Resumen

Encuentro 16 de Diciembre de 2015

Experiencias gestionando la Ciberseguridad Industrial. Medidas Técnicas y Organizativas

"Ciberseguridad Industrial es el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías"

Centro de Ciberseguridad Industrial

www.cci-es.org

Contenido

Introducción

El pasado día 16 de diciembre el Centro de Ciberseguridad Industrial (CCI) celebró el XII encuentro de la Voz de la Industria denominado “ Experiencias gestionando la Ciberseguridad Industrial. Medidas Técnicas y Organizativas”. Esta cita ha sido el quinto encuentro de 2015 , tras los celebrados en febrero, mayo, septiembre y noviembre. Con esta serie de encuentros, el CCI pretende actuar como punto de reunión, y diálogo de la industria para acercar la Ciberseguridad a los sistemas de automatización y control.

En esta última edición de “La Voz de la Industria” se hizo balance del ecositema del CCI en 2015 y se expusieron las principales características del SGCI (Sistema de Gestión de la Ciberseguridad Industrial); también se pudieron escuchar las propuestas de Cisco como fabricante, y Tecnocom como implantador de soluciones de Ciberseguridad aplicables a la Industria. Así mismo se adelantaron algunas novedades sobre el Esquema Nacional de Ciberseguridad Industrial (ENCI), y el organismo certificador DEKRA describió cómo se va a abordar la implantación y certificación del SGCI en las industrias españolas. Por último, se celebró una mesa de debate en la que distintos expertos trataron el tema de la colaboración entre IT y OT en materia de Ciberseguridad.

Algunos Datos acerca del evento

Como viene siendo costumbre, la asistencia al evento representa a todos los actores del ecosistema con el siguiente reparto:

Aplicando el SGCI en Entornos Industriales. CCI.

Miguel García-Menéndez, Responsable de Gobierno Corporativo y Estrategia del CCI, comenzó presentando el conjunto de publicaciones del CCI hasta la fecha y destacando la publicación del SGCI, Sistema de Gestión de CIberseguridad Industrial. Primera Parte, herramienta para gestionar de forma eficiente, continua y alineada con las necesidades de la organización, los riesgos a la disponibilidad, integridad y confidencialidad de la información tratada por los sistemas de control industrial con tres premisas.

Miguel presentó los nuevos dominios desarrollados durante 2015, el dominio 4, Normativas de ciberprotección en instalaciones industriales, el dominio 5, Resiliencia y Continuidad en Sistemas de Operación y el dominio 6, Marco para la gestión, revisión y mejorar del SGCI. Miguel indicó que este sistema es recomendable en organizaciones industriales que dispongan de un sistema de gestión de calidad, y sobre todo de seguridad de la información para ampliar el alcance incluyendo sistemas de operación. Terminó la presentación con el anunció de publicación de una versión completa del SGCI en el primer trimestre de 2015.

La red como un sensor. CISCO.

El fabricante tecnológico Cisco estuvo representado en el encuentro por su responsable de soluciones de Seguridad en España, Eutimio Fernández. Quien trasladó su visión de cómo integrar la Ciberseguridad en la industria mediante la utilización de la red de datos como un sensor. Este concepto se basa en la visibilidad de la actividad en la red; la cual se consigue observando el tráfico de forma integrada con las distintas soluciones de Cisco; como son los switches, el appliance de seguridad ASA , el equipo AMP (Advanced Malware Protection), y la gestión de identidades ISE. Además Cisco dispone de una API que permite desarrollar proyectos personalizados según las necesidades de cada instalación.

La solución de Cisco facilita la detección e identificación de patrones y anomalías, aportando una visión global de lo que ocurre en la red de datos. Cisco combina su software NetFlow con la tecnología aportada por su reciente adquisición de la compañía Lancope; lo que proporciona analítica de comportamiento, visibilidad de amenazas, e inteligencia de seguridad en tiempo real mediante StealthWatch System. Parte de la información recogida se puede aprovechar en la realización de auditorías de seguridad.

