Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas

Article · November 2015

CITATIONS
0

READS
152

4 authors, including:

Jorge Kamlofsky
Interamerican Open University
6 PUBLICATIONS **1** CITATION
SEE PROFILE

Hugo Roberto Colombo
University of Buenos Aires
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas

Jorge Kamlofsky, Hugo Colombo, Matías Sliafertas, Juan Pedernera
CAETI - Universidad Abierta Interamericana
Av. Montes de Oca 725 – Buenos Aires – Argentina.
{Jorge.Kamlofsky, Hugo.Colombo}@UAI.edu.ar
{MatiasNicolas.Sliafertas, JuanManuel.PedderneraGaitan}@alumnos.UAI.edu.ar

Abstract

Los Sistemas de Control Industrial (ICS según sus siglas en inglés) consisten en máquinas y equipos que automatizan procesos de producción. Los ICS no sólo automatizan la producción de bienes transables, sino que también se encuentran en las infraestructuras críticas de las naciones: plantas potabilizadoras, producción y distribución de energía, y demás. La convergencia entre las redes corporativas, con gran cantidad de falencias de seguridad y las redes industriales, han dejado a estas últimas en total vulnerabilidad. En este trabajo, se presenta una selección de ciber-ataques a redes industriales e infraestructuras críticas y se propone una solución para atenuar los efectos de ciber-ataques.

1. Introducción

1.1. Trabajos Relacionados

Los sistemas informáticos son cada vez más importantes y su seguridad se ha acentuado. Nuevos ataques, vulnerabilidades y profesionalización del "*malware*" requieren estrategias claras y concisas de seguridad que minimicen riesgos con un esquema de defensa en profundidad [1]. La interconexión creciente de dispositivos a través de internet ha llegado hasta el ámbito doméstico [2], haciendo que aparezcan vulnerabilidades nuevas.

Distinto es el caso de los ICS: Son redes de tele-mando y telecontrol de procesos compuestos por autómatas industriales (los "PLCs") interconectados entre sí y cada uno de ellos a sensores (caudalímetros, sensores de nivel, etc.) y/o a actuadores (motores, válvulas, etc.). Se diseñaron para supervisar y actuar sobre procesos industriales. El aislamiento del proceso de producción, les dio por muchos años una sensación de seguridad ilusoria gracias al ocultamiento.

Los ICS son muy robustos. Hoy están presentes en plantas de potabilización de agua, producción y distribución de energía, transporte, telecomunicaciones, es decir, están en infraestructuras críticas de naciones. Los SCADA (por sus siglas en inglés: Supervisory Control and Data Acquisition) se idearon para controlar sistemas industriales, conectando PC y redes de autómatas industriales; siendo la interfaz hombre máquina (HMI: Human – Machine Interface).

Con el tiempo surgió la necesidad de vincularlos a la red corporativa e incluso a internet. Su interconexión dejó a los ICS expuestos a amenazas y riesgos, los que suponen serias consecuencias [3]. Hoy es posible, mediante dispositivos móviles, controlar un ICS, desde cualquier lugar del mundo con cobertura de red móvil [4], lo que supone un escenario ideal para explotar vulnerabilidades e inyectar malware. Es evidente que la tecnología corporativa y la industrial dejaron a la seguridad entre ambas [5].

Hasta hace pocos años, era impensable que se pudiera infectar con virus informático a un ICS. En el año 2010 las plantas nucleares de Irán fueron atacadas por un virus informático llamado Stuxnet, lo que desconcertó a analistas estratégicos de todo el mundo. La comunidad internacional mostró preocupación por la seguridad [6 – 8], trabaja en soluciones [9 – 12] y se atienden los reportes de incidentes de los sistemas conectados [13].

