Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Master Universitario en Ingeniería Industrial
Facultad/Escuela:	Escuela de Postgrado y Formación Permanente
Asignatura:	Ciberseguridad Industrial
Tipo:	Obligatoria
Créditos ECTS:	3
Curso:	2
Código:	8276
Periodo docente:	Tercer semestre
Materia:	Tratamiento de Datos, Inteligencia y Aprendizaje
Módulo:	
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	75

Equipo Docente	Correo Electrónico
juan Ignacio Istúriz Lázaro	
Francisco Martín Abreu	francisco.martin@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

En esta asignatura el alumno aprenderá los conceptos básicos en torno a la ciberseguridad en la industria y se capacitarán para poder involucrarse en la implementación de la ciberseguridad en los procesos industriales. Mediante casos de estudio reales y prácticas, los estudiantes se familiarizarán con los procesos y herramientas necesarios para la protección de los procesos industriales frente a los ciberataques.
En concreto, los grandes bloques del curso serán:
1. Conceptos básicos, tipos de amezas y tecnologías base
2. Herramientas y servicios disponibles
3. Normativas, estándares y mejores prácticas

OBJETIVO

El objetivo final es que cada alumno tenga un conocimiento básico de las principales normativas, tendencias y elementos que configuran el mundo de la Ciberseguridad en el entorno industrial. De esta forma estará capacitado para involucrarse en los proyectos de protección de los procesos industriales frente a los distintos tipos de ciberamenazas.

CONOCIMIENTOS PREVIOS

Fundamentos de Informática y Redes TCP/IP

CONTENIDOS

1.1. Breve historia de la Ciberseguridad y ámbitos de la Ciberseguridad: Ciberataques contra las personas, contra las empresas, contra los gobiernos, contra la infraestructura e IoT. IA cibersecurity
1.2. Origen de los cibercriminales: Naciones, Terroristas, Espías industriales, Mafias de Crimen Organizado, Ciberdelincuentes en general, Trabajadores descontentos
2.Conceptos Básicos de Ciberseguridad
2.1. Ciberseguridad y Seguridad de la Información
2.2. Principios de la Seguridad de la Información
2.3. Etapas de un ciber-ataque
2.4. Clasificación de los ciber-ataques:
2.4.1. Según el sistema atacado: Computadores, Móviles, Redes, Infraestructuras, Personas
2.4.2.Según la relación del “target” con el atacante: “insider”, “outsider”
2.4.3. Según el impacto en el sistema atacado: activos, pasivos
2.4.4. Según el tipo de crimen: Ciber espionaje, Ciber terrorismo, Guerra cibernética, ciber asesinato, ciber crimen en general
2.4.5. Según el tipo de “Weaponization”: troyanos, macros, crackers, sql-injection, ataques xss, DDoS, backdoor, spoofing, snooping, man-in-yhe-middle
2.4.6. Según el mecanismo de “Delivery”: worm, spam, phishing, spear phishing, whale phishing, command and control, drive by, intrusion, zero-day exploit
2.4.7. Según el tipo de “Instalación”: aplicación, virus, rootkit, apt
2.4.8. Según la acción en el objetivo: spyware, keylogger, banker, adware, ransomware, credentials theft, crypto currency malware, bot, denegación de servicio, destrucción de datos, alteración de datos, toma de control del sistema, daño físico, muerte
3. “Best Practices”
3.1. ISO 27001 3.2. Prevención, Respuesta y Recuperación
3.3. Control de accesos a recursos
3.4. Política actualizaciones software
3.5. Business continuity and disaster recovery plan
3.6. Herramientas de seguridad preventivas
3.7. Security Information Event Monitoring
3.8. Implementación de un "Computer Security Incident Response Team" -CSIRT-
3.9. IoT Security
3.10. IA Security
3.11. Protección de infraestructuras
3.12. Protección de sistemas automatizados de producción. IEC 62433
3.13. Auditorías de ciberseguridad
3.14. Penetration Testing y Vulnerability Assessment
3.15. Hacking ético
3.16. “Best Practices” por parte de los usuarios: uso de correo electrónico de la web y las aplicaciones. Gestión de datos
4. Técnicas usadas por las herramientas de ciberseguridad
4.1. Control de autenticación y accesos
4.2. Encriptado
4.3. Control de flujos de tráfico
4.4. BBDD reputación

4.5. BBDD firmas
4.6. BBDD botnets
4.7. BBDD de centros de comando y control
4.8. Listas blancas y negras
4.9. Análisis heurístico
4.10. Machine Learning
4.11. Sandboxing
4.12. Patrones de tráfico
5. Mecanismos de entrega de la ciberseguridad
5.1. “End-Point” Stand-alone
5.2. Gateway
5.3. Managed Security Service Provider (MSSP)(SOC)
5.4. SECurity as a Service (SECaSS)
5.5. Hybrid Mechanisms
5.6. Mobile Threat Defense (MTD)
5.7 SASE
6. Tipos de Herramientas de Ciberseguridad
6.1. Anti-Malware: Anti-virus, Anti-Phishing, Anti-Spam, Anti-spayware, Anti-tracking, Ad-blocking (Anti-pop-ups), Filtrado de Contenido (Control Parental)
6.2. Firewall
6.3. Proxy
6.4. Secure Web Gateway
6.5. IDS/IPS
6.6. Data Leak Prevention (DLP)
6.7. Unified Thread Management (UTM)
6.8. Sandboxing
6.9. Anti-DDoS
6.10. MTD
6.11. IoT security tools
6.12. CASB
6.13. Firewall de aplicaciones
6.14. Sistemas de ofuscación
6.15. Encriptación (VPN, HTTPS, encriptado almacenamiento…)
6.16. SIEM
7. Normativas y estándares
7.1. ISO 27001
7.2. GDPR
7.3 IEC 62433

