Universidad de Valladolid

Trabajo Fin de Máster

MÁSTER EN PROFESOR DE EDUCACIÓN SECUNDARIA OBLIGATORIA Y BACHILLERATO, FORMACIÓN PROFESIONAL Y ENSEÑANZAS DE IDIOMAS

Especialidad de Tecnología e Informática

Tecnología Didáctica sobre Seguridad Informática en Formación Profesional

Autor:
D. Javier Argón del Caz
Tutor:
Dr. D. Santiago Blanco Suárez

Valladolid, 11 de Julio de 2019

El educador mediocre habla.
El buen educador explica.
El educador superior demuestra.
El gran educador inspira.

William Arthur Ward

TFM

Trabajo Fin de Máster de Profesorado en Secundaria: Tecnología Didáctica sobre Seguridad Informática en Formación Profesional

Javier Aragón del Caz

Universidad de Valladolid

Javier Aragón del Caz

MÁSTER EN PROFESOR DE EDUCACIÓN SECUNDARIA

TRABAJO FIN DE MASTER
Tecnología Didáctica sobre Seguridad Informática en Formación Profesional

Curso 2018/2019
Universidad de Valladolid

Dedicado a todas aquellas personas
que han contribuido de una manera u otra
al desarrollo de este trabajo.

Sobre todo, dedicado a Lorena, por su apoyo durante
el desarrollo de estos estudios que han supuesto
la metamorfosis de un ingeniero en un futuro profesor.

Resumen

Actualmente una de las mayores preocupaciones en el campo de las nuevas tecnologías de la información y las comunicaciones (TIC) es la seguridad, esto es debido al aumento de los ataques por parte de hackers informáticos, que cada vez usan técnicas y herramientas más avanzadas. Con motivo de ésta preocupación y con el aumento de los ataques informáticos, cada vez son demandados más perfiles de profesionales de las TIC formados en Seguridad Informática, además, se requiere una mejor y más específica formación en este campo.

Es por ello que se hace necesaria la revisión de los currículos y las programaciones didácticas de los ciclos formativos de la Formación Profesional que están relacionados con la Seguridad Informática, con el objetivo de formar profesionales que cumplan las necesidades actuales del mercado laboral, con la utilización de metodologías y herramientas específicas para este campo.

Este documento pretende recoger una revisión en cuanto a objetivos y contenidos de un posible currículo para formación profesional en Seguridad Informática, así como una propuesta coherente y meditada sobre las metodologías y herramientas para utilizar en el aula o en los laboratorios de estos estudios.

Palabras clave

Seguridad Informática, Educación en Seguridad TIC, Metodologías, Laboratorios de Seguridad Informática, Hacking Ético

Abstract

Security is one of the current hot topics in the field of information and communication technologies (ICT). The reason behind this is the increasing number of cyber-attacks by hackers who are able to take advantage from the use of the newest techniques and the most high-end tools. The raising awareness and the increasing number of cyber-attacks have incremented the demand of ICT professionals who are trained in cyber-security, with a deeper and more specific knowledge of this particular field.

Accordingly, a review of the curricula and of the programs of professional courses and studies on computer and cyber security is of the essence. The goal should be set on training professionals who are able to master these specific techniques and tools in order to be able to meet the current needs of the potential employers.

This report presents a throughout review of the goals and contents that a curriculum for professional training in Computer Security should cover. This report also presents a coherent and comprehensive proposal on the use of educational methodologies and skills to be implemented inside the lecture room and also as part of any laboratory training.

Keywords

Computer Security, IT Security Education, Methodologies, General Security Laboratories, Ethical Hacking

ÍNDICE DE CONTENIDOS

1. Introducción 9
2. Objetivos 10
3. Ámbito de estudio 12
4. Preocupaciones de la seguridad informática en la formación de profesionales 14
5. Estructura de la Formación Profesional en la familia de Informática y Comunicaciones. 16
5.1. Competencias Básicas y Contenidos de los títulos LOE de formación profesional para informática y comunicaciones 17
5.1.1. Título profesional Básico en informática de Oficina. 17
5.1.2. Título profesional Básico en Informática y Comunicaciones. 17
5.1.3. Técnico en Sistemas Microinformáticos y Redes. 18
5.1.4. Técnico Superior en Administración de Sistemas Informáticos en Red 19
5.1.5. Técnico Superior en Desarrollo de Aplicaciones Multiplataforma. 21
5.1.6. Técnico Superior en Desarrollo de Aplicaciones Web. 22
6. La Seguridad Informática y Privacidad de datos en la Formación Profesional. 24
6.1. Seguridad informática en la Formación Profesional 24
7. Concreción de la Seguridad informática en currículos 29
7.1. Objetivos de Seguridad Informática en la FP actual 29
7.1.1. Objetivos para los estudios de Grado medio de SMR 29
7.1.2. Objetivos para los estudios de Grado Superior de ASIR. 31
8. Propuesta de objetivos para Seguridad Informática en Formación Profesional 33
8.1. Objetivos de la Seguridad Informática en SMR 34
8.1.1. Principios de seguridad 34
8.1.2. Privacidad y protección de la información 34
8.1.3. Protección y privacidad en redes locales e inalámbricas 35
8.1.4. Legislación y normas de protección de datos y seguridad 35
8.2. Objetivos de la Seguridad Informática en ASIR 35
8.2.1. Amenazas, ataques y vulnerabilidades 35
8.2.2. Tecnologías y herramientas de seguridad 36
8.2.3. Arquitecturas y diseño de seguridad 36
8.2.4. Identidades digitales y control de acceso 37
8.2.5. Gestión de seguridad: riesgos y vulnerabilidades 37
8.2.6. Criptografía y cifrado de información. 37
9. Ampliación de contenidos de Seguridad Informática en Formación Profesional. 38
9.1. Contenidos de Seguridad Informática para FP de Grado Medio de SMR 38

9.1.1. Introducción y principios de Seguridad Informática. 38
9.1.2. Protección y seguridad de la información 39
9.1.3. Protección y privacidad en redes cableadas e inalámbricas. 40
9.1.4. Ética y normativa de Seguridad Informática. 41
9.2. Contenidos de Seguridad Informática para FP de Grado Superior de SMR 43
9.2.1. Seguridad de la Información 43
9.2.2. Amenazas y ataques en Seguridad Informática 44
9.2.3. Arquitecturas y servicios en Seguridad Informática 44
9.2.4. Sistemas y aplicaciones en Seguridad Informática 45
9.2.5. Gestión de la Seguridad Informática 46
10. Metodologías para Seguridad Informática en Formación Profesional. 48
10.1. Metodologías para aspectos teóricos de Seguridad Informática 49
10.2. Estudio de casos para el análisis de ataques informáticos 50
10.3. Participación en concursos de habilidades sobre Seguridad Informática 51
10.4. Hacking ético como metodología 52
10.5. La gamificación para prácticas de seguridad informática 55
11. Herramientas para la enseñanza de Seguridad Informática 57
11.1. Laboratorios específicos para Seguridad Informática 57
11.2. Aplicación de IoT para laboratorios virtuales 58
11.3. La virtualización para objetivos en Seguridad Informática 59
11.4. Entornos educativos virtuales para Seguridad Informática 62
11.5. Herramientas utilizadas en ataques informáticos orientadas a la educación 63
12. Conclusiones 67
13. Referencias 70

TABLAS

Tabla 1-Tabla de los estudios LOE y LOMCE para formación profesional en el campo de la informática y las comunicaciones. 16

Tabla 2- Organización de los contenidos de los módulos de FP 38

Tabla 3 - Contenidos para SMR: Introducción y principios de Seguridad Informática 39

Tabla 4 - Contenidos para SMR: Protección y Seguridad de la Información 40

Tabla 5 - Contenidos para SMR: Protección y privacidad en redes cableadas e inalámbricas 41

Tabla 6 - Contenidos para SMR: Ética y Normativa de Seguridad Informática 42

Tabla 7 - Contenidos para ASIR: Seguridad de la Información 43

Tabla 8 - Contenidos para ASIR: Amenazas y ataques en Seguridad Informática 44

Tabla 9 - Contenidos para ASIR: Arquitecturas y servicios en Seguridad Informática 45

Tabla 10 - Contenido para ASIR: Sistemas y aplicaciones en Seguridad Informática 46

Tabla 11 - Contenido para ASIR: Gestión de la Seguridad Informática 47

ILUSTRACIONES

Ilustración 1 - Ventajas y resultados de las metodologías hacking en educación. 55

1. Introducción

Este documento está orientado a analizar, definir y proponer una mejora, en cuanto objetivos, contenidos, metodologías y herramientas, para aquellos currículos y programaciones didácticas de los módulos profesionales de los ciclos formativos de Formación Profesional (FP), que están claramente orientados a la enseñanza de Seguridad Informática en los estudios de la rama de Informática, más en concreto en los estudios referidos a las titulaciones de Técnico de Grado Medio de Sistemas Microinformáticos y Redes (SMR) y Técnico Superior en Administración de Sistemas Informáticos y Redes (ASIR). Este Trabajo Fin de Master se enmarca dentro de la especialidad de Tecnología e Informática del Máster en Profesor de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanzas de Idiomas de la Universidad de Valladolid.

2. Objetivos

Este Trabajo Fin de Máster (TFM) tiene, en una primera parte, el objetivo de la búsqueda y análisis sobre los diferentes estudios que se relacionen con la Seguridad Informática, dentro de la familia profesional de Informática y Comunicaciones de Formación Profesional que se ofrecen en el ámbito de la Educación en España. Y una vez realizada esta búsqueda, estudiar y analizar todos los objetivos, contenidos y estándares de evaluación relativos a todo lo que tenga que ver con temas de Seguridad Informática, tanto de sistemas, infraestructuras de redes, hardware, privacidad de la información y en el uso de Internet.

Una vez analizados los estudios de Formación Profesional de la rama seleccionada y su desarrollo en cuanto a objetivos, contenidos y metodologías de Seguridad Informática que se proponen a nivel estatal y regional, y que se concretan en cada centro. Se va a plantear la modificación de estas propuestas para adaptarlas a las nuevas tendencias y técnicas de seguridad, tanto en la enseñanza como en la aplicación profesional. Aplicando para ello metodologías de aprendizaje innovadoras y activas, orientando estas hacia la práctica y desarrollo profesional, ya que este es uno de los principales objetivos de la Formación Profesional.

La FP en España ha reconocido, durante años, la necesidad de desarrollar unos planes de estudio para formar profesionales especializados en diferentes ramas o familias profesionales, y siempre ha intentado realizar un esfuerzo por la formación de profesionales en TIC. Aunque la necesidad de actualización de estos planes es evidente por las evoluciones tecnológicas que se producen en todos los campos de las TIC. Más especialmente en un campo como la gestión de la seguridad.

Por lo que el objetivo principal de este TFM es el de proponer un currículo actualizado y adaptado a las necesidades y requerimientos en cuanto a Seguridad Informática de los futuros profesionales, que deberían formarse en los ciclos formativos de FP que estén relacionados con la Seguridad Informática.

Además, se plantea identificar los componentes, teóricos, prácticos y metodológicos que deberían tener estos estudios, así como definir las características específicas de los mismos. Intentando asegurar y plasmar los objetivos y revisiones de los currículos de seguridad de entidades como ACM (acrónimo de Assoiaton For Computing Machinery) o de la asociación de profesionales IEEE-CS (acrónimo de Institute of Electrical and Electronics Engineers – Computer Society), entre otras entidades de certificación en infraestructuras de redes como la empresa CISCO.

Esta propuesta intenta basarse en las necesidades y expectativas de la profesión de seguridad de la información y la investigación previa de currículos académicos, programaciones didácticas, perfiles profesionales, organizaciones de auditoría y sociedades profesionales.

El desarrollo de esta propuesta para la enseñanza y la formación de la Seguridad Informática podría ser el punto de partida de una revisión profunda de los requisitos que los profesionales de este campo que deberían representar en base a intereses de

investigación, estándares, formación, técnicas, herramientas y certificaciones de seguridad.

Se intenta formular un plan para estimular el interés actual y futuro en el plan de estudios que ofrece la FP para la Gestión de la Seguridad de la Información en los ciclos formativos ofertados. Además de formular un punto de partida para un futuro procedimiento para que las instituciones educativas y académicas puedan desarrollar los programas de estudios de Seguridad Informática que demanda la sociedad.

Este plan de estudios que se propone, se basa en las consideraciones de que los planes y currículos de este tipo de estudios deben ser documentos vivos, que se deberían actualizar periódicamente. Por lo que se debe establecer un proceso de renovación para la reevaluación de los programas de la FP, para la alineación con planes de estudios que fomenten la innovación tanto en objetivos y metodologías, como en las herramientas utilizadas para garantizar la formación de profesionales capaces de cubrir las necesidades que el mercado laboral demande en cada momento.

3. Ámbito de estudio.

Antes de seleccionar los estudios objetivo de análisis de este TFM, y definir los ámbitos de búsqueda de los currículos de Seguridad Informática en FP, hay que conocer la situación, el contexto educativo y la normativa en lo que se refiere a la Educación en España y su concreción de los aspectos transferidos a Castilla y León, en cuanto a aquellos estudios relacionados con las Tecnologías de la Información (TIC) y la Seguridad Informática.

Hay que conocer la realidad del sistema educativo español y su relación con las TIC y la Seguridad Informática, de esta manera se podrá tener una visión concreta de las características y conocimientos con los que acceden los alumnos a cada uno de los estudios, y desde el análisis de este contexto poder definir los objetivos, contenidos y metodologías que mejor se adapten a las características de los alumnos y los conocimientos que se desean transmitir.

El sistema educativo en España está organizado, regulado y estructurado por dos leyes básicas, La Ley Orgánica de Educación (LOE), 2/2006 de 3 de mayo, y la Ley Orgánica para la Mejora de la Calidad Educativa (LOMCE), 8/2013 de 9 de diciembre que modifica la anterior pero no la deroga. En estas leyes (y anteriores) se dictamina que el profesorado de secundaria tiene por objeto la práctica docente en los ciclos de Educación Secundaria, Bachillerato y Formación Profesional. Por lo que nuestro estudio estará centrado en buscar las asignaturas, contenidos y competencias que se refieran a dicha especialidad en cualquiera de estos ciclos o enseñanzas para todas las materias que estén relacionadas con la Informática.

