Comisión de Regulación de Energía y Gas

DOCUMENTO DE CONSULTA

ESTRATEGIA INTEGRAL DE SEGURIDAD DIGITAL EN EL SECTOR ELÉCTRICO

DOCUMENTO CREG-065

30 DE AGOSTO DE 2019

CIRCULACIÓN:
MIEMBROS DE LA COMISIÓN DE REGULACIÓN DE ENERGÍA Y GAS

CONTENIDO

DOCUMENTO DE CONSULTA

ESTRATEGIA INTEGRAL DE SEGURIDAD DIGITAL EN EL SECTOR ELÉCTRICO

A través del presente documento la Comisión pone en conocimiento de las entidades prestadoras del servicio público domiciliario de energía eléctrica, los usuarios y demás interesados, el proceso de consulta para la definición de una estrategia integral seguridad digital en el sector eléctrico y la regulación necesaria para su implementación.

1 ANTECEDENTES E INFORMACIÓN GENERAL

1.1 Política nacional de seguridad digital

En la Asamblea General de la OEA en 2004, mediante la resolución AG/RES. 2004 (XXXIV-O/04), los Estados miembros aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética.

Entre los principales objetivos definidos se encuentran el establecimiento de grupos nacionales de "alerta, vigilancia y prevención", también conocidos como Equipos de Respuesta a Incidentes (CSIRT) en cada país, crear una red de alerta Hemisférica que proporcione formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos, promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio.

En el documento CONPES 3701 del 2011 se definen los lineamientos de política para ciberseguridad y ciberdefensa en el país, en las bases del Plan Nacional de Desarrollo 2014 - 2018 se definen los aspectos de la Política nacional de seguridad digital y en el Documento CONPES 3854 de 2016 se define la Política nacional de seguridad digital. El gobierno se encuentra en proceso de actualización de la política de seguridad digital, para esto se está trabajando en una nueva hoja de ruta.

En estos documentos, la Presidencia de la República y el Ministerio de Defensa, clasificaron al sector eléctrico como crítico.

El Ministerio de Defensa formuló el Plan nacional de protección y defensa para la infraestructura critica cibernética de Colombia, también estableció la primera versión del plan sectorial de protección y defensa para el sector electricidad, PSPSE, con colaboración del Consejo Nacional de Operación, CNO, y algunos agentes del sector.

1.2 Normatividad relacionada en el sector eléctrico

En el literal c) del artículo 74 de la Ley 142 de 1994 se señala que la Comisión tiene la función de establecer el reglamento de operación para el planeamiento y la coordinación de la operación SIN y del mercado y en el literal n) del artículo 23 de la Ley 143 de 1994, se establece la función de definir y hacer operativos los criterios técnicos de calidad, confiabilidad y seguridad.

Según lo definido en el artículo 25 de la Ley 143 de 1994, los agentes deben cumplir con el reglamento de operación y los acuerdo adoptados para la operación del SIN por parte del CNO.

La Resolución CREG 025 de 1995 establece el código de redes, la Resolución CREG 070 de 1998, que hace parte del código de redes, tiene dentro de sus objetivos asegurar el funcionamiento seguro, confiable y económico del SIN en general y de los sistemas de transmisión regional, STR, y de los sistemas de distribución local, SDL. Tales regulaciones incluyen el planeamiento operativo y la adecuada coordinación entre los diferentes agentes.

En la Resolución CREG 080 de 1999 se reglamentan las funciones de planeación, coordinación supervisión y control entre el Centro Nacional de Despacho, CND, y los agentes del SIN.

Mediante el Acuerdo 788 de 2015 del CNO se aprobó la guía de ciberseguridad y en el Acuerdo 1043 de 2018 del CNO se modificaron las condiciones mínimas de seguridad e integridad para la transmisión de lecturas de medidores [1].

En la Circular 034 de 2019, el CNO publicó la propuesta de Acuerdo "Por el cual se aprueba la modificación de la Guía de Ciberseguridad" y el documento de modificación de la Guía de Ciberseguridad, dicha actualización se encuentra en proceso de análisis y aprobación.

1.3 Estudios de ciberseguridad en Colombia

A continuación, se relacionan algunos apartes de las evaluaciones realizadas por el observatorio de la ciberseguridad en América Latina y el Caribe, de la Organización de los Estados Americanos, OEA, y el Ministerio de Comunicaciones de Colombia.

El observatorio de la ciberseguridad en América Latina y el Caribe, con base en el modelo de madurez de capacidad de seguridad cibernética, CMM[2], muestra el grado de madurez de los países de la región en las siguientes áreas o dimensiones: i) política y estrategia, ii) cultura y sociedad, iii) educación, iv) marcos legales y v) tecnologías.

En esta metodología, para cada dimensión se evalúan cinco posibles etapas de madurez: i) inicial, ii) formativo, iii) establecido, iv) estratégico y v) dinámico.

De manera general, las etapas de madurez corresponden al siguiente estado:

a. **Inicial:** no existe nada o lo que existe apenas está naciendo, el problema está planteado, pero aún no hay acciones.

b. **Formativo:** Las características han comenzado a crecer, pero pueden ser desorganizadas o mal definidas.

c. **Establecido:** Las acciones están establecidas y funcionando. Falta perfeccionar la asignación relativa de recursos. Ha habido poca toma de decisiones de compensación en relación con la inversión relativa.

