Podemos aprender de incidentes de seguridad en sistemas SCADA?

1 Introducción

Los expertos en seguridad de todo el mundo continúan alertando sobre la seguridad de los Sistemas de Control Industrial (SCI).[1] Los Sistemas de Control Industrial se asemejan cada vez más a los ordenadores personales (PCs). Se utilizan en todos lados y tienen una cantidad considerable de software que con frecuencia está desactualizado y emparchado.

Incidentes recientes de seguridad ocurridos en el contexto de los sistemas de SCADA y de Control Industrial han demostrado claramente la importancia de contar con un buen monitoreo y control de las infraestructuras de SCADA.[2] En particular, **es crucial tener la capacidad para responder ante incidentes graves y poder analizar y aprender sobre lo ocurrido.**

La UE ha reconocido la urgencia de este problema y recientemente propuso una estrategia de seguridad cibernética para la UE que focaliza en el mejoramiento de la red de seguridad y sistemas de información utilizados para las infraestructuras críticas[3]. La estrategia exhorta a los estados miembros de la UE y a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés) a aumentar el nivel de los sistemas nacionales de información (SIN) de los sectores críticos y a apoyar el intercambio de mejores prácticas.

ENISA respondió a este llamado lanzando varias actividades sobre seguridad de SIC y SCADA[4].

Antecedentes técnicos: SCI y SCADA

Los sistemas industriales y las infraestructuras críticas con frecuencia son monitoreados y controlados por computadoras simples llamadas (Sistemas de Control Industrial (SCI).Los SCI están basados en plataformas de sistemas integrados estándar y con frecuencia usan software comerciales. Los SCI son utilizados para controlar los procesos industriales, tales como la fabricación, el manejo de los productos y su distribución. Entre los sistemas bien conocidos de SIC se encuentran los sistemas de control y de adquisición de datos (SCADA), sistemas de control distribuido (DCS), y los controladores lógicos programables (PLC).

Los sistemas SCADA se distinguen de otros SIC desde hace mucho tiempo porque es el subgrupo de SCI más grande y que atiende procesos de gran escala que pueden incluir lugares múltiples y grandes distancias. Un Sistema de Control y de Adquisición de Datos (SCADA) puede ser visto generalmente como un conjunto de equipos interconectados que se utilizan para monitorear y controlar equipos físicos en entornos industriales. Son utilizados generalmente para procesos automatizados distribuidos geográficamente, tales como de generación, trasmisión y distribución de energía eléctrica, gestión de refinerías, oleoductos y gasoductos, procesamiento y producción de productos químicos y sistemas de transporte ferroviario y de otro tipo.

El nivel de monitoreo de redes incluye tecnologías comprobadas que han sido utilizadas con éxito durante muchos años para analizar incidentes de seguridad en entornos de redes tradicionales. La instalación de sensores para la detección de intrusos y el control de tráfico se ha convertido en una práctica más aceptable, especialmente porque una cantidad de sistemas modernos permiten el uso

[1] http://threatpost.com/hackers-aggressively-scanning-ics-scada-default-credentials-vulnerabilities
[2] http://www.wired.com/threatlevel/2012/01/10000-control-systems-online/
[3] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
[4] http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013

de PI. Cada vez es más frecuente que entidades de asesoramiento publiquen directrices y normas que son aplicables al campo de la seguridad en este tipo de entorno.

Este documento explora los problemas antes mencionados y ofrece recomendaciones para la implementación de un enfoque proactivo que facilitará una respuesta ágil e integrada a los incidentes y que servirá para su posterior análisis.

ENISA identificó varias actividades clave que pueden contribuir para alcanzar esta meta:

- Facilitar la integración de procesos de respuesta cibernéticos y físicos con un mayor conocimiento de donde se puede encontrar la evidencia digital y sobre cuales serían las acciones apropiadas para preservarla;
- Diseñar y configurar sistemas de forma que se pueda retener la evidencia digital,
- Complementar la base actual de capacidades con conocimientos y experiencia sobre los solapamientos entre los equipos de respuesta cibernética y física ante el incidente crítico,
- Incrementar los esfuerzos de colaboración interinstitucional entre públicos y privados y entre los diferentes países.

