes. Ahora bien, interoperabilidad e interfuncionamiento son conceptos aplicables en un contexto de interconexión de redes de telecomunicaciones que son diferentes entre sí o en relación con el acceso por parte de proveedores[26] a las redes de telecomunicaciones de los PRST.

En tal sentido, la tradición observada en el sector de telecomunicaciones en Colombia es que se establecen regulaciones técnicas sobre las redes únicamente para (i) garantizar la interconexión entre redes distintas (por ejemplo mediante la definición de protocolos de interconexión, características de transmisión o determinación de códecs) (CRC, 2011), o (ii) para asegurar la calidad del servicio y la seguridad de las redes.

Interoperabilidad y adopción de normas CEN-CENELEC-ETSI

No existe una definición formal en Colombia sobre la interoperabilidad de RI, en la medida en que se trata de un tema apenas en desarrollo.
Los Consultores de la Componente I han elegido como referencia para el análisis del conjunto de funcionalidades previstas, el modelo CEN-CENELEC-ETSI *Smart Grid Architecture Module* (SGAM) del *Smart Grid Coordination Group* (CEN-CENELEC-ETSI Smart Grid Working Group , 2012). Dicho modelo ha sido conformado por las tres organizaciones de estandarización oficialmente reconocidas por la Unión Europea (UE) como las responsables de la definición de estándares voluntarios a nivel Europeo[27]: el *Comité Européen de Normalisation*, el *Comité Européen de Normalisation Electrotechnique* y el *European Telecommunications Standard Institute* (CEN-CENELEC-ETSI).

Adopción de Normas ICONTEC

En relación con la adopción de Normas Técnicas Nacionales asociadas con la interoperación de Redes Inteligentes, se encontró evidencia únicamente de normalización en relación con medidores de energía eléctrica.

Medidores de energía eléctrica

El Instituto Colombiano de Normas Técnicas (ICONTEC) cuenta con el Comité Técnico 144, el cual trabaja el tema de Medidores de energía eléctrica, cuyo ámbito de Normalización incluye medidores de energía eléctrica y equipos de control de carga eléctrica, tales como medidores de energía activa, medidores de energía reactiva, indicadores de demanda máxima, telemedida para consumo y demanda, equipo para lectura remota e interruptores temporizados[28].

El Comité cuenta con un conjunto de Normas Técnicas Colombianas (NTC) que hacen referencia al tema de medidores de energía eléctrica, muchas de las cuales tienen correspondencia con Normas de la Comisión Electrotécnica Internacional (IEC) (Osorio Muñoz). Varias de estas NTC son mencionadas en la modificación del Código de Medida establecido por la Comisión de Regulación de Energía y Gas (CREG) mediante Resolución 038 de 2014 (CREG, 2014).

---

[26] ídem.
[27] Al respecto, ver por ejemplo:
https://www.cen.eu/about/Pages/default.aspx
http://www.cenelec.eu/aboutcenelec/whoweare/index.html
http://www.etsi.org/about/what-we-are
[28] Ver: http://icontec.org/index.php/es/inicio/comites-tecnicos-de-normalizacion/180-comite-144
Consulta realizada el 17 de septiembre de 2015.

Entre las Normas Técnicas Colombianas existe la NTC 6079 de 2014 (Icontec, 2014) que establece los requisitos para Sistemas de Infraestructura de Medición Avanzada (AMI) en redes de distribución de Energía Eléctrica.

La Norma en mención define un sistema AMI con una solución integral que tiene la capacidad de gestionar el intercambio de información y datos entre el sistema de gestión y las unidades de medida, permite la gestión remota de diferentes funcionalidades como la toma de lecturas, procesos de conexión y desconexión para los medidores que posean dicha capacidad, eventos y alarmas, el control de acceso a las interfaces entre otras funcionalidades. El sistema AMI incluye una amplia gama de aplicaciones que permite gestionar la demanda, optimizar la red de distribución, garantizar la integridad del sistema y proveer servicios de valor agregado.

La Norma NTC 6079 también define la interoperabilidad como la capacidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada. En este sentido, la definición usada es similar a la de la IEEE (IEEE), es decir: "La capacidad de dos o más redes, sistemas, dispositivos, aplicaciones o componentes de interfuncionar, intercambiar y utilizar la información con el fin de realizar las funciones requeridas." Es importante recordar que se había establecido la coincidencia entre la definición de la IEEE mencionada y la adoptada por el modelo CEN-CENELEC-ETSI (CEN-CENELEC-ETSI, 2014).

La Norma NTC 6079 establece los requisitos de tecnología, protocolos y modelos de datos para garantizar la interoperabilidad entre la unidad de medida y el sistema de gestión e indica que para la comunicación local o remota de los dispositivos se pueden emplear interfaces eléctricas, ópticas, por PLC o radiofrecuencia. Para los protocolos de capa de aplicación establece el uso de los estándares IEC 62056 (IEC, 2014), ANSI C12.22 (ANSI, 2009), IEC 61968-9 (IEC, 2010) o *Multispeak*. En cuanto al modelo de datos se deben utilizar los estándares IEC 62056 [30] y ANSI C12.19 (ANSI, 2009).

La Norma también indica los requisitos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.

El sector eléctrico colombiano y la interoperabilidad

Se discutió el tema de interoperabilidad con varias empresas del sector Eléctrico: CODENSA, EMCALI y EPSA[29] y se obtuvó un conjunto de respuestas de CODENSA a un cuestionario sobre el tema enviado a dichas empresas.

En general existe concenso en cuanto a que la interoperabilidad es un tema importante en el desarrollo de las RI y necesita un marco de referencia nacional.

Una de las empresas estuvo de acuerdo con la necesidad de apoyar la adopción de SGAM como referencia para Colombia e indicó que dicho estándar se considera el más avanzado a nivel mundial en términos de desarrollo y experiencia en el campo de RI. Sin embargo, manifestó que a la fecha, a nivel de la Comisión Europea no se ha definido un proceso de certificación de interoperabilidad y si bien estándares y guías han sido definidos una certificación de interoperabilidad de soluciones no es obligatoria.

[29] Con el propósito de establecer los tipos de relaciones, interacción y coordinación entre los actores del sector eléctrico y del sector de las telecomunicaciones y en concreto con el desarrollo de las Redes Inteligentes (RI) se realizó una teleconferencia el 22 de septiembre de 2015 en la cual participaron las empresas CODENSA (Ing Cesar Rincon e Ing Hector A Diaz), EPSA (Ing Carlos Andrés Becerra e Jaime Sánchez) y EMCALI (Ing Omar Arango e Ing Gerardo Rojas). Se discutieron además temas relacionados con Ciberseguridad e Interoperación para RI.

Otra de las empresas indicó que la interoperabilidad es un tema crítico para el sector eléctrico y el país, por lo que una vez se defina un modelo a nivel nacional, se espera que se le brinden indicaciones al sector sobre las normas que deben aplicarse para el desarrollo de las RI. También mencionó que a nivel de ingeniería se han enfrentado con el problema de haber adquirido tecnología propietaria que en el mediano y largo plazo les hace perder flexibilidad en nuevas compras y les dificulta cambiar de dirección. Entonces, si bien cuentan con interoperabilidad interna, el dilema es cómo podrían conectarse con otras empresas.

Otra empresa indicó que están trabajando en un RFI (*Request for Information*) de tipificación de tecnologías de *Smart Grid* dado que hay proveedores con soluciones propietarias que no son interoperables. Es por eso que las normas de CEN CENELEC ETSI, en particular las de Interoperabilidad (es decir la SG-CG/M490/I (CEN-CENELEC-ETSI, 2014)) son cada vez más importantes dado que se está dando una alta convergencia de tecnologías donde los marcos conceptuales deben salirse de lo estrictamente eléctrico y cada vez las empresas se acercan más al cliente. Consideran además que se necesitan arquitecturas más desacopladas de las soluciones, que los haga menos dependientes de soluciones tecnológicas particulares.

Como parte de este trabajo se identificó un caso donde el sector eléctrico ha realizado esfuerzos de estandarización para garantizar la interoperabilidad en relación con redes inteligentes y es la adopción de una norma técnica Colombiana para Sistemas de Infraestructura de Medición Avanazada (AMI) en redes de distribución de Energía Eléctrica NTC 6079 de 2014 (Icontec, 2014), la cual fue descrita en la sección 0. Durante la conversación, se preguntó cómo ha sido la experiencia con la adopción de la Norma.

Una de las empresas indicó que están familiarizados con el documento, participaron en el ejercicio para definir la Norma, lo consideran un buen ejemplo de visión de estandarización y una experiencia positiva para el sector. Opinan que la solución a los temas de interoperabilidad es por esa vía y mediante la adopción de soluciones abiertas que cumplan estándares bien sea americanos o europeos. Sin embargo ven que uno de los grandes retos es la certificación del cumplimiento de la Norma. Al respecto entienden que existe un equipo conformado por varias empresas trabajando en la definición de este aspecto y recomiendan, para agilizar la certificación, que se adopte la figura de autocertificación por parte de los proveedores de sistemas AMI, considerando la norma AMI existente y/o la normativa adoptada. Entonces, de acuerdo a las necesidades, procesos de auditoría por parte de autoridades nacionales deberían ser permitidos para verificar el cumplimiento de la Norma técnica. También mencionaron otro aspecto y es que la NTC 6079 en su opinión, no hace referencias importantes a temas relacionadas con seguridad de la información o ciberseguridad.

Otra empresa indicó que se logró mucho con la estandarización de los AMI. Se pasó de protocolos propietarios a otros más abiertos. Sin embargo consideró que faltó ir más allá a nivel de interoperabilidad en partiular en los temas de telecomunicaciones y ciberseguridad.

Finalmente otra empresa coincidió en que se trata de un esfuerzo positivo e indicó que la Norma define bien el qué pero no el cómo, siendo bastante amplia dado que abarca la caja, los medidores, las comunicaciones y la seguridad. Indicó que están trabajando en la validación del tipo de pruebas para los requisitos definidos en la Norma. También coincidió en que falta profundización en el tema de seguridad. Indicó que la norma es nueva y cada empresa tendrá que ver cómo la adopta dado que hay proveedores a los que les conviene la estandarización pero a otros no. El espíritu de la norma es hacer un trabajo que le permita a las empresas tener una herramienta abierta.

Por otra parte, en reunión realizada con la Dirección de Estándares y Arquitectura del MinTIC[30], se conversó sobre temas generales de interoperabilidad y su posible aplicación específica para RI. Se resaltó que entre las funciones establecidas en el Decreto 2618 de 2012 (MinTIC, 2012) para dicha Dirección del

[30] Reunión relaizada el 23 de septiembre de 2015, con participación del Director Ing. Jorge Bejarano y la Ing. Angela Cortés.

MinTIC, hay varias relacionadas con liderar la definición de estándares y estructura tecnológica necesaria para el manejo de entornos de información compartida que garanticen la interoperabilidad, pero específicamente entre los sistemas de Tecnologías de la Información asociados con las plataformas tecnológicas del Estado. Por tanto, es en tal sentido que han estado orientados los esfuerzos de la Dirección, por ejemplo en lo referente a la gestión de arquitectura de TI en las instituciones del estado.