[1] El Acuerdo 1043 de 2015 modifica 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" adoptado por el Consejo Nacional de Operación, mediante los acuerdos 1004 de 2017 y 701 de 2014.

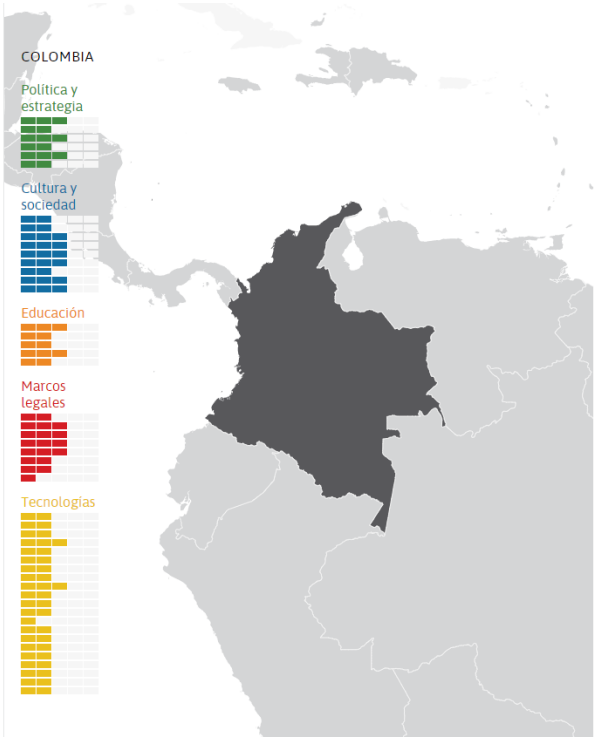
[2] Cybesecurity madurity model, CMM de la Universidad de Oxford.

d. **Estratégico:** Se han elegido las características más relevantes para el país, al igual que aquéllas que son menos importantes, en función de un objetivo buscado.

e. **Dinámico:** Existen mecanismos claros para alterar la estrategia en la medida en que las amenazas muten. La toma de decisiones es rápida al igual que la reasignación de recursos

En la Gráfica 1 se presentan los resultados para Colombia del informe de ciberseguridad del año 2016. Se observa que, de los 49 aspectos evaluados, el 35% (17) se encuentra en nivel establecido, el 61% (30) se encuentra en nivel formativo y el 4% en nivel inicial.

Gráfica 1 Evaluación madurez de capacidad de seguridad cibernética – Colombia. Fuente OEA



La dimensión que está más relacionada con el sector energético en general y el eléctrico en particular es la de tecnologías, la cual se encuentra compuesta por 21 sub-factores. En la Gráfica 2 se comparan los resultados del 2016 para Brasil, México, Chile y Colombia en la dimensión de tecnologías. Al comparar los resultados se observa que en la mayoría de aspectos Colombia se encuentra en el nivel de madurez 2 y que solamente en 2, se encuentra en nivel 3, en comparación de 7 de México y 6 de Brasil.

Gráfica 2 Comparación de la madurez en la dimensión tecnologías – Fuente OEA

De otra parte, el Ministro de Tecnologías de la Información y las Comunicaciones de Colombia, MINTIC, publicó el estudio *Impacto de los incidentes de seguridad digital en Colombia 2017*, en este informe se presenta un análisis de los ataques al sector público y el sector privado, así como su nivel de preparación para defenderse de dichos ataques.

Dentro de las principales conclusiones del estudio se destacan las siguientes:

a. El 37% de las empresas que participaron del estudio (empresas de los sectores Servicios, Industria y Comercio) creen que estaban preparadas para manejar un incidente digital.

b. el 70% de las grandes empresas se sienten muy preparadas o preparadas para gestionar un incidente digital, frente al 45% de las microempresas.

c. La precepción de estar muy preparados o preparados para enfrentar incidentes cibernéticos es mayor en las entidades nacionales que en las entidades territoriales.

d. Las organizaciones que se sienten más preparadas aún necesitan incrementar sus medidas de seguridad y deben incluir un mayor presupuesto para seguridad digital.

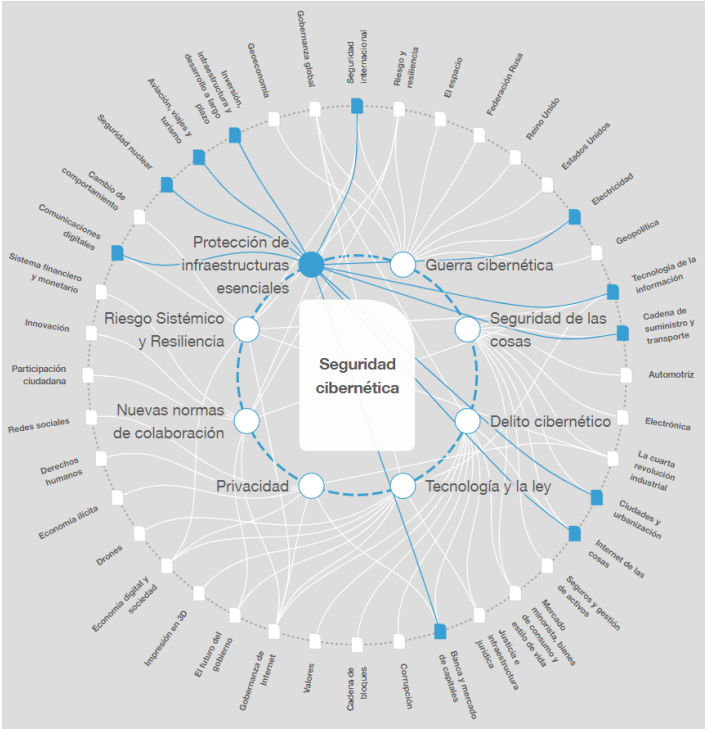
e. El 54% de empresas del sector Industrial dijo tener un equipo con dedicación exclusiva, frente a un 45% y el 42% de empresas de los sectores de servicios y comercio, respectivamente

