II Congreso Iberoamericano de Ciberseguridad Industrial

27 y 28 de Mayo, 2014
Hotel Dann Carlton, Bogotá (Colombia)

Centro de Ciberseguridad Industrial

www.cci-es.org

Introducción

Tras el éxito del Primer Congreso Iberoamericano de Ciberseguridad Industrial celebrado en Madrid (España) los pasados 2 y 3 de Octubre de 2013, donde se dieron cita casi 200 asistentes de la industria, y tras haberse convertido por ello, y por la calidad de sus contenidos y ponentes en el congreso internacional más relevante sobre la temática del año 2013, como parte de su actividad, el Centro de Ciberseguridad Industrial (CCI) organiza el II Congreso Iberoamericano de Ciberseguridad Industrial, como evento de referencia para el mercado hispanohablante y como punto de encuentro de intercambio de conocimiento, experiencias y relaciones de todos los actores involucrados en este ámbito.

Este segundo evento se celebrará en el Hotel Dann Carlton de **Bogotá (Colombia) los próximos 27 y 28 de Mayo** y alrededor del mismo se organizarán una serie de **talleres pre y post congreso** que complementarán las temáticas abordadas en el mismo.

Durante el evento se contarán con ponentes internacionales de primer nivel que repasarán el estado y experiencias desarrolladas en todo el mundo, desde Estados Unidos, pasando por Europa, Latinoamérica, Oriente Medio o Japón, entre otros. Estarán representados todos los actores. Fabricantes industriales, de ciberseguridad, ingenierías, consultoras, integradores, usuarios finales o infraestructuras críticas se darán cita en Bogotá para discutir sus distintas percepciones de la realidad que hoy en día es la Ciberseguridad Industrial.

El Congreso es la mejor oportunidad para conocer el estado del arte de esta disciplina de la mano de los líderes internacionales en cada uno de sus ámbitos y de establecer valiosas relaciones que favorezcan la colaboración en distintos ámbitos a nivel nacional e internacional.

Durante el congreso se contará con servicio de traducción simultánea y todos los contenidos del congreso serán accesibles posteriormente a través de grabaciones exclusivas para los asistentes.

Programa Mayo 2014

27 de Mayo: El Congreso

Hora	Descripción	Ponente
8:00 a 8:45h	Acreditaciones	
08:45h a 09:00h	Bienvenida y Presentación Congreso	Samuel Linares (Director, Centro de Ciberseguridad Industrial), Leonardo Huertas (Coordinador CCI Colombia, CSA Eleven Paths)
09:00h a 09:35h	Estado de la Ciberseguridad Industrial en España: el CCI  Samuel Linares es el Director del Centro de Ciberseguridad Industrial, Experto Evaluador de la Comisión Europea, ENISA (European Network and Information Security Agency), Experto CIIP y miembro de la Task Force de Ciberseguridad de ISACA. Con casi 2 décadas de experiencia en seguridad, integración de sistemas y gestión proyectos multinacionales y multiculturales, ha sido el principal impulsor del concepto "Ciberseguridad Industrial" en español, lo que le ha llevado a ser reconocido como uno de los mayores expertos iberoamericanos en este ámbito y a participar como ponente, chairman y profesor en numerosos eventos en todo el mundo (España, Reino Unido, Estados Unidos, Bélgica, Qatar, Emiratos Árabes Unidos, México, Cuba o Argentina, entre otros). Samuel cuenta en su haber con numerosas certificaciones en el ámbito de la ciberseguridad, como GICSP (Global Industrial Cyber Security Professional), CRISC (Certified in Risk and Information Systems Control), CGEIT (Certified in Governance of Enterprise IT), CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), GIAC Assessing Wireless Networks (GAWN), Systems and Network Auditor (GSNA) y Google Hacking & Defense (SSP-GHD), BSI BS 25999 Lead Auditor & BS 7799 Lead Auditor (desde 2002), además de otras específicas de distintos fabricantes el mercado. Es Ingeniero Técnico en Informática por la Universidad de Oviedo y Experto Universitario en Protección de Datos por el Real Centro Universitario Escorial Maria Cristina.	Samuel Linares (Director, Centro de Ciberseguridad Industrial)
09:35h a 10:25h	La Ciberseguridad Industrial en Latinoamérica: un recorrido por algunos países  Claudio Caracciolo  Leonardo Huertas  Marcelo Branquinho	Claudio Caracciolo (Coordinador CCI Argentina, CSA Eleven Paths), Leonardo Huertas (Coordinador CCI Colombia, CSA Eleven Paths) , Marcelo Branquinho (Coordinador CCI Brasil, TI Safe)

