Resumen

V Congreso Internacional de Ciberseguridad Industrial

6 y 7 de Octubre en Madrid

"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 congreso internacional **celebrado en Madrid el pasado 6 y 7 de Octubre** ha sido nuestro quinta edición. Ha servido para presentar la ciberseguridad industrial desde diferentes perspectivas, comenzando por los consejos de administración y las instituciones públicas, para continuar con la experiencia de operadores de infraestructuras críticas, expertos internacionales y proveedores de servicios y soluciones. Esta edición del congreso ha destacado por una gran representatividad del ecosistema y el incremento de madurez frente a los riesgos de ciberseguridad industrial.

El evento se ha celebrado en el Hotel Meliá Avenida de América en Madrid, reuniendo a 200 profesionales de la industria con el siguiente reparto de perfil de asistentes.

Resumen de la primera jornada del Congreso

La celebración del V Congreso Internacional de Ciberseguridad Industrial se ha convertido en un nuevo éxito de asistencia y contenidos, prueba de ello son algunos comentarios de los asistentes:

"I'm really impressed so far with the conference. Great job"

"The conference was: Well organized, Very interesting people, Opportunity to have discussion with people from different segments/markets/roles"

"Una vez finalizadas las jornadas, se observa que el ámbito industrial es un mundo complejo, en el que conviven multitud de actores muy distintos entre si, y con distinta historia y objetivos. Lo cual podría ser una de las causas de por qué la ciberseguridad tiene más dificultad para introducirse que en otros entornos."

"Enhorabuena por la organización del congreso …..se han presentando más soluciones a los problemas que en ediciones anteriores".

La mañana del primer día comenzó con la presentación del equipo de expertos del CCI https://www.cci-es.org/el-equipo/expertos y del nuevo coordinador de Francia. Acto seguido **Elizabeth Valentine, Directora General de Enterprise Governance Consulting presentó "Compentencias de los consejos de administración en Ciberseguridad Industrial"** donde demostró la importancia de que en los consejos de administración participen líderes digitales competentes, y en los que solo un 11% tienen suficiente capacidad IT en los consejos según estudio de NACD de 2015.

Manuel Sicilia, Jefe de Servicio de Ciberseguridad en el CNPIC, presentó "Siguientes Pasos en la Aplicación de la LPIC", comenzó explicando qué es CNPIC, y cual es su objetivo principal. Esta organización nació como respuesta a los nuevos desafíos de la sociedad actual como el terrorismo internacional y la proliferación de armas de destrucción masiva; que unidos a la mayor dependencia de la sociedad respecto de las infraestructuras que aseguran el mantenimiento de los servicios esenciales, hace que su protección sea una prioridad para los estados. Manuel comentó que mientras que en 2014 se habían redactado los cinco primeros planes estratégicos sectoriales: electricidad, gas, petróleo, nuclear, y financiero; en 2015 se han aprobado los planes para el transporte y el agua. Quedando pendientes para los próximos años, los planes para el sector de las TIC, el espacio, el sector químico, la salud y la alimentación.

En este segundo año de elaboración de planes estratégicos, el CNPIC ha mejorado su metodología en el desarrollo de los planes con idea de optimizar el tiempo de publicación de los mismos.

Alberto Hernández director de operaciones de Incibe habló sobre los datos recogidos por el CERT de Seguridad e Industria en 2015, y sobre los proyectos que actualmente tienen en marcha.

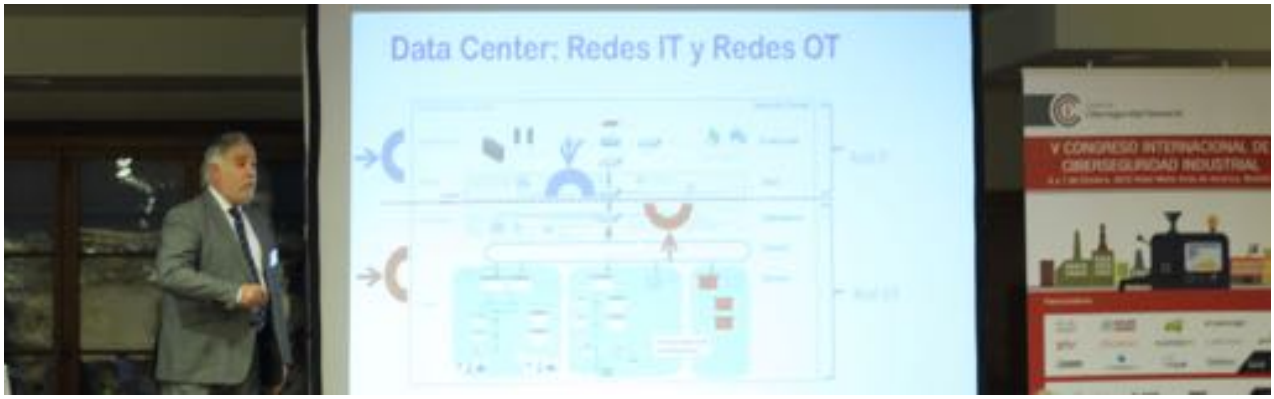
Este año el CERTSI contabilizó 35.000 incidentes de enero a septiembre, que comparado con los 10.000 recogidos el año pasado de enero a noviembre se han multiplicado por cuatro. Entre las incidencias reportadas destacan 52 alertas en infraestructuras críticas, y el aumento de la actividad de las botnets. Además coinciden con otros estudios internacionales en que el entorno más atacado ha sido el sector de la energía.

Una vez que el CERTSI registra una incidencia, lo comunica a la empresa y ofrece su ayuda para la resolución de la misma. Por otro lado, colaboran con otros CERT internacionales en el intercambio de conocimiento.

