Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Maestría
en
Seguridad Informática

Ciberseguridad Industrial

Situación actual de ciberseguridad en sistemas de control industrial en Argentina y resto de Latinoamérica

Autor: Ing. Erick Pazmiño

Director de Trabajo Final de Maestría : Dr. Pedro Hecht

Año 2020
Cohorte 2018

Declaración Jurada de origen de los contenidos.

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Erick Santiago Pazmiño Sosa

DNI 95817370

Resumen.

Este trabajo presenta una comparativa acerca del estado actual de ciberseguridad de las distintas industrias como energética, Oil&Gas y manufactura de la Argentina y otros países en Latinoamérica donde se han realizado evaluaciones de ciberseguridad. Este trabajo presentará algunos de los hallazgos más relevantes que se han encontrado. De estos hallazgos se presentarán los riesgos que estos representan para el *facility,* así como las recomendaciones para mitigar ese riesgo.

En el pasado no había requisitos para tener los ambientes de IT y OT conectados; por lo tanto, estaban completamente separados y gobernados independientemente por IT e Ingeniería. Sin embargo, hoy en día, debido a la necesidad por mejorar la eficiencia y reducir los costos, se requiere una conectividad avanzada entre las redes de IT y OT. Esto trae consigo riesgos de ciberseguridad que en tiempos pasados no se consideraban, así como una confusión con respecto a la gobernabilidad, la gestión de riesgos y la eficacia de la aplicación del control entre la TI y la ingeniería.

Palabras claves.

ICS - IIoT - SCADA – riesgos - ciberseguridad - smart – energía – concientización.

Tabla de contenido

Tabla de Figuras

Agradecimientos.

Quiero agradecer a Dios, por permitirme llegar hasta acá y darme la salud y sabiduría para poder culminar con éxito esta maestría que tanto me brindó.

A mis padres, hermanos y tías que a pesar de estar lejos nunca dejaron de apoyarme y sin ellos esto no hubiera sido posible. Gracias por darme ánimos para continuar con mis estudios, aunque haya sido fuera de mi país.

A mi novia, que siempre me dio aliento y estuvo conmigo durante toda mi carrera apoyándome y brindándome su hombro en buenos y malos momentos.

A todo el personal y profesores de la Maestría en Seguridad Informática, por brindar siempre sus mejores esfuerzos en pro de fortalecer nuestras virtudes académicas y profesionales.

1 . Introducción.

1.1. Planteo del problema.

Como se mencionó anteriormente, en la actualidad en la región Latinoamericana no se cuenta con un nivel de conciencia suficiente respecto a los riesgos que corren las compañías al no poseer un programa de Ciberseguridad Industrial. Además, que en varios países no se cuenta con una normativa o regulación que obligue a las empresas a tomar en cuenta este tema. Por este motivo, es importante mostrar a través de los hallazgos encontrados en las evaluaciones de ciberseguridad industrial , cuáles son los riesgos a los que se exponen las compañías y cuáles serían las consecuencias de la explotación de alguno de estos riesgos de modo que las compañías pueden tener una conciencia más seria acerca de la importancia de la ciberseguridad en infraestructuras críticas.

1.2. Estado actual.

América Latina es una de las regiones más importantes del mundo en cuanto a sus recursos naturales. Las grandes potencias necesitan recursos naturales para mantener su poder y continuar con el proceso de desarrollo. Un ejemplo de esto es China o EE.UU. En particular, China ha estado haciendo importantes inversiones en este tema en la región durante los últimos años.

El estudio está enfocado en Argentina puesto que aquí se descubrió hace unos años una gran zona denominada Vaca Muerta con petróleo y gas de esquisto, lo que convirtió a Argentina en el segundo país más grande con gas de esquisto. El cuarto país más grande del mundo con petróleo de esquisto. Y este ha sido el motivo por el cual actualmente se tienen varios proyectos en ejecución en lo que respecta ciberseguridad industrial. Actualmente, en el sector privado las empresas se dieron cuenta de que podían ser parte de un ataque cibernético. Este entendimiento, se aprovecha de empresas similares que sufrieron un Ciberataque, por ejemplo, el caso de PEMEX en el Petróleo y Gas quienes sufrieron un ciberataque. Así como en Brasil, se determinó que varias empresas fueron víctimas de ataques de malware que les produjeron desde problemas de rendimiento en sus instalaciones hasta una parada de sus líneas de producción. Las empresas más importantes de la región están empezando a desarrollar sus equipos de

Ciberseguridad Industrial con miembros multidisciplinarios, que componen gente del negocio de operaciones y gente de IT.

Por otro lado, está el sector público donde no se está prestando atención a la preocupación por la seguridad cibernética. La mayoría de las industrias están en un estado de desconocimiento. Es fundamental prestar atención en estas empresas puesto que los principales sectores críticos pertenecen al Estado o están bajo su control. Actualmente en Argentina, no existe una regulación de ciberseguridad para nuestra infraestructura crítica.

1.3. Justificación

En estos momentos donde la integración entre las redes corporativas y las redes industriales están emergiendo se abre un nuevo camino hacia los elementos críticos de un Sistema de Control Industrial, lo cual significa que un atacante que pudiese llegar a encontrar este camino para su posterior explotación sería capaz de causar grandes catástrofes. De acuerdo con distintas evaluaciones de ciberseguridad realizadas en diferentes rubros de la industria tales como Oil&Gas, generación de energía y manufactura se ha notado que las empresas de Latinoamérica aún no tienen una suficiente conciencia acerca de los riesgos que puede representar la existencia de un incidente de ciberseguridad en sus entornos. Esto ha motivado el desarrollo de este trabajo concientizar a los usuarios acerca de la importancia de la ciberseguridad en infraestructuras críticas a la vez que se recomiendan las medidas que se deben tomar a fin de reducir los vectores de ataque que se podrían presentar.

1.4. Hipótesis.

Las infraestructuras críticas de Argentina y resto de región Latinoamericana requieren empezar a desarrollar un programa de ciberseguridad industrial que sea flexible y permita mantener las operaciones de estas seguras. Sumado a esto, este programa de ciberseguridad industrial debería estar alineado con las características propias de la organización.

1.5. Objetivos.

- Definir los rubros que entrarán en alcance para la presentación de hallazgos.
- Presentar los hallazgos de las evaluaciones de ciberseguridad.
- Presentar los riesgos que representan los hallazgos encontrados.
- Determinar medidas de mitigación para estos riesgos.
- Presentar un resumen general de las estadísticas de los hallazgos.

1.6. Alcances y limitaciones de la propuesta.

- El alcance de la propuesta es presentar los hallazgos más relevantes que lograron ser identificados en los assessments de ciberseguridad industrial que fueron realizados a las distintas compañías en Argentina y alrededor de Latinoamérica, a fin de proponer medidas de mitigación que puedan prevenir que demás empresas sean víctimas de estas vulnerabilidades.
- Dentro de las limitaciones establecidas, está el trabajar con información confidencial de las compañías que han sido evaluadas, por lo cual en el documento final no contendrá nombres de las empresas involucradas ni detalles confidenciales.

2. Importancia de Latinoamérica y Argentina

2.1. ¿Por qué Latinoamérica?

Latinoamérica está conformada por un grupo de países ubicados en el Hemisferio Occidental, donde se hacen predominantes los idiomas español y portugués. El término Latinoamérica proviene del hecho que las lenguas predominantes de los países se originaron con la lengua latina.

América Latina está conformada por 20 países y 14 territorios dependientes. Tiene una superficie aproximada de 19.197.000 km^2, lo cual representa alrededor del 13% de la superficie terrestre de la Tierra. De acuerdo con las últimas estadísticas del 2020 se estima que esta región tiene una población de más de 652 millones. [1]

Ilustración 1. Mapa Latinoamérica

Fuente: https://en.wikipedia.org/wiki/Latin_America

América Latina es una de las regiones más importantes del mundo en cuanto a sus recursos naturales. Las grandes potencias necesitan recursos naturales para mantener su poder y continuar con el proceso de desarrollo. Un ejemplo de esto es China o EE.UU. En particular, China que ha estado haciendo importantes inversiones en este tema en la región durante los últimos años.

A lo largo de la historia, la región Latinoamericana ha basado sus economías a través de la riqueza en recursos naturales que esta posee. La producción de recursos naturales tales como metales preciosos, azúcar,

granos, café, cacao, petróleo, cobre, entre otros han hecho que varios países de esta región tengan picos de prosperidad en distintos períodos de la historia.

Las estadísticas indican que en América Latina se produjo alrededor del 80% de la plata del mundo en un periodo comprendido entre los siglos XVI y XIX. Esto fue aprovechado por Europa, China e India para sentar una base sólida de sus sistemas monetarios. [2]

2.2. Argentina y su relevancia en la región

Argentina, es un país situado en la mitad sur de Sudamérica. Cuenta con una superficie continental de 2.780.400 km2. Así mismo, Argentina es el octavo país más grande del mundo, y el segundo más grande de Sudamérica después de Brasil. El país tiene alrededor de 44.938.712 habitantes en su territorio. Argentina se destaca como una potencia en la región Latinoamericana, puesto que representa la segunda economía más grande de América del Sur y la tercera más grande en Latinoamérica. Además, es miembro fundador de las Naciones Unidas, el Banco Mundial, la Organización Mundial del Comercio, el Mercosur, la Unión de Naciones Sudamericanas, la Comunidad de Estados Latinoamericanos y del Caribe y la Organización de Estados Iberoamericanos. [3].

Ilustración 2. Mapa Argentina

Fuente: https://en.wikipedia.org/wiki/Argentina

Adicional a esto, se ha determinado que varios países de la UNASUR controlan una parte importante de las mayores reservas minerales del planeta. Por ejemplo, al menos 65% de las reservas mundiales de litio están repartidas entre Chile, Argentina y el Brasil. Así mismo Argentina, ha sido el principal productor de gas y petróleo no convencional. Esto debido a que hace pocos años atrás en Argentina se descubrió una gran zona que contenía estos recursos. Esta zona es llamada Vaca Muerta. Bajo esta situación Argentina se convirtió en el segundo país más grande con reservas de gas no convencional y el cuarto país más grande con petróleo no convencional. Vaca Muerta es una formación geológica de 30.000 km² ubicada principalmente en la provincia de Neuquén en el sur de Argentina y que contiene petróleo y gas que se encuentra a más de 2.500 metros de profundidad, lejos de las aguas subterráneas que en esta región se encuentran a una profundidad de entre 300 y 400 metros. Se estima que el total de hidrocarburos recuperables de esta formación es de 16.200 millones de barriles de petróleo y 308 billones de pies cúbicos de gas natural. Este ha sido el motivo por el cual se han desarrollado múltiples proyectos de ciberseguridad industrial en esta zona. [4]

Ilustración 3. Reserva Vaca Muerta

Fuente: https://www.pagina12.com.ar/237521-argentina-se-salva-con-vaca-muerta

3. Importancia de la Ciberseguridad en estas compañías.

Durante el 2019, los ciberataques a nivel mundial dirigidos a infraestructuras críticas crecieron exponencialmente respecto a años

anteriores. Por este motivo, es fundamental que las empresas en Latinoamérica tomen las medidas convenientes que les permitan prevenir ser víctimas de un incidente que pueda afectar a la seguridad de su personal y potencialmente detenga sus líneas de producción, lo que causaría pérdidas económicas representativas. A continuación, se listan los incidentes de ciberseguridad dirigidos a infraestructuras críticas que tuvieron un mayor impacto. Cabe mencionar que solo se listarán los incidentes ocurridos durante el 2019.

3.1. Noruega – Planta de fabricación de aluminio afectada por un ciberataque

Un ciber-ataque afectó las operaciones de la planta de producción de aluminio, Norsk Hydro, reconocida a nivel mundial. Se pudo conocer que el ataque fue ocasionado por una variante de Ransomware, el cual fue identificado como: LockerGoga. El ataque paralizó las actividades de la compañía en su casa matriz (Noruega) y además provocó que las acciones de la empresa cayeran y que el precio del aluminio, a nivel mundial, aumentara. Esta planta cuenta con varias sucursales operativas alrededor del mundo, y se vio obligada a cambiar su modo de operación de automatizado a manual. Esta fue otra consecuencia del ciberataque que afectó a los sistemas digitales de la planta de producción, impidiéndoles poder operar normalmente. [5].

