TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1 , Enero-Abril, 2021, p.36-46 ISSN 1729-3804

CIBERSEGURIDAD EN LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS ELÉCTRICAS

Jeanders Silvio Hinojosa Calzada[1]

[1]Empresa Eléctrica Guantánamo, Calixto García #956,Guantánamo, Cuba.
[1]e-mail:jeanders@elecgtm.une.cu

RESUMEN

La ciberseguridad en las infraestructuras críticas supone un reto para cualquier organización que las posea ante el incesante aumento de los ciberataques en todo el mundo. En una realidad tecnológica como la actual, en la que los dominios físico y lógico son cada vez más interdependientes, esta tarea es todavía más necesaria pues las acciones en cualquiera de estos ámbitos pueden acarrear consecuencias devastadoras en ambos. Más importante aún en el caso de infraestructuras críticas vinculadas al sector energético, pues de su correcto funcionamiento dependen el resto de los servicios vitales con que cuenta una nación. La normativa cubana actual sobre ciberseguridad y protección física garantiza, hasta un punto, la protección de estas infraestructuras, pero existe mucha dispersión legislativa al respecto, al no disponerse de una norma jurídica específica con este objetivo, en concordancia con los estándares internacionales vigentes y en relación con la realidad cubana. El diseño de las medidas a adoptar para la protección de las infraestructuras críticas deben proporcionar un enfoque escalonado, permitiendo la detección del ataque en cada una de sus fases y el retardo o eliminación de la amenaza en el menor tiempo posible. Para ello, es necesario la utilización de esquemas de defensa en profundidad con acciones de control y mitigación de daños escalonados y no dependientes. Deben implementarse acciones que aseguren la resiliencia de los sistemas de control industrial así como su tolerancia a fallos.

PALABRAS CLAVES: Infraestructuras Críticas, Energía, Riesgos, Ciberseguridad.

CYBER SECURITY IN THE PROTECTION OF ELECTRICAL CRITICAL INFRASTRUCTURES

ABSTRACT

Cybersecurity in critical infrastructures poses a challenge for any organization that owns them in the face of the incessant increase in cyberattacks around the world. In a technological reality such as the current one, in which the physical and logical domains are increasingly interdependent, this task is even more necessary since actions in either of these areas can have devastating consequences in both. Even more important in the case of critical infrastructures linked to the energy sector, since the rest of the vital services that a nation has depends on its proper functioning. Current Cuban regulations on cybersecurity and physical protection guarantee, up to a point, the protection of these infrastructures, but there is a lot of legislative dispersion in this regard, as there is no specific legal norm with this objective, in accordance with current international standards and in relationship with the Cuban reality. The design of the measures to be adopted for the protection of critical infrastructures must provide a stepped approach, allowing the detection of the attack in each of its phases and the delay or elimination of the threat in the shortest possible time. For this, it is necessary to use defense-in-depth schemes with staggered and non-dependent damage control and mitigation actions. Actions must be implemented to ensure the resilience of industrial control systems as well as their fault tolerance.

INDEX TERMS: Critical Infrastructures, Energy, Risks, Cybersecurity.

1. INTRODUCCIÓN

El desarrollo acelerado de las Tecnologias de la Información y las Comunicaciones (TIC), asociado al alto grado de automatización de los procesos industriales que garantizan el funcionamiento de servicios como el energético, la distribución de agua y el gas, han abierto nuevos escenarios para la explotación de vulnerabilidades existentes en los sistemas que controlan estos procesos. Unido a esto, la necesidad de interconectar a Internet o a otras redes ajenas al proceso industrial, la red propia del proceso, ha incrementado la superficie de ataque hacia el sistema y expuesto vulnerabilidades en los mismos que anteriormente no podían ser aprovechadas por los ciberdelincuentes. Esto supone

Manuscrito recibido:15-12-2020, aceptado:19-12-2020
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1 , Enero-Abril, 2021, p.36-46 ISSN 1729-3804

la introducción en los procesos industriales de tecnologías como el Cluod Computing, el Big Data o la Internet Industrial de las Cosas (IIoT por sus siglas en ingles, Internet of Industrial Things), lo que implica la necesidad de tener en cuenta medidas para protegerse de las nuevas amenazas que se presentan en estas tecnologías.

La (IIoT) aprovecha las ventajas del Internet de las Cosas (IoT, en ingles Internet of things) en los Sistemas de Control Industrial (SCI) los cuales son una parte integral de las infraestructuras críticas y se han utilizado durante mucho tiempo para supervisar máquinas y procesos industriales. Estos actúan en tiempo real monitoreando e interactuando con los dispositivos, recopilando y analizando datos, y registrando todos los eventos que ocurren en los sistemas industriales [1].

En este escenario términos como el de Ciberseguridad se abren espacio cuando la protección física tradicional de estas infraestructuras no es suficiente para garantizar el 100% de la integridad de las mismas, siendo este uno de los temas relacionados con la gestión, operación y control de sistemas de energía [2], [3]. Otros términos como el de ciberseguridad corporativa y ciberseguridad operacional también se hacen presentes en este sentido. Aunque ambos poseen puntos en común difieren al establecer su enfoque respecto a la primera línea de defensa ante amenazas. En el caso de la ciberseguridad en las redes corporativas, la prioridad radica en garantizar la confidencialidad de la información transmitida a través de ella, no siendo así en las redes tecnológicas, donde la prioridad es la continuidad y estabilidad de los procesos. Su primera línea de defensa se basa en garantizar la disponibilidad de los procesos en un esquema ininterrumpido.

La ciberseguridad es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente de la información contenida en computadoras o que circula a través de las redes de computadoras. Existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que signifique un riesgo si la información confidencial llega a manos de otras personas.