Alberto Hernández destacó los siguientes proyectos que actualmente están desarrollando:

- Desarrollo del Esquema Nacional de Ciberseguridad Industrial (ENCI).
- Red nacional de laboratorios industriales con capacidad para testeo, experimentación e investigación.
- Servicio de evaluación remota de riesgos de seguridad de entornos industriales.
- Honeypots de carácter específico industrial que recoja información sobre nuevos métodos de ataque
- Investigación aplicada de forma conjunta con la Universidad.

Enrique Martín de la empresa ITConic centró su ponencia en exponer su visión de las medidas de seguridad más adecuadas para **la protección de un data center.** No somos conscientes de que en realidad es un edificio que se compone de muchos más elementos que se deben gestionar y mantener, como los sistemas de refrigeración, generadores de energía, elevadores, alarmas, sensores ambientales, videovigilancia, etc.



Javier Olea y Antonio López presentaron "Presente y Futuro del IoT Industrial: Un caso práctico en Telefónica" describieron la propuesta de la compañía para el nuevo entorno de los "objetos conectados"; entre cuyas características tiene un lugar preferente la seguridad.

Carlos insistió en el concepto de objetos inteligentes. El Internet of Things (IoT) no se basa únicamente en la interconexión de objetos, sino en aprovechar la inteligencia de los dispositivos para que dispongan de una mayor autonomía, y que puedan actuar sobre los procesos ofreciendo respuestas.

Estos objetos inteligentes (Smart things) tienen una serie de capacidades como la autonomía, optimización, control, y monitorización, que facilitan su gestión global de forma centralizada.

La solución de Telefónica ha acogido el nombre de Telefónica IoT Platform; y está basada en el estándar Fiware impulsado por la Unión Europea. Esta plataforma dispone de una arquitectura totalmente abierta, pública y libre.

Mesa redonda: ¿Cual es la aproximación a las relaciones público-privadas y qué futuro les espera?

En esta mesa redonda, compuesta por Enrique Martín, Alberto Hernández, Manuel Sicilia y Carlos Olea, se debatió el tema propuesto y moderado por Miguel García-Menéndez; quien mediante las siguientes cuestiones fue preguntando su opinión a los participantes.

¿Qué consecuencia y que riesgos supone que no hubiera entendimiento entre el entorno privado y el público ?

Todos estuvieron de acuerdo en que debe existir confianza entre ambas partes; pero no se percibía mucho ánimo de colaboración entre ellos. Aunque si confirmaron que existe intercambio de información a nivel de alertas de seguridad.

Todos coincidieron que existen grandes retos y destacaron la importancia de la colaboración y articular mecanismos que lo permitan.

Desde la parte privada de la mesa redonda exponen que encuentran muchos problemas legales cuando quieren desarrollar proyectos debido principalmente a que hay poca legislación sobre el tema.

¿Qué canales de comunicación existen en las relaciones público-privadas ?

Existen varios canales como el CERTSI, acuerdos de confidencialidad entre el CNPIC e industrias concretas, y congresos y reuniones organizadas por INCIBE.

Por otro lado se apunta que es necesario disponer de los recursos humanos adecuados en ambos extremos de la comunicación que gestionen la colaboración.

¿Qué objetivos deben tener un mapa de ruta de las relaciones ?

En este aspecto cada uno de los participantes de la mesa aporta distintos aspectos que se pueden resumir en:

- Desarrollo de un framework de ciberseguridad industrial en el que participe la industria y que se particularice para cada uno de los sectores industriales.

- Promoción del talento en ciberseguridad.

- Concienciación del nivel ejecutivo de la industria.

- Implantación de la ley PIC 8/2011.

- Desarrollo de nueva legislación que regule la seguridad en las infraestructuras críticas.

Robert M. Lee hizo una brillante presentación con el título "**Descomponiendo Ciberataques ICS y Aprendiendo como Responder"** en la que mostró de forma clara y precisa cuales son las dificultades a la hora de realizar un ataque sobre sistemas de control industrial. Explicando ataques de poca dificultad, como es comprometer un acceso, pero la gran dificultad de dañar un sistema o proporcionar accesos para un ataque posterior. Explicó también de forma muy práctica el desarrollo y ejecución de los ataques realizados en Stunex, Havex.

Pero quizás lo más interesante para los asistentes fue la segunda parte de su presentación, donde expuso que se puede hacer para protegerse de los ciberataques. Donde señaló que lo primero es la arquitectura, es decir, la segmentación de red, la cadena de suministro, el mantenimiento y parcheado, después de tener la arquitectura resuelta, podremos ocuparnos de la defensa pasiva y activa, y como siguiente paso la inteligencia. Viene a decirnos que no deberemos empezar la casa por el tejado.

"Una Solución a las Amenazas: Cerrar la Brecha TI/TO mediante un Enfoque Fasado" fue otra interesante presentación técnica del proveedor **StormShield a cargo de Antonio Martínez y Frank Depierre.**

Antonio Martínez expuso la importancia de contemplar la diferencia en los tiempos IT y OT explicando el PDCA para un entorno de sistemas industriales y como adpatar las soluciones de StomShield en cada uno de los pasos.

Elena Maestre presentó "La experiencia de CEPSA en la adaptación a la LPIC". Explicó como Cepsa a abordado un año después la adaptación de la Ley PIC, desde su nombramiento como operador Crítico en Julio de 2014.

