



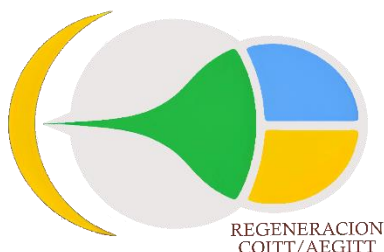
Jornada Formación profesional: Ciberseguridad Industrial e Infraestructuras Críticas



COMUNIDAD DE MADRID
Consejería de Educación
IES PACÍFICO

IES Pacífico

UNIÓN EUROPEA
Fondo Social Europeo
“El FSE invierte en tu futuro”



Introducción

Nos encontramos inmersos en la cuarta revolución industrial, llamada industria 4.0 donde la automatización y control industrial encuentra paso con la digitalización, hiperconectividad, la robótica, la impresión 3D y el internet de las cosas generando procesos óptimos y eficientes e impulsando una mayor calidad.

Gracias a la llegada de este tipo de tecnología a la Industria, las compañías deben cambiar su paradigma tradicional y apostar por una visión mucho más flexible y de futuro. Se hace necesario, por lo tanto, transformar la Industria.

Pero a su vez han generado riesgos que hay que abordar y mitigar. Las infraestructuras industriales son cada vez más atacadas, por lo que la ciberseguridad en la industria ha pasado a ocupar un punto clave en el orden del día de estas empresas.

Objetivo del documento

Por ello se propone en este dossier crear las primeras Jornadas de “Formación profesional: Ciberseguridad Industrial e Infraestructuras Críticas” que se conviertan en referente en la Comunidad de Madrid el próximo **21 de junio del 2023 por la tarde**. La entrada será gratuita previo registro para controlar aforo

Es un tema de completa actualidad y que se visualiza en el día a día- Recordemos cuando ocurrió el año pasado el incidente de ransomware de Colonial Pipeline en E.E.U.U, considerado el mayor ataque contra una infraestructura crítica de la historia que llevó a interrumpir el servicio de derivados del petróleo y puso en jaque al propio gobierno. Todo se hubiera minimizado siguiendo unas dosis mínimas de ciberseguridad (política de contraseñas, gestión de roles y permisos, deshabilitar escritorio remoto, actualización de sistemas con parches de seguridad). También en septiembre de este año se recibieron noticias de que hackers rusos tomaron el control de parques eólicos en Alemania, perdiendo el control de muchos de ellos durante más de 24h.

Valor añadido IES Pacífico en Ciberseguridad Industrial

Es necesario contar con profesionales que se adapten a los retos que se vienen en la ciberseguridad industrial. Por ello el IES Pacífico como referente en Electrónica y Telecomunicaciones podría convertirse en pionero en estos ámbitos y sobre todo formar profesionales líderes en el sector, con conocimientos en Operation Technology (OT), electrónica, buses de protocolos industriales y automatización.

¿Cuáles son las diferencias entre la seguridad en Tecnologías de la Información y Tecnologías de la operación o sistemas de control? Uno se centra en el dato y otro en el proceso de producción.

Otra de las diferencias más notables es en la prioridad de la triada de la seguridad de la información. La disponibilidad está muy por encima de todo. La fábrica debe producir todo lo que pueda y a máxima capacidad del 100% y si fuera las 24h mejor. Las otras dos (confidencialidad e integridad) quedan relegadas en menor importancia.

En IT si hay algún fallo puntual es tolerable y un reinicio del router o del ordenador suele ser algo sencillo. En cambio, los reinicios de los sistemas industriales son dificultosos porque la mayoría son manuales y necesitan sincronización entre ellos. Finalmente, el ciclo de vida de los productos hardware en Industria suelen ser hasta 20 años en contraposición a dispositivos comerciales que a los 5 años son totalmente obsoletos.

Por todo ello se piensa en que esta jornada de Ciberseguridad OT es sumamente interesante para la Familia profesional: Electricidad y Electrónica de las enseñanzas de Formación Profesional y a sus alumnos.

Objetivo del documento

Por ello se propone en este dossier crear las segundas Jornadas de “Formación profesional: Ciberseguridad Industrial e Infraestructuras Críticas” que continúen siendo un referente en la Comunidad de Madrid. La primera edición fue el pasado 21 de Junio del 2023 y hubo más de 65 participante. La entrada será gratuita previo registro para controlar aforo

Es un tema de completa actualidad y que se visualiza en las noticias - Recordemos cuando ocurrió el año pasado el incidente de ransomware de Colonial Pipeline en E.E.U.U, considerado el mayor ataque contra una infraestructura crítica de la historia que llevó a interrumpir el servicio de derivados del petróleo y puso en jaque al propio gobierno. Todo se hubiera minimizado siguiendo unas dosis mínimas de ciberseguridad (política de contraseñas, gestión de roles y permisos, deshabilitar escritorio remoto, actualización de sistemas con parches de seguridad). También en septiembre de este año se recibieron noticias de que hackers rusos tomaron el control de parques eólicos en Alemania, perdiendo el control de muchos de ellos durante más de 24h.

