II CONVENCIÓN CIENTÍFICA INTERNACIONAL " CCI UCLV 2019 "

XVIII Simposio de Ingeniería Eléctrica SIE-2019

Estrategia de Defensa en profundidad para el DCS de ELQUIM
(Defense in Deep Strategy for ELQUIM's DCS)

Héctor Enrique Socarrás Cabrera, Julio Ruben Cañizares Abreu, Iván Santana Ching

[a]*Empresa de Automatización Integral CEDAI VC*

[b]*Universidad Central "Marta Abreu"de las Villas*

Resumen

Gran parte de la infraestructura de un estado, se mantiene operativa gracias a los sistemas de control industrial (SCI). Dado que un ataque informático al SCI de una infraestructura critica puede llegar a tener consecuencias adversas para la población y el medio ambiente, es de vital importancia proteger al SCI de este tipo de ataques.

El objetivo de este trabajo es presentar una estrategia de ciberseguridad que permita el intercambio de datos entre el SCI y la red empresarial de forma segura, así como la protección de SCI ante amenazas de ataques cibernéticos.

Como resultado de este trabajo se crea el plan de seguridad del Sistema de Control Industrial de la plana Coro-Sosa de acuerdo a las regulaciones nacionales e internacionales.

Palabras clave: Ciberseguridad, DCS, SCI.

1. Introducción

La planta de producción de Cloro-Sosa de la empresa ELQUIM, única de su tipo en Cuba, es responsable de suplir la demanda de Cloro líquido e hipoclorito de sodio para la potabilizar el agua suministrada a la población cubana.

La planta actual, con más de 35 años de explotación y tecnología de celdas electrolíticas de mercurio, se encuentra al final de su ciclo de vida y fue reemplazada por una moderna planta con tecnología de mem-

Email addresses: hsocarras@cedai.com.cu (Héctor Enrique Socarrás Cabrera), julioruben@cedai.com.cu (Julio Ruben Cañizares Abreu).

.

branas, más amigable con el medio ambiente, que cuenta con un sistema de control industrial compuesto por un sistema de control distribuido (DCS), un sistema de apagado de emergencia (ESD) y controladores lógicos programables (PLC) en unidades auxiliares.

Durante la concepción de la nueva planta no se tuvo en cuenta la ciberseguridad de la misma, identificandose la necesidad de tomar medidas que garantizan la explotación estable del Sistema de Control Industrial.

Han sido varios los incidentes de seguridad que han afectado los Sistemas de Control Industrial (SCI) a lo largo de la historia.

- Fuga de químicos en la empresa Union Carbide en Virginia (1985).
- Acceso a la planta de tratamiento de aguas de Maroochy en Australia (2000).
- Detección de Stuxnet en centrales nucleares (2010).
- BlackEnergy Ucrania (2015).

Siendo considerada Stuxnet como la primera ciberarma.

Para la protección del SCI de la planta Cloro-Sosa se siguieron las recomendaciones de las normativas internacionales como las del Instituto nacional de estándares y tecnologías (NIST) (Stouffer et al., 2015) y las regulaciones nacionales como la Resolución 254 del MINEM (MINEM, 2015) implementando una estrategia de defensa en profundidad con los siguientes elementos claves:

1. Evaluación de riesgos.
2. Protección Física.
3. Separación de redes.
4. Protección del Perímetro.
5. Endurecimiento de los dispositivos.
6. Manejo de Vendedores.
7. Factor Humano. Entrenamiento y Capacitación.

2. Sistema de Control industrial (SCI) de la planta Cloro-Sosa

El SCI consiste en un DCS para el control del proceso tecnológico, un Sistema de apagado de Emergencia o ESD para la seguridad funcional de la planta y autómatas programables en las unidades auxiliares del proceso.