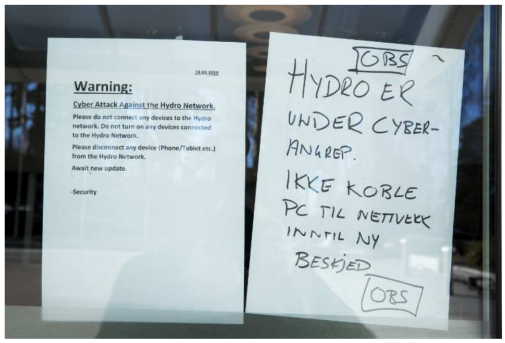


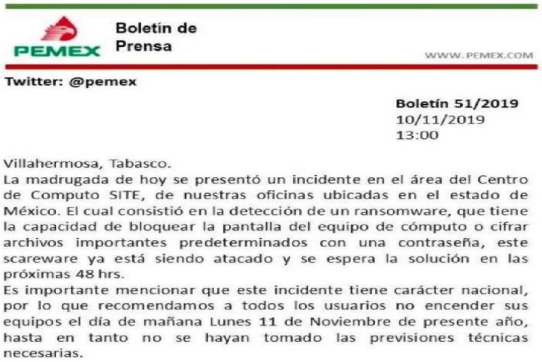
Ilustración 4. Mensaje fuera de las instalaciones de la compañía.

Fuente: https://www.thelocal.no/20190322/norways-norsk-hydro-hit-by-ransom-cyber-attack

3.2. México – PEMEX enfrenta problemas en sus sistemas de pago

Un ataque de ransomware que afectó a PEMEX interrumpió los sistemas de facturación de la compañía. Pemex vio sus sistemas de facturación interrumpidos por lo cual se afectó el proceso de pago del personal y los proveedores, además presentó dificultades en las operaciones de la cadena de suministro.

Además, se conoció, que algunos empleados no pudieron acceder al correo electrónico o a Internet y las computadoras funcionaban más lentamente. También se indicó que hay indicios de que el malware desplegado contra Pemex puede ser DoppelPaymer, según la firma de seguridad cibernética Crowdstrike Inc. [6]



PEMEX Boletín de Prensa

WWW.PEMEX.COM

Twitter: @pemex

Boletín 51/2019
10/11/2019
13:00

Villahermosa, Tabasco.
La madrugada de hoy se presentó un incidente en el área del Centro de Computo SITE, de nuestras oficinas ubicadas en el estado de México. El cual consistió en la detección de un ransomware, que tiene la capacidad de bloquear la pantalla del equipo de cómputo o cifrar archivos importantes predeterminados con una contraseña, este scareware ya está siendo atacado y se espera la solución en las próximas 48 hrs.
Es importante mencionar que este incidente tiene carácter nacional, por lo que recomendamos a todos los usuarios no encender sus equipos el día de mañana Lunes 11 de Noviembre de presente año, hasta en tanto no se hayan tomado las previsiones técnicas necesarias.

Ilustración 5. Boletín de Prensa PEMEX

Fuente: https://www.elsoldemexico.com.mx/finanzas/hackers-ransomware-computadoras-pemex-ataque-cibernetico-informatica-4440395.html

3.3. Campaña de malware contra empresas petroleras de USA

Un grupo de atacantes se infiltró en varias redes de comunicación de datos pertenecientes a distintas plantas petroleras de Estados Unidos. Hasta el momento, se conoce que los atacantes están utilizando una versión ofuscada del troyano de acceso remoto (RAT) Adwind, el cual es utilizado para robar datos. Este troyano ha sido utilizado anteriormente en ataques contra organizaciones minoristas y hoteleras.

Las capacidades de este malware que se infiltró en las compañías petroleras estadounidenses permitieron a los atacantes obtener, encriptar y filtrar datos; así como, capturar imágenes de cámara web, escanear discos duros en busca de archivos específicos, inyectar código malicioso en procesos legítimos para permanecer indetectable y monitorear el estado del sistema.

Además, se conoció que el malware tenía la capacidad especial de modificar la configuración del registro para lograr la persistencia y puede saltar los controles establecidos por firewalls, antivirus y otros servicios de seguridad en los dispositivos infectados. [7]

3.4. Johanesburgo – Ransomware causa disrupciones en una compañía de energía

Un ciber-ataque afectó las operaciones de la compañía de energía City Power ubicada en la ciudad de Johannesburgo. Hasta el momento se conoce que la compañía fue víctima de un ataque de Ransomware, del cual aún no se ha podido identificar que variante fue utilizada. El ataque afectó los sistemas y la red en general de la compañía.

Este ataque cifró todas las bases de datos y aplicativos e impactó la mayor parte de la red de la compañía. Este ciber-ataque provocó que la página web y los servicios de venta de electricidad no estén disponibles impidiendo que muchos de los usuarios no puedan adquirir unidades de electricidad y los dejen en oscuridad. Esto debido a que en Johannesburgo los clientes reciben medidores de energía prepaga y la cantidad de electricidad que pueden consumir depende de la cantidad de unidades de electricidad que adquieran. [8].

Ilustración 6. Tweet de la compañía afectada

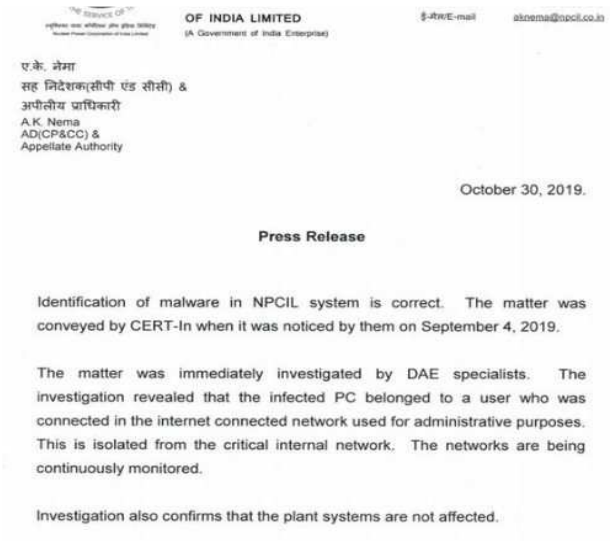
Fuente: https://thehackernews.com/2019/07/cyberattack-power-outage.html

3.5 India – Planta Nuclear atacada por un malware

La Planta de Energía Nuclear de Kudankulam ubicada en el estado indio de Tamil Nadu fue infectada por un malware de Corea del Norte denominado

Dtrack. Esta compañía es la mayor central nuclear de la India.

Los informes dan cuenta que los atacantes habían obtenido acceso a nivel de controlador de dominio de la planta. Por la información que se encuentra disponible hasta el momento se sabe que los atacantes obtuvieron acceso a cierta información confidencial de la compañía. Sin embargo, los directivos dijeron que los sistemas de control de la compañía no se vieron comprometidos puesto que estos no están conectados directamente con la red corporativa. [9]



OF INDIA LIMITED
(A Government of India Enterprise)

E-mail aknema@npcil.co.in

ए.के. नेमा
सह निदेशक(सीपी एंड सीसी) &
अपीलीय प्राधिकारी
A.K. Nema
AD(CP&CC) &
Appellate Authority

October 30, 2019.

Press Release

Identification of malware in NPCIL system is correct. The matter was conveyed by CERT-In when it was noticed by them on September 4, 2019.

The matter was immediately investigated by DAE specialists. The investigation revealed that the infected PC belonged to a user who was connected in the internet connected network used for administrative purposes. This is isolated from the critical internal network. The networks are being continuously monitored.

Investigation also confirms that the plant systems are not affected.

Ilustración 7. Boletín de prensa de la compañía afectada

Fuente: https://twitter.com/4w4r44/status/1189581854157889536

3.6 Medio Oriente - Malware ataca al sistema energético

Investigadores descubrieron un nuevo malware destructivo de borrado de datos, que estuvo atacando a organizaciones energéticas de Medio Oriente. El malware es denominado ZeroClear, el mismo se trata de una familia del malware Shamoon que fue utilizado en 2012 contra la organización Saudi Aramco y causó daños a cerca de 30000 ordenadores de esta compañía.

El equipo de investigadores de IBM asocia este nuevo malware ZeroClear a organizaciones patrocinadas por el estado Iraní. Los investigadores aún no han revelado los nombres de las compañías que se vieron afectadas por este malware. El impacto que tendría la ejecución exitosa de este ataque fue la pérdida completa de los datos almacenados en

los dispositivos que utilizan el sistema operativo Windows. [10]

3.7 Estados Unidos – Malware atacando al sector energético

El equipo de investigación de DRAGOS ha identificado que XENOTIME que fue el desarrollador del malware TRISIS que atacó al SIS (Safety Instrumented System) de la compañía Saudi Aramco en el reconocido ciberataque de 2017, actualmente se encuentra desplegando distintas técnicas de reconocimiento sobre compañías de provisión de energía eléctrica de Estados Unidos y otros países. De acuerdo con los investigadores, esta situación es preocupante debido a que el objetivo de este grupo es directamente la destrucción física del sistema de control industrial y/o vida humana. Además, las habilidades que posee este grupo son suficientes para perpetrar un ciberataque sobre los ambientes industriales.

El equipo de investigación identificó un patrón de actividad persistente que intentaba recopilar información y enumerar los recursos de red asociados con las empresas de electricidad de Estados Unidos. Este comportamiento corresponde a las técnicas utilizadas en la primera etapa de un ciberataque lo que podría indicar que el grupo XENOTIME se estaba preparando para un futuro ciberataque. [11]

Por otro lado, la exposición a ciberataques que enfrentan las infraestructuras críticas ya no solo se acota a grupos criminales patrocinadas por alguna nación, si no que durante los últimos años se han venido desarrollando herramientas de intrusión y ataque específicas para ICS, lo cual está ampliando el grupo de atacantes capaces de comprometer las redes de estas infraestructuras. En años anteriores, dado que los sistemas de control industrial son distintos a los sistemas de TI, para que las intrusiones contra los sistemas de control tengan éxito se requerían conocimientos especializados, lo que establecía un umbral más alto para que los ataques tengan éxito. Sin embargo, dado que las herramientas de intrusión y ataque suelen ser desarrolladas por alguien que ya tiene la experiencia, estas herramientas pueden ayudar a los atacantes a eludir la necesidad de adquirir ellos mismos la experiencia o conocimiento necesario para efectivizar un ataque.

Un estudio [12] encargado de rastrear un gran número de herramientas

de operación cibernética dirigida a sistemas de control industrial disponibles públicamente, demostró que:

- La mayoría de ellas han sido desarrolladas en los últimos diez años.
- La mayoría de las herramientas son agnósticas al vendedor.
- Algunas herramientas son "autónomas", otras vienen en forma de módulo de explotación populares.
- Existe una variedad de módulos de explotación específicos de sistemas de control industrial, como Metasploit (gratuito), Core Impact e Immunity Canvas, así como marcos de explotación más recientes: Autosploit, Industrial Exploitation Framework (ICSSPLOIT), y el Industrial Security Exploitation Framework.

Ilustración 8. Portal de Inicio Shodan

Fuente: https://www.shodan.io/

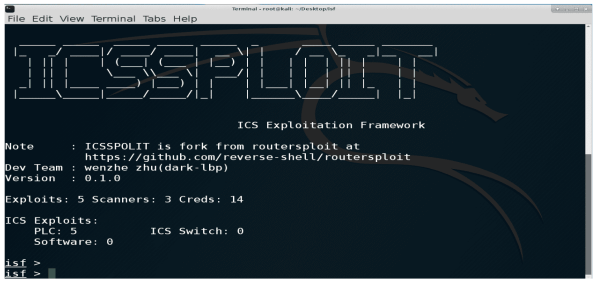


Ilustración 9. Framework de Explotación ICSSPLOIT

Fuente: https://securityonline.info/isfindustrial-exploitation-framework/

3.8 Ejemplo básico del uso de Shodan

Shodan es un potente motor de búsqueda que permite encontrar diferentes tipos específicos de equipos conectados a Internet a través de una variedad de filtros. bien es un motor de búsqueda, es muy diferente a los buscadores tradicionales como Google, Yahoo! o Bing. Los buscadores

tradicionales indexan contenido mientras que Shodan indexa banners.