De la conversación se deduce que si bien el MINTIC no tiene en estos momentos entre sus planes de acción temas relacionados con la interoperabilidad de RI en el sector eléctrico, desde el punto de vista de funciones y competencias es posible que conforme las necesidades lo vayan demandando, el MINTIC pudiera participar acompañando procesos como estos, siempre y cuando sean compatibles con las prioridades del plan sectorial (Plan Vive Digital) que han sido plasmadas en la Resolución 828 de 2015 (MinTIC, 2015).

Identificación de barreras y oportunidades de mejora relacionadas con interoperabilidad en Colombia

Desde una perspectiva de la legislación y la regulación de telecomunicaciones en Colombia surgen tres elementos muy relevantes en esta discusión:

1) Existe un principio de neutralidad tecnológica aplicable al sector TIC, que le garantiza a las empresas la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia
   a) Pero en su aplicación se debe preservar tanto la interoperabilidad de plataformas como el interfuncionamiento de redes.
2) Sin embargo, interoperabilidad e interfuncionamiento son conceptos aplicables en una interconexión de redes de telecomunicaciones que son diferentes entre sí o en una relación de acceso a una red de telecomunicaciones de un PRST.
3) En tal sentido, la tradición observada en el sector de telecomunicaciones en Colombia es que se establecen regulaciones técnicas sobre las redes únicamente para:
   a) Garantizar la interconexión entre redes distintas (por ejemplo mediante la definición de protocolos de interconexión, características de transmisión o determinación de códecs) (CRC, 2011), o
   b) Asegurar la calidad del servicio y la seguridad de las redes.

Por otra parte, como se presentó en las secciones previas, se identifican un conjunto de fortalezas en el tema de interoperabilidad en Colombia con aplicaciones a Redes Inteligentes:

1) Hay una recomendación para usar como referencia en Colombia, para el análisis del conjunto de funcionalidades previstas, el modelo CEN-CENELEC-ETSI *Smart Grid Architecture Module* (SGAM) del *Smart Grid Coordination Group*.
2) Se definió una Norma Técnica Colombiana que establece los requisitos para Sistemas de Infraestructura de Medición Avanzada (AMI) en redes de distribución de Energía Eléctrica.

Pero de igual manera, se identifican las siguientes oportunidades de mejora:

1) No existe un marco de interoperabilidad de redes inteligentes formalmente adoptado para Colombia. Al respecto existe consenso entre los actores del sector que fueron consultados (ver sección 0) así como en los documentos CEN-CENELEC-ETSI analizados (Ver documento SG-CG/M490/I (CEN-CENELEC-ETSI, 2014) y la Sección 2) sobre la importancia de la interoperabilidad de una red inteligente y la necesidad de que las funcionalidades e interfaces de sus componentes se especifiquen de antemano.
   a) La Recomendación de los Consultores de la Componente I es usar como referencia en Colombia, para el análisis del conjunto de funcionalidades previstas, el modelo CEN-CENELEC-ETSI *Smart Grid Architecture Module* (SGAM) del *Smart Grid Coordination Group*

b) El marco que se adopte debe permitir recopilar los requisitos de interoperabilidad mediante la identificación de casos de uso en cada una de sus fases (generación, transporte, distribución, almacenamiento y consumo) y asegurar que la validación de la interoperabilidad de los sistemas se realice a través de pruebas.
c) El marco también debe ser flexible para que las empresas de energía, aún actuando dentro de una conceptualización de arquitectura común para el país, cuenten con garantías de neutralidad tecnológica al interior de sus propias redes, que les permitan la diferenciación de sus competidores y el mantenimiento de una red de proveedores tecnológicos diversa.

2) Debe evaluarse la conveniencia de uso de Normas Internacionales o eventualmente de Normas Técnicas Nacionales que sean producto de un proceso con amplia participación de la industria, para que los elementos o las interfaces que puedan afectar la interoperabilidad entre distintas empresas de energía cuenten con una especificación común.
   a) Esto debe darse como un proceso por pasos, de acuerdo con el mapa de ruta que se defina para la red inteligente en Colombia.

El caso de Brasil analizado en la sección 0. es indicativo que los esfuerzos iniciales de estandarización Brasileños aplicables a RI se han concentrado en la especificación de medidores electrónicos de energía eléctrica (Norma ABNT NBR 14519 (ABNT, 2011) y en los procedimientos de acreditación de los medidores (Norma ABNT NBR 14521 (ABNT, 2011)).

7.5 Ciberseguridad en Colombia

Lineamientos de política para Ciberseguridad y Ciberdefensa

En el 2011 se publicó el documento CONPES 3701 (Consejo Nacional de Política Económica y Social) que estableció los lineamientos de política para Ciberseguridad y Ciberdefensa en Colombia (Conpes, 2011).

En cuanto a Ciberseguridad, el documento la define como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

En esencia, el Gobierno Nacional indicó que necesitaba conocer y actuar de una forma integral frente a las amenazas informáticas y contar con una estrategia que incluya la creación de instancias adecuadas que permitan ejercer una labor de ciberseguridad y ciberdefensa frente a cualquier amenaza o incidente informático que pueda comprometer información, afectar la infraestructura crítica del país y poner en riesgo la seguridad y defensa del Estado.

El Plan definió un objetivo central: Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio; y tres objetivos específicos: 1) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional; 2) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa; y 3) Fortalecer el cuerpo normativo y de cumplimiento en la materia.

El diagnóstico realizado por el documento CONPES 3701 encontró en su momento debilidad en regulación y legislación de la protección de la información y de los datos.
El CONPES 3701 recomendó que el Gobierno Nacional implementara las siguientes instancias: Una Comisión Intersectorial encargada de fijar la visión estratégica, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT que es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa, el Comando Conjunto Cibernético de las Fuerzas Militares – CCOC y el Centro Cibernético Policial - CCP. (ver

Figura 8).
El mismo CONPES 3701 propuesto que el ColCERT debía trabajar con base en el modelo relacional que se muestra en la Figura 9. Entre sus objetivos específicos se encuentran (i) promover el desarrollo de capacidades locales/sectoriales así como la creación de CSIRTs (*Computer Security Incident Response Team*) sectoriales para la gestión operativa de los incidentes de ciberseguridad en la infraestructura crítica nacional, el sector privado y la sociedad civil, (ii) coordinar y asesorar a CSIRTs y entidades tanto del nivel público, privado y de la sociedad civil en la respuesta a incidentes informáticos y (iii) ofrecer servicios de prevención ante amenazas informáticas y respuesta frente a incidentes informáticos.

Figura 8. Modelo de coordinación de ciberdefensa y ciberseguridad.

Fuente: Gráfica No 5 del documento CONPES 3701 (Conpes, 2011) que a su vez referencia al Ministerio de Defensa Nacional.

Por su parte el Comando Conjunto Cibernético de las Fuerzas Militares (CCOC) en cabeza del Comando General de las Fuerzas Militares, incluye entre sus funciones defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país.

En cuanto al Centro Cibernético Policial (CCP) sus funciones incluyen apoyar e investigar en coordinación con el ColCERT las vulnerabilidades, amenazas e incidentes informáticos que afecten la seguridad de la infraestructura informática crítica de la Nación.

Figura 9. Modelo relacional del ColCERT

Fuente: Gráfica No 6 del documento CONPES 3701 (Conpes, 2011) que a su vez referencia al Ministerio de Defensa Nacional.

El CONPES vigente tiene acciones programadas hasta el 2015, de manera que se está planeando un nuevo CONPES por parte de los ministerios de Defensa, Justicia y Tecnologías de la Información y las Comunicaciones[31].

En reunión realizada con la Dirección de Estándares y Arquitectura del MinTIC[32], se conversó respecto a los avances del nuevo CONPES el cual cuenta con la asesoría de expertos nacionales e internacionales incluyendo participantes del G20, OECD, Interpol y el Foro Económico Mundial.

Es de indicar que entre las funciones establecidas en el Decreto 2618 de 2012 (MinTIC, 2012) para dicha Dirección del MinTIC , se encuentra la de coordinar el diseño y la implementación de una gestión de riesgos asociada a la seguridad y privacidad de la información bajo las pautas de las entidades dedicadas a ciberseguridad y ciberdefensa en el país.

Los diagnósticos realizados para la elaboración del nuevo CONPES muestran que Colombia ha tenido avances desde la expedición del CONPES 3701 aunque no se había cuantificado apropiadamente el impacto de las acciones emprendidas. En cuanto al modelo de coordinación de ciberdefensa y ciberseguridad propuesto por el CONPES existente se han evidenciado fortalezas en el CCP, un estado de avance intermedio en el CCOC y oportunidades de mejora en el ColCERT a nivel de capacidad organizativa

[31] Ver: http://www.mintic.gov.co/portal/604/w3-article-11349.html
Consulta realizada el 16 de Septiembre de 2015.

[32] Reunión relaizada el 23 de septiembre de 2015, con participación del Director Ing. Jorge Bejarano y la Ing. Ángela Cortés.

y técnica. En cuanto a protección de infraestructuras críticas el avance no es tan rápido como se esperaba, aunque hay sectores como el financiero con desarrollos importantes.

El CONPES en elaboración incluiría entre sus líneas estratégicas, aspectos de gobernanza, fortalecimiento de capacidades de ciberseguridad y ciberdefensa, fortalecimiento del marco legal y regulatorio, aspectos de cultura de ciberseguridad y ciberdefensa, infraestructuras críticas cibernéticas y cooperación y diplomacia en el ciberespacio (MinTIC, 2015).

En relación a la gobernanza el nuevo CONPES incluiría acciones relacionadas con (i) el liderazgo del gobierno, (ii) los mecanismos de coordinación entre instituciones y (iii) los mecanismos de articulación y participación permanente entre todos los actores.

En los aspectos de infraestructuras críticas cibernéticas, se incluirían acciones relacionadas con la (i) estructura organizacional para la gestión, (ii) modelo de gestión de riesgos nacional, (iii) fortalecer protección y defensa y (iv) estrategias para gestión de incidentes y crisis.

En cuanto al fortalecimiento del marco legal y regulatorio se contemplarían acciones relacionadas con el (i) fortalecimiento del marco legal, (ii) análisis y armonización normativa y (iii) revisión y adopción de lineamientos para aplicación de aspectos de derecho internacional humanitario y derechos humanos en el ciberespacio.

Es de particular interés que el nuevo CONPES incluiría entre otros, un sustento normativo para la creación de los CSIRT sectoriales, aspecto que se ha identificado que no puede ser de carácter voluntario para las empresas y sectores con ciberactivos críticos.

Legislación relacionada con ciber-criminalidad

En el año 2009 la Ley 1273 (Congreso de Colombia, 2009) modificó el Código Penal Colombiano adicionando un nuevo título VII BIS denominado "De la Protección de la información y de los datos" mediante el cual se definieron en primer lugar los siguientes atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos:

1. Acceso abusivo a un sistema informático.
2. Obstaculización ilegítima de sistema informático o red de telecomunicación
3. Interceptación de datos informáticos.
4. Daño Informático
5. Uso de software malicioso.
6. Violación de datos personales.
7. Suplantación de sitios web para capturar datos personales.

Y en segundo lugar los siguientes atentados informáticos y otras infracciones:

1. Hurto por medios informáticos y semejantes
2. Transferencia no consentida de activos

Regulación desde la perspectiva de las comunicaciones en relación con la seguridad de las redes de los PRST.

