Universidad Católica “Nuestra Señora de la Asunción”

Campus Alto Paraná

Facultad de Ciencias y Tecnología

INGENIERÍA ELECTROMECÁNICA CON ORIENTACIÓN ELECTRÓNICA

Ciberseguridad, nuevo desafío para la Ingeniería de Control

Presentado por: Tomás Indalecio Armoa López

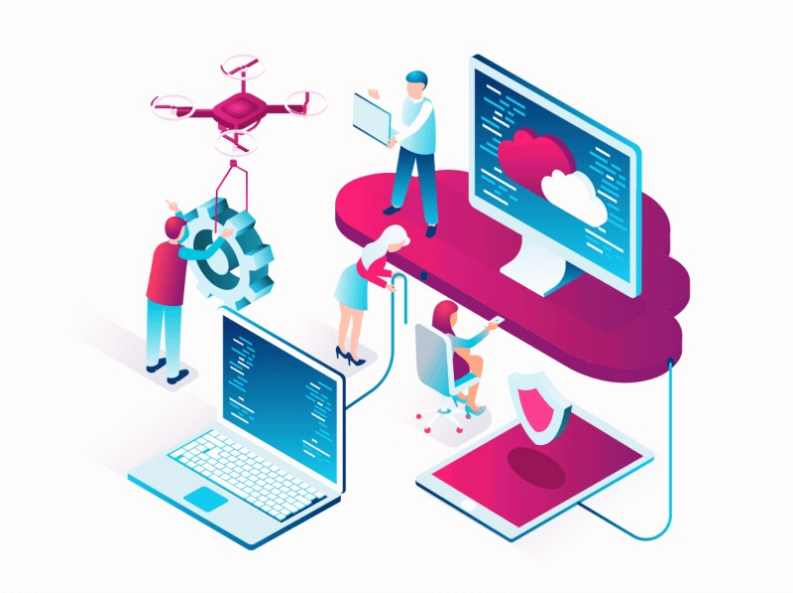
Tutor: Lic. Gregorio Ariel Guerrero Moral

Hernandarias, agosto de 2021

Contenido

Introducción

Este es un Proyecto del tipo exploratorio en el área de la ciberseguridad, orientado a explicar la importancia de la ciberseguridad para los sistemas de control industrial estableciendo una relación entre la tecnologías de información y comunicación y la Tecnología de Operación. También se evaluará casos de estudio con laboratorios virtuales tal como el propuesto por la empresa Fortiphyd Logic en conjunto con el Instituto tecnológico de Georgia creado para ser una herramienta open source para ayudar al estudio de la ciberseguridad en los sistemas de control industrial.

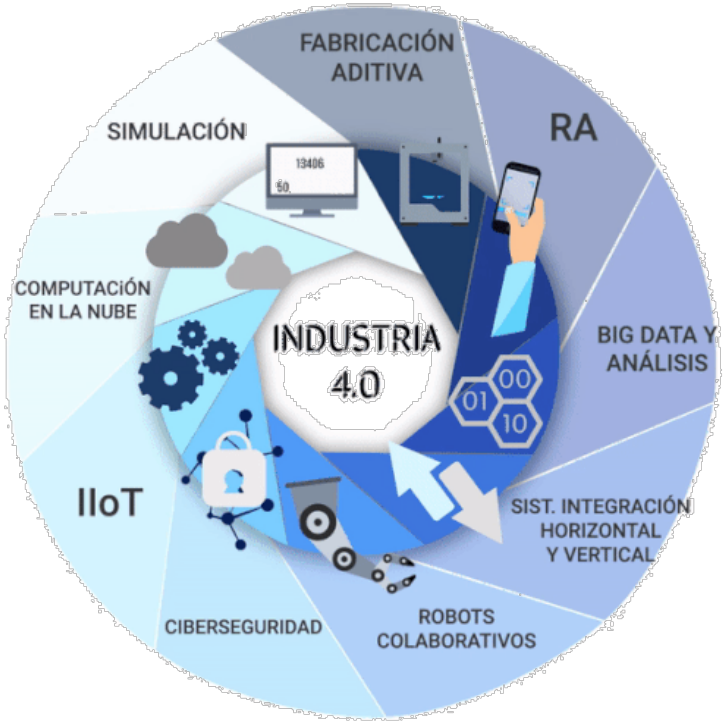


Fuente: namasteui.com, 2021

Contenido

Planteamiento del problema

La industria esta pasando por una transición a lo que hoy día es llamado como cuarta revolución industrial o industrial 4.0 y en ella aparecen nuevos conceptos como lo son IoT, IIoT, Computación en la nueve, Big Data, entre otros, lo que muchas mejoras en la industria, sin embargo consigo también trae nuevos desafíos como lo son la Ciberseguridad para los ICS



Fuente: lidtia.com.mx,2019

Contenido

Objetivo Principal

- Explicar la importancia de la ciberseguridad para los sistemas de control industrial estableciendo una relación entre la Tecnologías de información y la comunicación (TIC) y la Tecnologías de la Operación (TO), también utilizar a manera de ejemplo un caso que resulte de interés y explicar desde el punto de vista de la seguridad operacional lo que ocurrió.