f. Los principales factores que afectan la seguridad digital son la falta de personal con dedicación exclusiva, la falta de presupuesto y la falta de conciencia de los empleados.

1.4 La seguridad digital como uno de los temas claves a nivel global

Dentro de los temas destacados de la agenda global del Foro Económico Mundial, *WEF*, por sus siglas en inglés, se encuentra la seguridad cibernética, sobre la cual se señala que *A medida que el mundo se vuelve digitalmente más interconectado, será más difícil mantener la seguridad cibernética. Las herramientas digitales están cada vez más conectadas a la infraestructura física, por lo que es muy importante asegurar adecuadamente los sistemas esenciales. Las organizaciones tendrán que utilizar el aprendizaje automático y la inteligencia artificial para poder medir y reportar de mejor manera el riesgo cibernético, ya que enfrentan problemas asociados con la proliferación de dispositivos que alimentan ciudades inteligentes y el Internet de las cosas.*

Gráfica 3 Aspectos relacionados con la Ciberseguridad - WEF



De acuerdo con el WEF, existen ocho temas relevantes relacionados con la seguridad cibernética, que van desde la privacidad de la información hasta la guerra cibernética, así: Protección de

infraestructuras esenciales, guerra cibernética, seguridad de las cosas, delitos cibernéticos, tecnología y Ley, privacidad, nuevas normas de colaboración y riesgo sistémico y resiliencia.

A continuación, se presentan algunos apartes relacionados con los temas relevantes identificados por el WEF que se encuentran relacionados de manera importante con los sectores regulados por la Comisión, en especial el sector eléctrico.

Respecto a la protección de infraestructuras esenciales se encuentran, entre otras, el sector de electricidad y las cadenas de suministro y transporte. De acuerdo con el WEF, *la necesidad de proteger la integridad cibernética de la infraestructura esencial, como las redes de energía y sistemas de higiene, es uno de los retos primordiales de la sociedad. La proliferación de sistemas que fusionan el mundo cibernético y físico combinando la infraestructura física con la potencia de procesamiento puede aumentar la funcionalidad, pero también crea más objetivos para los ataques cibernéticos.*

Incluso un ataque en contra de un solo sector esencial de la infraestructura, o sea uno relacionado con la energía, el sistema financiero, las redes de comunicación o los servicios de agua, podría paralizar a comunidades o incluso naciones enteras.

Solo en el año 2016, el Equipo de Respuesta a Emergencias de Sistemas Informáticos de Control Industrial del Departamento de Seguridad Nacional de los Estados Unidos respondió a 290 incidentes, incluidos 63 del sector de fábricas fundamentales y 59 de industrias de energía, según el informe que se publicó; más del 25 % de los incidentes estaban relacionados con los llamados ataques "spear phishing", los cuales implican el envío de correos electrónicos fraudulentos para persuadir a alguien a revelar información confidencial.

Frente a la privacidad se señala la importancia de considerar la gran cantidad de transacciones, el intercambio de datos e información y la seguridad relacionada con estos. En el caso del sector eléctrico se prevé la incorporación de nuevas tecnologías, medición inteligente, cambios de reglas del negocio, nuevos agentes, etc. que requerirán un manejo adecuado de la información.

En relación con las guerras cibernéticas, se considera necesario que los países desarrollen capacidades y estrategias de gestión de las amenazas en este escenario. Como ejemplos se encuentra el ciberataque sucedido en Estonia en el 2007 que originó que todos los sitios web de las entidades oficiales, así como de algunos bancos y medios de comunicación no estuvieran disponibles y también estuvo afectado el servicio de Internet y de correo de algunas instituciones.

En Irán, en el 2010 se presentó un ciberataque empleando un malware destinado de manera específica a sistemas de control industrial basados en SCADA, que afectaron la operación de las unidades enriquecedoras de uranio en una central nuclear. En el 2019, se presentó otro ataque cibernético cuyo objetivo fueron los sistemas de control de las plataformas de lanzamiento de misiles.

En el sector eléctrico, en 2015 se presentó un ataque cibernético en Ucrania que afectó la operación del sistema de electricidad y dejó sin servicio a más de 200 mil usuarios.

1.5 Sector eléctrico y seguridad digital

En relación con los problemas de seguridad digital que puedan afectar el suministro de energía eléctrica, desde el punto de vista de análisis de riesgos, se pueden identificar tres situaciones que aumentan los riesgos e incrementan el impacto ante la materialización de estos riesgos.

a. La digitalización de la economía y del sector eléctrico

b. La transformación del sector eléctrico

c. La electrificación de la economía

La digitalización del sector eléctrico, tanto en la operación del sistema como en el manejo de las transacciones del mercado y la aparición de nuevos agentes y de usuarios activos aumenta las vulnerabilidades y genera un mayor riesgo de ocurrencia de eventos de seguridad digital.