2 Audiencia focalizada

El propósito de este documento es informar a los operadores de la comunidad relacionada con SCADA y a los ingenieros del campo de la seguridad y ofrecer otra conexión entre los encargados de adoptar políticas y los especialistas de tecnología en el delicado campo de la protección de la infraestructura crítica.

En particular, ENISA apunta a:

- Informar a los equipos de operaciones acerca de las capacidades de conexión y de análisis posterior del incidente que deberían considerar cuando diseñan e implementan sistemas de SCI con base en los niveles actuales de las amenazas que existen en su contexto operativo,
- Informar a los ingenieros en seguridad sobre la oportunidades y desafíos que se pueden presentar en este campo,
- Proponer un conjunto de recomendaciones para desarrollar un entorno proactivo de un nivel apropiado de preparación con respecto al análisis posterior al incidente y a la capacidad de aprendizaje,
- Facilitar y promover la discusión entre los dos primeros grupos de interesados y encargados de adoptar políticas en su lucha por facilitar el desarrollo y mantenimiento de infraestructuras críticas seguras y resilientes.

3 Análisis posterior al incidente

El objetivo principal de un análisis posterior a un incidente es obtener información valiosa sobre la seguridad a fin de adquirir un conocimiento profundo de lo ocurrido. Al examinar los diferentes aspectos de un sistema se pueden obtener conocimientos e información valiosa. Sin embargo, no es importante solo para conocer las circunstancias bajo las cuales hubo un problema de seguridad sino que esto permite además tener la capacidad para:

- Crear un conjunto de evidencias sólidas para responder al carácter cambiante de las amenazas internas y externas y minimizar las fallas de los sistemas SIC-SCADA[5],
- Asegurar suficiente aprendizaje para instalar sistemas resilientes.

Recopilar pruebas relacionadas con los incidentes puede revelar acciones que se llevaron a cabo durante el incidente junto con los incentivos y quizás la identidad del atacante.

En un sistema de redes puede haber muchos lugares donde se pueden recuperar evidencias. El tráfico de redes y los registros de los sistemas operativos ofrecen las fuentes más significativas de evidencias; sin embargo, el carácter diverso de los sistemas de control industrial impide el uso de una metodología única y coherente.

El análisis posterior al incidente es una parte fundamental de la gestión de seguridad. Si bien es la primera etapa de un proceso forense digital, se deben distinguir estos dos términos porque el análisis forense digital incluye la preparación de resultados de manera de permitir que los resultados sean presentados como evidencias ante un tribunal y es obligatoria la participación de las autoridades del poder judicial, en tanto que un análisis posterior al incidente procura fundamentalmente:

- Identificar el objetivo del ataque,
- Inferir el propósito real del atacante, si fuere posible,
- Identificar las vulnerabilidades del sistema en el cual se basó el ataque,
- Descubrir el posible robo de datos y rastros que se pueden utilizar para descubrir el origen del ataque.

3.1 El proceso

Los primeros pasos para realizar el análisis de un incidente en el campo de los sistemas de control industrial incluye el examen del sistema y la identificación de los componentes afectados. Luego, se recopilan y analizan todos los registros del SO y las transacciones relacionadas con estos componentes con base en directrices ampliamente conocidas que están fácilmente disponibles[67].

En la Figura 1 a continuación, se presentan los cinco pasos básicos para realizar el análisis posterior del incidente de cualquier dispositivo[89].

[5] *Al investigar un incidente de seguridad, se pueden obtener conocimientos valiosos que se pueden usar para fortalecer el sistema contra ataques futuros y mitigar los efectos de estos incidentes al incorporar mecanismos apropiados de defensa proactiva.*

[6] S. Wilkinson, “Good Practice Guide for Computer-Based Electronic Evidence,” Assoc. Chief Police Off., 2010.