2.1. DCS

El DCS de la planta esta implementado sobre la solución CENTUM VP de Yokogawa.(Corporation, 2015)

Este sistema está compuesto por:

- Estación de Interface Humana (HIS). Son PC con los paquetes de software de funciones de operación y monitoreo instalados.
- Estación de Ingeniería (ENG). Es un PC con los paquetes de software de Automation Design Suite instalados.
- Estación de Control de Campo (FCS). Son controladores con una alta fiabilidad, realizan funciones de control y de entrada/salida al proceso. Consisten en una Unidad de Control de Campo y varias unidades de nodos para el montaje de módulos de entrada/salida, haciéndola escalable en concordancia a las necesidades del proceso.
- Red de Control (Vnet/IP). En una red redundante a 1Gbps, conforme al estándar IEEE 802.3 Ethernet. Enlaza las FCS con las HIS. Incorpora tecnología propietaria de Yokogawa para lograr comunicaciones determinísticas, fiables y seguras.

2.2. ESD

El sistema de apagado de emergencia (ESD) se encarga de la seguridad funcional de la planta, la cual según el estudio HAZOP requiere funciones instrumentadas de seguridad SIL 1 y SIL 2.

El ESD fue implementado utilizado el sistema instrumentado de seguridad de Yokogawa ProSafe-RS el cual está certificado por TUV Rheinland, logra SIL 3 y se integra fácilmente con el DCS Centum VP.(Corporation, 2016)

Está compuesto por la Estación de Ingeniería de Seguridad (SENG) compartida estación de ingeniería del DCS y 2 Estaciones de control de seguridad (SCS).

3. Resultados y discusión

3.1. Evaluación de riesgos

El riesgo, es un valor que combina el impacto (Consecuencia) que produciría el deterioro o pérdida de un activo (o grupo de activos), junto con la probabilidad de que una vulnerabilidad existente en el activo sea explotada por una amenaza (de Ciberseguridad Industrial, 2016).

Primeramente se realiza un levantamiento detallado de los activos del Sistema de Control, considerándose como activos los siguientes elementos:

- Instrumentos y actuadores de campo.
- Controladores.
- Lógica en ejecución en los controladores.
- Equipos del proceso.
- Información del proceso.
- Elementos de redes y comunicación.

- Personal.

Evaluación de Consecuencias

Las consecuencias pueden dividirse en cuatro categorías principales (of Homeland Security, 2009).

- Seguridad y Salud: Efecto sobre la vida humana y bienestar. Ejemplo fatalidades, heridas, lesiones etc.
- Económicas: Perdidas económicas directas e indirectas. Ejemplo perdidas de producción, reconstrucción de algún activo.
- Psicológicas: Efectos en la moral pública y en la confianza en las instituciones estatales .
- Gobierno/Misión: Impactos en la habilidad del gobierno o la industria de mantener el orden, suministrar servicios públicos esenciales, garantizar la salud pública y realizar misiones relacionadas con la seguridad nacional.

Se evalúan de acuerdo a la siguiente tabla 1.

Cuadro 1
Tabla de evaluación de Impacto

Categoría	Impacto Bajo	Impacto Medio	Impacto Alto
Perdidas Financieras	Mas de 10000 USD	Mas de 100000 USD	Mas de 1000000 USD
Medio Ambiente	Daño pequeño y contenido	Daño pequeño sin contención	Impacto severo a largo plazo en el entorno
Interrupción de la producción	mas de 1 hora	mas de 1 Día	mas de 7 Días
Imagen Publica	N/A	Pérdida de confianza de los clientes	Daño a la Imagen de la Empresa
Impacto nacional	Pequeño impacto a un sector o servicios públicos	Impacto severo a un sector o servicios públicos	Impacto a múltiples sectores o interrupción grave de servicios público

Evaluación de Vulnerabilidades

Las vulnerabilidades son evaluadas para cada activo del SCI. Se tienen en cuenta factores físicos, como el grado de protección, si están expuesto a los elementos naturales, el acceso a la manipulación del activo o cuestiones desde el punto de vista de software.

se realiza una evaluación de la probabilidad de ocurrencia de acuerdo a la siguiente tabla 2 tomada de (de Ciberseguridad Industrial, 2016).