Eutimio Fernández apuntó que este tipo de solución se adapta bien a las redes industriales debido a la uniformidad del tráfico de proceso, y a que las anomalías se detectan mejor en la red que en puntos concretos de la instalación. Siendo también una funcionalidad bastante apreciada en este sector la segmentación de red por software.

Un parte fundamental de la propuesta de Cisco es la gestión de Identidades ISE; la cual facilita la identificación de usuarios y dispositivos; así como la asignación de permisos de acceso a los recursos.

Las distintas soluciones de Cisco se integran entre si para correlacionar información; pero también existen acuerdos de interoperabilidad con otros fabricantes como Rockwell Automation, Checkpoint y Siemens; gracias principalmente al empuje de los proyectos IIoT (Industrial Internet of Things, también conocido por Smart OT)

En definitiva, la estrategia de Cisco en el sector industrial se basa en proporcionar vigilancia en la red interna (en lugar de hacia afuera como en otros sectores) mediante la gestión de identidades, y la visibilidad de flujos y protocolos de red.

Para finalizar, Eutimio Fernández comentó que el despliegue de proyectos es sencillo dado que se intenta aprovechar la infraestructura de red existente. Aunque se observa cierta dificultad en encontrar profesionales con conocimientos de análisis de datos, que sean capaces de filtrar y aprovechar la gran cantidad de información que arrojan estas herramientas.

Integrando seguridad IT y OT. TECNOCOM.

Cisco colabora con la consultora española Tecnocom en proyectos de distintos sectores, y también en el industrial; es por esto que Juan Bautista López, Responsable Desarrollo Negocio Seguridad y Optimización en Tecnocom participó en el encuentro para compartir su experiencia en proyectos conjuntos.

Juan Bautista subrayó la necesidad de integración de las redes en los entornos industriales; y explicó por qué el compartir información de forma global es la clave para mitigar las nuevas amenazas a las que se enfrentan este tipo de escenarios. En su opinión la Ciberseguridad debe estar integrada en todos los procesos de la empresa/industria; y ésta debe estar fundamentada en la adecuada recolección de información de fuentes confiables, en el filtrado preciso de datos significativos, en la adición de información de contexto, y en el análisis inteligente de todo ello.

Tecnocom recomienda evolucionar desde el modelo de seguridad basado en appliances de seguridad puntuales, a la seguridad global como conjunción de la toma de datos en puntos concretos de red, gestión de identidades, inteligencia de amenazas global,

herramientas de análisis forense, y programas de concienciación. Este modelo se articula en tres pasos:

- Antes: Etapa de prevención mediante gestión de identidades
- Durante: Etapa de detección con elementos de vigilancia de red
- Después: Etapa de corrección gracias a la respuesta a incidentes

Juan Bautista destacó que con este modelo de Ciberseguridad se podría llegar a conseguir una reducción de 197 días a 46 horas, en el tiempo estimado para descubrir un incidente de seguridad desde que llega hasta ser detectado.

En el despliegue de los proyectos en el entorno industrial Tecnocom apuesta por un tipo de prestación de servicios mixto; en el que el proveedor comparta la gestión de la ciberseguridad con el cliente. De esta forma se facilita a los departamentos de OT el acceso a nuevas prestaciones; pero siempre bajo su control y atendiendo a sus necesidades.

Por último, al igual que lo había hecho anteriormente el portavoz de Cisco, se señaló la necesidad de profesionales cualificados capaces de tratar y analizar toda la información sobre amenazas que aportan este tipo de soluciones.

Avances del Esquema Nacional de Ciberseguridad Industrial (ENCI). INCIBE.

Por parte de Incibe participó como ponente Juan Peláez. El cual adelantó algunas características de la próxima publicación del Esquema Nacional de Ciberseguridad Industrial.