[7] M. Fabro and E. Cornelius, “Recommended Practice: Creating Cyber Forensics Plans for Control Systems,” Dep. Homel. Secur., 2008.

[8] R. Radvanovsky and J. Brodsky, Eds., Handbook of SCADA/Control Systems Security. CRC Press, 2013.

[9] T. Spyridopoulos and V. Katos, “Requirements for a Forensically Ready Cloud Storage Service,” Int. J. Digit. Crime Forensics Ijdcf, vol. 3, no. 3, pp. 19–36, 2011.

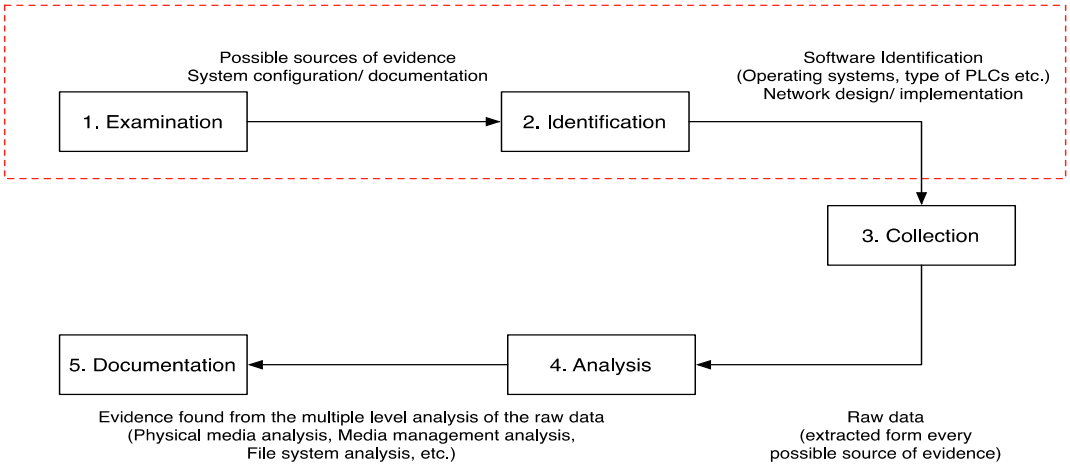

Fig 1. **Proceso del análisis posterior a un incidente de sistemas SCADA.**

Los pasos a seguir son los siguientes:

1. **Examen**: En la etapa del examen el investigador deberá conocer todas las fuentes potenciales de evidencias de un sistema SCADA. Además, también se debe tomar en cuenta en la investigación cualquier otro sistema relacionado con el sistema SCADA. Esto incluye el acceso a las terminales, servidores y routers.

2. **Identificación de evidencias**: El punto inicial de esta etapa es identificar el tipo de sistema que se investiga[10]. Una vez que se lo conoce, la próxima etapa es identificar el sistema operativo que se utiliza, los tipos y el fabricante de los PLC, y el diseño y la implementación de la red. Hacia esta dirección la información recopilada de los Puntos de Contacto del sistema pueden ofrecer datos valiosos. En el proceso de identificación pueden asistir, la documentación del fabricante, las especificaciones de diseño, los diagramas de la red y la Interfaz Humano-Máquina.

3. **Recopilación de evidencias**: La etapa de recopilación incluye la obtención de datos de todos los sistemas con los componentes de memoria que han sido identificados en la etapa 2. También deben ser capturados el tráfico de la red entre los componentes identificados del sistema, tales como el tráfico entre la red de control y la administración de la red y entre el sistema SCADA e Internet.

4. **Análisis de las evidencias:** En la etapa de análisis se identifican las evidencias en los datos recopilados. Eventualmente, se crea un cronograma de actividades con base en los datos

[10] El tipo de sistema puede ser RTU, PLC, HMI, etc. y el ámbito final es encontrar las herramientas apropiadas que pueden ser utilizadas con base en las especificaciones de equipo y software.

que fueron recopilados. Las principales categorías del análisis posterior al incidente se pueden definir mediante el uso de la noción de las capas de abstracción[11].