En cuanto a la Formación Profesional (FP), se ha realizado una búsqueda sobre los diferentes estudios de las diferentes ramas profesionales, y aunque en algunas ramas específicas hay módulos que tienen que ver con la Informática (como por ejemplo en los de Diseño o Telecomunicaciones), hay una rama profesional específica para la Informática y Comunicaciones que es en la que se desarrollan objetivos y contenidos de Seguridad Informática en algunos de sus módulos profesionales pertenecientes a los ciclos formativos de SMR y ASIR, aunque no hay un ciclo formativo dedicado específicamente a la Seguridad Informática. También se ha hecho un pequeño análisis de los ciclos de la Familia de Informática, en concreto con las diferencias que tienen en las leyes orgánicas de la LOE 2/2006 de 3 de mayo y LOMCE 8/2013 de 9 de diciembre, así como de las especialidades que se desarrollan y los perfiles que se solicitan en las empresas.

En nuestro caso, ya que los estudios se van a centrar en la Formación Profesional tenemos que detectar ciertas singularidades del contexto que abarca este TFM.

El bagaje sobre Seguridad Informática con el que acceden los alumnos a los estudios de FP de Grado Medio de SMR desde la ESO o FP Básica es bajo, no se desarrolla más allá desde la experiencia de usuario, implicaciones éticas y unas nociones básicas de seguridad. En función del enfoque por parte de las Comunidades Autónomas o centros educativos, pertenecientes a las mismas, de los currículos de unas asignaturas de las TIC, porque entre las asignaturas de libre configuración observadas en diferentes ofertas de centro educativos están más orientadas a la programación o la robótica.

Sin embrago, los alumnos que acceden a los estudios de Grado Superior de ASIR pueden tener ya unos conocimientos previos de seguridad, en particular aquellos que accedan a estos estudios desde el ciclo formativo de SMR. Por su parte, aquellos que accedan a través de Bachillerato pueden tener unos conocimientos básicos de seguridad, pero por otra parte aportan conocimientos sobre algoritmia y programación que pueden ser interesantes para los objetivos de currículo que tengan que ver con el cifrado y criptografía.

4. Preocupaciones de la seguridad informática en la formación de profesionales

La Seguridad Informática se ha posicionado en los últimos años como una prioridad para asegurar los sistemas, aplicaciones, arquitecturas y/o infraestructuras tanto para países como empresas de cualquier índole. Para abordar los problemas de seguridad, la educación tanto formal como no formal ha ido incorporando cada vez más en sus currículos la seguridad informática.

Aunque los estudios de Formación Profesional de SMR y ASIR no han sido diseñados específicamente para la educación de seguridad, se han adaptado de tal forma que solo cubren una pequeña parte de los principios fundamentales de seguridad.

La importancia de orientar la enseñanza de la seguridad hacia un aprendizaje más experimental es algo que está definido desde hace tiempo (Du, Jayaraman, & Gaubatz, 2010). Pero a pesar de ello, todavía se detectan algunas deficiencias en las programaciones de estos estudios específicos. Un programa orientado a la Seguridad Informática que cubre solo los aspectos teóricos de la misma no puede ser el idóneo para preparar a los estudiantes para superar las dificultades asociadas con la protección eficiente de sistemas informáticos. Además, un entorno de aprendizaje que no le da al estudiante la oportunidad de experimentar y practicar con métodos, técnicas y herramientas de seguridad no le proporciona las habilidades y conocimientos necesarios para realizar investigación y desarrollo en el campo de la seguridad informática, tan necesario actualmente.

La mayoría de los currículos de Seguridad Informática que, si han sido orientados para agregar un componente práctico más que teórico, se han centrado en incluir ejercicios y prácticas de laboratorio basados en técnicas defensivas de seguridad de la información (Whitman, Mattord, & Green, 2014; Trabelsi, Hayawi, Al Braiki, & Mathew, 2013). Sin embargo, para defender un sistema se necesita un buen conocimiento de los ataques a los que se puede enfrentar un sistema (Arce y McGraw, 2004). Los estudiantes que entienden cómo se diseñan y lanzan los ataques estarán mejor preparados para sus futuras carreras profesionales como administradores de seguridad en lugar de aquellos que no tienen tales habilidades (Logan y Clarkson, 2005). Por lo que habría que promover la inclusión de laboratorios y prácticas que permitan desarrollar métodos y técnicas utilizadas originalmente por hackers. Pero utilizar y enseñar técnicas de piratería conlleva unas implicaciones éticas, que se han convertido en un componente fundamental en los currículos que implican las TIC a cualquier nivel educativo.

Además, los entornos de aprendizaje y los laboratorios subyacentes que se suelen proporcionar al alumno en los módulos que se imparten de Seguridad Informática, son deficientes para el desarrollo de entornos que favorezcan la práctica de la seguridad, ya que son laboratorios que se comparten con otras disciplinas como las orientadas a la programación o tratamiento de información, por ejemplo, lo que hace que la integración de estos laboratorios sea inviable para un curso específico de Seguridad Informática. En la actualidad, todavía faltan laboratorios de seguridad en FP que puedan ser aceptados para la práctica de la Seguridad Informática, pero se detecta que tienen una gran demanda en educación de seguridad desde hace años. (Du & Wang, 2008).

A la hora de diseñar los objetivos, contenidos y metodologías en los currículos de informática, y más en concreto los estudios referidos a la Seguridad Informática, lo más importante es el realizar una propuesta coherente con la actualidad de los avances en las TIC. Estos desafíos no son únicos para el nivel de estudios de la Formación Profesional, si no que se comparten con estudios universitarios, estudios no formales o certificaciones por parte de empresas de seguridad y redes informáticas.

Muchos de los centros que imparten estudios de Seguridad Informática, tienen como objetivo formar a los futuros profesionales de las TIC, como programadores, técnicos de sistemas, diseñadores, etc., que sean capaces de desarrollar sistemas y software seguros. No solo se orientan los estudios de seguridad a la aplicación de técnicas y herramientas para proteger sistemas, sino que también a que el desarrollo y los avances de las nuevos sistemas, servicios, aplicaciones o tecnologías se desarrollen de una forma segura.

Uno de los principales desafíos de la enseñanza de la seguridad es la desactualización que se produce fácilmente debido a la aparición de nuevas técnicas y herramientas para romper las barreras de los sistemas de seguridad, el avance de los ataques informáticos es tan rápido como la de los propios sistemas. Cuando se lanza un nuevo sistema, programa, aplicación, juego o arquitectura se empieza la carrera por encontrar la brecha de seguridad que permita acceder a los datos de los usuarios de estos sistemas o el uso de los mismos de forma no lícita. Incluso hay sistemas de los que se han encontrado vulnerabilidades antes de su lanzamiento al mercado, como por ejemplo pasó en 2018 con el sistema de Nintendo Switch Online que se vio comprometido antes de ver la luz [1].

En muchos casos, el propio sistema es incapaz de adaptarse a estos cambios de manera razonable en tiempo, por lo tanto, es necesario proporcionar a los alumnos de las herramientas y métodos que sean atractivos para el autoestudio y el conocimiento autónomo sobre los avances en seguridad y ataques informáticos, que les sirvan durante la realización de sus estudios como para posteriormente en estudios superiores o en el desarrollo de sus funciones profesionales en el campo que elijan.

[1] A menos de 24 horas de su lanzamiento, la Nintendo Switch Online ha sido hackeada para añadir nuevos ROMs de juegos clásicos. (s. f.). Recuperado 9 de julio de 2019, de https://www.xataka.com/videojuegos/a-24-su-lanzamiento-nintendo-switch-online-ha-sido-hackeada-para-anadir-nuevos-roms-juegos-clasicos

5. Estructura de la Formación Profesional en la familia de Informática y Comunicaciones.

Se ha desarrollado una búsqueda sobre los diferentes estudios de una rama específica de la formación profesional, con las diferencias que tienen en las diferentes leyes orgánicas de la LOE 2/2006 de 3 de mayo y LOMCE 8/2013 de 9 de diciembre.

La rama elegida para investigar los estudios de formación profesional orientados ha sido informática y las comunicaciones, por ser la rama de la que provengo. La actividad principal ha sido hacer un pequeño estudio de sus currículos y atribuciones, competencias o cualificaciones profesionales que se obtienen al estudiar los diferentes niveles de la FP en España.

	**TÍTULOS LOGSE** **Familia: Informática**	**TÍTULOS LOE** **Familia: Informática y Comunicaciones**
	—	Título Profesional Básico en Informática de Oficina Título Profesional Básico en Informática y Comunicaciones
	Técnico en Explotación de Sistemas Informáticos	Técnico en Sistemas Microinformáticos y Redes
	Técnico Superior en Administración de Sistemas Informáticos Técnico Superior en Desarrollo de Aplicaciones Informáticas	Técnico Superior en Administración de Sistemas Informáticos en Red Técnico Superior en Desarrollo de Aplicaciones Multiplataforma Técnico Superior en Desarrollo de Aplicaciones Web

Tabla 1-Tabla de los estudios LOE y LOMCE para formación profesional en el campo de la informática y las comunicaciones.

La nueva organización que propone la LOE se diferencia en FP Básica, FP de Grado Medio y FP de Grado Superior, en el caso de la LOGSE los títulos sólo se organizaban en FP de Grado Medio y FP de Grado Superior.

5.1. Competencias Básicas y Contenidos de los títulos LOE de formación profesional para informática y comunicaciones.

5.1.1. Título profesional Básico en informática de Oficina.

Básicamente se tratan de las competencias de un técnico de oficina o ayudante para mantenimiento e instalación de los Sistemas Informáticos auxiliares (impresoras y escáneres) tratamiento de datos (digitales o no).

Las competencias que se atribuyen a los profesionales que superan esta formación son:

- Ayudante de montador de sistemas microinformáticos.
- Ayudante de mantenimiento de sistemas informáticos.
- Ayudante de instalador de sistemas informáticos.
- Ayudante de instalador de sistemas para transmisión de datos.
- Auxiliar de oficina.
- Auxiliar de servicios generales.
- Grabador-verificador de datos.
- Auxiliar de digitalización.
- Operador documental.

Los módulos que se imparten en este ciclo formativo son:

- Montaje y mantenimiento de sistemas y componentes informáticos.
- Operaciones auxiliares para la configuración y la explotación.
- Ofimática y archivo de documentos.
- Instalación y mantenimiento de redes para transmisión de datos.
- Ciencias aplicadas I.
- Ciencias aplicadas II.
- Comunicación y sociedad I.
- Comunicación y sociedad II.
- Formación en centros de trabajo

5.1.2. Título profesional Básico en Informática y Comunicaciones.

Más orientado a un técnico, que podríamos denominar de campo, tendríamos este módulo de formación que se aproxima más ayudante para instaladores de redes, teléfono y fax, enrutadores, etc. ayudante para mantenimiento de ordenadores, en

comparación con el otro título de formación básica este está más orientado a la electrónica y las comunicaciones.

- Ayudante de montador de antenas receptoras/ televisión satélite.
- Ayudante de instalador y reparador de equipos telefónicos y telegráficos.
- Ayudante de instalador de equipos y sistemas de comunicación.
- Ayudante de instalador reparador de instalaciones telefónicas.
- Ayudante de montador de sistemas microinformáticos.
- Ayudante de mantenimiento de sistemas informáticos.
- Ayudante de instalador de sistemas informáticos.
- Ayudante de instalador de sistemas para transmisión de datos.
- Operador de ensamblado de equipos eléctricos y electrónicos.
- Auxiliar de mantenimiento de equipos eléctricos y electrónicos.
- Probador/ajustador de placas y equipos eléctricos y electrónicos.
- Montador de componentes en placas de circuito impreso.

Los módulos que se imparten en este ciclo formativo son:

- Montaje y mantenimiento de sistemas y componentes informáticos.
- Operaciones auxiliares para la configuración y la explotación.
- Equipos eléctricos y electrónicos.
- Instalación y mantenimiento de redes para transmisión de datos.
- Ciencias aplicadas I.
- Ciencias aplicadas II.
- Comunicación y sociedad I.
- Comunicación y sociedad II.
- Formación en centros de trabajo

5.1.3. Técnico en Sistemas Microinformáticos y Redes.

Esta formación, que ya es de grado medio, proporciona las competencias para un técnico de informática para instalación de redes y mantenimiento equipos informáticos.

- Instalar y configurar software básico y de aplicación, redes locales cableadas, inalámbricas o mixtas y conectadas a redes públicas.
- Instalar, configurar y mantener servicios multiusuario, aplicaciones y dispositivos compartidos en un entorno de red local.
- Montar y configurar ordenadores y periféricos.
- Determinar la logística asociada a las operaciones de instalación, configuración y mantenimiento de sistemas microinformáticos.
- Diagnosticar disfunciones en sistemas microinformáticos y redes mediante pruebas funcionales.
- Replantear el cableado y la electrónica de redes locales en pequeños entornos y su conexión con redes de área extensa.

- Ejecutar procedimientos establecidos de recuperación de datos y aplicaciones ante fallos y pérdidas de datos en el sistema.
- Elaborar documentación técnica y administrativa del sistema, elaborar presupuestos y asesorar al cliente.

Los módulos que se imparten en este ciclo formativo son:

- Montaje y mantenimiento de equipo.
- Sistemas operativos monopuesto.
- Aplicaciones ofimáticas.
- Sistemas operativos en red.
- Redes locales.
- Seguridad informática.
- Servicios en red.
- Aplicaciones web.
- Formación y orientación laboral.
- Empresa e iniciativa empresarial.
- Formación en centros de trabajo

5.1.4. Técnico Superior en Administración de Sistemas Informáticos en Red

Un técnico Informático Superior en Administración de Sistemas Informáticos en red obtiene las competencias para administrar servidores y servicios de correo, por ejemplo. Sistemas de gestión de bases de datos, y todos aquellos sistemas informáticos de apoyo para el desarrollo y utilización de las tecnologías de la información en una empresa, organismo o institución tanto públicas como privadas.

Las ocupaciones y puestos de trabajo a los que puede dar acceso este título son amplias, pero las más relevantes pueden ser los siguientes:

- Técnico en administración de sistemas.
- Responsable de informática.
- Técnico en servicios de Internet.
- Técnico en servicios de mensajería electrónica.
- Personal de apoyo y soporte técnico.
- Técnico en teleasistencia.
- Técnico en administración de base de datos.
- Técnico de redes.
- Supervisor de sistemas.
- Técnico en servicios de comunicaciones.
- Técnico en entornos web.

Los módulos que se imparten en este ciclo formativo son:

- Implantación de sistemas operativos.
- Planificación y administración de redes.
- Fundamentos de hardware.
- Gestión de bases de datos.
- Lenguajes de marcas y sistemas de gestión de información.
- Administración de sistemas operativos.
- Servicios de red e Internet.
- Implantación de aplicaciones web.
- Administración de sistemas gestores de bases de datos.
- Seguridad y alta disponibilidad.
- Proyecto de administración de sistemas informáticos en red.
- Formación y orientación laboral.
- Empresa e iniciativa emprendedora.
- Formación en centros de trabajo.