Ilustración 10. Portal Inicio Shodan

Fuente: https://www.shodan.io/

3.8.1 Shodan: Sección Explorar

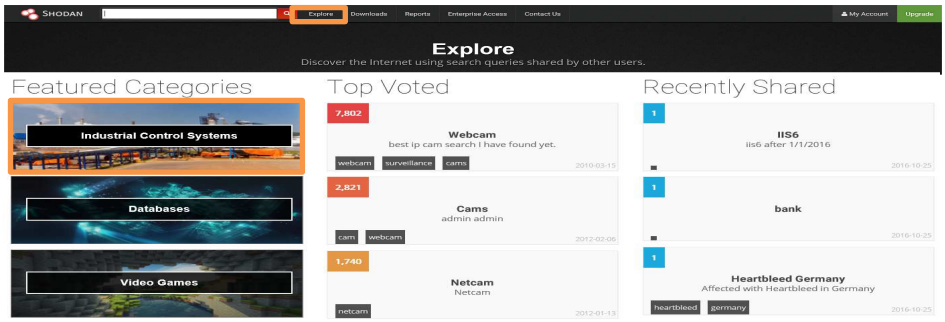


Ilustración 11. Sección Explorar Shodan

Fuente: https://www.shodan.io/

La sección Explore del motor de búsqueda desplegará una lista de búsquedas predeterminadas, entre las cuales se encuentra la sección Industrial Control Systems, el cual mostrará todos los sistemas de control o componentes del mismo que se encuentran expuestos a internet a los cuáles es posible tener acceso, así como, las vulnerabilidades que estos presentan.

3.8.2 Shodan: Uso Básico

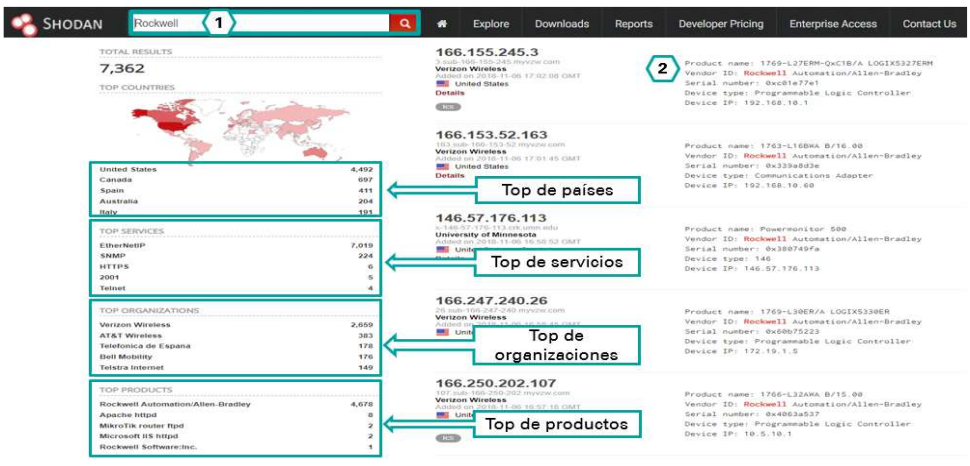


Ilustración 12. Búsqueda de un Sistema de Control

Fuente: https://www.shodan.io/

En la barra de búsqueda se puede ingresar términos relacionados con sistemas de control como son: PLCs, HMIs, SCADA, entre otros. Para este caso, se buscó con el nombre de uno de los proveedores con más presencia en el mundo industrial como es Rockwell Automation. Esta búsqueda nos presentó en la parte la izquierda se puede observar un compilado con información relevante relacionada a la búsqueda.

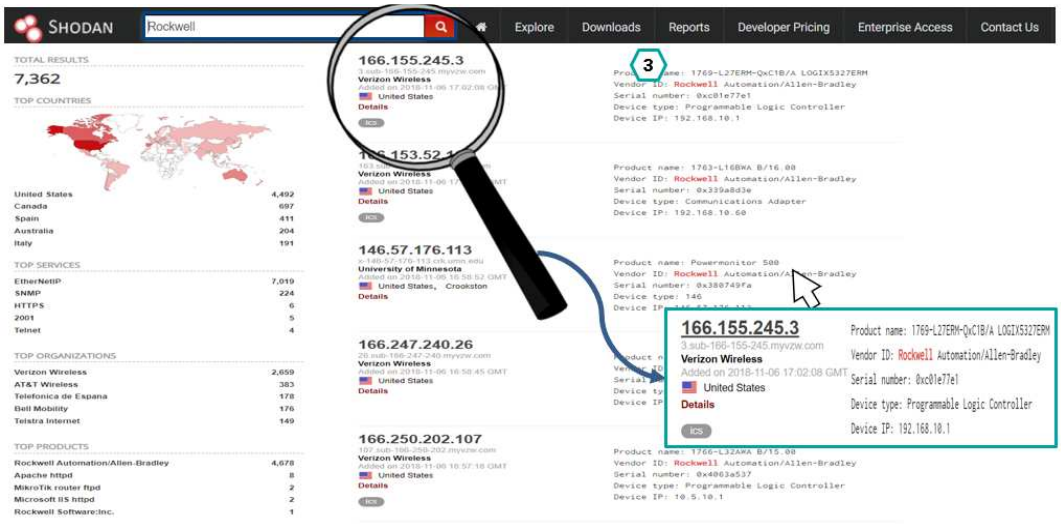


Ilustración 13. Identificación de sistemas de control expuestos

Fuente: https://www.shodan.io/

Como tercer paso, sobre la derecha podemos visualizar los distintos productos de marca Rockwell Automation que se encuentran expuestos a internet. En este caso específico se observa un PLC de esta marca, además se puede observar la respectiva dirección IP, nombre de host, ISP, el país donde se encuentra el equipo, entre otros detalles.

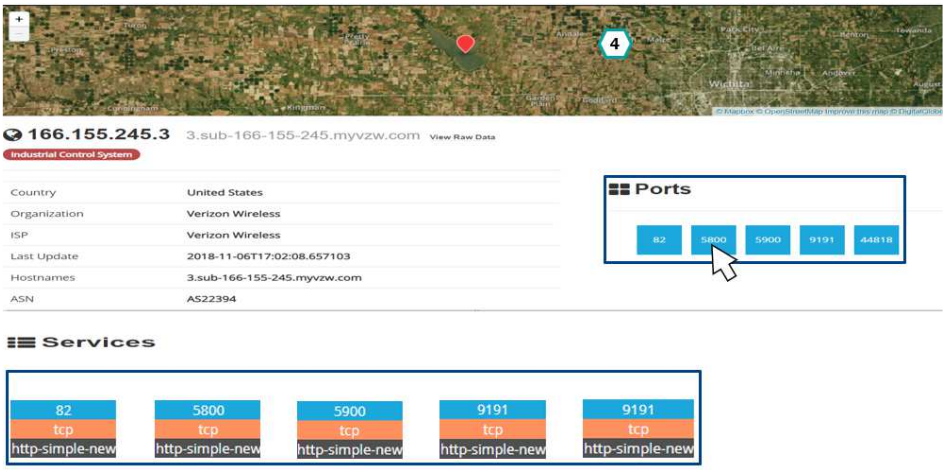


Ilustración 14. Identificación de puertos y servicios del sistema expuesto

Fuente: https://www.shodan.io/

Como cuarto paso hacemos click sobre el equipo deseado, y en el resultado podemos ver un mayor detalle sobre ese equipo. Los resultados de mayor relevancia son los puertos y los servicios que tiene el equipo, por los cuales se podría tener acceso al mismo.

3.8.3 Shodan: Filtros Básicos

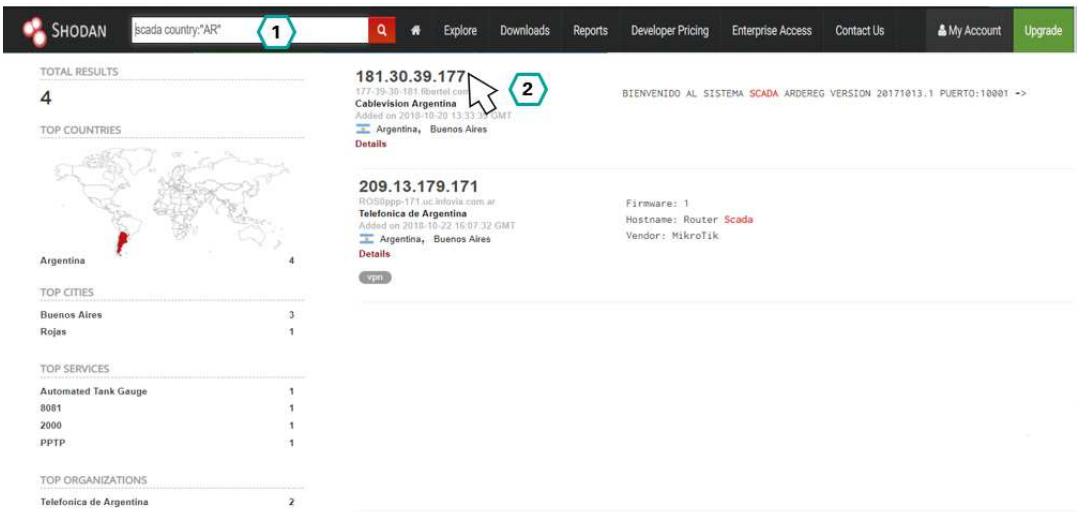


Ilustración 15. Filtros de Shodan

Fuente: https://www.shodan.io/

La herramienta permite el uso de filtros para encontrar con más exactitud lo que se busca. Para este caso la palabra clave es SCADA y con el filtro para que solo muestre los resultados que existen en Argentina. Si hacemos click sobre el primer resultado obtendremos lo siguiente.

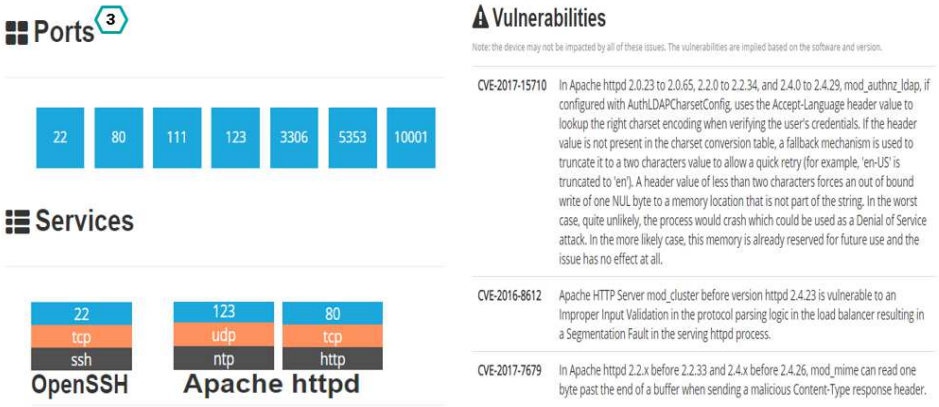


Ilustración 16. Puertos, servicios y vulnerabilidades del sistema expuesto

Fuente: https://www.shodan.io/

En este paso verificamos servicios y puertos que pueden ser utilizados para ingresar al dispositivo. Además, para este caso Shodan brindó un cuadro con vulnerabilidades conocidas en este dispositivo que pueden ser explotadas. En este caso se puede ver que el puerto 80 está abierto lo que permite ingresar a las configuraciones de este dispositivo mediante un servidor web, como se muestra a continuación.

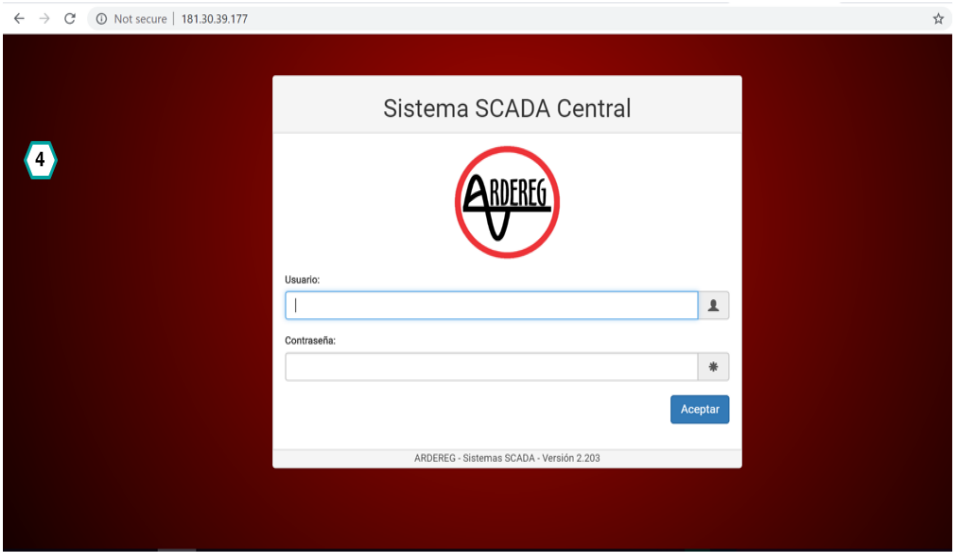


Ilustración 17. Interfaz web del sistema SCADA expuesto

Fuente: https://www.shodan.io/

La IP obtenida de Shodan se traslada a un web server, lo que nos dará acceso a la interfaz de administración del sistema SCADA.