La electrificación de la economía hace que tanto los procesos productivos como los hogares, sean más dependientes del suministro de energía eléctrica, por lo cual, un problema en el suministro conlleva un mayor impacto.

1.5.1 Digitalización del sector eléctrico

La implementación de nuevas tecnologías, el avance de la digitalización, y los nuevos modelos de negocio en el sector eléctrico, traen beneficios, tanto para la demanda (mayor información para tomar decisiones de consumo, gestión de la demanda), como para los agentes existentes (menores costos de control y gestión del sistema, mayor capacidad de toma de decisiones) y los nuevos agentes (nuevos negocios), pero también conlleva un mayor riesgo en el suministro de energía eléctrica por posibles incidentes relacionados con ciberseguridad

De acuerdo con lo señalado por NARUC *(National Association of Regulatory Utility Commissioners), el aumento de la digitalización también está ampliando el despliegue de una infraestructura de medición más avanzada. Hoy en día, más de 60 millones de medidores inteligentes miden el consumo de más del 40 % de los edificios de Estados Unidos. Se espera que el despliegue de los medidores inteligentes alcance el 72 % de los consumidores de la Unión Europea para el año 2020, en comparación con China, la cual, por sí sola, había instalado alrededor de 350 millones de medidores inteligentes para el 2016.*

Por otro lado, la infraestructura digital de la red y la recopilación de datos están habilitando una gestión más activa de la red; por ejemplo, en el Reino Unido, UK Power Networks desarrolló un programa para gestionar activamente la producción de las centrales de energía eólica, lo que permite interconectar de forma más rápida y económica los generadores con la demanda.

Sin embargo, el aumento de la digitalización del sistema de energía también ha creado nuevas vulnerabilidades, como lo demostró el ataque cibernético del 2015 a la red de energía de Ucrania.

Debido a que las tecnologías digitales recopilan datos valiosos, crean la necesidad de que las normas sobre cómo gestionar los datos de manera segura, las nuevas regulaciones que garantizan los servicios y las otras partes interesadas del sector de la energía estén preparadas adecuadamente para las amenazas cibernéticas.

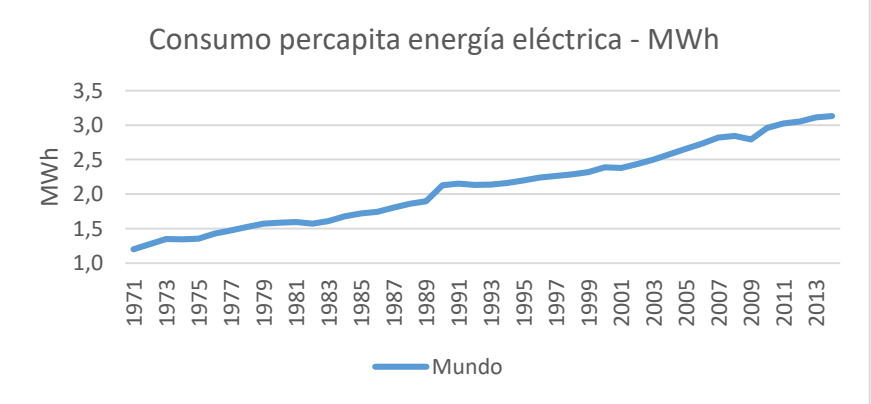
1.5.2 Transformación del negocio, redes inteligentes

En el mediano y largo plazo se prevén cambios en el modelo de negocio del sector con la incorporación de nuevas tecnologías de generación (a menor escala), mayor participación de la demanda, creación de nuevos agentes y servicios, entre otros. Gran parte de estos desarrollos se fundamentan en el uso intensivo de tecnologías de información, los cual crea mayor vulnerabilidad dado el mayor tráfico de datos entre agentes.

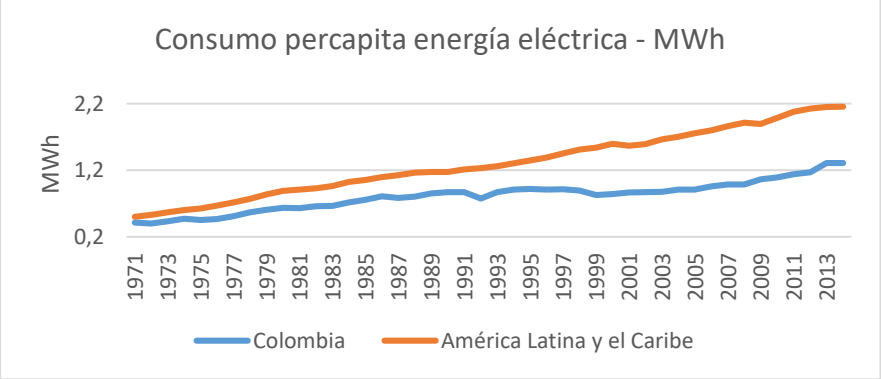
1.5.3 Electrificación de la economía

En los últimos años a nivel mundial y en Colombia se evidencia un mayor uso de la energía eléctrica como energético, tal como se observa en las siguientes tablas.