A continuación, se presenta la relación de cualificaciones y unidades de competencia del Catálogo Nacional de Cualificaciones Profesionales incluidas en el título. Ordenadas por cualificaciones profesionales completas e incompletas.

Cualificaciones profesionales completas.

- Gestión de sistemas informáticos IFC152_3 (R.D. 1087/2005, de 16 de septiembre), que comprende las siguientes unidades de competencia.
  - UC0484_3 Administrar los dispositivos hardware del sistema.
  - UC0485_3 Instalar, configurar y administrar el software de base y de aplicación del sistema.
  - UC0486_3 Asegurar equipos informáticos.

- Administración de servicios de Internet IFC156_3 (R.D. 1087/2005, de 16 de septiembre), que comprende las siguientes unidades de competencia.
  - UC0495_3 Instalar, configurar y administrar el software para gestionar un entorno web.
  - UC0496_3 Instalar, configurar y administrar servicios de mensajería electrónica.
  - UC0497_3 Instalar, configurar y administrar servicios de transferencia de archivos y multimedia.
  - UC0490_3 Gestionar servicios en el sistema informático.

- Administración de bases de datos IFC079_3 (R.D. 295/2004, de 20 de febrero), que comprende las siguientes unidades de competencia:
  - UC0223_3. Configurar y explotar sistemas informáticos.
  - UC0224_3. Configurar y gestionar un sistema gestor de bases de datos.
  - UC0225_3. Configurar y gestionar la base de datos.

Cualificaciones profesionales incompletas.

- Desarrollo de aplicaciones con tecnologías web IFC154_3 (R.D. 1087/2005, de 16 de septiembre).

- UC0493_3 Implementar, verificar y documentar aplicaciones web en entornos internet, intranet y extranet.

5.1.5. Técnico Superior en Desarrollo de Aplicaciones Multiplataforma.

Un Técnico Superior en Desarrollo de Aplicaciones Multiplataforma podrá realizar tareas de desarrollo y programación de aplicaciones informáticas de gestión, dirigidas al sector empresarial y de los negocios. Además de la implementación de otras aplicaciones de propósito general, de entretenimiento y para dispositivos móviles.

Las ocupaciones y puestos de trabajo a los que puede dar acceso este título son amplias, pero las más relevantes pueden ser los siguientes:

- Desarrollar aplicaciones informáticas para la gestión empresarial y de negocio.
- Desarrollar aplicaciones de propósito general.
- Desarrollar aplicaciones en el ámbito del entretenimiento y la informática móvil.

A continuación, se presenta la relación de cualificaciones y unidades de competencia del Catálogo Nacional de Cualificaciones Profesionales incluidas en el título. Ordenadas por cualificaciones profesionales completas e incompletas.

Los módulos profesionales de este ciclo formativo son los siguientes:

- Sistemas informáticos.
- Bases de Datos.
- Programación.
- Lenguajes de marcas y sistemas de gestión de información.
- Entornos de desarrollo.
- Acceso a datos.
- Desarrollo de interfaces.
- Programación multimedia y dispositivos móviles.
- Programación de servicios y procesos.
- Sistemas de gestión empresarial.
- Proyecto de desarrollo de aplicaciones multiplataforma.
- Formación y orientación laboral.
- Empresa e iniciativa emprendedora.
- Formación en centros de trabajo.

Cualificaciones profesionales completas.

- Programación en lenguajes estructurados de aplicaciones de gestión IFC155_3 (R.D. 1087/2005, de 16 de septiembre), que comprende las siguientes unidades de competencia.

  - UC0223_3: Configurar y explotar sistemas informáticos.
  - UC0226_3: Programar bases de datos relacionales.
  - UC0494_3: Desarrollar componentes software en lenguajes de programación estructurada.

- Programación con lenguajes orientados a objetos y bases de datos relacionales IFC080_3 (R.D. 295/2004, de 20 de febrero), que comprende las siguientes unidades de competencia:
  - UC0223_3: Configurar y explotar sistemas informáticos.
  - UC0226_3: Programar bases de datos relacionales.
  - UC0227_3: Desarrollar componentes software en lenguajes de programación orientados a objetos.

Cualificaciones profesionales incompletas.

- Administración y programación en sistemas de planificación de recursos empresariales y de gestión de relaciones con clientes IFC 363_3 (R.D. 1701/2007, de 14 de diciembre):
  - UC1213_3: Instalar y configurar sistemas de planificación de recursos empresariales y de gestión de relaciones con clientes.

- Programación de sistemas informáticos IFC303_3 (R.D. 1201/2007, de 14 de septiembre):
  - UC0964_3: Crear elementos software para la gestión del sistema y sus recursos.

5.1.6. Técnico Superior en Desarrollo de Aplicaciones Web.

Un Técnico superior en Desarrollo de Aplicaciones Web se dedicará aquellas tareas que tengan que ver con implementar, implantar, y mantener aplicaciones web, con independencia del modelo empleado y utilizando tecnologías específicas, garantizando el acceso a los datos de forma segura y cumpliendo los criterios de accesibilidad, usabilidad y calidad exigidas en los estándares establecidos.

Las ocupaciones y puestos de trabajo a los que puede dar acceso este título son amplias, pero las más relevantes pueden ser los siguientes:

- Programador Web.
- Programador Multimedia.
- Desarrollador de aplicaciones en entornos Web.

Los módulos profesionales de este ciclo formativo son los siguientes:

- Sistemas informáticos.
- Bases de datos.

- Programación.
- Lenguajes de marcas y sistemas de gestión de información.
- Entornos de desarrollo.
- Desarrollo web en entorno cliente.
- Desarrollo web en entorno servidor.
- Despliegue de aplicaciones web.
- Diseño de interfaces WEB.
- Proyecto de desarrollo de aplicaciones web
- Formación y orientación laboral.
- Empresa e iniciativa emprendedora.
- Formación en centros de trabajo.

A continuación, se presenta la relación de cualificaciones y unidades de competencia del Catálogo Nacional de Cualificaciones Profesionales incluidas en el título

Cualificaciones profesionales completas.

- Desarrollo de aplicaciones con tecnologías Web IFC154_3 (Real Decreto 1087/2005, de 16 de septiembre), que comprende las siguientes unidades de competencia:
  - UC0491_3 Desarrollar elementos software en el entorno cliente.
  - UC0492_3 Desarrollar elementos software en el entorno servidor.
  - UC0493_3 Implementar, verificar y documentar aplicaciones web en entornos internet, intranet y extranet.

Cualificaciones profesionales incompletas.

- Programación en lenguajes estructurados de aplicaciones de gestión IFC155_3 (Real Decreto 1087/2005, de 16 de septiembre).
  - UC0223_3 Configurar y explotar sistemas informáticos.
  - UC0226_3 Programar bases de datos relacionales.

- Programación con lenguajes orientados a objetos y bases de datos relacionales IFC 080_3 (Real Decreto. 295/2004, de 20 de febrero).
  - UC0223_3 Configurar y explotar sistemas informáticos.
  - UC0226_3 Programar bases de datos relacionales.

6. La Seguridad Informática y Privacidad de datos en la Formación Profesional.

Uno de los objetivos de este TFM es la búsqueda de los diferentes objetivos y contenidos sobre los que debería construirse un currículo de Seguridad Informática, adaptado a las necesidades laborales y los avances en el campo de la seguridad, en los estudios de FP dentro de la familia de la Informática y Comunicaciones que se ofrecen en el ámbito de la Educación en España. Objetivos y contenidos fundamentales de la seguridad en las programaciones de los módulos específicos de Seguridad Informática que se ven en estos estudios.

En estas asignaturas, en el caso de las que más completan unos objetivos de seguridad informática, de libre configuración los objetivos de las asignaturas están orientados a:

- La seguridad informática, como concepto y ámbitos de aplicación.
- Las amenazas informáticas, tipos que hay e implicaciones de los ataques o amenazas informáticas.
- La protección de los sistemas informáticos: antivirus, antyspyware, etc.
- La identidad digital, tanto en aspectos de identidad en las redes sociales e internet, como certificados y sistemas electrónicos de identificación en sistemas informáticos.
- La protección de datos y de la información, aspectos legales e implicaciones de los datos que se comparten con empresas públicas o privadas.
- Riesgos, implicaciones y consecuencias de los ataques informáticos y de la Seguridad Informática en las comunicaciones y sistemas informáticos.

Si bien en los estudios de Grado Medio de SMR no se profundiza en aspectos de seguridad como la auditoría, el cifrado de la información o gestión de la seguridad en sistemas informáticos, sí que dan una visión muy general y a nivel usuario de la seguridad en las TIC y su aplicación y gestión en el entorno de redes.

6.1. Seguridad informática en la Formación Profesional

En Formación Profesional (FP) hay tres niveles de estudios: básico, medio y superior. Para este estudio de la seguridad Informática en los estudios no universitarios se ha descartado el nivel básico, ya que en estos estudios no se desarrollan objetivos ni contenidos significativos que tengan relación con la Seguridad Informática.

Aunque en todos los estudios de Formación Profesional de Grado Medio y/o Superior se contempla algún aspecto de seguridad, las únicas titulaciones que ofrecen un módulo específico para la Seguridad Informática son: el Grado Medio de Técnico en Sistemas Microinformáticos y Redes, SMR, y el Grado Superior de Técnico Superior en

Administración de Sistemas Informáticos en Red, ASIR. Estos dos títulos son los que van a ser objetivo de nuestro análisis en profundidad de los objetivos, contenidos y metodologías. Aunque se ha realizado un estudio de todos los módulos para asegurar cuáles de ellos se deben descartar por encontrarse fuera del alcance o de los objetivos de este TFM.

A continuación, se van a presentar los objetivos y contenidos relativos a Seguridad Informática de los estudios de grado medio y grado superior de FP en España, dichos objetivos y contenidos se han obtenido las programaciones de diferentes centros que imparten estos estudios.

FP Grado Medio: Técnico en Sistemas Microinformáticos y Redes (SMR)

En esta titulación de grado medio hay un módulo específico de seguridad informática, que se suele desarrollar en el 2º curso, en el periodo previo a la realización de prácticas de alumnos en empresas. Con la aparición de la formación dual, formación que recibe el alumno en la empresa coordinado y compatibilizado con sus estudios, muchos alumnos no cursan este módulo, por lo que puede darse el caso de que un alumno en su formación dual no reciba los resultados de aprendizaje de este módulo en concreto.

De cualquier modo, los objetivos de este módulo de Seguridad Informática están divididos en cinco bloques claramente diferenciados, de los cuales se puede, de forma general, extraer los siguientes objetivos:

- Aplicación de medidas de seguridad pasiva: el alumno debe saber aplicar medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.

- Gestión de dispositivos de almacenamiento: el objetivo principal es aprender a gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

- Aplicación de mecanismos de seguridad activa: como en seguridad pasiva, se trata de aplicar mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.

- Aseguramiento de la privacidad: el alumno debe obtener las herramientas y técnicas para asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico

- Cumplimento de la legislación y las normas sobre seguridad: tiene como objetivo reconocer la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

Además, en varios módulos se ven aspectos de Seguridad Informática, concretamente dentro del módulo de Redes Locales hay contenidos referidos a la seguridad que se desarrollan tanto en aspectos de tipos seguridad activa y pasivo, o los diferentes niveles de la misma, ataques o configuraciones de red seguras. También en los módulos de

Sistemas Operativos se ven algunos aspectos de accesos de usuarios al sistema, cifrado de archivos, etc.

Grado Superior: Técnicos Superior en Administración de Sistemas Informáticos en Red (ASIR)

En el grado superior de asir, hay un módulo específico de Seguridad y Alta disponibilidad, de una media de 100 horas de duración, según el centro y el currículo de la comunidad autónoma.

Este módulo pretende que los alumnos obtengan las siguientes competencias profesionales:

- Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.
- Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.
- Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.
- Administrar usuarios de acuerdo a las especificaciones de explotación para garantizar los accesos y la disponibilidad de los recursos del sistema.
- Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.

En cuanto a objetivos son:

- Adoptar pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
- Implantar mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
- Implantar técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.
- Implantar cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.
- Instalar servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.
- Instalar soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.
- Conocer la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

Además, la seguridad informática tiene objetivos definidos en otros módulos de esta titulación, que son: Planificación y Administración de Redes, Administración de Sistemas Operativos y Servicios de Red e Internet, ya que el grueso de contenidos versa que sobre la seguridad de los sistemas operativos y la infraestructura de red.

FP Grado Superior: Técnicos Superior en Desarrollo de Aplicaciones Multiplataforma (DAM)

No se desarrolla un módulo específico que tenga que ver con la seguridad, aunque en muchos de los módulos se ven algunos conceptos y tienen contenidos con esta materia. Como la seguridad de acceso a las aplicaciones, seguridad en las comunicaciones, manejo de protocolos de seguridad. Sobre todo, van orientados hacia la seguridad de sistemas, solo en algunos casos nombra las pruebas de seguridad en el proceso de desarrollo de aplicaciones, que sería uno de los campos interesantes a desarrollar en este módulo.

FP Grado Superior: Técnicos Superior en Desarrollo de Aplicaciones Web (DAW)

Como en el caso anterior, no hay un módulo específico de Seguridad Informática, y tienen unos objetivos y contenidos muy parecidos. En este caso hay algún desarrollo más orientado los sistemas de seguridad de un servidor de aplicaciones web.

7. Concreción de la Seguridad informática en currículos

Como ya hemos comentado en el punto *"4. Estructura de la Formación Profesional en la Familia de Informática y Comunicaciones"*, los únicos títulos en los que se desarrolla un módulo específico de Seguridad Informática son los de SMR y ASIR. Por lo que son en los que vamos a centrar este primer acercamiento a los objetivos que se definen en estos estudios.

Este estudio de los objetivos actuales se va a basar en dos vertientes: por un lado, las programaciones didácticas de estos estudios para diferentes centros y por otro las recomendaciones que se dan por parte de entidades como IEEE o ACM.

7.1. Objetivos de Seguridad Informática en la FP actual

Los objetivos de las programaciones didácticas de los módulos de Seguridad Informática en Formación Profesional, tanto para SMR como para ASIR, se basan en los objetivos que fijan las entidades públicas estatales y regionales.

Por lo que en la mayoría de los casos los objetivos son comunes dentro de la misma región o comunidad, y solo se diferencian en algunos aspectos mínimos que pueden llegar a legislar los consejos, de gobierno o de educación según el caso, de cada región o autonomía.

En este punto lo que se ha intentado es realizar un compendio y agrupamiento de estos objetivos, de diferentes programaciones didácticas y comunidades autónomas, para poder identificar los objetivos que se imparten en cada uno de los módulos citados dentro del ámbito de estos estudios en España.

