Escuela Profesional de
Ciberseguridad Industrial

Dossier

2018-2019

"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 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, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la Sociedad actual, como puntales del estado del bienestar. Después de casi 5 años de existencia, se ha convertido en el **referente internacional en el ámbito de la ciberseguridad industrial, con un ecosistema de más de 1.300 miembros, un equipo de coordinadores regionales en casi 20 países, y un equipo multidisciplinar de 16 expertos.**

CCI viene trabajando en el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas, e intercambio de información y conocimiento, sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos -y su tratamiento- derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

CCI es, hoy, el ecosistema y el **punto de encuentro de las entidades -privadas y públicas- y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial**; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito.

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

Escuela Profesional del CCI

Presentación

Actualmente nos enfrentamos a una gran escasez de ingenieros de ciberseguridad de todo tipo. Para tener una idea de la magnitud de la escasez de habilidades en seguridad tecnológica, considere esto: A finales de este año, se predice que **uno o dos millones de trabajos de ciberseguridad permanecerán sin cubrir**. Se necesitarán alrededor de seis millones de profesionales de ciberseguridad, y estarán disponibles entre cuatro y cinco millones para cubrir los puestos.

De hecho, la escasez de habilidades de los ingenieros de ciberseguridad se está volviendo crítica: un informe de McAfee, "Hacking the Skills Shortage" concluye que el 82% de un grupo de 775 responsables de TI y ciberseguridad informaron de la escasez de habilidades de ciberseguridad dentro de su compañía.

Ante este escenario, desde el Centro de Ciberseguridad Industrial hemos decidido poner en marcha la **primera Escuela Profesional de Ciberseguridad Industrial** con el doble objetivo de proporcionar una **formación de calidad para profesionales con un enfoque práctico y la flexibilidad que necesitan los profesionales y sus organizaciones.**

En estos casi 5 años de existencia el CCI ha impartido 16 ediciones del "*Curso Multidisciplinar de Ciberseguridad Industrial y Protección de Infraestructuras Críticas*" y más de 20 talleres y cursos de distintas materias sobre ciberseguridad industrial, a los que han asistido unos 500 profesionales tanto de IT, como de OT a nivel internacional.

El equipo de formadores de la Escuela está formado por expertos (y colaboradores del CCI que han participado en la elaboración de contenidos para las publicaciones de CCI (https://www.cci-es.org/informes-y-analisis-estategicos) , así como en algunos de los talleres y cursos ya realizados.

Deseamos que esta escuela se convierta en una valiosa herramienta para adquirir experiencias y conocimiento en el campo de la ciberseguridad industrial para el ecosistema internacional del CCI.

Susana Asensio

Directora de la Escuela Profesional de Ciberseguridad Industrial

Programas

El contenido de los programas del master, dos cursos y cuatro talleres de la Escuela Profesional del CCI están basado en la documentación publicada por CCI (https://www.cci-es.org/informes-y-analisis-estategicos).

Talleres prácticos

Los talleres prácticos se celebrarán en el hotel Meliá Avenida de América, Calle de Juan Ignacio Luca de Tena, 36, Madrid. Se impartirán los lunes, en horario de 9:30 a 17:30 y con una duración de 7 horas. El número de plazas presenciales máximo es de 12 asistentes. También podrá accederse al taller de forma online, con un máximo de 6 asistentes. Los alumnos participantes en los talleres recibirán, además del **material práctico, el certificado de asistencia al taller y la Credencial Profesional Nivel Blanca** del Programa de Reconocimiento del Compromiso con la Ciberseguridad Industrial del CCI.

T01. Taller Evaluación de Madurez del Proceso de Ciberseguridad en Organizaciones industriales

