ESCUELA PROFESIONAL DE
CIBERSEGURIDAD INDUSTRIAL

MÁSTER PROFESIONAL ONLINE DE CIBERSEGURIDAD INDUSTRIAL 2020

CENTRO DE CIBERSEGURIDAD INDUSTRIAL
www.cci-es.org

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

Contenido

- **CCI, CENTRO DE CIBERSEGURIDAD INDUSTRIAL** 4
- **ESCUELA PROFESIONAL DEL CCI** 5
- **M01. MÁSTER PROFESIONAL ONLINE DE CIBERSEGURIDAD INDUSTRIAL** 6
  - OBJETIVOS 7
  - SISTEMA DE CAPACITACIÓN 7
  - A QUIEN ESTÁ DIRIGIDO -RELACIÓN PERFIL PROFESIONAL/FORMACIÓN 8
  - CIBERLEGO INDUSTRIAL DEL CCI 8
  - BLOQUES DE ESTUDIO 9
    - MÓDULO I. CONCEPTOS DE AUTOMATIZACIÓN INDUSTRIAL Y ESTADO DEL ARTE DE LA SEGURIDAD DIGITAL EN LA INDUSTRIA 4.0 9
    - MÓDULO II. DIAGNÓSTICO DE LA CIBERSEGURIDAD INDUSTRIAL 9
    - MÓDULO III. PREPARANDO UN PROGRAMA DE CIBERSEGURIDAD INDUSTRIAL 9
    - MÓDULO IV. HACKING Y ESTRATEGIA DE DEFENSA. 9
    - MÓDULO V. TRABAJO FIN DE MÁSTER 9
  - PLAN DE ESTUDIOS 10
    - MODULO I 10
    - MÓDULO II 11
    - MÓDULO III 11
    - MÓDULO IV 11
    - TRABAJO FINAL DE MÁSTER 11
  - RELACIÓN DE PUBLICACIONES ENTREGADAS DURANTE EL MÁSTER 12
  - ESQUEMA DE FORMACIÓN 13
  - CALENDARIO 2020 14
  - EQUIPO DE PROFESORES 19

CCI, 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, 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 6 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.

Escuela Profesional del CCI

El CCI ha puesto en marcha en 2018 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 6 años de existencia, previamente a la inauguración de la Escuela, 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 (https://www.cci-es.org/profesorado1) del conjunto de cursos, talleres y sesiones de concienciación (inmersiones) que la escuela imparte anualmente está formado por expertos (https://www.cci-es.org/el-equipo/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-analisisestategicos) , así como en algunos de los talleres y cursos ya realizados.

M01.
Máster Profesional Online de Ciberseguridad Industrial

El Máster Profesional de Ciberseguridad Industrial es un título propio del Centro de Ciberseguridad Industrial, CCI.

El Máster Profesional Online de Ciberseguridad Industrial capacita a los profesionales de automatización industrial y a los profesionales de tecnologías de información en los riesgos tecnológicos de los Servicios Esenciales industriales, las redes y sistemas de automatización industrial y SCADA, y a cómo aplicar medidas de protección.

Durante el Máster, el alumno analizará y comprenderá el riesgo asociado a estas infraestructuras y su relación básica con los Sistemas de Control Industrial, lo que es necesario para cualquier profesional de la automatización o seguridad relacionado con áreas como las TIC, energía, industria química y nuclear, fabricación, alimentación o transporte, entre otros; y para ello se profundizará en las siguientes materias:

- Conceptos de ciberseguridad en sistemas de control industrial y protección de infraestructuras críticas y su estado del arte a nivel internacional.
- Análisis de las amenazas y vulnerabilidades de los sistemas de control industrial reconociendo su riesgo asociado.
- Diseño y marco de gestión adecuado en los Servicios Esenciales y entornos industriales.
- Adopción de estándares y recomendaciones aplicables al entorno industrial.
- Diseño de un Programa de ciberseguridad en sistemas de control industrial.
- Aspectos organizacionales y de gestión importantes: Director de TI vs. Director de Seguridad vs. Director de Planta vs. Director de Producción.
- Aplicación de estrategias y técnicas de defensa para la protección de los sistemas de automatización industrial.