Este nuevo marco de referencia surge a partir de la Estrategia Nacional de Ciberseguridad y el Esquema Nacional de Seguridad. Entre sus objetivos destacan la mejora de la capacidad de resilencia, la homogeneización del tratamiento de la

Ciberseguridad, la mejora de la competitividad industrial, la dinamización del sector, la catalización de nuevas normativas, y el fomento de puntos de encuentro entre IT y OT.

Se observan distintos actores en el desarrollo del esquema; que podrían concretarse en los siguientes: operadores críticos, proveedores, CNPIC, sector industrial, y el CERTSI de Incibe.

A lo largo de su exposición Juan Peláez hizo un repaso de los cuatro pilares fundamentales del esquema.

esquema.

Análisis de riesgos ligero (ARLI)

El análisis comienza con una clasificación de activos según las normas ISA 99 y 27000; y se completa con la identificación del servicio esencial, la evaluación de escenarios de amenazas, las medidas de seguridad, y finalmente con la aceptación del riesgo residual.

Dentro de este apartado se proporcionará una herramienta de autoevaluación de riesgos compuesta de una hoja Excel; y que se empleará en dos experiencias piloto a principios de 2016.

Indicadores de ciberresilencia

El esquema dispondrá de 250 controles en total, de los que se han escogido 46 como los más significativos. El modelo de indicadores de ciberresilencia está basado en estándares internacionales como MITRE.

Al igual que en el análisis de riesgos ligero, se dispone de un herramienta de autoevaluación basada en Excel con los 46 controles principales. Esta utilidad permite a los operadores analizar su robustez frente a las amenazas. Hasta la fecha Incibe ha consultado a 31 operadores para evaluar su servicio esencial; siendo una de las conclusiones obtenidas del estudio el que hay sectores con importantes márgenes de mejora.

Modelo de construcción de capacidades

Se basa en metodologías de calificación, para facilitar la evaluación y seguimiento del nivel de madurez de las medidas de seguridad adoptadas. Este modelo podría ser considerado una herramienta muy valiosa de concienciación para la alta dirección.

Apoyo regulatorio

En este capítulo se desarrollará un catálogo de normativas, buenas prácticas y estándares de Ciberseguridad.

Juan Peláez confirmó que el esquema aún está en fase de borrador, y que será revisado por un conjunto de expertos antes de su publicación en 2016.

Proceso de Certificación del SGCI. Dekra.

Yvonne Rauh, Country Coordinator de Dekra en España, hizo una introducción de la compañía. Dekra no es aún muy conocida en nuestro país; pero es una empresa alemana con sede en Berlín con una larga trayectoria; que justo este año celebra su 90 aniversario. Es una multinacional, que entre otras actividades, actúa como organismo de certificación independiente de sistemas de gestión. Y aunque en sus inicios estuvieron centrados en el campo de la automoción, se han ido expandiendo paulatinamente al resto de los sectores industriales.

En España, Dekra tiene presencia desde 1992. Actualmente tienen delegaciones en Madrid, Barcelona, Málaga y Sevilla; y esperan crecer este año un 130%.

Dekra, como organismo de certificación, está preparando el plan de certificación del "Sistema de Gestión de la Ciberseguridad Industrial" (SGCI) creado por el CCI, y que se hará público en 2016. Susana Calvo, responsable de desarrollo de negocio de certificación de sistemas, resumió el proceso de certificación, indicando en qué partes participa Dekra.

Existen tres niveles de certificación SGCI:

Nivel 1: Auto-Evaluación

La empresa interesada adquiere el cuestionario de autoevaluación proporcionado por el CCI; con cuyo cumplimiento puede realizar un autodiagnóstico de su estado de protección. Si el resultado de la autoevaluación supera el 50%, se adquiere el Nivel 1 de certificación; y la empresa pasa a formar parte de las bases de datos del CCI y de Dekra

Nivel 2: Auditoría de certificación Dekra

Una vez superada la autoevaluación, la empresa debe implantar el SGCI; siendo aconsejable que lo haga con la ayuda de un partner tecnológico. A continuación entra Dekra en el proceso de certificación para auditar y garantizar que el proceso industrial cumple con el SGCI, y entrega el certificado SGCI de Nivel 2.