Descripción	Programa
El objetivo de este taller es proporcionar a los profesionales de organizaciones industriales, ingenierías, integradores IT y OT el conocimiento necesario para determinar el grado de madurez en materia de ciberseguridad de una organización industrial respecto a los requisitos de la organización, identificando las principales brechas de seguridad, así como establecer comparaciones entre distintas organizaciones en cuanto a su madurez en capacidades de Ciberseguridad Industrial permitiendo evolucionar la gestión de riesgos a niveles de excelencia. Todo esto gracias a la herramienta de evaluación de madurez basada en C2M2.. 	**9:30 Modelos de madurez** **10:00 Descripción general de la herramienta** **11:00 Áreas de estrategia y organización** **12:00 Áreas de activos, riesgos y operación** **14:00 Descanso** **15:00 Áreas de configuración y accesos** **16:00 Área de continuidad** **16:45 Benckmarking. 27 objetivos relevantes** **17:30 Clausura del taller**
Dirigido a:	**Documentación incluida**
Responsables de la gestión de riesgos de Ciberseguridad industrial, responsables de continuidad de negocio, responsables de seguridad de la información, responsables de seguridad operacional y responsables de informática industrial. .	• **Herramienta de evaluación: Madurez del proceso de ciberseguridad en organizaciones industriales.** • **Manual de usuario** • **Presentaciones del taller** • **Caso práctico**

T02. Taller Diagnóstico de ciberseguridad en un entorno de automatización industrial

Descripción

Taller basado en un caso práctico para adquirir el conocimiento preciso acerca del estado de la ciberseguridad en una instalación industrial mediante la identificación de puntos débiles y la comprensión de los ciberriesgos que la instalación está afrontando; y la propuesta de acciones para mejorar su ciberseguridad.

Todo ello teniendo en cuenta los requisitos especiales de este tipo de entornos y garantizando en todo momento el correcto funcionamiento de los sistemas implicados.

El taller está estructurado para aplicar un diagnóstico de ciberseguridad en un entorno industrial.

Programa

9:30 Tecnologías de automatización industrial y escenarios de riesgo
11:30 Caso de uso Industrial
12:00 Características del diagnóstico
12:30 Metodología y entrevistas
13:00 Diagnóstico de Arquitectura de redes
14:00 Descanso
15:00 Diagnóstico de Sistemas
15:30 Diagnóstico de seguridad física
16:00 Diagnóstico de terceras partes
16:30 El informe del diagnóstico y su presentación
17:30 Clausura del taller

Dirigido a:

Este taller está dirigido fundamentalmente a los responsables de contratar este tipo de servicios, así como a los profesionales de IT y OT que se encargan de realizar estos servicios.

Documentación incluida

- **Buenas Prácticas para el diagnóstico de ciberseguridad en entornos industriales**
- **Presentaciones del taller**
- **Caso práctico**

T03. Taller Ciberseguridad en el Ciclo de Vida de un Proyecto Industrial

Descripción

Le permitirá aplicar la ciberseguridad en el diseño de la automatización industrial, analizando los riesgos e impacto en el negocio.

La forma más eficaz de proteger las tecnologías digitales empleadas en la operación de una planta industrial, es hacerlo en las etapas más tempranas de su ciclo de vida -diseño, provisión e instalación/puesta en marcha-, incorporando, en cada una de ellas, las medidas y mecanismos adecuados de ciberseguridad, junto al resto de requisitos de funcionalidad, calidad y seguridad ligada a las operaciones.

Programa

9:30 Kit documental CCI. Guía de ciberseguridad en el ciclo de vida
10:00 Ciberseguridad en la etapa de diseño
11:00 Debate: Requisitos de ciberseguridad en la etapa de diseño.
11:50 Ciberseguridad en las etapas de provisión y ejecución
14:00 Descanso
15:00 Debate: Éxitos y fracasos en la implementación de proyectos industriales
15:30 Ciberseguridad en la etapa de operación
16:45 Ciberseguridad en la etapa de mantenimiento
17:30 Clausura del taller

Dirigido a:

Este taller está dirigido fundamentalmente a los a los profesionales de organizaciones industriales, ingenierías, integradores, así como fabricantes de IT y OT que estén involucrados en proyectos de automatización industrial.
.

Documentación incluida

- **Ciberseguridad en el ciclo de vida de un proyecto de automatización industrial**
- **Presentaciones del taller**
- **Caso práctico**

T04. Taller Aplicación de un Sistema de Gestión de la Ciberseguridad Industrial

Descripción

Taller basado en un caso práctico para implantar un sistema de Gestión de Ciberseguridad Industrial. Se aplicará de forma práctica la guía para la construcción de un SGCI en la que se han contemplado directrices específicas de los estándares ISO27001 e IEC62443, para un tratamiento eficaz y continuado de los riesgos sobre la disponibilidad, la integridad y la confidencialidad de las operaciones y de la información gestionadas por los sistemas industriales.

