20-21

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

# GUÍA DE ESTUDIO PÚBLICA

# SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

**CÓDIGO 31109114**

UNED

20-21

**SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS**

**CÓDIGO 31109114**

# ÍNDICE

| | |
|---|---|
| Nombre de la asignatura | SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS |
| Código | 31109114 |
| Curso académico | 2020/2021 |
| Título en que se imparte | MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD |
| Tipo | CONTENIDOS |
| Nº ETCS | 6 |
| Horas | 150.0 |
| Periodo | SEMESTRE 2 |
| Idiomas en que se imparte | CASTELLANO |

## PRESENTACIÓN Y CONTEXTUALIZACIÓN

Las redes industriales son vitales y, a la vez, vulnerables, con consecuencias potencialmente devastadoras en el caso de un incidente exitoso de ciberseguridad. Los ataques evolucionan rápidamente, haciéndose más inteligentes y adaptables, difíciles de detectar y muy persistentes. Tanto cuando se habla de sabotajes industriales como de problemas de seguridad en infraestructuras críticas, la tendencia es muy preocupante e implica la necesidad de profesionales mejor preparados, tanto desde el punto de vista puramente industrial como desde el punto de vista de la seguridad en redes y sistemas

Teniendo en cuenta todo esto, el objetivo general de esta asignatura es ubicar correctamente la ciberseguridad como uno de los puntos clave a tener en cuenta en cualquier proceso de análisis, diseño, desarrollo y mantenimiento de sistemas de comunicación industrial, enseñando a valorar la importancia que debe tener y qué consecuencias, siempre negativas, podría tener el no hacerlo así.

En cuanto a objetivos particulares la asignatura trata de conseguir que los estudiantes obtengan el conocimiento de los principales problemas de seguridad informática y de comunicaciones relacionados con las redes industriales y las infraestructuras críticas. Asimismo, se busca que los estudiantes obtengan el conocimiento de las principales soluciones técnicas y organizativas que se utilizan hoy en día en la industria para tratar de minimizar los riesgos asociados a tales problemas de seguridad. Este conocimiento debe además estar especialmente orientado a aspectos prácticos, por lo que se debe plantear al estudiante aspectos prácticos ligados a los conocimientos citados.

Muchos de los contenidos de esta asignatura se basan en el conocimiento y las competencias adquiridas en las asignaturas del primer cuatrimestre, especialmente en "Auditoría y monitorización de la seguridad", "Criptografía aplicada" y "Hacking ético". Las competencias y contenidos de esta asignatura completan, en el área de seguridad en infraestructuras críticas, el perfil profesional de un ingeniero informático experto en ciberseguridad.

## REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Es imprescindible el conocimiento en redes IP a nivel de arquitectura y protocolos más relevantes, así como conocimientos básicos de problemas de seguridad en sistemas operativos, aplicaciones y redes, alcanzable mediante conocimientos previos o mediante las asignaturas de primer cuatrimestre "Criptografía aplicada" y "Hacking ético".
También es muy importante un buen conocimiento previo en auditorías de seguridad y herramientas de monitorización de la misma, alcanzable mediante la asignatura de primer cuatrimestre "Auditoría y Monitorización de la Seguridad" de este mismo Máster.
Además, es necesario tener un buen conocimiento de inglés técnico que le permita leer y comprender la mayor parte de la bibliografía y de las referencias que están escritas en ese idioma.

## EQUIPO DOCENTE


| | |
|---|---|
| Nombre y Apellidos | GABRIEL DIAZ ORUETA (Coordinador de asignatura) |
| Correo Electrónico | gdiaz@ieec.uned.es |
| Teléfono | 91398-8255 |
| Facultad | ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES |
| Departamento | ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT. |

| | |
|---|---|
| Nombre y Apellidos | RAFAEL PASTOR VARGAS |
| Correo Electrónico | rpastor@dia.uned.es |
| Teléfono | 91398-8383 |
| Facultad | ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA |
| Departamento | SISTEMAS DE COMUNICACIÓN Y CONTROL |

| | |
|---|---|
| Nombre y Apellidos | RAFAEL PASTOR VARGAS |
| Correo Electrónico | rpastor@scc.uned.es |
| Teléfono | 91398-8383 |
| Facultad | ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA |
| Departamento | SISTEMAS DE COMUNICACIÓN Y CONTROL |