Objetivos Específicos

- Investigar estableciendo el estado del arte de la Ciberseguridad.
- Establecer un concepto de Ciberseguridad y sistemas de control industrial
- Relacionar la ciberseguridad con los sistemas HMI y SCADA existentes en los sistemas eléctricos industriales.
- Determinar el marco normativo existente en el país y/o en países vecinos y aplicables para la protección de los activos industriales del sector eléctrico industrial.

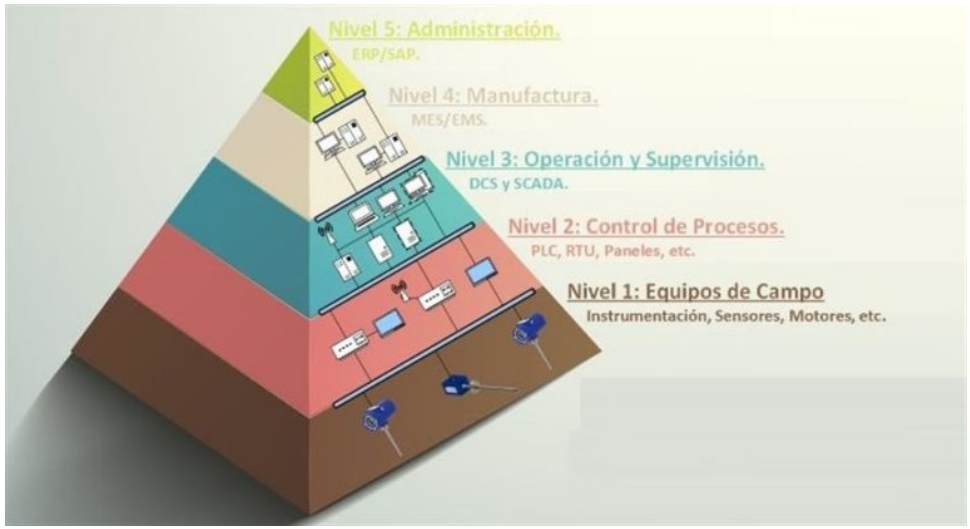
Contenido

Introducción a los ICS

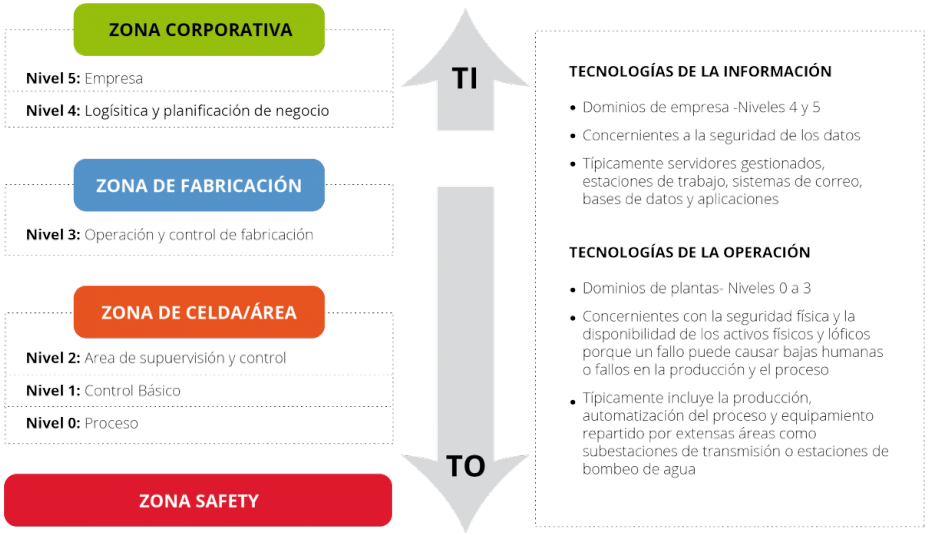
- Los ICS (Sistemas de Control Industrial) son sistemas utilizados para el control, monitorización y supervisión de los procesos industriales. Están conectados a los elementos que intervienen en el proceso (sensores y actuadores) y pueden interactuar con ellos enviando órdenes o recibiendo datos. (Barrero & Oscar Bou, 2020)
- Entre ellos podemos encontrar:
  - PLC
  - DCS
  - HMI
  - SCADA

Fuente: indagosl.com, 2021

Niveles de la ISA-95



Fuente: isamex.org, 2017



Marco lógico de jerarquía de control según el modelo de Purdue

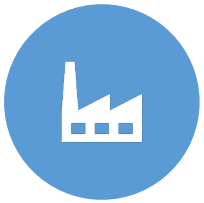
Fuente: (INCIBE, Incibe-Cert, 2019)

La nueva problemática que afronta los ICS

MALWARE CONVENCIONAL Y NUEVOS VIRUS.

ATAQUES DE RANSOMWARE

ERRORES DE LOS EMPLEADOS Y ACCIONES NO INTENCIONALES.



AMENAZAS POR OTROS ACTORES COMO LA CADENA DE SUMINISTROS O PROVEEDORES

FALLAS EN EL HARDWARE

¿Que es la ciberseguridad?