3.8.4 Shodan: Caso de estudio – PLC

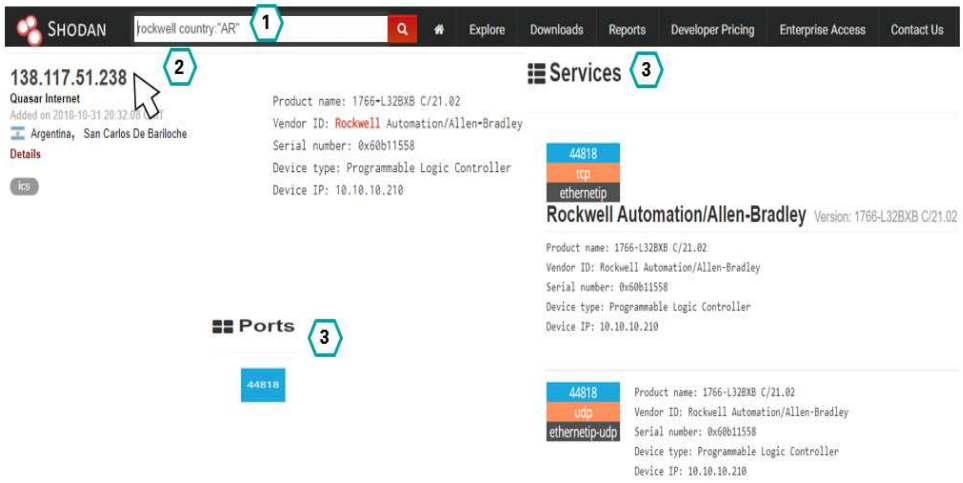


Ilustración 18. PLC expuesto en Shodan

Fuente: https://www.shodan.io/

Como primer paso, se debe realizar la búsqueda con la palabra clave "Rockwell" con el filtro para que solo aparezcan resultados de Argentina. Como segundo paso, se hace click sobre el dispositivo deseado y como tercer paso verificamos que servicios y puertos se encuentran disponibles para obtener acceso mediante estos.

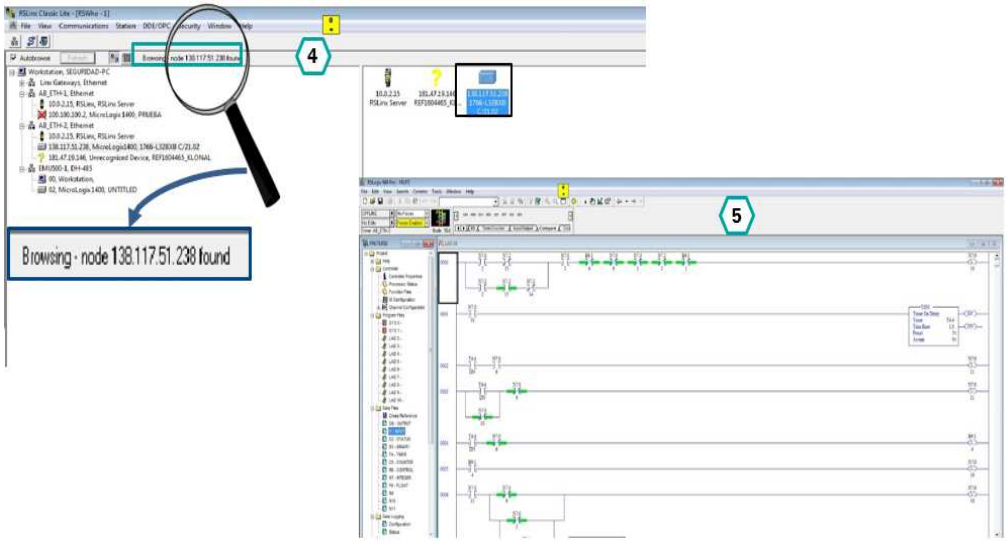


Ilustración 19. Lógica de Control del PLC expuesto

Fuente: Elaboración Propia

Como cuarto paso, se levantó una conexión con el dispositivo usando la dirección IP encontrada y utilizando el software RsLinx propietario de Rockwell Automation para levantar los drivers del dispositivo expuesto. Como quinto

paso, una vez levantados los drivers del PLC se pudo observar la lógica de control que tenía configurado este PLC mediante el software RSLOGIX. Cabe mencionar que las soluciones de software aquí presentadas se pueden utilizar solamente para PLCs de la marca Rockwell Automation, por lo general cada uno de los fabricantes poseen sus propias soluciones para configurar sus dispositivos.

3.8.5 Shodan: Caso de estudio – HMI

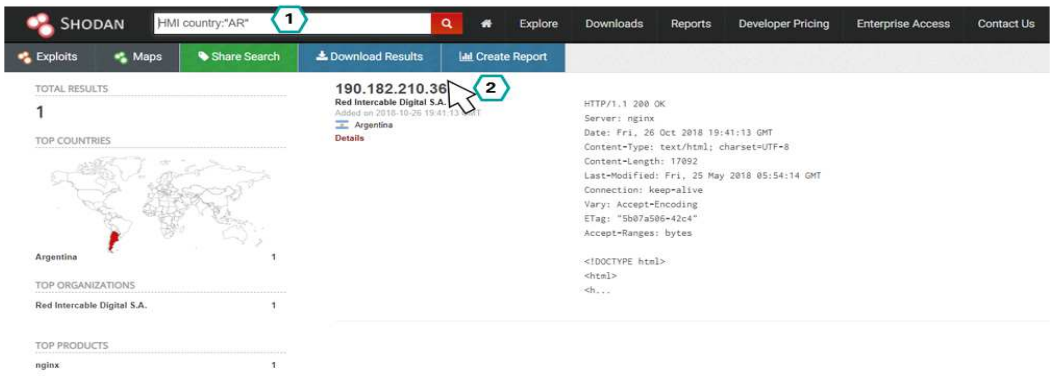


Ilustración 20. HMI expuesto en Shodan

Fuente: https://www.shodan.io/

Al igual que en los anteriores casos, como primer paso hacemos la búsqueda con la palabra HMI y filtramos para obtener resultados de Argentina. Como segundo paso, hacemos click sobre el dispositivo deseado, para este caso no nos brinda más detalles, sin embargo, nos redirige a la página web de administración del HMI, como se muestra a continuación.

Ilustración 21. Interfaz HMI del sistema expuesto

Fuente: Elaboración Propia

Una vez dentro de la interfaz de administración del HMI, podemos visualizar distintas variables del proceso que se está ejecutando, así como un

botón llamativo denominado “PARADA EMERGENCIA” sobre el cual se verificó que no existe un control que impida la modificación de estos parámetros, por lo cual, se podría detener el proceso que se encuentra ejecutando.

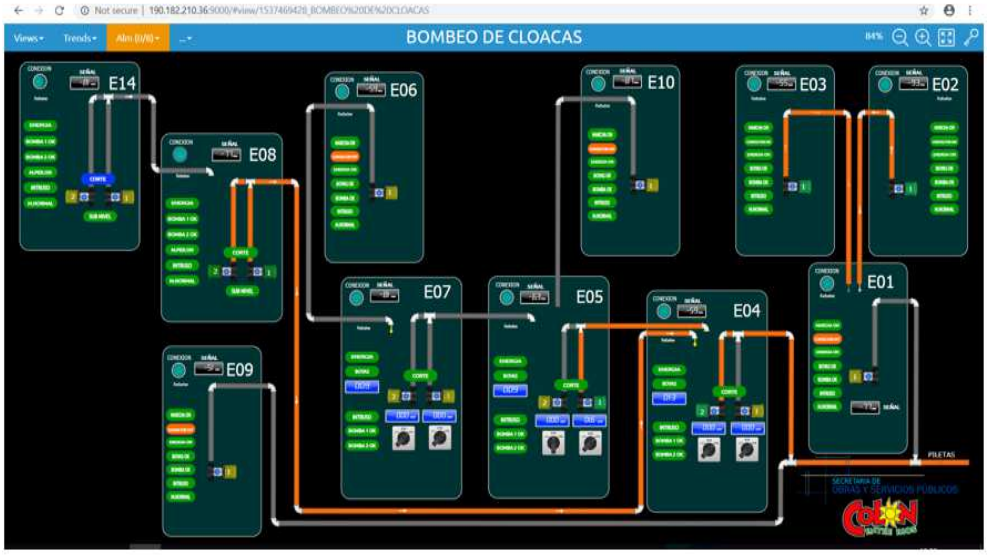


Ilustración 22. Interfaz Bombeo de Cloacas

Fuente: Elaboración Propia

De la misma forma se pudo visualizar otro proceso de la planta de agua, el cual no poseía variables que se puedan modificar, sin embargo, los atacantes podrían aprender cual es el proceso de control del bombeo de cloacas y encontrar otra forma de ingresar para causar una potencial irrupción o mal funcionamiento del mismo.

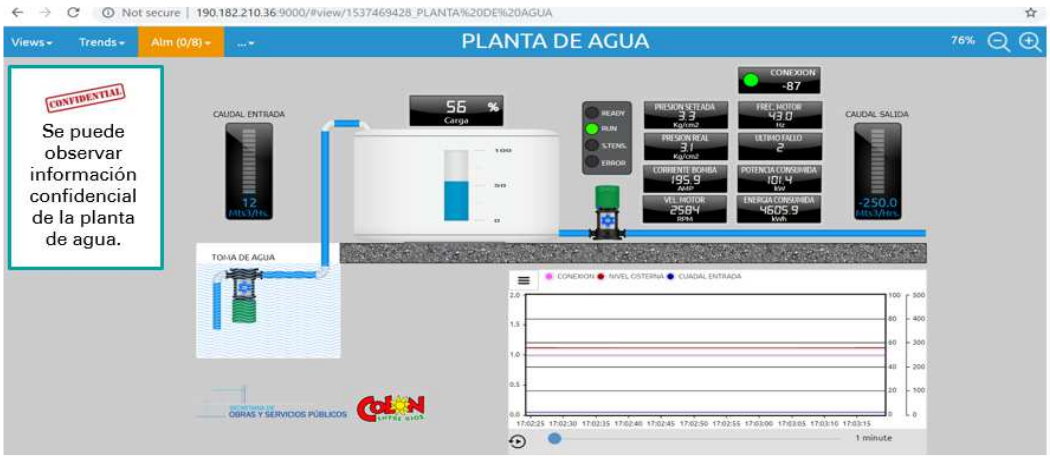


Ilustración 23. Interfaz Planta de Agua

Fuente: Elaboración Propia

Como se demostró durante la práctica, es sencillo buscar y encontrar sistemas del mundo OT expuestos a internet. La exposición a internet de

sistemas SCADA/HMI es una práctica no recomendada por distintos estándares internacionales ya que presenta un riesgo muy alto frente a Ciberataques.

3.9 Sistema y Distribución de tráfico

Diferentes medios de comunicación informaron acerca de un incidente que comprometía al sistema de control de las luces de los semáforos de la ciudad de La Plata, lo cual se demostró en investigaciones que fueron actos de ciber-atacantes. Este compromiso del sistema permitió que los actores maliciosos pudieran tomar control del tráfico en los semáforos, afectando a más de 400 dispositivos alrededor de toda la ciudad. En total el ataque tuvo impacto sobre el funcionamiento de las luces de los semáforos que fueron apagadas varias horas durante un par de semanas.

Ilustración 24. Portadas de noticias

Fuente:http://diariofull.com.ar/nota/3069/la_comuna_denuncia_que_un_hacker_esta_enloqueciendo_a_los_semaforos_en_la_plata

3.10 Sistema de distribución energética

Una de las compañías más grandes de distribución de energía de la ciudad de Buenos Aires sufrió un sabotaje en sus sistemas de control. Un atacante fue capaz de operar la red SCADA de la compañía remotamente desde una locación desconocida aún, para propósitos maliciosos. Como resultado de este incidente varios sectores de la ciudad se vieron afectados

por apagones eventuales. De las investigaciones que surgieron de este incidente no se logró identificar al atacante.


Apagón: Edesur investiga un eventual sabotaje

La compañía eléctrica no descartan que los cortes hayan sido provocados de forma intencional para "generar caos" en la Ciudad y en el Conurbano

EDESUR
SERVICIO DE EMERGENCIA

Notas relacionadas
- Continuan sin luz varios barrios porteños tras ...
- Sigue la baja presión de agua en barrios ...