## HORARIO DE ATENCIÓN AL ESTUDIANTE

La tutorización de los alumnos se llevará a cabo:
1- A través del curso virtual de la asignatura en la plataforma de e-Learning aLF
2- Por correo electrónico con el equipo docente:
Gabriel Díaz Orueta - gdiaz@ieec.uned.es, ETSI Industriales, C/Juan del Rosal, 12, 28040 Madrid
Rafael Pastor Vargas - rpastor@scc.uned.es, ETSI Informática, C/Juan del Rosal, 16, 28040 Madrid
3- En el horario de guardia del equipo docente, los martes de 14:00 a 18:00 en el Telf. 91-3988255 o los lunes de 16:00 a 18:00 en el Telf. 913988383

## COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

**COMPETENCIAS BÁSICAS**

CB6 - 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

CB7 - Que los estudiantes sepan 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 estudio

CB8 - Que los estudiantes sean capaces de 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

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

**COMPETENCIAS GENERALES**

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

**COMPETENCIAS TRANSVERSALES**

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

**COMPETENCIAS ESPECÍFICAS**

CE3 - Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.

CE4 - Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.

## RESULTADOS DE APRENDIZAJE

Los resultados de aprendizaje que alcanzará el estudiante son los siguientes:
•Ser capaz de describir términos como ICS, DCS, SCADA, red industrial, protocolos industriales, zonas, etc.
•Ser capaz de identificar el alcance de las recomendaciones de seguridad industrial más comunes y cómo se han alcanzado
•Identificar las topologías y esquemas de segmentación más comunes en las redes industriales y cómo se integran las redes inalámbricas y el acceso remoto
•Identificar las particularidades de rendimiento de las redes industriales, como el tratamiento de la latencia y el *jitter*
•Identificar las principales características de algunos de los protocolos más típicos de este entorno
•Entender las principales motivaciones y las posibles consecuencias de incidentes de seguridad en entornos industriales
•Identificar los objetivos de ataque más comunes, así como los métodos de ataque más comunes, entendiendo las principales vías de ataque
•Conocer las principales metodologías de evaluación de riesgos en el sector industrial
•Identificar las amenazas principales, así como las vulnerabilidades más típicas
•Ser capaz de hacer una clasificación general de los riesgos para un entorno industrial
•Conocer cómo segmentar redes para implantar controles de seguridad de redes, de host y de acceso
•Conocer a nivel básico la detección de anomalías y amenazas en redes industriales
•Identificar procedimientos para monitorizar zonas de seguridad en entornos industriales con éxito
•Conocer cómo hacer una gestión segura de la información obtenida, así como de los logs.

## CONTENIDOS

TEMA 1 - Introducción al contexto de seguridad en redes industriales

- Terminología y conceptos de redes industriales
- Historia de los problemas de ciberseguridad en redes industriales y tendencias actuales
- Introducción a los sistemas de control industrial y sus operaciones

TEMA 2 - Diseño, arquitectura y principales protocolos de redes industriales

- Conceptos fundamentales de diseño y arquitectura: topologías, segmentaciones de red, accesos, latencia, jitter, seguridad física, etc.
- Protocolos Fieldbus, backend, simuladores

TEMA 3 - Principales problemas de seguridad en sistemas de control industrial

- Motivos para los ataques y posibles consecuencias
- Objetivos más comunes de los ataques
- Métodos de ataque más comunes
- Ejemplos de amenazas reales
- Tendencias de los nuevos ataques

TEMA 4 - ¿Cómo hacer evaluaciones de vulnerabilidades y riesgos?

- Análisis de riesgos de ciberseguridad
- Metodologías de evaluación de riesgos en ICS
- Identificación de amenazas y vulnerabilidades
- Clasificación de riesgos
- Técnicas de mitigación y reducción de riesgso

TEMA 5 - Herramientas y procedimientos de defensa en ICS

- Segmentación de redes
- ¿Cómo establecer zonas y "canales" (conduits)?
- ¿Cómo implantar controles de seguridad en redes y hosts?
- Detección de anomalías de comportamiento y de amenazas

TEMA 6 - Monitorización de la seguridad de los ICS

- ¿Qué se debe monitorizar?
- Monitorización de las zonas de seguridad
- Gestión de la información y logs

TEMA 7 - Estándares y regulaciones

- Estándares NERC CIP
- ISA/IEC 62443
- Buenas prácticas para el análisis de riesgos
- Otros estándares