El taller está estructurado para aplicar un sistema de gestión según los siguientes dominios:

Programa

9:30 Ámbito de aplicación del SGCI
10:00 Descripción general de la guía y sus controles
11:00 Dominio 1: Definición de una estrategia.
12:00 Dominio 2: Gestión de los riesgos de Ciberseguridad Industrial
14:00 Descanso
15:00 Dominio 3: Promoción de una cultura de Ciberseguridad Industrial
15:30 Dominio 4: Establecimiento de Normativas de ciberprotección
16:45 Dominio 5: Garantia de Resiliencia y continuidad
17:30 Clausura del taller

Dirigido a:

Este taller está dirigido fundamentalmente a los responsables de gestionar los riesgos en organizaciones industriales, tanto con responsabilidad en la seguridad corporativa, como en la seguridad tecnológica (IT y OT), así como a consultores y auditores de sistemas de gestión basados en los estándares ISO 27001 e IEC 62443.

Documentación incluida

- **Guía para la implantación de un sistema de gestión de la ciberseguridad industrial**
- **24 plantillas de los 6 dominios**
- **Mapeo de controles SGCI – ISO27001 – IEC 62443**
- **Presentaciones del taller**
- **Caso práctico**

Cursos

Están planificados anualmente dos cursos prácticos de Ciberseguridad Industrial. El número de plazas es limitado, consultar el calendario. Los alumnos participantes en los cursos recibirán, además del **material práctico, el certificado de asistencia al curso y la Credencial Profesional Nivel Verde** del Programa de Reconocimiento del Compromiso con la Ciberseguridad Industrial del CCI.

C01. Curso multidisciplinar de Seguridad Digital en la Industria [4.0] y Protección de servicios esenciales

Descripción

Este curso llevará a los participantes a través del estudio del estado del arte de la Protección de Servicios Esenciales y la Seguridad digital en la Industria [4.0], tanto en lo que a legislación y normativa se refiere, como a los estándares, iniciativas,marcos de gestión y tecnologías aplicables, consiguiendo así una visión global de la gestión de la seguridad en este tipo de organizaciones que permita al final del día establecer claramente los siguientes pasos a seguir para asegurar una correcta supervisión, gestión e implantación de las medidas de protección adecuadas.

Programa

Día 1

Conceptos y estado del arte

Bienvenida, presentaciones individuales...
Introducción. Términos y Conceptos Generales
Estado del Arte Internacional
Relación entre Protección de Servicios Esenciales y Seguridad en Industria 4.0
Malware en entornos industriales [4.0]
Aproximación a los Sistemas de Control Industrial [4.0]
Trabajo en Grupo: Identificación Sistemas Control Industrial
Vulnerabilidades y Amenazas de los Sistemas de Control Industrial
Trabajo en Grupo: Análisis de un Caso Práctico (identificación vulnerabilidades, contramedidas...)
Situación Actual de la Ciberseguridad Industrial

Día 2

Diagnóstico, estándares y recomendaciones

Aspectos Organizacionales y de Gestión
Diagnóstico de la Ciberseguridad Industrial
Trabajo en Grupo: Discusión sobre el Diagnóstico
Estándares Aplicables
Recomendaciones y Siguientes Pasos:
Estableciendo un Programa de Ciberseguridad
Trabajo en Grupo: Caso Práctico y Desarrollo y Presentación por equipos del Plan de Seguridad

Día 3

Taller práctico

Presentación Taller Práctico HOL (Hands On Lab)
Taller y Actividades Prácticas
Conclusiones

Dirigido a:

Este curso está dirigido fundamentalmente a los responsables de gestionar los riesgos de ciberseguridad en organizaciones industriales, así como a consultores y auditores de sistemas de gestión de riesgos. Dirigido también a profesionales de automatización industrial que necesitan comprender como gestionar los riesgos OT.

Documentación incluida

- **Guía para la implantación de un sistema de gestión de la ciberseguridad industrial**
- **Buenas prácticas para el diagnóstico de ciberseguridad en entornos industriales**
- **Buenas Prácticas en el Análisis Forense de Sistemas de Automatización y Control Industrial**
- **Herramienta de evaluación de madurez**
- **Presentaciones del curso**

C02. Curso Responsable de Ciberseguridad en IACS (Sistemas de Automatización y Control Industrial)

Coorganizado por ISA España - CCI

Descripción

Curso práctico para implantar un sistema de Gestión de Ciberseguridad en un entorno IACS, basado tanto en un análisis de riesgos, como en un diagnóstico de ciberseguridad.
Se utilizará de forma práctica la guía para la construcción de un SGCI https://www.cci-es.org/sgci en la que se han aplicado directrices específicas de los estándares ISO27001 e IEC62443 para un tratamiento eficaz y continuado de los riesgos sobre la disponibilidad, la integridad y la confidencialidad de las operaciones y de la información gestionadas por los sistemas de automatización y control industrial.