Primera Jornada de Formación Profesional Ciberseguridad Industrial Infraestructuras Críticas



21 de junio de 2023

17:30 en IES Pacífico - C/ Luis Mitjans 41, Madrid

Registro



IES Pacífico



UNIÓN EUROPEA
Fondo Social Europeo
"El FSE invierte en tu futuro"



COMUNIDAD DE MADRID
Consejería de Educación
IES PACÍFICO



Registro

Aforo limitado mediante este registro web: <https://events.vtools.ieee.org/m/363521> , Boton "Register".

Se proveerá bebida en el networking.

Horario jornadas

El horario tentativo será el siguiente para el **miércoles 21 de junio a las 17:30:**

- 17:30 – Recepción y acreditación de asistentes
- 17:40 – Inauguración autoridades
- 17:50 – “Introducción a la Seguridad en Sistemas de Control y Automatización Industrial” por Manuel Ballesteros (IEEE IAS - Instituto Pacífico)
- 18:05 – “Vulnerabilidades en Infraestructuras Críticas” - Fast & Secure por Agustín Valencia Gil (Fortinet)
- 18:40 – “Descubrimiento de activos OT” por Carlos Jimenez (Mytra)
- 19:05 – Descanso. Demostración de empresas de Formación en Centros de Trabajo.
- 19:20 - "Quien tiene una IP tiene un tesoro" por José Manuel Baños - OSINT aplicada a la búsqueda de información de direcciones IP.
- 19:45 - Gestión de ciber incidentes en infraestructuras de Telecomunicación por Jose María Corsino (Delonia/Telefónica)
- 20:05 – 1) Proyecto FP: Introducción a Flipper Zero y vulnerabilidades en protocolos de Radiofrecuencia
 - 2) Proyecto FP: Gestión de red WIFI en Infraestructura Crítica
 - 3) Proyecto FP: Camarás robóticas con sistemas de Monitoreo y Control
- 20:30 – Saludos de personas de FP que trabajan en ciberseguridad
 - Marcos Burdalo (NTT Data) y José Antonio Montoya (Erion)
- 20:30 – IEEE Young Professionals por Javier Andión (UPM)
- 21:00 – Networking en el Bar.
Presentación de profesionales de prestigio de: Siemens Mobility, Delonia Software, Adif, Fortinet.

Ponentes



Agustín Valencia Gil-Ortega.

Responsable de ciberseguridad OT de Fortinet para Europa. Cybersecurity advisory for industry 4.0, energy and all digital transformations

Amplia experiencia en entornos energéticos, desde renovables a nucleares, pasando por dispositivos IoT. Ingeniero industrial por Universidad Comillas-ICAI, co-líder del Grupo de Trabajo de Ciberseguridad de ISA-Sección Españolas y Experto del CCI



Carlos Jiménez Saiz

General Manager at Mytra S.L. Experto en estándar de la seguridad en sistemas industriales ISA/IEC 62443

En el siguiente Link puedes ver los grandes proyectos de digitalización y automatización en el sector industrial realizados por Mytra, junto a las grandes empresas.

<https://www.mytra.es/casos-exito>



José Manuel Baños es Ingeniero Técnico de Telecomunicación por la UPM y Máster en Ciberseguridad por la UCJC. Su carrera profesional la ha desarrollado en redes IP en NOC de proveedores internacionales, siendo coordinador de uno en estos momentos. Entre sus intereses están la ciberinteligencia y la detección y respuesta ante incidentes de seguridad.



Jose María Corsino Emprendedor, inversor y CIO / CEO con más de 15 años de experiencia en proyectos de tecnología de la información con grandes corporaciones: seguros, banca, telecomunicaciones, salud y farmacia, ingeniería, ferrocarriles, procesamiento de señales y más. Amplia experiencia con clientes internacionales: LATAM, Reino Unido, Francia, Luxemburgo, Bélgica, India, Estados Unidos, China, Corea, etc.

Comité técnico



Pedro Plaza Merino - Ingeniero de Siemens Mobility. Doctor en Tecnologías Industriales por la UNED. Desarrolla tareas relativas al diseño de sistemas electrónicos orientados a los enclavamientos y control de trenes. Es autor de varias publicaciones en prestigiosas conferencias y revistas.



José Antonio Montoya es Técnico Superior en Sistemas de Telecomunicaciones e Informáticos. Con experiencia en el sector ferroviario ha desempeñado tareas de mantenimiento y puesta en servicio tanto en infraestructura como en material rodante. Actualmente es responsable técnico de garantía de una flota de locomotoras en Erion.