La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», ya que esta última solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse también en formato impreso. A tenor de la legislación vigente en Cuba, la Ciberseguridad es el estado que se alcanza mediante la aplicación de un sistema de medidas (organizativas, normativas, técnicas, educativas, políticas y diplomáticas), destinado a garantizar la protección y el uso legal del ciberespacio. En la protección del ciberespacio se incluye la reducción de riesgos y vulnerabilidades, la creación de capacidades para detectar y gestionar eventos e incidentes y el fortalecimiento de la resiliencia [4].

El Estado cubano ha establecido para ello una serie de normativas entre las que destaca el Decreto 360 Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional y el Decreto-Ley 370 sobre la Informatización de la Sociedad. En este último, se regula la capacidad del Estado para identificar las Infraestructuras Críticas de las TIC y su seguridad y protección para un correcto funcionamiento [5], y las define como aquellas que soportan los componentes, procesos y servicios esenciales que garanticen las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública [6].

Esta investigación aborda desde una perspectiva amplia el estudio de las normativas vigentes sobre protección de infraestructuras críticas, en especial las eléctricas. Proporciona una aproximación a los principales conceptos en la materia, así como el proceso de identificación de riesgos y gestión de la seguridad de estas infraestructuras. Provee una breve panorámica sobre la estructura del Sistema Electroenergético Nacional y los sistemas de control, supervisión y adquisición de datos. Permite arribar a conclusiones sobre la necesidad de establecer normas específicas con un enfoque integral, que garanticen la protección de las infraestructura críticas eléctricas más allá de los niveles actuales de seguridad implementados y acorde a la diversidad de tecnologías instaladas en la infraestructura eléctrica cubana.

2. CIBERSEGURIDAD Y PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS ELÉCTRICAS

Seguridad de las TIC e infraestructuras críticas

La seguridad de las TIC, se entiende como el conjunto de medidas administrativas, organizativas, físicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las

TIC. El empleo del término seguridad informática, tiene igual significado a los efectos de la legislación cubana en la materia [7].

El término Infraestructura Crítica (IC) es empleado por los estados para definir instalaciones y sistemas sobre los que recaen servicios esenciales cuyo funcionamiento no permite soluciones alternativas. Las IC existentes en un estado se agrupan dentro de los sectores estratégicos: aquellos que son esenciales para la seguridad nacional o para el conjunto de la economía del país, defensa, energía, transporte, administración, financiero, entre otros. El concepto de infraestructura crítica abarca a todos aquellos activos que son tan vitales para cualquier estado, que su destrucción o degradación tendría un efecto debilitante sobre las funciones esenciales del gobierno, la seguridad nacional, la economía nacional, o la salud pública [8].

Según el USA Patriot Act de 2001 las infraestructuras críticas están compuestas por aquellos sistemas y sus activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la inhabilitación o la destrucción de estos sistemas y sus activos tienen un alto impacto en la seguridad económica nacional, en la salud pública, en la seguridad nacional, o en cualquier combinación de estas cuestiones [9].

La Directiva 2008/114/CE de la Unión Europea define las infraestructuras críticas como todo elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones [10]. Lo cierto es que la interrupción de un solo sector de la infraestructura crítica, como consecuencia de los desastres naturales o daños provocados por el hombre, es probable que tuviera efectos en cascada sobre otros sectores vitales para el desarrollo y desenvolvimiento de la economía y la sociedad en su conjunto.

Protección de la infraestructura crítica

La Protección de las Infraestructuras Críticas (PIC) surge como respuesta de los gobiernos a la necesidad de proteger el complejo sistema de infraestructuras que dan soporte y posibilitan el normal funcionamiento de los sectores productivos, de gestión y de la vida ciudadana en general. La mayoría de los países tienen IC asociadas a empresas privadas y han abordado esta problemática desde diferentes puntos de vistas, los cuales pueden resumirse en: establecimiento de un marco normativo estricto, fomento de las relaciones público-privadas y establecimiento de un marco normativo básico acompañado de una serie de medidas para fomentar las relaciones público-privadas. En Cuba, el estado controla o es propietario de la totalidad de las empresas que garantizan los servicios básicos, lo que le permite ejercer un mayor control y fiscalización sobre estos objetivos. En cualquier caso, el objetivo fundamental de la PIC es el desarrollo, implantación o mejora de las medidas de seguridad oportunas, tanto en su vertiente física como lógica/cibernética, que deben acometer los operadores o responsables de su gestión, de cara a garantizar un nivel de protección eficiente.

A nivel mundial, los gobiernos y las organizaciones internacionales no siempre coinciden en sus visiones sobre cómo proteger las infraestructuras. Las fuentes de información consultadas demuestran que los países en Norteamérica, América Latina, la Unión Europea y Australia/Nueva Zelanda son aquellos donde se han realizado mayores avances en la planificación de la protección de las infraestructuras críticas [11]. En Cuba, el Ministerio de Comunicaciones, en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, establece el Programa para el Fortalecimiento de la Ciberseguridad y coordina la participación en las actividades internacionales requeridas a ese fin e implementa su control y fiscalización [12]. Teniendo en cuenta que nuestro país tiene entre sus principales proveedores de equipos de comunicaciones a China, es preciso dedicar un momento al análisis de las acciones desarrollados por estos para fortalecer su ciberseguridad.

Recientemente las autoridades chinas regularon la seguridad de la computación en la nube, con un proyecto orientado a ejercer un mayor control sobre el tráfico y los contenidos y servicios que se almacenan y soportan sobre internet. La Administración del Ciberespacio de China (CAC), la Comisión de Desarrollo y Reforma, el Ministerio de Industria y Tecnología de la Información y el Ministerio de Finanzas de China se han puesto de acuerdo para elaborar un conjunto de normas y procedimientos para regular la seguridad de sus servicios en la nube. Las llamadas “Medidas de evaluación de seguridad de los servicios de computación en la nube”. Estas entraron en vigor el 1 de septiembre y establecen la creación de una nueva oficina dentro del CAC, que se encargará de controlar que se cumplan las nuevas reglas. “Estas medidas están formuladas para mejorar la seguridad y la capacidad de control de los servicios de computación en la nube adquiridos y utilizados por los órganos gubernamentales y del partido y los operadores de infraestructura de información crítica” [13].