10:25h a 11:00h	**Tomando Prestada la Seguridad del Departamento de Operaciones**  Patrick Miller ha dedicado su carrera a la protección y defensa de infraestructuras críticas como reconocido consultor independiente. Es Socio Gerente en The Anfield Group, así como fundador, director y presidente emérito de EnergySec, una organización 501(c)(3) sin ánimo de lucro que se dedica a compartir información, concienciar sobre la situación y el desarrollo del personal de seguridad. Su amplia experiencia en diversos campos incluye puestos en agencias reguladoras, consultorías privadas, así como organizaciones en los sectores de Servicios de la Energía, las Telecomunicaciones y Financieros.	Patrick Miller (Presidente Emérito de EnergySec)
11:00h a 11:30h	**Café/Networking**	
11:30h a 12:15h	**La Aproximación Práctica a la Protección de Infraestructuras Críticas de las Ciber-Amenazas Emergentes**  Ayman tiene más de 20 años de experiencia en campos como la Automatización, las Tecnologías de la Información y la Ciberseguridad. Es licenciado en Ingeniería Electrónica y conoce a fondo segmentos como los sistemas de control industriales, la ingeniería de sistemas, elaborar y construir estrategias, diseños y modelos de ciberseguridad. Ayman tiene amplia experiencia en la protección de infraestructuras críticas, colabora en la ISA99/IEC62443 y es co-presidente del Grupo de Trabajo 1. Actualmente,es el Chief Technology Advisor del CCI en Oriente Meido y Asia y es miembro activo de múltiples consejos de Ciberseguridad en varias de las mejores universidades del mundo en temas relacionados con la mejora de la ciberseguridad industrial. Asimismo, es miembro activo de varias Alianzas para la Innovación en Seguridad que trabajan en un programa mundial para mejorar la seguridad de sistemas de control industriales, en estrecha colaboración con los principales fabricantes de seguridad de TI y los principales fabricantes de systemas de automatización industrial y de control. Consciente de que las medidas de seguridad siempre van por detrás de los riesgos cibernéticos que emergen, ha desarrollado un modelo de "defensa-en-profundidad" de SCI de ciberseguridad industrial que pretende la detección temprana de amenazas, basado en la seguridad a través de la visión y la integración.	Ayman Al-Issa (Digital Oilfields Cybersecurity Advisor, ADMA-OPCO)
12:15h a 12:45h	**Las Ciber-actividades del Control Systems Security Center para Infraestructuras Sociales en Japón**  Desde 1970, es Licenciado en Ciencias Aplicadas por la Universidad de Waseda y Doctor en Físicas desde 1972 por el Instituto Tecnológico de Tokio. Actualmente es Vicepresidene de Control System Security Center (CSSC) desde Hitachi, Ltd. y la Information Technology Promotion Agency (IPA) de Japón. Trabajaba en el campo de la seguridad y las redes.	Hideaki Kobayashi (VicePresidente, Control Systems Security Center, Japón)
12:45h a 13:45h	**Almuerzo**	
13:45h a 14:20h	**La Ciberseguridad Industrial en el Sector Eléctrico de Colombia**  Ingeniero de Sistemas, Executive MBA. Certificado internacionalmente en gestión y riesgos de TIC, seguridad en información y de sistemas de control industrial (CISM, CRISC, CGEIT, GICSP, ISO 27001 L.A.). Responsable de seguridad en información en ISAGEN, Lidera el grupo de expertos en ciberseguridad del Consejo Nacional de Operación del sector eléctrico colombiano, Con más de 15 años de experiencia en seguridad de información ha sido entre otros, consultor internacional con KPMG para empresas del sector público y privado, conferencista en múltiples escenarios nacionales e internacionales, ha dictado cátedra de pregrado, postgrado en universidades públicas y privadas y aporta en diferentes escenarios a mejorar la ciberseguridad de las infraestructuras críticas nacionales. Fue Galardonado con el premio “Americas Information Security Leadership Awards” de (ISC)², destacado como Joven Sobresaliente de Antioquia y de Colombia por la Cámara Junior Internacional en el Programa Ten Outstanding Young Persons y condecorado con el distintivo de inteligencia de la Policía Nacional de Colombia.	Diego Zuluaga (Responsable de Seguridad en Información, ISAGEN)

14:20h a 15:05h	**Mesa Redonda: La Perspectiva Internacional**  Patrick Miller  Ayman Al-Issa  Hideaki Kobayashi  Diego Zuluaga  Moderador: Samuel Linares	Patrick Miller (EnergySec), Ayman Al-Issa (ADMA-OPCO), Hideaki Kobayashi (CSSC), Diego Zuluaga (ISAGEN). Modera: Samuel Linares (CCI)
15:05h a 15:40h	**SEC4SCADA: Testbed de Ciberseguridad Industrial, Smart Grid y Centro de Desarrollo de Productos**  Iñaki Eguia es investigador en cibersegruidad industrial dentro del área de negocio de IT Competitiveness en la división ICT-European Software Institute de Tecnalia. Ha participado en varios proyectos europeos relacionados con la seguridad y la heterogeneidad de redes. Es miembro de la plataforma tecnológica PESI (Seguridad Industrial) considerado como experto por ésta para asesorí, y miembro de la Plataforma NIS recientemente constituida sobre ciberseguridad en Europa y Artemis (Plataforma Tecnológica Europea de Sistemas Embebidos). Como líder el grupo de seguridad, establece la estrategia y la despliega, con el fin último de desarrollar activos tecnológicos que impacten en mercado y en la sociedad. Iñaki es también coordinador del proyecto europeo ARCADIA (www.arcadia-project.eu) para la elaboración de una hoja de ruta en el área de sistemas embebidos y el proyecto RISC (convergencia de seguridad física y lógica en Infraestructuras Críticas). Actualmente estudia para realizar un doctorado sobre gestión de la innovación en la Escuela de Ingenieros industriales y Telecomunicaciones en Bilbao. Obtuvo su doble ingeniería de Informática y Organización Industrial en la Universidad de Deusto y Lund.  Arkaitz Gamino es investigador en cibersegruidad industrial dentro del área de negocio de IT Competitiveness en la división ICT-European Software Institute de TECNALIA. Ha participado en diferentes proyectos europeos relacionados con la ciberseguridad industrial, convergencia entre los sistemas físicos y lógicos, seguridad web y sistemas embebidos. Por otro lado, ha participado en numerosos proyectos en el ámbito de la seguridad IT y certificación de normativas de seguridad; LOPD (Ley Órganica de Protección de Datos) y legislación que regula los sistemas de juego on-line y presencial. Estudio Ingeniería Informática y realizó el Master en Seguridad de la Información en la Universidad de Deusto.	Iñaki Eguía , Arkaitz Gamino (Tecnalia)
15:40h a 16:00h	**15 in 15: 15 Ciberincidentes reales en 15 minutos**  Bryan Owen es gerente de ciberseguridad de OSIsoft LLC (www.osisoft.com) - una compañía de San Leandro, EE.UU. que fabrica sistemas para la monitorización de información en tiempo real, principalmente de instalaciones industriales pesadas. Bryan fue pionero en el uso de sistemas de información de planta durante su etapa como ingeniero de sistemas de control en 1985. Desde entonces, OSIsoft ha crecido hasta convertirse en una multinacional de altos rendimientos con actividades en 110 países. Tiene más de 1.200 empleados en todo el mundo de los cuales unos 400 trabajan en San Leandro. La carrera de Bryan en OSIsoft empezó oficialmente en 1996 como ingeniero de aplicaciones de campo, viajando mucho para encargarse de proyectos de monitorización remota e instalar sistemas de apoyo para la toma de decisiones en tiempo real. Esto era 'big data' para la industria antes de que este término formara parte de la tecnología ordinaria. Más adelante, Bryan fue el encargado de gestionar los servicios de ingeniería de OSIsoft para la zona de Oceanía, antes de volver a los EE.UU. para centrarse en la ciberseguridad en la era posterior a los atentados del 11 de	Bryan Owen (OSISoft, Cybersecurity Manager)