Una vez presentados los contenidos mínimos de los planes, Elena Maestre expuso como Cepsa abordó el análisis de riesgos requerido con un enfoque integral y la necesidad de homogeneizar los resultados. También presentó el enfoque integral de la gestión de incidentes para contemplar los niveles de alerta definidos por el ministerio del interior y la aproximación de coordinación interna y externa con el CNPIC/CERTSI.

Elena Maestre destacó como puntos más importantes a la hora de la adaptación a la LPCI en el caso de CEPSA:

- La necesidad de concienciar
- La visión integral para compartir y homogeneizar.
- Lograr procedimentar el ámbito Ciberindustrial
- El reporting a la alta dirección y a terceros.
- Nuevas responsabilidades organizativas.

Fernado Sevillano presentó "La Ciberseguridad en Industria 4.0" donde explicó que es Industria 4.0, como fue en 1969, cuando con la aparición del primer autómata programable (PLC), denominado Modicon 084 , se utiliza por primera vez el término de automatización industrial, iniciándose así la tercera revolución industrial. Desde ese momento hasta nuestros días, la irrupción y adopción de las tecnologías de la información y la comunicación en el ámbito industrial ha sido constante.

Actualmente paradigmas tecnológicos como Cloud Computing, Computación Ubicua, BYOD (Bring Your Own Device) o IoT (Internet of Things) están revolucionando la forma de entender la tecnología y la forma en que las personas interactuamos con ella. Estos paradigmas, aunque lentamente, van llegando también al ámbito industrial, acuñándose términos como WSN (Wireless Sensor Networks), IIoT (Industrial Internet of Things), M2M (Machine to Machine) comentaba Fernando.

En pocas palabras, el término Industria 4.0 hace referencia a la convergencia entre el mundo físico y el virtual, a partir del uso de una comunicación inteligente entre los seres humanos y las máquinas (de hecho se habla de sistemas CPS o Cyber-Physical

Systems), con la misma naturalidad que se desarrolla en una red social.

En este punto Fernando recordó que es preciso mencionar que aunque tradicionalmente la ciberseguridad industrial ha incidido mucho en asegurar la “disponibilidad” como elemento clave, en el contexto de la Industria 4.0, se remarca la importancia de la “confidencialidad” de la información y datos. Recordemos que la ubiquidad, el acceso remoto, el comportamiento autónomo de los CPS son características esenciales de la Industria 4.0 y que en este contexto, la preocupación porque los datos e información sólo sean accesibles por las personas autorizadas, o porque el know-how o la propiedad intelectual de las empresas no sea revelado, son aspectos clave a considerar.

Además, Fernando recalcó que es necesario abordar estratégicamente dos circunstancias que ocurren actualmente en los entornos industriales:

La heterogeneidad y la existencia de dispositivos y sistemas obsoletos o en fase de obsolescencia, hace tremendamente difícil desplegar programas de seguridad y ciberseguridad.

En segundo lugar, y estrechamente relacionada con la primera, para sustituir estos dispositivos y sistemas, es necesario que la industria cuente con soluciones que hagan que la transición de la Industria 3.0 a la Industria 4.0 sea lo menos disruptiva posible. En este sentido, sería imprescindible que los grandes fabricantes consensuaran qué funcionalidades y arquitecturas deberían ser las básicas para ayudar a realizar esta transición.

“Ciberseguridad Industrial, las amenazas y la realidad” fue la presentación a cargo de Vladimir Dashchenko, Research developer de **Kaspersky Lab**. En la que se abordaron los tres tipos de incidentes con más impacto en los sistemas industriales, por un lado la infección accidental de malware, pasando por las acciones de amenazas internas y terminando por las APTs. Se planteo en la presentación los principales

problemas de detección, entre los que se encuentran la falta de supervisión de la red industrial, la falta de conocimiento en el tratamiento de malware o la falta de firma de los ficheros en entorno SCADA.

La jornada finalizó con una interesante mesa sobre la Ciberresiliencia, en la que participaron: Robert M. Lee de SANS Institute, Frank Depierre de StormShield, Claudio Caracciolo de CCI y Fernando Sevillano de Logitek. En la que se respondieron a preguntas como ¿Qué riesgos están asumiendo las organizaciones que no están preparadas a un ciberataque dirigido?

Resumen de la segunda jornada del Congreso

La segunda jornada del congreso comenzó con el mismo interés de los asistentes y una agenda llena de presentaciones de alto nivel, unas técnicas y otras basadas en la experiencia de sus ponentes.

La jornada arranco con la presentación "**De la Teoría a la práctica: Hacking en el mundo industrial**", a cargo de **Gabriel González García, de la empresa IOActive,** quien expuso algunas debilidades de la seguridad de los sistemas embebidos. En concreto explicó cómo se puede realizar un ataque a un satélite de comunicaciones, y cómo manipular los contadores eléctricos inteligentes (smart meters).

Gabriel mostró que cierto modelo de satélite puede ser vulnerado mediante la ejecución de comandos sin permisos (inyección de código), y que se puede extraer la contraseña del administrador con herramientas sencillas.

El segundo caso de hacking estaba dirigido al entorno de las Smart Grids (redes eléctricas inteligentes). Una red inteligente se compone de distintos elementos desplegados. Desde el punto de acceso al consumo, donde se encuentra el contador inteligente, pasando por la red de distribución y comunicaciones, hasta el centro de gestión donde se realiza la tarificación, y el control de suministro. Uno de los puntos más delicados de la red es precisamente el contador inteligente; el cual está expuesto a distintas amenazas como son el fraude en la tarificación, el corte del suministro, ataques a gran escala, y sabotajes de la infraestructura física. Gabriel describió cómo teniendo acceso físico al contador, y con unos conocimientos básicos de electrónica, se puede realizar un ataque de ingeniería inversa hardware que intercepte las comunicaciones del contador (bus interno); lo cual puede facilitar el fraude en la medida del contador o en el tipo de tarifa.