Escenarios de Riesgos

Todos los riesgos son evaluados respecto a un escenario especifico o grupo de escenarios. El escenario de riesgo debe responder a la pregunta: El riesgo de que?. Todas las consecuencias, vulnerabilidades y

Cuadro 2
Tabla de evaluación de Probabilidad de Ocurrencia

Nivel	Descripción
Alta	Es probable que la amenaza explote la vulnerabilidad durante el próximo año.
Media	Es probable que la amenaza explote la vulnerabilidad durante los próximos diez años.
Baja	Es poco probable que la amenaza explote la vulnerabilidad y no existen datos históricos de su ocurrencia.

amenazas estimadas son especificas al el escenario de riesgo. El riesgo puede ser evaluado a un activo, red, sistema o una combinación de estos (of Homeland Security, 2009).

Se crea una plantilla por cada escenario de riesgo que incluye el nombre del escenario, descripción, activos involucrados, probabilidad de ocurrencia de acuerdo a la tabla 2 aplicada a las vulnerabilidades identificadas en los activos involucrados en el escenario de riesgo, amenazas, evaluación del impacto de materializarse el escenario de acuerdo con la tabla 1, y por último una clasificación del riesgo de acuerdo a la tabla 3 (de Ciberseguridad Industrial, 2016).

Cuadro 3
Tabla de evaluación de Riesgo

Probabilidad	Categoría del Impacto			
		Alto	Medio	Bajo
	Alta	Riesgo Alto	Riesgo Alto	Riesgo Medio
	Media	Riesgo Alto	Riesgo Medio	Riesgo Bajo
	Baja	Riesgo Medio	Riesgo Bajo	Riesgo Bajo

Una ves identificados los escenarios de riesgos se comienzan a implementar contramedidas que mitiguen los mismos.

3.2. Protección Física.

Las medidas de protección físicas están encaminadas a prevenir impactos indeseados en el SCI tales como:

- Acceso no autorizado a locales sensibles.
- Modificación, manipulación, robo o destrucción de dispositivos, interfaces de comunicación etc.
- Observación no autorizada de documentación sensible, toma de fotografías, notas, etc.
- Introducción no autorizadas de nuevo hardware, como puntos de acceso inalámbricos, memorias USB, etc.

Primeramente se clasificaran los locales con equipamiento del SCI de acuerdo a la resolución 127/2007 del Ministerio de la Informática y las Comunicaciones (de la Informática y la Comunicaciones, 2007).

Areas Limitadas:

- Sus puertas y ventanas estarán provistas de cierres seguros.
- Las ventanas que se comuniquen con el exterior de la instalación, se le aplicarán medidas que garanticen su seguridad y que eviten la visibilidad hacia el interior del mismo;
- Se prohíbe el acceso de personal no autorizado por la dirección de la entidad.
- Se prohíbe la permanencia del personal fuera del horario laboral sin la debida justificación y autorización por escrito de la dirección de la entidad. Las autorizaciones referidas serán conservadas para su verificación en caso de necesidad.

Areas Restringidas: En las Áreas Restringidas, además de las medidas requeridas en las Áreas Limitadas, se aplicarán las siguientes:

- Tienen que permanecer cerradas, incluso cuando existan personas laborando en ellas, y el acceso a las mismas debe ser controlado mediante los documentos de registro que para ello se establezcan;
- Los medios informáticos no podrán estar conectados de manera física o lógica a medios que se encuentren fuera del alcance de estas áreas ni a redes públicas de transmisión de datos;
- Se aplicarán sistemas de detección y alarma que permitan una respuesta efectiva ante accesos no autorizados cuando no se encuentre el personal que labora en las mismas;
- Se prohíbe la introducción de soportes ópticos y magnéticos personales,excepto los que hayan sido autorizados de forma expresa por la dirección de la entidad.
- Se prohíbe la introducción de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a la misma.

Tambien es recomendado que la información relacionada con el DCS sea analizada y clasificada en el plan de seguridad del SCI ya que puede aumentar el riesgo de un ataque al SCI (API, 2009).

Información Confidencial

La información confidencial esta altamente protegida y solo debe accederse para realizar alguna tarea concreta por personal autorizado. En esta categoría están:

- Esquemas eléctricos de los paneles de la sala de Racks.
- Documento de detalle de la red de control.

