risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 28/02/2019
Aceitação/Acceptance: 10/04/2019

# Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM.

Héctor Enrique Socarrás[1], Ivan Santana[2]

**hector@cedai.com.cu, ching@uclv.edu.cu**

[1] Empresa de Automatización Integral CEDAI, División Villa Clara, Calle 4ta no 7, C.P. 50100, Santa Clara, Villa Clara, Cuba.

[2] Universidad Central "Marta Abreu" de las Villas, Facultad de Ingeniería Eléctrica, Departamento de Automática, Carretera a Camajuaní Km. 5 y 1/2, C.P. 50100, Santa Clara, Villa Clara, Cuba.

**DOI: 10.17013/risti.32.83–96**

**Resumen:** Después de Stuxnet la protección de los Sistemas de Control Industrial, en especial aquellos que controlan procesos de infraestructuras críticas, ha tomado vital importancia para los gobiernos. Ya solo no basta la protección física de estas instalaciones, sino una amenaza como los ciberataques deben ser tenidas en cuenta. Es en este escenario que la implementación de medidas de ciberseguridad para el sistema de control industrial (SCI) de la nueva planta de Cloro-Sosa de la empresa ELQUIM es un requerimiento de las autoridades nacionales. En este artículo se presenta la implementación de una estrategia de defensa en profundidad para la protección de este SCI siguiendo las reglas internacionales y nacionales lo cual es definitorio para el arranque de la nueva planta.

**Palabras-clave**: Ciberseguridad; Infraestructura Crítica; Sistemas de Control Industrial.

***Cyber Security for the Industrial Control System of the ELQUIM's Chlorine Plant.***

***Abstract:*** After Stuxnet, the protection of Industrial Control Systems, especially those that control critical infrastructure processes, has taken vital importance for governments. The physical protection of these facilities alone is not enough, but a threat such as cyber-attacks must be taken into account. It is in this scenario that the implementation of cybersecurity measures for the industrial control system (ICS) of the new ELQUIM company's chlorine plant is a requirement of the national authorities. In this article we present the implementation of a defense in depth strategy for the protection of this ICS.

***Keywords****:* Cyber Security; Critical Infrastructure; Industrial Control Systems.

## 1. Introducción

Las Infraestructuras Críticas son aquellas instalaciones y sistemas sobre los que recaen servicios esenciales cuyo funcionamiento no permite soluciones alternativas, por lo que

su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales prestados a la sociedad. (CCN-CERT, 2016). 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.

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 membranas, más amigable con el medio ambiente. La nueva planta 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.

Muchos de los Sistemas de Control Industrial de hoy evolucionaron desde la inserción de las capacidades de tecnologías de la información en los sistemas físicos existentes, a menudo reemplazando o complementando los mecanismos de control físico. Las mejoras en el costo y el rendimiento han fomentado esta evolución, dando como resultado muchas de las tecnologías "inteligentes" de hoy en día, como la red eléctrica inteligente, el transporte inteligente, los edificios inteligentes y la fabricación inteligente. Si bien esto aumenta la conectividad y la criticidad de estos sistemas, también crea una mayor necesidad de adaptabilidad, resiliencia y seguridad (Stouffer et al, 2015).

Para utilizar los recursos y los activos del SCI de manera eficiente, este debe estar bajo el control de una administración de seguridad y gobernanza adecuada. La gobernanza se refiere al conjunto de controles de seguridad que se utilizan para gobernar una organización (Alcaraz, C. et al, 2015).

Para fortalecer la seguridad de los SCI, una solución es implementar una defensa en profundidad mediante la combinación de controles de seguridad para reducir el riesgo para los activos que se están protegiendo. Al aplicar múltiples controles sobre el SCI se introducen otras barreras, que un atacante debe superar (Maglaras, L. A. et al, 2018).

Este trabajo tuvo como objetivo la implementación de una estrategia de defensa en profundidad para la protección del SCI de la planta de producción de Cloro-Sosa de la empresa ELQUIM. En la sección 2 se describe el SCI de la planta, la sección 3 presenta los aspectos fundamentales de la estrategia de defensa en profundidad y describe la implementación de la misma, finalmente se presentan las conclusiones.