## METODOLOGÍA

La metodología con la que se ha diseñado el curso, y que se seguirá durante su desarrollo, es la **específica de la educación a distancia del modelo de la UNED,** en la que el trabajo en la asignatura y el proceso de evaluación son continuos a lo largo del curso y están de acuerdo con la organización del contenido dado en los apartados anteriores.
El alumno, basándose en el curso virtual como herramienta principal, debe desarrollar las siguientes actividades:

- Leer atentamente la guía de estudio de la asignatura
- Seguir su propio ritmo valiéndose, si le resulta útil, de la planificación aproximada que aparecerá en el Plan de Trabajo de esta guía y del curso virtual
- Estudiar la bibliografía básica, suficiente para aprobar la asignatura, complementándola con la bibliografía adicional cuando sea necesario.
- Revisar periódicamente los foros del curso virtual, donde encontrará preguntas y comentarios de otros estudiantes. Responder a las preguntas de otros estudiantes cuando sea posible.
- Leer y comprender la documentación disponible para su descarga en el curso virtual de la asignatura.
- Participar en debates (no obligatorios pero evaluables) propuestos en los foros sobre asuntos relacionados con la materia
- Realizar las Pruebas de Evaluación Continua (PEC) y realimentar lo aprendido basándose en las correcciones del Equipo Docente

El equipo docente facilitará, **al principio de cada curso**, y en el curso virtual, un cronógrama gráfico ajustado al calendario de ese curso, que contenga la secuencia aproximada de aprendizaje propuesta.

## SISTEMA DE EVALUACIÓN

**TIPO DE PRUEBA PRESENCIAL**

| | |
|---|---|
| Tipo de examen | Examen de desarrollo |
| Preguntas desarrollo | 4 |
| Duración del examen | 120 (minutos) |
| Material permitido en el examen | |
| Calculadora no programable | |
| Criterios de evaluación | |

- El examen será de desarrollo, **no habrá preguntas de tipo test**.

COMPOSICIÓN:

3 preguntas cortas (nota máxima de dos puntos por cada una) que deben responderse en un máximo de una página cada una

1 pregunta de desarrollo mayor (nota máxima de cuatro puntos) que debe responderse sin límite de espacio, aunque se tendrá muy en cuenta la correcta estructuración y presentación de la respuesta

---

Las preguntas cortas podrán versar sobre la resolución de un ejercicio práctico corto o la demostración del conocimiento de aspectos concretos de los contenidos de la asignatura

La pregunta larga estará relacionada con aspectos más complejos de un ejercicio práctico o la demostración de conocimientos relacionados con las secciones más relevantes de los contenidos de la asignatura.

NO es necesario contestar a todas las preguntas

Este examen constituye el 40% de la nota final. **Es necesario obtener al menos un 5 en este examen** para ser evaluado para la nota final de la asignatura.

| | |
|---|---|
| % del examen sobre la nota final | 40 |
| Nota del examen para aprobar sin PEC | |
| Nota máxima que aporta el examen a la calificación final sin PEC | |
| Nota mínima en el examen para sumar la PEC | 5 |
| Comentarios y observaciones | |

Las fechas del examen se podrán consultar en:

**http://portal.uned.es/portal/page?_pageid=93,14024325&_dad=portal**

**CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS**

| | |
|---|---|
| Requiere Presencialidad | Si |
| Descripción | |
| Criterios de evaluación | |
| Ponderación de la prueba presencial y/o los trabajos en la nota final | |
| Fecha aproximada de entrega | |
| Comentarios y observaciones | |

**PRUEBAS DE EVALUACIÓN CONTINUA (PEC)**

| | |
|---|---|
| ¿Hay PEC? | Si,PEC no presencial |
| Descripción | |

- Son **dos pruebas prácticas de evaluación continua** sobre contenidos estudiados, que deben demostrar que se han entendido los conceptos, procedimientos y análisis asociados a la asignatura.

**- Es OBLIGATORIA su realización**

Criterios de evaluación

Teniendo en cuenta que los contenidos de la asignatura no permiten aplicar una solución única al mismo problema, se evaluará la correcta estructuración del análisis aplicado al problema concreto, así como los detalles propuestos para su resolución dentro de una aproximación global al problema de la seguridad en infraestructuras críticas,

Ponderación de la PEC en la nota final: El peso de la nota media de las PEC será del 40% de la nota final. Se aplicará siempres que se obtenga al menos un 5 en la prueba presencial.