Desde la perspectiva de las comunicaciones se han identificado dos marcos regulatorios relevantes para este análisis. El primero se deriva del Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones y el segundo está asociado con los Indicadores de Calidad de los Servicios de Telecomunicaciones. A continuación se presentan los puntos más relevantes de ambos marcos.

Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones

En el 2011 la Comisión de Regulación de Comunicaciones (CRC) expidió el Régimen Integral de Protección de los Derechos de los usuarios de los Servicios de Comunicaciones mediante la Resolución CRC 3066 (CRC, 2011), el cual aplica a las relaciones surgidas entre los proveedores de servicios de comunicaciones (PSC), de que trata la Ley 1341 de 2009 (Congreso de la República, 2009) y los usuarios, a partir del ofrecimiento y durante la celebración y ejecución del contrato de prestación de servicios de comunicaciones.

Un PSC está definido por la misma Resolución CRC 3066 (CRC, 2011) como: "La persona jurídica pública, mixta o privada, que de acuerdo con la Ley 1341 de 2009 se encuentra habilitada para prestar servicios de comunicaciones a terceros y es responsable de dicha prestación." Es decir, que las obligaciones contenidas en la Resolución aplican a personas jurídicas que se hayan habilitado y estén inscritos en el Registro TIC de conformidad con el Decreto 4948 de 2009 del MinTIC (MinTIC, 2009), los artíuclos 10 y 15 de la Ley 1341 de 2009 (Congreso de la República, 2009) y sean responsables de dicha prestación.

A su vez la Resolución CRC 3066 (CRC, 2011) define los servicios de comunicaciones como: "(...) los servicios de que trata la Ley 1341 de 2009, los cuales proporcionan la capacidad de envío y/o recibo de información, de acuerdo con las condiciones para la prestación de tales servicios, previamente pactadas entre un proveedor y un usuario."

En la Resolución CRC 3066 (CRC, 2011) se indica que los proveedores de servicios de comunicaciones deben asegurar el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y la prestación de los servicios de seguridad de la información (autenticación, autorización y no repudio), requeridos para garantizar la inviolabilidad de las comunicaciones, de la información que se curse a través de ellas y de los datos personales del usuario en lo referente a la red y servicios suministrados por dichos proveedores.

Se dice además que el secreto de las comunicaciones aplica a voz, datos, sonidos o imágenes y a la divulgación o utilización no autorizada de la existencia o contenido de las mismas y que salvo orden de autoridad judicial competente, los PSC, siempre y cuando sea técnicamente factible, no pueden permitir, por acción u omisión, la interceptación, violación o repudio de las comunicaciones que cursen por sus redes. Para efectos de lo anterior, los PSC deben implementar procesos formales de tratamiento de incidentes de seguridad de la información.

Indicadores de calidad de servicios de telecomunicaciones

En el 2011 la CRC expidió la Resolución CRC 3067 de 2011 (CRC, 2011), por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones, modificada posteriormente por la Resolución CRC 4734 de 2015 (CRC, 2015).

Como preámbulo, es de anotar que la Resolución 202 de 2010 del MinTIC (MinTIC, 2010) define a los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) como: "Persona jurídica responsable de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros. En consecuencia todos aquellos proveedores habilitados bajo regimenes legales previos se consideran cobijados por la presente definición". A su vez, la misma Resolución define los Servicios de Telecomunicaciones como los "Servicios ofrecidos por los proveedores de redes y servicios para satisfacer una necesidad específica de telecomunicaciones de los usuarios" y define una Telecomunicación como "Toda emisión, transmisión y recepción de signos, señales, escritos, imágenes, sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos".

Las obligaciones contenidas en la Resolución CRC 3067 de 2011 (CRC, 2011) modificada posteriormente por la Resolución CRC 4734 de 2015 (CRC, 2015), aplican a personas jurídicas que se hayan habilitado y estén inscritos en el Registro TIC de conformidad con el Decreto 4948 de 2009 del MinTIC (MinTIC, 2009) y los artículos 10 y 15 de la Ley 1341 de 2009 (Congreso de la República, 2009).

Como parte de este marco regulatorio por el cual se definen los indicadores de calidad para los servicios de telecomunicaciones se indicó que PRST que ofrezcan acceso a Internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo. Para tal efecto, deben informar en su página Web sobre las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtros antivirus y la prevención de *spam*, *phishing*, malware entre otras. La responsabilidad a cargo de los PRST que ofrezcan acceso a Internet no cubre los equipos del cliente, dado que los mismos son controlados directamente por el usuario del servicio. En cuanto a los proveedores de contenidos o de cualquier tipo de aplicación la regulación indica que estos deberán tomar las respectivas medidas de seguridad de conformidad con lo que para el efecto disponga la normatividad que les sea aplicable.

Además de las medidas de seguridad antes descritas, PRST que ofrezcan acceso a Internet deben implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT en lo relativo a las recomendaciones pertenecientes a las series X.800 dictadas por este organismo, al menos en relación con los siguientes aspectos, y en lo que aplique para cada entidad que interviene en la comunicación:

1) Autenticación: Verificación de identidad tanto de usuarios, dispositivos, servicios y aplicaciones. La información utilizada para la identificación, la autenticación y la autorización debe estar protegida (Recomendaciones UIT X.805 y UIT X.811).
2) Acceso: Prevenir la utilización no autorizada de un recurso. El control de acceso debe garantizar que sólo los usuarios o los dispositivos autorizados puedan acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones (Recomendaciones UIT X.805 y UIT X.812).
3) Servicio de No repudio: Es aquél que tiene como objeto recolectar, mantener, poner a disposición y validar evidencia irrefutable sobre la identidad de los remitentes y destinatarios de transferencias de datos. (Recomendaciones UIT X.805 y X.813).
4) Principio de Confidencialidad de datos: Proteger y garantizar que la información no se divulgará ni se pondrá a disposición de individuos, entidades o procesos no autorizados (Recomendaciones UIT X.805 y X.814).
5) Principio de Integridad de datos: Garantizar la exactitud y la veracidad de los datos, protegiendo los datos contra acciones no autorizadas de modificación, supresión, creación o reactuación, y señalar o informar estas acciones no autorizadas (Recomendaciones X.805 y X.815).
6) Principio de Disponibilidad: Garantizar que las circunstancias de la red no impidan el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones (Recomendación X.805).
7) Por último los PRST a través de redes móviles, además de las soluciones de seguridad antes descritas, deberán implementar modelos de seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación, utilizando modelos de cifrados, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122.

Acuerdos sobre Ciberseguridad del Consejo Nacional de Operación para redes eléctricas

El Consejo Nacional de Operación fue creado mediante el artículo 172 de la Ley 142 de 1994 (Congreso - Ley 142, 1994) y el artículo 36 de la Ley 143 de 1994 (Congreso de Colombia, 1994) con la función principal de acordar los aspectos técnicos para garantizar que la operación integrada del sistema interconectado nacional sea segura, confiable y económica y ser el organo ejecutor del reglamento de operación, con sujeción a los principios generales de la Ley 142 de 1994 (Congreso - Ley 142, 1994) y a la preservación de las condiciones de competencia. Sus decisiones pueden ser recurridas ante la CREG.

Es importante mencionar lo siguiente en relación con los Acuerdos que expida el CNO:

Según el artículo 28 de la Ley 143 de 1994 (Congreso de Colombia, 1994) las empresas que sean propietarias de líneas, subestaciones y equipos señalados como elementos de la red nacional de interconexión, deben operarlos con sujeción al Reglamento de Operación y a los acuerdos adoptados por el Consejo Nacional de Operación, punto que también es abordado por el artículo 168 de la Ley 142 de 1994 (Congreso - Ley 142, 1994).

El artículo 29 de la la Ley 143 de 1994 (Congreso de Colombia, 1994) indica que la conexión a la red nacional de interconexión de una red regional de transmisión, de una red de distribución, de una central de generación o de un usuario impone a los interesados las obligaciones de cumplir las normas técnicas que dicte el Ministerio de Minas y Energía y operar su propio sistema con sujeción a las normas que expida la CREG y el CNO.

De igual forma el artículo 34 de la Ley 143 de 1994 (Congreso de Colombia, 1994) indica que el Centro Nacional de Despacho debe ceñirse a lo establecido en el Reglamento de Operación y en los acuerdos del Consejo Nacional de Operación.

En cuanto al tratamiento para los que no cumplan los Acuerdos del CNO, el artículo 28 de la Ley 143 de 1994 (Congreso de Colombia, 1994) indica que esto da lugar a las sanciones que establezca la autoridad competente. En este caso, la CREG estaría habilitada de conformidad con el numeral 73.18 de la Ley 142 de 1994 p (Congreso - Ley 142, 1994) para pedir al superintendente que adelante las investigaciones e imponga las sanciones de su competencia, cuando tenga indicios de que alguna persona ha violado las normas de la Ley 142 de 1994, en este caso particular el artículo 168 de la misma.

Es de anotar que el Decreto 2023 de 1999 (Ministerio de Minas y Energía, 1999) había modificado algunas funciones del CNO dándole una categoría más de cuerpo consultivo. Sin embargo, dicho Decreto fue derogado por el Decreto 1274 de 2001 (Ministerio de Minas y energía, 2001) que restableció las funciones previstas en los artículos 168, 169 y 172 de la Ley 142 de 1994 (Congreso - Ley 142, 1994) y los artículos 28, 29 literal b), 34 y 36 de la Ley 143 de 1994 (Congreso de Colombia, 1994).

Habiendo realizado las consideraciones anteriores, se identificó un Acuerdo expedido por el CNO el cual contiene una Guía de Ciberseguridad de Activos Críticos.

Adicionalmente se identificó un Acuerdo expedido por el CNO, en relación con las condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el Administrador del Sistema de Intercambios Comerciales (ASIC).

Ambos acuerdos se describen a continuación.

Guía de Ciberseguridad

En septiembre de 2015, el CNO mediante el Acuerdo 788 (CNO, 2015) expidió una Guía de Ciberseguridad para el sector eléctrico. Dicha guía surgió luego que el Comité Tecnológico del Consejo Nacional de Operación realizara un estudio de las normas aplicables a la industria eléctrica para mitigar los riesgos de

ciberseguridad en el sector y en el Sistema Interconectado Nacional (SIN) y concluyera que la mejor referencia de aplicación, es la Norma NERC CIP para tecnologías de activos críticos. La Guía surgió después de un trabajo de casi 4 años.

El Acuerdo establece que los agentes generadores, transmisores y distribuidores del Sistema Interconectado Nacional deben designar una persona responsable de dirigir y administrar la implementación de la Guía de Ciberseguridad, en un plazo máximo de (6) seis meses el cual se cumplirá a comienzos de febrero de 2016.

Adicionalmente el operador del Sistema y los agentes generadores, transmisores y distribuidores del SIN, deben realizar la identificación de los activos críticos y ciber activos críticos, los riesgos y vulnerabilidades y el nivel de gestión de ciberseguridad en la operación de sus empresas en un plazo máximo de (1) un año, que se cumplirá a comienzos de septiembre de 2016.