## 2. Descripción del Sistema de Control Industrial

### 2.1. DCS

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

Este sistema está compuesto en la planta, por 3 estaciones de control de campo o (FCS), las cuales son controladores con una alta fiabilidad, realizan funciones de control y de entrada/salida al proceso, formadas por una Unidad de Control de Campo y varias

unidades de nodos para el montaje de módulos de entrada/salida; 2 estaciones de interface humana (HIS) que son PC con los paquetes de software de funciones de operación y monitoreo instalados a través de las cuales los operadores interactúan con el proceso; una estación de Ingeniería, que es un PC con los paquetes de software necesarios para la configuración, programación y administración del sistema; todo esto interconectado a través de una red de control Vnet/IP, que es una red ethernet redundante a 1Gbps.

Adicionalmente la red ethernet estándar de las estaciones HIS es utilizada para la comunicación con las impresoras de alarmas y la comunicación con la red de gestión empresarial a través de un servidor de datos OPC DA y AE.

### 2.2. Sistema de Apagado de Emergencia. (ESD)

La protección contra eventos peligrosos como explosiones, escapes de productos tóxicos etc., se realiza a través de un esquema de protección por capas Figura 1, en la cual los ESD se encuentran en la capa de prevención y mitigación de eventos peligrosos.

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

Está compuesto por la estación de ingeniería de seguridad (SENG) compartida con la estación de ingeniería del DCS y 2 estaciones de control de seguridad (SCS).

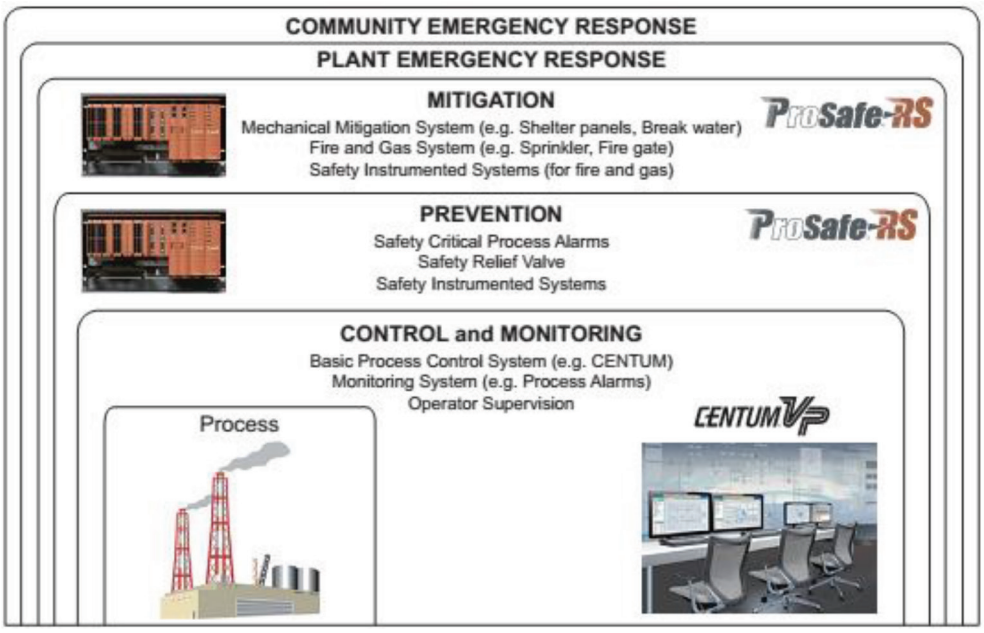


Figura 1 – Seguridad funcional. Protección por capas (Yokogawa Electric Corporation, 2016).

## 3. Estrategia de Ciberseguridad

Para la protección del SCI de la planta Cloro-Sosa se determina seguir las recomendaciones del Instituto nacional de estándares y tecnólogas (NIST) (Stouffer et al.,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. Monitoreo y Actualizaciones.
7. Manejo de Vendedores.
8. Factor Humano. Entrenamiento y Capacitación.