	septiembre. OSIsoft empezó a investigar la ciberseguridad industrial junto con Idaho National Lab (INL) en 2005 bajo el liderazgo de Bryan con evaluaciones de productos y una intensa actividad formativa. Así mismo, aprovechando la estrecha colaboración con Microsoft para ayudar a arrancar los procesos y prácticas formales de ciclo de vida de desarrollo de seguridad (SDL) en OSIsoft. Bryan está acreditado por Microsoft y es Ingeniero Profesional por el Estado de Washington, y tiene una licenciatura en Ingeniería Química por la universidad de Oregon (1981). Las actividades de divulgación en las que Bryan está involucrado incluyen ser miembro del Comité de Ciberseguridad de los American Fuel & Petrochemical Manufacturers, el Grupo de Trabajo Conjunto de Sistemas de Control Industriales del Departamento de Seguridad Nacional de los EE.UU., y diversos equipos de normas de la Sociedad Internacional de Automatización (ISA). Bryan es activo en las redes sociales y publica un blog sobre la seguridad del sistema PI para la comunidad de OSIsoft.	
16:00h a 16:30h	**Café/Networking**	
16:30h a 17:05h	**Sistemas de Seguridad y Protección Nacidos para el Mundo Industrial - Cuidando la Seguridad en la Convergencia de Redes Corporativas y SCADA**  Ha estado dedicado a Seguridad de la Información por más de 12 años. Durante este tiempo ha estado pasado por departamentos de soporte, ingeniería, servicios, pre-venta y post-venta habiendo adquirido certificaciones en varias tecnologías y fabricantes. Posée un título de Licenciado en Sistemas de Información y es estudiante de post-grado de Criptografía y Seguridad en Comunicaciones en el Instituto de Enseñanza Superior del Ejército Argentino (IESE). Actualmente desempeña la función de Gerente de Ingeniería para Sud-América en Fortinet.	Marcelo Mayorga (Gerente de Ingeniería de Sistemas Sudamérica, Fortinet)
17:05h a 18:00h	**Mesa Redonda: Aprendiendo de los Incidentes de Ciberseguridad en el Mundo Industrial**  Bryan Owen  Marcelo Mayorga  Arkaitz Gamino  Robin Salcedo  Moderador: José Valiente	Bryan Owen (OSISoft), Marcelo Mayorga (Fortinet), Arkaitz Gamino (Tecnalia), Robin Salcedo (CEO, Identian) Modera: José Valiente (CCI)
18:00h a 18:15h	**Conclusiones Primer Día y Cierre Jornada**  José Valiente es el Responsable de Coordinación y Comunicación del Centro de Ciberseguridad Industria. Diplomado en Informática de Gestión por la Universidad Pontificia de Comillas, es Especialista en Consultoría Tecnológica y de Seguridad. Con más de 20 años de experiencia trabajando en Consultoras como Davinci Consulting y Tecnocom en proyectos de Seguridad y TI para Gran Cuenta y Administración Pública. Cuenta con múltiples certificaciones de soluciones de fabricantes de seguridad y TI (Cisco CCNA y CCDA, System Security Mcafee, Security Specialist Juniper, Websense Certified Enginer, F5 Bigip Specialist y Radware certified security Specialist) y certificación CISM de ISACA. José es experto en la dirección de proyectos para gran cuenta y administración pública. Ha dirigido proyectos de implantación de SGSIs en compañías del IBEX 35 y administración pública, con equipos de trabajo de alta capacitación en seguridad y cuenta con amplios conocimientos en ITIL y PMI, impartiendo formación a empresas del sector industrial, financiero y administración pública.	José Valiente
18:15h a 20:00h	**Tiempo Libre**	
20:00h a 23:30h	**Cocktail/Party/Fiesta**	

28 de Mayo: El Congreso

Hora	Descripción	Ponente
8:00 a 9:00h	Acreditaciones	
09:00h a 09:15h	Bienvenida y Presentación Jornada	José Valiente (Coordinación y Comunicación, CCI)
09:15h a 09:45h	Ciberlavado de activos: Un riesgo para la seguridad de las infraestructuras críticas  Luis es abogado de la Universidad de los Andes, con especialización en Economía de la misma Universidad y en Derecho Administrativo de la Universidad del Rosario. Se ha desempeñado en varios cargos tanto dentro del sector público como en el privado, como en el Departamento Nacional de Planeación. También, como Gerente de Suárez & Asociados desarrolló actividades de asesoría, consultoría y litigio en temas relacionados con Derecho económico, constitucional y administrativo. Así mismo, ha sido profesor y conferencista de temas de Derecho Económico en la Universidad de los Andes y la Universidad Javeriana. Actualmente es profesor de la Maestría en Derecho con énfasis en Derecho Bancario y Bursátil de la Universidad Externado de Colombia. Luis asumió la Dirección General de la Unidad de Información y Análisis Financiero - UIAF en noviembre de 2010, donde inspiró y lideró la ejecución de la construcción e implementación de un nuevo enfoque basado en la innovación para combatir el lavado de activos y la financiación del terrorismo, con base en el cual se han obtenido resultados sin precedentes a nivel nacional y global. Bajo su liderazgo obtuvo para Colombia el premio BECA (Premio al mejor caso Egmont) como reconocimiento al mejor caso de inteligencia financiera del mundo en el año 2013-2014. Asimismo, ejerce la Secretaría Técnica de la Comisión de Coordinación Interinstitucional para el Control del Lavado de Activos de Colombia - CCICLA, y ejerce como representante por Colombia, ante el Grupo de Acción Financiera para Suramérica – GAFISUD, siendo elegido como Presidente del Grupo para el año 2014.	Luis Edmundo Suárez Soto (Director, Unidad de Información y Análisis Financiero UIAF)
09:45h a 10:15h	Experiencias en Ciberseguridad Industrial  Egresado de la UTFSM en Chile, consultor con 20 años de experiencia en tecnológica de la información con fuerte background en seguridad informática, prevención de fraudes, respuesta de incidente y análisis forense. Ha analizado, diseñado e implantado soluciones, procedimientos y mecanismos enfocados en mitigación del riesgo informático para sector financiero, telecomunicaciones y gobierno en Mexico, Europa y Latinoamérica. Siendo destacado creador de "Planes de Seguridad" para mitigación de fraude en la industria de pago con tarjeta, cajeros automáticos y operaciones bancarias en línea, como innovadores sistemas de prevención de ataques de Cyberplagas y Cybercrimen ,que permiten la disminución efectiva de riesgos en la infraestructuras críticas e Industrial. Ha sido Director de Seguridad en varias consultoras, cuenta con varias certificaciones de la industria.	Alexis Hidalgo Donoso (CISO, PEMEX)
10:15h a 11:00h	Nuevos Planteamientos para Reducir la Brecha en la Seguridad en Entornos SCADA  Stephen es Arquitecto Consultor de Seguridad e Instructor de Seguridad para Cisco Security Business Group Inc. en la región de Latinoamérica. Entre sus proyectos, se incluyen el análisis, el diseño y la implementación de arquitecturas de seguridad informática y evaluaciones de seguridad en los sectores comercial, financiero, gobierno y SCADA. Tiene más de 20 años de experiencia en tecnologías de la información, y desde hace 15 está especializado en	Stephen Fallas (Arquitecto Consultor de Seguridad/ Instructor de Seguridad LATAM , Cisco - Sourcefire)