Dada la sensibilidad de los datos y aplicaciones que estas organizaciones trasladan a la nube, las autoridades chinas han decidido endurecer mucho las medidas de seguridad para las empresas proveedoras de estos servicios. Y no solo se trata de las políticas de seguridad convencionales, sino que los reguladores han establecido controles muy estrictos

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1 , Enero-Abril, 2021, p.36-46 ISSN 1729-3804

en numerosos ámbitos. Por un lado, se encargarán de verificar desde las cuestiones técnicas y operativas de las plataformas de estos proveedores. Pero, por otro, investigarán a fondo las credenciales de los profesionales dedicados a trabajar en sus servicios, la solvencia de las empresas implicadas y su capacidad para garantizar la continuidad comercial de sus productos.

Rusia por su parte puso en vigor una nueva ley que obliga a las empresas de telecomunicaciones a implantar "medios técnicos" para redirigir todo el tráfico de Internet de Rusia a través de unos puntos de intercambio que administra o aprueba el organismo de las telecomunicaciones ruso, Roskomnazor. Esta agencia inspecciona el tráfico y tiene facultades para bloquear contenido prohibido, según recoge la ley. El proyecto de Internet soberana rusa establece que el país eurasiático construirá su propia versión del sistema de direcciones de red (conocido como DNS) para que RuNet pueda funcionar si se les corta el acceso a los servidores situados fuera de Rusia. Así, podría operar sin problemas de forma autónoma. El Kremlin trata a toda costa de mantener el intercambio de datos entre usuarios de Internet en Rusia dentro de sus fronteras. Un punto muy criticado por las organizaciones de derechos civiles, que alertan de que los usuarios críticos pueden volverse vulnerables. Sin embargo la administración rusa tiene como objetivo reducir la cantidad de tráfico que se enruta a través de servidores exteriores del 50% actual al 10% en 2024 [14].

Los gobiernos de los países latinoamericanos han encargado generalmente la protección de las infraestructuras críticas a los operadores de los sistemas y redes. Esta tarea se realiza siempre a través de una fuerte relación con las autoridades civiles y militares, con el fin de garantizar la protección de los activos y las redes que componen la infraestructura. La mayoría de los planes de protección de infraestructuras críticas en los países latinoamericanos se basan en los marcos de gestión de riesgos conocidos, ya sea el estándar australiano [15] o la norma ISO 31000 [16].

Infraestructuras eléctricas en Cuba

Los riesgos asociados a los sistemas eléctricos no están localizados solamente en la etapa de producción de electricidad; afectan en general a todas las etapas o segmentos: generación, transmisión, distribución y comercialización. Coincidentemente la infraestructura eléctrica cubana puede dividirse en los 4 segmentos antes mencionados, concentrándose en los tres primeros las mayores IC. El segmento de generación está compuesto por las centrales termoeléctricas, emplazamientos diésel y fuel oil, las plantas generadoras de electricidad a partir del gas acompañante de la extracción de petróleo y las de biomasa, los parques eólicos, los parques solares fotovoltaicos y las mini hidroeléctricas. En el caso de las grandes generadoras como es el caso de las centrales eléctricas, estas inyectan de forma directa a las líneas de transmisión de 110 kV y 220 kV, hasta las subestaciones de transmisión que la sirven hacia las redes de distribución de 33kV y desde ahí hacia pequeñas subestaciones de distribución que hace llegar la electricidad hasta nuestros hogares. Fig. 1.

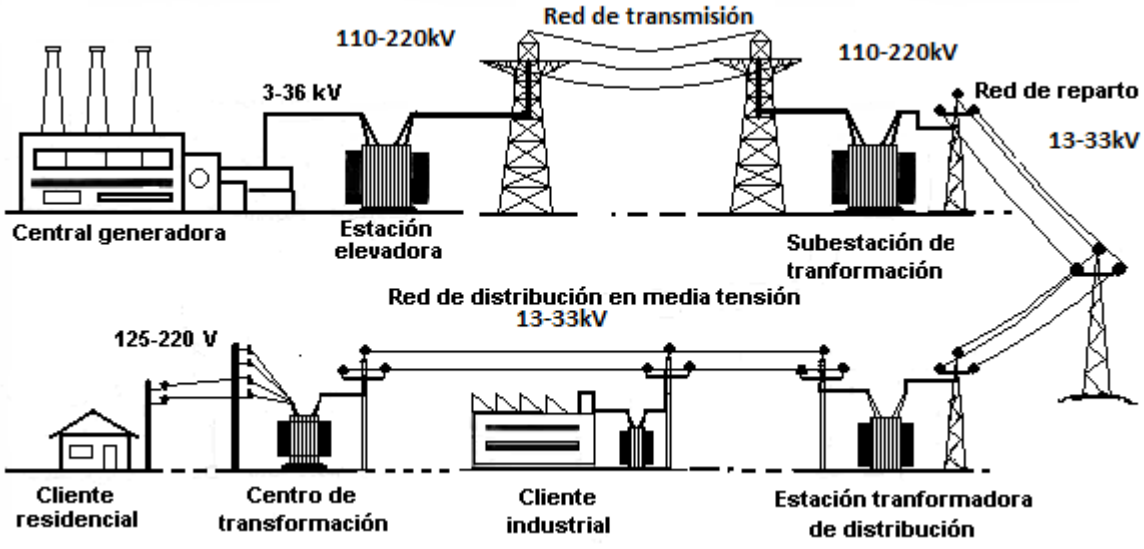

Figura 1. Representación del proceso de generación, transporte y distribución de energía eléctrica

Particularmente, la red de transporte de energía eléctrica está constituida por los elementos necesarios para llevar hasta los puntos de consumo y a través de grandes distancias la energía eléctrica generada en el subsistema de generación. Para ello, los niveles de energía eléctrica producidos deben ser transformados, elevándose su nivel de tensión. La Unión Eléctrica es el organismo responsable de llevar a cabo estos procesos y tiene como misión fundamental garantizar un servicio eficiente y de calidad a la población y la economía nacional [17].