### 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 (Centro de Ciberseguridad Industrial, 2016).

#### *Activos*

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

- Instrumentos y actuadores de campo. Transmisores de presión, flujo, etc., así como válvulas de control y variadores de frecuencia.
- Controladores. PLC, RTU o dispositivos electrónicos inteligentes.
- Interfaces Hombre-Máquina. Paneles de operación y consolas de operación.
- Lógica en ejecución en los controladores. Programas de usuario de los PLC.
- Equipos del proceso.
- Información del proceso. Planos eléctricos, diagramas de instrumentación y tuberías, etc.
- Elementos de redes y comunicación.
- Personal.

#### *Evaluación de Vulnerabilidades*

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

Las vulnerabilidades se pueden agrupar en las siguientes categorías (Stouffer et al, 2015):

- Políticas y Procedimientos
- Arquitectura y Diseño.
- Configuración y Mantenimiento.
- Físicas.

- Software
- Redes y Comunicaciones.

Las vulnerabilidades específicas de diferentes fabricantes se pueden encontrar en sus sitios oficiales o en sitios de los diferentes CERT de seguridad industrial.

Yokogawa:

https://www.yokogawa.com/library/resources/white-papers/yokogawa-security-advisory-report-list/

ICS-CERT Estados Unidos: https://ics-cert.us-cert.gov/advisories

La evaluación de la probabilidad de que la vulnerabilidad sea explotada se calcula de acuerdo a la Tabla 1 (Centro de Ciberseguridad Industrial, 2016).

| Nivel | Descripcion |
|---|---|
| *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. |

Tabla 1 – Evaluación de probabilidad de ocurrencia

### *Evaluación de Consecuencias*

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

- Seguridad y Salud: Efecto sobre la vida humana y bienestar. Ejemplo fatalidades, heridas, lesiones etc.
- Económicas: Pérdidas económicas directas e indirectas. Ejemplo pérdidas 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.

### *Escenarios de Riesgo*

Todos los riesgos son evaluados respecto a un escenario específico o grupo de escenarios. El escenario de riesgo debe responder a la pregunta: ¿El riesgo de qué? Todas las consecuencias, vulnerabilidades y amenazas estimadas son específicas al escenario de riesgo. El riesgo puede ser evaluado a un activo, red, sistema o una combinación de estos (U.S. Department of Homeland Security, 2009b).

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

| Categoria | Impacto Bajo | Impacto Medio | Impacto Alto |
|---|---|---|---|
| *Pérdidas Financieras* | Más de 10000 USD | Más de 100000 USD | Más 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* | más de 1 hora | más de 1 día | más de 7 días |
| *Imagen Pública* | 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 |

Tabla 2 – Evaluación de Impacto o Consecuencia

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 (Centro de Ciberseguridad Industrial, 2016).

| | Categoria del Impacto | | |
|---|---|---|---|
| **Probabilidad** | **Alta** | **Media** | **Baja** |
| Alta | Riesgo Alto | Riesgo Alto | Riesgo Medio |
| Media | Riesgo Alto | Riesgo Medio | Riesgo Bajo |
| Baja | Riesgo Medio | Riesgo Bajo | Riesgo Bajo |

Tabla 3 – Evaluación del Escenario de Riesgo

Una vez identificados los escenarios de riesgos se procede a priorizar los esfuerzos de gestión de riesgos con respecto a los activos más significativos, para enfocar la planificación, aumentar la coordinación, la asignación efectiva de recursos y mejorar la gestión de incidentes, respuesta y restauración (U.S. Department of Homeland Security, 2009b).

Se definieron los siguientes órdenes de prioridades:

1. Seguridad funcional de la planta.
2. Continuidad del Proceso Productivo.
3. Servicios Auxiliares.

### *Equipo de respuesta a incidentes de seguridad (CSIRT)*

Las acciones para mitigar el riesgo involucran medidas diseñadas a prevenir, determinar y mitigar las amenazas, reducir las vulnerabilidades, minimizar las consecuencias y habilitar una respuesta eficiente y restauración posterior a la ocurrencia de un incidente.