	seguridad informática. Ha trabajado conjuntamente con clientes y gestionando la relación entre ellos y el equipo de prestación de servicios de ISS, como PSS y MSS. Stephen tiene un sólido perfil en administración de sistemas y redes y en el desarrollo de aplicaciones, y tiene una profunda experiencia en diseñar e implementar redes seguras. También tiene amplia experiencia en gestión de la seguridad, creando e implementando políticas de seguridad, programas de análisis de riesgos e infraestructuras de seguridad. Ha llevado a cabo numerosos análisis de riesgos de información y pruebas de penetración para distintos clientes financieros y civiles.	
11:00h a 11:30h	**Café/Networking**	
11:30h a 12:10h	**La Ciberseguridad Industrial en las Industrial del Petróleo y Gas: Un Caso Real** **Johanna Orjuela.** Actualmente, Johanna se desempeña como Coordinadora de Mantenimiento SCADA de la Vicepresidencia de Transporte y Logistica de Ecopetrol. Ha trabajado desde 2006 en el desarrollo de Seguridad de la Información en Sistemas de Control Industrial en la empresa logrando generar lineamientos corporativos y específicos para la vicepresidencia en el cual trabaja, así como un plan operativo y táctico para implementar y sostener los mismos en el tiempo. La ingeniera Orjuela es graduada de la facultad de Ingeniería Electrónica de la Pontificia Universidad Javeriana de Bogotá y cuenta con una maestría en ingeniería Electrónica de la misma universidad gradada con honores con grado Magna Cum Laude. Adicionalmente, cuenta con una certificación internacional como profesional SCADA y es profesional certificada PMP. **Paulo Orozco.** Actualmente, Paulo se desempeña como Profesional de Seguridad de la información y telecomunicaciones en sistemas de control industrial para la Vicepresidencia de Transporte (VIT) de ECOPETROL. Es Ingeniero electrónico, especialista en automática e informática industrial y certificado como SCADA Security Architect. Desde 2010 es el responsable del programa de seguridad de la información en sistemas de control de la VIT definiendo y asegurando el cumplimiento de lineamientos para los sistemas de control y la implementación de controles bajo estándares internacionales. Además de la implementación del programa de seguridad, es responsable del aseguramiento de la arquitectura de comunicaciones en los sistemas de control bajo el principio de defensa en profundidad.	Johanna Orjuela Parra (Coordinadora Mtto. SCADA y Aplicaciones Avanzadas) Paulo Orozco Torres (Profesional de SI y Telecomunicaciones en Sistemas de Control) Ecopetrol.
12:10h a 13:00h	**Mesa Redonda: El Impacto de la Ciberseguridad Industrial en nuestra Sociedad**  José Valiente  Stephen Fallas  Luis E. Soto Johanna Orjuela  Moderador: Claudio Caracciolo	José Valiente (CCI), Stephen Fallas (Cisco-Sourcefire), Luis Edmundo Suárez Soto (UIAF), Johanna Orjuela (Ecopetrol). Moderador: Claudio Caracciolo
13:00h a 14:00h	**Almuerzo**	

14:00h a 14:30h — **Ciber-Amenazas Industriales y Tendencias** — Andrey Nikishin (Director de Proyectos Especiales - Tecnologías del Futuro, Kaspersky Lab)

En una carrera que se remonta a los primeros días de Kaspersky Lab, Andrey ha trabajado como Ingeniero Sénior y Arquitecto de Software antes de cambiar al Departamento de Marketing Estratégico como Director de Estratégia de Producto. Antes de su rol actual, Andrey lideró el Cloud and Content Technologies Research and Development Department. Antes de unirse a Kaspersky Lab, Andrey tenía ya varios años de experiencia desarrollando sus propios programas de antivirus.
Andrey es licenciado por la Baltic State Technical University en St. Petersburgo y recibió su MBA por la London Business School.