En el ámbito de las tecnologías corporativas se tiene experiencia en Seguridad. Las recomendaciones de las normas ISO27000 ayudan a proteger la seguridad de los activos informáticos [14]. La criptografía es clave para asegurar sistemas informáticos. Es posible dar seguridad criptográfica a dispositivos con baja capacidad de cómputo (como son los "PLCs") gracias al desarrollo de algoritmia criptográfica de clave pública basada en estructuras algebraicas de anillos no conmutativos [15] la cual a fecha actual es inmune a ataques cuánticos.

Este trabajo contiene una selección de incidentes en ICS y/o en infraestructuras críticas; con sus causas y un enfoque para mitigar los efectos de ciber-ataques.

1.2. Motivación y Alcance

El incremento en la conectividad de los ICS a otras redes es inevitable, y por consiguiente la aparición de nuevas vulnerabilidades. Motivo por el cual, este trabajo pretende realizar aportes a las estrategias de ciber-defensa de infraestructuras críticas, tanto desde el aspecto

metodológico, como algorítmico, acompañado por mejoras sugeridas en las redes de comunicaciones.

1.3. Estructura del Trabajo

La Sección 2 presenta detalles técnicos (Estado del arte) de Redes Industriales y conceptos de Seguridad Informática. La Sección 3 presenta incidentes causados por ciber-ataques a sistemas SCADA. La Sección 4 detalla ciber-ataques graves, y presenta conceptos relacionados. La Sección 5 muestra diagnóstico de ataques. La sección 6 presenta un enfoque para reforzar la ciber-defensa y la sección 7 muestra su impacto.

2. Marco Teórico

Al considerar dónde se producen estos ataques, se debe pensar en los bloques que conforman un sistema de control industrial: Gestión corporativa y producción industrial. En el sector industrial, hay sistemas de control de producción, que vinculan las redes de gestión e industrial en sí. La última posee dos capas, la que efectúa controles, además de controladores lógicos programables [16], donde estos reciben información de la capa de detectores e instrumentos de medición, que se conectan al equipo de producción propiamente dicho, ejecutando acciones y/o efectuando controles y mediciones de variables de los procesos productivos. Las mediciones se envían mediante el sistema de control, al sistema de gestión para cerrar el ciclo de la entidad considerada.

Los vínculos entre capas se construyen con redes industriales, en las capas inferiores y luego se llega a la red de administración / gestión, la que en la mayoría de los casos contiene tramos del tipo "*ethernet*" con capas de red bajo el protocolo TCP IP [17].

2.1. Redes Industriales

Las redes industriales poseen exigencias propias de un ambiente más agresivo por vibraciones, ruido eléctrico, temperatura y tensión con rangos más amplios a los convencionales [18]. La particularidad de la pequeña cantidad de dígitos a transmitir hace que las grandes tasas de transferencia que se poseen en una empresa, resulten menos relevantes. Son sistemas de medición y en muchos casos, de tiempo real [19] [20], que brindad datos periódicos [18]. De ahí que la seguridad es fundamental [18]: si se altera un dato, el resultado del comando será inadecuado. Este es el concepto básico a considerar en el proyecto "*Cripto/CIDEI*" de la UAI [21].

En una red "*ethernet*", hay colisiones [22] y retardos en caso de un error de transmisión [23] que puede ocasionar que se desconozca el orden de las alarmas, los que debe solucionarse, por ejemplo, como propone Ferreira [18], con el uso de un sello de hora.

A la fecha hay un vuelco hacia el uso de redes inalámbricas, lo que genera potenciales puntos de falla.

Se presentan los principales protocolos usados en ICS.

Modbus: Líneas RS232 o RS485 (EIA/TIA). Existe versión para protocolo de "internet". Comunicación maestro esclavo. Envía un comando a la dirección del esclavo, quien responde con formato similar y lleva el código de la instrucción solicitada y la respuesta [24].

Bluethoot: Enlace tipo punto a punto, que usan equipos homologados (Res. CNC N°511 /2000), con inscripción innecesaria, si la potencia isotrópica radiada equivalente es inferior a 10 mW, usan banda de 2,4 GHz.