Desde el punto de vista de la infraestructura, la red cuenta con algunos nodos críticos en los cuales el sistema requiere ser suficientemente seguro como para consentir una interrupción controlada en caso de un suceso no previsto. En otras circunstancias, los nodos críticos tienen que ser lo suficientemente resistentes como para garantizar el funcionamiento autónomo durante horas, días, semanas o incluso más tiempo, en caso que se requiera. En consecuencia, el reforzamiento del sistema de infraestructura eléctrica implica la realización de actividades que se extiendan más allá y con mayor profundidad que las acciones tradicionales.

Aunque es indudable la necesidad de proteger la red de transporte en alta tensión, también requieren cuidado las redes de distribución, que por medio de un extenso conjunto de instalaciones, permiten el suministro eléctrico a todos los consumidores. Es importante tener presente que la tarea de protección de estas infraestructuras tan extensas y numerosas debe realizarse en la medida que sea viable técnica y económicamente. Las redes eléctricas siempre han sido vulnerables y quienes precisan el aseguramiento de sus necesidades energéticas por cuestiones estratégicas adoptan habitualmente soluciones basadas en recursos disponibles in-situ [18]. Las instalaciones militares se dotan habitualmente de suministros eléctricos alternativos y autónomos que le garanticen respaldo al abastecimiento energético en caso de fallo de la fuente principal de suministro, de igual forma las IC deben dotarse de mecanismos similares.

Los sistemas de control industrial (SCI) constituyen una parte integral de las IC y requieren de altos niveles de seguridad. Han sido utilizados durante mucho tiempo para supervisar máquinas y procesos industriales. El sistema de control de supervisión y adquisición de datos (SCADA) es el subconjunto más grande de un SCI como se muestra en la Fig. 2. Este proporciona una interfaz gráfica de usuario (GUI) a través de su interfaz hombre-máquina (HMI). La HMI facilita a los operadores observar el estado del sistema, interactuar con los dispositivos IoT y recibir alarmas que indican comportamientos anormales. En el caso de Cuba, las redes tecnológicas no utilizan internet como soporte de comunicación. Estas utilizan canales específicos de comunicaciones con protocolos propios de automatización. El canal de transmisión de datos utilizado no queda expuesto en ninguno momento a la internet o intranet nacional, utilizándose para ello una red de área local virtual (VLAN, en ingles Virtual Local Area Network) propia de la Unión Eléctrica (UNE).

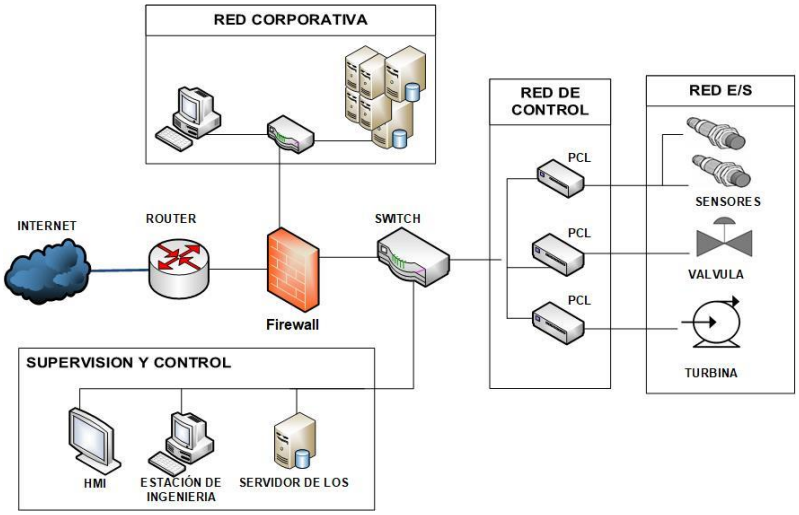

Figura 2. Representación de un SCADA.

Estos sistemas constan de cuatro subsistemas: red de E/S, red de supervisión, red de control y red corporativa. La red de E/S consta de dispositivos IoT (incluidos sensores y actuadores) desplegados en el proceso industrial. En Cuba la red de control incluye controladores lógicos programables (PLC) que detectan y gestionan directamente los procesos físicos. Dado que los sensores y actuadores no pueden comunicarse directamente, los PLC se utilizan para recopilar los datos detectados y enviar comandos a los actuadores. La red corporativa está formada por servidores, computadoras y otros usuarios conectados a la red y en ella eventualmente pueden brindarse otros servicios generales como la

Revista Telemática. Vol.20 No.1 , Enero-Abril, 2021, p.36-46 ISSN 1729-3804

transferencia de archivos, el alojamiento de sitios web, etc. Finalmente, el sistema de supervisión es el principal sub sistema responsable de asegurar, controlar y monitorear los dispositivos IoT.