7.1.1. Objetivos para los estudios de Grado medio de SMR

Los objetivos del módulo de Seguridad Informática en SMR de las programaciones didácticas que se han estudiado objetivos están definidos por:

- REAL DECRETO 1691/2007, de 14 de diciembre, por el que se establece el título de Técnico en Sistemas Microinformáticos y Redes y se fijan sus enseñanzas mínimas (BOE 17/01/2008).

- DECRETO 34/2009, de 2 de abril, del Consejo de Gobierno de la Comunidad de Madrid, por el que se establece para la Comunidad de Madrid el currículo de ciclo formativo de grado medio correspondiente al título de Técnico en Sistemas Microinformáticos y Redes (BOCM 20/04/2009).

- DECRETO 59/2009, de 3 de septiembre, por el que se establece el currículo correspondiente al Título de Técnico en Sistemas Microinformáticos y Redes en la Comunidad de Castilla y León (BOCYL 09/09/2009).

- DECRETO 193/2013, de 9 de julio, por el que se establece el currículo del ciclo formativo de grado medio de sistemas microinformáticos y redes en Catalunya (CVE-DOGC Núm. 6415-11/07/2013).

- ORDEN de 29 de julio 2009, de la Consejería de Educación de la Comunidad Valenciana, por la que se establece para la Comunitat Valenciana el currículo del ciclo formativo de Grado Medio correspondiente al título de Técnico en Sistemas Microinformáticos y Redes. (DOCV Núm. 6094-03/09/2013)

- ORDEN de 26 de junio de 2009, de la Consejera de Educación, Cultura y Deporte de Aragón, por la que se establece el currículo del título de Técnico en Sistemas Microinformáticos y Redes para la Comunidad Autónoma de Aragón.

De esta manera, los objetivos que deben desarrollar los alumnos que cursan los módulos específicos de Seguridad Informática en SMR, que se pueden obtener de la documentación anterior y de algunas programaciones didácticas de este módulo son:

a) Aplicar medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.

b) Aplicar mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.

c) Gestionar dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

d) Realizar las pruebas funcionales en sistemas microinformáticos y redes locales, localizando y diagnosticando disfunciones, para comprobar y ajustar su funcionamiento.

e) Asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

f) Reconocer la legislación y normativa sobre seguridad y protección de datos analizándolas repercusiones de su incumplimiento.

g) Identificar, ensamblar y conectar componentes y periféricos utilizando las herramientas adecuadas, aplicando procedimientos, normas y protocolos de calidad y seguridad, para montar y configurar ordenadores y periféricos.

h) Ejecutar procedimientos establecidos de recuperación de datos y aplicaciones ante fallos y pérdidas de datos en el sistema, para garantizar la integridad y disponibilidad de la información

i) Ubicar y fijar equipos, líneas, canalizaciones y demás elementos de una red local cableada, inalámbrica o mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.

j) Sustituir y ajustar componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.

k) Interpretar y seleccionar información para elaborar documentación técnica y administrativa.

l) Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.

m) Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas.

n) Analizar y describir procedimientos de calidad, prevención de riesgos laborales y medioambientales, señalando las acciones a realizar en los casos definidos para actuar de acuerdo con las normas estandarizadas.

o) Identificar y valorar las oportunidades de aprendizaje y empleo, analizando las ofertas y demandas del mercado laboral para gestionar su carrera profesional.

7.1.2. Objetivos para los estudios de Grado Superior de ASIR.

Los objetivos del módulo de Seguridad Informática en SMR de las programaciones didácticas que se han estudiado objetivos están definidos por:

a) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.

b) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.

c) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.

d) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.

e) Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.

f) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.

g) Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para resolver problemas y mantener una cultura de actualización e innovación.

h) Reconocer sus derechos y deberes como agente activo en la sociedad, analizando el marco legal que regula las condiciones sociales y laborales para participar como ciudadano democrático.

i) Adoptar pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

j) Implantar mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

k) Implantar técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

l) Implantar cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

m) Implantar servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

n) Implantar soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.

o) Reconocer la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

p) Implantar soluciones de alta disponibilidad

q) Uso de técnicas seguras de acceso remoto a un sistema.

8. Propuesta de objetivos para Seguridad Informática en Formación Profesional

Los objetivos de Seguridad en los módulos de Formación Profesional, además de la configuración y administración adecuada de equipos, sistemas, servidores y la infraestructura de red, también debe abarcar las políticas y procedimientos relacionados con el control de acceso y la auditoría de los elementos ya citados.

Dentro de estos objetivos generales de la Seguridad Informática también habría que incluir el conocimiento y la utilización de las metodologías que habitualmente utilizan los hackers en ataques informáticos, sabiendo reutilizarlas y orientarlas hacia la auditoría de los sistemas informáticos y su uso ético, en lo que se denomina Hacking Ético.

Comprender y analizar las necesidades actuales de los sistemas informáticos, en cuanto a seguridad, traducidos en los objetivos generales que se presentan a continuación, deberían conducir a la conclusión de programas de estudios en los que realmente se utilicen técnicas y conceptos innovadores de Seguridad Informática, ya que con el avance rápido de los riesgos, vulnerabilidades y ataques de sistemas informáticos, se hace necesario formar a profesionales que entiendan y sepan adaptarse rápidamente a estas evoluciones.

Por lo tanto, el enfoque de cualquier programa de formación orientado a la Seguridad Informática y la práctica profesional, debería ser desarrollar e implementar soluciones de cualquier índole para las necesidades de seguridad reales de una empresa o un usuario de sistemas informáticos a través del conocimiento y control de los riesgos, los ataques, incidentes, vulnerabilidades y fallos de seguridad.

Los siete objetivos generales para estos títulos o módulos que se orientan hacía la Seguridad Informática serían:

- Crear soluciones para el control de ataques y fallos de seguridad.
- Implementar y desarrollar buenas prácticas para asegurar la seguridad y controlar las vulnerabilidades de los sistemas informáticos.
- Comunicar e implantar las estrategias de seguridad necesarias para asegurar el funcionamiento correcto de todos los sistemas.
- Identificar e implementar sistemas de control e identificación para el acceso los sistemas e información de una infraestructura en red.
- Integrar hardware y software de supervisión, auditoría y control en tiempo real de la seguridad y disponibilidad de los sistemas.

- Reconocer y comprender el diseño de software y algoritmos de cifrado de la información que se transmite por servicios distribuidos y protocolos de red.

- Identificar y entender los riesgos de la Seguridad Informática, así como las implicaciones éticas, morales, sociales y profesionales de las herramientas informáticas y su uso no lícito.

Por otro lado, fuera de los objetivos específicos de la Seguridad Informática, para que el alumno profundice en los conceptos de Seguridad Informática, que le resulten más interesantes para su desarrollo profesional, habrá que facilitar las herramientas y métodos necesarios para investigue en ellos y se promueva el conocimiento autónomo.

Se podrían desarrollar otros objetivos más transversales que busquen el desarrollo de habilidades blandas y competencias como el pensamiento crítico, el autoaprendizaje y la investigación. Pero no es el cometido de este punto, en el que se busca la concreción, desarrollo y ampliación de unos objetivos específicos de la Seguridad Informática.

8.1. Objetivos de la Seguridad Informática en SMR

Según el contexto y el tipo de alumnado que se suele dar en los estudios de Formación Profesional de Grado Medio, que son prácticamente una vía de acceso a una formación básica que se supondrá se ampliará durante la carrera profesional de alumno o con la continuación de otros estudios, los objetivos que se deben plantear han de abarcar los siete objetivos generales planteados en el punto anterior, pero sin profundizar en aspectos excesivamente teóricos o complejos.

De esta manera el alumno debería obtener una visión global de la Seguridad Informática, las técnicas, métodos y herramientas que se deben utilizar para asegurar los requisitos necesarios de seguridad en redes y dispositivos informáticos, así como las que se utilizan en los ataques informáticos.

8.1.1. Principios de seguridad

- Conocer e identificar los diferentes los tipos de seguridad: activa y pasiva.

- Conocer y aplicar los diferentes niveles de seguridad.

- Conocer e identificar los diferentes tipos de amenazas, ataques y vulnerabilidades.

- Instalar y gestionar las herramientas básicas de protección contra ataques, virus y amenazas en sistemas informáticos.

8.1.2. Privacidad y protección de la información

- Diferenciar los tipos de protocolos de comunicaciones seguros y no seguros.

- Conocer diferentes algoritmos de cifrado de información.

- Instalar y manejar diferentes tipos de certificados y cifrado de aplicaciones informáticas.

8.1.3. Protección y privacidad en redes locales e inalámbricas

- Implementar y configurar servicios de red seguros.

- Despliegar redes cableadas e inalámbricas seguras.

- Configurar controles de acceso y cifrado de datos en redes inalámbricas y cableadas.

- Instalar y configurar elementos de protección en redes.

- Identificar y auditar infraestructuras de red.

8.1.4. Legislación y normas de protección de datos y seguridad

- Conocer e implantar las necesidades de seguridad en función a la legislación y normativa actual para la protección de la privacidad y la información de los usuarios.

- Entender las implicaciones éticas y morales del tratamiento de información sensible.

- Discutir y determinar las implicaciones de uso de herramientas de hacking.

8.2. Objetivos de la Seguridad Informática en ASIR

Los objetivos estos estudios deberían ser la continuación y ampliación de los objetivos del módulo de grado medio de SMR.

8.2.1. Amenazas, ataques y vulnerabilidades

- Conocer, identificar y comparar los diferentes tipos de ataques

- Analizar y determinar indicadores de compromiso de seguridad en escenarios virtualizados.

- Explicar y analizar los tipos y atributos de los diferentes actores en ataques informáticos.
- Identificar las consecuencias e impacto asociados a los diferentes tipos de ataques y vulnerabilidades del sistema.

- Entender los conceptos asociados a pruebas de penetración y de búsqueda de vulnerabilidades.

8.2.2. Tecnologías y herramientas de seguridad

- Instalar y configurar componentes de seguridad, tanto software como hardware, en sistemas en red.

- Utilizar las herramientas hardware y software para evaluar la seguridad de sistemas en red.

- Solucionar ataques y vulnerabilidades de seguridad comunes.

- Analizar e interpretar los resultados de los análisis de vulnerabilidades y seguridad.

- Implementar y desplegar dispositivos móviles y de internet de las cosas de manera segura en una red.

- Conocer e implementar protocolos seguros de comunicación.

8.2.3. Arquitecturas y diseño de seguridad

- Definir y adaptar casos de uso, frameworks de seguridad, guías de configuración y de buenas prácticas de seguridad para sistemas en red.

- Implementar y desplegar arquitecturas y diseños de redes seguras en escenarios virtuales.

- Dar ejemplos y clasificar los sistemas de almacenamiento seguro en la nube y en red.

- Clasificar y explicar los conceptos de seguridad asociados a sistemas empotrados.

- Dar ejemplos y clasificar los sistemas de virtualización seguros.

- Implementar elementos de control y seguridad físicos.

8.2.4. Identidades digitales y control de acceso

- Identificar y comparar los conceptos de identidad y control de acceso.
- Implementar, instalar y configurar sistemas hardware y software de identificación y control de acceso en sistemas en red.
- Comprender y utilizar el control y firma con certificados digitales.
- Instalar y configurar sistemas y protocolos seguros usando certificados digitales propios.

8.2.5. Gestión de seguridad: riesgos y vulnerabilidades

- Analizar y explicar la importancia de las políticas, planes y procedimientos de seguridad para asegurar la seguridad en los sistemas en red.
- Exponer y explicar los conceptos y procesos de gestión de riesgos de seguridad.
- Entender e implementar los procedimientos de gestión y seguimiento de respuesta ante ataques e incidentes de seguridad.
- Implementar y desarrollar prácticas de seguridad y privacidad en escenarios virtuales.

8.2.6. Criptografía y cifrado de información.

- Entender y comparar los diferentes conceptos de cifrado y criptografía.
- Identificar y explicar los diferentes tipos de algoritmos de criptografía y sus principios básicos.
- Instalar, configurar y desplegar entornos de red inalámbrica seguras.
- Instalar, configurar y desplegar infraestructuras de clave pública.

9. Ampliación de contenidos de Seguridad Informática en Formación Profesional.

Los contenidos que se deben desarrollar los módulos profesionales de FP quedan organizados y establecidos en función de los objetivos definidos en punto anterior de este documento. De la misma manera se deben organizar y secuenciar de tal forma que faciliten en lo posible su asimilación, distribuyéndose en lo bloques o unidades didácticas coherentes y realizables por los alumnos objetivo de cada uno de los módulos objeto de estudio de este TFM.

Cada apartado o tema en los que se han dividido los contenidos están definidos por tres elementos: primero los conceptos clave de cada tema, segundo los ejemplos, técnicas, herramientas y/o tecnología que se relacionan con cada tema y por último los resultados de aprendizaje que se desarrollan en el tema seleccionado.

Conceptos clave	Conceptos clave, principios y definición de contenidos de un tema.
Ejemplos, técnicas, herramientas y tecnología	Definiciones, ejemplos, metodologías, herramientas y tecnologías que se asocian o se utilizan para ilustrar la aplicación o implementación del tema seleccionado.
Resultados de Aprendizaje	La comprensión, el conocimiento, aprendizaje y aplicación que se espera de los alumnos en cada tema.

Tabla 2- Organización de los contenidos de los módulos de FP

9.1. Contenidos de Seguridad Informática para FP de Grado Medio de SMR

9.1.1. Introducción y principios de Seguridad Informática.

Los contenidos dirigidos a la introducción de la Seguridad Informática, sus conceptos básicos y actores que participan de la misma. Realizando una instrucción a los protocolos, algoritmos criptográficos, tipos de técnicas y herramientas de Seguridad Informática, principios de autenticación, tipos de ataques y software malicioso.

Los contenidos de este bloque serían:

- Introducción a la Seguridad Informática: principios, términos y actores fundamentales.

- Requisitos de seguridad en cuanto a confidencialidad, integridad y disponibilidad.

- Confidencialidad: privacidad y confidencialidad de la información.
- Privacidad y almacenamiento de la información.
- Diferencias entre integridad de la información e integridad de los sistemas o servicios.
- Disponibilidad y acceso autorizado a servicios en red.

- Acrónimos, protocolos de seguridad, definiciones técnicas críticas de Seguridad Informática: TCP / IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, DNS, etc.

- Tipos de seguridad: activa y pasiva.

- Tipos de ataques y vulnerabilidades.