Otros tipos de redes: CANbus, Red de Área de Control, DeviceNet, Profibus, Profibus PA, Hart [16].

2.2. Seguridad Informática (SI)

La Seguridad en Sistemas Informáticos, asegura los activos informáticos. La política de SI debe ser integral.

La SI en los Usuarios: Gran parte de los problemas de SI se deben a acciones negligentes o a causa de la falta de capacitación. Los riesgos no pueden eliminarse totalmente: deben gestionarse por medio políticas de buenas prácticas y uso de estándares recomendados [14].

La SI en las Redes: Se debe evitar el acceso de intrusos manteniendo la confidencialidad, integridad, disponibilidad y control de la red. Es útil un sistema de seguridad en capas: cortafuegos, IDS ("Sistemas de Detección de Intrusos"), IPS ("Sistemas de Prevención de Intrusos"), ACL ("Listas de Control de Accesos") y sistemas de autenticación. El perímetro se protege con cortafuegos. En la red puede crearse una DMZ ("zona desmilitarizada") para acceso externo a servidores FTP, web, etc., dejando al resto de la red protegida. Dentro del mismo cortafuego pueden instalarse IDP, IDS para que actúen inmediatamente.

La SI en las comunicaciones: Las comunicaciones se pueden cifrar sin demoras notables ni complicaciones para las tareas de los usuarios. Por eso es recomendable el cifrado de las comunicaciones donde sea posible.

La SI en los Terminales: Las terminales no deben presentar vulnerabilidades ante ataques. Tanto el sistema operativo, como el antivirus deben estar actualizados.

Algunos Riesgos a la SI: Hay herramientas muy útiles, las cuales son peligrosas en manos de intrusos: Wireshark[1] escucha los puertos, por lo que es posible obtener claves de acceso, Cain & Abel[2] copia de la red información mediante un ataque del tipo "*man in the middle*" logrado por "*ARP-Poissoning*". NMap[3] escucha puertos de red.

[1] https://www.wireshark.org/
[2] http://antisec-security.blogspot.com.ar/2012/09/sniffing-cain-abel-cain-abel-es-una.html
[3] https://nmap.org/

2.3. SI en Redes Industriales

Las redes ICS, se diseñaron para estar aisladas. Su conexión a las redes corporativas da puntos de falla y/o ataque. Hay topologías que omiten la separación lógica lo que permite el acceso de usuarios no deseados.

Las redes WIFI, ocultan el punto de acceso y de ahí que se pueda acceder tanto accidentalmente o bien para atacarlas. Mediante dispositivos móviles, puede accederse fácilmente. Permitir estos accesos puede dejar inoperativa una red mediante lectura de puertos TCP o UDP de los servidores críticos ya que estos no fueron pensados para ese escenario y actúan inestablemente frente a ataques tipo Fuzzing, de denegación de servicio (DOS) o simples escaneo de puertos. Podrían lograrse ataques clásicos como "*man in the middle*".

3. Algunos Eventos de Ciber-seguridad en Redes Industriales

En esta sección, se presenta una selección de incidentes de ciber-seguridad en sistemas SCADA.

3.1. Incidentes documentados en RISI

Selección obtenida de la base de datos RISI [13].

Industria Papelera, Canadá, 1998: Un empleado enojado cambió las claves de acceso a los PLCs. Se debió reinstalar el software en cada PLCs. La clave maestra había sido hallada en un post-it.

Industria Electrónica, Reino Unido, 2002: Hackers enviaron un mensaje con código java scritp y el texto: "*Hello! Welcome to http://worm.com Hacked by Chinese*". Expuso un bug en la pila TCP/IP.

Industria Química, Estados Unidos, 2002: La IP de la PC de control se cambió por la IP de la PC de monitoreo de emisiones provocando el bloqueo de la segunda. El operador de control cambió la IP para poder acceder a juegos por internet. Se debió apagar la planta.