José Luis Laguna, director técnico de Fortinet con la ayuda de **Antonio Navarrete**

de Grupo CMC abordaron la problemática de la gestión de parches en el entorno industrial; y de cómo las soluciones de Fortinet ayudan a solventarlo en la presentación "**Virtual Patching en sistemas DCS y SCADA**".

Aunque Fortinet es un fabricante de seguridad global, implementa en sus equipos Fortigate características que lo hacen muy adecuado para muchos casos del mundo industrial. Una de estas funcionalidades es el Virtual Patching; el cual facilita la aplicación de actualizaciones de software sin modificar el programa/aplicación que se está ejecutando. Existen buenas razones para aplicar esta técnica en los sistemas DCS y SCADA; entre las que se pueden nombrar sistemas operativos sin soporte del fabricante, muy pocos antivirus, vulnerabilidades conocidas, coste de actualizaciones, equipos conectados directamente a Internet según ha comentado Jose Luis Laguna.

Otras características que ha destacado de la solución Fortigate son la posibilidad de crear firmas de malware manuales, la capacidad para crear áreas de seguridad dentro de la red OT, o la facultad de crear redes privadas virtuales de acceso remoto y seguro para el mantenimiento de los equipos industriales.

Ciberataques dirigidos en infraestructuras críticas. Los famosos ataques avanzados persistentes (APT) desgraciadamente también se manifiestan en las infraestructuras críticas; y sobre ello centró su exposición **Enrique Martín del grupo tecnológico GMV**.

La ponencia comenzó con la definición de "infraestructura crítica" como servicio esencial para los ciudadanos; y cuyo funcionamiento y disponibilidad debe estar garantizado. De ahí la enorme importancia de una gestión adecuada de los ataques avanzados persistentes en este tipo de sistemas críticos; como son el transporte, las industrias química, petrolífera, y nuclear, o la distribución de aguas, gas y electricidad.

Enrique Martín hizo un repaso del concepto del ataque avanzado persistente, insistiendo en que se trata de una acción dirigida a objetivos concretos. Este tipo de ataques se caracterizan por su capacidad de sobrepasar las protecciones habituales de seguridad, porque permanecen ocultos en los sistemas incluso durante años, y porque van dirigidos a objetivos estratégicos normalmente con un propósito económico.

Como solución para intentar frenar este tipo de amenazas, GMV propone la tecnología de la “inteligencia de amenazas”. La cual mediante el conocimiento del comportamiento externo y de las tácticas de los atacantes, permite identificar y bloquear las acciones antes de que lleguen al objetivo. Además proponen un ciclo de gestión de amenazas basado en la realización de tareas de detección, respuesta y protección.

Maria Pilar Torres, responsable de proyectos de cibersguridad en la compañía **Everis**, hizo un repaso del estado de la ciberseguridad en 2015, y aportó su punto de vista sobre los impedimentos que encuentran actualmente tanto la propia industria, como las empresas de servicios de seguridad para aplicar la cibersguridad en su presentación “**Barreras para un mejor avance en la protección de infraestructuras crítica**”.

La primera de las barreras encontradas ha sido que la formación y concienciación no obtenían los resultados esperados debido a su carácter demasiado teórico; por lo que se aconseja introducir más elementos prácticos, tales como los simulacros de crisis. Dentro del tema formativo, también se ha encontrado una carencia de conocimientos en los profesionales; y por ello se propone la creación de un nuevo esquema de certificaciones ICS/SCADA; y que el desarrollo de la documentación sea diferenciada por sectores industriales.

Por otro lado, dentro de la propia organización se echa en falta en muchas compañías el suficiente apoyo desde la dirección hacia el CISO (Chief Information Security Officer). Esta figura es el responsable de una gran cantidad de actividades como son la definición y seguimiento de las políticas de seguridad, del análisis y gestión de riesgos, del apoyo al plan estratégico de seguridad, del cumplimiento de las leyes LOPD y PIC, de la implantación del sistema de continuación del negocio. La ejecución adecuada de estas tareas tiene una consecuencia directa sobre los procesos de la organización, y sobre el servicio que proporciona; por lo que en algunos casos al CISO se le puede llegar a considerar como un superhombre.

Maria Pilar Torres propuso algunas prácticas para reforzar la ciberseguridad industrial como la contratación de ciberpólizas para manejar las crisis, las auditorías de seguridad, la creación de entornos virtualizados para la realización de pruebas o pentesting, el despliegue de honey-pots, y el empleo de herramientas de simulación como Tacit.

Estado Actual del Estándar ISA 99 (IEC-62443), es el título de la presentación que **Ragnar Schierholz, de ABB y Hector Puyosa, profesor de la Universidad Politécnica de Cartagena** en la que destaca el estándar ISA 99, dentro de las normativas o guías de buenas prácticas de seguridad en la automatización industrial,. Aunque de origen norteamericano, esta normativa está cada vez más introducida en Europa; siendo el capítulo español de la organización ISA uno de los más activos. En España disponen de un amplio calendario de actividades; en las que predominan la impartición de cursos y la celebración de reuniones técnicas.

Héctor Puyosa y Ragnar Schierholz hicieron una presentación de la organización ISA, y repasaron los principales conceptos de la norma, tales como la gestión del ciclo de vida de la seguridad, y la

segmentación de sistemas mediante la creación de zonas de seguridad y conductos (Security zone y Conduits). Igualmente destacaron los documentos en los que han estado trabajando este año 2015; en concreto el 62443-2-3 sobre gestión de actualizaciones de seguridad, y el 62443-2-4 a cerca de las certificaciones de los proveedores de productos de seguridad.