- “la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, la redes y los datos de ataques maliciosos” (Kaspersky, 2020)

Fuente: cic.es, 2020

Deficiencias existentes en los ICS

CONTRASEÑAS FÁCILMENTE EVITABLES

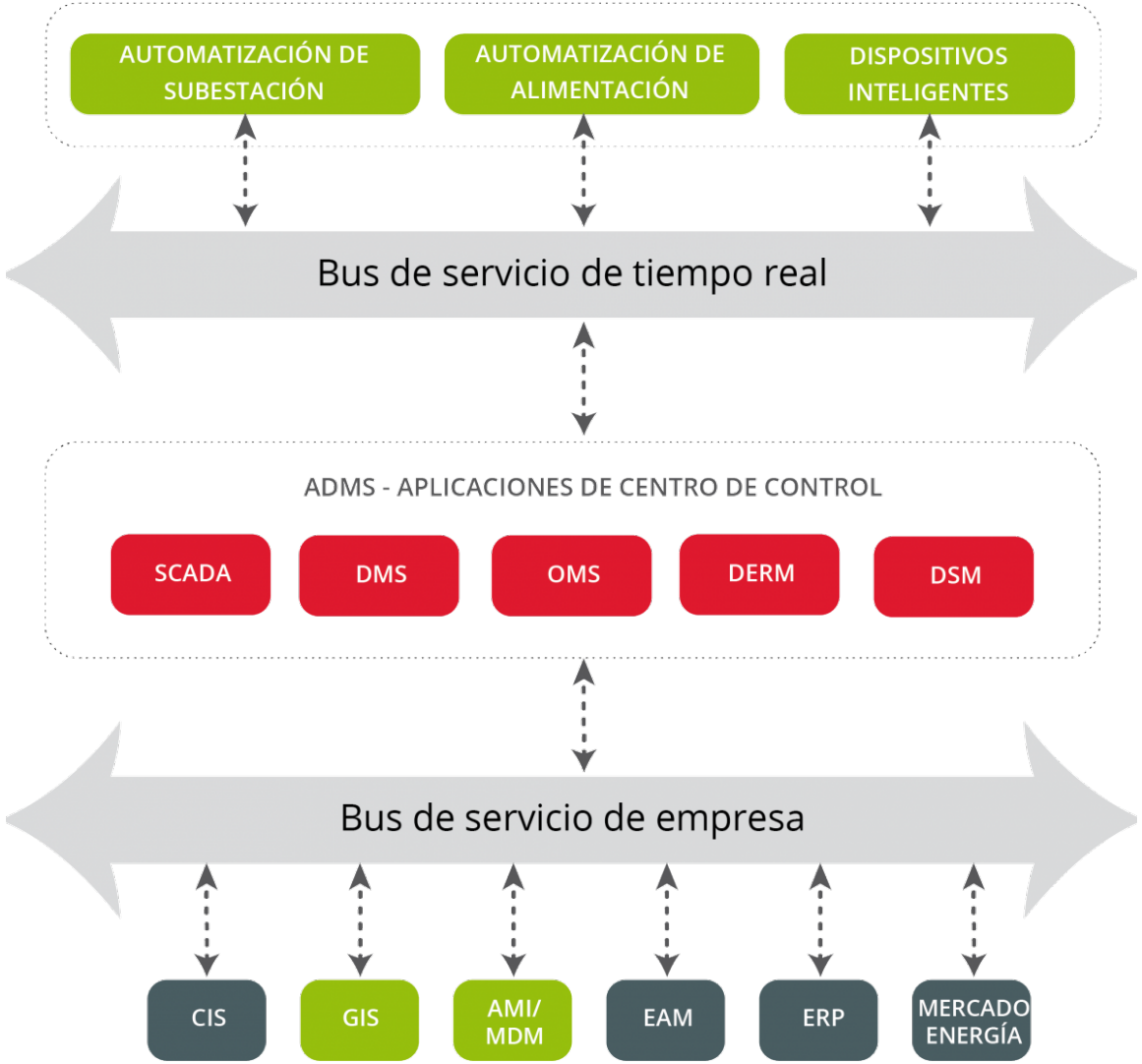
PROTOCOLOS SIN AUTENTIFICACIÓN

WEB SERVER SIN CONTRASEÑAS

QOS (QUALITY OF SERVICE) POBRE

DIFICULTAD DE PARCHEO

Convergencia TIC y TO



Redes Industriales

Protocolo Modbus

- Es un protocolo de comunicación abierto
- Un maestro puede tener hasta 247 esclavos
- Se integra fácilmente con todo tipo de dispositivos
- No posee cifrado

DNP3

- Define los datos por tipo y comportamiento
- Ancho de banda limitado para transportar datos y comandos simples
- Permite el envío de enlaces en serie, multipunto, radioenlaces, etc
- Posee un cifrado TLS que salvaguarda los sistemas conectados a través de canales TCP/IP

IEC 61850

- Lo conforman 4 protocolos, cada uno con una tarea especifica.
- Se centra en la comunicación de los activos y la protección de los equipos
- Diseñado con un enfoque orientado a objetos, permite un a configuración mas sencilla para los diseñadores.