Gráfica 4 Consumo per cápita a nivel mundial – Fuente Banco mundial



Gráfica 5 Consumo per cápita en Colombia y Latinoamérica– Fuente Banco mundial



De acuerdo con un informe de la agencia internacional de energía del año 2018, se prevé un aumento de la demanda de energía del orden del 25% en el 2040. El mismo informe señala que el mayor aumento se dará en la demanda de energía eléctrica y que en los países en desarrollo se duplicará la demanda de electricidad.

1.6 Integración de sistemas tradicionales y nuevas tecnologías en la operación

El modelo de operación tradicional del sistema eléctrico ha cambiado en los últimos años, asociado con la incorporación de nuevas tecnologías y sistemas basados en comunicaciones. Esto trae beneficios en la operación, pero a su vez implica mayores riesgos.

En la Gráfica 6 se presenta un modelo que representa la integración de los sistemas de control, los sistemas de información y los nuevos elementos de las redes inteligentes.

Gráfica 6 Modelo de integración de sistemas tradicionales y redes inteligentes

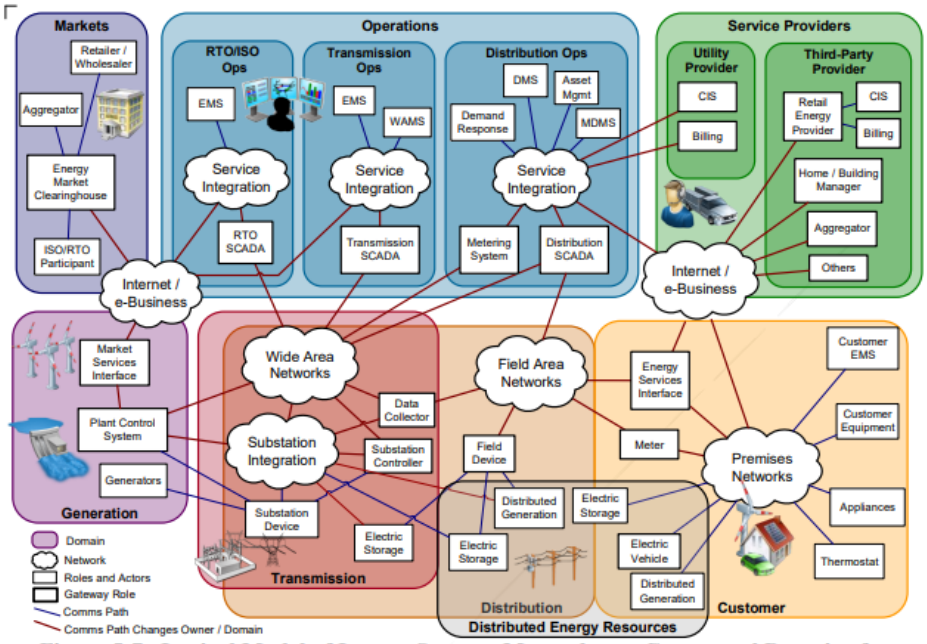


Figure 5-7. Logical Model of Legacy Systems Mapped onto Conceptual Domains for Smart Grid Information Networks

Fuente: NIST Framework and Roadmap for Smart Grid Interoperability Standards, 2014.

Desde el punto de vista de procesos, se pueden clasificar en las siguientes dimensiones:

a. Tecnologías de operación, *OT*[3], y sistemas de control: Están relacionadas con los sistemas de control y adquisición de datos, SCADA, los cuales soportan la operación del sistema.

b. Tecnologías de información, *IT*: se relaciona con los sistemas de información que permiten la operación del negocio en actividades que van desde la gestión administrativa hasta las transacciones del mercado, medición y facturación de consumos, etc.

[3] Operation technology, OT

c. Redes inteligentes: Está relacionada con las nuevas tecnologías incorporadas en el sistema como PMU, medidores inteligentes, electrodomésticos inteligentes, vehículos eléctricos, etc.

En general se observan mayores procesos de recolección, almacenamiento e intercambio de datos, mayor interacción entre los elementos de la red, así como órdenes y respuestas automáticas dentro de la red.

1.7 Avances en el sector eléctrico

Colombia cuenta con una política de seguridad digital que establece que en los diferentes sectores se deben incorporar mecanismos para la seguridad digital.

La política pública en relación con la seguridad digital señala que se debe adoptar un enfoque basado en la gestión de riesgos, que permita a los individuos el libre, seguro y confiable desarrollo de sus actividades en el entorno digital.

De otra parte, se definió que el coordinador nacional de seguridad digital apoyará la creación de CSIRT sectoriales, los cuales permitirán la adecuada gestión de incidentes digitales en los diversos sectores de la economía. En el sector eléctrico, XM se encuentra desarrollando algunas funciones básicas de CSIRT[4], sin embargo, como parte de la estrategia integral de seguridad digital, se requiere la definición del alcance del CSIRT sectorial, así como el agente y el esquema de prestación de estos servicios.

Varios agentes han empezado a desarrollar estrategias de seguridad al interior de sus empresas, *IT* y *OT*, y se han desarrollado acuerdos, como el CNO 788 de 2015[5], relacionados con la seguridad en los sistemas de operación *OT*.

De acuerdo con lo establecido en la Resolución CREG 038 de 2014, 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.