Nivel 3: Auditoría de certificación anual Dekra

Como último paso, para conseguir el certificado de nivel 3 la empresa debería pasar una auditoría anual. El certificado obtenido en este caso tiene una validez de 3 años, pero debe ser revisado anualmente.

La certificación SGCI, como indica su nombre, puede ser solicitada por cualquier empresa del ámbito industrial; y aunque el certificado no está respaldado por una entidad superior, el asunto está en estudio, y se espera que con el tiempo se alcance. Al fin y al cabo, la validez de las certificaciones la otorga el mercado.

Es interesante para las compañías que ya están certificadas en ISO 27001, el hecho de que el SGCI aúna las directrices de las normas ISO 27001 e ISA 99; por tanto el proceso de certificación de SGCI es muy probable que sea más rápido.

Susana Calvo anunció que van a iniciar el proyecto de certificación con dos empresas piloto en Febrero de 2016; y a partir de Marzo se comenzará a ejecutar certificaciones reales.

Mesa debate: En un escenario donde IT y OT están integrados ¿Cómo debería ser la gestión de la ciberseguridad? Fortinet, Incibe, SIDE y Trend Micro

Para finalizar la jornada se organizó una mesa de debate donde los participantes intercambiaron opiniones acerca de cómo debe ser la gestión de la Ciberseguridad dentro de la corporaciones industriales. El debate fue dirigido por José Valiente del CCI. Intervinieron en la mesa dando su opinión cuatro expertos en Ciberseguridad industrial: José Luis Laguna de Fortinet, Juan Peláez de Incibe, José Ignacio Redondo de Side, y Olivier Bailliez de Trend Micro.

José Valiente fue haciendo distintas preguntas a los expertos; cuyas respuestas se resumen a continuación.

¿Qué situación debe producirse en una organización para que IT y OT colaboren en los proyectos de Ciberseguridad ?

En este aspecto las respuestas fueron variadas. Por una parte J.L. Laguna apuntaba que normalmente hasta que no se sufre una incidencia, no se toma conciencia del peligro; y que es entonces cuando desde la alta dirección se impulsa un entendimiento entre las dos áreas.

Por otro lado, Juan Peláez opinaba que lo deseable es que la colaboración entre IT y OT comience en el desarrollo de un análisis de riesgos elaborado conjuntamente, y que sea presentado en común a la gerencia. Además subrayó que sería interesante que ambos departamentos pudieran obtener algún tipo de incentivo por esta labor.

Olivier Bailliez propone formación y concienciación tanto en IT como en OT para que se pueda apreciar el impacto; y con ello propiciar la colaboración

José Ignacio Redondo comentó su experiencia personal, en la que en algunas ocasiones es él mismo como proveedor, el que tiene que solicitar a los dos departamentos la asistencia a las reuniones de adquisición de nuevas soluciones de seguridad.

¿ Cuáles deberían ser las funciones y responsabilidades del personal de IT y OT ?

A esta cuestión comenzó respondiendo José Ignacio Redondo, quien proponía aprovechar la experiencia de cada uno para colaborar en la definición de los sistemas y características de Ciberseguridad de los elementos que hacen de nexo entre la red corporativa y la red de operación.

Olivier Bailliez piensa que por una parte el departamento de IT debe tener conocimiento de los procesos industriales y de su tecnología; y por otra, que el personal de OT debe ser consciente de que por estar en contacto directo con los procesos, deberían ser ellos los primeros en incorporar las medidas de seguridad en sus procedimientos.

Juan Peláez planteó un responsable de Ciberseguridad con un perfil mixto que tenga conocimiento tanto de IT como de OT. También sugirió la figura de un comité multidisciplinar que se reúna para analizar el riesgo y las medidas de Ciberseguridad cada vez que se introduzca un cambio tecnológico en el proceso industrial.