La empresa Edesur investiga desde esta mañana las causas d masivo corte de energía eléctrica que sufrieron ayer durante más de dos horas varios barrios de Capital Federal y el Gran Buenos Aires.

En ese sentido, desde Edesur no descartaban ninguna

Ilustración 25. Portada Noticia

Fuente: https://www.diariopopular.com.ar/general/apagon-edesur-investiga-un-eventual-sabotaje-n136366

4. ¿Qué están haciendo las compañías en Argentina?

Durante este punto, es necesario mencionar cómo las compañías están manejando los temas relacionados a ciberseguridad industrial. Sin embargo, esto se lo realizará haciendo una comparativa entre el sector público y privado de Argentina. Puesto que, las evaluaciones de ciberseguridad realizadas en compañías tanto públicas como privadas arrojaron resultados muy distintos para cada uno de estos sectores.

4.1. Sector Privado

La principal diferencia que arrojaron las distintas evaluaciones de ciberseguridad fue una marcada tendencia que demostró que las compañías del sector privado se encuentran más desarrolladas respecto a ciberseguridad industrial.

Los altos directivos de las compañías del sector privado son conscientes de que sus empresas podrían ser parte de un ataque cibernético. Esta comprensión es posible debido a empresas similares que sufrieron un ciberataque, como, por ejemplo, el caso de PEMEX que es una empresa de renombre a nivel Latinoamericano. También de los assessments realizados se descubrió que algunas compañías fueron víctimas de ataques de malware

que produjeron breves interrupciones en su línea de producción y produjeron problemas de rendimiento. Por este motivo, las compañías del sector privado están realizando las siguientes actividades en relación con ciberseguridad industrial.

- Formación de equipos de Ciberseguridad Industrial, con miembros multidisciplinarios, es decir personal del negocio OT (Tecnologías operativas) y IT (Tecnologías de Información).
- Los equipos de IT y OT están uniendo esfuerzos, para lograr una integración de redes segura.
- Desarrollo de evaluaciones de ciberseguridad dentro de sus infraestructuras.
- Establecimiento de planes de acción priorizados para la implementación de mejores prácticas de ciberseguridad.
- Realización de campañas de concientización y formación sobre ciberseguridad en infraestructuras críticas.

4.2. Sector Público

En contraste, con empresas del sector privado, durante las evaluaciones de ciberseguridad realizadas, el hallazgo principal fue que la ciberseguridad no es una preocupación para los involucrados. Sin embargo, esto es preocupante porque los principales sectores de infraestructura crítica pertenecen al estado o están bajo su mando. El motivo principal por el cual estas empresas muestran despreocupación es que en Argentina hasta el momento no se cuenta un proyecto de ley para regular la ciberseguridad en infraestructuras críticas. A fin de contrarrestar esta situación, desde el Gobierno de Argentina durante el 2019, se liberó la resolución 829/2019 [13], la cual “crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, que tiene como objetivo la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas.” [14].

Es importante destacar que, en el sector público, se presenta un total desconocimiento respecto a ciberseguridad, por lo cual estas empresas no tienen áreas de Ciberseguridad centradas exclusivamente en el sector OT, ni

políticas de ciberseguridad relacionadas.

5. Principales Hallazgos por industria.

Los hallazgos que se mostrarán durante este capítulo se basan en múltiples evaluaciones de ciberseguridad realizadas en distintas compañías de Latinoamérica. A continuación, se presenta qué países e industrias fueron las involucradas para este estudio.

- **Argentina**
  - (4) Compañías de Manufactura
  - (9) Plantas de generación de energía
  - (2) Compañías de Oil&Gas
- **Chile**
  - (1) Compañía de Oil&Gas
- **México**
  - (2) Compañías de Manufactura
- **Ecuador**
  - (3) Compañías de Manufactura
- **Costa Rica**
  - (1) Compañía de Manufactura
- **Colombia**
  - (2) Compañías de Manufactura

De estas múltiples evaluaciones de ciberseguridad realizadas, se recopiló información sustancial que permitió comprender el panorama actual de ciberseguridad industrial en la región.

Así mismo, es importante destacar que todas las empresas involucradas en este estudio nunca antes habían realizado una evaluación de ciberseguridad sobre sus infraestructuras.

5.1. Hallazgos en Manufactura

De este estudio, se puede considerar que el sector de manufactura es el menos desarrollado en la región en términos de ciberseguridad. Además, las

entrevistas realizadas al personal operativo de esta industria demostraron que la mayoría, solo se centra en la producción y confirman que las interrupciones de las líneas de producción son un problema común, por lo cual desestiman el posible impacto de un ataque cibernético. A continuación, se presentan los hallazgos más comunes que se encontraron en las compañías evaluadas, cabe mencionar que las categorías a las que pertenecen las industrias evaluadas son: automotriz, cervecero, acería, fábrica de acero.

- El acceso físico a las salas de Control y Computación no está restringido, esto quiere decir que, si algún usuario mal intencionado quiere acceder a las salas de control, este no se encontrará con ninguna barrera lo cual puede causar que el mismo pueda manipular los activos que se encuentran en esta sala, como estaciones de ingeniería, servidores SCADA, HMI´s, entre otros y causar una disrupción en la línea de producción.
- Hardening de los servidores no se encuentra estandarizado, esto quiere decir que la mayoría de los activos no cuenta con medidas básicas de protección, como por ejemplo paches actualizados, soluciones antivirus instaladas, restricciones de puertos para el uso de pendrives, entre otros.
- La mayoría de los sistemas comparten la misma identificación de usuario y la misma contraseña para todos los usuarios, esto es común en la mayoría de los ámbitos industriales, sin embargo, esto presenta un gran riesgo puesto que, si esta credencial que comparten todos los usuarios se ve comprometida, no existirá ningún usuario a excepción del administrador que pueda contrarrestar este problema.
- No existen controles de acceso lógico, esto quiere decir que, al no existir un usuario y contraseña distinta para los usuarios, se imposibilita , la verificación de que todas las cuentas de usuario, grupos o roles de usuario, y sus privilegios asociados, sean correctos. Así como, se presenta la inexistencia de un procedimiento para revocar las cuentas de usuario cuando esto sea necesario por cualquier motivo.
- No existen controles de gestión de parches y antivirus, esto quiere decir que sobre los activos informáticos que forman parte del sistema

de control industrial no se lleva un control que permita mantener las soluciones de antivirus actualizadas con las últimas firmas de detección y que los sistemas operativos de los mismos se mantengan actualizados. Esto provoca que estos activos informáticos sean más vulnerables a amenazas de malware.

- Los controles para la Gestión del Cambio y Desarrollo de Programas son ejecutados por los proveedores de software a su discreción
- Las políticas y procedimientos de IT no están definidos ni documentados.

5.2. Oil & Gas

De acuerdo con este estudio, se pudo determinar que la industria de Oil & Gas está liderando el camino para el desarrollo de una fuerte postura de ciberseguridad sin centrarse únicamente en la seguridad de sus operaciones, si no también trabajando fuertemente en programas de concientización y formación de ciberseguridad en sistemas de control industrial para solidificar el conocimiento de su personal operativo y poder utilizarlos eficazmente como primera línea de defensa ante un posible compromiso de ciberseguridad. Las categorías de las compañías evaluadas son las siguientes: Upstream: Early Productions Facilities (EPF), Central Processing Facilities (CPF), Natural-Gas Processing Plants, LNG Facilities, Ports; Midstream: Gas pipelines and LNG carriers y Downstream: Gas Stations. A continuación, se presentan los hallazgos comunes.

- Las políticas y procedimientos de IT no están definidos ni documentados.
- No existen controles de gestión de parches y antivirus, tal como se identificó en el sector de manufactura no tener estos controles aumenta el riesgo de ser vulnerables a amenazas de malware.
- Hardening de los servidores no se encuentra estandarizado.
- Los controles para la Gestión del Cambio y Desarrollo de Programas son ejecutados por los proveedores de software a su discreción
- El acceso físico a los equipos de campo no está restringido, esto podría permitir a un usuario mal intencionado manipular estos

dispositivos pudiendo causar una disrupción o perturbación en el proceso físico que podría afectar potencialmente al SAFETY del personal de la planta.

- Inexistencia de un inventario de activos, esto es de fundamental importancia ya que al no contar con un inventario de activos es imposible saber que activos posee la compañía y de esta forma no se puede categorizar la prioridad de cada uno de estos activos para su debida protección.

5.3. Plantas de Generación y Distribución de energía eléctrica.

El sector de la generación de energía está compuesto por infraestructuras críticas de servicio civil que podrían afectar a la vida cotidiana de las personas si se produjera una interrupción. Además, de acuerdo con este estudio se identificó que esta industria tiene un nivel de madurez de ciberseguridad muy bajo. Sin embargo, esta situación ha ido cambiando en los últimos años. Las compañías de este rubro han estado trabajando duramente para resolver problemas comunes. Por ejemplo, una de las empresas más importantes de Argentina está trabajando en un plan de 5 años que incluye múltiples planes de remediación, tales como, segmentación de la red, control de acceso, gestión de parches, concientización y otros. Entre las categorías que entraron en el estudio se encuentran las estaciones de generación: Centrales Térmicas, Centrales Hidroeléctricas, Centrales de Carbón, Parques de Turbinas Eólicas y estaciones de distribución: Subestaciones. A continuación, se presentan los principales hallazgos detectado durante las evaluaciones de ciberseguridad realizadas:

- Falta de restricciones para el acceso físico a equipos de campo y salas de control.
- Sistemas operativos obsoletos y en estado end-of-life.
- Falta de segregación entre las redes corporativas e industriales.
- Muestras de malware detectado durante las evaluaciones.
- Inexistencia de soluciones antimalware.
- Falta de un programa para la gestión de parches de los sistemas.

- Usuarios no privilegiados que poseen permisos de administrador.
- Accesos remotos mediante herramientas vulnerables como TeamViewer o TightVNC.

5.4. Estadísticas Generales

La mayoría de los países no cuentan con una regulación de ciberseguridad para las infraestructuras críticas. Lo que si existe en algunos países es una normativa, sin embargo, la misma no alcanza el nivel de madurez que podría presentar una regulación, debido a que la normativa solo describe procedimientos básicos y genéricos de seguridad cibernética y tiene importantes vacíos en cuanto a controles y procedimientos para aplicar un plan de seguridad cibernética. Es por esto por lo que en dentro de las evaluaciones de seguridad realizadas para este estudio se tomaron dos principales estándares.

- ISA 62443 - es ampliamente aceptada en el sector de la manufactura y la industria de Oil&Gas.
- NERC CIP – es un estándar aceptado para la industria de generación y distribución de energía eléctrica.

A continuación, se presentan las estadísticas que están basadas en el primer contacto que tuvimos con las empresas que fueron evaluadas para el presente estudio.

- Las empresas alineadas con el estándar ISA 62443 poseen un cumplimiento del 26%.

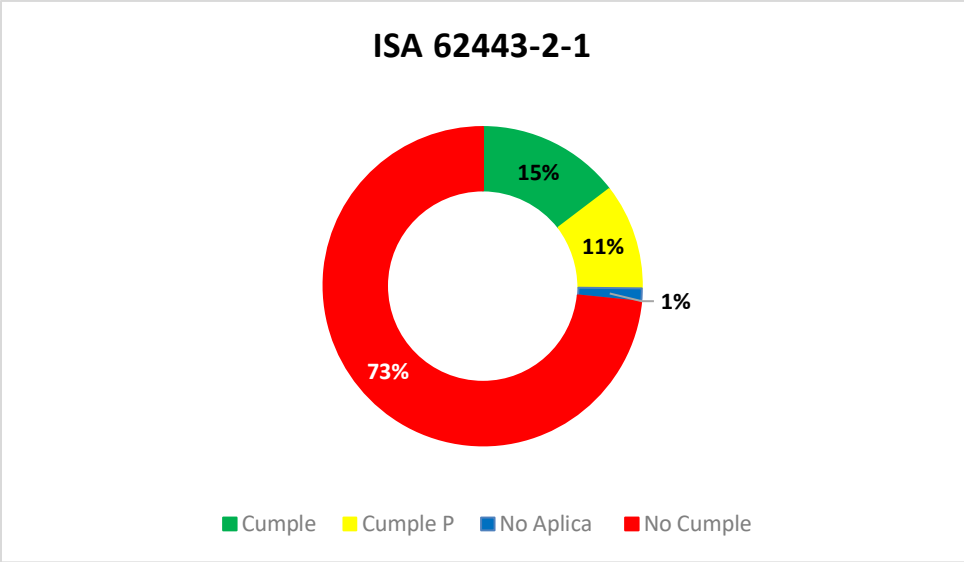


Ilustración 26. Estadísticas de Cumplimiento de las compañías respecto al estándar ISA 62443-2-1

Fuente: Elaboración Propia

- Por otro lado, las empresas alineadas con el estándar NERC CIP es decir todas las compañías del sector energético que entraron en alcance poseen un nivel de cumplimiento del 35%.