Industria Petrolera, Noruega, 2003: Los Sistemas Grane de ABB instalados en la planta fueron infectados por virus. Se solucionó instalando antivirus.

Industria Metalúrgica, Estados Unidos, 2003: Todos los PLC-5[4] (ethernet) de la planta perdieron su memoria. Se descargó la solución por conexión serie.

Industria Petrolera: Estados Unidos, 2003: El virus SQL Slammer[5] ingresó a los terminales SCADA desde de la red corporativa. Se instalaron paquetes y/o se retiraron servidores con MS SQL-Server.

Industria sin Definir, Estados Unidos, 2002: Antiguos PLC-5 enviaron paquetes ICMP redirect[6] mal formados a todos los dispositivos en el sistema.

Industria Petrolera, País no Especificado, 2003: Una laptop que tenía una versión no actualizada de MS SQL-Server se conectó a Internet vía un ISP y se contagió con el virus SQL Slammer.

Industria sin Definir, País no Especificado, 2003: Código malicioso fue encontrado en un PLC.

Industria Petrolera, Chad, 2004: Una falla grave de la red ocurrió luego de una infección con un virus. Se identificaron dos virus.

Industria Energética y de Servicios públicos, Estados Unidos, 2004: Tres terminales de operación del SCADA fueron atacadas por el virus W32/Korgo[7].

Planta de Tratamiento de Agua, Canadá, 2004: Se halló virus en las terminales HMI: contenía un keylogger y apertura de un túnel hacia un sitio externo.

Transporte Ferroviario, Japón, 2005: Una definición de virus errante fue distribuida desde una empresa de antivirus: Trend Micro[8], causando una interrupción a gran escala (10 millones de usuarios).

Tratamiento de Agua, Australia, 2005: Se detectaron tres tipos de virus en laptops.

Industria Energética, Estados Unidos, 2012: Se descubrió un virus en 10 PCs del sistema de control de una turbina de una planta de energía. Un técnico externo usó una memoria USB infectada.

Planta Energética, Estados Unidos, 2012: En una memoria USB usada habitualmente para hacer resguardos de los sistemas, se hallaron tres virus.

Planta industrial, Estados Unidos, 2012: Usando un backdoor en los sistemas Niagara AX ICS de Honeywell, hackers accedieron al sistema de control.

Industria Energética, Estados Unidos, 2012: Un reactor de una planta nuclear, se apagó ya que una PC de control del reactor no funcionaba correctamente.

Industria Petrolera, Irán, 2012: Varias plantas petroleras tuvieron que desconectarse tras sufrir un ataque con malware.

Industria Metalúrgica, Alemania, 2014: Atacantes perpetraron un ataque de Ingeniería Social que les permitieron acceder a la red de los sistemas de control lo que provocó daños masivos en toda la planta.

3.2. Otros Ataques documentados

Ataques documentados en otros orígenes de datos.

Malware Slammer, 2003: La planta de energía nuclear de Davis-Besse fue víctima del malware Slammer [25]. Provocó un agujero de entre 5 a 6 pulgadas en la cabeza de un reactor.

Malware Sasser, 2004 (dos ataques): Las empresas Railcorp, British Airways y Delta Airlines fueron afectadas por el malware Sasser, que explotó una vulnerabilidad del archivo lsass.exe en Windows [26].

[4] http://ab.rockwellautomation.com/es/Programmable-Controllers/PLC-5-Controllers
[5] https://es.wikipedia.org/wiki/SQL_Slammer
[6] https://support.microsoft.com/es-es/kb/195686
[7] https://www.f-secure.com/v-descs/korgo.shtml
[8] http://www.trendmicro.es/

Malware Conficker, 2009: El virus Conficker, afecto al ejército francés gracias a una vulnerabilidad de Windows. Este ataque trajo inconvenientes en la descarga de planes de vuelos [26].