Amenazas de los ICS

- Amenazas Internas Intencianales
- Amenazas Internas Involuntarias
- Amenazas Externas no dirigidas
- Actores Maliciosos

Vulnerabilidades de los ICS

Políticas y procedimientos

Vulnerabilidades pertenecientes al sistema

Diseño y arquitectura

Configuración y Mantenimiento

Físicos

Desarrollo de Software

Redes y comunicación

Casos de Estudio

Stuxnet

- Ataque avanzado dirigido contra la planta de enriquecimiento de uranio de Natanz, Irán
- Malware Stuxnet diseñado para funcionar únicamente en planta de Irán
- Se descubrió únicamente debido a que se propago fuera de la planta
- Se cree que el virus llego a través de una unidad USB
- El Virus alteraba la velocidad de las centrifugadoras a mayor velocidad causando daños en las mismas.

Fuente: safebytes.com, 2021

Ukraine Cyber-Induced Power Outage:

1. Spear Phishing
2. Malware usado para explorer y moverse a traves de la Red
3. Obtencion de Credenciales
4. Creacion de un tunel VPN
5. Reconocer y comprometer computadores con HMI
6. Manipulacion de Cortocircuitos
7. Ataques Adicionales
   - TDOS (Telephony Denial of Service)
   - UPS Remote Access and Shutdown
   - Malicious Firmware Update
8. Malicius Firmware Update

Fuente: cdn.videoplasty.com,2021

Ethical Hacking

- Ethical Hacking o Hacking Ético como su nombre lo indica trata sobre el uso correcto de los conocimientos informáticos, y con estos mismo conocimientos mejorar la seguridad de la empresa mediante auditorias de seguridad.

Fuente: encrypted-tbn0.gstatic.com, 2020

¿Que es un Hacker?

- Según la RAE en su segunda definición hacker se podría definir como “Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora”. (Mendoza, 2018)