Conceptos clave	
• Principios de Seguridad • Conceptos básicos de Seguridad • Actores y componentes de los sistemas de Seguridad Informática	• Confidencialidad, integridad y disponibilidad • Protocolos de seguridad • Seguridad Activa y Pasiva • Tipos de ataques y vulnerabilidades
Tecnología y herramientas	
• Tipos de protocolos seguros y no seguros • Herramientas de seguridad activa	• Componentes de la seguridad pasiva • Características de los diferentes tipos de ataques
• Resultados de aprendizaje	
• Conocer los conceptos básicos de Seguridad Informática • Utilizar un lenguaje y términos correctos de Seguridad Informática • Identificar los actores en la Seguridad Informática	• Definir las necesidades de la Seguridad Informática en función de los requisitos de confidencialidad, integridad y disponibilidad • Diferencias entre vulnerabilidad, amenaza y ataque • Conocer y definir tipos de ataques

Tabla 3 - Contenidos para SMR: Introducción y principios de Seguridad Informática

9.1.2. Protección y seguridad de la información

En este tema o unidad se pretende dar una visión general de la seguridad de la información, esto incluye la seguridad y almacenamiento de la información, tanto en local, en red o en servicios distribuidos o en la nube, y una introducción al cifrado de la información.

- Soportes de almacenamiento de la información:

- Almacenamiento distribuido de la información: copias locales y remotas, servicios de almacenamiento distribuido en red y en la nube.

- Eliminación segura de la información.

- Cifrado y criptografía de la información: cifrado simétrico y asimétrico.

Conceptos clave	
· Almacenamiento de la Información · Clusters de Servidores · Redundancia y distribución de la Información · Recuperación de información · Tratamiento seguro de la información	· Cifrado de información · Certificados digitales y firma electrónica · Algoritmos de Criptografía simétrica · Algoritmos de Criptografía asimétrica · Infraestructura de clave pública
Tecnología y herramientas	
· Samba · Almacenamiento en la nube: Owncloud, NextCloud · PKI · Certificados digitales · Firma Digital	· File Inyector · Esteganografía · Método LSB · Low Bit Encoding · Discrete Cosine Transform (DCT)
Resultados de aprendizaje	
· Valora la importancia de la seguridad de la información y los datos · Contempla factores y características del almacenamiento de la información: rendimiento, disponibilidad, accesibilidad, etc. · Maneja e instala sistemas de almacenamiento en red y en la nube	· Maneja e instala sistemas de identificación como la firma electrónica, certificado digital, entre otros · Utiliza métodos de cifrado de información · Conoce diferentes métodos y técnicas de codificación y ocultación de información

Tabla 4 - Contenidos para SMR: Protección y Seguridad de la Información

9.1.3. Protección y privacidad en redes cableadas e inalámbricas.

Los contenidos de seguridad, protección en redes cableadas e inalámbricas buscará el conocimiento general de los conceptos como: disuasión, prevención, detección y respuesta a cualquier tipo de vulnerabilidad o ataque a los dispositivos que componen una red.

Conceptos clave	
· Identificación digital · Sistemas biométricos · Protocolos de comunicación seguros · Protocolos de cifrado y seguridad en comunicaciones inalámbricas · Cortafuegos	· Control de acceso · Fraudes informáticos · Ataques informáticos · Software malicioso · Monitorización · Hacking
Tecnología y herramientas	
· Herramientas de filtrado de paquetes · Firewalls hardware · Firewalls software · Herramientas de ataques informáticos	· Servidores DNS: PiHole, AdAway · Proxies: HotSpot, AFW Proxy Server · Monitorización de accesos y seguridad · Gestión de eventos de seguridad
Resultados de aprendizaje	
· Utiliza sistemas de seguridad activa · Maneja sistemas de monitorización de redes · Conoce los diferentes tipos de ataques · Configura firewalls y sistemas de seguridad en redes	· Instala y configura redes inalámbricas seguras · Conoce y maneja las técnicas de ataques informática · Bloqueo de la publicidad y comunicaciones no deseadas

Tabla 5 - Contenidos para SMR: Protección y privacidad en redes cableadas e inalámbricas

9.1.4. Ética y normativa de Seguridad Informática.

Los contenidos de ética en la Seguridad Informática están orientados hacia el análisis y estudio de los comportamientos respecto al uso de la información y su privacidad. Así como al análisis y estudio de conceptos como delitos informáticos, fraudes, marcos legales y normativas de protección de la información.

Conceptos clave	
· Cibercimen · Delitos informáticos · Hacking · Hacking ético	· Fraudes · Marcos legales · Información sensible · Leyes de protección de datos

Tecnología y herramientas	
▪ Ley Orgánica de Protección de Datos (LOPD) ▪ Reglamento General de Protección de Datos Europeo (GPRD)	▪ Buenas prácticas éticas en seguridad Informática. ▪ Planes de actuación ante eventos de seguridad
Resultados de aprendizaje	
▪ Reconoce hitos e implicaciones de la Seguridad Informática. ▪ Utiliza lenguaje y contenidos éticos.	▪ Debate y analiza las implicaciones de la propiedad intelectual ▪ Analiza las implicaciones de técnicas de recopilación de datos masiva.

Tabla 6 - Contenidos para SMR: Ética y Normativa de Seguridad Informática

9.2. Contenidos de Seguridad Informática para FP de Grado Superior de SMR

9.2.1. Seguridad de la Información

La privacidad y la seguridad de la información es uno de los temas más importantes en los últimos tiempos, por la proliferación de conceptos como la sociedad de la información, los servicios en la nube, Internet de las Cosas (IOT) o conceptos de BigData.

Por eso se hacen necesarios los conocimientos en cuanto a la gestión, análisis de riesgos, vulnerabilidades, ataques y amenazas sobre los sistemas de información.

Conceptos clave	
· Utilidad e importancia de la Información · Tipos de información y datos · Ciclo de vida de la información · Características de la información · Sistemas de Información · Normativas y estándares de seguridad de la Información.	· Riesgos, peligros y vulnerabilidades de la información. · Riesgos del procesamiento y almacenamiento de la información. · Riesgos de los factores humanos · Sistemas maliciosos · Estándares de gestión de riesgos.
Tecnología y herramientas	
· NIST SP800-30 · Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) · CCTA Risk Analysis and Management Method (CRAMM) · ISO 31000	· ISO/IEC 27005 · Sistemas de control de acceso, autenticación y autorización · Auditoria de sistemas de Información · Sistemas de denegación de acceso
Resultados de aprendizaje	
· Reconoce la importancia de la definición de la seguridad para la información · Define el ciclo de vida de la información: creación, almacenamientos y eliminación · Aplica conceptos de auditoría de seguridad.	· Entiende la naturaleza dinámica y evoluciones de la seguridad informática · Clasifica y categoriza las amenazas y ataques según importancia y probabilidad. · Entiende y aplica estándares de seguridad

Tabla 7 - Contenidos para ASIR: Seguridad de la Información

9.2.2. Amenazas y ataques en Seguridad Informática

Actualmente los sistemas de información pueden recibir gran cantidad de ataque diferentes, según crecen los sistemas, las funcionalidades que tienen y los servicios que proporcionan aumentan las amenazas y riesgos.

Es importante entender las metodologías que se utilizan en los ataques informáticos, como funcionan y que objetivos persiguen. Y todo ello con la finalidad de poder defenderse de estos ataques.

Conceptos clave	
· Amenazas. · Ataques informáticos. · Objetivos de ataques. · Ingeniería Social. · Tipos de malware · Ataques combinados · La mentalidad Hacker · Ataques específicos y dirigidos.	· Rutas de ataque. · Evidencias y monitorización de ataques informáticos. · Patrones y metodologías de ataques informáticos. · Nuevos a taques a servicios en la nube · Ataques a la Industria, adquisición de datos y a Internet de las Cosas (IOT)
Tecnología y herramientas	
· Clasificación y caracterización de amenazas y ataques · Vulnerabilidades, defectos y bugs. · Herramientas de reconocimiento de ataques	· Test de vulnerabilidad · Ataques típicos: DDOS, phishing, ingeniería social · Open Web Application Security Project (OWASP)
Resultados de aprendizaje	
· Diferencia entre amenaza, ataque, riesgo y vulnerabilidad · Identifica como las amenazas se transforman en ataques	· Maneja bases de información confiables sobre amenazas y ataques a sistemas de información · Analiza en profundidad de ataques informáticos

Tabla 8 - Contenidos para ASIR: Amenazas y ataques en Seguridad Informática

9.2.3. Arquitecturas y servicios en Seguridad Informática

Los sistemas de seguridad se componen de métodos, técnicas y procedimientos para asegurar la Seguridad Informática de todo un sistema, tanto la información, los servicios y los procedimientos.

Normalmente todos estos componentes se organizan en planes y marcos de actuación para asegurar la confiabilidad y uso seguro de dichos sistemas. Para ello se crea toda una arquitectura e infraestructura de servicios de Seguridad Informática.

Conceptos clave	
· Confiabilidad de servicios · Arquitectura de Seguridad Informática · Procesos de seguridad · Control de la seguridad	· Sistemas de defensa · Técnicas de control de la seguridad · Test y auditoria · Monitorización ·
Tecnología y herramientas	
· Confiabilidad de servicios · Arquitectura de Seguridad Informática · Procesos de seguridad · Control de la seguridad	· Sistemas de defensa · Técnicas de control de la seguridad · Test y auditoria · Monitorización
Resultados de aprendizaje	
· Conoce los tipos de control de la seguridad: prevención, detección, respuesta y acciones correctivas · Conoce y aplica técnicas de control de la seguridad como la criptografía, la gestión de acceso, dispositivos de seguridad de red y cómo funcionan	· Maneja técnicas forenses, de investigación y monitorización de cómo se han llevado a cabo los ataques informáticos · Aplica técnicas y herramientas para la gestión de la seguridad

Tabla 9 - Contenidos para ASIR: Arquitecturas y servicios en Seguridad Informática

9.2.4. Sistemas y aplicaciones en Seguridad Informática

Para asegurar completamente la seguridad de un sistema, hay que asegurar la seguridad de cada uno de sus componentes. El proceso de análisis y desarrollo de aplicaciones, servidores, servicios, dispositivos deben establecerse sobre unos principios de seguridad, que además permitan el desarrollo de los requisitos funcionales y los estándares de calidad de los mismos.

Conceptos clave	
· Diseño, creación y test de sistemas y software seguros · La seguridad en el ciclo de vida del software · Seguridad y calidad · Tolerancia a fallos y limitación del daño	· Aumento de las políticas de seguridad · Requisitos de seguridad en el diseño funcional de sistemas seguros · Comunicaciones, acceso remoto, control de acceso y conectividad · Diseño orientado a la resiliencia

Tecnología y herramientas	
· Capability Maturity Model (CMM) · BS PAS 754 · Building Security In Maturity Model Software Security Framework (BSSIM SSF) · Open Web Application Security Project (OWASP)	· ISO/IEC 27034 · Implementación segura de sistemas y servicios · Test de seguridad sobre componentes y librerías externas · Programación defensiva
Resultados de aprendizaje	
· Entiende la importancia de los requisitos y funcionalidades para desarrollas sistemas seguros · Aplica procesos de diseño de sistemas seguros	· Entiende, analiza y aplica estándares de seguridad en el desarrollo de aplicaciones y sistemas

Tabla 10 - Contenido para ASIR: Sistemas y aplicaciones en Seguridad Informática

9.2.5. Gestión de la Seguridad Informática

Este tema se centra en los sistemas de gestión de la Seguridad Informática en un entorno empresarial. Con el objetivo de diseñar y auditar la seguridad en los sistemas de una empresa.

Conceptos clave	
· Gestión de la seguridad de la información · Políticas, estrategias y planes de Seguridad Informática · Prácticas éticas en seguridad	· Privacidad de la información · Datos sensibles · Recuperación de ataques · Análisis y auditoría
Tecnología y herramientas	
· Estándares para crear marcos de actuación de seguridad · ISO/IEC 27001 Information Security Management System · ISO/IEC 27005 risk management · ISO 22301	· ISO/IEC 27031 · Estrategias de Seguridad Informática · Herramientas para definir políticas de accesos y seguridad · Procedimientos de gestión de ataques y fallos de seguridad ·

Resultados de aprendizaje	
· Utiliza e implementa planes de gestión de la seguridad · Implementa estándares de seguridad · Describe técnicas y herramientas para la gestión de la seguridad	· Entiende, analiza e implementa regulaciones y aspectos legales de la seguridad · Estructura los componentes de una solución de seguridad completa

Tabla 11 - Contenido para ASIR: Gestión de la Seguridad Informática

10. Metodologías para Seguridad Informática en Formación Profesional.

Podemos definir la metodología como el conjunto de técnicas y herramientas que organizan, de manera global, el proceso de enseñanza-aprendizaje.

Las programaciones didácticas y la concreción de currículos de centros de Formación Profesional que se han revisado no concretan que metodologías se utilizarán en el aula para el aprendizaje de la Seguridad Informática.

En este punto, se pretende realizar un estudio y presentación de aquellas metodologías que podrían ser más interesantes para alcanzar los objetivos de la Seguridad Informática en la Formación Profesional. Indicando que ventajas e inconvenientes se pueden obtener del uso de cada una de estas metodologías.

Para desarrollar una metodología correcta para la enseñanza y la transmisión de los objetivos y contenidos necesarios respecto a la Seguridad Informática, presentados en los apartados anteriores, debemos:

- Desarrollar metodologías eminentemente activas y motivadoras por un lado y, por otro, unas metodologías creativas y personalizadas, atendiendo tanto a las necesidades del grupo como a cada uno de los alumnos.

- Utilizar metodologías investigadoras y expositivas, motivando siempre con una participación activa por parte del alumnado, buscando por su cuenta contenidos sobre temas más teóricos de seguridad.

- Centrar las metodologías en el alumnado y en los problemas de seguridad actuales que se pueden encontrar tanto en el ámbito laboral como en el personal.

- Proponer metodologías flexibles, motivadoras y participativas, siendo su función principal no tanto impartir contenidos que los alumnos asimilen pasivamente, sino facilitar su aprendizaje.

- Aplicar estrategias didácticas expositivas en los planteamientos de introducción, en el establecimiento de las coordenadas generales del tema y al subrayar sus partes destacadas. Con posterioridad serán usadas para clarificar, reforzar y enriquecer la comprensión.

- Fomentar el espíritu crítico constructivo sobre la actividad tecnológica y las diversas propuestas de mejora de seguridad.

- Aplicar metodologías que enfrenten al alumno a situaciones, más o menos problemáticas, en las que debe poner en práctica y utilizar reflexivamente conceptos, procedimientos y actitudes de Seguridad Informática, para así adquirirlos de manera consciente.

- Aplicar estrategias y metodologías orientadas a realizar investigaciones simplificadas, debates, estudio de casos, resolución de problemas simulados o reales y visitas o excursiones a centros de datos o de trabajo en los que apliquen de manera activa la seguridad.