La Guía reconoce que los riesgos asociados a la seguridad de la operación deben ser cubiertos mediante la estructuración de lineamientos y procedimientos que conlleven a las empresas del sector eléctrico colombiano a la aplicación de requerimientos mínimos de ciberseguridad, reduciendo riesgos de ciber terrorismo y guerra electrónica debido a que este sector es estratégico y crítico para la seguridad y estabilidad nacional e indica que es necesario una actualización continua de las normas de ciberseguridad de acuerdo con los cambios tecnológicos que impacten el sector eléctrico colombiano.

La Guía de Ciberseguridad adoptada por el CNO se basa en las normas NERC CIP-002 a la NERC CIP-009, las cuales se relacionan a continuación:

- CIP-002: Definición de ciber activos críticos (NERC, 2012).
- CIP-003: Controles en la gestión de seguridad e información (NERC, 2012).
- CIP-004: Personal y entrenamiento (NERC, 2012).
- CIP-005: Perímetros de seguridad electrónica (NERC, 2012).
- CIP-006: Seguridad física (NERC, 2012).
- CIP-007: Gestión del sistema de seguridad (NERC, 2012).
- CIP-008: Reporte de incidentes y planes de respuestas (NERC, 2012).
- CIP-009: Planes de recuperación para ciber activos críticos (NERC, 2012).

La Guía desarrolla cuatro aspectos clave:

1. **Identificación de activos críticos.** Incluye criterios de identificación de activos críticos y ciber activos críticos. Estos últimos pueden usar protocolos enrutable para comunicarse afuera del perímetro de seguridad electrónica, o con un centro de control, o ser accesibles por marcación
2. **Gestión de ciberseguridad de los activos críticos.** Incluye el establecimiento de una política de Ciberseguridad, el control de acceso a la información, el control de acceso electrónico, el control de cambios y gestión de configuraciones, la prevención de software malicioso, la administración de cuentas y el plan de respuesta de incidentes de ciberseguridad, así como evaluaciones bianuales de ciberseguridad.
3. **Seguridad física de ciberactivos críticos.** Incluye el establecimiento de plan de seguridad física; de control, monitoreo y registro de acceso físico; y de mantenimientos y pruebas
4. **Plan de recuperación de ciberactivos críticos.** Incluye el establecimiento de planes de recuperación, la realización de simulacros, el manejo de control de cambios, el establecimiento de los procesos y procedimientos para el respaldo y almacenamiento de la información necesaria para la recuperación efectiva de los ciber activos críticos y las pruebas a los medios de respaldo.

Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas

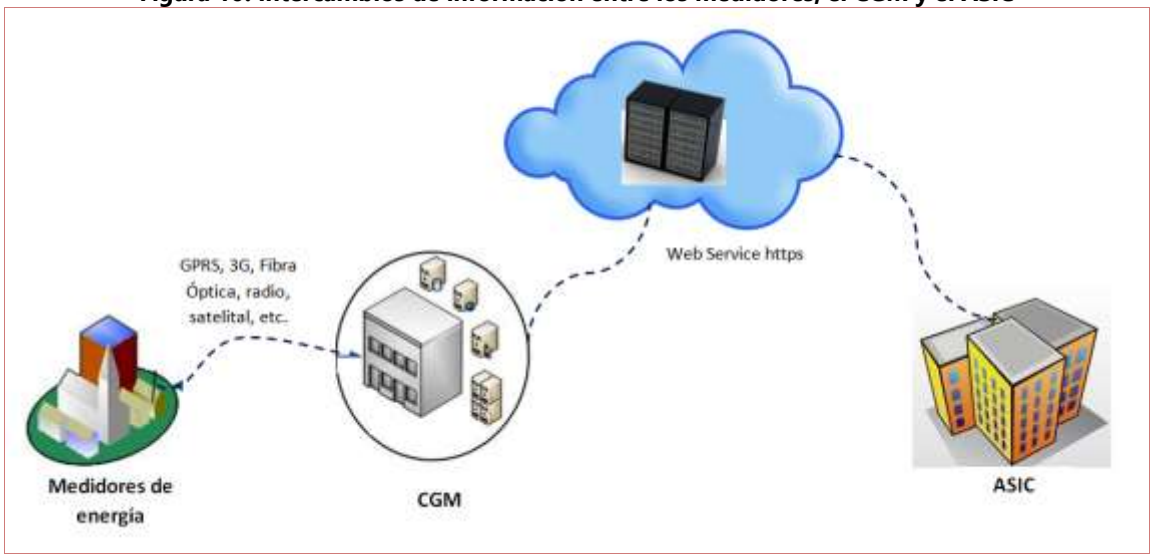
En el 2014 el CNO expidió el Acuerdo 701 (CNO, 2014) en relación a las condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC. Este Acuerdo surgió en respuesta a lo requerido por la Resolución CREG 038 de 2014 (CREG, 2014) (ver sección 0).

El CNO estableció un conjunto de funcionalidades mínimas para el intercambio de datos o capa de comunicaciones entre un nodo donde se conecta el medidor de energía y otro nodo donde está el concentrador de datos del Centro de Gestión de Medidas (CGM), debe contar con mecanismos de cifrado; tales como VPN, IPSEC, cifrado por firewall, QoS o aquellos que los sustituya o mejoren, o mecanismos de protección de datos. En los casos en que el medidor tenga embebida la tarjeta de comunicaciones con la funcionalidad de encriptación se considera esta como el nodo y aplica la definición.

Indicó además que el intercambio de datos entre el CGM y el ASIC deberá realizarse a través de redes privadas virtuales autenticadas en doble vía con el uso de certificados digitales y que el cumplimiento de las medidas de seguridad mínimas deberá verificarse por lo menos 2 veces al año por medio de auditorías internas.

Además se establecieron niveles mínimos de seguridad para las etapas de la transmisión de la información, desde los medidores hacia el CGM y entre el CGM y el ASIC; así como para el acceso a la base de datos desde el CGM (ver Figura 10).

Figura 10. Intercambios de información entre los medidores, el CGM y el ASIC



Fuente: Anexo al Acuerdo 701 del CNO (CNO, 2014)

Adopción de Normas ICONTEC

Seguridad de la información.

De conformidad con el Decreto 2269 de 1993 (Presidencia de la República, 1993) el Instituto Colombiano de Normas Técnicas (ICONTEC) es el organismo nacional de normalización, es decir, la entidad reconocida por el Gobierno Nacional cuya función principal es la elaboración, adopción y publicación de las normas técnicas nacionales y la adopción como tales de las normas elaboradas por otros entes.

Entre las funciones del ICONTEC se encuentran las siguientes que son relevantes para este análisis: (i) estudiar, aprobar y adoptar las normas técnicas colombianas, ya sean elaboradas totalmente por él o

preparadas por las unidades sectoriales de normalización; (ii) evaluar y comparar el grado de desarrollo de las normas técnicas colombianas frente a los estándares internacionales y su aplicación y (iii) asesorar técnicamente al Consejo Nacional de Normas y Calidades y a las entidades que tengan a su cargo la adopción de reglamentos técnicos y normas obligatorias y (iv) Asesorar al Gobierno en todo lo concerniente a la normalización técnica y en la definición de las políticas oficiales sobre el uso de las normas;

En relación a seguridad de la información el ICONTEC aprobó la NTC-ISO-IEC 27001 (Icontec, 2013) mediante la cual se establecen requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información, la cual es una adopción de la norma ISO-IEC-27001. También aprobó la NTC-ISO/IEC 27002 (Icontec, 2007) que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización

El sector eléctrico colombiano y la ciberseguridad

Se discutió el tema de Ciberseguridad con varias empresas del sector Eléctrico: CODENSA, EMCALI y EPSA[33] y se obtuvo un conjunto de respuestas de CODENSA a un cuestionario sobre el tema enviado a dichas empresas.

Varias de las empresas del sector eléctrico cuentan con programas y acciones específicas en el tema de Ciberseguridad y algunas de ellas están trabajando activamente en el tema desde el año 2010. Incluso una de las empresas realizó implementaciones de Ciberseguridad en centros de control desde el año 2014.

En cuanto a la implementación del Acuerdo 788 del CNO, todas las empresas entrevistadas indicaron que estaban trabajando en el mismo, si bien se evidencian distintos grados de avance. Una de las empresas cuenta con la experiencia internacional de su casa matriz y cuenta con una iniciativa interna que considera los siguientes aspectos:

- *Cyber Security Assessment*
- *Integrated security framework definition*
- *Integrated security framework implementation*

En cuanto a la aplicación de otras normas no contempladas en el Acuerdo 788 del CNO, algunas de las empresas consultadas coincidieron en que se aplican normas tales como ISO 27001. Una de las empresas reportó la adopción de un conjunto completo de estándares para Ciberseguridad, que se incluye en la

[33] Con el propósito de establecer los tipos de relaciones, interacción y coordinación entre los actores del sector eléctrico y del sector de las telecomunicaciones y en concreto con el desarrollo de las Redes Inteligentes (RI) se realizó una teleconferencia el 22 de septiembre de 2015 en la cual participaron las empresas CODENSA (Ing Cesar Rincon e Ing Hector A Diaz), EPSA (Ing Carlos Andrés Becerra e Jaime Sánchez) y EMCALI (Ing Omar Arango e Ing Gerardo Rojas). Se discutieron además temas relacionados con Ciberseguridad e Interoperación para RI.

Tabla 13 y considera recomendaciones ISO, NERC, ENISA, NIST, ISA e IEC.

Tabla 13. Normas relacionadas con Ciberseguridad utilizadas por una de las empresas del sector eléctrico en Colombia

Conjunto de normas adoptadas	Descripción y ámbito de aplicación
Normas ISO	ISO/IEC 27001 – Information Technology – Security Techniques - Code of practice for information security management (ISO, 2007) ISO/IEC 27019 – Information Technology – Security Techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry (ISO/IEC, 2013).
Normas NERC (North American Electric Reliability Corporation)	NERC CIP 002-4, January 2011, Cyber Security-Critical Cyber Asset Identification (NERC, 2011). NERC CIP003-4, January 2011, Cyber Security-Security Management Controls (NERC, 2011). NERC CIP004-4, January 2011, Cyber Security-Personnel & Training (NERC, 2011). NERC CIP006-4c, January 2011, Cyber Security-Physical Security of Critical Cyber Assets (NERC, 2011). NERC CIP007-4, January 2011, Cyber Security-Systems Security Management (NERC, 2011). NERC CIP008-4, January 2011, Cyber Security-Incident Reporting and Response Planning (NERC, 2011). NERC CIP009-4, January 2011, Cyber Security-Recovery Plans for Critical Cyber Assets (NERC, 2011).
Normas ENISA (Smart Grid Security)	ENISA European Network and Information Security Agency - Protecting Industrial Control.
Otras?	NIST 800-82, June 2011, – Guide to Industrial Control Systems Security (NIST, 2011). NIST SP 800-53, August 2009 (Actualización: Abril 2013), – Recommended security controls for information systems (NIST, 2013). ISA 99.00.01, October 2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models (ANSI/ISA, 2007). ISA 99.02.01, January 2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program (ANSI/ISA, 2009). ISA 99-03-02 – Security for Industrial Automation and Control Systems (ANSI/ISA, 2009). ISA-TR99.00.01, October 2007, Security Technologies for Industrial Automation and Control Systems (ANSI/ISA, 2009) International Electrotechnical Commission, IEC 62351 Security Standards, Power systems management and associated information exchange - Data and communications security ITU, ITU-T Recommendations (no especificadas)

Fuente: Consultor Julián Gómez (con base en información de Una de las empresas participantes)

Sin embargo, no se identificó ninguna evidencia que el sector eléctrico cuente con un CSIRT de carácter sectorial.