14:30h a 15:00h — **Hacia la Detección Temprana de Amenazas Avanzadas en el Mundo Industrial** — María Pilar Torres Bruna (Gerente de proyectos de ciberseguridad, EVERIS)

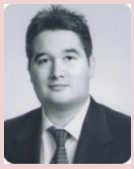
María Pilar es actualmente la Gerente responsable de proyectos de ciberseguridad en everis Aeroespacial y Defensa. A punto de cumplir 11 años en el grupo everis, cuenta con amplia experiencia en grandes proyectos de IT. Pasó 5 años en el área de sector público en España, 3 en Sector Público en la oficina de everis México y finalmente, hace 3 años asumió la responsabilidad de desarrollar el área de seguridad en everis Aeroespacial y Defensa apalancándose en servicios que ya da el grupo everis y en pequeñas y medianas compañías de nicho. Actualmente ya ha ejecutado proyectos relacionados con planes directores de seguridad en los ámbitos español y europeo y está impulsando proyectos en la compañía de protección contra el malware; privacidad en datos personales; uso de simuladores de ciber ataques para el training en infraestructuras críticas; análisis de certificaciones necesarias para un director de seguridad en una infraestructura industrial; ciber seguridad en Smart Grids; monitorización de infraestructuras en las redes; Finalmente está participando en varios proyectos relativos a roadmaps de ciberseguridad con el objetivo de alimentar los principales programas de inversión en innovación en Europa.

15:00h a 15:30h — **Los Investigadores de Seguridad y el Mundo Industrial** — Rony Lerner (Vicepresidente de Ingeniería, Tripwire)

Rony, Bogotáno de nacimiento, es un ejecutivo veterano en la industria del software, con un historial probado en organizaciones de ingeniería de grandes y pequeñas empresas. Rony lidera el grupo de Investigación y Desarrollo de Tripwire. La technologia de Tripwire se especializa en conectar ciberseguridad con los negocios, y ofrece visibilidad en riesgos de seguridad, provee contexto empresarial e inteligencia de negocios, y le da a las empresas la seguridad de proteger los datos sensibles en contra de vulnerabilidades y amenazas, a través de su cartera de controles de seguridad de alta prioridad. Antes de unirse a Tripwire, Rony fue Vicepresidente de Investigación y Desarrollo de la Unidad Productos para Bases de Datos de Quest Software Inc. Él ha liderado organizaciones en más de 20 paises del mundo en cuatro continentes y lanzado más de 40 productos de gran éxito . Rony obtuvo su Licenciatura en Ciencias de la Computación en el Instituto de Tecnología de Israel en Haifa. Rony también sirvió ocho años en la Fuerza Aérea de Israel, donde recibió intensivo capacitación tecnica y para el liderazgo del oficial. Se retiró con el rango de Mayor.

15:30h a 16:00h — **Seguridad Física, Entrando a tu Empresa como en las Películas** — Jaime Andrés Restrepo (CEO , DragonJAR)

Jaime es Ingeniero en Sistemas y Telecomunicaciones de la Universidad de Manizales. CEH. Información Security Researcher con más de 10 años de experiencias en Ethical Hacking, Pen Testing, Análisis de Vulnerabilidades y Análisis Forense. Gerente de DragonJAR Soluciones y Seguridad Informática SAS, Co-Fundador del ACK Security Conference y Creador de La Comunidad DragonJAR, una de las comunidades de seguridad informática mas grandes de habla hispana y referente en el sector.
Ha sido Speaker en diferentes eventos de Seguridad (EKO Party en Argentina, iSummit en Ecuador, e-Security Guayaquil, OWASP Latam Tour, Campus Party Colombia y Mexico, 8.8 Security Conference en Chile, INFOTEK 2012 Perú, Ethical Hacker Conference Bolivia, GuadalajaraCON en Mexico, BSides PR en Puerto Rico, HubCON en Paraguay, CSI Security 2013, Encuentro Internacional de Seguridad informática, Congreso de Hacking Ético, SegurINFO, entre muchos otros).

16:00h a 16:30h	**Café/Networking**	
16:45h a 17:30h	**Mesa Redonda: Vulnerabilidades en el mundo Industrial y Tecnologías de Protección**  Rony Lerner  Andrey Nikishin  MªPilar Torres  Jaime A. Restrepo  Moderador: Ignacio Paredes	Rony Lerner (Tripwire), Andrey Nikishin (Kaspersky), Maria Pilar Torres (Everis), Juan Carlos Guel (Mnemo), Jaime Andrés Restrepo (DragonJAR). Moderador: Ignacio Paredes (CCI)
17:15h a 18:00h	**Mesa Redonda: Las Organizaciones Industriales Opinan: ¿Y ahora qué? (Conclusiones, lecciones aprendidas y siguientes pasos)**  Diego Zuluaga  Alexis H. Donoso  Fernando Guerrero Johanna Orjuela  Moderador: Samuel Linares	Diego Zuluaga (ISAGEN), Alexis Hidalgo Donoso (PEMEX), Johanna Orjuela (EcoPetrol), Fernando Guerrero (CISO & CIO, CELEC EP) Moderador: Samuel Linares (CCI)
18:00h a 18:15h	**Resumen Jornada y Clausura Congreso**	Samuel Linares (CCI)

26 de Mayo: Talleres Pre-Congreso

- **9:00 a 13:00h: Taller Avanzado sobre Seguridad en los Sistemas de Control Industrial**
  - Profesor(es): Samuel Linares, Nacho Paredes, José Valiente, Claudio Caracciolo, Leonardo Huertas, Carlos Jumbo
  - Coste de Inscripción: US$ 300

  Hace un tiempo, Patrick Miller realizó una encuesta a los mayores expertos globales en Ciberseguridad Industrial, pidiéndoles identificar los mayores retos y más preocupantes en el ámbito de la Ciberseguridad Industrial. Los resultados ya están disponibles y necesitan soluciones. Samuel Linares ha estado desarrollando esa misma encuesta en distintas partes el mundo (España, Qatar, Abu Dhabi, Reino Unido, Argentina, Estados Unidos…). Únase a sus colegas en este taller colaborativo para discutir las medidas más efectivas para solucionar esos difíciles obstáculos.

  Con todas las noticias sobre la Ciberseguridad alrededor de los SCADA y los Sistemas de Control Industrial, es difícil decir qué es verdad y qué no lo es. Entendiendo las amenazas reales, las vulnerabilidades y los impactos a estos sistemas críticos supone un reto importante. Discernir cuáles son las estrategias prácticas, efectivas y con un coste adecuado, puede llegar a ser igualmente difícil. Las aproximaciones específicas para la seguridad requerida en los Sistemas de Control Industrial no son entendidas totalmente por muchos profesionales. En esta sesión, podrá escuchar también algunos de los éxitos y fracasos relativos a la tecnología, los procesos y la gestión, así como posibles aproximaciones para avanzar en el difícil camino que se tiene por delante.