Los alumnos recibirán una formación integral de ciberseguridad industrial capacitándoles como responsables de ciberseguridad en un proyecto de automatización o responsables de ciberseguridad en la operación industrial.

El profesorado del máster lidera a nivel internacional el campo de la ciberseguridad industrial.

OBJETIVOS

Al finalizar satisfactoriamente el Máster, el alumno será capaz de:

- Realizar un diagnóstico de ciberseguridad en un entorno industrial tanto a nivel técnico como organizativo.
- Elaborar un programa de ciberseguridad industrial basado en análisis de riesgos y análisis gap de las mejores prácticas y estándares actuales.
- Utilizar técnicas y herramientas de hacking para identificar componentes vulnerables en la infraestructura del sistema de control y SCADA.
- Aplicar estrategias y técnicas de defensa para proteger los sistemas de automatización industrial.

SISTEMA DE CAPACITACIÓN

El Máster comprende cuatro módulos didácticos y un trabajo final de proyecto que supone un ejercicio completo de todo lo aprendido en los módulos.

Cada módulo incluye dos trabajos prácticos y un test que superar.

No existen exámenes teóricos o presenciales.

La nota final del Máster será la media obtenida de los cuatro módulos (superados de forma independiente) más el proyecto; siendo la nota de cada módulo: un 40% cada trabajo (los trabajos son puntuados por la nota obtenida, más la valoración de esfuerzo de cada participante) y un 20% el test.

A QUIEN ESTÁ DIRIGIDO -RELACIÓN PERFIL PROFESIONAL/ FORMACIÓN

El Máster está dirigido a:

- **Profesionales TIC y de Seguridad de la información**
- **Profesional de ciberseguridad en organización industrial; de la automatización industrial, a profesionales de instrumentación y control**
- **Profesional de ciberseguridad en ingeniería o fabricante industrial.**

CIBERLEGO INDUSTRIAL DEL CCI

En el master online se trabajará con la herramienta didáctica CiberLego Industrial que ha sido adaptada a VR (realidad virtual) y AR (realidad aumentada), de forma que los alumnos puedan interactuar con una herramienta que simula la realidad de los entornos industriales.

BLOQUES DE ESTUDIO

MÓDULO I.
CONCEPTOS DE AUTOMATIZACIÓN INDUSTRIAL Y ESTADO DEL ARTE DE LA SEGURIDAD DIGITAL EN LA INDUSTRIA 4.0

Aproximación a la automatización y los sistemas de control industrial. Introducción a las redes y los sistemas de control industrial. Definiciones y explicación de conceptos y componentes claves: SCADA, DCS, RTU, IED, PLC, HMI, FEP, PCS, DCS, EMS, sensores, comunicaciones, wireless (radio, Wifi, microondas, celulares), protocolos (ModBus, ProfiBus OPC, etc.) y capas de red.

Conceptos y estado del arte de la Ciberseguridad en la transformación digital industrial. Definición e identificación de los distintos términos y conceptos claves: Seguridad SCADA, infraestructura crítica, infraestructura estratégica, servicios esenciales, sectores afectados, operadores críticos. Descripción de la situación socio económica actual y el impacto que la Protección de Infraestructuras Críticas y la Seguridad en Entornos de Industria 4.0.

MÓDULO II.
DIAGNÓSTICO DE LA CIBERSEGURIDAD INDUSTRIAL

Análisis y puesta en común del diagnóstico de la Seguridad en Entornos Industriales (visión del usuario, del fabricante, de la organización, de las ingenierías, etc.). Análisis de las Vulnerabilidades y Amenazas de los Sistemas de Control. El perímetro. Vectores de ataque (líneas de comunicación, accesos remotos y módems, accesos de fabricantes, conexiones a bases de datos, manipulaciones del sistema, etc.). Análisis y contramedidas.

MÓDULO III.
PREPARANDO UN PROGRAMA DE CIBERSEGURIDAD INDUSTRIAL

Estándares aplicables. Estableciendo un Programa de Seguridad de Sistemas de Control Industrial. Diseño de un plan de seguridad y protección de la infraestructura crítica. Estructura. Contenido y Aproximación práctica.