Fuente: sithcomputers.com, 2021

Tipos de Hackers

- White Hat Hacker
- Grey Hat Hacker
- Black Hat Hacker

Fuente:techcrunch.com,2021

Pentesting

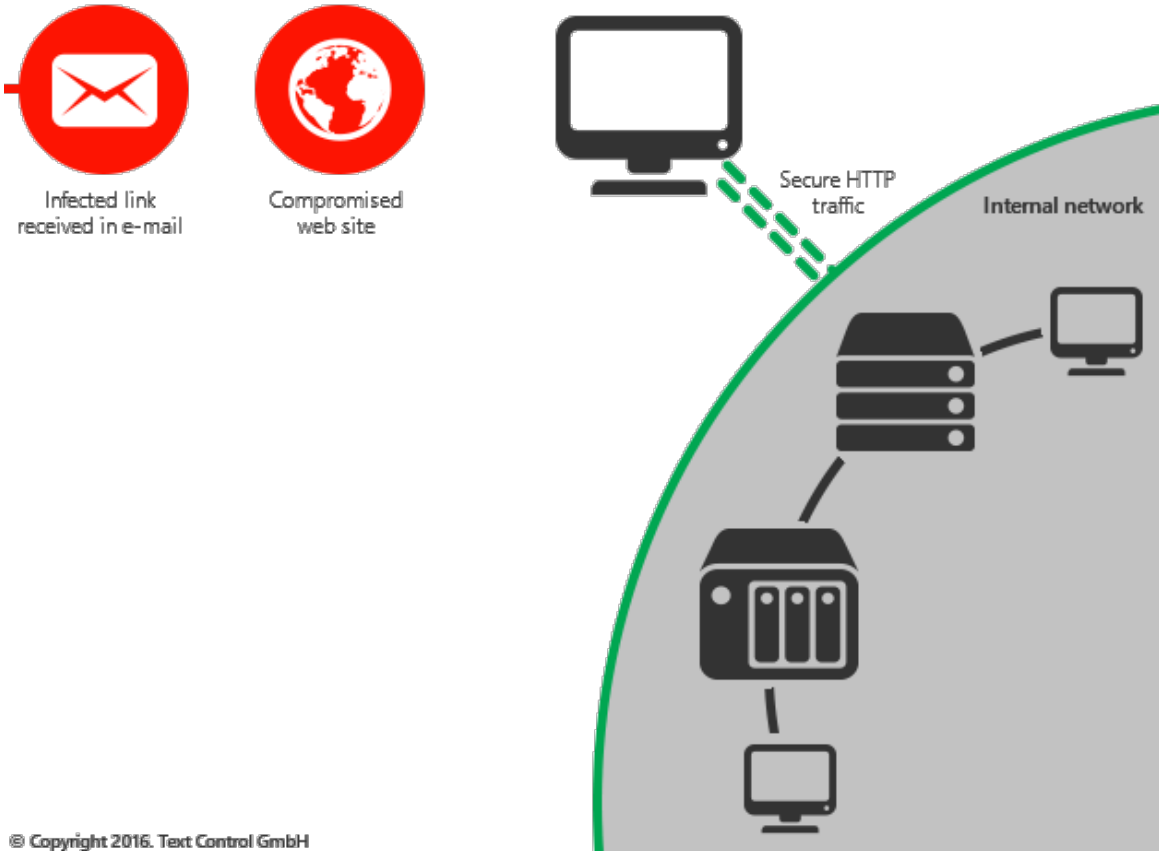
- White Box
- Black Box
- Grey Box

Fuente: exevi.com,2020

Contenido

Aproximaciones a la protección de los ICS

- Firewalls
- VPN
- IDS
- IPS
- Antivirus
- Protocolos Encriptados



Normativas referentes a la ciberseguridad y a ICS

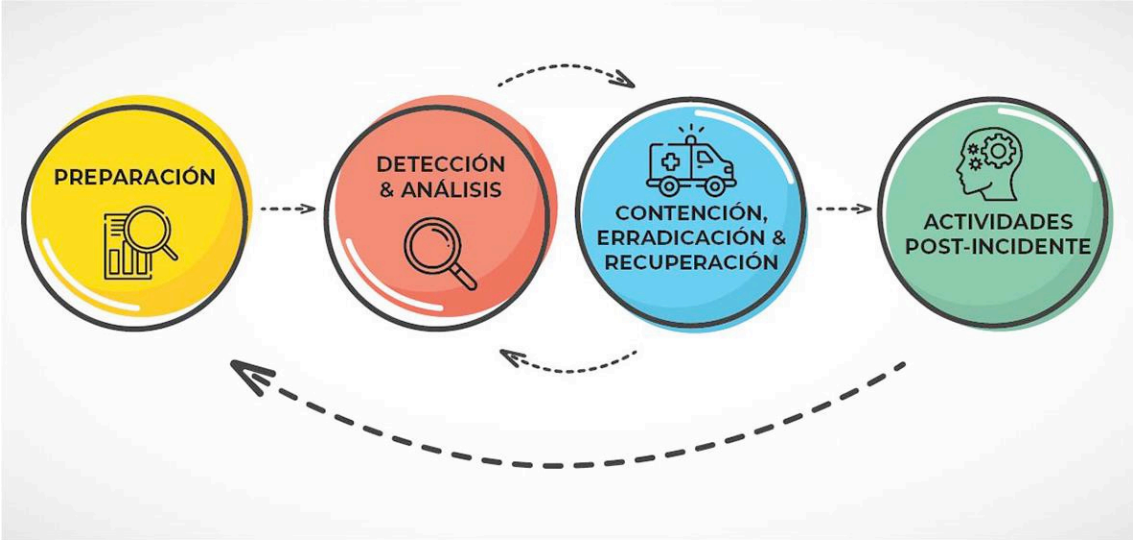
- ISA 99/ IEC 62443
- NIST SP 800-82 “Guía para la Seguridad de los Sistemas de Control Industrial (ICS)”.
- La Familia de normas ISA 27000

Estado de preparación de Paraguay con respecto a la Ciberseguridad

Fuente: cert.gov.py, 2021

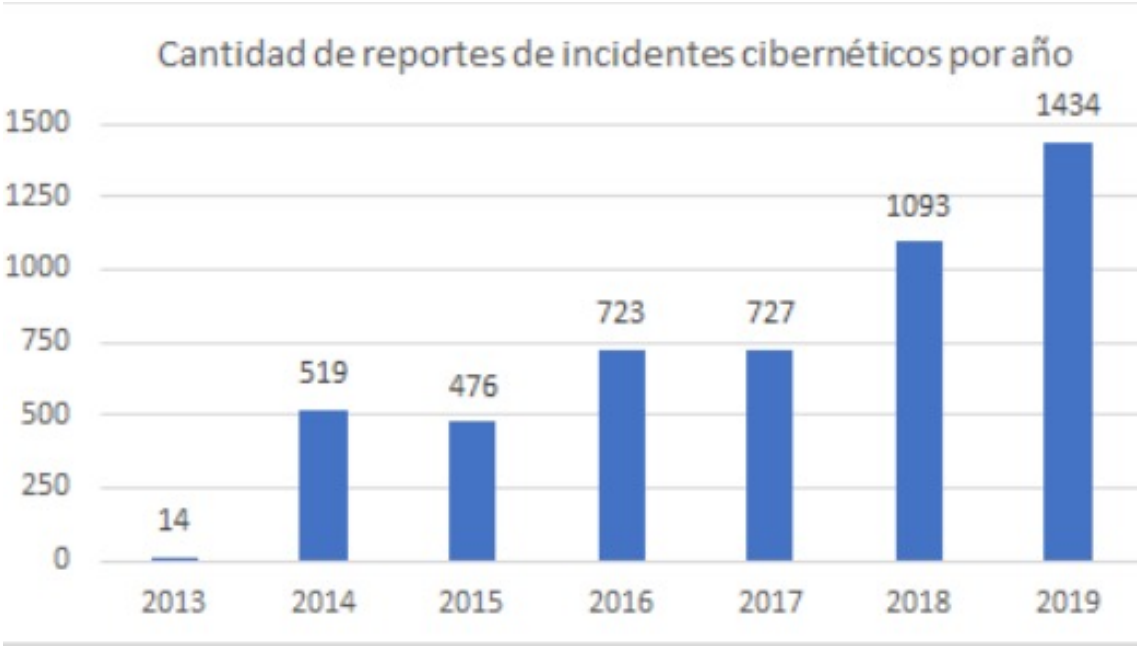
CERT-PY

- El Centro de Respuestas a Incidentes Cibernéticos (CERT-PY) es el organismo coordinador de incidentes cibernéticos que afectan al ecosistema digital nacional bajo la estructura funcional de la MITIC (anteriormente SENATIC).