Información Restringida

Puede ser accedida por un mayor grupo de personas, como tecnólogos, operadores etc, no obstante debe estar igualmente protegida y no de conocimiento general. En esta categoría están:

- Esquemas PID.
- Documento de descripción de Interlocks.
- Documento de descripción de Secuencias.
- Documento de valores umbrales.
- Documento de Sumario de lazos.
- Documento de cableado de señales del DCS.

- Documento de asignación de Cajas de conexiones.
- Documento de Especificación de Instrumentos.
- Documento de Esquemas eléctricos del CCM.
- Documentación asociada a las unidades paquetes.

Información Pública

La información pública es accesible a toda la empresa y no es necesaria para la realización de alguna tarea.

3.3. Separación de redes.

La separación de la red de control con la red administrativa se realiza a través de una zona desmilitarizada (DMZ) implementada con dos cortafuegos de acuerdo a la figura (1) tomada de (Stouffer et al., 2015)

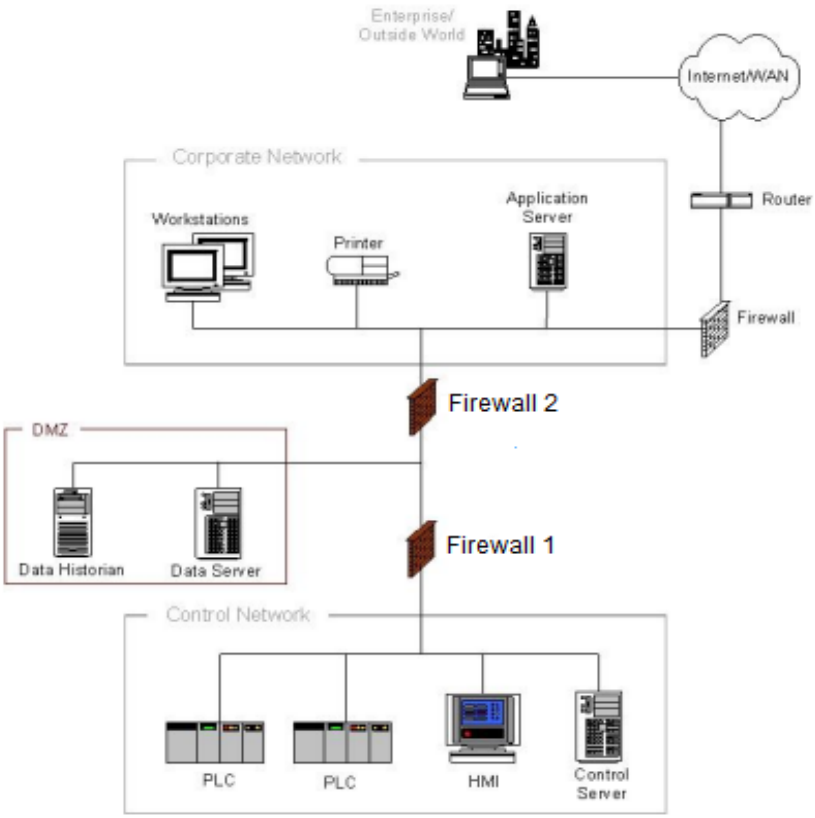

Figura 1. DMZ con dos Firewall.

Los dispositivos compartidos se ubican en la DMZ, en el caso de la planta de ElQuim estaria el servidor de datos históricos. El firewall 2 protege tanto la DMZ como la red de control, mientras que el firewall 1 protege la red de control de alguna estación comprometida de la DMZ además de prevenir trafico no deseado afecten el desempeño de los servidores de la DMZ.

Es recomendado el uso de firewall de diferentes fabricantes, adicionalmente permite al grupo de administración del SCI, como al grupo de IT tener claramente separadas sus responsabilidades. El grupo de administración del SCI seria responsable del firewall 1, mientras que el grupo IT del firewall 2.

3.4. Protección del Perímetro.

La protección del perímetro del SCI incluye la medidas de protección física y lógica para los activos informáticos como son el uso de cortafuegos y software de detección y prevención de intrusiones o (IDS).