Javier Andión (miembro de IEEE) es profesor ayudante doctor en la Universidad Politécnica de Madrid, Departamento de Ingeniería de Sistemas Telemáticos – ETSI de Telecomunicación desde 2020. Es ingeniero de telecomunicaciones, en 2020 obtuvo su Ph.D. (Cum Laude) en Ingeniería de Sistemas Telemáticos

Comité organizador



Manuel Ballesteros es ingeniero SCADA y Ciberseguridad industrial. Con experiencia en energía renovable y en Oil/Gas. es máster en ciberseguridad por la UCJC dedicándose al ámbito de las tecnologías de la Operación (OT), IEC 62443, automatización e industria 4.0. También es director de la sociedad española de Aplicaciones Industriales y Sistemas de Control del IEEE. Ingeniero técnico de telecomunicación por la UPM y Profesor de Sistemas Electrónicos en IES Pacífico.



Jonathan Rogelio Salas Gamez es ingeniero en sistemas computacionales por la UVM y Master en Ciberseguridad por la IMF. su carrera profesional la ha desarrollado en area de IT operations managment & infrastructure, asi como en Ethical hacking & penetration testing.

Voluntarios IEEE - IES Pacífico

Aitor Andrés
Nicolas Vico
Jaime Delgado
Samuel Gomes,
Cristian Garcia Gonzalez
Alejandro de la morena
Javier Moreira
Javier Olivares
Manuel Diaz
Oscar del Hierro
Jhojan Guzmán
Jorge Clares
Luis Heredia
Jorge Fernando Jimenez

Eventos previos IEEE Ciberseguridad

El 27 de noviembre de 2022 se realizó el evento “Ciberseguridad y cañas” (IEEE Cyber & Beers UCJC). con más de 55 asistentes 71 inscritos. A través de IEEE Cybersecurity Initiative y con un alto componente industrial fue todo un éxito.

Inspirándose en el formato “MeetUp” y en un ambiente distendido de cervecería, buscó reconocer el enorme trabajo realizado por los estudiantes del Máster oficial de Ciberseguridad y divulgar su conocimiento en los Trabajo Fin de Máster. Así también contaremos con profesionales de prestigio de principales empresas de ciberseguridad que transmitieron la relevancia e importancia de su trabajo, sus contribuciones, y de qué manera impacta éste positivamente en la sociedad.



El 25 de mayo de 2023 se realizó en la Universidad Carlos III de Madrid la Jornada de Ciberseguridad en Telecomunicaciones. Un evento que contará con la participación de destacados expertos en la materia.



Ponentes:

- 🎤 Luis Hidalgo Gutiérrez - Responsable de Gabinete, Relaciones Institucionales y Eventos en INCIBE - Instituto Nacional de Ciberseguridad
- 🎤 Julio César Miguel - CEO del Grupo CFI , Presidente de AETICAL y Vocal de la AEI de Ciberseguridad
- 🎤 Roberto Hernández Berlinches - Director del Dpto. de Sistemas de Comunicación en UNED - Universidad Nacional de Educación a Distancia (Spain)
- 🎤 Tte. Coronel Juan A. Rodríguez Álvarez de Sotomayor - Unidad Ciberdelincuencia de la Guardia Civil
- 🎤 Arturo Ribagorda Gamacho - Catedrático emérito de la Universidad Carlos III de Madrid
- 🎤 Manuel Ballesteros. IEEE Spain Young Professionals / SCADA Engineer and Cybersecurity OT y Profesor Sist. Elec. del IES Pacífico de Madrid
- 🎤 Luis Panizo Alonso, Director del título de Formación Permanente en Ciberseguridad de la Universidad de León y candidato a Decano del Colegio Oficial de Ingenieros Técnicos de

Telecomunicaciones (COITT)

Organizaciones centradas en Ciberseguridad y que apoyan actividades

	<p>El IEEE (Institute of Electrical and Electronics Engineers) es la organización internacional de ingeniería más grande del mundo y que involucra gran parte del desarrollo tecnológico/científico en la actualidad.</p>
	<p>Empresa multinacional de Estados Unidos con sede en California. Se dedica al desarrollo y la comercialización de software, dispositivos y servicios de ciberseguridad</p>
	<p>Soluciones de automatización, ciberseguridad y desarrollo de software para la industria, basadas en la innovación y en tecnologías de última generación.</p>
	<p>Sociedad Científica de Aplicaciones Industriales y Sistemas de Control</p>
	<p>Consultoria Tecnológica que trabaja en el sector de telecomunicaciones e infraestructuras críticas</p>
	<p>Ecosistema para avanzar juntos en Ciberseguridad Industrial. Networking, Conocimiento y Experiencias</p>
	<p>Compañía de Sistemas SCADADA y Software Industria</p>
	<p>Infraestructuras críticas: sistema de monitorización y control de activos IT/OT y técnicas de ciberseguridad</p>
	<p>Fabricante de dispositivos PLC, HMI, para industria</p>