Los SCI son en su mayoría sistemas de misión crítica con alta disponibilidad. Sus operaciones continuas producen una gran cantidad de datos que se pueden administrar a través del análisis de big data. En el pasado, estos sistemas eran independientes y estaban aislados del mundo, lo que los hacía menos sensibles a ataques maliciosos externos. Una mayor conectividad de los SCI con las redes corporativas y la utilización de Internet como plataforma de comunicación ha repercutido en que estos sean más vulnerables a ataques maliciosos. Debido a la naturaleza sensible de muchas aplicaciones industriales, la seguridad se ha convertido en la principal preocupación en los sistemas SCADA. Precisamente por esto, en Cuba los SCI están asilados de Internet, lo que reduce de forma considerable la superficie de ataque sobre los mismos. Esto provoca que la utilización de herramientas de análisis de datos requiera que estas sean implementadas garantizando la separación entre la red de control y el resto de las redes, garantizándose el flujo de datos siempre desde la primera y hacia el resto y nunca en sentido contrario.

Con el objetivo de fortalecer la seguridad en estos sistemas, se hace indispensable avanzar hacia la implementación del estándar IEC 61850 [19] para la automatización de las subestaciones eléctricas. Si bien el desarrollo original de este estándar tuvo sus raíces en abordar los requisitos de la subestación y los sistemas de control y protección, las nuevas ediciones de IEC 61850 y los estándares asociados a este amplían la funcionalidad más allá de la subestación a otros dominios del sistema de energía. Los nuevos modelos de datos y funciones ya cubren la gestión de parques eólicos; centrales hidroeléctricas y recursos energéticos distribuidos. Con el tiempo, se espera que se agreguen modelos y funciones adicionales para cubrir todos los aspectos de la gestión de datos para la operación del sistema eléctrico. IEC 61850 es un estándar complejo y rico en funciones que facilita la creación de una potente automatización de sistemas. Ya se ha implementado en miles de nuevos sistemas de automatización de subestaciones en todo el mundo y está ganando terreno en otros dominios de sistemas de energía [20].

Sin embargo, para su implementación en Cuba, es preciso tener en cuenta que el estándar IEC 61850 es producido y gestionado por los Estados Unidos. Esto provoca un nivel de dependencia tecnológica de sus estructuras de desarrollo, dígase Comisión Internacional de Electrónica (IEC), Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), entre otras. Durante años el país ha sido objeto de una política hostil por parte del gobierno norteamericano. Es entonces perfectamente razonable prever que la implementación del estándar, unido a la utilización de Internet, constituye una oportunidad para que las agencias especiales norteamericanas accedan a los procesos de IC sin ser detectados, realizando acciones de ataque o monitoreo de las mismas.

Los sistemas eléctricos controlados (WAC) dependen en gran medida de la seguridad de las redes de comunicación subyacentes. La ubicación óptima de dispositivos de Sistemas de Transmisión de Corriente Alterna Flexibles (FACTS) y la seguridad cibernética del intercambio de datos asociados a estos, son cruciales para la capacidad de control de las redes eléctricas de área amplia. Recientes estudios presentan una perspectiva teórica de grafos novedosa basada puramente en las características topológicas de los gráficos físicos subyacentes de las redes eléctricas. Con este fin se utiliza el principio de coincidencia máxima (MMP) para encontrar el conjunto de dispositivos FACTS necesarios para la controlabilidad de la red [21].

El aumento de los requerimientos de seguridad va aparejado al proceso de mejora continua de los servicios a la población, lo que hace imprescindible la necesidad de incrementar la fiabilidad de sus actividades de suministro. Sin embargo, teniendo en cuenta que se trata de una infraestructura tan vasta, es imposible garantizar su seguridad física al 100% [22]. En general, se detecta una alta vulnerabilidad del sistema eléctrico en aquellos nodos de la red donde un fallo pueda propagarse en cascada y causar apagones en una región determinada. Para evaluar el nivel de amenaza, deben alcanzarse grados superiores de coordinación entre todas las empresas que contribuyen al funcionamiento del Sistema Eléctrico Nacional.

Identificación de riesgos y gestión de la seguridad en infraestructuras críticas eléctricas

El sector eléctrico concentra una importante cantidad de estudios y análisis, dada la alta interdependencia de todos los sectores de actividad con las infraestructuras de suministro de electricidad. De ahí que las mayores medidas de seguridad se enfoquen en las grandes unidades generadoras, los grupos de generación de diésel y fuel oil y las subestaciones eléctricas de 110 kV y 220 kV. De igual forma, los parques solares fotovoltaicos, lo parques eólicos y las mini hidroeléctricas se suman al conjunto de objetivos antes mencionados considerados como estratégicos por

cuanto inciden de forma determinante en la generación y distribución de energía eléctrica y por tanto en la seguridad energética cubana. Se incluyen en esta denominación los nodos y subnodos de redes y servicios de comunicaciones que garantizan la interconexión, operación y mantenimiento del Sistema Electroenergético Nacional (SEN).

En Cuba cada entidad que haga uso de las TIC diseña, implanta, gestiona y mantiene actualizado un Sistema de Seguridad, a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos dichos medios [23]. El Sistema de Seguridad de las Tecnologías de la Información y la Comunicación vigente tiene como objetivo minimizar los riesgos sobre los sistemas informáticos y garantizar la continuidad de los procesos informáticos.

El diseño de este sistema y la elaboración del Plan de Seguridad de cada entidad se realizan en correspondencia con la metodología establecida al respecto por el Ministerio de Comunicaciones. Estas se regulan en la Resolución 129/2019, específicamente en su anexo único. La metodología para la gestión de la seguridad informática tiene como objeto determinar las acciones a realizar en una entidad durante el diseño, la implementación y posterior operación de un Sistema de Gestión de la Seguridad Informática (SGSI), y está compuesta por dos partes. La primera dedicada al SGSI y la segunda a la estructura y contenido del Plan de Seguridad Informática. Este documento constituye un complemento a lo exigido en el Decreto de Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional y el Reglamento de Seguridad para las Tecnologías de la Información y la Comunicación en cuanto a la obligación de diseñar, implantar y mantener actualizado un Sistema de Seguridad Informática, a partir de los bienes a proteger y de los riesgos a que están sometidos. Esta metodología garantiza un proceso continuo de mejoras a través de la evaluación periódica de los riesgos a los que están sometidos las tecnologías. No obstante, ninguna de las normas antes mencionadas tiene como objetivo la protección de las infraestructuras de los SCI.