- **14:00h a 18:00h: Ciberseguridad Industrial en los Digital Oilfield**
  - Profesor(es): Ayman Al-Issa
  - Coste de Inscripción: US$ 500

  Descripción completa pendiente de recepción.

29 de Mayo: Talleres Post-Congreso

- **9:00 a 13:00h: Introducción a la Seguridad en Smart Grid**
  - Profesor(es): Iñaki García y Arkaitz Gamino (Tecnalia)
  - Coste de Inscripción: US$ 300

Durante los últimos años la red eléctrica ha evolucionado hasta convertirse en la nueva Smart Grid, una nueva red que pretende ser más eficiente y respetuosa con el medio ambiente. Unos de los cambios más influyentes en estas nuevas redes, han sido la instalación de contadores inteligentes (Smart Metes) y la gestión remota, para ello ha sido necesaria la conexión de los diferentes componentes a las redes de telecomunicaciones. La próxima masificación en la instalación de nuevos contadores inteligentes y la conexión a la red de telecomunicaciones abre nuevos vectores de ataque a posibles atacantes. En este curso se pretende dar una visión global de la seguridad en las Smart Grids, analizando la problemática de seguridad en el ámbito de la baja tensión y media tensión.

Contenido general:

- Introducción a las Smart Grid
- Problemáticas de seguridad
- Retos de seguridad en el ámbito de la Smart Grid
- Estándares y normativas
- Cómo abordar la seguridad (algunas soluciones)
- La utility del 2020

Iñaki Eguía Elejabarrieta

Iñaki Eguía es investigador en cibersegruidad industrial dentro del área de negocio de IT Competitiveness en la división ICT-European Software Institute de Tecnalia. Ha participado en varios proyectos europeos relacionados con la seguridad y la heterogeneidad de redes. Es miembro de la plataforma tecnológica PESI (Seguridad Industrial) considerado como experto por ésta para asesorí, y miembro de la Plataforma NIS recientemente constituida sobre ciberseguridad en Europa y Artemis (Plataforma Tecnológica Europea de Sistemas Embebidos). Como líder el grupo de seguridad, establece la estrategia y la despliega, con el fin último de desarrollar activos tecnológicos que impacten en mercado y en la sociedad. Iñaki es también coordinador del proyecto europeo ARCADIA (www.arcadia-project.eu) para la elaboración de una hoja de ruta en el área de sistemas embebidos y el proyecto RISC (convergencia de seguridad física y lógica en Infraestructuras Críticas). Actualmente estudia para realizar un doctorado sobre gestión de la innovación en la Escuela de Ingenieros industriales y Telecomunicaciones en Bilbao. Obtuvo su doble ingeniería de Informática y Organización Industrial en la Universidad de Deusto y Lund.

Arkaitz Gamino

Arkaitz Gamino es investigador en cibersegruidad industrial dentro del área de negocio de IT Competitiveness en la división ICT-European Software Institute de TECNALIA. Ha participado en diferentes proyectos europeos relacionados con la ciberseguridad industrial, convergencia entre los sistemas físicos y lógicos, seguridad web y sistemas embebidos. Por otro lado, ha participado en numerosos proyectos en el ámbito de la seguridad IT y certificación de normativas de seguridad; LOPD (Ley Órganica de Protección de Datos) y legislación que regula los sistemas de juego on-line y presencial. Estudio Ingeniería Informática y realizó el Master en Seguridad de la Información en la Universidad de Deusto.

- **14:00h a 18:00h: Introducción a los Sistemas de Control Industrial para profesionales TIC**
  - Profesor(es): José Valiente (CCI)
  - Coste de Inscripción: US$ 300

  Aunque los Sistemas de control industrial (OT) utilizan cada vez con mayor frecuencia sistemas comerciales estándar del mercado IT, se observan importantes diferencias respecto a estos últimos (la importancia ante todo de la disponibilidad, los requerimientos de rendimiento y de fiabilidad, las configuraciones del Sistema Operativo y de aplicaciones, las arquitecturas, etc.), por lo que las contramedidas tradicionales para un sistema IT pueden resultar inapropiadas para un sistema OT. El objetivo del taller es dar a conocer a los profesionales de los sistemas TIC en qué consiste un sistema de control industrial y sus diferentes componentes, incluyendo instrumentación y sensórica, dispositivos de control (PLCs, RTUs, DCS...), redes de control industrial y protocolos específicos (OPC, DNP3, Profibus, etc...), sistemas SCADA, historizadores y sistemas MES, según los niveles 0 a 3 de la ISA. Asimismo nos adentraremos en aspectos relacionados con la ciberseguridad y cómo estos dispositivos de última generación se adaptan a las necesidades de seguridad y alta disponibilidad. Para el taller se utilizarán equipos de control industrial y redes reales.

- **14:00h a 18:00h: Introducción a la Ciberseguridad para profesionales de la Automatización e Instrumentación**
  - Profesor(es): Ignacio Paredes (CCI), Claudio Caracciolo y Leonardo Huertas (Eleven Paths, CCI)
  - Coste de Inscripción: US$ 300

  El objetivo del taller es preparar al personal responsable de los sistemas de control y automatización para afrontar los retos de ciberseguridad surgidos de aplicar las nuevas tecnologías de la información y las comunicaciones a las instalaciones industriales.

  Durante el taller se discutirá cuál es el estado actual de la ciberseguridad en estas instalaciones, por qué se ha llegado a esta situación, qué se puede hacer para solucionar los problemas aparecidos y mitigar el impacto de posibles incidentes y qué herramientas tenemos disponibles para ayudarnos en esta labor.

Ignacio Paredes

Ignacio Paredes es ingeniero Superior en Informática y es el Responsable de Estudios e Investigación en el Centro de Ciberseguridad Industrial además de Experto Evaluador de la Comisión Europea. Desde el año 1999 ha desarrollado su carrera profesional involucrado en proyectos de tecnologías de la información y telecomunicaciones para empresas de distintos sectores (telecomunicaciones, industria, logística, ingeniería, administración pública). Es experto en el diseño e implantación de soluciones de seguridad tanto a nivel físico y lógico como organizativo. Con amplia experiencia en campos como el diseño seguro de redes, hacking éticos, la seguridad en entornos industriales, la seguridad en aplicaciones, planes de continuidad del negocio, la implantación de sistemas de gestión de la seguridad ISO 27001, gestión y tratamiento de riesgos.