Programa

Día 1

9:00 Bienvenida y presentaciones
9:15 Contexto. Automatización industrial
10:00 Consecuencias de los riesgos tecnológicos en IACS.
10:30 Diagnóstico de ciberseguridad en entornos industriales.
11:10 Ciberseguridad Industrial e Infraestructuras Críticas Industriales
12:10 Ámbitos de aplicación de un sistema de gestión de ciberseguridad Industrial
13:30 Descanso
14:30 Dominio 1: Definición de una estrategia.
15:30 Dominio 2: Gestión de los riesgos de Ciberseguridad Industrial
17:30 Clausura jornada

Dia 2

9:00 Dominio 3: Cultura en ciberseguridad
10:00 Dominio 4: Normativas de protección
11:10 Dominio 5: Garantía de Resiliencia y continuidad
12:00 Modelos de Madurez. Ciberseguridad
12:30 Herramienta de evaluación. Parte 1
13:30 Descanso
14:30 Herramienta de evaluación. Parte 2
15:00 Benckmarking práctico. 27 objetivos
16:30 Clausura del curso

Dirigido a:

Este curso está dirigido fundamentalmente a los responsables de gestionar los riesgos de ciberseguridad en organizaciones industriales, así como a consultores y auditores de sistemas de gestión de riesgos. Dirigido también a profesionales de automatización industrial que necesitan comprender como gestionar los riesgos OT

Documentación incluida

- **Guía de implantación del SGCI**
- **Diagnóstico de ciberseguridad**
- **Herramienta de evaluación de madurez**
- **Presentaciones del curso**
- **Caso práctico**

Máster Profesional Online

El Máster Profesional Online de Ciberseguridad Industrial capacita a los profesionales de automatización industrial, y a los profesionales de tecnologías de información en la gestión de riesgos tecnológicos de las infraestructuras industriales esenciales, así como de las redes y los sistemas de supervisión y control, y las medidas de protección que deben de aplicarse. Este máster es **completamente online**, un total de 450 horas de dedicación divididas en 12 sesiones masterclass, en directo, de 50 minutos (que también serán grabadas), 9 trabajos y 4 foros. Tendrá una duración de 4 meses, realizándose 3 sesiones de masterclass y 2 trabajos por cada módulo. Los alumnos participantes en el Máster recibirán, además del **material práctico, el Diploma de Máster CCI y la Credencial Profesional Nivel Negro** del Programa de Reconocimiento del Compromiso con la Ciberseguridad Industrial del CCI.

M01. Máster Profesional Online de Ciberseguridad Industrial

Descripción

Máster que permitirá analizar y comprender el riesgo asociado a las infraestructuras industriales y su relación básica con los Sistemas de Control Industrial. Conocimiento necesario para cualquier profesional de ingeniería industrial o informática relacionado con áreas como las TIC, energía, industria química y nuclear, agua, fabricación o transporte, entre otros.

Programa

Módulo 1: Conceptos de automatización industrial y estado del arte de la Seguridad Digital en la industria [4.0]

Módulo 2: Diagnóstico de la Ciberseguridad Industrial

Módulo 3: Preparando un programa de Ciberseguridad Industrial

Módulo 4: Hacking y estrategia de Defensa

Módulo 5: Trabajo fin de Master

Dirigido a:

Este Máster está dirigido a profesionales de la automatización industrial, a profesionales de instrumentación y control, a profesionales TIC y de Seguridad de la información.