Marc Blackmer, de la multinacional Cisco, describió cómo las soluciones de seguridad de su compañía siguen la normativa IEC-62443 en la ponencia titulada "**IEC-62443 en el mundo real**".

El representante de Cisco habló del ciclo de vida de la seguridad en el desarrollo de los productos de acuerdo con el IEC-62443-4-1, y del cumplimiento de los niveles de seguridad según IEC-62443-3-3, conseguidos mediante la colaboración de sus soluciones de seguridad de red, seguridad de contenidos, y seguridad de acceso.

Las soluciones y servicios de Cisco han sido desarrolladas para las necesidades verticales específicas, destacando el desarrollo de soluciones para el ámbito IoT vertical.

¿Están las tecnologías de ciberseguridad de hoy preparadas para proteger los SCI del futuro?, fue el título de la mesa debate que José Valiente y en la que participaron los representantes de Ioactive, Everis, Cisco y GMV.

En la mesa de debate se habló de la problemática de la seguridad de las nuevas tecnologías del Smart OT, término acuñado por el Centro de Ciberseguridad Industrial; y que se refiere al conjunto de tecnologías de operación inteligentes que integran la información, la interoperabilidad y la conectividad como principales caracterísitcas.

La primera consideración que se hizo sobre este nuevo campo dentro de la ciberseguridad industrial, es el gran tamaño de su superficie de exposición en Internet, y por tanto susceptible de ser atacada.

Entre las posibles amenazas se destacaron como principales la denegación de servicio, y el fraude sobre todo en las Smart Grids. Y como medidas más relevantes se apuntaron las auditorías periódicas por empresas autorizadas, la incorporación de la seguridad en el diseño y desarrollo de los productos, la monitorización, y la concienciación.

Por último, a la pregunta de cuáles serían los principales requisitos a seguir en una hoja de ruta, los participantes del debate eligieron los siguientes conceptos, y en este orden: escalabilidad, previsión de incidentes, inversión, conocimiento compartido, colaboración público-privada, y detección.

La multinacional Eulen, líder en España de servicios generales, presentó su visión sobre la ciberseguridad industrial a través del su director de consultoría **Ricardo Cañizares en Eulen Seguridad** con la ponencia titulada **“La monitorización un requisito imprescindible en la Ciberseguridad Industria”**.

En Eulen Seguridad tiene un lema “Si algo sucede en su empresa, lo sabremos antes que nadie”. Con este objetivo, la pieza clave de su servicio es la monitorización continúa de la seguridad. Su plan de protección específica se basa en la monitorización, supervisión y evaluación de los activos físicos, y de los sistemas de operación. Y para ello, los procedimientos que utilizan persiguen la búsqueda de patrones de comportamiento para la detección de anomalías.

El servicio de Eulen está orientado a la detección, y resolución de incidentes más que a la prevención de los mismos. El ciclo del servicio se desarrolla en tres fases: captura, detección y análisis; mediante las cuales se recolecta información, se identifican incidencias, se generan alertas, se analizan y se resuelven.

Ricardo Cañizares hizo hincapié en la importancia de las técnicas de inteligencia para conocer cómo se comportan los atacantes y así mitigar su impacto sobre los sistemas. Y en el turno de preguntas expresó su opinión a cerca de cómo ve en la actualidad el estado de la ciberseguridad. Dijo que la mayor diferencia con el pasado es que ahora existe legislación como la LOPD, y la PIC; y propuso la creación de una nueva ley específica para el entorno industrial que obligue a las organizaciones a cumplir un conjunto mínimo de medidas de seguridad.

La ética como elemento clave en la ciberseguridad, fue una exposición diferente, a cargo de **Federico Sauter de la empresa Innominate, Phoenix Contact**. La ponencia no estuvo basada en los aspectos técnicos de la ciberseguridad, sino que trató el tema desde el punto de vista humano, es decir, de cómo las personas se enfrentan en su día a día a las actividades de la cibersguridad.

Un ejemplo donde se puede aplicar la ética es en las campañas de concienciación de seguridad dentro de la plantilla de trabajadores. En este sentido se recomienda que los directivos den ejemplo del cumplimiento de las medidas de seguridad; y así mediante la emulación de sus jefes, los empleados incorporen más rápidamente estas medidas

Otro aspecto donde se aplica la ética, aunque muchas veces sin ser consciente de ello, es en la gestión de vulnerabilidades. Cuando un técnico encuentra una nueva vulnerabilidad en alguna pieza de software, podría actuar de distintas formas. La primera es comunicárselo inmediatamente al fabricante; la segunda posibilidad es hacer pública la vulnerabilidad para que la conozca toda la comunidad; y la última sería crear un malware que aproveche esa vulnerabilidad y o bien publicarlo, o bien venderlo. De todas

estas opciones, la forma que se considera ética para gestionar las vulnerabilidades es comunicárselo urgentemente a la compañía responsable, y darles un plazo de 5 días para que puedan crear una actualización de seguridad; a partir del cual la vulnerabilidad se publicaría. De esta forma se evita que los cibercriminales creen malware con este fallo, y se multipliquen los ataques.

En definitiva Federico quiso transmitir que para la toma de decisiones en ciberseguridad deberíamos aplicar la ética más allá de la normativa. Y en mi opinión, sobre todo porque esta última está aún en los inicios de su desarrollo.