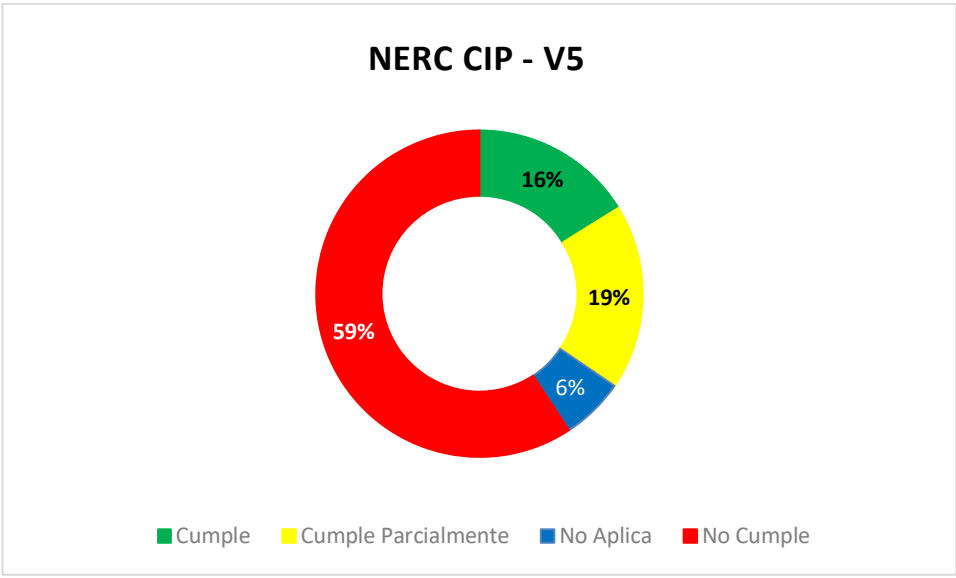


Ilustración 27. Estadísticas de Cumplimiento de las compañías respecto al estándar NERC CIP v5

Fuente: Elaboración Propia

5.5. Estadísticas Detalladas

A continuación, se presentan estadísticas más detalladas que se pudieron identificar durante las evaluaciones de seguridad, respecto a los

estándares internacionales utilizados durante una de las fases de los assessments realizados.

5.5.1. ISA 62443

- El 100% de las empresas evaluadas no posee una política de ciberseguridad industrial y la gobernanza respecto a seguridad en sistemas de control industrial apenas está en una fase inicial.
- El 100% de las empresas no poseen un programa de concientización y capacitación de ciberseguridad industrial para sus empleados.
- El 86,7% de las empresas evaluadas posean deficiencias en la segmentación de las redes corporativas e industriales.
- El 89,1% de las compañías no poseen un plan de respuesta a incidentes de ciberseguridad que les permita detectar y responder ante eventos anómalos de ciberseguridad.
- El 70,3% no posee un plan de continuidad de negocios que les permita recuperar las operaciones si es que fueran víctimas de un ciber incidente.

5.5.2. NERC CIP

- El 60,4% de las empresas evaluadas no poseen un plan de continuidad de negocios para la recuperación de las operaciones después de un evento anómalo de ciberseguridad.
- El 85,7% de las compañías, no poseen sus sistemas críticos hardenizados, incluso se identificó aplicaciones no necesarias para el proceso industrial instaladas en estos sistemas.
- El 94% de las empresas no poseen un plan de respuesta ante incidentes de ciberseguridad industrial.
- El 82,5 de las compañías evaluadas, no poseen un programa de gestión de parches, por lo tanto, los parches que son aplicados al sistema se los realiza basado en la experiencia del personal que opera los sistemas.
- El 100% de las compañías, no poseen un programa de ciberseguridad

industrial y su gobernanza aún no ha sido desarrollada.

6. Remediaciones

En esta sección, se presentan una serie de recomendaciones para mitigar los hallazgos identificados en las compañías.

6.1. Análisis de Riesgo

Para realizar un análisis de riesgo de acuerdo con [15] se deben contemplar dos categorías que serán explicadas a continuación:

6.1.1 Entendimiento del Negocio

En esta fase se realizará la identificación y documentación de las necesidades de la organización para abordar los riesgos de ciberseguridad asociados. Para esto se requiere que la organización desarrolle una lógica empresarial de alto nivel como base para su esfuerzo de gestión de la ciberseguridad del sistema de control industrial, que aborde la dependencia única de la organización con respecto al sistema de control industrial.

6.1.2 Evaluación, identificación y clasificación del riesgo

Una vez desarrollado el entendimiento del negocio se debe identificar el conjunto de riesgos de ciberseguridad industrial a los que se debe enfrentar la organización, para tener como una próxima fase la evaluación de la probabilidad de ocurrencia y la gravedad de estos riesgos. Para cumplir con esto, se deben llevar a cabo los siguientes requerimientos:

- Seleccionar un enfoque y una metodología particular de evaluación y análisis de riesgos que identifique y priorice los riesgos en función de las amenazas a la seguridad, las vulnerabilidades y las consecuencias relacionadas con los activos del sistema de control industrial.
- Proporcionar a los participantes en la actividad de evaluación de riesgos la información apropiada, incluida la formación metodológica, antes de comenzar a identificar los riesgos.
- Ejecutar la evaluación de riesgos del sistema para comprender

las consecuencias financieras y de salud, seguridad y medio ambiente en caso de que la disponibilidad, integridad y confidencialidad del sistema de control se vean comprometidas.

- identificará los activos que componen el sistema de control industrial y recopilar datos sobre los mismos para caracterizar la naturaleza del riesgo de seguridad.

6.2. Inventario de Activos

El desarrollo de un inventario de activos completo permitiría a la organización tener una comprensión entre todos los interesados con la infraestructura de soporte (IT/OT). Para este fin la organización deberá identificar los sistemas donde se incluya las operaciones, el equipamiento del proceso, el software, las redes involucradas y el personal a fin del sistema de control y analizar las dependencias para comprender tanto la función del activo en sí como los recursos necesarios para soportar funciones críticas.

Las organizaciones deben combinar diagramas de red, el inventario físico y una comprensión de los flujos de información, a fin de determinar los niveles de protección para cada sistema y los controles que deben implementarse para proteger el sistema sin comprometer ni degradar su rendimiento.

Además, se deberá contar con una categorización de la criticidad de los activos. Para este fin, él o los propietarios de los activos deben realizar una categorización de seguridad en función del impacto potencial (bajo, moderado o alto) que podría generar la ocurrencia de un evento que ponga en peligro la capacidad de la organización para cumplir su misión, proteger sus activos y personal y mantener su operación estable. De esta forma se podrá obtener con más detalle cuáles son los activos a los que se debe prestar especial atención cuando se esté aplicando las medidas de seguridad correspondientes.

Así mismo, un inventario detallado que contenga las características del activo como marca, modelo, versiones de firmware, versiones de software entre otros, permitiría a la organización identificar con prontitud que activos podrían estar afectados por una vulnerabilidad. Esto se realizaría

aprovechando los boletines de seguridad (también conocidos como advisories) que liberan los principales proveedores de la industria.

6.3. Seguridad Física

Los controles de seguridad física aplicables a las compañías pueden ser activos o pasivos y los mismos deben ser utilizados para limitar el acceso físico a cualquier activo de información que se encuentre bajo propiedad del entorno del sistema de control industrial. Estos controles permiten evitar incidentes de seguridad física, como pueden ser:

- Introducción no autorizada de nuevos sistemas.
- Acceso físico no autorizado a ubicaciones sensibles.
- Modificación física, manipulación, robo u otra eliminación, o destrucción de sistemas existentes.
- Observación visual no autorizada de activos de información confidencial.
- Introducción no autorizada de dispositivos para causar manipulación de hardware como dispositivos USB, puntos de acceso inalámbricos o dispositivos celulares, que también podrían ser utilizados para la primera fase de un ataque que consiste en recolección de información.

Por estos riesgos presentados anteriormente, es necesario aplicar medidas de seguridad física que permitirá reducir el riesgo de pérdidas o daño accidental de los activos de la organización y el entorno asociado. Entre los activos que la seguridad física busca proteger están los siguientes:

- Herramientas y equipos de planta
- Medio ambiente
- Propiedad intelectual (datos de la propiedad, configuraciones del proceso, información del cliente, entre otros.)
- Personal operativo

A fin de proteger el perímetro donde se encuentra la instalación industrial se puede utilizar cercas, zanjas anti-vehículos, montículos de tierra, muros reforzados, personal de guardia, puertas, sistemas CCTV, entre otros.

Una vez, dentro de la instalación se debe considerar la implementación

de un sistema de control de acceso físico, el cual debe pasar por una etapa previa de verificación para constatar que el mismo sea altamente confiable, es decir que solo otorgue acceso a las personas que puedan confirmar quienes dicen ser. Usualmente las personas deben usar algo que tienen, como tarjetas de acceso; algo que saben, como una clave PIN; o algo que son, como huellas biométricas.

También es recomendable utilizar sistemas de monitoreo de acceso, como son cámaras de video, sensores, entre otros. Estos dispositivos son utilizados para registrar la presencia física de individuos y pueden alertar acerca de un acceso no autorizado.

6.4. Gestión de Parches y Vulnerabilidades

La aplicación de parches y actualizaciones a un componente del ICS presenta grandes desafíos puesto que estos pueden interferir con el normal funcionamiento del ICS. Esto debido a que los parches o actualizaciones podrían modificar la forma en que funciona un componente, dando como resultado una operatoria anómala o pérdida de funcionalidad. Por este motivo, se recomienda que los parches atraviesen una etapa de test donde los mismos sean aplicados en un entorno de prueba que emule la operación normal del sistema de control para determinar si el parche puede traer consecuencias o no al mismo. Así mismo, antes de aplicar un parche se debe pedir la aprobación del proveedor del sistema de control, esto dificulta muchas veces las tareas de aplicación de parches. Una vez que el parche ha sido probado y verificado por el proveedor, se debe aplicar el parche durante una parada de planta, a fin de no comprometer el funcionamiento normal de la misma.

Existen muchos casos donde los trabajadores de la compañía no tienen acceso o permiso para manipular el equipamiento industrial puesto que los proveedores al momento del contrato aplican estas restricciones. Para estos casos, al momento de desarrollar el contrato se debe exigir al proveedor que se realicen mantenimientos correctivos y preventivos de los sistemas a su cargo.

6.5. Protección de dispositivos de campo

Algunos dispositivos utilizados en campo que son antiguos como PLC, RTU, IED entre otros por lo general no son compatibles con un mecanismo de administración central que distribuya medidas de seguridad. Esto debido a que muchos de ellos por defecto no poseen las mismas capacidades de seguridad que otros componentes. Por este motivo, los administradores de la organización deben optar por brindar una protección física a estos dispositivos utilizando mecanismos como cercas, puertas y racks cerrados.

Por otro lado, para los dispositivos de automatización utilizados en campo que poseen la capacidad de configurar una clave de acceso, se recomienda que esta característica sea habilitada.

6.6. Segmentación de Redes

La convergencia existente entre los sistemas de control industrial y los componentes del entorno corporativo puede ser utilizado por atacantes o usuarios mal intencionados para aprovechar vulnerabilidades del entorno corporativo y obtener acceso a la red industrial, es por esto por lo que los propietarios de los activos deben abordar este tema antes que se efectivice esta amenaza. Los factores importantes que pueden ser aprovechados para comprometer las redes industriales son los siguientes:

- Conexión mediante enlaces inseguros a redes internas y externas.
- Tecnologías utilizadas dentro del ámbito de control que poseen vulnerabilidades conocidas.
- Falta de comprensión de los requisitos para tener en cuenta antes de establecer un enlace entre el dominio corporativo y de control.

El aislamiento existente entre estas redes en tiempos anteriores causaba que los sistemas de control industrial solo estén amenazados por los riesgos relacionados a accesos físicos no autorizados a la planta industrial. Sin embargo, interconectar una arquitectura de IT con una red aislada puede presentar distintos conflictos, por lo cual a fin de abordarlos la Sociedad Internacional de Automatización propone una arquitectura integrada entre los ámbitos industriales y corporativos. Esta representación puede ser observada en la siguiente ilustración.