Para el caso concreto de las infraestructuras del sector eléctrico, la Unión Eléctrica establece los procedimientos necesarios para el cumplimiento de las normas vigentes. De igual forma implementa listas de chequeo periódicas para velar por el cumplimiento de las normas de seguridad informática y tecnológicas, aplicando un enfoque holístico de la seguridad de las tecnologías. No obstante, la diversidad de tecnologías que se manejan y el perfeccionamiento de los sistemas de trabajo implican una constante actualización de las mismas.

La identificación de riesgos y amenazas al sistema de infraestructura. Constituye la piedra angular de la actuación en la protección de infraestructuras críticas, ya que los criterios para la selección de las posibles amenazas y el análisis detallado de sus componentes de riesgo serán determinantes en la calidad del proceso de gestión de riesgos en IC. La identificación de riesgos es la etapa fundacional de cualquier proceso de gestión de riesgos, y es previa a la valoración, definición e implementación de acciones para mitigarlos.

En un marco de gestión de riesgos, el proceso de identificación se enfoca en detectar cuáles son las fuentes principales de riesgo [24], [25].En resumen, el propósito al realizar el proceso de identificación de riesgos se limita a un ejercicio cualitativo, mediante el cual se definen los posibles riesgos en el sistema, y se obtiene un listado completo de riesgos y sus componentes aplicable a la cadena de valor y al ciclo de vida de la red de infraestructura [26]. Una revisión del estado del arte de las herramientas y metodologías para la identificación de riesgos permite concluir que la aplicación sistemática de una metodología debe seleccionar activos críticos, verificar interdependencias e impactos económicos y sociales de los riesgos, desde el punto de vista organizacional, empresarial y gubernamental [27].

La identificación de riesgos por medio de las herramientas y metodologías citadas tiene aplicación en los subsistemas de la cadena de valor de la infraestructura eléctrica, con especial énfasis en la prevención de amenazas sobre los siguientes aspectos:

- Activos, edificios, equipos y sedes de las empresas propietarias/operadoras de la infraestructura eléctrica.
- Plantas de generación eléctrica.
- Redes de transporte y de distribución.
- Interdependencias con otros sectores de infraestructura crítica.
- Nodos críticos de la red eléctrica.
- Regulaciones y políticas que impactan la operación del sistema.
- Impacto sobre la población afectada.

Marco legal para la protección de infraestructuras críticas en Cuba

Cuba no dispone de una ley específica para la PIC, lo que provoca una considerable dispersión legislativa en este sentido. Su protección se aborda fundamentalmente desde la protección de los Sistemas de Control Industrial (SCI),

Revista Telemática. Vol.20 No.1 , Enero-Abril, 2021, p.36-46 ISSN 1729-3804

la protección física de los activos informáticos según las funciones que realizan y la protección de las instalaciones consideradas como objetivos estratégicos.

Respecto a la protección de los SCI, el Ministerio de Energía y Minas (MINEM) aprobó la resolución 254, Reglamento de Seguridad de los Sistemas de Control Industrial para el MINEM. Esta tiene como objeto establecer un conjunto de regulaciones y medidas de obligatorio cumplimiento para todo el sistema empresarial atendido y entidades adscritas y subordinadas al organismo. Establece un conjunto de medidas a implementar que aseguren el nivel de seguridad mínimo razonable en los SIC, y contribuyan a evitar la comisión de acciones intencionales o involuntarias sobre los mismos que produzcan afectaciones o daños al proceso tecnológico, su equipamiento o a las personas. La norma proporciona un programa de seguridad para sistemas de control y automática industrial, que incluye medidas adicionales adecuadas a nuestras condiciones, en correspondencia con la norma IEC 61443-2 "Redes de Comunicación lndustriales. Seguridad de Sistemas y Redes y las NIST 800-82 [28] y NIST 800-53 [29].

Esta norma provee a los especialistas en seguridad industrial, automáticos y especialistas en seguridad tecnológica un punto de partida para la elaboración del Plan de Seguridad del Sistema de Control Industrial el cual debe garantizar la protección de la instalación tecnológica, los medios técnicos del sistema de control y la integridad de las personas. Este plan incluye los siguientes objetivos:

a) Actualización del levantamiento de riesgos.
b) Garantizar la continuidad de los procesos productivos ante la ocurrencia incidente que afecten a los Sistemas de Control Industrial.
c) Minimizar los riesgos que afectan a los Sistemas de Control Industrial.

La Ley No. 1321, de fecha 27 de noviembre de 1976, reguló la política de seguridad y protección física en las instalaciones y demás bienes sociales asignados a los ministerios, organismos centrales y entidades estatales de producción y de servicios. Siendo así, cada entidad solicitaba la declaración como objetivos estratégicos de aquellas instalaciones dedicadas a la producción y servicios vitales para la economía y el consumo de la población tuvieran una importancia estratégica para la economía y la defensa del país.

En este marco, el Ministerio de la Industria Básica, actualmente Ministerio de Energía y Minas (MINEM), solicitó se declararan como objetivos de carácter estratégico nacional a los centros e instalaciones siguientes:

- Centrales de generación eléctrica.
- Subestaciones a 220 kV y 110 kV del SEN.
- Despachos de carga eléctrica nacional y territoriales.
- Refinerías de petróleo.
- Base de supertanqueros de Matanzas.
- Las terminales 221, 223, 230 de Ciudad de La Habana y el depósito de Pastelillo en Nuevitas, Camagüey.
- Planta de gas manufacturado de Melones y Marianao.
- Bases de amoniaco de Nuevitas y otros grandes depósitos de amoniaco.
- Electroquímica de Sagua.

