Cursos de postgrado

35 créditos

Curso académico 2017-2018

Ciberseguridad en Sistemas de Control Industrial, ICS/SCADA

del 15 de enero al 14 de septiembre de 2018

DIPLOMA DE EXPERTO UNIVERSITARIO

Características: prácticas y visitas, material impreso, material multimedia, actividades presenciales obligatorias, curso virtual y guía didáctica.

Departamento
Informática y Automática
E.t.s. de Ingeniería Informática

PROGRAMA DE POSTGRADO
Máster, Diploma de Especialización, Diploma de Experto y Certificado de Formación del Profesorado.
Curso 2017/2018

El Programa de Postgrado acoge los cursos que dan derecho a la obtención de un Título Propio otorgado por la UNED. Cada curso se impartirá en uno de los siguientes niveles: Máster, Diploma de Especialización, Diploma de Experto y Certificado de Formación del Profesorado.

Requisitos de acceso:

Estar en posesión de un título de grado, licenciado, diplomado, ingeniero técnico o arquitecto técnico. El director del curso podrá proponer que se establezcan requisitos adicionales de formación previa específica en algunas disciplinas.

Asimismo, de forma excepcional y previo informe favorable del director del curso, el Rectorado podrá eximir del requisito previo de la titulación en los cursos conducentes al Diploma de Experto Universitario. Los estudiantes deberán presentar un curriculum vitae de experiencias profesionales que avalen su capacidad para poder seguir el curso con aprovechamiento y disponer de acceso a la universidad según la normativa vigente.

El estudiante que desee matricularse en algún curso del Programa de Postgrado sin reunir los requisitos de acceso podrá hacerlo aunque, en el supuesto de superarlo, no tendrá derecho al Título propio, sino a un Certificado de aprovechamiento.

Destinatarios

Será requisito mínimo para matricularse en los cursos del Programa de Postgrado que el estudiante esté en posesión del título de licenciado, graduado, diplomado, ingeniero técnico, arquitecto técnico o equivalente según los sistemas educativos de los diferentes países. Dicha equivalencia será valorada por el director del correspondiente curso y, en todo caso, autorizada por el Vicerrectorado competente. En cualquier caso, dicho informe y autorización para matricularse en el curso no tendrá efecto alguno sobre posibles homologaciones de las titulaciones presentadas por los candidatos.

Asimismo, de forma excepcional y previo informe favorable del director del curso, el Rectorado podrá eximir del requisito previo de la titulación a aquellos estudiantes que presenten un curriculum vitae de experiencias profesionales que avalen su capacidad para poder seguir el curso con aprovechamiento, siempre y cuando dispongan de acceso a la universidad según la normativa vigente. El director del curso podrá proponer que se establezcan requisitos adicionales de formación previa específica en algunas disciplinas.

El curso va dirigido a todos aquellos estudiantes o profesionales con los siguientes perfiles:

- Alumnos o titulados de Grado Ingeniería Informática, ingenieros en Informática, telecomunicaciones e industriales así como alumnos que desarrollen o hayan desarrollado en su formación módulos relativos a las TIC.
- Profesionales tales como analistas de ciberseguridad, y/o trabajadores inmersos en desarrollo, control y vigilancia de procesos industriales y Jefes de Seguridad de empresas en donde se lleven a cabo procesos industriales automatizados y se gestionen y controlen a través de sistemas ICS/SCADA.
- Profesionales del mundo de la seguridad (Fuerzas y Cuerpos de Seguridad, militares, seguridad privada, etc.) que deseen darle a su currículo un perfil de especialización en ciberseguridad en sistemas de control industrial.
- Todo aquel personal que sin poseer un perfil excesivamente especializado desde el punto de vista técnico desee ampliar su formación o funciones laborales concretas en el campo de la ciberseguridad como rama de especialización.
- El curso CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL ICS/SCADA cuenta con una proyección en materia colaborativa con diferentes entidades que a lo largo del curso se irán comunicando, puesto que, en el momento de la elaboración de esta guía, se están concretando. Se mantendrá convenientemente informados a los alumnos de los posibles acuerdos en materia formativa, becas e incluso bolsas de trabajo.

Esto representa para el alumnado una oportunidad más de acceder al mercado laboral.

1. Presentación y objetivos

El fenómeno de la ciberseguridad no es nuevo: desde los tiempos de Kevin Mitnick tanto la literatura como el cine nos han ido presentando dicha problemática de manera más o menos acertada, mediante historias en las que una o varias personas,muchas veces jóvenes sin malicia, lograban introducirse en los sistemas centrales del gobierno saltándose las medidas de seguridad o encontrando una puerta trasera.

La realidad a la que actualmente nos enfrentamos hoy en día ha rebasado con mucho la ficción: el hacker ya no es un solitario sin ánimo de lucro, sino todo lo contrario: poderosas mafias internacionales y agencias de inteligencia pujan por el control de una actividad en la que cualquier pieza de información que se pueda obtener tiene un valor: datos personales, bancarios, historiales médicos, secretos industriales, etc . Es un mercado boyante donde todos somos víctimas propicias. Y de todas las víctimas,las empresas e industrias son las más jugosas.

La cantidad que se puede llegar a pagar en el mercado negro por conseguir parar la producción de una planta industrial mediante el ataque remoto a sus sistemas de control puede ser millonaria. El valor estratégico de dichas operaciones es incalculable, en este nuevo escenario las guerras y conflictos ya no se desarrollan de forma tradicional, sino mediante la especulación en los mercados internacionales y la realización de operaciones ofensivas y de espionaje en el ciberespacio. La lista de incidentes de gran envergadura, así como su complejidad, no deja de crecer: Stuxnet, Shamoon,Octubre Rojo

En este contexto, estamos hablando ya no sólo de robo de información, sino de aquellas instalaciones que prestan servicios esenciales para la población (electricidad, transporte, agua, alimentación), esto es, las infraestructuras críticas. En este entorno el profesional de la ciberseguridad es un perfil cada vez más demandado y puesto en valor, y dentro de éstos el especialista en gestionar la ciberseguridad industrial.

Por ello, la UNED ha considerado el ofrecer este curso, el primero especializado en introducir al estudiante en la ciberseguridad de los entornos de control industrial, desde una perspectiva holística, que abarque todo aquello que el profesional que desarrolle su labor en este campo deba conocer: legislación que le afecta, principales técnicas utilizadas tanto por atacantes como por responsables de la ciberseguridad,principales estándares y guías de buenas prácticas, cómo implementar correctamente la ciberseguridad de una instalación, cómo reportar un incidente,etc., todo ello enfocado a formar a los presentes y futuros responsables de gestionar

correctamente las líneas defensivas de la ciberseguridad de una planta de producción industrial. Es un curso cuyo principal ánimo es ser un activo en el currículo del estudiante, y que a buen seguro representa un valor diferencial en el mercado laboral de la ciberseguridad.

2. Contenido

TEMA 1. INTRODUCCIÓN A LA LEGISLACIÓN Y NORMATIVA RELATIVA A LA CIBERSEGURIDAD INDUSTRIAL

Visión general de todaaquella normativa que de una manera u otra afectará a su actividad comoresponsable de la ciberseguridad de una planta industrial.

- Legislación y normativa, conceptos básicos.- Cibercriminalidad en la UE

- Código Penal español

- Infraestructuras Críticas

- Iniciativas legislativas nacionales en materia de ciberseguridad industrial

- Estrategia de Ciberseguridad Nacional

- Agenda Digital para España

TEMA 2. INTRODUCCIÓN A LA CIBERSEGURIDAD

Repaso a los principales conceptos relativos ala ciberseguridad que el profesional debe de conocer para su adecuada gestión.

- Introducción a la monitorización de seguridad en redes

- Productos para la monitorización de seguridad en redes

- Procesos de monitorización de seguridad en redes

- El personal de monitorización de seguridad en redes

- El intruso contra la monitorización de seguridad en redes

TEMA 3. ORGANIZACIONES NACIONALES E INTERNACIONALES

Breve recorrido por las principalesorganizaciones tanto a nivel nacional como internacional.

- Organizaciones Nacionales

- Organizaciones Europeas

- Organizaciones Internacionales

TEMA 4. GUÍAS DE BUENAS PRÁCTICAS, ESTÁNDARES Y NORMAS

Se analizan los textosmás significativos de las entidades descritas en el tema anterior, profundizando enlos elaborados por entidades nacionales y, por lo tanto, más vinculantes ycercanos al operador de infraestructuras controladas mediante sistemas ICS/SCADA.

- Documentos,estándares y guías de buenas prácticas.

- Otros documentos de interés de ámbito nacional en España y otros países.

TEMA 5. INTRODUCCIÓN A LOS SISTEMAS DE CONTROL INDUSTRIAL ICS/SCADA

Se tratan los conceptos y definiciones que engloban a lossistemas de control industrial (Industrial Control System I.C.S.) así como lacatalogación en un sentido más amplio de todos aquellos dispositivos encargadosde monitorizar y recopilar información para el control.

- Introducción a los sistemas de control industrial (ICS / SCADA)

- Norma ISA- 95.

- Descripción de los Niveles propuestos por la Norma ISA-95

- Conceptos base en sistemas de control industrial.

TEMA 6.IMPLANTACIÓN DE LA CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL ICS/SCADA

Se muestran los riesgos existentes para estos sistemas, poniendo en práctica unescenario que nos marque las pautas desde la motivación para atacar estos entornos, hasta el efecto queesto pudiera desencadenar pasando por la identificación y análisis de losriesgos potenciales.

- Safety.

- Security.

- ¿Por qué es diferente la seguridad respecto a otros elementos de las tecnologías de la información?.

- Aspectos básicos de Seguridad de Redes.

- Descubrimiento de riesgos en los sistemas SCADA.

- Vulnerabilidades SCADA.

- Contra medidas.

- Ingeniería social.

- Recomendaciones de seguridad.

TEMA 7. REPORTE DE CIBERINCIDENTES

Puesta en conocimiento del ¿ecosistema de laciberseguridad¿ nacional, que van desde los CERTs que la administración públicaespañola pone a disposición del profesional hasta las capacidades deinvestigación y persecución del delito por parte de las Fuerzas y Cuerpos deSeguridad del Estado.

- Qué es un CERT. CERTs nacionales.

- Incidentes: tipologías más comunes.

- Reporte de incidentes. Gestión de un ciberincidente por parte de un CERT.

- Reporte en infraestructuras críticas. Enlace con Fuerzas y Cuerpos de Seguridad.

3. Metodología y actividades

Se utilizará la metodología de e-learning que se define como «la utilización de las nuevas tecnologías multimedia y de Internet, para mejorar la calidad del aprendizaje facilitando el acceso a recursos y servicios, así como los intercambios y la colaboración a distancia » y que se caracteriza por:

a) Se realiza en red, lo que permite una actualización y distribución inmediata de los contenidos y la información;

b) Se hace llegar al usuario final a través de un ordenador utilizando estándares de Internet;

c) Está centrada en la más amplia visión de soluciones al aprendizaje que vayan más allá de los paradigmas tradicionales de la formación. En este curso sólo una parte del material está impreso. El resto se proporcionará mediante entrega en formato pdf a través de los medios y soportes que se estimen oportunos. Además en la plataforma donde se aloja el curso virtualizado existe una zona de descarga de materiales donde estarán las actualizaciones de los mismos.

La evaluación consistirá en la realización de varios trabajos prácticos fortalecidos todos ellos con búsquedas de documentación principalmente en publicaciones oficiales del mundo científico-universitario.

4. Material didáctico para el seguimiento del curso

4.1 Material obligatorio

4.1.1 Material enviado por el equipo docente (apuntes, pruebas de evaluación, memorias externas, DVDs, ...)

- Normativa, Legislación y Directivas UE.

· Guías, estándares,normativas técnicas y buenas prácticas nacionales e internacionales.

· Documentación nacional e internacional que se vaya generando y que por parte del equipo docente se considere de interes.

- SIEMENS, en su colaboración con el mundo universitario y a través del acuerdo gestionado desde el equipo docente del curso, cede (con carácter exclusivamente formativo) un uso por un periodo de 365 días, a los alumnos que se matriculen en el curso, una licencia del siguiente software:

SIMATIC STEP 7PROFESSIONAL

2010 SR4 / V13 SP1COMBO

ENGINEERING-SW

SOFTWARE AND

DOCUMENTATION ONDVD;

6 LANGUAGES:GE,EN,IT,FR,SP,CN;

EXECUTABLE UNDER

WINDOWS 7 (32 BIT,64 BIT);

FOR CONFIGURATIONOF

SIMATICS7-1200/1500,

SIMATICS7-300/400/WINAC,

SIMATIC BASICPANELS;

Todo ello para que el alumno no encuentre ningún problema y se le aporte calidad a la hora de la realización de la/s prácticas que le sean encomendadas."

4.2 Material optativo, de consulta y bibliografía

4.2.1 Material editado y de venta al público

Hacking y seguridad en Internet

Autores	Ramos Varón, Antonio Ángel
Editorial	Ra-Ma S.A. Editorial y Publicaciones
Edición	2011
Precio aproximado	33.56€
ISBN	8499640591

Puede adquirir dichos materiales a través de la Librería Virtual de la UNED.

4.2.2 Otros Materiales

El **Centro de Ciberseguridad Industrial** (www.cci-es.org) cede gratuitamente a los alumnos documentación valorada en 500 €, y que representa un aporte fundamental a la biblioteca del experto en esta materia:

- La Protección de Infraestructuras Críticas y la Ciberseguridad Industria

- Buenas prácticas para el Diagnóstico de Ciberseguridad en Entornos Industriales

5. Atención al estudiante

Las tutorías se realizarán preferentemente a través del foro del curso. El objetivo de este foro es que sirva como canal preferente de comunicación entre los participantes para que se fomente el intercambio de opiniones, experiencias, recomendaciones y, en general, todo aquello que se considere interesante para llevar a buen fin los objetivos del curso.

Santiago González González, tlfno: 696400360

Rafael Pedrera Macías, tlfno: 644793228.

Ricardo Nieto Salinero, tlfno:650140056

Horario: de lunes a viernes de 18:00 a 20:00 hrs

Email del equipo docente: srr.ics.scada@gmail.com

6. Criterios de evaluación y calificación

Se considerará aprobado el curso y se expedirá el correspondiente Título con la superación del 50% del conjunto de la nota obtenida, tanto de la parte teórica como práctica. Para la evaluación se tendrá en cuenta:

· Actitud participativa del alumno *(10%)*

· Acceso a la plataforma *(*módulo de contenidos, glosario, utilización de enlaces web y bibliografía complementaria, etc.*) (15%)*

· Participación en foros y chats *(15%)*

· Entrega de actividades *(50%)*

· Realización de consultas y utilización del resto de herramientas de comunicación *(10%)*

La evaluación consistirá en la realización de varios trabajos prácticos fortalecidos todos ellos con búsquedas de documentación, principalmente en publicaciones oficiales del mundo científico-universitario *(*papers*)*. Esta aportación permitirá al alumnado descubrir posibles vías de investigación y profundización en el campo de la ciberseguridad ICS/SCADA.

7. Duración y dedicación

Del 15 de enero de 2018 al 14 de septiembre de 2018.

Para el buen seguimiento del curso, los temas se irán liberando paulatinamente así como la documentación extra que se aporte. De esta manera se pretende dar una continuidad a los temas desarrollados y que así el alumnado se sienta cómodo según transcurra el tiempo del curso, viendo la interrelación que conllevan todos los campos a tratar.

8. Equipo docente

Director/a

Director - UNED

DORMIDO CANTO, SEBASTIAN

Directores adjuntos

Director adjunto - Externo

GONZÁLEZ GONZÁLEZ, SANTIAGO

Colaboradores UNED

Colaborador - UNED

DORMIDO BENCOMO, SEBASTIAN

Colaborador - UNED

SANCHEZ MORENO, JOSE

Colaboradores externos

Colaborador - Externo

NIETO SALINERO, RICARDO

Colaborador - Externo

PEDRERA MACÍAS, RAFAEL

9. Precio público del curso

Precio público de matrícula: 980 €

10. Matriculación

Del 7 de septiembre al 15 de diciembre de 2017.

Teléfonos: 91 3867275 / 1592

Fax: 91 3867279

http://www.fundacion.uned.es/