- **Análisis de los medios físicos:** El análisis de los medios físicos traduce el contenido de un diseño de almacenamiento a una interfaz estándar (IDE o SCSIs). Entre los ejemplos se incluyen, un disco duro, compact flash, y chips de memoria.
- **Análisis de la gestión de medios:** En el análisis de la gestión de medios se organizan las fuentes de evidencias con base en ciertos criterios vinculados a las estructuras de los datos. Entre los ejemplos de esta actividad se incluyen la división de un disco duro en particiones, la organización de discos múltiples en un volumen y la integración de chips de memoria múltiples en un espacio de memoria.
- **Análisis del sistema de archivos:** El análisis de la capa de abstracción del archivo, que traduce los bites y sectores de la partición en directorios y archivos, incluye ver observar los directorios y el contenido de los archivos lo cual conduce a la recuperación de los archivos eliminados.
- **Análisis de la aplicación:** El análisis en esta capa incluye examinar los archivos de acceso, los archivos de configuración, las imágenes, los documentos y la ingeniería inversa ejecutable. Los datos almacenados generalmente se encuentran en el sistema de archivo aunque algunas aplicaciones, tales como las bases de datos pueden leerlos directamente del disco duro.
- **Análisis de la red**: El análisis en esta etapa incluye los paquetes de la gestión de la red y los alertas. El análisis de los registros generados por los servicios de la red, también se incluyen dentro del análisis de la red, un cortafuegos o un servidor de la web.
- **Análisis de la memoria:** El análisis en esta área incluye identificar el código de que un proceso estaba en marcha y extraer datos sensibles que estaban almacenados en este código.

5. **Documentación del proceso y resultados:** En cada proceso del análisis posterior al incidente es esencial mantener la documentación integral. Se deben mantener notas detalladas, registrando la hora, la fecha y el nombre de la persona responsable además de otros datos e información esenciales. De esta manera se facilita a que las evidencias no puedan ser adulteradas por alguien de adentro durante el análisis posterior al incidente y en el caso de futuros incidentes la documentación podrá servir como referencia para el manejo de la situación.

3.2 Estructuras y procedimientos orgánicos

Para que las capacidades antes mencionadas puedan funcionar dentro de una organización debe contarse con la estructura y procedimientos apropiados con respecto a la respuesta ante incidentes

[11] B. Carrier, "Defining digital forensic examination and analysis tools using abstraction layers," Int. J. Digit. Evid., vol. 1, no. 4, pp. 1–12, 2003.

y al análisis posterior al incidente y su investigación. Tradicionalmente, un programa de análisis posterior a un incidente será iniciado después de la finalización de la mitigación del incidente y de la restauración de los sistemas mediante la capacidad de respuesta existente. Establecer la capacidad de respuesta a un incidente no es algo trivial, aunque existen muchos recursos que describen las funciones esenciales y papel orgánico con sus responsabilidades.[12]

Las operaciones de respuesta a los incidentes son importantes porque si no están bien diseñadas tienen el potencial de impedir cualquier empeño de investigación posterior al incidente porque las evidencias esenciales pueden haber sido eliminadas o afectadas durante las actividades de mitigación, recuperación y restauración. Sin embargo, si se planea correctamente, la integración y capacidad de análisis posterior al incidente dentro de los procedimientos de respuesta pueden funcionar, siendo la función de investigación un aspecto contenido de la capacidad de respuesta al incidente, incluida la presentación de datos para fines de enjuiciamiento.