Reporte de incidentes cibernéticos

- Según el ultimo reporte emitido por la CERT-PY en 2019
  - Reportes recibidos: 4986
  - Cantidad total de incidentes atendidos: 470
  - Investigaciones realizadas: 770



Protección de Infraestructuras Criticas

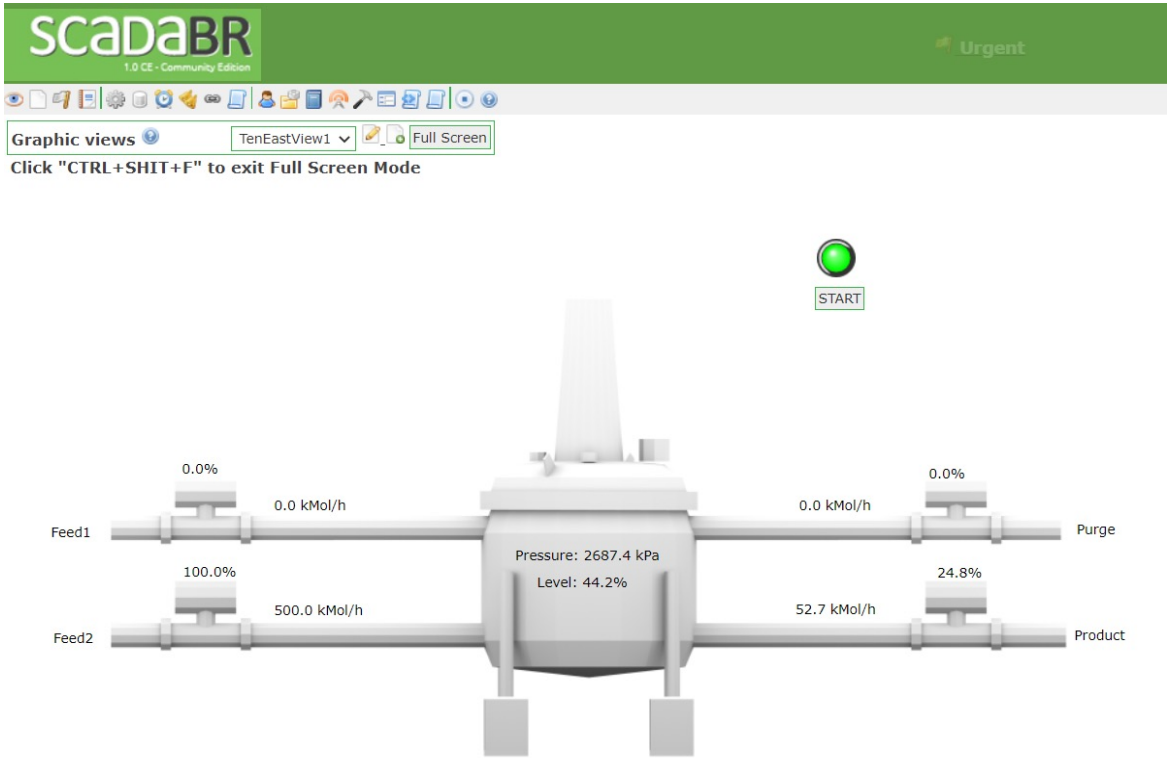
En el Plan Nacional de Ciberseguridad también se anexa un plan de acción enfocado a las infraestructuras críticas en la cual divide la misma en dos aspectos fundamentales:

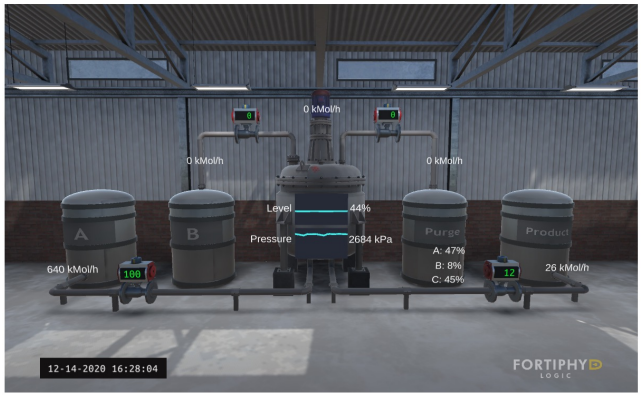
- La resiliencia de las infraestructuras criticas ante las amenazas cibernéticas y garantizar la estabilidad de los servicios esenciales.
- La responsabilidad por la ciberseguridad de las infraestructuras criticas es compartida tanto entre el estado y el sector privado, para fomentar la cooperación público-privada