- Recurrir a diferentes tipos de agrupamientos, empleando diferentes dinámicas de grupo en función del desarrollo e interés de las actividades y del funcionamiento del grupo. Fomentando así el trabajo en grupos y parejas en la realización de prácticas y proyectos, incentivando la motivación del alumno.

- Promover en el alumnado, mediante la integración de los contenidos teóricos, tecnológicos y organizativos, una visión global y coordinada de las implicaciones de la Seguridad Informática, sus técnicas y herramientas, así como sus problemas derivados.

10.1. Metodologías para aspectos teóricos de Seguridad Informática

Las nuevas metodologías de aprendizaje, así como las herramientas educativas on-line como son los Entornos de Aprendizaje Virtual (VLE), el acceso a Internet y a la información masiva utilizadas por parte de los alumnos, permite cada vez más al profesorado liberar tiempo de explicación teórica en clase y realizarlo como tareas para casa de los alumnos, este tiempo ahorrado o liberado, hace que se pueda dedicar más tiempo a los ejemplos, y al estudio de casos o prácticas en clase.

Esto hace más atractivo el aprendizaje teórico para los alumnos, huyendo del método expositivo. Una metodología que será necesaria en algunos aspectos, pero que la situación ideal será la de encontrar el equilibrio entre el uso de esta metodología y otras más actuales o innovadores. No se trata de oponer un modelo a otro, sino más bien de analizar las posibilidades de ambos para logar de la manera más eficaz posible el desarrollo de las capacidades de los alumnos (Tourón y Santiago, 2015).

Los estándares de aprendizaje puramente teóricos son más significativos en ciertos objetivos y contenidos de los currículos de Seguridad Informática, donde se hace necesario el aprendizaje por parte de los alumnos de grandes listas de conceptos, protocolos, tipos de ataques, etc.

Uno de los ejemplos que mayor facilitan el aprendizaje autónomo y entre pares, es el concepto de *"Flipped Classroom" o "Aula Invertida"*, que es un enfoque pedagógico que se centra en el aprendizaje centrado en el alumno. Esta metodología se basa en el principio de invertir una clase tradicional, donde son los alumnos los que investigan y estudian en casa ciertos conceptos o apartados de un tema o unidad didáctica, para su posterior exposición en clase. En este caso los profesores deben actuar como facilitadores del trabajo de los alumnos, así como de las herramientas, fuentes de información y actividades para conseguir los objetivos deseados.

El método de aula invertida, como un nuevo concepto y modo de enseñanza, puede aplicarse en la enseñanza de la Seguridad informática, ya que puede aumentar el atractivo y la participación del alumno. Al convertir las clases de teoría, típicamente centradas en la enseñanza, en una centrada en el aprendizaje, con una búsqueda de la interacción entre los alumnos, la investigación y los contenidos. Los estudiantes pasan a formar parte activa en el proceso de enseñanza-aprendizaje, que pasa a ser más interactivo, promoviendo la iniciativa de investigación de los alumnos (Min Zhao & Ping Chen, 2018).

Las ventajas de aplicar el método de aula invertida son, por ejemplo:

- El tiempo dedicado al aprendizaje de los contenidos se realiza como deberes o tareas para casa, lo que no solo implica la interacción entre los alumnos, sino la liberación del tiempo en clase para dedicarlo, por ejemplo, a trabajos prácticos.

- Fomenta el trabajo en grupo o entre pares.

- Aumenta la independencia, la autoestima y las herramientas de autoconocimiento e investigación de los alumnos.

Si existen beneficios significativos de aplicar nuevas metodologías, también existen algunas desventajas como:

- Requiere una mayor preparación de las fuentes de información y los contenidos que se desean desarrollar por parte del profesor. No solo planificar las clases, si no asegurar la disponibilidad de los recursos necesarios para los alumnos.

- Gran parte de la responsabilidad del proceso de enseñanza-aprendizaje recae sobre el alumno.

10.2. Estudio de casos para el análisis de ataques informáticos

El estudio de casos presenta situaciones concretas y reales que se pueden usar para comprender aspectos de la Seguridad Informática, así los estudiantes pueden detectar posibles vulnerabilidades, analizar cómo actuar y que herramientas utilizar ante posibles situaciones reales de ataques que se puede encontrar en el desempeño de su futura labor profesional.

Básicamente el estudio de casos en Seguridad Informática se basa en la presentación de historias, situaciones o una serie de hechos, que pueden estar basadas en acciones de ataques reales o hipotéticos. Estos hechos deben provocar en el alumno el interés por el tema expuesto, presentando problemas claros y concisos en los que identificar tanto el problema como la solución.

El estudio de casos, al igual que otras metodologías se pueden orientar hacia la educación ubicua con la ayuda de VLE o plataformas online. No hay mayores complicaciones que las de publicar online los casos propuestos y que los alumnos aporten sus ideas utilizando las mismas herramientas.

Por otra parte, una de las principales desventajas de la utilización de esta metodología es que los alumnos se pueden centrar en la idiosincrasia del caso presentado, dificultando generalizar y extrapolar las conclusiones del análisis de caso hacia otros escenarios. Por lo tanto, se hace necesaria la utilización de varios casos con los que comparar y contrastar múltiples situaciones de Seguridad Informática, para ayudar a los estudiantes a formular soluciones y extraer conclusiones generalizables y que se puedan aplicar en los futuros escenarios que pueden encontrarse en su desarrollo profesional.

10.3. Participación en concursos de habilidades sobre Seguridad Informática

No solo la utilización de debates o juegos de preguntas online (quizzes) ayudan a la formación, aprendizaje, promueven la investigación, la excelencia, las habilidades y la confianza de los alumnos, sino que también las competiciones y concursos, propuestos por empresas o entidades públicas, en las que se premian las habilidades de los participantes. Por ejemplo, es común que empresas de seguridad lancen propuestas y concursos para encontrar profesionales con talento.

Estas competiciones organizadas por empresas buscan el talento de los estudiantes o profesionales de Seguridad, ofreciendo un premio económico o una carrea profesional.

Para ello, proponen o retan, en muchas ocasiones, a los profesionales de Seguridad Informática o Hacker a que prueban a detectar las vulnerabilidades, amenazas y debilidades de sus sistemas. Con lo que consiguen detectar nuevos talentos, pero además auditar la seguridad de la empresa.

En otros casos, son entidades públicas o educativas, las que proponen concursos para que los participantes demuestren sus habilidades en Seguridad Informática. En estos concursos se proponen supuestos prácticos en entornos controlados y delimitados por las bases del propio concurso, en los que los concursantes tienen que mostrar todas sus habilidades.

Un ejemplo es el concurso Spainskills, promovido y organizado por el Ministerio de Educación y Formación Profesional de España, por el que se premian las destrezas de los estudiantes de la FP [1].

[1] Spainskills - Inicio. (s. f.). Recuperado 9 de julio de 2019, de https://spain-skills.es/

Los resultados y beneficios, tanto para los organizadores como participantes, de estas competiciones van más allá de ganar un premio o reconocimiento. Por ejemplo:

- Desarrollar nuevas habilidades y conocimientos sobre seguridad informática.

- Fomentar la innovación e investigación en nuevas técnicas y herramientas para poder competir contra iguales.

- Crear y mantener una red de contactos con profesionales de la misma rama.

- Realizar un análisis y evaluar las fortalezas y debilidades de una empresa, no solo en los aspectos de seguridad, si no aspectos del personal y de su preparación con respecto a otros profesionales del sector.

- Proporcionar un feedback a los profesores de los resultados de sus metodologías y de su esfuerzo por el aprendizaje de sus alumnos.

- Aumentar la visibilidad y concienciación de la sociedad e instituciones educativas sobre los problemas de Seguridad Informática, por la aparición de los ganadores de estos concursos en medios de comunicación. Los que puede provocar una mayor participación y apoyo, tanto financiero como en esfuerzo, para promover los estudios relativos a Seguridad Informática.

Por otro lado, el fomento de la participación en este tipo de eventos por parte de los profesores tiene algunas implicaciones:

- Tiempo y dedicación en la búsqueda de estas competiciones, así como en el estudio de la normativa para transmitirlo a alumnos y facilitar su participación, además de solicitar la participación en los mismos.

- Proporcionar a los alumnos los métodos y técnicas, así como las fuentes de información necesaria, para que participen en las mejores condiciones posibles en estas competiciones.

- El tiempo de clase necesario para exponer y/o preparar la participación, incluso la dedicación y esfuerzo por parte de los alumnos en casa o su tiempo libre.

En la mayoría de los casos la participación en estos concursos de habilidades se presenta como premio o recompensa por la buena actitud de los alumnos, y los alumnos así lo perciben. Pero debería, por parte de los profesores, centrar estos concursos como una metodología de aprendizaje, que proporciona los mismos beneficios que la gamificación.

10.4. Hacking ético como metodología

El hacking ético se define como las metodologías, entendidas como técnicas y herramientas, que utilizan los hackers para detectar vulnerabilidades en los sistemas informáticos existentes. Se puede decir que se utilizan los mismos métodos que los

ataques informáticos, pero se diferencia en el hecho de la utilización lícita o no de ellas, los objetivos no maliciosos y la aceptación o permiso que ha sido acreditado para realizar test de vulnerabilidad y seguridad de sistemas informáticos por el propietario del sistema objetivo del ataque ético (Oriyano, 2016).

Uno de los grandes centros de atención de la Seguridad Informática y la Privacidad es la de los ataques informáticos o virus. Es por ello, que puede resultar interesante introducir las técnicas de estas prácticas en el ámbito de la enseñanza. Para desmitificar a aquellas personas que se consideran hackers de sombrero blanco o que se dedican al Hacking ético, además de intentar proporcionar a los alumnos unos valores éticos y morales a la hora de enfrentarse en estos términos a la seguridad.

Las técnicas, métodos y conocimiento que utilizan los hackers son motivadores, ingeniosos y creativos. Siempre investigan para encontrar nuevas formas de atacar un sistema y cada vez, de formas más creativas e ingeniosas según se van corrigiendo los defectos o las puertas traseras de los sistemas.

Estas técnicas, se encaminan a buscar un aprendizaje significativo y realmente profundo de cómo funcionan las cosas, hasta el punto de saber cómo tomar el control y conocer los sistemas informáticos mejor que sus creadores. Esto les permite volver a pensar incluso en grandes ideas y evoluciones de la seguridad de un sistema porque realmente pueden profundizar en el trasfondo de cómo funcionan.

No existe mucha diferencia entre los test de penetración o las técnicas de hacking ético, en concepto y forma son similares, así como en la contratación de empresas o personal que realiza una auditoría externa de seguridad. Aunque cada vez se utilizan las técnicas de hacking en detrimento de los test de penetración, las empresas acuden a profesionales de los ataques informáticos para detectar las vulnerabilidades y la efectividad de los sistemas de seguridad para aplicar las correcciones necesarias (Sheoran & Singh 2014).

Sin embargo, en entornos educativos, la aplicación de estas técnicas no está bien vista ni valoradas de la misma manera. Provocando cierto rechazo y preocupación por la utilización de técnicas y herramientas que pueden ser maliciosas. Pero es indudable que la utilización de las mismas hace que la formación y educación de los administradores de sistemas, expertos en Seguridad Informática, esté mejor adaptada y preparada para enfrentarse a situaciones reales de amenazas y ataques de seguridad.

Además, es importante que los profesionales dedicados a seguridad tengan por lo menos las mismas habilidades y formación que los atacantes o hackers, lo deseable es que los primeros tuvieran mayores conocimientos y herramientas para poder asegurar la integridad y estabilidad de los sistemas que gestionan y protegen.

Las ventajas más destacables de la utilización del hacking ético como metodología en la educación de títulos referidos a Seguridad Informática son:

- Las técnicas y métodos de hacking ético se pueden considerar como técnicas proactivas de seguridad, más que reactivas. Que preparan mejores profesionales de seguridad informática.

- Son técnicas que motivan la investigación e innovación educativa de profesores y alumnos, ya que obliga a estar bien informado de los últimos avances en ataques informáticos.

- Fomentan el aprendizaje autónomo y el pensamiento crítico, ya que los alumnos que quieran aprender más de estas técnicas deberán seguir investigando en los métodos de hacking cuando terminen su formación.

- Promueven la investigación, ya que una de las características de las técnicas de hacking son la evolución continua de las mismas, así como de las medidas de seguridad y la necesidad que provoca en los hackers investigar nuevos métodos de burlar las medidas de seguridad de los sistemas informáticos.

- Fomentan el ingenio y la creatividad, cada evolución de los ataques informáticos, las técnicas y herramientas que utilizan son cada vez más ingeniosas y creativas. Conocer sus métodos de trabajo promueve también estas características en los alumnos.

Por el contrario, existe mucha controversia y rechazo sobre la aplicación de estas técnicas en entornos educativos, por las implicaciones éticas y legales que tiene el uso no lícito de la misma.

Los inconvenientes con los que nos podemos encontrar a la hora de introducir estas técnicas en un currículo educativo pueden ser:

- Aspectos negativos y mala prensa de los aspectos maliciosos y delictivos de las metodologías utilizadas por los hackers en ataques informáticos.

- Aspectos éticos y morales del uso de herramientas que se utilizan para vulnerar la privacidad de datos e información de usuarios en redes informáticas.

- La necesidad de conocer las normativas y leyes referentes a la legislación de diferentes países, y realizar un esfuerzo por que los alumnos entiendan las implicaciones delictivas de utilizar las herramientas enseñadas durante su formación para actividades no lícitas.

- El rechazo por parte de la comunidad educativa para aplicar estas técnicas en el aula, por la aprensión y miedo que genera la posible utilización de los alumnos de los aprendizajes obtenidos en el aula para fines delictivos o malintencionados.

El temor y rechazo de la aplicación de las técnicas de hacking en el aula no son infundados, varios estudios demostraron que los ataques informáticos crecieron a los sistemas de una universidad cuando los alumnos realizaban actividades de laboratorio sobre ataques de denegación de servicio (Trabelsi, 2012). Pero, es más, más del 85% de los alumnos que han experimentado con técnicas de monitorización y análisis de tráfico en las redes de sus centros educativos, y más del 70% reconoce haber utilizado técnica de hacking (Trabelsi & McCoey, 2016).

Ilustración 1 - Ventajas y resultados de las metodologías hacking en educación.

Como resumen, la aplicación de las técnicas de hacking ético en un currículo educativo de Seguridad Informática, pasando por alto las implicaciones y controversias sobre su uso, aumentan la motivación e interés por parte de los alumnos en los aspectos de este campo. Además, fomentan el ingenio, la creatividad y la investigación. Todo esto unido provoca un aprendizaje profundo y significativo de cómo funcionan los sistemas y contingencias de seguridad.