Los componentes básicos de una respuesta a un incidente cibernético con un componente de investigación integrado serían modificados de la siguiente manera:

1. Detección
2. Inicio de la respuesta
3. Acción de respuesta al incidente**/Recopilación de evidencias**
4. Recuperación del incidente**/Análisis de las evidencias**
5. Finalización del incidente**/Proceso de información**

Debido a la singularidad de los datos y a las relaciones entre los recursos de información y el campo de los sistemas de control, un equipo compuesto de personas que tienen un conocimiento avanzado del sistema deberá completar un análisis de las evidencias recopiladas.

Por lo tanto, además de quienes responden tradicionalmente a los incidentes, los miembros del equipo necesitarían incluir algunos papeles y responsabilidades, a saber[13]:

- **Director del Sistema de Comando de Incidentes (DSCI)** – una persona que supervise las operaciones de respuesta en el campo de los sistemas de control. Ejercerá la supervisión de las actividades para asegurar las interrelaciones entre las operaciones y el personal de tecnologías de la información (TI) y asegurar que los requisitos de ambos campos pueden ser comunicados en una forma comprensible para todas las partes interesadas.
- **Especialista del Sistema de Comando de Incidentes (ESCI)** – encargado de asegurar cuáles son los aspectos críticos que pueden ser impactados. Esta persona trabajará también estrechamente tanto con los ingenieros como con los administradores de casos de incidentes apoyando tanto la investigación como las actividades de contención y tendrá actividades tácticas específicas apoyando la restauración, información y análisis de la situación.
- **Apoyo de Ingeniería para el Sistema de Control (AISC)** – Tener a alguien de apoyo de ingeniería para el sistema de control contribuiría a las funciones básicas tales como las de contención, planificación para la recuperación y restauración (así como de mejoramiento del sistema), lo cual ofrecerá un valor significativo al análisis posterior al incidente.

[12] "CPNI Good Practice Guide, PROCESS CONTROL AND SCADA SECURITY GUIDE 3. ESTABLISH RESPONSE CAPABILITIES."

[13] M. Fabro and E. Cornelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," Dep. Homel. Secur., 2008.

Cuadro 1. Matriz de funciones para la respuesta a incidentes y el análisis de los sistemas de control[14].

Actividad de respuesta a incidentes	Equipo de manejo de incidentes	Coordinador RI (con SC)	Seguridad Básica (POC)	Director Respuesta Incidentes	Director Incidente SC	Especialista Seguridad SC	Apoyo Ingeniería SC	(Coordinador SC)
Detección								
Detección	P	S	P					
Información inicial y documentación	P	P	P					
Inicio de la respuesta								
Incidente Clasificación	P		P	S	P			
Aumento			P	P	P	S		
Acción de emergencia	P		P	P		S	S	P
Respuesta al incidente/ Obtención de evidencias								
Movilización	S	P	S	P	P	S	S	S
Investigación	S	P	P	S	P	P	S	S
Contención	P	P	S	S	P	P	P	S
Recuperación del incidente/Análisis de evidencias								
Recuperación Planificación		S	S	S	P	P	P	S/P
Restauración		S	S	S	P	P	P	S
Mejoramiento del sistema		S	S	S	P	P	P	S
Finalización del incidente/ Proceso de información								
Resumen de la información		P	S	S	S	P	S	
Mitigaciones/Información			P	P	P	P	S	S
Mejoramiento del sistema	P		P	P	P	P	S	

En este cuadro se indican las actividades primarias como P y las funciones secundarias como S.

3.3 Las pruebas y su dimensión integral

Para asegurar que el analista tiene un marco conciso y efectivo para ejecutar un análisis post mortem del entorno de un sistema de control, se deberán examinar los siguientes elementos tradicionales[15]:

[14] M. Fabro and E. Cornelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," Dep. Homel. Secur., 2008.

[15] M. Fabro y E. Cornelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," Dep. Homel. Secur., 2008.