La configuración de los cortafuegos de la DMZ se realizara de acuerdo a las políticas generales recomendadas en (CPNI, 2005).

- La regla básica deberá ser Denegar todo, permitir ninguno.
- Todas las reglas de permitir, deben configurarse por ip y puerto.
- Todo el trafico debe terminar en la DMZ.
- Todo protocolo diferente a IP deberá ser descartado.
- Todo protocolo permitido entre la red de control y la DMZ deberá estar denegado entre la DMZ y la red corporativa y viceversa.
- La dispositivos de la red de control no deberán tener acceso a internet.
- El trafico de administración de los firewalls deberá realizarse sobre una conexión encriptada. El trafico también deberá ser restringido por direcciones IP de estaciones especificas de administración.

Para el cortafuego 1 se debe utilizar un cortafuego físico configurado de manera tal que solo permita el trafico OPC entre la red de control y el servidor de datos históricos, y el protocolo FTP desde la red de control a un servidor en la DMZ para la transferencia de salvas y backups de proyecto.

En el caso del cortafuego 2 se especifica el uso de una distribución de linux para su uso como cortafuegos como es el caso de IPFire en un PC con dos interfaces de red. Este cortafuegos solo deberá permitir el paso del protocolo de consultas que utilise el motor de base de datos utilizada en el servidor de históricos y la aplicacion de reportes instalada en la red corporativa para acceder a los datos del mismo.

Sistemas de detección y prevención de Inrusiones

Como parte de la estrategia de Defensa en profundidad, se debe detectar y alertar a la organización de una intrusión tempranamente para que la misma pueda tomar acciones defensivas antes de que un activo critico sea vulnerado (ICS-CERT, 2016).

Un IDS o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.

Los SCI proveen una oportunidad única cuando se considera utilizar un IDS/IPS en la red, ya que a pesar del tráfico considerable, este tráfico es muy predecible (ICS-CERT, 2016).

Se utiliza Snort como software IDS en la estación del cortafuegos 2 ya que esta disponible en la distribución de IPFire de linux utilizada en el mismo.

3.5. Endurecimiento de los dispositivos.

El endurecimiento de las medidas de seguridad para cada activo constituye una capa mas en la estrategia de defensa en profundidad conocida como ”device hardening”.

En las estaciones de trabajo por ejemplo deberán tomarse las siguientes medidas:

- Instalar y configurar un firewall personal.
- Contraseñas personales e intransferible con un mínimo de 8 o mas caracteres, utilizando caracteres alfanuméricos y signos especiales.
- Configurar los registros de eventos.
- Lista Blanca.
- Desinstalar cuentas de usuarios y servicios que no se utilizan, como email, multimedia, juegos.
- Reemplazar servicios inseguros como telnet por alternativas seguras como SSH.
- Inhabilitar puertos USB y torres de discos flexibles si existieran.

3.5.1. Estación de Ingenieria

En el caso de la estación de ingeniería se toman las siguientes medidas adicionales:

Servidor OPC

La estación de Ingeniería tendrá solo dos cuentas habilitadas, el usuario Ingeniero perteneciente al grupo de administradores y el usuario OPC_logger perteneciente al grupo OPC que tiene privilegios limitados.

El DCOM de la estacion de ingenieria se endurece tomando las siguientes medidas:

Primeramente, es necesario dar solo los permisos necesarios para los usuarios por cada objeto DCOM. Por ejemplo, si en una misma estación hay varios servidores opc, pero solo uno necesita ser accedido remotamente, permitir entonces acceso únicamente a ese servidor, si todos los servidores y clientes opc se encuentran en la misma estación entones se inhabilita el acceso remoto en el DCOM (Byres and Peterson, 2007).

En segundo lugar, es necesario el uso de diferentes cuentas de usuarios con diferentes privilegios. Solamente el usuario Ingeniero sera el único capaz de arrancar y configurar las aplicaciones opc. La cuenta de OPC_logger puede ser usada por usuarios que solamente necesitan conectarse y acceder a servidores opc.