Malware Night Dragon, 2009 (varios ataques): Petroleras y petroquímicas como Exxon, Shell, BP, fueron atacados por el virus Night Dragon permitiendo control total en forma remota. Los atacantes filtraron planos de los sistemas SCADA [26].

4. Ciber-guerra y Ciber-terrorismo

Las infraestructuras críticas de las naciones son objetivos de máximo interés en escenarios de ciber-guerra o ciber-terrorismo: pueden realizarse ataques certeros a objetivos de países enemigos sin dejar huellas. La ciber-guerra mundial (WWC) contempla desde espionaje hasta ataques destructivos. Se desarrolla en un campo de batalla oscuro. Se usan botnets y malware. Los combates son permanentes. No producen imágenes dramáticas frente a la opinión pública mundial, pero los daños crecen día a día [29]. Los ciber-terroristas, en cambio, realizan daños físicos a instalaciones de empresas o infraestructuras críticas. Dragonfly es un grupo de hackers que se especializa ICS. Se dice que es de origen ruso: dado que los ataques con Stuxnet se los atribuye a Estados Unidos, surgen como contrapeso.

En esta sección se presentan algunos ataques cibernéticos trascendentes y de alto impacto mundial.

4.1. Ataques DDoS masivos: Estonia, 2007

En Estonia, en Abril de 2007, reiterados ciber-ataques dejaron fuera de servicio sitios gubernamentales, de medios de comunicación y universidades (ataques *Distributed Denial of Services - DDoS*). El 19 de Mayo de 2007 todos los sitios volvieron a funcionar. Así finalizó la primer ciber-guerra. Los ataques se iniciaron luego de que el gobierno de Estonia decidiera retirar un monumento del centro de Tallin lo que provocó la queja de Rusia. Estonia acusó a Rusia: nada se pudo probar [7].

4.2. Uso del Virus Stuxnet: Irán, 2010

El virus Stuxnet fue usado para atacar las plantas de enriquecimiento de uranio de Natanz. El ataque fue un éxito. Esta fue, entonces, la primer oportunidad en la que se usaron herramientas informáticas con fines y contra objetivos puramente bélicos [27]. El vector de la infección fue una memoria USB.

Stuxnet solo ataca equipos que tienen en ejecución software SCADA WinCC y PCS 7 de Siemens usando un exploit llamado MS08-067[9]. Microsoft ha realizado un patch. Pero se supone que los atacantes sabían que en los SCADA pocas veces se instalan las actualizaciones priorizando la estabilidad de los sistemas por sobre todo.

4.3. Ciber-ataque a la mayor petrolera del mundo: Aramco (Arabia Saudita, 2012)

Aramco sufrió un ataque masivo que dejó fuera de servicio 35.000 terminales con sistema operativo Windows por casi 6 meses. El reestablecimiento estuvo a cargo de la analista Cris Kubecka quien publicó los detalles en la última Black hat[10] [28].

La infección se inició cuando un empleado abrió un correo electrónico fraudulento en un ataque del tipo phishing ejecutando el virus Shamoon/W32.distract. Su principal función es la eliminación indiscriminada de archivos de los discos rígidos.

4.4. El ciber-espionaje masivo y el hacktivismo.

A fecha actual, el espionaje se realiza masivamente usando tecnologías informáticas. La violación a privacidad de las personas es cotidiana y no tiene frontera, tal como fuera expuesto por Edward Snowden[11].

El hacktivismo comprende acciones de activistas políticos de escala mundial que usan herramientas informáticas para golpear a sus objetivos. Anonymous[12] es el referente hacktivista más importante del mundo. Poseen alta capacidad ciber-bélica. Su rango de acción es muy amplio: atacan a empresas, gobiernos y organismos que cometen abuso de poder sobre la ciudadanía.

5. Análisis de los Ataques

Un breve análisis de los casos expuestos (ver Tabla 1), deja en evidencia la necesidad de contar con una gestión integral que permita tratar riesgos y minimizar pérdidas.