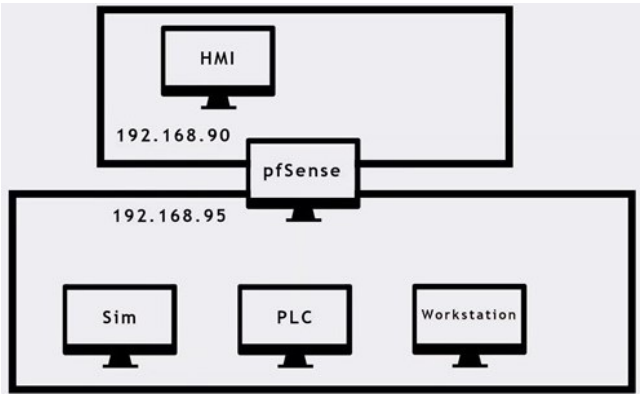
Prueba de Concepto

Fuente: icon-library.com, 2021

Segunda Escenario

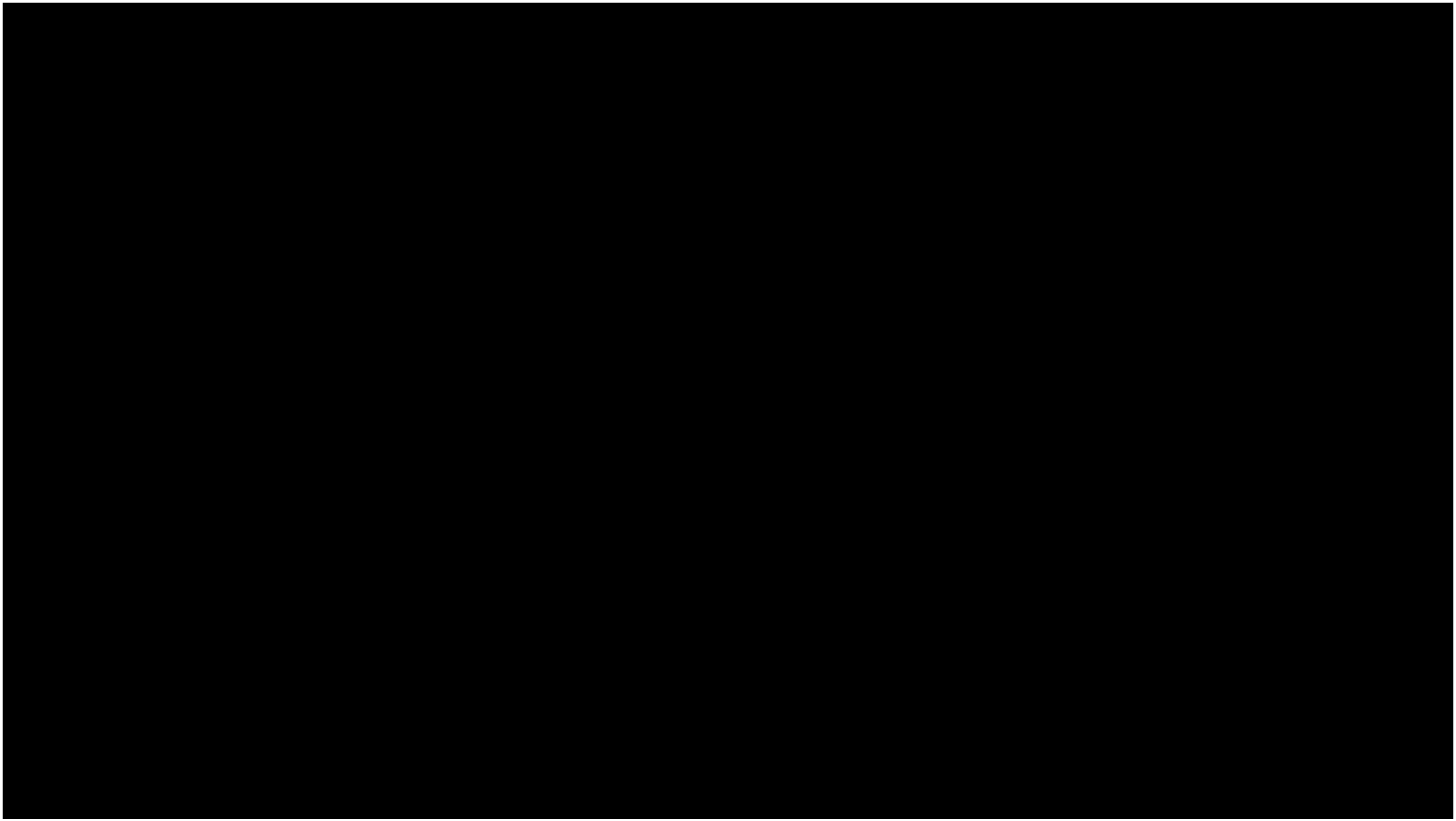






Fuente: preventionofcybercrime.com, 2021

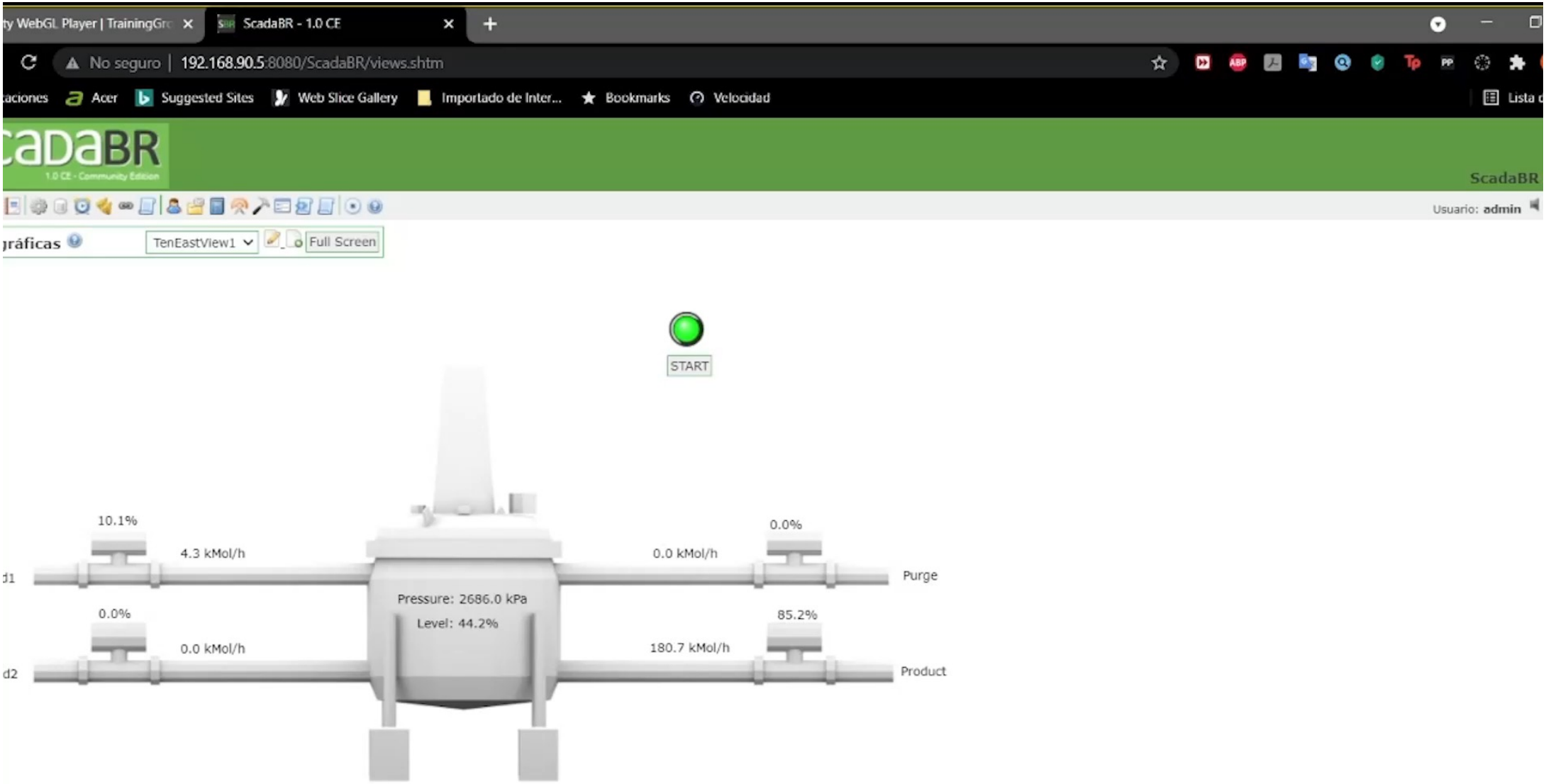
Ataque



Defensa

- Limitar la comunicación entre las redes mediante IP

Fuente: cybergood.io, 2021


ScadaBR - 1.0 CE
No seguro | 192.168.90.5:8080/ScadaBR/views.shtm
Acer
Suggested Sites
Web Slice Gallery
Importado de Inter...
Bookmarks
Velocidad
ScadaBR
Usuario: admin
TenEastView1
Full Screen
START
10.1%
4.3 kMol/h
0.0%
0.0 kMol/h
Purge
Pressure: 2686.0 kPa
Level: 44.2%
0.0%
0.0 kMol/h
85.2%
180.7 kMol/h
Product

Contenido

Resultados

- En ambas prueba pudimos observar lo fácil que es para el atacante acceder a la red TO si no se segmenta correctamente.
- La importancia de contar con un protocolo que cuente con autentificación y encriptado
- También lo importante de una buena configuración del Web Server, esto quiere decir que este parcheado en su ultima versión y que cuente con un sistema de autentificado

Contenido

Conclusión