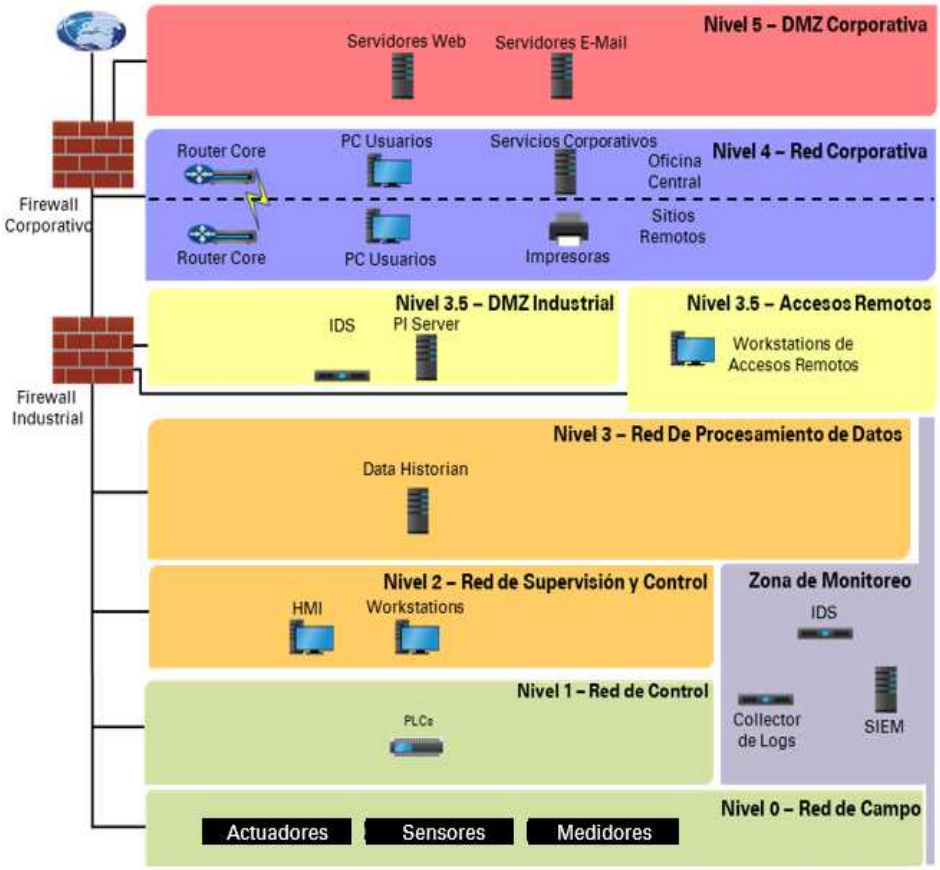


Ilustración 28 Arquitectura del modelo Purdue de segmentación de redes

Fuente: Elaboración propia

A continuación, se describirá brevemente los componentes de cada uno de los niveles del modelo Purdue.

- **Nivel 5:** En este nivel se deben ubicar los sistemas que tengan contacto directo con internet como servidores web, email, entre otros.
- **Nivel 4:** En este nivel se deben ubicar los sistemas necesarios para el negocio, como aplicaciones corporativas.
- **Nivel 3.5:** En este nivel se deben ubicar todos los sistemas que serán accedidos por los usuarios de la red corporativa
- **Nivel 2 y 3:** En estos niveles deben ubicarse los colectores de datos del ICS, workstations y servicios IT que den soporte a la red (DNS, DHCP, AD, entre otros)
- **Nivel 0 y 1:** En estos niveles deben ubicarse los dispositivos de campo con sus respectivos dispositivos controladores (PLCs) o censadores de variables (RTUs).
- **La zona de monitoreo** contendrá equipos colectores de eventos que

monitorearán los eventos de los dispositivos ubicados en los niveles 0, 1, 2 y 3.

- **DMZ** por sus siglas en inglés (Demilitarized Zone) es una subred física o lógica que contiene los servicios externos de una organización y los expone a una red no confiable como internet. La DMZ agrega una capa adicional de protección a la red local de la organización, pues si un usuario no autorizado obtiene acceso directo a un equipo que se encuentra dentro de la DMZ, este no será capaz de desplazarse a otra parte de la red.

Por otro lado, existen las LAN Virtuales (VLAN) que son redes locales virtuales que permiten dividir las redes físicas en subredes lógicas más pequeñas que son utilizadas para aislar el tráfico entre subredes. Existen dos categorías de VLAN que serán explicadas a continuación:

- **Dinámicas:** Son VLAN que se configuran automáticamente en función de direccionamiento IP o direcciones MAC.
- **Estáticas:** También conocidas como VLAN basadas en puertos, ya que estas son asignadas a puertos específicos de un switch.

En una arquitectura de un sistema de control industrial las VLAN son utilizadas para segmentar funcionalidades y capacidades de red. Por este motivo, las mejores prácticas recomiendan descomponer cada uno de los dominios operativos o líneas de proceso en segmentos y zonas más pequeñas a fin de facilitar la administración de estos.

6.7. Buenas prácticas de gestión de cambio

A continuación, se describen brevemente algunas de las mejores prácticas para la gestión del cambio. Estas prácticas aplican siempre y cuando se posea un área de ciberseguridad industrial o se haya identificado a algún responsable de esta tarea.

- Todo proyecto o cambio mayor que se genere en el sistema de control industrial debe involucrar al área de ciberseguridad industrial de la compañía para determinar posibles riesgos asociados ya sean operativos, de medio ambiente y de seguridad.
- Se recomienda incluir durante la parada de planta, los procedimientos

de ciberseguridad necesarios para la ejecución de cualquier cambio que se genere en el sistema de control. Esto incluye, la evaluación de riesgos analizando el posible impacto que el cambio puede ocasionar al sistema de control.

- Todo cambio generado en el entorno del sistema de control debe ser documentado a fin de llevar un control de cambios.
- Una vez ejecutado el cambio, el área o responsable de ciberseguridad industrial de la compañía debe validar si el cambio fue ejecutado de acuerdo con los lineamientos sugeridos.

6.8. Accesos remotos seguros

Los accesos remotos son conexiones que desean establecer los usuarios con las estaciones de ingeniería que no se encuentran en el mismo sitio físico que ellos.

Cuando estas conexiones son realizadas en condiciones inseguras pueden permitir que un usuario no autorizado intercepte la información que esté siendo transmitida. Por este motivo a continuación se listarán los casos más comunes donde se necesita una conexión remota a una red OT.

- **Fabricantes de equipos -** En la mayoría de los casos, en el momento de la compra, los sistemas de control industrial que comprenden estas redes incluyen un contrato de mantenimiento remoto por parte de los propios fabricantes.
- **Trabajadores remotos –** Hoy en día se necesita proporcionar a cualquier empleado que anteriormente trabajaba en el sitio pero que ahora está trabajando fuera de las instalaciones, acceso en línea para que puedan seguir haciendo su trabajo.
- **Contratistas externos -** Por último, muchas empresas subcontratan servicios a compañías que se especializan en áreas operativas específicas, como la optimización de la producción. Los contratistas que antes prestaban estos servicios físicamente ahora necesitan acceso remoto al equipo pertinente para apoyar su contrato y mantener las líneas de producción funcionando sin problemas.

Mejores prácticas para los accesos remotos

- Los usuarios que intenten acceder a la red de la organización deberán primero establecer un túnel VPN encriptado hacia el gateway VPN de la organización. En este punto se debe asegurar mediante reglas de Firewall y configuraciones en el Active Directory que los accesos solo sean permitidos al personal necesario y no se lo otorgue a todos.
- Para obtener acceso al entorno de la red ICS, el usuario deberá conectarse a un servidor de acceso remoto ubicado en la DMZ.
- En la DMZ industrial cada usuario/proveedor debe tener su propio entorno virtual especialmente creado en base a sus necesidades y privilegios. El acceso a estas máquinas virtuales debe ser a través de Microsoft RDP o similares.
- Así mismo, existen herramientas de monitoreo de ciberseguridad industrial que poseen capacidades para otorgar el acceso a personal necesario, además pueden visualizar en vivo y grabar las sesiones de acceso remoto, de esta forma se puede verificar en tiempo real las acciones que se están ejerciendo sobre el activo involucrado en la sesión remota.

6.9. Capacitación y Concientización

La organización debe desarrollar un programa de capacitación y concientización que alcance a todos los usuarios del sistema de control industrial. Este programa debe ser enfocado en brindar talleres donde se impartan conocimientos acerca de las medidas básicas y acciones necesarias que deben cumplir los usuarios para asegurar la protección del sistema, así como los pasos necesarios para responder ante un incidente.

También se deberá abordar una temática que permita asegurar que los usuarios que tienen acceso al sistema de control tengan claros cuáles son sus roles y responsabilidades con respecto a ciberseguridad mientras realizan sus tareas diarias.

Estos talleres de capacitación deben contener un material que sea

adecuado en función de cada uno de los roles del personal alcanzado. Esto se debe realizar a fin de evitar sobrecargar de información al personal.

6.10. Monitoreo de Ciberseguridad

Dentro del concepto de defensa en profundidad se aborda la temática de monitoreo, la cual propone utilizar un mecanismo de monitoreo que permita alertar a los operadores ante el acceso no autorizado a los activos críticos de la organización, así como los cambios no autorizados y comportamientos anómalos. Estas alertas deben ser enviadas apenas sean detectadas pues esto ayudará a tomar medidas defensivas necesarias antes que ocurra un evento no deseado de gran magnitud. Los mecanismos de monitoreo que se pueden desplegar en un ambiente industrial son:

- Uso de servidores syslog.
- Uso de soluciones SIEM.
- Uso de soluciones de monitoreo de tráfico. Estas soluciones en general tienen la capacidad de realizar monitoreo pasivo y activo. El monitoreo pasivo de tráfico consiste en realizar un port mirroring (también conocido como SPAN Port) sobre uno de los switches por los que circula la mayor cantidad de tráfico en función de capturar con más detalle el tráfico. Esta suele ser la opción más recomendada al instalar este tipo de soluciones. Por otro lado, también tienen la característica de captura de tráfico activo, que consiste, en que la herramienta envía queries para levantar la mayor cantidad de activos posibles, sin embargo, estos queries pueden interrumpir o afectar el performance de las líneas de proceso, por lo cual esta opción no es la más recomendable, en todo caso, esta opción se debe desplegar durante una parada de planta.

6.10.1 Sistemas de detección y prevención de intrusiones

Los sistemas IDS pueden funcionar adecuadamente en un entorno ICS típico puesto que ya existen predefinidos que componentes se van a comunicar entre sí, esto permite a la organización que utiliza un IDS monitorear y generar alarmas cuando exista una desviación de tráfico normal.

Los IDS funcionan de forma pasiva, es decir solo escucha el tráfico de red y evalúa que este se encuentra acorde a la operatoria normal del ICS

Por otro lado, se encuentran los IPS que tienen un funcionamiento parecido a los firewalls. Sin embargo, estos sistemas no son recomendados puesto que tienen la capacidad de tomar acciones en caso de que reciban una alarma. Por ejemplo, podrían detener un proceso normal del ICS cuando reciban una alarma. Sin embargo, como todas las soluciones los IPS son susceptibles a obtener falsos positivos.

6.11. Control de Acceso

En un entorno donde se encuentre desplegada una red de un sistema de control industrial, existen varios usuarios que utilizan una gran variedad de sistemas de control los cuales deben permitir el acceso oportuno a los mismos según lo requieran las operaciones de la compañía.

La autenticación, autorización y prácticas de control de acceso utilizadas en entornos corporativos, no se puede implementar de la misma manera en un sistema de control industrial, ya que estos por motivos operativos deben permanecer “siempre encendidos” por lo cual no es factible que los usuarios cierren sesión y vuelvan a iniciarla. Por lo general, los propietarios de los activos pueden controlar el acceso a los ICS utilizando dos metodologías, explicadas a continuación:

- **Distribuido:** La administración de los accesos bajo esta modalidad, requiere que la autenticación se realice en cada sistema por separado, es decir que cada sistema debe poseer un conjunto separado de cuentas de usuario, credenciales y roles. Este enfoque por lo general ha demostrado ser una buena solución para pequeñas implementaciones de ICS.
- **Centralizado:** Este enfoque es normalmente utilizado para administrar una gran cantidad de usuarios y cuentas. Esto lo hace mediante un sistema de autenticación central para la administración de cuentas ya sea (Active Directory o LDAP). Este sistema actúa conjuntamente con un protocolo de autenticación (Kerberos, RADIUS o TACACS) para comunicarse entre el servidor de

autenticación y el sistema de control industrial deseado

6.12. Políticas y Procedimientos

6.12.1 Políticas

Las políticas de la organización deben ser claras y describirán las reglas y controles necesarios para asegurar el desempeño óptimo del sistema de control industrial. Estas reglas y controles detallarán cuales son los comportamientos esperados dentro del ámbito operativo y los controles. La política también deberá reflejar cuales son las sanciones que se deberán aplicar en caso de incumplimiento de la misma.