Tabla 1: Resumen de los ataques

	Alta	Baja
Gravedad de los ataques	46,43%	53,57%
	Si	**No**
¿Hubo pérdidas económicas?	64,29%	35,71%
	Si	**No**
¿Se perdió el control del sistema?	57,14%	39,29%
	Si	**No**
¿Hubo ataques activos de hackers?	21,43%	78,57%
	Si	**No**
¿Hubo fallas humanas de empleados?	32,14%	67,86%
	Si	**No**
¿Hubo alguna falla de un sistema?	50,00%	50,00%
	Si	**No**
¿Se encontró Virus?	71,43%	28,57%
	Si	**No**
¿Funcionó la prevención?	10,71%	89,29%

[9]Gracias a una vulnerabilidad en sistemas Windows, atacantes pueden ganar acceso total al sistema para ejecución de cualquier código.

[10]https://www.blackhat.com/us-15/

[11]http://www.theguardian.com/us-news/the-nsa-files

[12]https://twitter.com/youranonnews

6. Solución Propuesta

Se propone una solución que incluye: red con seguridad perimetral, gestión de la SI, criptografía y consideraciones respecto de hardware y software.

6.1. Topología de Red

Se recomienda trabajar con redes segmentadas lógicamente, utilizando Firewalls que permitan realizar un filtrado del trafico, Routers con manejo de Vlans para efectuar una separación lógica de los diferentes segmentos, con ACL, contar con IDS/IPDS a fin de poder detectar ataques en el momento en el que suceden. La figura 1 presenta una topología propuesta. Puede evidenciarse la presencia de controles de acceso físicos rigurosos, redes segmentadas, firewall back-to-back, red DMZ para la granja de servidores comunes críticos, routers que permiten una segmentación mediante Vlans. Asi mismo se debería contar con un SOC (Securty Operation Center) y un NOC (Network Operation Center) desde donde se pueda efectuar el monitoreo en tiempo real de los servidores y dispositivos de seguridad.

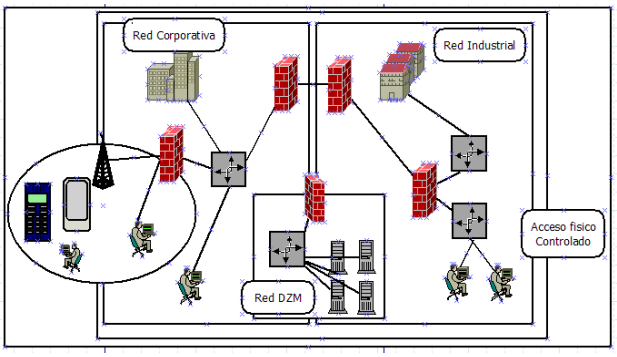

Fig. 1. Topología de red propuesta

6.2. Consideraciones acerca de la Gestión de la SI

Las normas ISO 27001 por sí mismas presentan un conjunto de buenas prácticas para la gestión de la SI.

El factor humano es el mas vulnerable. Es importante contar con un plan de capacitación continua y otorgarles permisos de acceso mínimo. Todos los terminales y los puntos de acceso a la red deben poseer antivirus actualizado. Se sugiere contar con una correcta gestión de la seguridad física del entorno. Es necesario tomar medidas preventivas y correctivas en base a procedimientos de gestión y manejo de incidentes, *Penetration tests* y análisis de vulnerabilidades tanto por equipos internos como externos. Así se podrá tener un esquema de defensa en profundidad que afecte a la empresa y a sus proveedores.

6.3. Criptografía en la red

En la Sección 2 se presentó la conveniencia de poseer algoritmia criptográfica en la mayor parte de las comunicaciones que se produzcan dentro de la red. En [30] se usaron curvas elípticas para el encriptado dentro de la red. Sin embargo, en [21] se mostró la conveniencia de implementación de la solución presentada en [15] dado que la misma es apta para procesadores de bajo poder de cómputo como es el caso de los PLCs.