Jose Luis Díaz y Alberto Domínguez, **consultores del área Security en Everis han presentado "TACIT - Herramienta de Simulación de ciberataques en SmartGrids"** un proyecto CIP de 18 meses, en el que participan dentro del consorcio D'Appolonia, Everis, Tecnalia y CCI.

José Luis Díaz comenzó su presentación exponiendo que tipos de ataques existen en Smart Grid y cuales son las prioridades identificadas, en base a las cuales se han establecido los objetivos de la herramienta de simulación, la cual permita establecer las mejores prácticas, desarrollando para ello una metodología de simulación totalmente basada en estándares.

La segunda parte de la exposición estuvo a cargo de Alberto Domínguez, que presentó de forma detallada los componentes de la herramienta y el proceso para realizar la simulación.

"Seguridad en Ambientes de Control Industrial: Sector Eléctrico. Desde la Experiencia en Colombia" un título contundente, para una presentación excelente a cargo de Diego Zuluaga, CISO de ISAGEN. La presentación comenzaba con un rótulo que indicaba textualmente "Las opiniones presentadas en esta conferencia, son personales y NO comprometen, ni reflejan las posiciones de la empresa para la cual trabaja el presentador", lo cual, dice mucho de la responsabilidad de Diego Zuluaga con su compañía y cumple con las expectativas de este congreso, que consisten, en recoger las experiencias y opiniones personales de los ponentes. Su presentación continuaba con un interesante repaso de diversos estudios que presentaban la situación en Latinoamérica, y que permitió contextualizar la situación.

Diego Zuluaga también hizo un repaso a los principales malware, como Stuxet, Duqu, Flame, y ataques al sector energético de los últimos años e incidentes de la base de datos RISI para concluir como hemos pasado de la seguridad por oscuridad antes a la

seguridad por diseño hoy.

Presentó de forma didáctica la anatomía de un ataque y como basar nuestra protección en la adaptación de estándares y destacando cinco medidas clave:

- Políticas de seguridad específicas
- Bloquear el acceso a recursos mediante filtrado
- Detectar la actividad maliciosa
- Mitigar donde no es posible controlar
- Arreglar los problemas centrales.

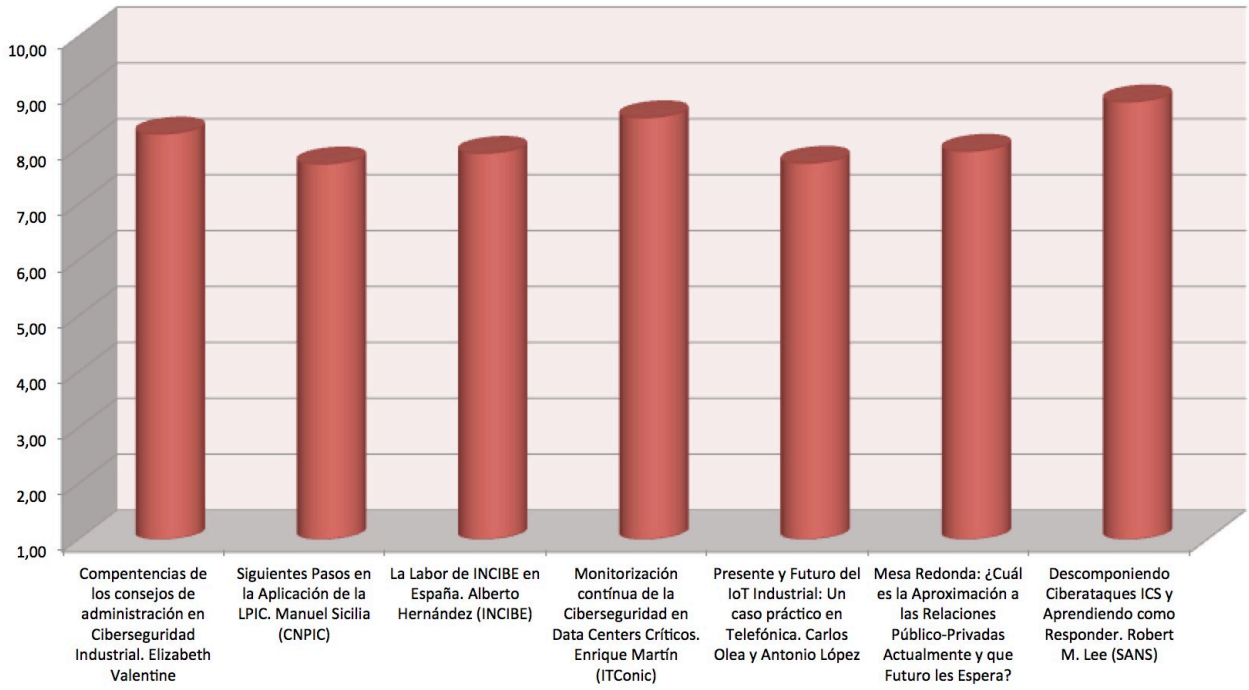
Samuel Linares, Coordinador del CCI en Medio Oriente, cerró la segunda jornada del congreso con una presentación sobre la realidad en Estados Unidos, Europa y Oriente Medio a la hora de afrontar la Ciberseguridad Industrial. Donde presento las similitudes, mismos actores, mismas normas, mismas tecnologías y las diferencias, diferente cultura, diferente motivaciones y diferentes recursos.

Concluyo que debemos inyectar la ciberseguridad en todas las fases del ciclo de vida del proyecto de automatización, establecer un modelo de gobierno de ciberseguridad industrial y la existencia de un actor con un rol independiente.