Entre otras, posee las certificaciones CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), CRISC (Certified in Risk and Information Systems Control), CISSP (Certified Information Systems Security Professional), PMP (Project management Professional), GIAC Systems and Network Auditor (GSNA), GIAC Assessing Wireless Networks (GAWN), ISO 27001 (BS 7799) Lead Auditor por BSI (British Standards Institution), EC-Council Certified Ethical Hacker, NetAsq CNE y CNA, Sun SCNA y Sun SCSA

PATROCINIO DEL CONGRESO

Están disponibles distintos niveles de patrocinio del evento basados en la presencia y posicionamiento del patrocinador en el mismo y en su deseo de transmitir su aproximación al mercado:

Patrocinio Bronze

El patrocinador Bronze dispondrá de los siguientes beneficios:

- **1 invitación** al congreso.
- I**nserción del logo**, dentro del nivel de patrocinadores Bronze, en el portal del Congreso, en el email de invitación y agenda del congreso, así como en el agradecimiento de asistencia.
- Aparición del logo en **anuncios que se publicarán en al menos tres medios** de referencia.

El coste de patrocinio Bronze es de 1.000 € / 1.500 US$

Patrocinio Silver

El patrocinador Silver dispondrá de los siguientes beneficios:

- **2 invitaciones** al congreso.
- I**nserción del logo**, dentro del nivel de patrocinadores Silver, en el portal del Congreso, en el email de invitación y agenda del congreso, así como en el agradecimiento de asistencia.
- Aparición del logo en **anuncios que se publicarán en al menos tres medios** de referencia.
- Tendrá a su disposición **un espacio de stand**.

El coste de patrocinio Silver es de 2.000 € / 3.000 US$

Patrocinio Gold

- **3 invitaciones** al congreso.
- I**nserción del logo**, dentro del nivel de patrocinadores GOLD, en el portal del Congreso, en el email de invitación y agenda del congreso, así como en el agradecimiento de asistencia.
- Aparición del logo en **anuncios que se publicarán en al menos tres medios** de referencia.
- Tendrá a su disposición **un espacio de stand**.
- Posibilidad de una ponencia de 30 minutos.

El coste de patrocinio Gold es de 3.000 € / 4.500 US$

Patrocinio Platinum (Máximo 1 patrocinador)

- **6 invitaciones** al congreso.
- I**nserción del logo**, dentro del nivel de patrocinadores PLATINUM, en el portal del Congreso, en el email de invitación y agenda del congreso, así como en el agradecimiento de asistencia.
- Aparición del logo en **anuncios que se publicarán en al menos tres medios** de referencia.
- Tendrá a su disposición **un espacio de stand**.
- Posibilidad de una ponencia de 40 minutos y participación en Mesa Redonda.

El coste de patrocinio Platinum es de 6.000 € / 9.000 US$

El Centro de Ciberseguridad Industrial

El Centro de Ciberseguridad Industrial (CCI) es una organización independiente sin ánimo de lucro cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial desarrollando actividades de análisis, desarrollo de estudios e intercambio de información sobre 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 y cómo éstas suponen una de las bases sobre las que está construida la sociedad actual.

El CCI es el punto independiente de encuentro de los organismos, privados y públicos, y profesionales relacionados con las prácticas y tecnologías de la Ciberseguridad Industrial, así como en la referencia hispanohablante para el intercambio de conocimiento, experiencias y la dinamización de los sectores involucrados en este ámbito

Para ello, el CCI se ha marcado los siguientes objetivos:

- Aglutinar a los principales actores y expertos implicados en la Ciberseguridad Industrial con objeto de que colaboren, intercambien experiencias y conozcan los últimos avances y desarrollos.
- Proporcionar un Ciber-Estado de Situación, prestando especial atención a la evolución de las ciberamenazas y las nuevas formas de ataque.
- Establecer canales de interlocución con autoridades y reguladores, para facilitar la comunicación entre los diferentes actores involucrados en la Ciberseguridad Industrial (principalmente: administración, organizaciones industriales e infraestructuras críticas, ingenierías e integradores, fabricantes, consultoras, asociaciones, organismos de estandarización y buenas prácticas y los ciudadanos).
- Mejorar la concienciación de todos los actores mencionados mediante cursos, eventos, seminarios, publicaciones y la presencia en los medios de comunicación.
- Cualificar a profesionales en Ciberseguridad Industrial con el fin de facilitar a las empresas su contratación.
- Fomentar la dinamización y difusión de la industria española de la Ciberseguridad Industrial.

Algunos Datos acerca de CCI

- Organización independiente sin ánimo de lucro.
- Único centro dedicado a la Ciberseguridad Industrial en español en toda Iberoamérica.
- Más de 300 miembros en 26 paises.
- Liderazgo en el desarrollo de marcos de referencia y buenas prácticas en el ámbito de la Ciberseguridad Industrial.
- Referente internacional en el ámbito de la Ciberseguridad Industrial en español.
- Organizador del único Congreso Iberoamericano sobre Ciberseguridad Industrial y de los eventos periódicos “La Voz de la Industria” dedicados a la promoción, formación y fomento de la Ciberseguridad Industrial.
- Representación de miembros activos en eventos nacionales e internacionales.
- Equipos de Conocimiento de miembros activos sobre ámbitos específicos de la Ciberseguridad Industrial.

- Publicación de Estudios, Informes y Análisis sobre Ciberseguridad Industrial.

Nuestros Patrocinadores

El Centro cuenta con el patrocinio en España de algunas de las principales organizaciones internacionales en el ámbito de la Ciberseguridad Industrial (aún están disponibles opciones de patrocinio para este evento y para el Centro):

Registro e Inscripción de Asistentes

El acceso al Congreso Iberoamericano de Ciberseguridad Industrial es gratuito para los miembros activos y patrocinadores del Centro de Ciberseguridad Industrial. Si aún no es miembro del Centro tiene distintas opciones para asistir al Congreso.