Para cumplir estos objetivos se utiliza la herramienta IT Security Tools del propio Centum VP, evitando que se tenga que realizar de manera manual.

Software Antivirus

La instalación de software antivirus en los SCI deben seguir las reglas generales especificadas en (MINEM, 2015).

- Instalar en el sistema de control solo la protección contra programas malignos previamente aprobada por el fabricante del SCI
- Se instalara en la estación de ingeniería el programa de protección y desde ella se realizaran los diagnósticos a las estaciones de operación.
- Los diagnósticos a las estaciones de operación solo se realizaran con la misma fuera de servicio.
- Solo se podrá tener en servicio algún programa de protección en las estaciones de operación cuando el fabricante del SCI garantice por escrito que no afecta el funcionamiento de la estación.
- Las actualizaciones de los programas de protección se realizaran durante los mantenimientos programados al SCI.
- Se prohíbe realizar actualizaciones desde la red administrativa en ninguna circunstancia.

Es software antivirus para productos Yokogawa esta basado en Intel Security (McAffe)el cual debe ser adquirido como parte del Servicio de Seguridad a Usuario Final (Endpoint Security Service) de Yokogawa.

Software de Lista Blanca

Lista blanca(Whitelisting): es un mecanismo para examinar objetos para permitirlos o rechazarlos. En este método, se crea una lista (lista blanca) que enumera las aplicaciones que deben permitirse, y las aplicaciones que no están en la lista se rechazan.

Basado en la tecnología de Intel Security (McAfee) Aplication Control, es el software de lista blanca para sistemas de control Yokogawa IA.

3.5.2. Switch Capa 3 de la red Vnet/IP

Es prácticamente imposible configurar una red de manera segura sin el soporte de los fabricantes de dispositivos de red. (Hirschmann, 2015). Los switch utilizado por la red de control Vnet/Ip para comunicar las estaciones de operación y los controladores de campo, son del fabricante Hirschmann modelo MACH104-20TX-F, en los mismo se aplicaran las recomendaciones del fabricante para switches industriales de SCI, algunas de ellas son:

- Desactivar los protocolos DHCP, BOOTP, Profinet, Ethernet/IP, LLDP y el uso del adaptador de autoconfiguración.
- Desactivar telnet, ssh y la configuración por linea serial.

Funcionalmente en todos los switches se aplicaran las medidas de protección por contraseña, y se inhabilitarán los puertos que no estén en uso.

3.6. Manejo de Vendedores

Los vendedores presentan un caso especial de la estrategia de Defensa en Profundidad. En los últimos años los vendedores han tomado conciencia de la importancia de la ciberseguridad en las soluciones de control industrial y en muchos casos han incorporado seguridad en el ciclo de vida de sus productos.

3.6.1. Cadena de suministro

La cadena de suministro representa un riesgo significativo en los SCI; incluye inserción de falsificaciones o equipamiento no genuino, sabotajes, inserción de software malicioso etc. Es necesario establecer un programa de manejo de vendedores incluyendo por ejemplo reglas para solamente comprar directamente de fabricantes o sus distribuidores oficiales (Boyens et al., 2015).

3.6.2. Servicios Subcontratados

Es común que las organizaciones subcontraten servicios altamente especializados que utilizan poco frecuente o de los que carenen personal calificado. Cuando se contrate a terceros para la realización de servicios, ambas partes deberán establecer y acordar reglas de contratación.Se proponen las siguientes reglas generales:

- Se deberán especificar cuales actividades se van a realizar, en que sistema y quien va ser el encargado de realizarla.
- Solo se utilizaran los programadores de campo suministrado por ELQUIM. Bajo ningún concepto se utilizaran los dispositivos de terceros para conectarse con ningún activo de la red de control.
- Los trabajadores de terceros estarán siempre acompañado de un miembro del equipo de automática de la planta, quien documentará cada acción de los mismo en una orden de trabajo.

3.7. Recursos Humanos

El manejo de recursos humanos dentro de los SCI presenta desafíos para la organización. Los SCI grandes y complejos son susceptibles a errores hecho por personal inexperto y falta de entrenamiento, así como de actividades de personal malicioso dentro del SCI.