Aunque se observan avances en el caso de algunos agentes, el CNO ha desarrollado encuestas para identificar el estado de las empresas de sector en materia de ciberseguridad con base en el acuerdo CNO 788 de 2015. Al respecto, se identifican oportunidades para mejorar y ampliar el alcance a mayores agentes del sector y en particular se evidencia:

a. Baja participación de los agentes en las encuestas para conocer el avance en la implementación del Acuerdo 788 de 2015, en promedio se tienen 15 empresas.

b. Para el año 2018, el 86% de los encuestados tienen identificados los ciberactivos críticos.

c. El 60% de las empresas que respondieron en el año 2018 han realizado un análisis o estudio de riesgo.

[4] Denominada fase 0 de implementación del CSIRT.

[5] El CNO se encuentra en proceso de actualización del acuerdo 788 de 2015.

d. Solamente el 30 % de las empresas que respondieron la encuesta en el 2018 disponen de un plan de recuperación de sus ciberactivos críticos.

De otra parte, la iniciativa Colombia Inteligente, en abril de 2018, elaboró un análisis de referenciamiento con el objetivo de identificar características funcionales de un CSIRT aplicado al sector eléctrico en Colombia y lecciones aprendidas y la Unidad de Planeación Minero Energética, UPME, adelantó un estudio sobre Gobernanza, interoperabilidad y ciberseguridad para las redes inteligentes en Colombia, en noviembre de 2018.

2 ANÁLISIS GENERAL SOBRE LA NECESIDAD DE DEFINIR UNA ESTRATEGIA INTEGRAL DE SEGURIDAD DIGITAL

2.1 Definición del problema

El problema inicialmente identificado corresponde al aumento en el riesgo de fallas en el suministro de energía eléctrica asociado con problemas de seguridad digital y mayor impacto por una eventual falta de suministro.

Esta es una situación que se ha incrementado a nivel mundial en los últimos años y se prevé que en Colombia aumente por la creciente incorporación de nuevas tecnologías en la operación de los sistemas eléctricos, por la mayor dependencia de sistemas de comunicaciones y por la mayor cantidad de dispositivos conectados al sistema.

De otra parte, la creciente electrificación de la economía hace que la ocurrencia de eventos en el sector eléctrico (interrupciones, apagones, etc.) tengan un impacto mayor.

Teniendo en cuenta el alto impacto en la economía por la falta de suministro de energía eléctrica, ocasionada por la materialización de riesgos en la operación del sistema y del mercado eléctrico por eventos de ciberseguridad, se considera necesario definir una estrategia integral que permita al sector minimizar los riesgos asociados con eventos de seguridad digital, así como el manejo y recuperación del sistema ante la materialización de dichos riesgos.

2.2 Causas

Entre las principales causas asociadas al problema se encuentran las siguientes:

a. Creciente integración de tecnologías de información, IT, con tecnologías de operación, OT, e incorporación de redes inteligentes en la operación del sector eléctrico.

b. Bajo conocimiento y falta de conciencia sobre los problemas asociados con incidentes de seguridad digital por parte de los agentes y usuarios.

c. Avances únicamente para la protección de ciberactivos críticos.

d. Falta de una estrategia integral de seguridad digital que permita incorporar las mejores prácticas de mitigación de riesgos y estrategias de reacción ante este tipo de eventos.

e. Recursos bajos o inexistentes destinados al aseguramiento de los sistemas de operación y de información.

f. Incorporación de nuevas tecnologías a la red sin considerar aspectos de seguridad digital.

2.3 Consecuencias

a. Riesgo en la prestación del servicio, lo cual viene acompañado de elevados costos económicos.

b. Riesgo en los procesos del mercado asociados con la liquidación, facturación, medición, etc.

c. Pérdida o manipulación de información de usuarios, por ejemplo, en los sistemas de medición inteligente.

d. Mayores costos en la prestación del servicio como consecuencia de las actividades necesarias para mitigar los riesgos asociados. Los costos para su implementación no son fáciles de identificar, estandarizar, evaluar o asignar.

2.4 Actores interesados

Entre los principales agentes involucrados se encuentran:

a. Gobierno como garante de la prestación de los servicios públicos domiciliarios: Instituciones encargadas de la política de seguridad energética, reguladores, etc.

b. Agentes y usuarios relacionados con la operación de infraestructura crítica: actuales y nuevos.

c. Agentes y usuarios relacionados con la operación del mercado: actuales y nuevos

d. Usuarios en general.

2.5 Objetivos

Como parte del análisis la Comisión plantea como objetivo general el siguiente:

> *Desarrollar una estrategia integral de ciberseguridad que prepare al sector eléctrico para enfrentar los riesgos asociados con incidentes de ciberseguridad que puedan afectar la operación del sector y poner en riesgo el suministro de energía eléctrica de manera oportuna y confiable*.