6.4. Algunas consideraciones acerca de equipos y sistemas de proveedores

Se observó que gran parte de los ataques se basó en fallas de seguridad de las soluciones y/o equipos. Se pone énfasis en solo permitir en la red segura la instalación de equipos y dispositivos que garanticen cumplimiento de normas de seguridad y estabilidad a largo plazo.

7. Impacto de la solución sobre los casos de mayor gravedad

Se contemplan aquellos casos cuyo impacto fue Grave y que hayan producido pérdidas económicas: Dentro de este grupo está el 46% de todos los casos. En el 69% de estos casos, se perdió control del sistema. En el 77% hubo ataque explícito de hackers. De éstos, el 69% presentó virus, el 46% falla o vulnerabilidad en los sistemas, y/o falla humana y en total conforman el 100% del grupo de casos Graves.

La implementación de la topología propuesta evitaría accesos no deseados, mientras que la criptografía desde el nivel más bajo de la red la reforzaría.

8. Conclusiones

Las interconexión entre las redes corporativas y los ICS, ha dejado expuestas vulnerabilidades en los ICS.

La solución propuesta pone fuerte énfasis en la implementación en los ICS de soluciones de SI ya existentes para las redes corporativas complementándolas con algoritmia criptográfica y con ciertos requisitos de seguridad acerca de equipos y sistemas que se instalen en segmentos seguros de la red.

Así, la implementación de estas mejoras tendría un impacto muy positivo en la mitigación de efectos de ciber-ataques.

Referencias

[1] Jara, Hector y Federico Pacheco. *Ethical Hacking 2.0*. Usershop, 2012.

[2] Gustafson, S., and Sheth, A. *Web of Things*. Computing Now 7.3, 2014.