ACTIVIDADES FORMATIVAS

A1 Clases teórico- prácticas y seminarios, conferencias…
A2 Laboratorios, talleres, prácticas…
A3 Tutoría
A4 Aula Virtual (seguimiento docencia, foros/ chats, tareas, trabajos individuales y/o material docente)
A5 Trabajo Autónomo. (Estudio teórico, Estudio práctico, Actividades complementarias...)
A6 Evaluación

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
24,75 horas	50,25 horas

COMPETENCIAS

Competencias básicas

Poseer las habilidades de aprendizaje que permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

Aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudios.

Integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

Saber comunicar conclusiones -y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades.

Competencias generales

Capacidad para saber comunicar las conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

Competencias específicas

Capacidad de identificar, diagnosticar y analizar los riesgos potenciales relacionados con la ciberseguridad.

Capacidad para comprender y asumir la ética y la deontología profesional asociada al trabajo del ingeniero industrial.

RESULTADOS DE APRENDIZAJE

Identificar y analizar los riesgos potenciales relacionados con la ciberseguridad

Conocer y saber aplicar el marco legal y normativo en infraestructuras críticas y entornos industriales

Aplicar los elementos tecnológicos de la ciberseguridad industrial

Analizar los riesgos de las infraestructuras críticas industriales

Aplicar medidas de protección y crear un CERT/CSIRT

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

La nota final del alumno tendrá en cuenta los siguientes factores:
[1] Prácticas / trabajos individuales y en grupo: Todas las prácticas son de entrega obligatoria. Cada una de ellas se evaluará de 0 a 10, no entregar una práctica supone recibir una calificación de 0 puntos en la misma. Para que una práctica se considere aprobada deberá obtener una calificación igual o superior a 5. El promedio de todas estas calificaciones prácticas reflejará el 40% de la calificación final.
[2] Examen de carácter teórico que se realizará a la finalización del temario con el fin de evaluar la asimilación de conocimientos que ha realizado el alumnado de los contenidos de la asignatura. Se puntuará de 0 a 10 y reflejará el 50% de la calificación final. Es necesario obtener en este examen una calificación mínima de 5 para superar la asignatura.
[3] Evaluación Continua. Esta nota reflejará, principalmente, la participación y actitud del alumno en las clases prácticas de la asignatura. Reflejará un 10% de la nota final. CÁLCULO DE LA NOTA FINAL: Teniendo en cuenta estos tres componentes, la nota final del alumno será un valor entre 0 y 10 y se calculará como: 0,4 * [1] + 0,5 * [2] + 0,10 * [3].
ALUMNOS CON DISPENSA ACADÉMICA O EN SEGUNDA MATRÍCULA O SUCESIVAS: Los alumnos que tengan concedida dispensa académica por causas justificadas o bien estén en segunda matrícula o sucesivas, estarán exentos de asistir a clase. Este hecho no exime de la obligación de realizar exámenes, prácticas y ejercicios en los mismos plazos que el resto de sus compañeros. Respecto del porcentaje del 10 % correspondiente a participación en la asignatura y realización de ejercicios, será evaluado mediante la asistencia a Página 5 un mínimo de una tutoría, en el horario convenido entre profesor y alumno. En dicha tutoría el alumno hará entrega de los ejercicios del curso y responderá a las preguntas que le efectúe el profesor sobre ellos.
RECUPERACIÓN EN CONVOCATORIA EXTRAORDINARIA: Los alumnos que no hayan alcanzado la nota mínima en el examen escrito o hayan suspendido en el computo de la nota global según la formula indicada más arriba, habiendo suspendido por tanto en la convocatoria ordinaria, podrán optar a una recuperación en la convocatoria extraordinaria, que consistirá en la recuperación de las prácticas y/o la recuperación del examen teórico.
NORMATIVA ANTIPLAGIOS: Cualquier tipo de fraude o plagio por parte del alumno en una actividad evaluable, será sancionado según se recoge en la Normativa de Convivencia de la UFV. A estos efectos, se considerará "plagio" cualquier intento de defraudar el sistema de evaluación, como copia en ejercicios, exámenes, prácticas, trabajos o cualquier otro tipo de entrega, bien de otro compañero, bien de materiales o dispositivos no autorizados, con el fin de hacer creer al profesor que son propios.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Pascal Ackerman Industrial Cybersecurity: Efficiently secure critical infrastructure systems

Francisco Martín Abreu Material Docente Canvas 2024

Complementaria

European Parliament and Council of the European Union General Data Protection Regulation 2018
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:02016R0679-20160504

ISO ISO 27001/2

ISACA Planning for and Implementing ISO 27001
https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001