Por otra parte, ninguna de las empresas consultadas indicó que haya detectado ataques informáticos sobre sistemas de control o activos críticos.

Finalmente, a las empresas se les preguntó cómo ha sido la experiencia con la adopción de las modificaciones en el Código de Medida establecido mediante Resolución CREG 038 de 2014, y en

particular: ¿Cómo se gestionan las condiciones de seguridad e integridad para la transmisión de lecturas? relacionado con el Acuerdo CNO 701 de 2014.

Una de las empresas indicó que tienen importantes dudas sobre el alcance e implementación de la Resolución y por otro lado no tienen señales claras del beneficio real de la exigencia vs el recurso invertido y el impacto operativo que tendrá. Expresaron preocupación por el vencimiento del plazo en mayo del 2016 e indicaron que hay un tema de cifrado que no es claro. Están optando por soluciones de mercado y en la parte de integridad de transmisión de datos se realizará bajo los criterios de seguridad corporativos y teniendo en cuenta las normas mencionadas líneas arriba y la exigencia regulatoria

Otra empresa dijo que el gran Pareto de AMI es con una red celular y que basados en la normatividad 3GPP el cifrado se incorpora desde la SIM card. Y luego dentro de la red WAN del Operador celular la información ya está cifrada. Añadió que para colocar VPN o IPSec no existen *firewalls* que manejen 5.000 ó 6.000 sesiones de VPN y que el problema es de volúmenes porque no hay *firewall* que lo soporte.

Otra empresa mencionó que ven la solución de protección y cifrado a nivel de la red WAN, pero que desde el medidor hasta el centro de gestión la norma es incumplible porque el medidor tendría que tener el cifrado. El medidor tiene un puerto que va hacia el modem y ahí lo toma el TELCO. A nivel de WAN sí está validado el tema de integralidad y cifrado. Pero el tramo responsabilidad del medidor al router es un alambrado que es vulnerable con un *sniffer*. Entonces del medidor al sistema de gestión muy difícil cumplir con la norma porque tendrían que cambiar todos los medidores con modems 3G o 4G con cifrado incorporado y esto es algo que la Norma no lo define bien. Controvirtieron que sí pueden tener 6.000 direcciones IP en capa 3 y capa 4, pero no en el medidor que está en capa 2 y no va con direccionamiento IP. En cuanto a los costos mencionaron que implica necesariamente el cambio de medidor o pasar de un módem a un elemento de red en capa 3 y dijeron que el Art. 146 de la Ley 142 (Congreso - Ley 142, 1994) establece que para la medición de los consumos se empleen los instrumentos de medida que la técnica haya hecho disponibles.

Identificación de barreras y oportunidades de mejora relacionadas con ciberseguridad en Colombia

Como se presentó en las secciones previas, se identifican un conjunto de fortalezas en el tema de ciberseguridad en Colombia con aplicaciones a Redes Inteligentes:

1) Desde el año 2009 cuenta con tipificaciones penales relacionadas con cibercriminalidad,
2) Desde el 2011 tiene una política nacional de Ciberseguridad la cual se cuenta en proceso de actualización,
3) Existe regulación específica en Telecomunicaciones que obliga a que los PRST aseguren el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y la prestación de los servicios de seguridad de la información (autenticación, autorización y no repudio), requeridos para garantizar la inviolabilidad de las comunicaciones
4) Existen normas nacionales que adoptan recomendaciones internacionales ISO-IEC relacionadas con la seguridad de la información
5) A nivel del sector eléctrico el CNO viene liderando iniciativas que han culminado con la expedición de acuerdos para:
   a) Definir una Guía de Ciberseguridad de Activos Críticos, así como
   b) Las condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el Administrador del Sistema de Intercambios Comerciales.
6) Adicionalmente las empresas del sector entrevistadas muestran conciencia sobre la importancia del tema, así como la existencia de iniciativas internas para la adopción de estándares de ciberseguridad.

Pero de igual manera, se identifican las siguientes oportunidades de mejora:

1) El ColCERT, establecido por el CONPES 3701, requiere de mayores capacidades organizativas y técnicas, aspecto que ya ha sido identificado por el MinTIC en la elaboración del nuevo CONPES sobre Ciberseguridad. Esto ha generado impactos relevantes para este trabajo:
   a) No hay evidencia de que el sector eléctrico cuente con un CSIRT de carácter sectorial.
   b) Tampoco existe evidencia que se hayan dado pasos para establecer una coordinación efectiva entre el sector eléctrico y las entidades creadas por el CONPES 3701, en particular el ColCERT y el CCOC.
2) El CNO ha dado un importante paso con la adopción de las normas NERC-CIP-002 a la NERC-CIP-009. Sin embargo las recomendaciones de los Consultores de la Componente I de elegir como referencia para el análisis del conjunto de funcionalidades previstas, el modelo CEN-CENELEC-ETSI *Smart Grid Architecture Module* (SGAM) del *Smart Grid Coordination Group* hacen necesaria la conveniencia de estudiar la adopción de un conjunto más amplio de normas incluyendo:
   a) El documento CEN-CENELEC-ETSI SG-GC/M490_H (CEN-CENELEC-ETSI, 2014)[34].
   b) El documento ENISA con recomendaciones para *Smart Grid Security* (ENISA (European Network and Information Security Agency), 2012)[35].
   c) Una adaptación de la iniciativa ENISA sobre certificación de seguridad de las Redes Inteligentes en Europa (ENISA, 2014)[36]
   d) Algunas normas específicas ISO/IEC, IEC, IEEE, IETF, NIST e ISA.
3) Las empresas consultadas dentro del sector eléctrico coincidieron en expresar preocupaciones sobre el alcance y la implementación de la Resolución CREG 038 de 2014 (CREG, 2014) y el Acuerdo 701 del CNO (CNO, 2014).
   a) Más allá del debate técnico y económico específico que plantearon las empresas del sector eléctrico sobre estas regulaciones, se evidencia una dificultad en el sector para tener una comprensión común sobre conceptos nuevos, que no han sido parte de las discusiones tradicionales dentro de la industria eléctrica.

De las conversaciones con el Sector se evidencia que existen distintos niveles de alistamiento frente al tema de Ciberseguridad entre las empresas del sector. Algunas se muestran muy avanzadas, mientras que otras están apenas dando los primeros pasos.

[34] Ver sección 3.1 – Unión Europea

[35] Ídem

[36] Ídem

8. Medidas de política pública y medidas regulatorias recomendadas

8.1 Medidas relacionadas con la protección de la privacidad de los consumidores y las Redes Inteligentes

¿Qué medidas deben adoptarse?

1) Considerando lo establecido por la Ley Estatutaria 1581 de 2012 en relación al tratamiento de datos sensibles de personas naturales, es necesario precisar para las empresas del sector eléctrico qué datos se pueden obtener de los usuarios que son personas naturales y qué tipo de Tratamiento puede hacerse con los mismos, entendiendo como "Tratamiento" cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. También debe establecerse qué tipo de datos deberían ser públicos para preservar la libre competencia.

    a. Sobre el manejo de datos personales, en el sector de telecomunicaciones se han establecido lineamientos de carácter general que pueden constituir una guía de interés para la implementación en el sector de energía eléctrica (ver sección 0).

        i. Para el sector eléctrico posiblemente se requiera un mayor grado de precisión en tecnologías de RI que ya se encuentran bajo implementación, como los medidores AMI.

        ii. Se recomienda considerar que la recolección de datos debe limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos y que solo se podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el Tratamiento.

        iii. Adicionalmente, se recomienda hacer una revisión periódica de la evolución de la implementación de las RI en el país, para garantizar que estas cumplan con las disposiciones de protección de datos.

    b. Adicionalmente se debe definir qué Tratamiento se debe dar a los datos de personas jurídicas.

        i. Sobre este aspecto y considerando las mejores prácticas identificadas en la comparación internacional (Ver Sección 0 y Sección 6), se recomienda que a los usuarios empresariales regulados se les dé el mismo tratamiento que a los usuarios que son personas naturales.

¿Quién debe adoptar las medidas?

Estas medidas podrían ser adoptadas por la CREG, considerando que de acuerdo con el artículo 73.21 de la Ley 142 de 1994 está entre sus funciones la de establecer criterios generales sobre la protección de los derechos de los usuarios en lo relativo a facturación, comercialización y demás asuntos relativos a la relación de la empresa con el usuario.

8.2 Medidas relacionadas con la interoperabilidad de las Redes Inteligentes

¿Qué medidas deben adoptarse?

1) Debe definirse a nivel nacional una arquitectura que permita establecer un marco común de referencia de las RI.
    a. La Recomendación de los Consultores de la Componente I es usar como referencia en Colombia, para el análisis del conjunto de funcionalidades previstas, el modelo CEN-CENELEC-ETSI *Smart Grid Architecture Module* (SGAM) del *Smart Grid Coordination Group*
        i. Esta recomendación debe ser analizada y validada a nivel nacional y en caso de corroborarse su conveniencia, debe adoptarse como marco común de referencia de las RI.
    b. Se recomienda que la decisión que se adopte incluya los siguientes elementos:
        i. Debe ser flexible para que las empresas de energía, aún actuando dentro de una conceptualización de arquitectura común para el país, cuenten con garantías de neutralidad tecnológica al interior de sus propias redes, que les permitan la diferenciación de sus competidores y el mantenimiento de una red de proveedores tecnológicos diversa.
        ii. Debe darse como un proceso por pasos, de acuerdo con el mapa de ruta que se defina para la red inteligente en Colombia.
        iii. Las especificaciones que sean de obligatorio cumplimiento para todas las empresas bien sea mediante la adopción de Normas Internacionales o de Normas Técnicas Nacionales deben resultar como producto de un proceso con amplia participación de la industria y en principio debería considerar únicamente los elementos o las interfaces que puedan afectar la interoperabilidad entre distintas empresas de energía, que son los que pueden necesitar de una especificación común.

¿Quién debe adoptar las medidas?

Respecto a quién debe hacerlo, se revisaron las funciones y facultades de (i) el Ministerio de Minas y Energía con base en el Decreto 381 del 16 de febrero de 2012, el artículo 59 de la Ley 489 de 1998, el artículo 67 de la Ley 142 de 1994 y el Decreto Único Reglamentario Sectorial 1073 del 2015, (ii) la Comisión de Regulación de Energía y Gas, con base en el Artículo 73 y 74 de la Ley 142 de 1994 y en el artículo 23 de la Ley 143 de 1994 y (iii) El Consejo Nacional de Operación con base en los artículos 168, 169 y 172 de la Ley 142 de 1994 y los artículos 28, 29 literal b), 34 y 36 de la Ley 143 de 1994.