10.5. La gamificación para prácticas de seguridad informática

La gamificación se define como la aplicación de las mecánicas y características de los juegos a contextos no lúdicos con el propósito de aumentar la motivación y el compromiso de los alumnos.

El aspecto más importante de la gamificación es el sistema de recompensas o premios que se proporcionan a los alumnos por superar las diferentes fases del juego o ganarlo. Esto permite incentivar la participación en un juego educativo, que no se aplica en un entorno lúdico donde la propia diversión ya sería una motivación suficiente para participar en el juego o actividad.

Los juegos educativos o actividades prácticas gamificadas pueden ser presenciales en un recinto físico, donde todos los participantes compiten en mismo tiempo y lugar, o se pude hacer de manera distribuida y ubicua usando aplicaciones móviles, páginas Web o entornos virtuales.

Si la gamificación se aplica en un VLE o través de una aplicación online, hay que tener en cuenta que las recompensas aparte de motivar la participación deben incentivar el uso de la aplicación o plataforma de aprendizaje. Para ello, se pueden usar tablas de clasificación actualizadas en tiempo real, también se pueden recompensar tareas de moderación o control de juego, para evitar las trampas en el juego, y también se pueden otorgar recompensas gratuitas diarias o cada cierto tiempo.

Todas las técnicas y aplicaciones de la gamificación han experimentado resultados satisfactorios en entornos educativos y en la consecución de objetivos, conocimientos y habilidades en diferentes campos, por lo que parece razonable sugerir que estos resultados puedan ser aplicados en otros contextos o campos, como la Seguridad Informática.

Si bien, hay que tener en cuenta que la gamificación puede no funcionar para todos los grupos o alumnos, objetivos y contextos. Por ejemplo, la aplicación de la gamificación en entornos de educación ubicua puede producir, que mediante recompensas por acceso diario o cada cierto tiempo para mantener la participación de los alumnos, que los participantes dejen de realizar los retos o actividades del juego y sólo obtengan los puntos necesarios para finalizar el juego a través de estas recompensas (Ibañez & Di-Serio, 2014). Por lo que, para asegurar el éxito de la aplicación de la gamificación en un contexto educativo de Seguridad Informática, donde prolifera el uso de tecnologías, aplicaciones y VLE, hay que analizar correctamente el contexto y planificar cuidadosamente para asegurar los beneficios que proporciona.

El rol y la aplicación de la gamificación en los cursos o estudios vinculados con la Seguridad Informática, y dirigidos a alumnos de escuelas superiores o universitarios, lleva tiempo desarrollándose tanto por la Agencia de Seguridad Nacional (NSA) y Fundación Nacional de Ciencia (NSF) en Estados Unidos. Varios cursos de verano, denominados GenCyber [1], se han venido desarrollando en los últimos años para concienciar sobre los aspectos más relevantes de la Seguridad Informática, fomentar el interés de los alumnos en este campo, abarcando aspectos que van desde el uso seguro de internet hasta las técnicas de protección y ataques de ingeniería social.

[1] GenCyber. (s. f.). Recuperado 9 de julio de 2019, de https://www.gen-cyber.com/

11. Herramientas para la enseñanza de Seguridad Informática

En la actualidad existen herramientas que pueden ayudar al proceso de enseñanza-aprendizaje y a la transferencia de habilidades para Seguridad Informática. De todas ellas, habría que seleccionar aquellas que mejor aceptación tengan entre los alumnos, ya que forzar el uso de las herramientas que desea el profesor, ante las mismas características y facilitación de la consecución de los objetivos, puede provocar frustración y rechazo en los alumnos.

En este punto se han analizado las herramientas innovadoras que pueden contribuir y ayudar en las tareas de enseñanza a los profesores, realizando un pequeño análisis de cada una de ellas y que aportan a la formación de los alumnos de cursos de Seguridad Informática. Estas herramientas están orientadas a la práctica y al desarrollo profesional de los alumnos, ya que es el objetivo central de los ciclos formativos de FP.

11.1. Laboratorios específicos para Seguridad Informática

Tener un laboratorio de Seguridad informática totalmente aislado resulta muy interesante en dos aspectos importantes para la enseñanza de los tipos de ataques y vulnerabilidades que afectan a los sistemas informáticos, tanto a dispositivos como a infraestructuras de red.

Primero, se puede mantener una granja de dispositivos infectados con diferentes virus, con dispositivos infectados en entornos totalmente controlados y aislados, con un control de las conexiones de estos dispositivos, bien por red, comunicaciones inalámbricas o por dispositivos de plug and play, para evitar el uso malintencionado de estos virus.

Segundo, poner a disposición de los alumnos la infraestructura y los dispositivos necesarios donde poder lanzar ataques informáticos y practicar la defensa de los mismos.

Las utilizaciones de este tipo de laboratorios fomentan la motivación y el aprendizaje autónomo de los alumnos, donde ellos mismos experimentan las consecuencias de los ataques informáticos, pudiendo aplicar técnicas de seguridad activa y pasiva para prevenir estos ataques lanzados por sus compañeros o de manera automática por script o bots, y así prepararse mejor para prevenir el compromiso y la seguridad de los sistemas que tengan que proteger en su entorno personal o profesional.

La capacidad de modificación y reconfiguración rápida de estos laboratorios debe ser una de sus características principales, ya que modificar la infraestructura y la topología de red del laboratorio permite plantear diferentes escenarios para reproducir ataques informáticos, por ejemplo, con ataques producidos en la misma red o desde redes externas, con o sin configuración de un proxy o firewall entre las diferentes redes.

Otra característica importante que se debe implementar en estos laboratorios es la capacidad de restablecer o configurar los procedimientos necesarios para volver a un punto de recuperación del laboratorio, con el que rápida y fácilmente se pueda volver a

un punto de partida de control total por parte del profesor o administrador del laboratorio. Así cuando se termina un escenario de ataques, de infección de virus u otra práctica se pueda volver fácilmente a la configuración inicial del laboratorio.

Uno de los principales inconvenientes de la utilización de este tipo de laboratorios, o entornos de pruebas para virus y ataques, es la necesidad de una alta carga de trabajo por parte de profesional con perfil de administrador de redes. En muchos casos, en los contextos y centro educativos, en los que se imparten los ciclos formativos de FP de ASIR y SMR, no existe un administrador de equipos, y tienen contratada una empresa que da este servicio, pero solo a nivel de configuración inicial y resolución de contingencias, por lo que estas tareas de administración recaerían sobre el profesor. Lo que le quitará tiempo de dedicación a la innovación e investigación docente, entre otras tareas.

11.2. Aplicación de IoT para laboratorios virtuales

Los avances tecnológicos, el desarrollo de la electrónica y la conectividad de los dispositivos de cualquier índole ha provocado la aparición del término Internet de las Cosas (IoT). En el que se engloban una gran cantidad de dispositivos tecnológicos los cuales tienen cierta lógica o inteligencia y una conectividad con otros sistemas para compartir sus datos.

Los dispositivos más utilizados para el desarrollo de arquitecturas o sistemas de IoT son los denominados dispositivos u ordenadores de bajo coste, basados en proyectos de desarrollo de FreeHardware, estos dispositivos han avanzado en los últimos años optimizando los recursos, la potencia y eficiencia. Los ejemplos más conocidos son Arduino [1], Raspberry Pi [2] u Orange Pi [3].

Estos dispositivos son usados en educación por su abaratamiento en costes y su flexibilidad en cuanto a configuración. Y se aplican en campos que van desde la robótica y la inteligencia artificial hasta la programación. Además, en estudios de todas las edades, desde estudios primarios hasta la universidad.

En el caso de la seguridad informática, estos dispositivos pueden servir para la construcción de una infraestructura de red con elementos de computación de bajo coste (del anglicismo Low-cost computing, LCC), para montar un laboratorio de prácticas flexible y que permita reproducir situaciones de vulnerabilidad o ataques informáticas con un bajo coste.

Añadiendo características de flexibilidad, para cambios en los escenarios y facilidad de configuración. Características que también se pueden tener con entornos de pruebas realizados con virtualización.

[1] Arduino - Home. (s. f.). Recuperado 10 de julio de 2019, de https://www.arduino.cc/
[2] orange pi - Buscar con Google. (s. f.). Recuperado 10 de julio de 2019, de http://www.orangepi.org/
[3] Teach, Learn, and Make with Raspberry Pi – Raspberry Pi. (s. f.). Recuperado 10 de julio de 2019, de https://www.raspberrypi.org

Pero la utilización de estos dispositivos en los laboratorios de Seguridad Informática puede aportar una motivación extra a los alumnos, por el hecho de estar utilizando herramientas tangibles y haciendo sesiones de laboratorio más dinámicas y motivacionales, sobre todo si se aplica en estudios de formación de profesionales técnicos, y puede aportar más beneficios que la virtualización dependiendo el contexto en que se apliquen.

11.3. La virtualización para objetivos en Seguridad Informática

Las tecnologías y herramientas de virtualización se pueden utilizar para facilitar los aspectos y actividades prácticas de la formación en Seguridad Informática. Estas herramientas permiten diseñar, implementar y reproducir redes virtuales con máquinas virtuales o con el uso de virtualización en la nube.

Con las herramientas de virtualización se pueden desplegar diferentes tipos de sistemas operativos y aplicaciones en un ordenador personal, o en los equipos de un laboratorio de prácticas sencillo, sin necesidad de características especiales de infraestructura o de configuración de equipos y de red. Además, las herramientas de virtualización permiten guardar el estado de una virtualización para continuar o realizar el trabajo en diferentes sesiones en el aula o laboratorio, también permite configurar y gestionar el hardware de la máquina virtual fácilmente.

Además, también permite infectar sistemas operativos virtualizados, pudiendo realizar prácticas de técnicas de protección, desinfección y planes de seguridad sobre entornos controlados y aislados para evitar la propagación de los virus.

En el mercado existen muchas herramientas de virtualización y de cloud computing, la selección de cada tipo de herramienta dependerá de:

- La aceptación de las herramientas, los alumnos al principio preferirán las herramientas de escritorio tradicionales de virtualización, por ser con las que más familiarizados pueden estar.

- La conveniencia, sobre todo en las soluciones en la nube, en función de la comunidad de soporte y la flexibilidad y capacidad en cuanto a configuración, almacenamiento de las imágenes de las máquinas virtuales para hacer copias de seguridad y restaurarlas que proporcione cada tipo de herramienta.

- El coste de cada una de las herramientas, muchos de los servicios de virtualización en la nube son de pago, mientras que las aplicaciones de escritorio más extendidas y utilizadas son gratuitas.

- El rendimiento de cada una de las soluciones, en este caso las soluciones de virtualización en la nube son mejores para escenarios o supuestos prácticos en los que se necesiten varias por sus recursos ilimitados, mientras que, si solo se necesitan una o dos máquinas, los alumnos pueden preferir el uso de aplicaciones tradicionales, siempre que los requisitos de las virtualizaciones no superen los recursos del ordenador.

- La seguridad y la desconfianza de compartir su trabajo en la nube o mantenerlo en su máquina.

11.3.1. Herramientas de escritorio o servidor para virtualización

Las herramientas de virtualización tradicionales para ordenadores personales más extendidas y utilizadas son VMWare Player [1] y Oracle Virtual Box [2].

Ambas proporcionan características similares:

- Los discos de almacenamiento de las diferentes máquinas virtuales son almacenados en el equipo como ficheros de imagen.

- La configuración de los adaptadores de red de las máquinas virtuales acepta configuración como puente, NAT o solo para uso interno de la máquina.

- Las máquinas virtuales pueden acceder a los dispositivos hardware del equipo, como por ejemplo los dispositivos conectados por USB, o carpetas en red.

- Se pueden crear puntos de restauración y ramas de los cambios de las máquinas virtuales, para su posterior recuperación o para compartirlas en otros dispositivos.

Estas herramientas para la creación de máquinas virtuales generan un entorno aislado a través de la utilización de la configuración de los adaptadores de red, lo que permite la encapsulación de la propia máquina virtual.

Los usuarios y permisos para utilizar una máquina virtual pueden ser superusuarios o usuarios normales. El superusuario puede realizar tareas de administración sobre la máquina virtual como: instalar software, cambiar la configuración del adaptador de red, compartir carpetas, dispositivos de almacenamiento USB, etc. Lo que puede llegar a comprometer la seguridad del ordenador donde se ejecuta la máquina virtual y la red a la que esté conectado.

Los ficheros de imágenes de las máquinas virtuales tienen un tamaño excesivo, de varios gigabytes, lo que hace que pueda ser un inconveniente a la hora de mover las máquinas virtuales a otros ordenadores, compartirlas o incluso entregarlas al profesor como elemento entregable y evaluable de una práctica o trabajo de laboratorio.

[1] VMware Workstation Player | VMware. (s. f.). Recuperado 10 de julio de 2019, de https://www.vmware.com/products/workstation-player.html
[2] Oracle VM VirtualBox. (s. f.). Recuperado 10 de julio de 2019, de https://www.virtualbox.org/

11.3.2. Servicios de virtualización en la nube

Los beneficios y ventajas de utilizar servicios de virtualización, como pueden ser Amazon AWS [1], HP Cloud [2], Google Cloud [3], Microsoft Azure [4], and IBM Cloud [5], son los mismos que las aplicaciones de escritorio, pero con las ventajas inherentes a soluciones o servicios en la nube.

Estas soluciones son arquitecturas basadas en servicios bajo demanda a través de plataformas online, por lo que se pueden usar para prácticas puntuales. Si se va a realizar un uso continuado puede que otras de las soluciones de virtualización se adapten mejor a las necesidades y reduzcan los costes.

Estas soluciones pueden ser interesantes para soluciones o prácticas de aprendizaje ubicuo y entornos colaborativos, ya que permiten de una forma sencilla compartir y acceder de forma remota y por varios usuarios a los mismos recursos.

11.3.3. Arquitecturas basadas en contendores.

Los sistemas de virtualización, tanto tradicionales como los basados en servicios en la nube, son complejos en varios aspectos y requieren un gran esfuerzo de gestión, manejo de la seguridad y requisitos de los sistemas. Para facilitar estas tareas y la gestión de los elementos que se desean virtualizar han aparecido en los últimos años las arquitecturas ligeras de virtualización basadas en contenedores como pueden ser Docker [6], CoreOs rkt [7], OpenShift [8], OpenVZ [9] o LXC (Contenedores de Linux) [10].

Estas arquitecturas de virtualización son de reciente aparición y se han extendido rápidamente, convirtiéndose en una alternativa real a las máquinas virtuales y a los servicios en la nube por su agilidad, flexibilidad y eficiencia.