La capacidad de respuesta a incidentes debe incluir varios elementos proactivos como la prevención (U.S. Department of Homeland Security, 2009) y otros centrados en la gestión de los mismos, (contención, corrección, restauración y recuperación)

El primer paso es crear un equipo interno de respuesta a incidentes de seguridad, siguiendo las recomendaciones de (U.S. Department of Homeland Security, 2009) y los resultados de los análisis de (Muñoz et al, 2015).

El CSIRT de la planta tendrá el propósito de responder a la ocurrencia de un incidente, identificar impactos operacionales para la planta, reportar la ocurrencia de un incidente a los organismos de control, recopilar información forense para asistir análisis y acciones legales, restaurar el SCI después del incidente y crear y mantener un plan de respuesta incidentes.

El equipo debe estar compuesto por:

- Ingeniero en control de procesos: Es el experto en la arquitectura de control. Es capaz de determinar el impacto potencial de sacar un componente del SCI fuera de servicio.
- Administrador de red del SCI: Es una persona clave si el incidente involucra un ataque cibernético.
- Administrador del DCS: Es la persona que conoce los permisos de acceso al SCI de los diferentes usuarios, se encarga de servir de interface con los vendedores del DCS.
- Jefe de Seguridad y Protección de la empresa.
- Jefe de planta: Está facultado en la toma de decisiones involucradas en la interrupción de la producción de ser necesario como respuesta a un incidente.
- Especialista Legal: Es opcional, la asesoría legal en necesaria en varias áreas asegurando el cumplimiento con leyes y regulaciones nacionales.
- Especialista en Recursos Humanos: Tiene un papel en este equipo cuando un incidente involucra a un trabajador de la planta, y es el encargado de las medidas disciplinarias a aplicar.

### 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 u otros activos.
- Observación no autorizada de documentación sensible, toma de fotografías, notas, etc.
- Introducción no autorizadas de nuevo hardware, como puntos de acceso inalámbricos y memorias USB.

Primeramente, se clasifican los locales con equipamiento del SCI en Áreas Limitadas, Restringidas o Estratégicas de acuerdo a la resolución 127/2007 del Ministerio de la Informática y las Comunicaciones y se implementan las medidas indicadas en esta resolución.

Áreas Limitadas:

- Sala de Control.
- Cuarto de Armarios del Rectificador.

- Cuarto de Racks de la planta de tratamiento de Agua.
- Subestación eléctrica media tensión.
- Subestación eléctrica baja tensión.

Áreas Restringidas:

- Sala de gabinetes del DCS/ESD.
- Armario del controlador de seguridad SCS0105 en la sala de celdas.
- Oficina de Estación de Ingeniería.

### 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 2.

Los dispositivos compartidos se ubican en la DMZ, en el caso de la planta de ELQUIM están el servidor de datos históricos y un servidor ftp para la realización de salvas de respaldo. El cortafuegos 2 protege tanto la DMZ como la red de control, mientras que el cortafuegos 1 protege la red de control de alguna estación comprometida de la DMZ.