- **Referencia de la hora**[16]: Muchos sistemas SCADA, debido al carácter de sus procesos requieren actividades y transacciones que sean logrados en milésimas de segundos. Tomando también en cuenta la volatilidad de las pruebas en un sistema de control, el analista necesita un sistema de referencia del tiempo de alto precisión a fin de llevar a cabo el análisis posterior al incidente. El registro del tiempo y de las actividades durante la investigación requieren un reloj de referencia de alta precisión.
- **Registros de actividades y registros de transacciones**: Dependiendo del tipo de un sistema de SCADA durante un análisis posterior a un incidente se pueden extraer diferentes datos de los diversos componentes.

Cuadro 1. Tipos de datos que se pueden extraer de un sistema SCADA, con base en la tecnología de control y las herramientas de adquisición utilizadas

	Centro de control	***Dispositivos de campo***
Tecnologías de sistemas de control Modernas/Comunes	- Captura de tráfico en la red. - Administrador del sistema de control en caso de un SO modificado sobre HMIs.	- Registros de red. - Registros del centro de control relacionados con los dispositivos de campo. • Dispositivo apagado: Examen del dispositivo por posible evidencia. • Dispositivo prendido: Fecha y hora, procesos actualmente activos y procesos en marcha.
Tecnologías de sistemas de control Modernas/Propietary	- Pueden ser aplicables herramientas modernas de análisis posterior al incidente. - Captura de tráfico en la red. - Es obligatoria la interacción entre el investigador y el proveedor.	- Registros de redes. - Registros del centro de control sobre dispositivos de campo. - Es obligatoria la interacción entre el investigador y el proveedor. - Puede incluir mecanismos de seguridad específicos integrados del proveedor.
Tecnologías de sistemas de control Legacy/Propietary	- No se pueden aplicar métodos de análisis tradicionales post mortem. - No hay funcionalidad de registro. - Ya no hay apoyo del proveedor. - Interacción con el propietario del equipo puede ofrecer alguna información. - Basado en comunicaciones en serie, tráfico de redes no puede ser capturado.	- Basado en comunicaciones en serie, tráfico de redes no puede ser capturado. - Rápida frecuencia del muestreo y anulación de datos - Rápida frecuencia del muestreo y anulación de datos. - Es esencial la interacción con el proveedor. - Debe estar a disposición un ingeniero con experiencia para apoyar la investigación

- **Otras fuentes de datos:** Entre otras fuentes de datos que deberían ser consideradas en un análisis posterior a un incidente se incluyen los diversos dispositivos de almacenamiento que se pueden encontrar en el centro de control de un sistema SCADA. Estos dispositivos incluyen medios móviles tales como disquetes, CDs/DVDs, USB u otras formas de medios de

[16] Cuando se realiza un análisis posterior al incidente es de vital importancia establecer la referencia del tiempo para el progreso normal de la investigación. En los sistemas de control la sincronización del tiempo desempeña un papel importante no solo para la investigación del incidente sino que también para la operación regular del sistema.

dispositivos de almacenamiento de datos móviles que se pueden encontrar en las instalaciones de los centros de control.

- **Fallas generales del sistema**
- **Monitoreo en tiempo real**
- **Monitoreo de la integridad del dispositivo**

El proceso de documentación incluye también la producción de un Informe Resumido detallado que describe todo el procedimiento. Este informe también incluye el estado y la condición del sistema capturado a través del proceso de recopilación de información. Más adelante se concentra la atención en los primeros tres aspectos, como los últimos tres son temas que tradicionalmente son bien comprendidos dentro del contexto de las operaciones de los sistemas SCADA, debido al énfasis en las fallas de administración, seguridad y confiabilidad de la información.