Se deben diseñar procedimientos para establecer como el personal debe conducirse en un proceso particular o configurar un sistema, dichos procedimientos deberán servir para rápidamente entrenar al personal nuevo asegurándose que ellos siguen todas las rotulaciones y estándares de operación del SCI.

Se recomienda entrenar los administradores del SCI en la instalación desde cero del sistema valiéndose de maquinas virtuales y ejercitandolo con una periodicidad de al menos una vez al año. Así mismo se recomienda adquirir una estación de control de campo del DCS, con al menos un modulo de comunicaciones Profibus y 1 modulo de E/S de cada tipo que sirva como plataforma de entrenamiento a los

administradores del sistema.

4. Resultados

Como resultado final de esta investigación, se dispone de un expediente de seguridad para el Sistema de Control industrial que tiene en cuenta la resolucion 254 del Ministerio de Energía y Minas, las normativas internacionales y la mejores prácticas en los temas de ciberseguridad, así como las condiciones reales de la industria cubana.

El expediente de seguridad está compuesto por los siguientes documentos principales:

1. DESSCI-00-Control de documentos.
2. DESSCI-01-Datos generales.
3. DESSCI-02-Roles y atribuciones.
4. DESSCI-03-Procedimientos de la seguridad del SCI.
5. DESSCI-04-Arquitectura de la red de control.
6. DESSCI-05-Análisis de riesgo.
7. DESSCI-06-Gestión de la configuración.
8. DESSCI-07-Controles técnicos.
9. DESSCI-08-Controles físicos y medio ambientales.
10. DESSCI-09-Plan de contingencia.
11. DESSCI-10-Sistema de autoevaluación.
12. DESSCI-11-Gestión de incidentes.
13. DESSCI-12-Adquisición de servicios.
14. DESSCI-13-Capacitación.
15. DESSCI-14-Plan de acción.

5. Conclusiones

El tema de la ciberseguridad en Cuba es algo novedoso en las plantas del ministerio de industria, no así en el ministerio de Energía y Minas, donde se cuenta con medidas de ciberseguridad como la DMZ implementadas, como es el caso de la termoeléctrica de Felton visitada durante la realización de este trabajo.

No obstante es la primera realización de un plan de seguridad para el SCI de una planta que sigue las directrices de la Comisión Nacional de Automática.

La metodología empleada para la evaluación de riesgo, difiere de las utilizadas en los planes de seguridad informática de las empresas y es el principal aporte de este trabajo.

6. Referencias bibliográficas

Referencias

API, 2009. Pipeline SCADA Security API Standard 1164.

Boyens, J., Paulsen, C., Moorthy, R., Bartol, N., 2015. NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations.
URL http://dx.doi.org/10.6028/NIST.SP.800-161

Byres, E., Peterson, D., 2007. OPC Security Whitepaper #3 Hardening Guidelines for OPC Hosts.

Corporation, Y. E., 2015. Integrated Production Control System CENTUM VP System Overview (General Overview).

Corporation, Y. E., 2016. Safety Instrumented System ProSafe-RS System Overview.

CPNI, 2005. FIREWALL DEPLOYMENT FOR SCADA AND PROCESS CONTROL NETWORKS GOOD PRACTICE GUIDE.

de Ciberseguridad Industrial, C., 2016. GUIA PARA LA CONSTRUCCION DE UN SGCI. SISTEMA DE GESTION DE LA CIBERSEGURIDAD INDUSTRIAL, primera edición Edition.

de la Informática y la Comunicaciones, M., Aug. 2007. Resolución No 127/2007. Gaceta Oficial de la Republica de Cuba No 057, 899 – 910.

Hirschmann, 2015. ICS Security Guide to Hirschmann Switches.

ICS-CERT, 2016. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.

MINEM, 2015. Reglamento de Seguridad de los Sistemas de Industriales para el Ministerio de Energia y Minas.

of Homeland Security, D., 2009. National Infrastructure Protection Plan.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A., May 2015. NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security.
URL http://dx.doi.org/10.6028/NIST.SP.800-82r2