MÓDULO IV.
HACKING Y ESTRATEGIA DE DEFENSA

Comprender y aplicar los conceptos relaciones con el diseño de redes seguras. Descubrir y analizar vulnerabilidades en sistemas de control mediante técnicas y herramientas de hacking. Desarrollar y aplicar estrategias y técnicas de defensa.

MÓDULO V.
TRABAJO FIN DE MÁSTER

Se realizará un proyecto en el que se integren todos los contenidos aprendidos.

PLAN DE ESTUDIOS

MODULO I

Aproximación a la automatización y los sistemas de control industrial

- Introducción a la automatización industrial
- La pirámide de automatización
- Tecnologías de automatización
- Sistemas de control industrial
  - Nivel 0: Tecnología de instrumentación
  - Nivel 1: Controladores y DCS
  - Nivel 2: SCADA, HMI e Historiadores
  - Nivel 3: EMS
  - Nivel 4: ERP
- Redes y protocolos industriales
  - Niveles y arquitecturas de comunicación.
  - Medios de comunicación.
- Protocolos industriales.

Conceptos y estado del arte de la Ciberseguridad Industrial

- Introducción
- Descripción de la situación socio económica actual y el impacto que la Protección de Infraestructuras Críticas y la Seguridad en Entornos Industriales.
- Términos y Conceptos. Definición e identificación de los distintos términos y conceptos claves: infraestructura crítica, infraestructura estratégica …
- Relación entre Protección de Infraestructuras Críticas y Ciberseguridad
- Estado del arte internacional de la Protección de Infraestructuras Críticas
  - Estados Unidos y Canadá
  - Latinoamérica
  - Europa
- Aspectos organizacionales
- Director de TI vs. Director de Seguridad
- Director de Planta vs. Director de Producción/Fabricación

MÓDULO II

Diagnóstico de la Ciberseguridad Industrial

› Vulnerabilidades y amenazas en los Sistemas de Control
› Amenazas y vulnerabilidades en el perímetro
› Vectores de ataque
› Análisis y contramedidas
› Diagnóstico de la Seguridad en Entornos Industriales
› Ciclo de vida de un proyecto de diagnóstico de ciberseguridad industrial
› Presentación de resultados.

MÓDULO III

Preparando un programa de Ciberseguridad Industrial

› Análisis de riesgos
› Evaluación de madurez
› Elaboración del programa de ciberseguridad industrial
› Presentando el plan de ciberseguridad a la dirección

MÓDULO IV

Hacking y estrategias de defensa

› Comprender y aplicar los conceptos relaciones con el diseño de redes seguras.
› Descubrir y analizar vulnerabilidades en sistemas de control
› Desarrollar y aplicar estrategias y técnicas de defensa

TRABAJO FINAL DE MÁSTER

Realización de un proyecto que integre todos los contenidos aprendidos. Caso de uso para la preparación de un programa de ciberseguridad industrial aplicando los conocimientos adquiridos durante el máster.

RELACIÓN DE PUBLICACIONES ENTREGADAS DURANTE EL MÁSTER

1.	Operadores de Infraestructuras Críticas españolas 2017	150 €
2.	Documento PIC y CI	- €
3.	El CCI y la Estrategia de Ciberseguridad Nacional de España LR	- €
4.	Análisis forense en SCI 2016	350 €
5.	Desarrollo y despliegue seguro de software industrial	350 €
6.	Documento Buenas prácticas diagnostico	250 €
7.	Guía Bolsillo - Pirámide de Automatización Industrial	- €
8.	Prevención, defensa y respuesta frente a 3 tipos de ciberataques	- €
9.	Ciberseguridad en Ciclo de Vida de proyecto de automatización industrial	350 €
10.	Estrategia Ciberseguridad Nacional	- €
11.	GUIA DE SGCI y plantillas	450 €
12.	Documento Como impacta en el negocio el uso de software sin soporte	- €
13.	Herramientas de evaluación de madurez	300 €
	TOTAL	**2.200 €**