4 Desafíos

La alta volatilidad de sus datos, los limitados mecanismos de acceso que se pueden usar y otras características de los sistemas SCADA presentan muchos desafíos en el proceso para la recopilación y análisis de datos, tanto desde el punto de vista técnico como operativo. Esta sección describe los desafíos que pueden surgir durante un análisis de un incidente post mortem de sistemas SCADA:

A. Desafíos para la recopilación de datos:

- **Mecanismos de registro inadecuados**: Los mecanismos de registro de los sistemas de SCADA están orientados hacia los procesos de distorsión en vez de los casos de violación de la seguridad y por lo tanto ofrecen una contribución limitada en el campo de respuesta ante incidentes,

- **Alta volatilidad de datos:** El carácter de los sistemas de control impone la supresión, eliminación o reemplazo de datos en algunos componentes del sistema, tales como grabadores de datos de alta velocidad a tal velocidad que es prácticamente improbable o imposible coleccionar los datos. El costo de los mecanismos de registro en estos dispositivos es tan elevado que resultan prohibitivos,

Investigación posterior al incidente: Cuando los datos no volátiles, tales como los datos almacenados en un disco duro son recopilados en un sistema que está apagado, este procedimiento corresponde a la categoría de una investigación posterior al incidente.
Investigación actual: Cuando se necesita recopilar datos, tales como volcados de memoria o actividad de la red, este procedimiento corresponde a la categoría de las investigaciones actuales.

- **Núcleos del sistema operativo hechos a la medida**: Un sistema SCADA puede utilizar núcleos hechos a medida en sus componentes a fin de mejorar el rendimiento del sistema, a pesar de que actualizar dichos núcleos es difícil. Esto puede hacer que las herramientas de obtención de datos tradicionales como discos duros o volcados de memoria no se ejecuten debido a problemas de incompatibilidad o a la falta de módulos del núcleo.

- **Gran cantidad de datos menores**: Recopilar información sobre los niveles menores de una red SCADA, como por ejemplo los datos producidos por los sensores, resultaría en gran cantidad de información que requiere un enorme espacio de almacenamiento.

- **Bajo poder computacional**: Los sistemas Legacy tienen muy poco poder computacional para el registro y análisis de datos producidos en conjunto con los datos de control. Por lo tanto, a este nivel no se pueden implementar más operaciones con respecto a otros procesos como el análisis de incidentes.

B. Desafíos del análisis de datos:

- **Herramientas para el análisis posterior al incidente**: Las herramientas modernas para realizar el análisis posterior al incidente recurren a guiones y programas compilados anteriormente que automatizan el proceso de recopilación de evidencias mediante el uso de ciertas técnicas, tales como procesos de copia de bits y generadores de verificación de suma, que no pueden ser aplicados en plataformas y elementos de software de un sistema de control en su forma original de manera que pueden realizarse después del análisis. Las modificaciones del software deben ser implementadas en las herramientas tradicionales de análisis a fin de cumplir con las especificaciones de un sistema de control.

- **Análisis de datos y correlación:** La recopilación de datos de los repositorios clave (tales como Datos Históricos y HMIs) y los datos volátiles no persistentes obtenidos de los diferentes dispositivos (tales como dispositivos PLCs e I/O) deben ser correlacionados a fin de crear una representación informativa del incidente que pueda ser considerada como evidencia.

C. Desafíos operativos:

- **La aparente brecha cultural** entre los especialistas de tecnología de la información (TI) y el personal de operaciones: A primera vista, esta división parece ser creada por las diferencias de objetivos operativos entre la comunidad de control industrial (disponibilidad, confiabilidad, seguridad) y la focalización en seguridad tradicional de las TI (confidencialidad, integridad, disponibilidad).

- **La ausencia de estudios científicos dedicados**: Hay una falta de estudios científicos dedicados al rendimiento de los equipos de operaciones e instrumentos de control que operan en un entorno de configuraciones de seguridad que exigen un control de acceso estricto, una sólida codificación criptográfica y un registro integral de eventos. El usuario final de la comunidad resulta ser un poco conservador para adoptar arquitecturas de seguridad que estén basadas en estas premisas.

- **La gestión de la obsolescencia** y la disponibilidad de habilidades para manejar los sistemas Legacy: Actualmente la comunidad de usuarios identifica una significativa falta de

capacidades en esta área en la que personas clave se están retirando y la nueva generación de ingenieros no poseen las habilidades para trabajar en sistemas más viejos.