Con base en lo señalado en el documento *Cybersecurity White paper, MIT – 2016,* estos deberían ser los objetivos sobre seguridad digital para el sector eléctrico de cualquier país:

a. Debe ser capaz de operar en un ambiente con ciberataques

b. Reducir el efecto y el alcance de los ataques a los sistemas.

c. Adaptación de los sistemas, “tratamiento adecuado”.

d. Contar con estrategias de defensa cibernética por niveles, estar preparados para ataques extremos.

e. Monitoreo continuo y aplicación de mejores prácticas, no solo estándares.

f. Incorporación de mecanismos de seguridad digital desde el diseño de los sistemas.

g. Considerar procesos como el ciclo de vida de seguridad (identificar, proteger, detectar, responder y recuperar).

h. Establecer sistemas de respuesta efectiva, mejorar los sistemas de monitoreo y alarmas.

i. Contar con un sector resiliente, preparado para eventos de alto impacto.

j. Promover la innovación por parte de los agentes.

k. Determinar los costos asociados con la implementación de medidas de seguridad digital y su adecuada asignación entre los agentes y usuarios.

l. Privacidad y seguridad de información, definición de políticas de protección de datos y disponibilidad de información.

m. Grupos de seguimiento, creación de "comunidades" para el manejo de riesgos, prioridades de acción, soporte a otras empresas, integración del conocimiento y definición de tecnologías para enfrentar amenazas.

Esta lista de objetivos sirve como referencia para construir los objetivos de la estrategia de seguridad digital del sector eléctrico en Colombia.

2.6 Identificación de alternativas

En la Gráfica 7 se presentan algunas características de los principales instrumentos regulatorios de intervención, dentro de los que se encuentra la regulación tradicional y algunos instrumentos alternativos.

Aunque cada instrumento tiene características que lo hacen más o menos eficaz dependiendo de la estructura y de las condiciones de la actividad a regular, no son instrumentos mutuamente excluyentes en su implementación. El diagnóstico de los problemas puede concluir sobre la necesidad de utilizar varios instrumentos para alcanzar los fines de la regulación.

Gráfica 7 Instrumentos de intervención

	INSTRUMENTOS TRADICIONALES	INSTRUMENTOS ALTERNATIVOS			
Instrumentos	**Comando y control**	**Incentivos de mercado**	**Autorregulación por iniciativa de los agentes**	**Corregulación**	**Información y pedagogía**
Problema	Altos costos y riesgos ante libertad de agentes	Externalidades que afectan eficiencia	•Mercados de difícil supervisión •No exigible por el Estado	• Procesos heterogéneos • Necesidad de ser exigible por el Estado	Asimetrías de información
Cuando Aplica	•Mismo remedio para todos los agentes •Interés privado NO alineado con objetivo de la regulación	•Asignación de recursos escasos •Mercados dinámicos	•Objetivos claros, medibles •Intereses privados alineados con objetivo de la regulación	• Objetivos claros, medibles • Interés privado NO alineado con objetivo de la regulación	Reduce costos de búsqueda
Riesgos	•Rigideces en mercado •Ineficiencia x homogenización	Abuso de la regulación (debilidad en vigilancia)	Limitar la participación de otros agentes	Posible conflicto con regulación específica existente	No generar efectos inmediatos
Ejemplo	Obligación de hacer o no hacer	Señales de precios, derechos de uso	Manuales de buenas prácticas	Códigos de conducta Procedimientos	Información mínima al público

Dentro de las alternativas identificadas para cumplir con los objetivos regulatorios tratados en este documento se encuentran las siguientes:

a. Regulación tipo comando y control: definición de reglas precisas y detalladas para la implementación de estrategias de ciberseguridad y monitoreo.

b. Co-regulación: definición de lineamientos generales y el desarrollo recae en agentes que tengan capacidad técnica, como el CNO.

c. Auto-regulación: permitir que las empresas implementen voluntariamente estrategias de ciberseguridad.

d. Información - campañas educativas: dar información relevante a los agentes involucrados para que tomen conciencia de la importancia de implementar estrategias de ciberseguridad

Con base en los análisis realizados se plantea, de manera inicial, el uso de los instrumentos señalados en los literales b., c. y d.

De otra parte, se plantea que la estrategia integral de ciberseguridad y la regulación resultante hagan parte del código de redes, bien como parte de los reglamentos existentes o como un nuevo reglamento. Como parte del análisis regulatorio se identificará cual es el espacio más apropiado para incorporar las reglas relativas a la seguridad digital.

3 PROPUESTA DE TRABAJO DE LA ESTRATEGIA DE SEGURIDAD DIGITAL

3.1 Principales elementos

Los principales elementos de la propuesta de trabajo son los siguientes:

a. Definir una estrategia integral de ciberseguridad del sector eléctrico con la participación y el compromiso de todos los agentes, usuarios y entidades involucradas, para lo cual se plantea un proceso participativo.

b. Es importante tener en cuenta que para la definición de una estrategia integral de ciberseguridad del sector eléctrico se requiere la coordinación con las entidades encargadas de la seguridad digital.

c. Las alternativas planteadas buscan mitigar el riesgo asociado con los ciberataques a través de la implementación de estrategias sectoriales, las cuales requieren el compromiso de todos los agentes involucrados.

d. Se propone utilizar como referencia para el desarrollo de la estrategia el documento *Cybersecurity Strategy Development Guide*, publicado por *National Association of Regulatory Utility Commisiosioners, NARUC*.

e. Las empresas del sector: generadores, transmisores, distribuidores y comercializadores deben diligenciar el formulario adjunto a ese documento[6], esta información servirá de base para

[6] Cuestionario tomado del documento Understanding Cybersecurity Preparedness: Questions for Utilities, NARUC, 2019.