Documentación incluida

- **Guía para la implantación de un sistema de gestión de la ciberseguridad industrial**
- **Buenas prácticas para el diagnóstico de ciberseguridad en entornos industriales**
- **Buenas Prácticas en el Análisis Forense de Sistemas de Automatización y Control Industrial**
- **Herramienta de evaluación de madurez**
- **Ciberseguridad en el Ciclo de Vida de un proyecto de automatización industrial**
- **Presentaciones del master**
- **Caso práctico**

Calendario

ESCUELA PROFESIONAL DE CIBERSEGURIDAD INDUSTRIAL CCI
Lugar (Hotel Meliá Avenida de América, Calle de Juan Ignacio Luca de Tena, 36, 28027 Madrid)

Cursos, talleres y sesiones de concienciación prácticos	Duración	Plazas disponibles	Precio Oficial	Precio M.B	Precio M.A o M.P	Precio M.A.S	CALENDARIO 2018 SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	CALENDARIO 2019 ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
T01.Taller Evaluación de Madurez del Proceso de Ciberseguridad en Organizaciones industriales 9:30 a 17:30	7 horas	12 presenciales 6 virtuales	350 €	300 €	250 €	200 €	Lunes 24		Lunes 26		Lunes 14		Lunes 4		Lunes 6		Lunes 1		Lunes 14		Lunes 2
T02.Taller Diagnóstico de ciberseguridad en un entorno de automatización industrial 9:30 a 17:30	7 horas	12 presenciales 6 virtuales	350 €	300 €	250 €	200 €		Lunes 15		Lunes 17		Lunes 4		Lunes 1		Lunes 3		Lunes 16		Lunes 4	
T03.Taller Ciberseguridad en el Ciclo de Vida de un proyecto Industrial 9:30 a 17:30	7 horas	12 presenciales 6 virtuales	350 €	300 €	250 €	200 €	Lunes 17		Lunes 19		Lunes 28		Lunes 18		Lunes 20		Lunes 8		Lunes 28		Lunes 16
T04.Taller Aplicación de un Sistema de Gestión de la Ciberseguridad Industrial 9:30 a 17:30	7 horas	12 presenciales 6 virtuales	350 €	300 €	250 €	200 €		Lunes 8		Lunes 3		Lunes 18		Lunes 29		Lunes 17		Lunes 30		Lunes 18	
C01.Curso multidisciplinar de Seguridad Digital en la Industria [4.0] y Protección de Servicios esenciales 2 jornadas completas + 1 mañana	22 horas	35 presenciales 10 virtuales	1.350 €	1.012 €	800 €	1 plaza sin coste			Martes 13 Miércoles 14 Jueves 15											Martes 12 Miércoles 13 Jueves 14	
C02.Curso Responsable de Ciberseguridad en IACS (Sistemas de Automatización y Control Industrial) ISA-CCI 9-17:30 y 9-16:30	16 horas	25 presenciales 10 virtuales	1.050 €	950 €	800 €	700 €								Miércoles 10 Jueves 11							
M01.Master Profesional Online de Ciberseguridad Industrial 19:00 a 20:30	450 horas 12 master class 9 trabajos Título propio	20 virtuales	3.450 €	3.050 €	2.850 €	2.450 €							Jueves 7 Jueves 14 Jueves 21	Jueves 4 Jueves 11 Jueves 25	Jueves 9 Jueves 16 Jueves 23	Jueves 6 Jueves 13 Jueves 27					

BONO Anual para Miembros Activos del CCI	10 plazas anuales taller	1.500 €
Mensual de la Escuela	10 plazas anuales taller	2.000 €

M.B. = Miembro Básico M.A. Miembro Activo

M.P = Miembro Profesional M.A.S.= Miembro Activo con Suscripción

PRECIO SIN IVA INCLUIDO

Mínimo 7 asistentes para celebrar cualquier curso o taller

Equipo de profesores

El equipo de profesores de la escuela profesional de Ciberseguridad Industrial está formado por expertos y colaboradores del CCI que cuentan con gran experiencia en proyectos de ciberseguridad en entornos de automatización industrial.

Samuel Linares	**https://www.linkedin.com/in/samuellinares/**
José Valiente	**https://www.linkedin.com/in/jvaliente/**
Silvia Villanueva	**https://www.linkedin.com/in/silviavillanueva/**
David Marco	**https://www.linkedin.com/in/davidmarcofreire/**
Edorta Echave	**https://www.linkedin.com/in/edortaechave/**
Joan Figueras	**https://www.linkedin.com/in/joanfiguerastugas/**
Enrique Martín	**https://www.linkedin.com/in/enriquemartingarcia/**
Javier Zubieta	**https://www.linkedin.com/in/javierzubieta/**
Jesús Mérida	**https://www.linkedin.com/in/jesusmerida/**
Belén Pérez	**https://www.linkedin.com/in/belenpr/**
Antonio Rodríguez	**https://www.linkedin.com/in/antonio-rodriguez-usallan-66407613/**
Claudio Caracciolo	**https://www.linkedin.com/in/claudiocaracciolo/**
Javier Pagès	**https://www.linkedin.com/in/javierpages/**
Ignacio Álvarez	**https://www.linkedin.com/in/ignacioa1/**