ESQUEMA DE FORMACIÓN

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 laSeguridad 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 máster
› etc.
› Caso práctico

CALENDARIO 2020

El Máster comprende un total de 450 horas de esfuerzo en formación distribuidas de acuerdo con las siguientes actividades:

MARZO

MÓDULO 1 (AV y JV)

05-MAR	12-MAR	18-MAR	31-MAR
Masterclass de 19:00 a 20:30h	Masterclass de 19:00 a 20:30h	Masterclass de 19:00 a 20:30h	
ACCESO A DOCUMENTACIÓN MOD1			ENTREGA PRIMERA ACTIVIDAD
ACCESO A PRIMERA ACTIVIDAD MOD1			ENTREGA SEGUNDA ACTIVIDAD
ACCESO A SEGUNDA ACTIVIDAD MOD1			
ACCESO A FORO MOD1		ACCESO A TEST MOD1	FIN PLAZO TEST MOD1

ABRIL

MÓDULO 2 (CC)

16-ABR	23-ABR	30-ABR	30-ABR
Masterclass de 19:00 a 20:30h	Masterclass de 19:00 a 20:30h	Masterclass de 19:00 a 20:30h	
ACCESO A DOCUMENTACIÓN MOD2			ENTREGA PRIMERA ACTIVIDAD
ACCESO A PRIMERA ACTIVIDAD MOD2			ENTREGA SEGUNDA ACTIVIDAD
ACCESO A SEGUNDA ACTIVIDAD MOD2			
ACCESO A FORO MOD2		ACCESO A TEST MOD2	FIN PLAZO TEST MOD2

MAYO

MÓDULO 3 (AV y JV)

07-MAY	13-MAY	21-MAY	31-MAY
Masterclass de 19:00 a 20:30h	Masterclass de 19:00 a 20:30h	Masterclass de 19:00 a 20:30h	
ACCESO A DOCUMENTACIÓN MOD3			ENTREGA PRIMERA ACTIVIDAD
ACCESO A PRIMERA ACTIVIDAD MOD3			ENTREGA SEGUNDA ACTIVIDAD
ACCESO A SEGUNDA ACTIVIDAD MOD3			
ACCESO A FORO MOD3		ACCESO A TEST MOD3	FIN PLAZO TEST MOD3

JUNIO

MÓDULO 4 (SV)

04-JUN	11-JUN	18-JUN	30-JUN
Masterclass de 19:00 a 20:30h	Masterclass de 19:00 a 20:30h	Masterclass de 19:00 a 20:30h	
ACCESO A DOCUMENTACIÓN MOD4			ENTREGA PRIMERA ACTIVIDAD
ACCESO A PRIMERA ACTIVIDAD MOD4			ENTREGA SEGUNDA ACTIVIDAD
ACCESO A SEGUNDA ACTIVIDAD MOD4		**ACCESO A TRABAJO FINAL**	
ACCESO A FORO MOD4		ACCESO A TEST MOD4	FIN PLAZO TEST MOD4

JULIO

TRABAJO FINAL

31-JUL
ENTREGA TRABAJO FINAL

EQUIPO DE PROFESORES

El equipo de profesores del Máster está formado por expertos y colaboradores del CCI que cuentan con gran experiencia en proyectos de ciberseguridad en entornos de automatización industrial y forman parte del Equipo Docente de la Escuela Profesional CCI (https://www.cci-es.org/profesorado1).

En concreto, la edición 2020 del Máster será impartida por:

CLAUDIO CARACCIOLO
EXPERTO HACKING INDUSTRIAL

Es Coordinador del Centro de Ciberseguridad Industrial en Latinoamérica. Además de:

- Chief Security Ambassador de Eleven Paths
- Presidente de ISSA Argentina (2011-2013 y 2013-2015).
- Socio Fundador de Root-Secure SRL.
- Consultor especialista en Seguridad de la Información con certificaciones internacionales.
- Miembro de asociaciones relacionadas al ambiente como: ISSA International, OWASP, Usuaria, Argentina Cibersegura, Miembro del comité académico de Segurinfo desde el 2007 a la actualidad.
- Orador en una gran cantidad de eventos tanto nacionales como internacionales, inclusive en TEDxUTN 2012 (http://holename.wordpress.com/2012/07/13/tedxutn-de-las-emociones-a-las-experiencias/), LatinCACS, Isaca Lima Full Day, Campus Party Br 2014 y Ec 2011, Owasp Latam Tour 2011/12 y 13, Segurinfo 2007-2014, 8dot8 (2011-2014) entre otros grandes eventos
- Instructor sobre temas relacionados con Ethical Hacking, Metodologías de Defensa, Hardering de Plataformas, Seguridad Web, Técnicas Anti-Forenses.
- Apasionado por la Ingeniería Social.
- Autor junto a sus socios en Root-Secure del libro "Ethical Hacking, un enfoque metodológico" publicado por Editorial Alfaomega con ISBN-13: 978-9871609017
- Co-Organizador del evento MS Doing Blue en Buenos Aires.

Más información http://claudiocaracciolo.com.ar/@holesec
Claudio Caracciolo https://www.linkedin.com/in/claudiocaracciolo/

AGUSTÍN VALENCIA GIL-ORTEGA
EXPERTO EN CIBERSEGURIDAD
DE INFRAESTRUCTURAS CRÍTICAS

Ingeniero Industrial por ICAI, con formación adicional en distintos ámbitos como Gestión de Mantenimiento, Tecnología Nuclear BWR y más recientemente Director de Seguridad y Master de Seguridad Informática. Con más de 15 años de experiencia, ha cubierto todos los ámbitos del mundo de la energía, desde Ingeniería a Operación y Mantenimiento en centrales de ciclo combinado y nuclear.

Desde 2011, responsable de ciberseguridad en sector nuclear. Liderando desarrollo de planes y análisis de riesgos de ciberseguridad en infraestructuras críticas de acuerdo con Ley PIC. También como Jefe de Ingeniería de proyectos de instrumentación y control y ciberseguridad, modernizando plataformas de control distribuido e introduciendo ciberseguridad desde el diseño o rediseñando arquitecturas de redes y sistemas de control enfocado a bastionado, segmentación de redes, whitelisting y SIEM-IDS sobre sistemas de los principales fabricantes (GE, Honeywell, Schneider-Electric, etc).

Actualmente Responsable de OT en el área de Ciberseguridad Global de Iberdrola, coordinando estrategias OT entre los distintos negocios de su corporación (Generación, Renovables, Redes, Smartgrids) y colaborador con ISA 99/62443 para dispositivos de campo y con ISA84/61511 para integración con 62443.

Agustín Valencia Gil-Ortega
https://www.linkedin.com/in/agustin-v-6035849/?originalSubdomain=es

JOSÉ VALIENTE
EXPERTO ES SISTEMAS DE GESTIÓN DE CIBERSEGURIDAD

José Valiente es Director y Responsable de Coordinación 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 https://www.linkedin.com/in/jvaliente/

SILVIA VILLANUEVA
EXPERTA EN HACKING INDUSTRIAL

Con más de 15 años de experiencia en gestión de riesgos tecnológicos, y con un perfil multidisciplinar que combina áreas de seguridad tanto técnicas como estratégicas, Silvia ha centrado su carrera en gestionar y realizar múltiples proyectos en el ámbito de la Seguridad y Protección de la Información.

Pionera en España en Seguridad Industrial, especializada en Bastionado de Servidores y Revisiones de Seguridad, Análisis y Diseño de Arquitectura de Red y Seguridad en Redes SCADA/ICS/DCS. Adicionalmente dispone de las certificaciones CISSP y CSSLP de ISC2, CISM y CISA de ISACA, CEH de EC-COUNCIL, CSSA de IA Certification y GISCP (Industrial Cyber Security Ceritification) de GIAC, estando esta última focalizada en Ciberseguridad Industrial.

Silvia Villanueva https://www.linkedin.com/in/silviavillanueva/

Paseo de las Delicias, 30 · 2º piso
28045 MADRID
+34 910 910 751
info@CCI-es.org
www.CCI-es.org
blog.CCI-es.org
@info_CCI