El Ministerio de Minas y Energía tiene como objetivo formular, adoptar, dirigir y coordinar las políticas, planes y programas del Sector de Minas y Energía. En particular, de acuerdo con del Decreto 381 de 2012: (i) formular, adoptar, dirigir y coordinar la política en materia de generación, transmisión, distribución y comercialización de energía eléctrica (ii) formular, adoptar, dirigir y coordinar la política en materia de uso racional de energía y el desarrollo de fuentes alternas de energía y promover, organizar y asegurar el desarrollo de los programas de uso racional y eficiente de energía y (iii) expedir los reglamentos técnicos sobre producción, transporte, distribución y comercialización de energía eléctrica y gas combustible, sus usos y aplicaciones.

El Ministerio de Minas y Energía también tiene que Señalar los requisitos técnicos que deben cumplir las obras, equipos y procedimientos que utilicen las empresas de servicios públicos del sector, cuando la comisión respectiva haya resuelto por vía general que ese señalamiento es realmente necesario para garantizar la calidad del servicio, y que no implica restricción indebida a la competencia de acuerdo con el

artículo 67.1 de la Ley 142 de 1994. También debe recoger información sobre las nuevas tecnologías, y sistemas de administración en el sector, y divulgarla entre las empresas de servicios públicos, directamente o en colaboración con otras entidades públicas o privadas según el artículo 67.5 de la misma Ley.

Por tanto el Ministerio sería competente para expedir Reglamentos Técnicos de manera directa o Requisitos Técnicos por solicutd de la CREG cuando sea necesario para garantizar la calidad del servicio.

En cuanto a la CREG, de acuerdo con la Ley 142 de 1994 puede fijar las normas de calidad a las que deben ceñirse las empresas de servicios públicos en la prestación del servicio (artículo 73.4) y definir en qué eventos es necesario que la realización de obras, instalación y operación de equipos de las empresas de servicios públicos se someta a normas técnicas oficiales, para promover la competencia o evitar perjuicios a terceros, y pedirle al ministerio respectivo que las elabore, cuando encuentre que son necesarias (artículo 73.5)

En la misma Ley, el artículo 23 donde se discuten las funciones generales de la CREG indica, entre otras, establecer el Reglamento de Operación para realizar el planeamiento y la coordinación de la operación del Sistema Interconectado Nacional, después de haber oído los conceptos del CNO y establecer pautas para el diseño, normalización y uso eficiente de equipos y aparatos eléctricos.

Por tanto las competencias de la CREG en este aspecto están más asociadas a normas de calidad, que promuevan la competencia o las relacionadas con el planeamiento del SIN.

Respecto del CNO, su función principal de acordar los aspectos técnicos para garantizar que la operación integrada del sistema interconectado nacional sea segura, confiable y económica y ser el órgano ejecutor del reglamento de operación, con sujeción a los principios generales de la Ley 142 de 1994 y a la preservación de las condiciones de competencia. Sus decisiones pueden ser recurridas ante la CREG.

El Decreto 2238 de 2009 (artículo 2.2.3.5.1.1.) indica además que las discusiones y decisiones del Consejo Nacional de operación estarán relacionadas exclusivamente con aspectos técnicos para garantizar que la operación integrada del sistema interconectado nacional sea segura, confiable y económica o sobre aspectos del reglamento de operación

Con base en lo anterior, en mi opinión, la definición del modelo de interoperabilidad, podría darse mediante un Decreto del Ministerio de Minas y Energía o mediante un Acuerdo del CNO. Es decir resulta posible usar una aproximación "*top-down*" o una "*botom-up*". Las dos tienen pros y contras.

En un modelo "*top-down*" la adopción por parte del Ministerio de Minas y Energía surgiría a partir de una decisión de implementación de una política pública que establecería una directriz nacional clara sobre el modelo de arquitectura a implementar en las Redes Inteligentes en Colombia, pero tiene dos inconvenientes importantes: (i) hacer cambios es difícil y (ii) no garantiza una adecuada participación de las empresas del sector en la toma de dichas decisiones.

El modelo "*botom-up*" cuenta entre sus virtudes que la decisión es tomada por un órgano que cuenta con amplia participación de las empresas del sector eléctrico[37], sus miembros son de áreas técnica y operativas[38] por lo que debe esperarse una adecuada experticia técnica en la toma de decisiones, en el

[37] El artículo 37 de la Ley 143 de 1994 establece que: " El Consejo Nacional de Operación estará conformado por un representante de cada una de las empresas de generación, conectadas al sistema interconectado nacional que tenga una capacidad instalada superior al cinco por ciento (5%) del total nacional, por dos representantes de las empresas de generación del orden nacional, departamental y municipal conectadas al sistema interconectado nacional, que tengan una capacidad instalada entre el uno por ciento (1%) y el cinco por ciento (5%) del total nacional, por un representante de las empresas propietarias de la red nacional de interconexión con voto sólo en asuntos relacionados con la interconexión, por un representante de las demás empresas generadoras conectadas al sistema interconectado nacional, por el Director del Centro Nacional de Despacho, quien tendrá voz pero no tendrá voto, y por dos representantes de las empresas distribuidoras que no realicen prioritariamente actividades de generación, siendo por lo menos una de ellas la que tenga el mayor mercado de distribución."

[38] El Decreto 2238 de 2009 establece que: "La representación de las empresas que conforman el Consejo Nacional de Operación se

que tienen voz delegados del gobierno[39] y donde es previsible que sea más fácil gestionar cambios, si se compara con las decisiones tomadas a nivel Ministerial. Pero tiene un inconveniente importante y es que no garantiza la participación del gobierno en la decisión (sus delegados en el CNO tiene voz pero no voto).

Un paso intermedio es que el CNO adopte un conjunto de Acuerdos sobre el tema y de ser necesario, recomiende a la CREG que fije normas de calidad a las que deben ceñirse las empresas de servicios públicos en la prestación del servicio, asociadas a garantizar la interoperabilidad de Redes Inteligentes. Eventualmente, la CREG podría evaluar la necesidade de solicitarle al Ministerio de Minas y Energía la expedición de normas técnicas oficiales sobre interoperabilidad, si es que encontrara que las mismas son necesarias para promover la competencia.
Considerando lo anterior, se recomienda la adopción de un modelo de decisión "*bottom-up*" y que los primeros pasos sobre la definición de una arquitectura de redes inteligentes que garantice la interoperación sea discutida a nivel del CNO y sea confirmada mediante un Acuerdo del mismo.

8.3 Medidas relacionadas con la Ciberseguridad y las Redes Inteligentes

¿Qué medidas deben adoptarse?

1. Debe formalizarse la obligatoriedad para que el sector eléctrico establezca un CSIRT, dentro de plazos específicos, el cual debe además tener las adecuadas coordinaciones con el ColCERT y el CCOC.
    a. En el establecimiento del CSIRT sectorial pueden considerarse los lineamientos dados por ENISA, para la creación de un CSIRT paso a paso (ENISA) o las especificaciones nacionales que sean definidas al respecto.
    b. Además deben indicarse las obligaciones específicas de las empresas del sector eléctrico frente al CSIRT, como parte de una estrategia nacional más amplia que busca dotar de CSIRT a los ciberactivos críticos de la nación.
2. En caso que decida adoptarse como referente de arquitectura a nivel nacional el modelo CEN-CENELEC-ETSI *Smart Grid Architecture Module* (SGAM) del *Smart Grid Coordination Group,* se recomienda analizar dentro de plazos específicos, un conjunto más amplio de normas de ciberseguridad al que menciona el Acuerdo CNO 788 del 2015 incluyendo:
    a. El documento CEN-CENELEC-ETSI SG-GC/M490_H (CEN-CENELEC-ETSI, 2014)
    b. El documento ENISA con recomendaciones para *Smart Grid Security* (ENISA (European Network and Information Security Agency), 2012)

---

hará a través de personas vinculadas al área técnica u operativa de dichas empresas. En las reuniones del Consejo Nacional de Operación no se permitirá la presencia ni la participación de personas vinculadas al área comercial de las empresas mencionadas.

Parágrafo: Las discusiones y decisiones del Consejo Nacional de operación estarán relacionadas exclusivamente con aspectos técnicos para garantizar que la operación integrada del sistema interconectado nacional sea segura, confiable y económica o sobre aspectos del reglamento de operación, conforme con lo dispuesto en el artículo 36 de la Ley 143 de 1994"

[39] El Decreto 2238 de 2009 establece que: " Serán invitados a las sesiones de los Comités y Subcomités del Consejo Nacional de Operación, el Superintendente Delegado de Energía y Gas de la Superintendencia de Servicios Públicos Domiciliarios, el Director de Energía del Ministerio de Minas y Energía y el Director de la UPME, quienes serán invitados permanentes a las sesiones y podrán delegar su participación en las mismas.

Parágrafo. La participación en las sesiones de los Comités y Subcomités del Consejo Nacional de Operación por parte de los anteriores funcionarios, será con voz pero sin voto y atendiendo a las funciones legales y reglamentarias que se encuentren en cabeza de cada entidad."

c. La adopción de normas específicas ISO/IEC, IEC, IEEE, IETF, NIST e ISA, considerando las mejores prácticas identificadas a nivel nacional (ver Tabla 13).

3. En el largo plazo, se recomienda hacer seguimiento a la iniciativa ENISA sobre certificación de seguridad de las Redes Inteligentes en Europa (ENISA, 2014) y evaluar la conveniencia de solicitar en forma obligatoria a las empresas del sector eléctrico que se certifiquen en seguridad de RI bien sea mediante la adopción de una práctica internacional o una especificación nacional.
4. No es una medida, pero sí una recomendación de carácter general y es que frente al surgimiento de las RI se fortalezcan las capacidades TIC de actores claves en el sector eléctrico como el CNO y la CREG.

¿Quién debe adoptar las medidas?

Se recomienda que el DNP y el MinTIC como parte de la actual estrategia para la expedición de un nuevo CONPES sobre Ciberseguridad y Ciberdefensa, incluya el establecimiento del CSIRT sectorial para el sector eléctrico, con obligaciones y tiempos específicos para las empresas del sector eléctrico y con esquemas de articulación con el ColCERT y el CCOC a nivel nacional.

Se recomienda que una vez sea definido el referente de arquitectura a nivel nacional para las RI, el CNO analice un conjunto más amplio de normas de ciberseguridad, como las mencionadas en el numeral 2 de la sección previa y establezca la conveniencia de obligar la implementación de las que juzgue más apropiadas en las empresas del sector eléctrico, estableciendo plazos específicos de cumplimiento.

En el largo plazo, se recomienda que el Ministerio de Minas y Energía en colaboración con el MinTIC establezca la conveniencia de generar una Norma Nacional o adoptar una Norma Internacional que obligue a las empresas del sector eléctrico a obtener certificaciones en seguridad de RI.Los sistemas de medición inteligente.