José Luis Laguna coincidía con Juan Peláez en que es aconsejable un responsable ó un departamento transversal de Ciberseguridad que reporte directamente a la alta dirección y esté apoyado por ella. José Luis cree que los componentes de este departamento deben tener principalmente habilidades y conocimientos de IT; pero que debe conocer también el ambiente OT. Para concluir su turno de debate, José Luís quiso recordar la necesidad de concienciación en seguridad del personal de OT, puesto que la aplicación de la seguridad es un aspecto incómodo que inicialmente presenta rechazo.

¿ Quien debe liderar la Ciberseguridad dentro de la compañía ?

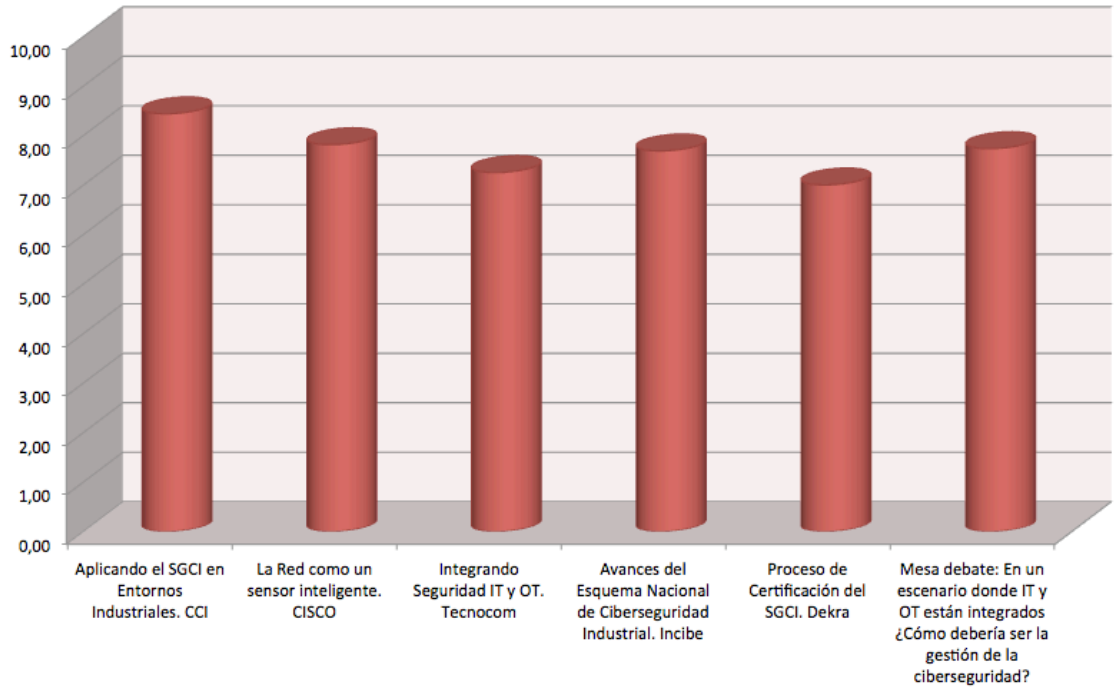
En esta pregunta los participantes de la mesa redonda coincidían en que el liderazgo lo debería llevar una responsable de Ciberseguridad que tenga conocimiento de las dos áreas. Y en caso de no existir esta figura, sería el departamento de IT el responsable de la Ciberseguridad; pero siempre basado en un análisis de riesgos en el que hubieran participado responsables de OT.
Por último José Ignacio señalaba que el éxito sería mayor si la Ciberseguridad viniera impulsada directamente desde la gerencia.

¿ Cuál sería el organigrama adecuado para gobernar la Ciberseguridad industrial de forma integral ?