Sobre el Centro

Tras varios años analizando el mercado de la Ciberseguridad Industrial, sus actores, las necesidades del mundo hispanohablante en general y de nuestro país en particular, así como los casos de éxito y fracaso de otros países de Europa y Estados Unidos, la iniciativa del Centro se hizo pública el 5 de Marzo de **2013** de la mano de tres profesionales respetados por sus conocimientos y experiencia en este ámbito: Samuel Linares (**Linkedin Samuel Linares**), Ignacio Paredes (**Linkedin Ignacio Paredes**) y José Valiente (**Linkedin José Valiente**). Durante dos años este equipo directivo ha logrado que el Centro de Ciberseguridad Industrial se convierta en un referente internacional de la colaboración, coordinación y compromiso en la Ciberseguridad Industrial y la Protección de Infraestructuras Críticas. Un ejemplo internacional de ecosistema consolidado en torno a una disciplina como la Ciberseguridad Industrial, en el que todo el sector se encuentra, hoy, representado. Durante este tiempo han sido cientos los profesionales que -procedentes de países con culturas muy diversas y con roles igualmente variados dentro de las organizaciones- han conducido al Centro hasta lo que hoy representa en el panorama internacional (**artículo: dos años de vida de CCI**).

De esta forma se concluyó el primer ciclo de vida del Centro, en el que se consiguieron cumplir los objetivos iniciales que se habían marcado, los objetivos de **COLABORACIÓN**: concienciación, incremento del conocimiento, establecimiento de relaciones de confianza entre todos los actores, alcance global (con coordinadores de ecosistemas locales en distintos países de Latinoamérica) y máxima difusión, para avanzar en el desarrollo de una disciplina como la Ciberseguridad Industrial a través de la conjunción de todas sus distintas percepciones.

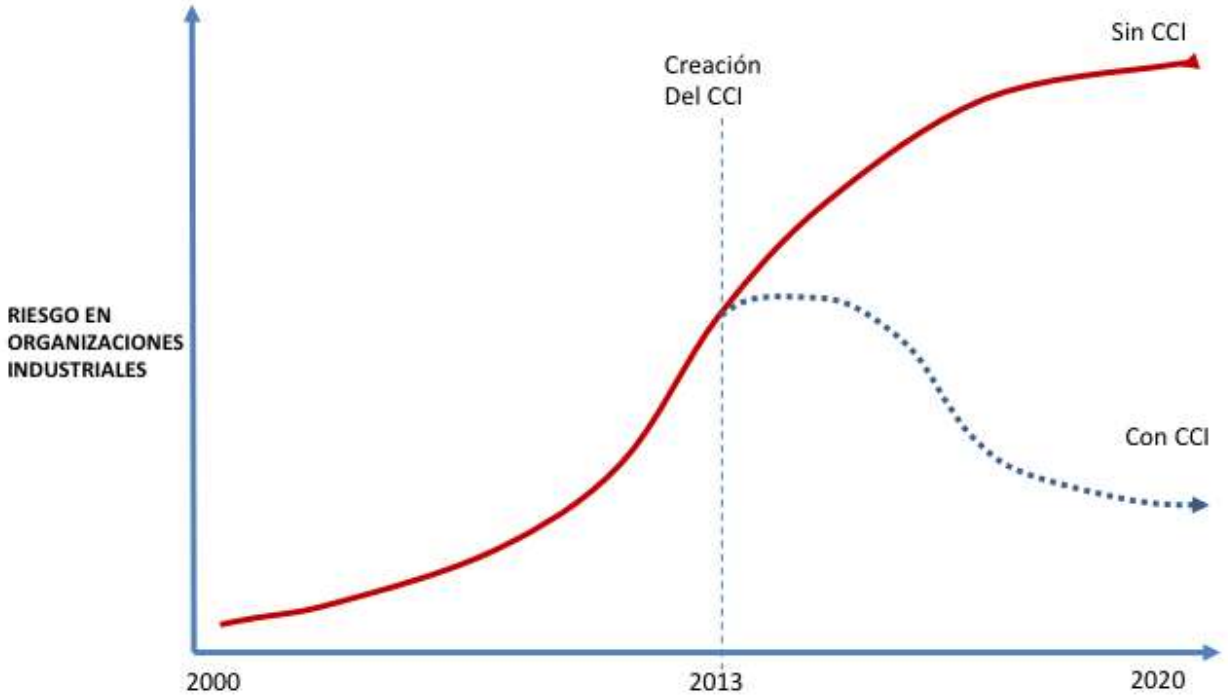
La siguiente fase del Centro, la **de ECOSISTEMA PARA COMPARTIR EXPERIENCIAS**, en la que actualmente nos encontramos, cuenta por tanto con un ecosistema maduro, estable, y de referencia, con grandes expertos entre nuestros miembros y patrocinadores que están aportando conocimiento, experiencias, documentos, análisis y recursos extremadamente valiosos al mercado, además de casos de éxito y numerosos ejemplos de colaboración entre distintos actores del ecosistema, que suponen una referencia para otros países de nuestro entorno. Esta fase de **INTERCAMBIO DE EXPERIENCIAS**, es totalmente necesaria antes de alcanzar el que parece su destino natural -pero para el que aún faltan algunos pasos-: la fase de **COMPARTICIÓN DE INFORMACIÓN**. Llegados a ella, habremos conseguido el grado máximo de inteligencia colectiva de un ecosistema avanzado (artículo: evolución de CCI).