realizar un diagnóstico inicial de la ciberseguridad en el sector eléctrico. La información debe ser entregada a la Comisión a más tardar el 31 de octubre de 2019.

f. Hasta el 15 de octubre de 2019 se recibirán comentarios sobre la propuesta de trabajo contenida en los capítulos 2 y 3 de este documento, los comentarios deben realizarse en el formato Excel adjunto a este documento.

g. Como parte del proceso, la Comisión contratará un estudio de consultoría con expertos en ciberseguridad para obtener apoyo en la definición de la estrategia integral de ciberseguridad del sector eléctrico. Los resultados del estudio, servirán de base para construir la estrategia del sector.

h. En el cuarto trimestre de 2019 y el primero de 2020 se realizarán reuniones de trabajo con los principales agentes involucrados en temas de ciberseguridad del sector eléctrico, estas reuniones serán convocadas por la Comisión, o a solicitud de los agentes, gremios o interesados.

Como parte de este ejercicio, se espera contar con una estrategia que incluya como mínimo los siguientes aspectos:

- Definición de los objetivos estratégicos.
- Definición del alcance.
- Definición de indicadores de desempeño.
- Identificación de actores clave.
- Identificación de la estrategia.
- Plan de implementación de las estrategias.
- Cronograma de implementación.

3.2 Cronograma propuesto

a. Desarrollo del estudio de consultoría: cuarto trimestre de 2019.

b. Reuniones con interesados: cuarto trimestre de 2019 y primero de 2020.

c. Talleres: primer trimestre de 2020.

d. Elaboración propuesta para consulta: primer trimestre de 2020.

e. Revisión propuesta para consulta: segundo trimestre de 2020.

f. Definición de estrategia integral de seguridad digital del sector: segundo trimestre de 2020.

g. Expedición regulación sobre seguridad digital: segundo trimestre de 2020.

4 BIBLIOGRAFÍA

a. Risk Management in Critical Infrastructure Protection: An Introduction for State Utility Regulators. National Association of Regulatory Utility Commissioners (NARUC). September

2016. Recuperado el 12.08.2019 en https://pubs.naruc.org/pub/D10AF40A-AD04-3983-7421-9FBE970D87F3.

b. Cybersecurity: A Primer for State Utility Regulators Version 3.0. National Association of Regulatory Utility Commissioners (NARUC). January 2017. Recuperado el 12.08.2019 en https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

c. Cybersecurity Strategy Development Guide. National Association of Regulatory Utility Commissioners (NARUC). October, 2018. Recuperado el 12.08.2019 en https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204.

d. Understanding Cybersecurity Preparedness: Questions for Utilities. National Association of Regulatory Utility Commissioners (NARUC). June 2019. Recuperado el 12.08.2019 en https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220.

e. Cybersecurity Preparedness Evaluation Tool. National Association of Regulatory Utility Commissioners (NARUC). June 2019. Recuperado el 12.08.2019 en https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0.

f. Cybersecurity White Paper Cyril W. Draffin, Jr. Project Advisor, MIT Energy Initiative MIT ENERGY INITIATIVE UTILITY OF THE FUTURE 15 December 2016. Recuperado el 12.08.2019 en https://energy.mit.edu/wp-content/uploads/2016/12/CybersecurityWhitePaper_MITUtilityofFuture_-2016-12-05_Draffin.pdf.

g. CEER Cybersecurity Report on Europe's Electricity and Gas Sectors. Cyber Security Work Stream. Council of European Energy Regulators (CEER). Ref: C18-CS-44-04. October 2018. Recuperado el 12.08.2019 en https://www.ceer.eu/documents/104400/-/-/684d4504-b53e-aa46-c7ca-949a3d296124.

h. Buenas Prácticas para establecer un CSIRT nacional. Organización de Estados Americanos (OEA). Abril 2016. Recuperado el 12.08.2019 en https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

i. Impacto de los incidentes de seguridad digital en Colombia 2017. Organización de Estados Americanos (OEA). Ministerio de Tecnologías de la Información y de las Telecomunicaciones de Colombia. 2017. Recuperado el 12.08.2019 en https://publications.iadb.org/es/publicacion/17294/impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017.

j. Acuerdo 788 de 2015. Por el cual se aprueba la Guía de Ciberseguridad. Consejo Nacional de Operación. 3 de septiembre de 2015. Recuperado el 12.08.2019 en https://www.cno.org.co/content/acuerdo-788.

k. Acuerdo 1043 de 2018. Por el cual se aprueba la modificación del 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. Consejo Nacional de Operación. 26 febrero de 2018. Recuperado el 12.08.2019 en https://cno.org.co/content/acuerdo-1043-por-el-cual-se-aprueba-la-modificacion-del-documento-de-condiciones-minimas-de

l. Circular 034 de 2019. Modificación de la Guía de Ciberseguridad. Consejo Nacional de Operación. 03 Julio 2019. Recuperado el 12.08.2019 en https://www.cno.org.co/content/circular-34-modificacion-de-la-guia-de-ciberseguridad.

m. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016. Observatorio de la ciberseguridad en américa latina y el caribe. Banco Interamericano de Desarrollo. 2016. Recuperado el 12.08.2019 en https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe.

n. Referenciamiento equipo de respuesta a incidentes de seguridad informática del sector eléctrico colombiano, CSIRT SEC. Iniciativa Colombia Inteligente. Abril 2018.