Nombre:	
Apellidos:	
Cargo:	
Organización/Empresa:	
Email:	
NIF:	
Dirección Postal:	
Ciudad	
Código Postal:	
País:	
Teléfono:	
Fax:	
Teléfono Móvil:	

☐ **US$ 200 de descuento por subscripción anticipada antes del 15 de Abril**

☐ **US$ 100 de descuento por subscripción anticipada antes del 1 de Mayo**

	Asistencia al Congreso	**US$ 500**
	Cocktail/Party/Fiesta	+ US$ 50
	Asistencia al Congreso + Cocktail/Party/Fiesta + Asistencia a todos los talleres pre y post congreso	**US$ 1.250**
	Asistencia al Congreso + Asistencia a una jornada de talleres	US$ 900
	Asistencia al Congreso + Asistencia a media jornada de talleres	US$ 700
	Taller Pre-congreso: Ciberseguridad Industrial Avanzada	US$ 300
	Taller Pre-congreso: Ciberseguridad Industrial en los Digital Oilfield	US$ 500
	Taller Post-congreso: Introducción a la Seguridad en Smart Grid	US$ 300
	Taller Post-congreso: Introducción a los Smas. de Control Ind. para profesionales TIC	US$ 300
	Taller Post-congreso: Introducción a la Ciberseguridad para profesionales del ámbito industrial	US$ 300
	Oferta Membresía CCI Activa con Subscripción Anual hasta 31 Diciembre 2014 (al registrarse en el Congreso)	+ US$ 1.250

Nota: Todos los precios no incluyen IVA

Métodos de Pago

☐ **Transferencia Bancaria:**

ING Direct
Entidad: 1465 – Oficina: 0170 – Cód. Control: 11 – Nº Cuenta: 1900044819
IBAN: ES47 1465 0170 1119 0004 4819

☐ **Tarjeta de Crédito:**

Tipo de Tarjeta: ☐ **VISA** ☐ **MasterCard** ☐ **American Express**
Número Tarjeta: _____
Caduca: _____/_____ **Código de Seguridad (CVV):** _____
Nombre y Apellidos (como aparece en la tarjeta)_____

CONDICIONES GENERALES

El término «Organizador» representa al Centro de Ciberseguridad Industrial, de ahora en adelante CCI.
El término «Asistente» incluye cualquier persona física o jurídica que desee patrocinar, asistir, colaborar o esponsorizar el Congreso de Iberoamericano de Ciberseguridad Industrial

Todos los asistentes, por el mero hecho de formalizar su contrato, aceptan las presentes condiciones generales y las disposiciones del organizador.

1. ADMISIÓN

El Organizador se reserva el derecho de admisión y podrá rechazar aquellas solicitudes que, a su criterio, no se ajusten a las finalidades del evento. Si la solicitud no pudiera ser admitida por la razón expuesta, el organizador procederá a la devolución de las cantidades ya ingresadas.

2. GESTIÓN DE DOCUMENTACIÓN, EVENTOS, FORMACIÓN y MEDIOS PROPIOS DE COMUNICACIÓN.

El Organizador se reserva el derecho de establecer las reglas que considere necesarias para el contenido de la documentación y su elaboración, el buen funcionamiento de los eventos o medios propios de comunicación. También se reserva el derecho de prohibir cualquier tipo de exhibición, manifestación o comportamiento que –en opinión del Organizador- sea de mal gusto, o esté fuera de línea del resto de contenidos en los documentos y en los eventos o medios propios de comunicación, que pueda dar a los visitantes una idea del contenido de los documentos, de los eventos o medios de comunicación diferente de la que desea dar el Organizador.

3. CANCELACIÓN.

En caso de que el Asistente cancelase su participación, deberá tener en cuenta los costes de dicha cancelación que se determinan de la siguiente forma:
• Cuando la comunicación de la cancelación sea antes del 15 de Mayo de 2014, la cuota de cancelación equivaldrá al 10% del total convenido y dará derecho a la devolución del 90% del importe pagado.
• Cuando la comunicación de la cancelación sea después del 15 de Mayo de 2014, la cuota de cancelación equivaldrá al total del convenido.

El Asistente considera que todo pago hecho al Organizador será considerado pago ganado y merecido y por tanto no retornable, dado que el Organizador habrá incurrido en gastos y asumido compromisos relacionados con esta PROPUESTA y podrá haber perdido la oportunidad de alcanzar acuerdos con otros posibles Asistentes. Todas las cuotas de cancelación mencionadas en este párrafo deberán incrementarse con el IVA correspondiente.

En caso de que el Asistente no efectuara alguno de los pagos especificados antes de o en la fecha indicada para dicho pago, el Organizador se reserva el derecho de considerar la PROPUESTA como cancelada por el Asistente en la fecha en la que el pago debería haberse efectuado.

4. DESCONVOCATORIA O SUSPENSIÓN

Si por causas imputables al Organizador, el evento donde se posibilita la ponencia o participación fuera desconvocado, el asistente tendrá derecho a la devolución del 100% de las cantidades entregadas hasta dicho momento, sin derecho a indemnización alguna.

Se considera que no es causa imputable a la Organización la desconvocatoria o suspensión, temporal o definitiva y total o parcial del evento por causas fortuitas o de fuerza mayor, entendiéndose por tales, además de las definiciones al uso, otras con origen en terceros tales como huelgas, corte de suministro de agua y electricidad o casos de similar gravedad.

5. CESIÓN DE DERECHOS

El Asistente tendrá derecho a las actividades y documentación previstas en el contrato.
Dichas actividades y documentación no serán transferibles ni podrán ser compartidas.

6. FOTOGRAFÍAS Y REPRODUCCIÓN DE CONTENIDOS

Será preciso contar con la autorización del Organizador para obtener fotografías y filmaciones en los eventos.
Será imprescindible contar con la autorización del Organizador para reproducir parcialmente cualquier contenido de documentos publicados o en estado de borrador, o cualquier material de formación objeto de este contrato.
Este contrato obliga al Asistente a no difundir, ni distribuir los documentos e información facilitada por ningún medio.