9. Referencias

1. *Knapp, E., Samani, R., & Langill, J. (2013). Applied Cyber Security and the Smart Grid Implementing Security Controls into the Modern Power Infrastructure.*
2. *CEN-CENELEC-ETSI. (12 de 2014). SG-CG/M490/H_ Smart Grid Information Security .*
3. *CNO. (2015). Acuerdo 788 - Por el cual se aprueba la Guía de Ciberseguridad.*
4. *Organización de los Estados Americanos. (2015). http://www.oas.org. (OAS) Retrieved 14 de Septiembre de 2015 from http://www.oas.org/es/sms/cicte/programas_cibernetica.asp*
5. *CICTE & OEA. (2015). CICTE/DEC.1/12 rev. 1, OEA/Ser.L/X.2.12. - DECLARACIÓN "FORTALECIMIENTO DE LA SEGURIDAD CIBERNÉTICA EN LAS AMÉRICAS" (Aprobado durante la cuarta sesión plenaria, celebrada el 7 de marzo de 2012). DÉCIMOSEGUNDO PERÍODO ORDINARIO DE SESIONES CICTE/DEC.1/12 rev. 1, OEA/Ser.L/X.2.12. Washington, D.C.*
6. *OEA - CICTE. (20 de marzo de 2015). Declaración de Protección de infraestructura crítica ante las amenazas emergentes. CICTE/doc.1/15 - OEA/Ser.L/X.2.15 . Washington, D.C.*
7. *OEA - CICTE. (20 de marzo de 2015). Strategic plan of the secretariat of the interamerican committee against terrorism. Washington D.C., USA.*
8. *OEA - CICTE. (20 de marzo de 2015). Plan del trabajo para 2015 del CICTE. OEA/Ser.L/X.2.15 - CICTE/doc.6/15 Cor.1 . Washington D.C.*
9. *OEA - TREND MICRO. (Abril de 2015). Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. Washington, D.C., USA.*
10. *ESCSWG - Energy Sector Control System Working Group. (Septiembre de 2011). Roadmap to Achieve Energy Delivery Systems Cybersecurity. Washington D.C., USA.*
11. *U.S. Government - 110th United States Congress. (19 de Diciembre de 2007). PUBLIC LAW 110–140—DEC. 19, 2007 - ENERGY INDEPENDENCE AND SECURITY ACT OF 2007. Washington D.C., USA.*
12. *NIST (National Institute of Standars and Technology). (Septiembre de 2014). NISTIR 7628 Revision 1 - Guidelines for Smart Grid Cybersecurity. Gaithersburg MD, Maryland, USA.*
13. *NIST. (12 de Febrero de 2014). Framework for Improving Critical Infrastructure Cybersecurity. Washington D.C., USA.*
14. *NIST - Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology. (febrero de 2012). NIST SP 1108R2 - Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0. Washington D.C., USA.*
15. *FERC (Federal Energy Regulatory Commission). (16 de Julio de 2009). Smart Grid Policy, 128 FERC 61,060 [Docket No. PL09-4-000]. Washington, USA.*
16. *U.S. Department of energy. (Mayo de 2013). Electricity Subsector Cybersecurity Risk Management Process - DOE/OE-0003. Washington D.C., USA.*
17. *CRS - Congressional Research Service. (10 de Junio de 2015). Cybersecurity Issues for the Bulk Power System. USA.*
18. *Presidência da República. (13 de Junio de 2000). DECRETO No 3.505, DE 13 DE JUNHO DE 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.DECRETO No 3.505, DE 13 DE JUNHO DE 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasil.*
19. *Departamento de Segurança da Informação e Comunicações . (Noviembre de 2010). GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO . Brasilia, Brasil.*
20. *Departamento de Segurança da Informação e Comunicações . (2015). ESTRATÉGIA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES E DE SEGURANÇA CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL 2015 - 2018. Brasilia, Brasil.*
21. *Ministério das Minas e Energia. (15 de Abril de 2010). Portaria nº 440 de 15/04/2010 / MME Implantação de um Programa Brasileiro de Rede Elétrica Inteligente - "Smart Grid". Brasil.*
22. *ABDI. (2012). Relatório de acompanhamento setorial Smart Grid. Tendênciasno mundo e no Brasil e possibilidades de desenvolvimento produtivo e tecnológico.*
23. *Lima, C. (7 de Maio de 2014). Geração Distribuída e Smart Grid. Cenários Nacional/Internacional. Curitiba, Brasil.*
24. *ABDI. (2014). Mapeamento da Cadeia Fornecedora de TIC e de seus Produtos e Serviços para Redes Elétricas Inteligentes (REI). Normas Técnicas, Padrões e Regulamentos Aplicados à Cadeia de Produtos e Serviços de TIC para REI .*

25. *Ministerio del Interior y Seguridad Pública de Chile. (2015). Cuenta Pública 2015. Santiago de Chile, Chile.*
26. *MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA. (17 de Abril de 2015). Decreto 533 - CREA COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD. Santiago, Chile.*
27. *Ministerio del Interior y Seguridad Pública - Subsecretaría del Interior. (20 de Abril de 2015). http://subinterior.gob.cl/. (subinterior.gob.c) Retrieved 14 de Septiembre de 2015 from Gobierno crea comité interministerial para elevar estándares en materia de Ciberseguridad: http://subinterior.gob.cl/noticias/2015/04/20/gobierno-crea-comite-interministerial-para-elevar-estandares-en-materia-de-ciberseguridad/*
28. *Minister for the Cabinet Office. (2011). The UK Cyber Security Strategy Protecting and promoting the UK in a digital world . United Kingdom.*
29. *Cabinet Office. (December de 2013). The National Cyber Security Strategy Our Forward Plans.*
30. *Tristschler, M., & Mackay, W. (25 de June de 2011). The National Cyber Security Strategy Our Forward Plans – December 2013. London, UK.*
31. *ENSG. (United Kingdom de February de 2010). 1Electricity Networks Strategy GroupA Smart Grid Routemap.*
32. *Consejo de la Unión Europea. (8 de Diciembre de 2008). DIRECTIVA 2008/114/CE DEL CONSEJO sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.*
33. *ENISA. (May de 2012). National Cyber Security Strategies Setting the course for national efforts to strengthen security in cyberspace .*
34. *ENISA (European Network and Information Security Agency). (07 de Julio de 2012). Smart Grid Security - Recommendations for Europe and Member States. Heraklion, Grecia.*
35. *ENISA. (December de 2014). Smart grid security certification in Europe Challenges and recommendations .*
36. *Presidencia del Gobierno de España - Departamento de Seguridad Nacional. (2013). NATIONAL CYBER SECURITY STRATEGY. España.*
37. *Llombart Estopiñán , A., Comech Moreno , M., Alonso Hérranz , A., Borroy Vicente , S., Fumanal Achon , G., Goicoechea Bañuelos , G., et al. (2015). "Estudio de factibilidad técnica y económica de soluciones de redes inteligentes para el sector eléctrico colombiano" - Informe 2.*
38. *ABNT. (2008). NBR 14522 Intercâmbio de informações para sistemas de medição de energia elétrica.*
39. *ANEEL. (7 de Agosto de 2012). RESOLUÇÃO NORMATIVA Nº 502, DE 7 DE AGOSTO DE 2012 Regulamenta sistemas de medição de energia elétrica de unidades consumidoras do Grupo B.*
40. *ANEEL. (1 de Abril de 2014). RESOLUÇÃO NORMATIVA No 610, DE 1º DE ABRIL DE 2014 Regulamenta as modalidades de pré- pagamento e pós-pagamento eletrônico de energia elétrica.*
41. *ABNT. (25 de 12 de 2011). NBR 14519 Medidores eletrônicos de energia elétrica — Especificação. Brasil.*
42. *ABNT. (25 de 12 de 2011). Aceitação de lotes mediadores eletrônicos de energia elétrica - Procedimento. Brasil.*
43. *INMETRO. (15 de Agosto de 2013). Portaria no 401, de 15 de agosto de 2013. Estabelecer requisitos adicionais aos já fixados no Regulamento Técnico Metrológico de medidores eletrônicos de energia elétrica multitarifação. . Brasil.*
44. *INMETRO. (1 de Novembro de 2012). Portraia NO 586 - Establecer os requisitos técnicos de software; Garantir que o software proporcione medidas corretas e dentro dos erros admissíveis: Garantir que o software nao seja afetado por outros softwares. Brasil.*
45. *ANEEL. (25 de Agosto de 2009). RESOLUÇÃO NORMATIVA No 375, DE 25 DE AGOSTO DE 2009 Regulamenta a utilização das instalações de distribuição de energia elétrica como meio de transporte para a comunicação digital ou analógica de sinais.*
46. *Ministerio de Energía. (n.d.). Estrategia Nacional de Energía 2012-2030. Chile.*
47. *MINISTERIO DE TRANSPORTES Y TELECOMUNICACIONES. (1982). LEY GENERAL DE TELECOMUNICACIONES (Ley 18168 de 1982. Última modificación Ley 20808 de 2015). Chile.*
48. *Ministerio de Economía, Fomento y Reconstrucción. (29 de Abril de 1925). NSEG 3 E.n71. Normas Técnicas sobre Medidores. Chile.*
49. *Parlamento Europeo y Consejo Europe. (25 de Octubre de 2012). REGLAMENTO (UE) No 1025/2012 DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión no 1673/20. Estrasburgo.*
50. *European Commission. (1 de March de 2011). M/490 Smart Grid Mandate. Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment. Brussels, Belgium.*
51. *IEA (International Energy Agency). (25 de Abril de 2012). ISGAN White paper - Smart Grid Cyber Security.*