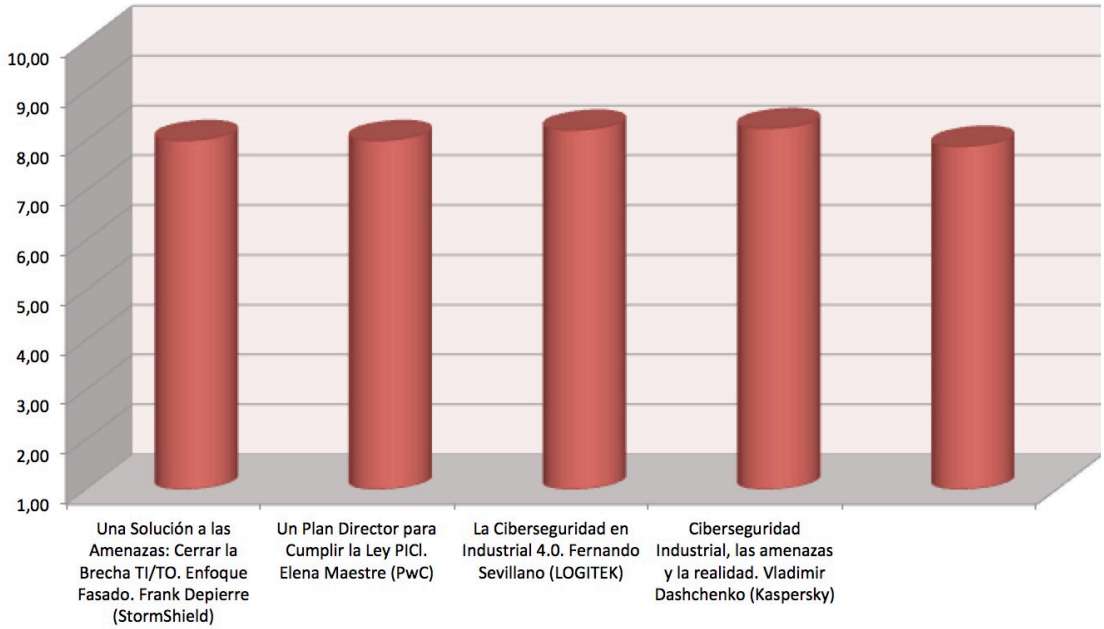
Valoraciones del Congreso

La valoración de las sesiones y de los contenidos de la jornada del 6 de octubre ha sido muy buena, con una valoración media de un **8,1**.