- Con estas pruebas realizadas se pudo constar de la importancia que tiene la ciberseguridad en los Sistemas de control industriales y la importancia de su constante estudio ya que cada día mas vulnerabilidades son detectadas
- Con esto también cabe resaltar la necesidad de incorporar en la carrera de Ing. Electromecánica la materia de ciberseguridad industrial o al menos incorporar este estudio a las material de automatismo ya que es ahí donde mas se presentan estos casos.

Trabajos Futuros

- Estudio del estado preparación de la infraestructura críticas del Paraguay
- Estudio de la normativa ISA 62443 para ciberseguridad industrial
- Estudio de la normativa IEC 61850 para ciberseguridad en las subestaciones Eléctricas.

¡Gracias por su atención!

Bibliografía

- Barrero, V., & Oscar Bou, E. J. (2020). *Estado de preparación en ciberseguridad del sector eléctrico en América Latina.*
- Weiss, J. (2010). *Protecting Industrial Control Systems From Electronic Threats.* New York: Momentum Press.
- SENATIC. (2017). *Plan Nacional de Ciberseguridad.*
- David E. Whitehead, K. O. (2017). *Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies.*
- (NIST), N. I. (2021). *National Institute of Standards and Technology U.S. Department of Commerce*. Obtenido de https://www.nist.gov/