Esto se hizo efectivo a través del Decreto-Ley 200 de 1995. En este se otorgan entre otras facultades la responsabilidad a los diferentes organismos implicados con la capacitación del personal que labora en dichos centros, la adquisición de técnicas necesarias para el cumplimiento de la seguridad y protección de los objetivos y el cumplimiento de las normas de seguridad industrial vigentes en el país. En 1998 fue aprobado el Decreto-Ley 186, sobre el Sistema de Seguridad y Protección Física, con su correspondiente reglamento, el cual tenía como objeto establecer y regular el sistema de seguridad y protección física y los servicios a prestar en esta materia. En este no se hace referencia a la PIC sino a las normas generales para garantizar la seguridad y protección.

A lo interno del MINEM, la resolución 293/2014 constituye el Sistema de Seguridad y Protección del organismo y tiene entre sus objetivos lograr el perfeccionamiento de los Sistemas de Seguridad y Protección Física (SSPF) en todas las entidades que conforman el Ministerio. Además, se definen los principios y funciones del dicho sistema, dentro

de las cuales figura el lograr que los objetivos categorizados como estratégicos y de relevante importancia económica trabajen bajo el régimen de máxima seguridad y este se aplique de forma integral teniendo en cuenta las amenazas definidas en el subsistema operativo y los parámetros de máxima seguridad.

Con la aprobación del Decreto-Ley 370 de 2018, se alcanza una forma superior de organización para la protección de las PIC, al actualizar las categorías de edificios e instalaciones según el valor de los activos informáticos que se ubican en estos. La norma establece que, en los edificios e instalaciones de cada entidad, su dirección determina las áreas o zonas controladas con requerimientos específicos, protegidas por un perímetro de seguridad definido, en dependencia de la importancia de los bienes informáticos que contiene y su utilización de acuerdo con la denominación siguiente:

a) Áreas limitadas: en las que se concentran bienes informáticos de valor medio, cuya afectación puede determinar parcialmente los resultados de la gestión de la entidad o de terceros.

b) Áreas restringidas: donde se concentran bienes informáticos de alto valor e importancia crítica, cuya afectación pueda paralizar o afectar severamente la gestión de sectores de la economía o de la sociedad; territorios o entidades.

c) Áreas estratégicas: en las cuales se concentran bienes informáticos de alto valor e importancia crítica, que inciden de forma determinante en la seguridad y la defensa nacional; la seguridad aeronáutica; biológica; industrial; la generación y distribución de energía eléctrica; las redes informáticas y de comunicaciones del país; las relaciones exteriores y de colaboración; la economía nacional; las investigaciones científicas y el desarrollo tecnológico; la alimentación de la población; la salud pública, y el suministro de agua u otra que por su importancia se considere necesaria.

No obstante, los avances alcanzados, no existe en la actualidad ninguna disposición legal sobre la seguridad de los SIC. El Decreto-Ley 370 de 2018 define solo las infraestructuras críticas vinculadas a la informática y las comunicaciones dejando un vacío legal en el resto de los sistemas, incluyendo los SCI. Se impone la necesidad de avanzar en una norma con enfoque integral que regule la PIC, de acuerdo a los estándares internacionales establecidos y en consonancia con la realidad cubana.

3. CONCLUSIONES

La PIC eléctricas adquiere una especial importancia al constituir estas el motor impulsor del resto de las actividades económicas y sociales del país. La legislación cubana actual garantiza los niveles de protección mínimos razonables para la protección de estas infraestructuras, pero no se dispone de una norma que regule la PIC desde un enfoque integral, de acuerdo a los estándares internacionales vigentes y en relación con la realidad cubana actual. El diseño de las medidas a adoptar para la PIC, en especial de las eléctricas, deben proporcionar un enfoque escalonado, permitiendo la detección del ataque en cada una de sus fases y el retardo o eliminación de la amenaza en el menor tiempo posible, utilizando para ello esquemas de defensa en profundidad, con acciones de control y mitigación de daños escalonados y no dependientes. Estas medidas deben asegurar la resiliencia de los SCI así como su tolerancia a fallos lo que permitirá alcanzar una mayor efectividad al momento de protegerlos y defenderlos. Es vital establecer procedimientos proactivos que permitan adelantarse a las acciones de los posibles atacantes y establecer desde el presente las líneas de acción ante cada posible amenaza con el objetivo de minimizar los daños y garantizar la continuidad del proceso productivo.

RECONOCIMIENTOS

El autor desea agradecer al compañero Ernesto Trujillo Rodríguez, Jefe de Grupo de Seguridad Tecnológica de la Unión Eléctrica por su colaboración en la revisión de este artículo y sus aportes al perfeccionamiento del mismo.

REFERENCIAS

[1] M. Zolanvari, Marcio A. Teixeira , Lav Gupta, Khaled M. Khan, Raj Jain, «Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things»,IEEE Internet of Things Journal, vol. 6, No. 4, 2019.

[2] B. Li, Y. Chen, S. Huang, R. Yao, Y. Xia y S. Mei, " Evolución gráfica modelo de juego tradicional de intrusión basada en virus al sistema de energía a largo plazo evaluación de riesgos de ciberseguridad ", IEEE Access , vol. 7, págs. 178605–178617, 2019, doi: 10.1109 / ACCESS.2019.2958856.

[3] M. Z. Gunduz and R. Das, ‘‘Cyber-security on smart grid: Threats and potential solutions,’’ Comput. Netw., vol. 169, Mar. 2020, Art. no. 107094, doi: 10.1016/j.comnet.2019.107094.