6.12.2 Procedimientos

Debido a la creciente integración de los ambientes IT/OT, las organizaciones deben actualizar los procedimientos de seguridad que tenían para los sistemas IT, con objeto de que los nuevos procedimientos también alcancen a los sistemas de control existentes. Estos procedimientos deben establecer la metodología que se deberá utilizar para llevar a cabo un proceso o configuraciones de un sistema de control, en función de asegurar su funcionamiento. A su vez, estos procedimientos proporcionan una metodología estándar para llevar acabo determinadas funciones.

Un procedimiento de seguridad bien definido permite capacitar rápidamente al nuevo personal que se adhiera a la compañía. Los procedimientos de seguridad del ICS también abarcan instrucciones para que los operadores conozcan cuales son las tareas a realizar en caso de detectar un incidente, de manera que desde esta primera línea de defensa se pueda proteger a los sistemas de control.

6.13. Plan de Respuesta a Incidentes

Un plan de respuesta a incidentes ayudará a predefinir cómo la organización detectará y reaccionará ante los incidentes de ciberseguridad. Al desarrollar un programa para la planificación y respuesta a incidentes, es

importante incluir todos los sistemas en su alcance y no sólo limitar el esfuerzo a las instalaciones tradicionales de la sala de ordenadores. Parte del plan de respuesta a incidentes debe incluir procedimientos para la forma en que la organización responderá a los incidentes, incluyendo métodos de notificación y documentación, investigaciones, recuperaciones y prácticas de seguimiento subsiguientes.

La identificación temprana de un incidente y la respuesta adecuada pueden limitar las consecuencias del evento. La planificación y respuesta a incidentes proporciona a la organización la oportunidad de planificar los incidentes de seguridad y, a continuación, responder de acuerdo con las prácticas establecidas de la empresa. A continuación, se presentan algunos requerimientos base que se deben cumplir a fin de satisfacer el desarrollo de un plan de incidentes exitoso.

- La organización deberá implementar un plan de respuesta a incidentes que identifique al personal responsable y defina las acciones a realizar por las personas designadas.
- El plan de respuesta a incidentes se comunicará a todas las organizaciones apropiadas.
- La organización debe establecer un procedimiento de información para comunicar actividades y eventos inusuales que puedan tratarse de incidentes de ciberseguridad.

7. Seguimientos de los planes de remediación en las compañías

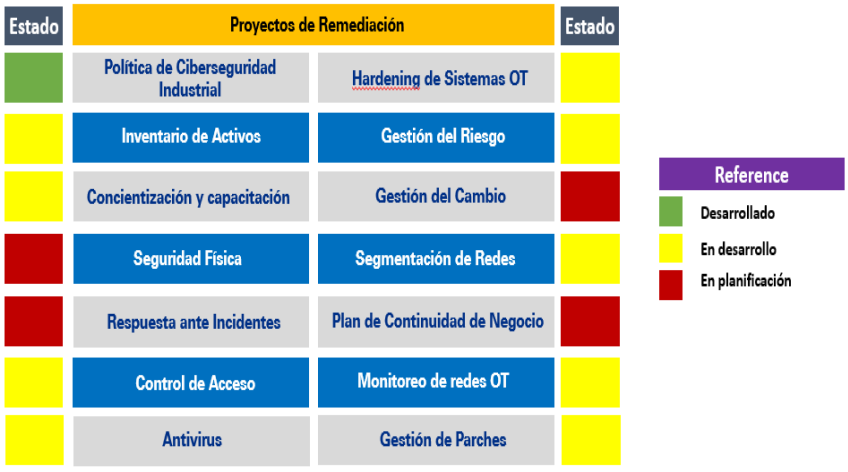


Ilustración 29. Estado actual de los planes de remediación

Fuente: Elaboración Propia

El gráfico muestra una síntesis del estado de situación de como las compañías en Argentina y Latinoamérica han ido manejando los planes de remediación que fueron recomendados después de realizar la respectiva evaluación de ciberseguridad industrial. Cabe mencionar que estas estadísticas fueron realizadas en base a un promedio de las compañías realizadas, por lo cual no refleja la situación actual de todas las empresas que entraron en alcance de este estudio.

- La mayoría de las empresas evaluadas, actualmente cuentan con una política de ciberseguridad industrial lo que muestra que los altos directivos han entrado en conciencia acerca de los riesgos que corren sus compañías en caso de que sufrieran un ciber-ataque por lo cual han empezado a establecer una gobernanza sobre esta área. Así mismo, cabe destacar que este ha sido el único plan de remediación que ya está desarrollado y se está ejecutando en las empresas.

Así mismo, se ha podido observar que actualmente las empresas han estado desarrollando los planes de remediación como:

- Hardening en sistemas OT
- Inventario de Activos
- Gestión de Riesgo
- Concientización y capacitación
- Segmentación de redes
- Control de Acceso
- Monitoreo de redes OT
- Despliegue de soluciones antivirus/antimalware en los sistemas OT
- Gestión de Parches

Cabe destacar que muchas de estas empresas aún no han empezado el desarrollo de su gobernanza acerca de ciberseguridad industrial, sin embargo, por la complejidad y la inversión que se requiere en estas tareas ha sido posible ejecutarlas escalonadamente de forma tal que puedan ir mitigando vulnerabilidades de a poco aunque todavía no cuenten con un equipo especializado en ciberseguridad industrial, esto ha sido factible ya que los

equipos de trabajo de las áreas de IT/OT se han integrado a fin de proteger su infraestructura.

Por último, las grandes deficiencias en el desarrollo y ejecución de los planes de remediación que se pudieron encontrar en la mayoría de estas compañías fueron las siguientes:

- Gestión del Cambio
- Seguridad Física
- Respuesta ante incidentes
- Plan de Continuidad de Negocio

En este caso se encontró que la gran mayoría de las empresas aún se encuentran en fase de planificación para un posterior desarrollo y ejecución de estos planes. Esto debido a que en el ambiente de operaciones no es común realizar cambios sobre la infraestructura de los sistemas de control. Así mismo, por lo general este tipo de infraestructuras se encuentran en locaciones remotas a las que no se tiene acceso fácilmente y poseen un perímetro que protege el sitio. Adicionalmente, en los ambientes industriales, los operadores suelen poseer instrucciones específicas que les permite recuperar la funcionalidad operativa de los sistemas y esto se realiza basado en la experiencia del personal. Por estos motivos, estos son los planes que más han tomado tiempo en ser desarrollados.

8. Conclusiones

Las industrias argentinas, así como las latinoamericanas, presentan enormes deficiencias en cuanto a la ciberseguridad de las infraestructuras críticas y sus operaciones. Esto las expone a riesgos que pueden detener sus operaciones y poner en riesgos la seguridad pública.

Al no poseer una regulación de ciberseguridad nacional, las empresas no tienen la obligación de informar los incidentes. Sin embargo, si tuvieran la obligación, las empresas no poseen la capacidad para detectar si fueron objeto de ciberataques. Por eso algunos incidentes son públicos y muchos otros permanecen ocultos.

Es importante destacar que en las empresas que cuentan con un área de ciberseguridad industrial, los cambios o desarrollos de nuevos productos

son ejecutados sin involucrar a esta área. Por lo cual, al no incorporar a ciberseguridad en estos proyectos, se expone a la organización a nuevos riesgos ciberseguridad que impactarían en sus líneas de proceso.

Entre los hallazgos observados, se destaca que en la mayoría de las compañías no existe una separación clara entre la red corporativa y la red industrial, esto debido a que actualmente hay servicios del ámbito corporativo que están siendo consumidos directamente desde la red industrial, sin los mecanismos de protección correspondiente. De igual forma, se observó que las compañías utilizan aplicaciones de acceso remoto no seguras como TeamViewer o TightVNC.

Algunos de los activos de control que fueron analizados en los múltiples assessments poseen varias vulnerabilidades para las cuales existen exploits publicados en internet, lo cual facilita el trabajo del atacante.

Otro punto a destacar es que en la mayoría de las empresas no hay procesos de hardening de activos industriales o de gestión de vulnerabilidades, como así tampoco procesos de monitoreo de eventos de ciberseguridad. Así mismo, en múltiples compañías se detectó que las aplicaciones utilizadas para el control del proceso industrial utilizan cuentas de usuario con privilegios elevados, y en algunos casos los sistemas operativos de los activos industriales tienen activas y en uso las cuentas de usuario de invitado.

Bibliografía.

[1] Anónimo, «Latin America,» [En línea]. Disponible: https://en.wikipedia.org/wiki/Latin_America. [Último acceso: 03 04 2020].

[2] E. Sinnott, J. Nash y A. De La Torre, Natural Resources in Latin America and the Caribbean : Beyond Booms and Busts?, Washington D.C: The World Bank, 2010.

[3] Anónimo, «Argentina,» [En línea]. Disponible: https://en.wikipedia.org/wiki/Argentina. [Último acceso: 06 04 2020].

[4] H. Altomonte, Recursos Naturales en UNASUR: Situación y tendencias para una agenda de desarrollo regional, Santiago de Chile: Cepal, 2013.

[5] L. O´Donell, «Norsk Hydro Calls Ransomware Attack 'Severe',» [En línea]. Disponible: https://threatpost.com/norsk-hydro-calls-ransomware-attack-severe/142924/. [Último acceso: 25 Marzo 2020].

[6] A. Stillman y A. Sebenius, «Pemex Faces Payment Problems After Cyber Attack Shut System,» [En línea]. Disponible: https://www.bloomberg.com/news/articles/2019-11-11/pemex-workers-barred-from-computers-after-unexpected-shutdown. [Último acceso: 08 Abril 2020].

[7] J. Vijayan, «New Malware Campaign Targets US Petroleum Companies,» [En línea]. Disponible: https://www.darkreading.com/attacks-breaches/new-malware-campaign-targets-us-petroleum-companies/d/d-id/1335966. [Último acceso: 08 Abril 2020].

[8] E. Kovacs, «Ransomware Causes Disruptions at Johannesburg Power Company,» [En línea]. Disponible: https://www.securityweek.com/ransomware-causes-disruptions-johannesburg-power-company. [Último acceso: 11 Abril 2020].

[9] E. Kovacs, «Nuclear Power Plant in India Hit by North Korean Malware: Report,» [En línea]. Disponible: securityweek.com/nuclear-power-plant-india-hit-north-korean-malware-report. [Último acceso: 09 Abril 2020].

[10] S. Khandelwal, «ZeroCleare: New Iranian Data Wiper Malware Targeting Energy Sector,» [En línea]. Disponible: https://thehackernews.com/2019/12/zerocleare-data-wiper-malware.html. [Último acceso: 13 Abril 2020].

[11] Dragos, Inc, «Threat Proliferation in ICS Cybersecurity: XENOTIME Now

Targeting Electric Sector, in Addition to Oil and Gas,» [En línea]. Disponible: https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/. [Último acceso: 15 Marzo 2020].

[12] Z. Zorz, «Widely Disponible ICS attack tools lower the barrier for attackers,» [En línea]. Disponible: https://www.helpnetsecurity.com/2020/03/24/ics-attack-tools/. [Último acceso: 21 Marzo 2020].

[13] JEFATURA DE GABINETE DE MINISTROS SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN, «Boletín Oficial de la República de Argentina,» [En línea]. Disponible: https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528. [Último acceso: 18 Marzo 2020].

[14] CCN CERT, «Argentina crea un Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad,» [En línea]. Disponible: https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/522-argentina-crea-un-programa-nacional-de-infraestructuras-criticas-de-informacion-y-ciberseguridad.html. [Último acceso: 24 Marzo 2020].

[15] ISA, ANSI/ISA–62443-2-1 (99.02.01)–2009, Nueva York: ISA, 2009.

[16] E. Knapp y J. Langil, Industrial Network Security, Massachusetts: Elsevier, 2015.