[3] Sánchez, Pablo. *Sistema de Gestión de la Ciberseguridad Industrial* [En línea]. Universidad de Oviedo, (2013). [Consulta: 11/02/15]. Disponible en: <http://dspace.sheol.uniovi.es / dspace / bitstream / 10651/17741 / 1 / TFM%20-%20PABLO%20SANCHEZ.pdf>.
[4] Opto 22, *Press Release: Updates groov to Easily Connect Modbus/TCP Devices with Smartphones and Tablets* [En línea], (2015). Disponible en: <http://www.modbus.org / member_docs / OPTO22-Jan2015.pdf> [Consulta: 14/08/2015].
[5] Carrasco Navarro, Oscar Navarro, y Villalón Puerta, Antonio. *Una visión global de la ciberseguridad de los sistemas de control*. Revista SIC: ciberseguridad, seguridad de la información y privacidad 106, (2013), pp. 52-55.
[6] Veramendi, Roland Rollano, *Ataques a la Seguridad Informática y Telecomunicaciones en el Contexto Internacional*. Revista del Instituto de Estudios Internacionales IDEI-Bolivia, 45(2), (2012), pp. 4-11.
[7] Vazquez, Santiago. *Ciberseguridad en Paraguay.* III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información, Buenos Aires, 2015.
[8] Corvalan, Fernando. *Seguridad de Infraestructuras Críticas: Visión desde la Ciberdefensa*. III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información, Buenos Aires, 2015.
[9] Blackmer, Marc. *Cibersecurity for Industrial Control Networks.* III Conferencia Internacional y Taller de Ciberseguridad e Infraestructuras Críticas de Información, Buenos Aires, 2015.
[10] Paulo Simoes, Tiago Cruz, Jorge Proença and Edmundo Monteiro. *Honeypots especializados para Redes de Control Industrial*. VII CIBSI. Panamá, 2013.
[11] Arias, Diego. *Seguridad en Redes Industriales*. Trabajo Final, Universidad de Buenos Aires, 2013.
[12] Paredes, I. *La protección de infraestructuras críticas y ciberseguridad industrial*. Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones 62, (2013), pp. 49.
[13] Security Incidents Organization, *RISI: The Repository of Industrial Incidents* [En línea], (2015). Disponible en: <http://www.risidata.com/Database> [Consulta: 14/08/2015].
[14] ISOTools, *ISO 27001* [En línea], (2015). Disponible en: <https://www.isotools.org / normas / riesgos-y-seguridad / iso-27001>. [Consulta: 14/08/2015].
[15] Hecht, Juan Pedro. *Un modelo compacto de criptografía asimétrica empleando anillos no conmutativos*. V CIBSI, Montevideo, 2009.
[16] López, Rubén; Arruvito; Bretaña; Petrillo; Rizzuto; Romero. *Autómatas programables. Norma IEC 1131. Material de Cátedra Sistemas de Hardware para la Administración.* Facultad de Tecnología Informática de la Universidad Abierta Interamericana, 2010.
[17] Colombo, Hugo. *Las redes en "tele-procesamiento" avanzado*. Facultad de Tecnología informática de la Universidad Abierta Interamericana (*mimeo*), 2015.
[18] Ferreira, F.. *Comunicaciones industriales* [En línea], (2007). Disponible en: <http://www.aadeca.org / pdf / apuntes_cursos / 2007_Comunicaciones_industriales / 1_parte.pdf> [Consulta: 01/08/2015].
[19] Aldea Rivas, M.; González Harbour, M. *MaRTE OS: Minimal real time operating system for embedded applications* [En línea], (2014). Disponible en: <http://marte.unican.es / documentation / readme / README_1.9_21Aug2014.txt> [Consulta: 14/08/2015].
[20] Cucu, L. *On the complexity of optimal priority assignment for periodic tasks upon identical processors*. 20th Euromicro Conference on Real-time Systems, Czech Republic (2008).
[21] Kamlofsky, Jorge; Hecht, Pedro; Colombo, Hugo; Veiga, Daniel; Abdel Masih, Samira. *Ciberdefensa de Infraestructuras Industriales*. 17o Workshop de Investigadores en Ciencias de la Computación. RedUNCI, Salta, 2015.
[22] IEEE 802.3 working group. *Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.* IEEE Std 802.3, 2000 Edition. Part 3. Nueva York, Estados Unidos de Norteamérica, 2000.
[23] Comer, Douglas E. *Redes globales de información con "internet" y "TCP/IP". Principios básicos, protocolos y arquitectura.* 3ra. Edición. Prentice Hall, Nueva York, Estados Unidos de Norteamérica, 1995. P 195-199.
[24] Modicon, Inc. *Modbus protocol reference guide* [En línea], (1996). Disponible en: <http://modbus.org / docs / PI_MBUS_300.pdf> [Consulta: 18/01/2015].
[25] Miller, Bill; Dale Rowe. *A survey SCADA of and critical infrastructure incidents.* Proceedings of the 1st Annual conference on Research in information technology, (2012).
[26] Channelbiz. *Anatomía de los ataques a los sistemas SCADA* [En línea], (2015). Disponible en: <http://www.channelbiz.es / 2015 / 06 / 17 / anatomia-de-los-ataques-a-sistemas-scada> [Consulta: 12/08/2015].
[27] Chen, Thomas. *Stuxnet, the real start of cyber warfare?* [Editor's Note].Network, IEEE 24.6 (2010): 2-3.
[28] Kubecka, Chris. *How to Implement IT Security after a Cyber Meltdown* Black Hat USA 2015, Las Vegas (2015).
[29] Geers, Kenneth, Kindlund, Darien; Moran, Ned and Rachwald, Rob. *WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*. [En línea] (2015). Disponible en: <https://www.fireeye.com / resources / pdfs / fireeye-wwc-report.pdf> [Consulta: 15/08/2015].
[30] Bertolín, Javier Areitio. *Mejora de la protección de la seguridad de los sistemas SCADA utilizados en el control de procesos industriales*. Revista española de electrónica 686 (2012): 60-70.