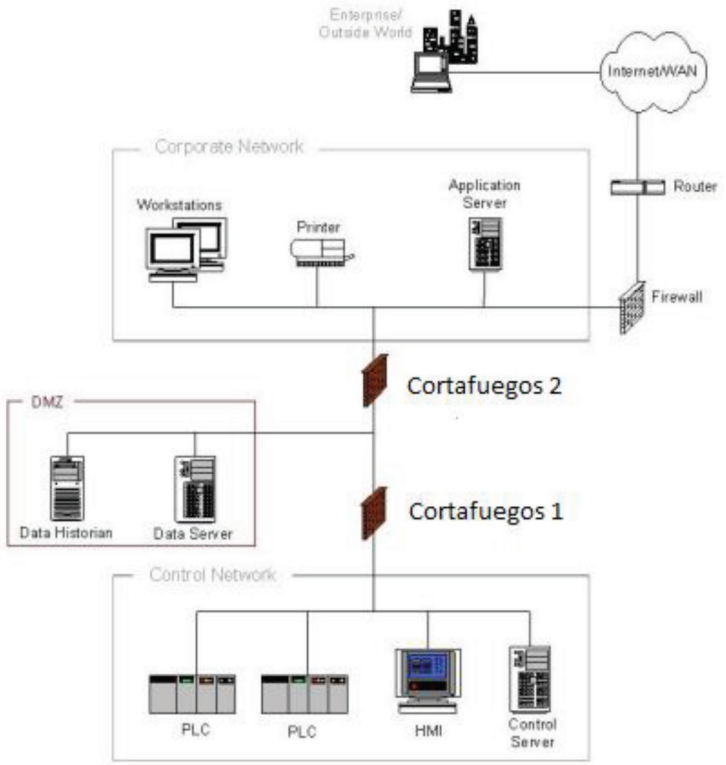


Figura 2 – Arquitectura de la DMZ entre la red de control y la red corporativa del ELQUIM

Esta configuración hace uso de cortafuegos de diferentes fabricantes, el cortafuegos 1 fue desarrollado por la empresa XETID y es administrado exclusivamente por esta, se instaló en el local de Racks del SCI.

El cortafuegos 2 fue implementado con un "dual-homed" PC y la distribución de Linux IPFire, fue configurado igualmente por la empresa XETID, pero su administración es asumida por el grupo de informática de la empresa ELQUIM.

## 3.4. Protección del Perímetro

La protección del perímetro del SCI incluye tanto la protección física, como la protección lógica para la protección de los activos. La protección lógica, incluye controles como mecanismos de autenticación, sistemas de detección y prevención de intrusos, listas de control de acceso y otros medios para proteger el sistema desde un punto de vista cibernético (ICS-CERT, 2016).

### *Reglas Generales para los cortafuegos*

Un cortafuegos es solo tan efectivo, como la precisión de las reglas con las que está configurado (ICS-CERT, 2016). Las reglas de los cortafuegos 1 y 2 deben cumplir con las siguientes políticas generales.

- El tráfico de administración de los cortafuegos deberá realizarse sobre una conexión encriptada. El tráfico también deberá ser restringido por direcciones IP de estaciones específicas de administración. Cualquier otro tráfico dirigido al cortafuegos será bloqueado sin notificación. (Evita que el cortafuegos sea visible al escáner atacante).
- Bloquear cualquier tráfico de salida originado en el cortafuegos. (El cortafuegos no debe establecer ninguna conexión directa)
- Todo tráfico debe terminar en la DMZ.
- Todas las reglas de permitir, deben configurarse por dirección IP y puerto.
- Todo tráfico debe estar basado en protocolos enrutables TCP/IP o UDP/IP.
- Todo protocolo no 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.
- Los dispositivos de la red de control no deberán tener acceso a internet.
- La última regla es la regla por defecto y es siempre bloquear/denegar sin notificación cualquier tráfico que no esté explícitamente permitido por las reglas precedentes.

### *Cortafuegos 1.*

El cortafuegos 1 además de cumplir con las políticas generales fue configurado teniendo en cuenta las siguientes reglas específicas:

Debe permitir la conexión del servidor de datos históricos en la DMZ hacia la estación de ingeniería, solamente a los puertos destinados para los servicios del DCOM especificados en la guía de seguridad de CENTUM VP, necesarios para la comunicación OPC.

El tráfico FTP estará restringido por el cortafuegos, solamente deberá permitir conexiones a los puertos configurados en el servidor FTP para el modo pasivo.

Los registros de este cortafuegos pueden ser auditados desde la estación de ingeniería por parte del equipo de administradores del SCI

### *Cortafuegos 2*

Este cortafuegos solo permite el tráfico desde el servidor de datos de la red de gestión con destino al servidor de datos históricos que utiliza PostgreSQL.

Adicionalmente permite la administración remota desde la estación del especialista de seguridad informática de la empresa.