Fecha aproximada de entrega: PEC1 05/04/2021 PEC2 30/05/2021

Comentarios y observaciones

- La nota media de las PEC se tendré en cuenta únicamente **si se obtiene al menos una nota de 5 en la prueba presencial.**

**OTRAS ACTIVIDADES EVALUABLES**

¿Hay otra/s actividad/es evaluable/s?: Si,no presencial

Descripción

Se celebrarán 2 debates, **no obligatorios pero evaluables**, que se abrirán y cerrarán conforme a la secuencia aproximada de aprendizaje señalada en el curso virtual, hacia el final de los temas 3 y 6.

**Dada la naturaleza no completamente determinista de muchos de los contenidos de esta asignatura, muy asociada a la toma de decisiones basadas en el análisis y la gestión de riesgos, los debates deben servir como otro medio de aprendizaje para entender mejor, de una forma abierta, una serie de aspectos prácticos de los contenidos, mediante el intercambiolibre de diferentes puntos de vista entre estudiantes y profesores.**

**DINÁMICA DE LOS FOROS:**

El profesor propondrá una noticia o un tema específico, pidiendo opiniones sobre el mismo en el foro de debates

Cada estudiante, de manera completamente libre, puede participar contestando con su análisis, opinión y/o proponiendo soluciones o haciendo comentarios

**DURACIÓN: Cada debate permanecerá abierto durante dos semanas aproximadamente**

Criterios de evaluación

- Son **EVALUABLES pero NO OBLIGATORIOS**

**Para obtener la nota máxima en cada debate el estudiante debe participar con, al menos, 2 mensajes que deben demostrar un interés cierto por el tema en discusión y el aprendizaje adquirido hasta ese moment.**

**La participación en los debates cuenta como el 20% de la nota final de la asignatura, siempre que en la prueba presencial se obtenga una nota de 5 o mayor.**

| | |
|---|---|
| Ponderación en la nota final | Es del 20% de la nota final de la asignatura, que se añade solo si se obtiene una nota de al menos un 5 en la prueba presencial. |
| Fecha aproximada de entrega | Debate 1 15/03/2021 Debate 2 15/04/2021 |
| Comentarios y observaciones | |

**¿CÓMO SE OBTIENE LA NOTA FINAL?**

La nota final de la asignatura se compone de la siguiente forma:

**NOTA FINAL = 0,4 * (Nota de la prueba presencial) + 0,4 * (Nota media de las PEC) + 0,2 * (Nota de los debates)**

En cualquier caso, para aprobar la asignatura, el estudiante deberá obtener al menos un 5 en la prueba presencial y realizar al menos una PEC con nota suficiente para llegar a un 5 en la nota final

Si se suspende la prueba presencial pero se han aprobado las PEC, la nota de estas se guarda para la siguiente convocatoria.

SI se suspenden (o no se realizan) las PEC pero se aprueba la prueba presencial, la nota de la prueba presencial se guarda para la siguiente convocatoria.

## BIBLIOGRAFÍA BÁSICA

ISBN(13):9780124201149
Título:INDUSTRIAL NETWORK SECURITY (Segunda)
Autor/es:Joel Thomas Langill ; Eric D. Knapp ;
Editorial:SYNGRESS

## BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):9788436267167
Título:PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES (2013)
Autor/es:Castro Gil, Manuel Alonso ; Ignacio Alzórriz ; San Cristóbal Ruiz, Elio ; Díaz Orueta, Gabriel ;
Editorial:UN.E.D.

Durante el desarrollo del curso se irán añadiendo diferentes artículos, guías y presentaciones para dinamizar y permitir profundizar en diferentes aspectos de los

contenidos a aquellos alumnos que así lo deseen.

## RECURSOS DE APOYO Y WEBGRAFÍA

**Curso Virtual**

La plataforma aLF de e-Learning de la UNED proporcionará el adecuado interfaz de interacción entre el alumno y sus profesores. aLF es una plataforma de e-Learning y colaboración que permite impartir y recibir formación, gestionar y compartir documentos, crear y participar en comunidades temáticas, así como realizar proyectos online. Se ofrecerán las herramientas necesarias para que, tanto el equipo docente como los estudiantes, encuentren la manera de compaginar tanto el trabajo individual como el aprendizaje cooperativo.

---

## IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.