- **Los ciclos de vida fundamentalmente diferentes** de las infraestructuras: Los componentes de una infraestructura tradicional de TI tendrían un ciclo de vida limitado en comparación con los instrumentos y equipos de control de un sistema SCADA (generalmente 5-7 años versus unas pocas décadas).

5 Recomendaciones

ENISA ha identificado las siguientes áreas clave en las que se puede tomar medidas a fin de desarrollar capacidades de investigación que logren el nivel del riesgo percibido:

A. **Facilitar la integración con las estructuras actuales para la elaboración de informes y análisis**:
   a. Percibir donde se pueden encontrar las evidencias: Como parte del proceso tradicional de evaluación de riesgos, podría ser beneficioso considerar junto con los escenarios de violación de la seguridad donde la evidencia es crucial e identificar donde se encuentran las pruebas.
   b. Comprender el impacto de la retención de datos: Es recomendable que se realice algún tipo de evaluación de impacto de las políticas de retención de datos en una infraestructura de prueba que se asemeje al entorno operativo. Es esencial conocer si se van a introducir algunos costos (y a cuanto ascienden), cuando se agreguen dispositivos de registro más avanzados por encima y más allá del registro de fallas y paradigma tradicional de operaciones de seguimiento del rendimiento tradicional.
   c. Gestionar la obsolescencia y la interfaz de TI/Operaciones: Aunque no está directamente relacionado con el análisis posterior al incidente, un plan estructurado para la gestión de la obsolescencia, cuando fuere aplicable, asegurará contar con el conocimiento adecuado de los sistemas Legacy y es posible el acceso a las instalaciones apropiadas para su gestión.

B. **Sistemas y configuraciones de protección**:
   a. Instalar controles adecuados de seguridad que al mismo tiempo realicen operaciones de registro – tales como cortafuegos (*firewalls*) y sistemas de detección de intrusos: El punto crítico de una gestión de seguridad efectiva es la implementación de controles apropiados y bien probados capaces de equilibrar el riesgo y ofrecer mecanismos para enfrentar los incidentes y hacer su seguimiento.
   b. Diseñar sistemas teniendo presente la protección de las evidencias: Una protección adecuada de los datos históricos es esencial para la retención de las evidencias de carácter forense. Los sistemas modernos pueden registrar una gran diversidad de eventos pero el acceso a los registros puede ser comprometido por un atacante que podría eliminar fácilmente sus huellas.
   c. Facilitar el registro de eventos comunes en todo el sistema, como mínimo: La mayoría de los sistemas y equipos de control modernos son capaces de producir y retener una gran cantidad de información relacionada con su situación operativa y también con el contexto de los eventos. Sin embargo, qué eventos pueden ser registrados y cuál es la forma exacta de los datos puede variar tremendamente entre un equipo y otro.

C. Revisión de los papeles clave y responsabilidades:

a. Identificar las brechas en materia de capacidad para la investigación digital: Es importante conocer cuál es el nivel disponible (o falta del mismo) de capacidades y conocimientos en materia de investigación, entre el personal actual.

b. Identificar interfaces y solapamientos de respuesta física y cibernética: Una revisión de los papeles de organización y de responsabilidades relacionados con la respuesta a incidentes -- incluidos los incidentes operativos, físicos y cibernéticos-- puede facilitar la integración de la capacidad de respuesta tanto desde la perspectiva física como cibernética.

D. Procurar una estrategia orgánica pública y privada y de cooperación en todo el país:

a. Un enfoque coordinado a nivel nacional (por ejemplo, paneuropeo): Esta podría ser otra dimensión que podría promover un mayor desarrollo comunitario.

b. La experiencia de compartir la colaboración múltiple a nivel privado y público puede mejorar las posibilidades de lograr una solución que sea integral y que se aplique en forma más general: Fomentar la colaboración entre los Estados es percibido como algo de importancia crítica en vista de que los ataques pueden estar dirigidos a través de diferentes lugares y desde diversas jurisdicciones extranjeras.