### *Sistema de detección y prevención de intrusos*

Un IDS (Instrusion Detection System), es una herramienta de seguridad que actúa como un monitor del tráfico de red, describiendo y analizando ahora el contenido de los paquetes que ingresan a la organización. Sus principales funcionalidades son las siguientes (Miranda et al, 2016):

- Detectar ataques y otras violaciones de seguridad.
- Implementar calidad de control para eventos de seguridad y administración.
- Proporciona información acerca de los intrusos que intentan acceder a la red o sistemas.
- Previene problemas de comportamiento de abusos en el sistema o red.

Los IDS aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. 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 el IDS Snort que trae consigo la distribución de IPFire instalada en la estación del cortafuegos 2 para monitorear todo el tráfico dirigido a la DMZ desde la red de gestión.

## 3.5. Endurecimiento de los dispositivos

El endurecimiento de las medidas de seguridad para cada activo constituye una capa más 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 cortafuegos personal.
- Contraseñas personales e intransferibles con un mínimo de 8 o más caracteres, utilizando caracteres alfanuméricos y signos especiales.
- Configurar los registros de eventos.
- Software Antivirus
- Software de Lista Blanca.
- Deshabilitar 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.

### *Endurecimiento de OPC*

La comunicación con la red de gestión empresarial por parte del SCI se realiza a través de un servidor de datos OPC DA instalado en la estación de ingeniería.

A lo largo de su historia las implementaciones de llamadas de procedimientos remotos (Remote Procedure Call o RPC) han tenido pobres antecedentes relacionados con la seguridad. Dado que OPC está basado en la tecnología de DCOM de Microsoft y esta a su vez está basada en RPC, las estaciones con OPC son vulnerables a todas las banderas de pre-autenticación de RPC como las explotadas por el gusano Blaster en 2003. (Byres and Peterson, 2007a).

OPC DA le permite a un atacante no solo ganar acceso a datos de control del proceso, sino también modificar parámetros de ajustes en los controladores, valores de alarmas u otros parámetros de control.

Solo un parche agresivo de las estaciones OPC o el bloqueo de todo el tráfico OPC en el cortafuegos pueden mitigar el riesgo de estas vulnerabilidades (Byres and Peterson, 2007b).

Para manejar los riesgos asociados a OPC es necesaria una configuración cuidadosa de las cuentas de usuarios y poner restricciones en la configuración del DCOM. Primeramente, es necesario dar solo los permisos imprescindibles 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, 2007b).

En segundo lugar, es necesario el uso de diferentes cuentas de usuarios con diferentes privilegios. Solamente el usuario Ingeniero con privilegios de administración en la estación, será el único capaz de arrancar y configurar las aplicaciones OPC. La cuenta de Process_logger puede ser usada por usuarios que solamente necesitan conectarse y acceder a servidores OPC.

La configuración del DCOM, así como del cortafuegos personal de las estaciones de ingeniería y de operación se realiza a través de la herramienta IT Security Tools del propio Centum VP, evitando que se tenga que realizar de manera manual.

Adicionalmente a las medidas de fortalecimiento del DCOM, se configura en el DCS el usuario correspondiente a la conexión OPC, en función de los privilegios de este usuario es posible comandar la planta a través de OPC, o incluso pasar a manual lógicas de enclavamientos para que no se ejecuten.

Se configura por tanto el usuario OPC con el mismo nivel de seguridad que el usuario OFFUSER que es el usuario por defecto y tiene privilegios mínimos.

## 3.6. Actualizaciones

Aplicar los parches a un componente de SCI es un desafío para los administradores, debido a que los parches y actualizaciones pueden interferir con el funcionamiento del SCI (ICS-CERT, 2016).

La aplicación de parches solo deberá realizarse durante las paradas de plantas. No se realizará ninguna actualización del sistema operativo, solo se realizarán actualizaciones indicadas por el vendedor del SCI, de ser posible deberán probarse en una estación de prueba.

## 3.7. 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.

### *Cadena de suministro*

La cadena de suministro representa un riesgo significativo en los SCI; incluye inserción de falsificaciones o equipamiento no genuino, sabotajes e inserción de software malicioso (Boyens et al., 2015).

Se establece un programa de manejo de vendedores incluyendo por ejemplo reglas para solamente comprar directamente de fabricantes o sus distribuidores oficiales en Cuba.