Para afrontar este nuevo reto, **en 2015**, se realizó un análisis profundo de las actividades a desarrollar y de los recursos necesarios para garantizar su éxito, y se decidió reorganizar la composición del equipo directivo, estando compuesto actualmente por los profesionales: Jose Valiente y Susana Asensio (Equipo Directivo CCI), soportado por un amplio elenco de expertos en las distintas áreas de esta disciplina (Equipo de Expertos) que **durante 2018-2019** se centrará, como objetivo principal, en proporcionar herramientas de valor al responsable de ciberseguridad industrial, que es la figura que debe liderar la gestión del riesgo tecnológico en las organizaciones industriales, ingenierías y fabricantes de tecnología industrial. Asimismo, CCI cuenta ya con presencia internacional notable, con Coordinadores regionales en más de 15 países, en distintas áreas geográficas del mundo (Equipo de Coordinadores).

Actualmente, el CCI es el único centro de estas características que nace desde la industria y sin subvenciones, independiente y sin ánimo de lucro, con la misión de impulsar y contribuir a la mejora de la Ciberseguridad Industrial, especialmente en España y Latinoamérica, aunque con visión internacional, 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.

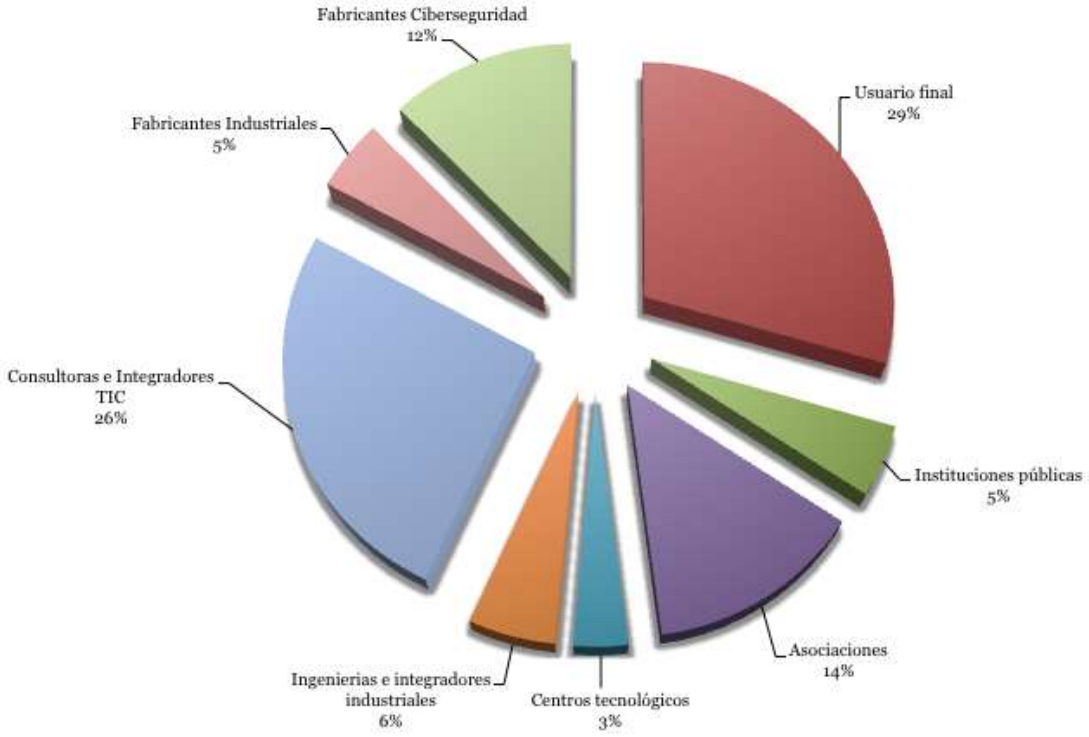
El Centro es ya, hoy en día, el punto independiente de encuentro de los organismos, privados y públicos, y profesionales relacionados con las prácticas y tecnologías de la Ciberseguridad Industrial, así como la referencia hispanohablante para el intercambio de conocimiento.