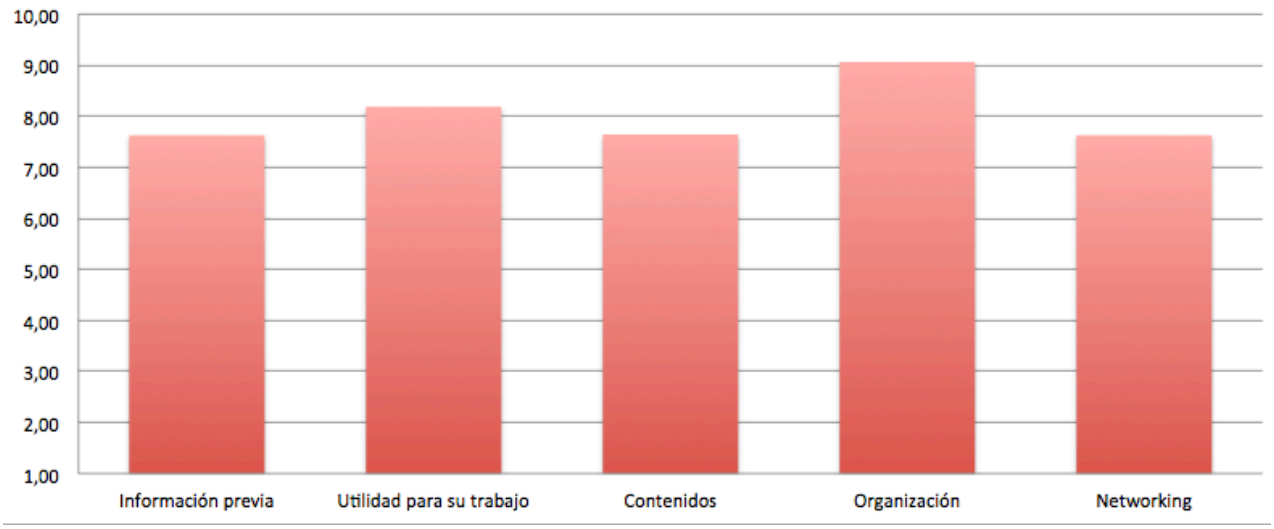
Aunque a esta cuestión se fue respondiendo con las intervenciones anteriores, este punto sirvió para consensuar entre los ponentes una posible propuesta de gobierno; que podría ser la siguiente:
A la cabeza del organigrama estaría la gerencia de la compañía impulsando y apoyando la Ciberseguridad; a continuación y directamente dependiendo de ella debería existir un responsable/departamento de Ciberseguridad Industrial compuesto por un perfil de IT con conocimientos de OT. Este departamento de Ciberseguridad podría ampliarse también con competencias de seguridad física para centralizar la Ciberseguridad y el Safety en un punto único. Además se deberían crear grupos multidisciplinares en los nuevos proyectos, en los que participasen profesionales de IT y OT e incluso los fabricantes de tecnología.

Valoraciones del evento

La valoración de las sesiones y de sus contenidos del encuentro ha sido muy buena, con una valoración media de un 8,03.



La valoración del encuentro de la voz de la industria ha mejorado superando un 8 de media y de forma muy significativa el apartado organización con un 9. A continuación mostramos la valoración de los asistentes:



Los temas que más interesan a los asistentes al evento son:

- La seguridad integral (Security & Safety).
- Actividades de INCIBE y CNPIC.
- Esquema Nacional de Ciberserguridad Industrial.

En nombre de todo el equipo del CCI, ¡Muchas gracias!

Patrocinador PLATINUM

Telefónica

Patrocinadores GOLD

Check Point · cisco · FORTINET · paloalto NETWORKS · Symantec · TREND MICRO

Patrocinadores SILVER

DEKRA · Honeywell · indra · pwc · S21sec · Tecnocom · TSK · TÜVIT

Patrocinadores BRONZE

Atos · accenture · EULEN SEGURIDAD · everis · gmv · Intermark it · CMC · KASPERSKY · PHOENIX CONTACT · S2 GRUPO · SIEMENS · tecnalia · TECNICAS REUNIDAS

Muchas gracias a todos por apoyar y confiar en el Centro de Ciberseguridad Industrial