### *Servicios Subcontratados*

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

Las tareas de mantenimiento preventivo y correctivo por terceros al SCI siguen las siguientes reglas:

- Se deberán especificar cuáles actividades se van a realizar, en que sistema y quien va ser el encargado de realizarla.
- Solo se utilizarán los programadores de campo suministrado por ELQUIM. Bajo ningún concepto se utilizarán los dispositivos de terceros para conectarse con ningún activo de la red de control.

## 3.8. Factor Humano. Entrenamiento y Capacitación.

El manejo de recursos humanos dentro de los SCI presenta desafíos para la organización. Los SCI grandes y complejos son susceptibles a errores cometidos 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 regulaciones y estándares de operación del SCI. Los administradores del SCI se entrenarán en la instalación desde cero del sistema valiéndose de máquinas virtuales y ejercitándolo con una periodicidad de al menos una vez al año.

## 4. Conclusiones

El número de potenciales problemas de seguridad y sus riesgos asociados, aumenta con el crecimiento de la complejidad y la conectividad de los SCI con redes externas. La seguridad de los mismos debe ser tenida en cuenta durante la etapa de proyecto y deben ser utilizadas las soluciones tanto de hardware como de software del vendedor del SCI.

La estrategia implementada para la defensa en profundidad es de diseño inédito en el sector industrial cubano por lo que puede servir como guía para otras soluciones con sistemas similares.

En la estrategia se empleó hardware estándar de tecnologías de la información, así como software de producción nacional de la empresa XETID para la comunicación con el servidor OPC y software libre como Snort y PostgreSQL, todo esto permite asegurar la soberanía tecnológica de la solución.

## Referencias

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, 8 53-66.

Boyens, J., Moorthy, R., & Bartol, N. (2015). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800-161. [Internet]. Retrieved from: http://dx.doi.org/10.6028/NIST.SP.800-161

Byres, E., & Peterson, D. (2007a). OPC Security White Paper #2 OPC Exposed. Lantzville: Byres Research

Byres, E., & Peterson, D. (2007b). OPC Security White Paper #3 Hardening Guidelines for OPC Hosts. Lantzville: Byres Research

CCN-CERT (2016). Amenazas y análisis de riesgos en Sistemas de Control Industrial (ICS). [Internet]. Retrieved from: https://www.ccn-cert.cni.es/gl/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-publicos/1381-ccn-cert-ia-04-16-amenazas-y-analisis-de-riesgos-en-sistemas-de-control-industrial-ics/file.html

Centro de Ciberseguridad Industrial. (2016). Guia para la construccion de un sgci. Sistema de gestion de la ciberseguridad industrial. Madrid: Centro de Ciberseguridad Industrial. 1ra edición. ISBN: 978-84-942379-8-0

ICS-CERT. (2016). Recomended Practice: Developming an Industrial Control Systems Cybersecurity Incident Response Capability. [Internet]. Retrieved from: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Maglaras, L.A., Kim, K.-H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., ...& Cruz, T.J. (2018). Cyber security of critical infrastructures. ICT Express 4(1) 42-45.

Ministerio de la Informática y la Comunicaciones (2007). Resolución No 127/2007. Gaceta Oficial de la República de Cuba 57, 899 – 910.

Miranda, J.M., & Ramirez, H. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (17), 1-15. doi: 10.17013/risti.17.1–15

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (E3), 1-15. doi: 10.17013/risti.e3.1-15

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

U.S. Department of Homeland Security. (2009). Recomended Practice: Developming an Industrial Control Systems Cybersecurity Incident Response Capability. [Internet]. Retrieved from: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

U.S. Department of Homeland Security. (2009b). National Infrastructure Protection Plan: Partnering to enhance protection and resiliency. [Internet]. Retrieved from: https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Yokogawa Electric Corporation. (2015). Integrated Production Control System CENTUM VP System Overview (General Overview). Tokyo: Yokogawa Electric Corporation.

Yokogawa Electric Corporation. (2016). Safety Instrumented System ProSafe-RS System Overview. Tokyo: Yokogawa Electric Corporation.