Representación

El éxito del Centro y la consecución de sus objetivos pasa por contar con la mayor representatividad en el sector industrial involucrando a todos los actores: usuarios finales, fabricantes, ingenierías e integradores, consultoras, gobierno y academia.

Esta es otra de las fortalezas del Centro que supone un hito en el sector TIC e industrial: en apenas unos años de vida, ha logrado involucrar a más de 1.300 miembros y más de 30 patrocinadores de las principales organizaciones internacionales de referencia procedentes de más de 30 países (con principal representación española inicialmente) y con la procedencia que puede verse en la figura siguiente.



Entre sus patrocinadores, se encuentran las principales organizaciones internacionales del ámbito industrial y de la ciberseguridad:

Usuarios finales como ABERTIS, ADMA OPCO, Arkossa, Central Lechera Asturiana, CEPSA, CLH, EDP, Eléctrica de Ceuta, EMASESA (Empresa Metropolitana de Abastecimiento y Saneamiento de Aguas de Sevilla, S.A.), Enagas, ENDESA, FCC Industrial, Gas Natural, Iberdrola, Inditex, Industrial Química del Nalón, Repsol, Sabic, Serviabertis, Gestamp, Enersa o Grupo CMC, ingenierías como Técnicas Reunidas, Initec, Sener, TSK, IDOM, Inerco o Tecnatom, o fabricantes como Checkpoint, Cisco, Fortinet, Honeywell, Juniper, Kaspersky, Mcafee, Panda Security, Red Hat, Siemens, Symantec, Trendmicro, Waterfall o Symantec, son sólo una muestra del ecosistema que integra el Centro, complementado por distintas universidades, entidades públicas y centros tecnológicos (como Tecnalia, el mayor centro tecnológico de España y cuarto de Europa).

Además, tienen un lugar especial aquellas organizaciones y colaboradores con los que existe un marco de colaboración específico en el ámbito de la Ciberseguridad Industrial, entre los que podríamos destacar en España la Fundación Borredá, INCIBE, CNPIC, CCN, ISACA, ISA, ITTI o PESI (Plataforma Española de Seguridad Industrial), en el Reino Unido a ABI Research, IRN y SMi, en Estados Unidos IQPC, en Argentina ISSA e ICIC, o a nivel europeo ENISA, entre otros.

En definitiva, el ecosistema del Centro es su principal valor y su continuo crecimiento y respaldo absoluto de la iniciativa, desde la actividad y recursos, no hace sino confirmar, la relevancia e impacto de la organización.

Conclusiones

No existe mejor forma de cumplir los objetivos marcados, que la sostenibilidad del propio Centro.

Ni mejor demostración de su cumplimiento, que el respaldo real (y económico) de todos los actores. Es la energía imprescindible para su actividad.

Sin duda, es momento de liderar desde el ejemplo (*leading by doing*), y es lo que tenemos la oportunidad de hacer todos nosotros.

Centro de Ciberseguridad Industrial

www.cci-es.org