Sesión de Mañana

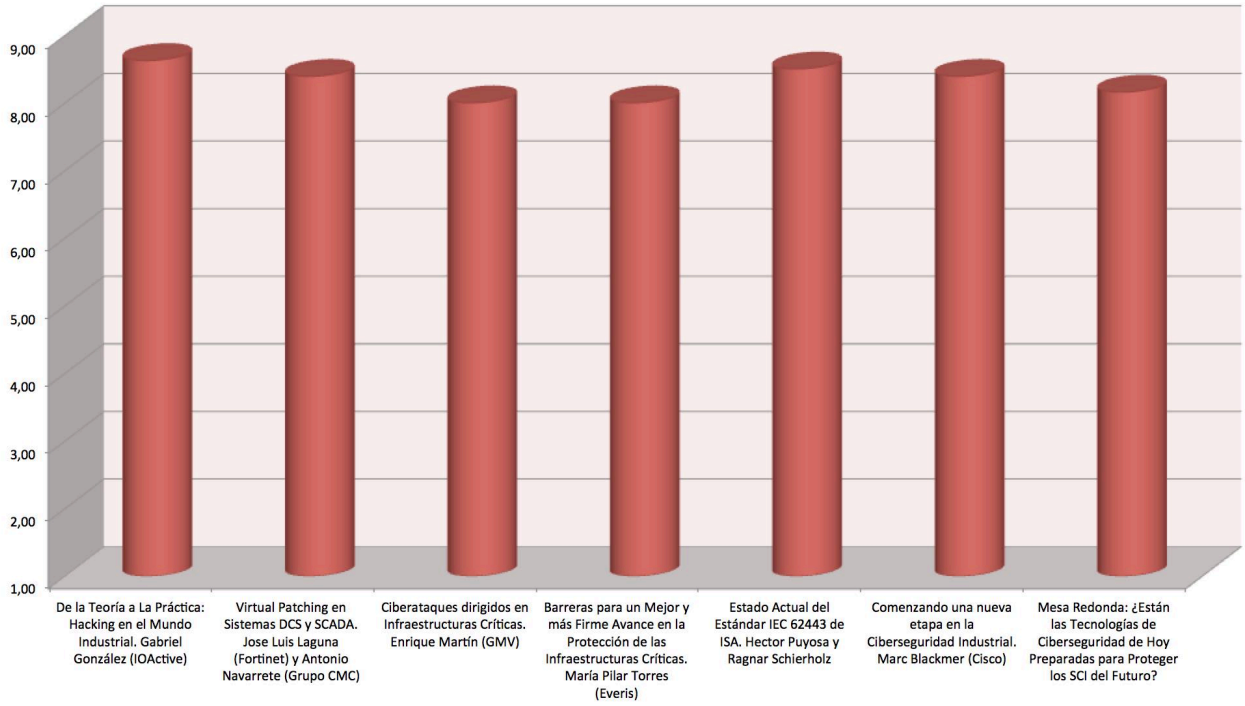


Sesión de Tarde

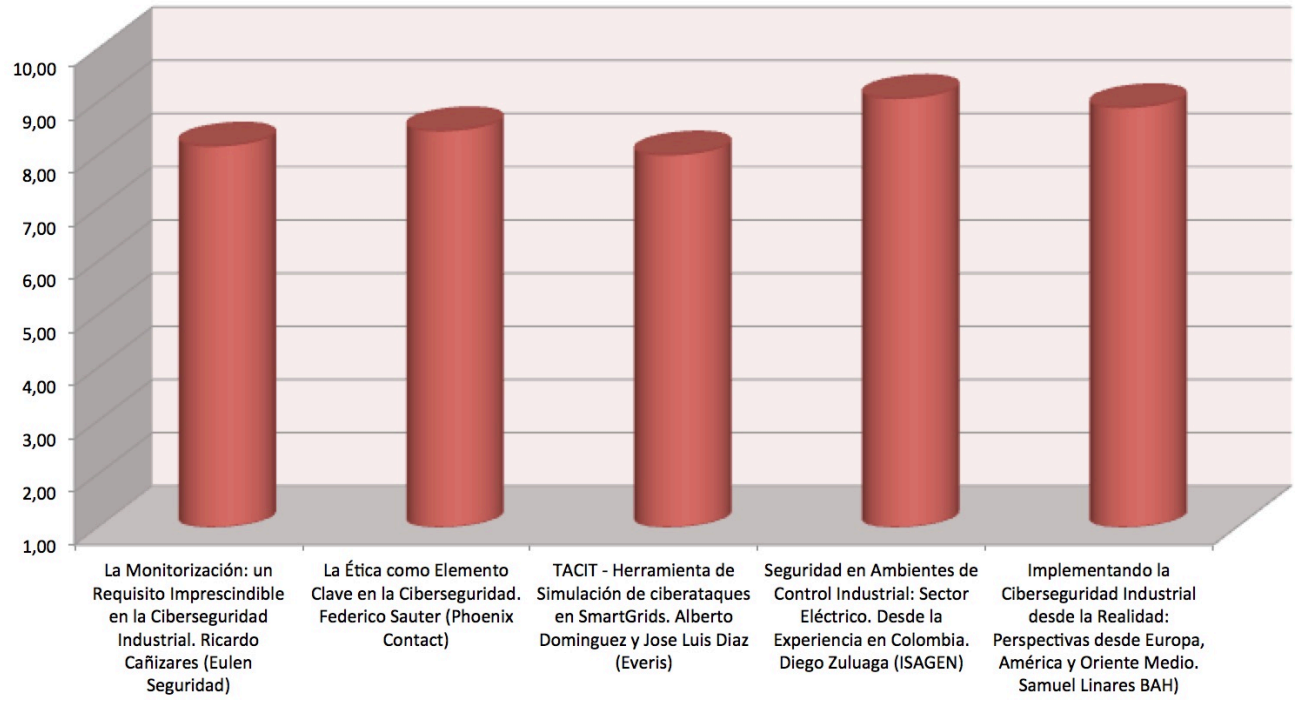


La valoración de las sesiones y de los contenidos de la jornada del 7 de octubre ha sido igual de buena, con una valoración media de un **8,4**.

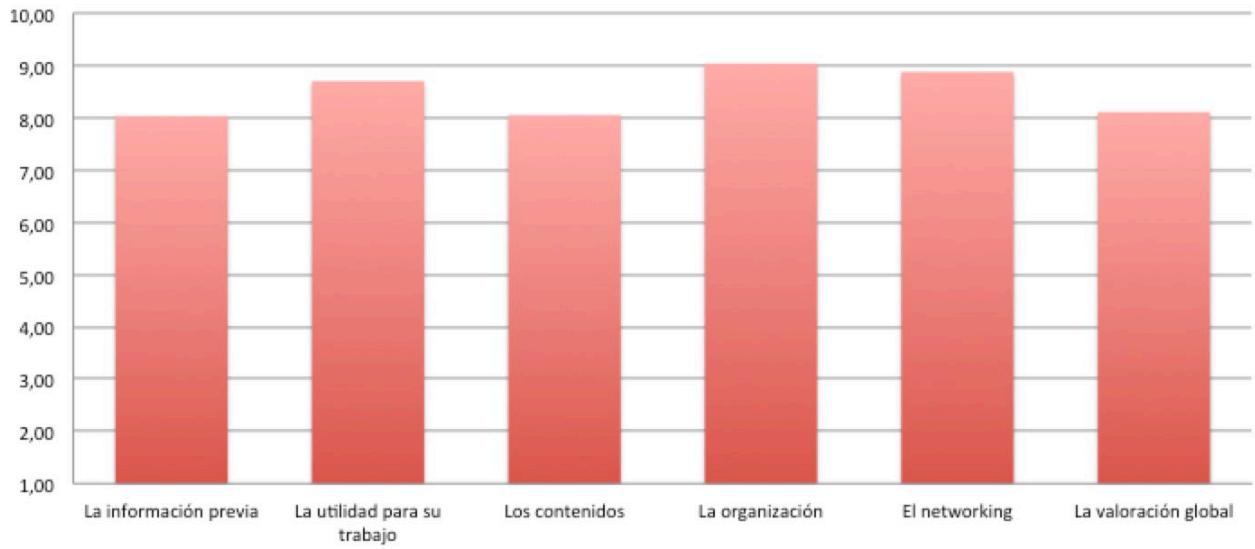
Sesión de Mañana



Sesión de Tarde



La valoración general del V Congreso Internacional ha sido de un **8,47** de media. A continuación mostramos la valoración de los asistentes:



Muchas gracias a todos por apoyar y confiar en el Centro de Ciberseguridad Industrial, y especialmente a Ana González Monzón que ha elaborado dos artículos sobre el congreso en los que están basadas algunas partes del desarrollo del mismo.

Muchas gracias a los patrocinadores del Congreso: