CURSO PROFESIONAL

INTRODUCCIÓN A LA CIBERSEGURIDAD INDUSTRIAL PARA INGENIEROS

Objetivos:

COITIVIGO pone en marcha este curso en colaboración con la Escuela de Ingeniería Industrial e INCIBE, dirigido a estudiantes y titulados de la Rama Industrial, con el que se pretende cubrir la demanda de profesionales con formación básica en Ciberseguridad Industrial, para el desempeño de funciones en entornos con presencia de sistemas de información y de las comunicaciones, colaborando en el desarrollo e implantación de políticas y medios de ciberseguridad en ambientes industriales en colaboración con profesionales de este ámbito en el marco de la normativa en vigor.

Dirigido a:

Personal de Ingeniería que deseen complementar su conocimiento del diseño e implementación de sistemas industriales (automatización, comunicaciones, etc.) con el manejo de los conceptos, métodos y políticas propios de la ciberseguridad, un ámbito profesional con una importante demanda de profesionales formados adecuadamente.

Metodología:

El curso se realiza a través de la modalidad de **formación semipresencial**, combinando las explicaciones teóricas del profesor con ejemplos prácticos de aplicación donde sea posible, y con ejercicios a desarrollar por el alumno de forma autónoma e individual (30 horas).

Ponentes:	Belén Pérez Rodríguez (profesional de la seguridad en sistemas TIC, coordinadora del curso), junto con otros miembros del Grupo de Ciberseguridad Industrial de COITIVIGO con formación específica y adecuada a los temas a impartir.
Fecha/Horario:	23 de enero a 23 de febrero, lunes y jueves, de 16:00 h. a 21:00 h.
Duración:	80 horas: 50 presenciales + 30 no presenciales.
Lugar:	Escuela de Ingeniería Industrial, Sede Campus (antigua Escuela de Ingenieros Industriales). Campus Lagoas-Marcosende – Vigo.
Nº de Plazas:	Mínimo 15; Máximo 25 plazas.
Matrícula:	No colegiados: 250 € Colegiados y alumnos pre-asociados: 150 €, i/ subvención colegial (la pre-colegiación no supone coste alguno). NOTA: Los ingresos de esta actividad se dedicarán de forma íntegra a la formación en Ciberseguridad Industrial.
Preinscripción:	Se realizará a través de la Web de COITIVIGO, (http://www.coitivigo.es), en el apartado → "**Formación" → "Actividades Programadas"** Formulario de inscripción: http://www.coitivigo.es/inscrip-ciberseg-ingenieros-2017

La **fecha tope** para la recepción de las preinscripciones finaliza el **viernes**, **13 de enero.**

Jorge Cerqueiro Pequeño – Decano

NOTAS

Requisitos: Este curso es de nivel introductorio, sin otros conocimientos previos necesarios que los adquiridos a lo largo de la titulación, o del ejercicio profesional habitual.

Documentación: Cada asistente tendrá a su disposición las diapositivas de las clases impartidas para el adecuado seguimiento del curso, así como material complementario para el desarrollo de las actividades individuales, y una sugerencia de lecturas para ampliar conocimientos.

Certificado de asistencia: A los participantes que acrediten una asistencia de al menos el 80% de horas de la duración del curso se les hará entrega de un certificado acreditativo de la asistencia y aprovechamiento.

Asignación de plazas: La asignación de plazas se realizará por riguroso orden de preinscripción y a los seleccionados se les comunicará personalmente los detalles relativos al pago de la matrícula. El Colegio se reserva el derecho a cancelar el curso si no se alcanzase el mínimo de inscritos indicado.

Equipos informáticos: Existen ordenadores en el aula en que se impartirá el curso, pero con determinadas limitaciones respecto a trabajar como administradores del sistema. **Es recomendable, si se desea optimizar el aprovechamiento del curso, que cada alumno lleve su propio ordenador portátil. No es necesario disponer de software específico, ya que el necesario se proporcionará a lo largo del curso**

PROGRAMA

PARTE TEÓRICA:

TEMA 01: ¿QUÉ ES LA CIBERSEGURIDAD? ¿POR QUÉ ME INTERESA COMO INGENIERO?
INTRODUCCIÓN: Conceptos, “Safety” vs. “Security”, objetivos, principios, etc.

TEMA 02: ¿POR QUÉ ES IMPORTANTE LA CIBERSEGURIDAD EN LA EMPRESA?
ESCENARIOS Y ELEMENTOS: Activos, vulnerabilidades, amenazas, plan de seguridad, plan de protección, planes de contingencia, etc.

TEMA 03: ¿QUÉ DE MALO PUEDE PASAR?
AMENAZAS: Ataques y orígenes.

TEMA 04: ¿CÓMO FUNCIONAN LAS COMUNICACIONES EN RED?
NETWORKING: Modelos OSI/TCP, direccionamiento, protocolos, servicios, DHCP, NAT, IPv5, IPv6, etc.

TEMA 05: ¿QUÉ TIPOS DE REDES INFORMÁTICAS HAY EN UNA EMPRESA?
REDES: LAN, WAN, WLAN, elementos físicos y lógicos.

TEMA 06: ¿SON SEGURAS LAS REDES INFORMÁTICAS?
SEGURIDAD EN REDES: Servicios: navegación web, email, intercambio de información, cloud, virtualización, servidores de intercambio de archivos (FTP, NFS, CIFS), etc.

TEMA 07: ¿POR QUÉ EXISTEN LOS PROGRAMAS MALICIOSOS?
CÓDIGO MALICIOSO: Virus, troyanos, APT, etc.

TEMA 08: **¿CÓMO SE PUEDE ESCONDER Y/O PROTEGER LA INFORMACIÓN?**
CRIPTOGRAFÍA BÁSICA: Seguridad por contraseña, tipos y complejidad de claves, modalidades de encriptación, etc.

TEMA 09: **¿CÓMO DEBEMOS ACCEDER A LAS REDES DE FORMA SEGURA?**
ACCESO EXTERNO: Redes abiertas, portales cautivos, redes móviles, telefonía, túneles, VPN, virtualización, etc.

TEMA 10: **¿CÓMO PODEMOS PROTEGERNOS DE LAS TRAMPAS DE LA RED DIRIGIDAS A NOSOTROS?**
INGENIERÍA SOCIAL: Riesgos, estrategias de protección, etc.

TEMA 11: **¿ES SEGURO COMPRAR Y VENDER EN LA RED?**
E-COMMERCE: Aplicaciones y sistemas.

TEMA 12: **¿CÓMO SE PUEDEN EVALUAR LOS RIESGOS EN CIBERSEGURIDAD?**
RIESGO Y CONTROL: Evaluación y normativa (ISO 27000, LOPD, CP, CC, LPIC, MAGERIT, NIST, …).

TEMA 13: **¿CÓMO SE PUEDE HACER MÁS SEGURA UNA RED INFORMÁTICA?**
SEGURIDAD PERIMETRAL: Firewall, IDS (Host-IDS, Network-IDS), IPS, WAFs, honeypots, etc.

TEMA 14: **¿CÓMO SON LOS SERVIDORES DE EMPRESA?**
DATA CENTER: Instalaciones y servicios.

TEMA 15: **¿CÓMO SE PUEDE EVALUAR LA SEGURIDAD DE UNA RED?**
AUDITORÍAS DE SEGURIDAD: Tests de penetración.

TEMA 16: **¿QUÉ SE DEBE HACER DESPUÉS DE SUFRIR UN ATAQUE?**
ANÁLISIS FORENSE: Recogida y análisis de evidencias.

TEMA 17: **¿CÓMO SON LAS COMUNICACIONES EN LAS INSTALACIONES DE PRODUCCIÓN?**
COMUNICACIONES INDUSTRIALES: Introducción a las redes industriales y a los buses de campo.

TEMA 18: **¿CÓMO SE APLICA LA CIBERSEGURIDAD A LOS SISTEMAS INDUSTRIALES?**
SISTEMAS DE CONTROL INDUSTRIALES: Aplicación de los principios de ciberseguridad a sistemas de control basados en PLCs, PCs industriales, SCADA, etc.

PARTE PRÁCTICA:

PRÁCTICA 01: **NETWORKING:** Topologías de red, IPv5 e IPv6.

PRÁCTICA 02: **CRIPTOGRAFÍA:** Creación y utilización de claves simétricas y asimétricas.

PRÁCTICA 03: **INGENIERÍA SOCIAL:** Ejercicio práctico en el entorno del alumno.

PRÁCTICA 04: **EVALUACIÓN DE RIESGOS:** Estudio de un caso real.

PRÁCTICA 05: **AUDITORÍA DE SEGURIDAD:** Test de penetración sobre un sistema de laboratorio.

PRÁCTICA 06: **TRABAJO FIN DE CURSO:** Securización de un Sistema de Control Industrial.