[4] Decreto No. 360 Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, artículo 5. Decreto No. 360 del 31 de mayo de 2019.
[5] Decreto-Ley No. 370 Sobre la Informatización de la Sociedad en Cuba, artículo 45. Decreto-Ley No. 370 del 17 de diciembre de 2018.
[6] Decreto-Ley No. 370 Sobre la Informatización de la Sociedad en Cuba, artículo 46. Decreto-Ley No. 370 del 17 de diciembre de 2018

[7] Decreto-Ley No. 370 Sobre la Informatización de la Sociedad en Cuba, artículo 12. Decreto-Ley No. 370 del 17 de diciembre de 2018.
[8] R. Hull, D. Belluck, & C. Lipchin, "A framework for multi-criteria decision making with special reference to critical infrastructure: policy and risk management working group summary and recommendations" in *Ecotoxicology, Ecological Risk Assessment and Multiple Stressors*. Springer, pp. 355-370, 2006.
[9] US Dept Energy Office, "Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities", Washington DC (USA): U.S. Department of Energy, Office of Energy Assurance, p. 26, 2002.
[10] Consejo Europeo. "Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección". Directiva 114 CE/2008.

[11] G. J. Correa Henao & J. M Yusta Loyo, «Seguridad energética y protección de infraestructuras críticas» Lámpsakos No.10, pp. 92-108, jul-dic 2013, ISSN: 2145-4086.
[12] Decreto-Ley No. 370 Sobre la Informatización de la Sociedad en Cuba, artículo 48. Decreto-Ley No. 370 del 17 de diciembre de 2018.
[13] «Las autoridades chinas quieren regular la seguridad de la computación en la nube», oct. 18, 2019. https://www.ittrends.es/negocios/2019/07/las-autoridades-chinas-quieren-regular-la-seguridad-de-la-computacion-en-la-nube (accedido oct. 18, 2019).
[14] «Rusia aprueba la ley que refuerza su capacidad de censura en internet», abr. 16, 2019, https://elpais.com/internacional/2019/04/16/actualidad/1555427376_009178.html (accedido abr. 16, 2019).
[15] «Estándar Australiano de Administración del Riesgo», pp 36, 1999, AS/NZS 4360.
[16] «ISO International Standard Organization, Risk Management», ISO 3100:2010.
[17]«Todos los cubanos ya disponen de servicio electrico», sep. 12, 2019. http://www.cubadebate.cu/especiales/2018/12/14/todos-los-cubanos-ya-disponen-de-servicio -electrico/#.Xbc4DPzB_IU (accedido sep. 12, 2019).
[18] P. Curtis, Maintaining Mission Critical Systems in a 24/7 Environment, ed. J.W. Sons. Rosenwood, MA (EEUU), 2011.
[19] Communication networks and systems for power utility automation, IEC Standard 61850, 2019
[20] A. West. Integrating IEC 61850 & IEEE 1815 (DNP3), SUBNET Solutions, Inc, 2018
[21] H. Parastvand, O. Bass, M. A. S. Masoum, A. Chapman, and S. Lachowicz, "Cyber-Security Constrained Placement of FACTS Devices in Power Networks From a Novel Topological Perspective," IEEE Access, vol. 8, pp. 108201–108215, 2020, doi: 10.1109/ACCESS.2020.3001308
[22] C. Masterson, « The Crash Course», PhD,US, 2009.
[23] Decreto No. 360 Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, artículo 18. Decreto No. 360 del 31 de mayo de 2019.
[24] «Estándar Australiano de Administración del Riesgo», pp 36, 1999, AS/NZS 4360.
[25] «Norma Técnica Colombiana para 5254 la Gestión de Riesgos», pp 44, 2004.
[26] J. Johansson, «Risk and Vulnerability Analysis of Interdependent Technical Infrastructures», PhD, University of Lund, Sweden, 2010.
[27] J. M. Yusta, G. J. Correa, and R. Lacal Arántegui, «Methodologies and applications for critical infrastructure protection: State-of-the- art», Energy Policy, vol. 39, pp. 6100-6119, 2011.
[28] K. Stouffer, V. Pillitteri , S. Lightman, M. Abrams, A. Hahn, «Guide to Industrial Control Systems (ICS) Security» US, 2015. http://dx.doi.org/10.6028/NIST.SP.800-82r2.
[29] Join Task Force, «Security and Privacy Controls for Information Systems and OrganizationsNIST Special Publication 800-53. Revision 4»,US, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

SOBRE EL AUTOR

Graduado de Ingeniero en Ciencias Informáticas en las Universidad de Ciencias Informáticas de La Habana en 2010, Graduado de Licenciado en Derecho (2017) y Master en Ciencias Pedagógicas, mención Tecnología Educativa (2018) en las Universidad de Guantánamo. Profesor Asistente de la Facultad de Ingeniería y Ciencias Técnicas de la

Universidad de Guantánamo donde ha impartido las asignaturas de Sistemas de Bases de Datos, Configuración de Redes, Sistemas Operativos y Seguridad Informática. Se desempeña como especialista en seguridad informática y tecnológica en la Empresa Eléctrica Guantánamo. Miembro de la Unión de Informáticos de Cuba y de la Unión de Juristas de Cuba. Obtuvo la categoría de Destacado con el trabajo Delitos Informáticos. Propuestas para su configuración en el ordenamiento penal cubano presentado en la XVII Conferencia Anual de la Unión de Juristas Guantánamo y Segundo Premio en el Concurso Anual de la Sociedad Cubana de Derecho e Informática con el trabajo ¨Informática Criminalística: Una especialidad en desarrollo. Identificador ORCID https://orcid.org/0000-0001-7901-8753

CONFLICTO DE INTERESES

No existe conflicto de intereses entre el autor y la Unión Eléctrica en relación al contenido del artículo.

CONTRIBUCIONES DE LOS AUTORES

- **Jeanders Silvio Hinojosa Calzada**: Conceptualización, preparación, creación y desarrollo del artículo. Revisión crítica de cada una de las versiones del borrador del artículo y aprobación de la versión final a publicar.