52. *PUC (Public Untilities Commission). (29 de Julio de 2011). Decision 11-07-056 - Decision Adopting Rules to Protect The Privacy and Security of The Electricity Usage Data of The Customers of Pacific Gas and Electric Company, Southern California Edison Company, And San Diego Gas & Electric Company. San Francisco, California, USA.*
53. *California Government. (29 de Septiembre de 2010). Senate Bill No. 1476, Padilla; Chapter 497. Public utilities: customer privacy: advanced metering infrastructure. San Francisco, California, USA.*
54. *European Commission. (25 de Enero de 2012). General Data Protection Regulation - REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Bruselas.*
55. *European Parliament. (24 de Octubre de 1995). Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*
56. *the guardian. (15 de Junio de 2015). http://www.theguardian.com/. Retrieved 13 de Septiembre de 2015 from http://www.theguardian.com/technology/2015/jun/15/eu-privacy-laws-data-regulations*
57. *Ofgem. (27 de Julio de 2010). Smart Metering Implementation Programme: Data Privacy and Security. UK.*
58. *Department for Business, Innovation & Skills . (8 de Mayo de 2015). 2010 to 2015 government policy: consumer protection. https://www.gov.uk/government/publications/2010-to-2015-government-policy-consumer-protection/2010-to-2015-government-policy-consumer-protection#appendix-4-personal-data . UK.*
59. *Department for Business, Innovation & Skills. (8 de Mayo de 2015). www.gov.uk. Retrieved 14 de Septiembre de 2015 from https://www.gov.uk/government/publications/2010-to-2015-government-policy-consumer-protection/2010-to-2015-government-policy-consumer-protection#appendix-8-consumer-rights-act-2015*
60. *UK Government. (Marzo de 2015). Consumer Rights Act 2015. Londres, Inglaterra, UK: Majesty's Stationery Office and Queen's Printer of Acts of Parliament.*
61. *CEN-CENELEC-ETSI. (2014). SGCG/M490/G_Smart Grid Set of Standards 24 Version 3.1 .*
62. *Congreso - Ley 1341. (2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.*
63. *CRC. (15 de Mayo de 2015). Resolución 4734 de 2015 Por la cual se modifican las Resoluciones CRC 3067 y 3496 de 2011 y se dictan otras disposiciones. Colombia.*
64. *Asamblea Nacional Constituyente. (1991). CONSTITUCION POLITICA DE COLOMBIA. Colombia.*
65. *Congreso de Colombia. (31 de Diciembre de 2008). LEY ESTATUTARIA 1266 DE 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Bogotá, Colombia.*
66. *Congreso de Colombia. (17 de Octubre de 2012). LEY ESTATUTARIA 1581 DE 2012 Por la cual se dictan disposiciones generales para la protección de datos personales. Colombia.*
67. *Presidencia de la República de Colombia. (27 de Junio de 2013). DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá, Colombia.*
68. *CRC. (18 de Mayo de 2011). Resolución 3066 Regimen Integral de Protección de los Derechos de los usuarios de los Servicios de Comunicaciones . Colombia.*
69. *CREG. (14 de Mayo de 2014). Resolución 038 Por la cual se modifica el Código de Medida contenido en el Anexo general del Código de Redes . Bogotá, Colombia.*
70. *MinTIC. (8 de Marzo de 2010). Resolución 202 "Por la cual se expide el glosario de definiciones conforme a lo ordenado por el inciso segundo del artículo 6 de la Ley 1341 de 2009". Colombia.*
71. *CRC. (10 de agosto de 2011). Resolución No 3101 de 2011 por medio de la cual se expide el régimen de acceso, uso e interconexión de redes de telecomunicaciones, y se dictan otras disposiciones. Bogotá, Colombia.*
72. *UIT. (2007). Recomendación UIT-T Y.2261 (09/2006) - Evolución de la RTPC/RDSI hacia las redes de la próxima generación. Ginebra.*
73. *CEN-CENELEC-ETSI Smart Grid Working Group . (2012). SmartGrid Reference Architecture.*
74. *Gómez Pineda, J. (15 de Septiembre de 2015). ATN/KK-14254-CO Primer Entregable: Revisión de experiencias a nivel internacional de aspectos de política y regulación de Telecomunicaciones y TIC involucradas en la implementación de RI . Bogotá, Colombia.*
75. *Osorio Muñoz, H. (n.d.). Estándares técnicos para medición de energía eléctrica en Colombia.*
76. *Icontec. (27 de 10 de 2014). NTC 6079 requisitos para Sistemas de Infraestructura de MEdición Avanazada (AMI) en redes de distribución de Energía Eléctrica. Colombia.*
77. *IEEE. (n.d.). 610 IEEE Standard Glossary of Software Engineering Terminology .*
78. *CEN-CENELEC-ETSI. (31 de 10 de 2014). SG-CG/M490/I_Smart Grid Interoperability Methodologies to facilitate Smart Grid system interoperability through standardization, system design and testing.*

79. *IEC. (2014). IEC 62056-1-0:2014 Smart metering standardisation framework.*
80. *ANSI. (2009). ANSI C12.22-2008. Protocol Specification For Interfacing to Data Communication Networks. USA: American National Standards Institute, Inc.*
81. *IEC. (2010). 61968-9 Message profiles for DLMS/COSEM. IEC TC 13.*
82. *ANSI. (2009). ANSI C12.19-2008. For Utility Industry End Device Data Tables. USA: American National Standards Institute, Inc.*
83. *MinTIC. (17 de Diciembre de 2012). Decreto 2618 de 2012 Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones. Colombia.*
84. *MinTIC. (11 de Mayo de 2015). Resolución 8282 de 2015 Por la cual se adopta el Plan Estratégico Sectorial e Institucional del Ministerio de Tecnologías de la Información y las Comunicaciones, para el periodo 2014-2018. Colombia.*
85. *Conpes. (14 de julio de 2011). 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa. Bogotá, Colombia.*
86. *MinTIC. (2015). Fortalecimiento de la estrategia de Ciberseguridad y Ciberdefensa. Colombia.*
87. *Congreso de Colombia. (5 de Enero de 2009). LEY 1273 DE 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá, Colombia.*
88. *Congreso de la República. (30 de Julio de 2009). Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Colombia.*
89. *CRC. (2011). Resolución 3067 "Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones". Bogotá.*
90. *Congreso de Colombia. (11 de Julio de 1994). Ley 143 de 1994 por la cual se establece el régimen para la generación, interconexión, trasmisión, distribución y comercialización de electricidad en el territorio nacional, se conceden unas autorizaciones y se dictan otras disposiciones en materia energética. Colombia.*
91. *NERC. (26 de 11 de 2012). CIP-002-5 - Cyber Security — BES Cyber System Categorization. (Version 5). Washington, DC, USA.*
92. *NERC. (26 de 11 de 2012). CIP-003-5 — Cyber Security — Security Management Controls. (Version 5). Washington, DC, USA.*
93. *NERC. (26 de 11 de 2012). CIP-004-5 — Cyber Security – Personnel & Training. (Version 5). Washington, DC, USA.*
94. *NERC. (26 de 11 de 2012). CIP-005-5 — Cyber Security – Electronic Security Perimeter(s). Version 5. Washington, DC, USA.*
95. *NERC. (26 de 11 de 2012). CIP-006-5 — Cyber Security — Physical Security of BES Cyber Systems. (Version 5). Washington, DC, USA.*
96. *NERC. (26 de 11 de 2012). CIP-007-5 — Cyber Security – Systems Security Management. (version 5). Washington, DC, USA.*
97. *NERC. (26 de 11 de 2012). CIP-008-5 — Cyber Security — Incident Reporting and Response Planning. (version 5). Washington, DC, USA.*
98. *NERC. (26 de 11 de 2012). CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems. (version 5). Washington, DC, USA.*
99. *CNO. (16 de Septiembre de 2014). Acuerdo 701 Por el cual se aprueba el documento de "Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC". Colombia.*
100. *Presidencia de la República. (16 de Noviembre de 1993). Decreto 2269 de 1993 por el cual se organiza el Sistema Nacional de Normalización, Certificación y Metrología. Colombia.*
101. *Icontec. (11 de 12 de 2013). NTC-ISO-IEC 27001 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS. Colombia.*
102. *Icontec. (16 de 11 de 2007). NTC-ISO/IEC 27002 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. Colombia.*
103. *ISO. (2007). ISO/IEC 27001:2007 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Ginebra.*
104. *ISO/IEC. (2013). ISO/IEC TR 27019. First edition (2013-07-15). Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. Geneva: ISO/IEC.*

105. *NERC. (24 de 01 de 2011). CIP–002–4 — Cyber Security — Critical Cyber Asset Identification. (Version 4). Washington, DC, USA.*
106. *NERC. (24 de 01 de 2011). CIP-003-4 — Cyber Security — Security Management Controls. (Version 4). Washington, DC, USA.*
107. *NERC. (24 de 01 de 2011). CIP-004-4 — Cyber Security – Personnel & Training. (Version 4). Washington, DC, USA.*
108. *NERC. (24 de 01 de 2011). CIP-006-4c — Cyber Security — Physical Security. (Version 4c). Washington, DC, USA.*
109. *NERC. (24 de 01 de 2011). CIP-007-4 — Cyber Security – Systems Security Management. (version 4). Washington, DC, USA.*
110. *NERC. (24 de 01 de 2011). CIP-008-4 — Cyber Security — Incident Reporting and Response Planning. (version 4). Washington, DC, USA.*
111. *NERC. (24 de 01 de 2011). CIP-009-4 — Cyber Security — Recovery Plans for Critical Cyber Assets. (version 4). Washington, DC, USA.*
112. *NIST. (June de 2011). NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controller. Washington D.C., USA: U.S. Department of Commerce.*
113. *NIST. (April de 2013). NIST Special Publication 800-53 (Revision 4) - Security and Privacy Controls for Federal Information Systems and Organizations. Washington, DC., USA.*
114. *ANSI/ISA. (2007). ANSI/ISA 99.00.01, October 2007. Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models. Durham, North Carolina (USA).*
115. *ANSI/ISA. (2009). ANSI/ISA–62443-2-1 (99.02.01)–2009. Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. Durham, North Carolina (USA), USA.*
116. *ANSI/ISA. (February de 2009). ISA-99.03.02-2009D3E4 - Security for Industrial Automation and Control Systems: Technical Requirements, Target Security Levels. Durham, North Carolina (USA), USA.*
117. *ANSI/ISA. (February de 2009). ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems. Durham, North Carolina (USA), USA.*
118. *Congreso - Ley 142. (1994). Por la cual se establece el régimen de los servicios públicos domiciliarios y se dictan otras disposiciones.*
119. *UPME. (2015). Plan Energético Nacional - Colombia: Ideario Energético 2050.*
120. *Colombia Inteligente. (2013). Ejes estratégicos y temáticos.*
121. *Universidad del Valle. (2015). Convenio de asociación CV-010 suscrito entre la Unidad de Planeación Minero Energética, la Universidad del Valle, Empresas Municipales de Cale (EMCALI) y Empresa de Energía del Pacífico S.A. E.S.P (EPSA).*
122. *UPME. (2013). Plan de expansión de referencia generación-transmisión 2013-2027.*
123. *MErcados Energéticos Consultores. (2015). Prestación de servicios para determinar los niveles de calidad exigibles en las redes del SIN.*
124. *UPME. (2014). Plan de expansión de referencia generación - transmisión 2014 - 2018.*
125. *Llombart Estopiñán, A., Comech Moreno, M., Alonso Hérranz, A., Borroy Vicente, S., Rodríguez Sánchez, F., Girón Casares, C., et al. (2015). Informe I - Estudio de factibilidad técnica y económica de soluciones de redes inteligentes para el sector eléctrico Colombiano.*
126. *IEC. (2011). IEC62357-1, TR Ed.1: Reference architecture for power system information exchange. .*
127. *ENISA. (31 de 03 de 2012). Annex IV - Security related standards, guidelines and regulatory documents .*
128. *Unión Europea. (25 de Octubre de 2012). REGLAMENTO (UE) No 1025/2012.*
129. *Ministerio del Interior y Seguridad Pública - Subsecretaría del Interior. (20 de Abril de 2015). http://subinterior.gob.cl/. (subinterior.gob.cl) Retrieved 14 de Septiembre de 2015 from Gobierno crea comité interministerial para elevar estándares en materia de Ciberseguridad: http://subinterior.gob.cl/noticias/2015/04/20/gobierno-crea-comite-interministerial-para-elevar-estandares-en-materia-de-ciberseguridad/*
130. *U.S. Department of Energy. (22 de July de 2015). http://www.energy.gov/. (Office of Energy Efficency & Renewable Energy) Retrieved 8 de October de 2015 from http://www.energy.gov/eere/articles/green-button-initiative-makes-headway-electric-industry-and-consumers*
131. *MinTIC. (18 de Diciembre de 2009). Decreto 4948 "Por el cual se reglamenta la habilitación general para la provisión de redes y servicios de telecomunicaciones y el registro TIC". Colombia.*
132. *Ministerio de Minas y Energía. (21 de Octubre de 1999). Decreto 2023 de 1999 "Por el cual se modifican unas funciones del Consejo Nacional de Operación". Colombia.*

133. *Ministerio de Minas y energía. (29 de Junio de 2001). Decreto 1274 de 2001 "Por el cual se derogan los Decretos 2023 de 1999 y 2804 de 2000.". Colombia.*
134. *ENISA. (n.d.). Cómo crear un CSIRT paso a paso.*
135. *Mercados Energéticos Consultores. (2015). Prestación de servicios para determinar los niveles de calidad exigibles en las redes del SIN.*