---

[1] Informática en la nube para la educación. (s. f.). Recuperado 10 de julio de 2019, de https://aws.amazon.com/es/education/

[2]Soluciones de nube híbrida. (s. f.). Recuperado 10 de julio de 2019, de https://www.hpe.com/es/es/solutions/cloud.html

[3] Google Cloud Platform. (s. f.). Recuperado 10 de julio de 2019, de Google for Education website: https://edu.google.com/intl/es-419_ALL/products/google-cloud-platform/

[4] Azure for Education | Microsoft Azure. (s. f.). Recuperado 10 de julio de 2019, de https://azure.microsoft.com/es-es/education/

[5] IBM Cloud | IBM. (s. f.). Recuperado 10 de julio de 2019, de https://www.ibm.com/cloud

[6] Application Solutions for Higher Education | Docker. (s. f.). Recuperado 10 de julio de 2019, de https://www.docker.com/solutions/higher-education

[7] CoreOS. (s. f.). Recuperado 10 de julio de 2019, de https://coreos.com/rkt/docs/latest/

[8] OpenShift: Container Application Platform by Red Hat, Built on Docker and Kubernetes. (s. f.). Recuperado 10 de julio de 2019, de https://www.openshift.com

[9] Open source container-based virtualization for Linux. (s. f.). Recuperado 10 de julio de 2019, de https://openvz.org/

[10] Linux Containers. (s. f.). Recuperado 10 de julio de 2019, de https://linuxcontainers.org/

Las arquitecturas basadas en contenedores permiten guardar el estado de los mismos, pudiendo lanzar nuevos contenedores compartiendo la misma imagen, lo que permite que diferentes contenedores en ejecución compartan las mismas características. En otras palabras, se puede crear una nueva imagen sobre una existente agregando capas. En comparación con las máquinas virtuales tradicionales, los contenedores brindan más flexibilidad y versatilidad para mejorar la utilización de los recursos.

11.4. Entornos educativos virtuales para Seguridad Informática

Los entornos virtuales o de realidad virtual permiten desarrollar prácticas de aprendizaje con alto impacto en los alumnos, así como proporcionar una inmersión profunda para trabajar varios aspectos de la informática, entre ellos la seguridad.

Los objetivos principales de estas herramientas son:

- Entrenar y desarrollar nuevos conocimientos y habilidades a través de ejercicios prácticos en entornos controlados.

- Aumentar el interés y la motivación por participar en las actividades propuestas por el profesor, tanto si son desarrolladas de manera presencial u online.

Estas herramientas permiten la simulación, por ejemplo, de ataques de seguridad y los alumnos deben gestionar retos que provocan estos ataques y amenazas. Así, los alumnos pueden poner en práctica las herramientas y habilidades sobre Seguridad Informática en diferentes escenarios, en los que no existen consecuencias reales y pueden aprender de los fallos o errores que realizan en la gestión y defensa ante ciertas amenazas.

Una de las soluciones más interesantes y utilizadas en la educación de la Seguridad Informática es el Karspersky Interactive Simulaion Protection Simulation (KIPS) [1]. En esta aplicación se introduce a los jugadores en un entorno empresarial simulado, donde deberán enfrentarse a una serie de amenazas de seguridad mientras intentan aplicar planes de gestión de la seguridad, maximizar las ganancias de la empresa y mantener la confianza en la misma y sus sistemas informáticos.

En el caso de la realidad virtual, hay varias propuestas y desarrollos que se encuentran en fase de prototipo, pero las pruebas y resultados obtenidos en las primeras aproximaciones son alentadoras (Hwaryoung & Bruner, 2019). Si bien, habría que esperar a la maduración y aplicación extendida tanto de las soluciones propuestas como de la tecnología aplicada a la Seguridad Informática.

La utilización de estas aplicaciones o juegos aplicados a Seguridad Informática, basados en las metodologías de gamificación o Serious Games, arrojan unos resultados positivos ya que contribuyen a la formación de profesionales, posibilitando la transferencia de habilidades y la práctica en entornos o escenarios reales (Yonemura & Sato, 2018).

[1] Kaspersky Security Awareness Training | Kaspersky. (s. f.). Recuperado 10 de julio de 2019, de https://www.kaspersky.es/enterprise-security/security-awareness

11.5. Herramientas utilizadas en ataques informáticos orientadas a la educación

Las herramientas que utilizan los hackers para lanzar ataques informáticos sobre sus objetivos puede ser interesante que sean utilizadas en la educación de la Seguridad Informática. Ya que proporcionan una visión de los métodos y técnicas que utilizan los hackers para aprovechar las vulnerabilidades de los sistemas informáticos.

La utilización de estas herramientas en un contexto educativo tiene las mismas implicaciones que las metodologías de hacking ético aplicadas en el aula, tanto en ventajas y desventajas. Todas estas consideraciones ya se han expuesto en el punto *"10.4 Hacking ético como metodología"*.

A la hora de la selección de las herramientas hacking que se desean utilizar en el aula habrá que considerar los aspectos necesarios para proteger los sistemas del centro, y que la aplicación o uso de las mismas en el aula no provoque fallos de seguridad con consecuencias no deseadas en el propio centro.

También hay que tener en cuenta y analizar los aspectos educativos de las herramientas que se desean introducir a los alumnos, tienen que tener un claro objetivo educativo, por eso se tienen que descartar aquellas que solo presenten escenarios de ataques no analizables o reutilizables en técnicas provechosas y lícitas para la Seguridad Informática.

11.5.1. Distribuciones o suites informáticas

Son conjuntos de herramientas o distribuciones de sistemas operativos con diferentes propósitos como la monitorización y análisis, de paquetes de red, manipulación de flujos de información, descifrado de contraseñas y test de penetración.

De entre todas las distribuciones se podrían destacar en primer lugar Kali Linux [1], por su continua actualización, y Live Wifislax [2], por ser de las primeras que aparecieron asociadas a la vulnerabilidad de redes Wi-Fi.

Pero también se pueden destacar otras como Parrot Security OS [3] utilizada para el anonimato en ataques de seguridad, es ligera y con una interfaz muy intuitiva, y por otro lado estaría BlackArch [4] que es un proyecto reciente que se dirige a los test de penetración.

[1] Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. (s. f.). Recuperado 10 de julio de 2019, de https://www.kali.org/
[2] Live Wifislax. (s. f.). Recuperado 10 de julio de 2019, de Live Wifislax website: https://www.wifislax.com/
[3] Faletra, L. (s. f.). The best choice for security experts, developers and crypto-addicted people. Recuperado 10 de julio de 2019, de Parrot Security website: https://www.parrotsec.org
[4] BlackArch Linux - Penetration Testing Distribution. (s. f.). Recuperado 10 de julio de 2019, de https://blackarch.org/

11.5.2. Herramientas para descifrar contraseñas

Estas herramientas están orientadas a la recuperación de contraseñas almacenadas en diferentes tipos de sistemas o al procesamiento de los datos de acceso trasmitidos por la red. Una utilización no lícita de estas herramientas sería para la recuperación de contraseñas olvidadas, por ejemplo, pero en la mayoría de los casos se intentan utilizar para el acceso no autorizado a sistemas, plataformas o servicios en red.

Muchas de estas herramientas se basan en la utilización de algoritmos de cifrado inverso para descifrar las contraseñas, o bien utilizan ataques de fuerza bruta o con diccionarios de datos, aunque estas últimas suelen tener menos éxito en sus propósitos.

De entre todas las herramientas que existen para descifrar contraseñas, se pueden destacar las siguientes para su análisis y utilización en los laboratorios de Seguridad Informática:

- Brutus [[1]: Una de las herramientas más populares y extendidas, está solo disponible para Windows. Tiene una gran variedad de funcionalidades.

- Medusa [2]: Esta herramienta utiliza ataques de fuerza bruta, se ejecuta desde línea de comando.

- Hydra [3]: Es una de las herramientas que más efectividad tiene en los ataques que se realizan con ella, también tiene uno de los mejores resultados en cuanto a tiempo.

- John de Pipper [4]: es un desarrollo de código abierto que, en un principio está diseñada para Linux, Unix o Mac OS, aunque existe una versión no oficial para Windows.

- Rainbowcrack [5]: Es una herramienta que se utiliza para algoritmos de cifrado hash, es una de las mejores herramientas de fuerza bruta.

- Crunch [6]: es una herramienta que utiliza los diccionarios de datos para obtener las contraseñas de un sistema. Está incluido en la suite Kali Linux, entre otras.

[1] Brutus – SecTools Top Network Security Tools. (s. f.). Recuperado 10 de julio de 2019, de https://sectools.org/tool/brutus/
[2] Servicios de redes Foofus - Medusa. (s. f.). Recuperado 10 de julio de 2019, de http://foofus.net/goons/jmk/medusa/medusa.html
[3] THC Hydra – SecTools Top Network Security Tools. (s. f.). Recuperado 10 de julio de 2019, de https://sectools.org/tool/hydra/
[4] John the Ripper. (s. f.). Recuperado 10 de julio de 2019, de https://www.openwall.com/john
[5] RainbowCrack - Crack Hashes with Rainbow Tables. (s. f.). Recuperado 10 de julio de 2019, de http://project-rainbowcrack.com/
[6] crunch. (s. f.). Recuperado 10 de julio de 2019, de https://tools.kali.org/password-attacks/crunch

11.5.3. Herramientas de ataque a bases de datos

Existen muchos tipos y sistemas de bases de datos, lo que implica numerosas y diversas vulnerabilidades y forma de atacarlas por parte de los hackers.

En muchos casos estas herramientas son sencillas, o son simples pasos fácilmente ejecutables desde un navegador Web o desde línea de comandos. Los hackers con conocimientos básicos de bases de datos y de consultas sobre las mismas pueden llegar a acceder a los datos almacenados por servicios distribuidos o aplicaciones Web.

Pero entre los sistemas gestores de bases de datos, lo más utilizados en la actualizad se encuentran MySQL y MongoDB que tienen sus propias herramientas específicas para hackear estos sistemas, jSQL [1] y noSQLMap [2].

11.5.4. Herramientas de análisis de vulnerabilidades y test de penetración

Los test de penetración, o también pentest, pentesting o ethical hacking (aunque esta última definición no es del todo correcta), son las técnicas y herramientas automatizadas usadas para la comprobación de las vulnerabilidades y brechas de seguridad de los sistemas informáticos, tales como redes, servidores, o aplicaciones Web.

Estas herramientas se pueden utilizar en el aula para el aprendizaje de técnicas activas y pasivas de Seguridad Informática, tanto desde el enfoque de la protección de sistemas informáticos por un administrador o para realizar pruebas durante el ciclo de vida del desarrollo de un sistema informático.

Las herramientas que se pueden utilizar para estos cometidos son:

- Golismero [3]: es una framework de código abierto que se utiliza para realizar test de penetración en aplicaciones Web, pero en ocasiones se reutiliza para otro tipo de ataques.

- Lynis [4]: es una herramienta de código abierto que se utiliza para auditar y comprobar las vulnerabilidades de sistemas operativos basados en Unix y Linux. Esta herramienta realiza algunas comprobaciones sobre el sistema, como configuraciones por defecto que no se han cambiado, y además permite la búsqueda de software instalado con fallos de configuración o seguridad.

[1] jSQL Injection. (s. f.). Recuperado 10 de julio de 2019, de https://tools.kali.org/vulnerability-analysis/jsql
[2] NoSQLMap. (s. f.). Recuperado 10 de julio de 2019, de Cybrary website: https://www.cybrary.it/0p3n/nosqlmap/
[3] GoLismero. (s. f.). Recuperado 10 de julio de 2019, de https://tools.kali.org/information-gathering/golismero
[4] Lynis - Security auditing and hardening tool. (s. f.). Recuperado 10 de julio de 2019, de https://cisofy.com/lynis/

- Nikto [1]: Es una herramienta que comprueba las vulnerabilidades de servidores Web, Es una de las más potentes, ya que permite múltiples tipos de ataques y permite el desarrollo de plugins para evoluciones y mejoras.

- Nmap [2]: Es un programa de código abierto para rastrear puertos abiertos y posibles accesos para servidores o equipos. Es una herramienta sencilla, pero altamente extendida.

11.5.5. Monitorización, captura y filtrado de paquetes

Wireshark [3] es la principal herramienta multiplataforma de software libre que se utiliza para la monitorización, análisis y captura de los paquetes que se envían y reciben a través de las tarjetas de red de un dispositivo.

Con esta herramienta podemos ver el tráfico que se genera durante la simulación de un ataque informático, para posteriormente poder filtrar dicho tráfico a través de proxies o fierwalls. Pero también se puede utilizar para realizar test de seguridad y comprobar que la información se envía cifrada a través de la red por un sistema.

El caso de uso más típico de esta herramienta es la de capturar los paquetes de las peticiones de autenticación sobre una plataforma Web, y ver las diferencias entre el envío de los paquetes con protocolos no seguros y cifrados, como son HTTP y HTTPS respectivamente.

Hay varias alternativas a esta herramienta, como pueden ser Cloaud Shark [4] y Sysdig [5], pero Wireshark sigue siendo la más utilizada y más extendida desde su aparición en 1998 con el nombre de Ethereal.

[1] Nikto –Network Security. (s. f.). Recuperado 10 de julio de 2019, de https://sectools.org/tool/nikto/
[2] Nmap: the Network Mapper . (s. f.). Recuperado 10 de julio de 2019, de https://nmap.org/
[3] Wireshark · Go Deep. (s. f.). Recuperado 10 de julio de 2019, de https://www.wireshark.org/
[4] CloudShark - Network Analysis Evolved | CloudShark: Network Analysis Evolved. (s. f.). Recuperado 10 de julio de 2019, de https://cloudshark.io/
[5] Sysdig | Cloud-Native Visibility and Security for Kubernetes. (s. f.). Recuperado 10 de julio de 2019, de Sysdig website: https://sysdig.com/

12. Conclusiones

La Seguridad Informática o ciberseguridad es un campo o rama de la informática que crece y cambia rápidamente, tan rápido como avanzan los diferentes campos de la informática. Con cada nuevo avance tecnológico, nacen nuevas necesidades de seguridad, y crecen las amenazas o ataques a los nuevos sistemas.

Esto hace que la revisión de las titulaciones y currículos que se utilizan en estudios centrados en este campo sea realmente crítica. Ya que como hemos expuesto durante el documento el avance de los ataques informáticos es tan o más rápido que el desarrollo de la propia tecnología.

La importancia de la Seguridad Informática hace, que tanto entidades públicas, como privadas, y asociaciones de profesionales hagan grandes esfuerzos en la formación y el desarrollo de la Seguridad Informática. También provoca que cualquier publicación o avance relevante en este campo tenga un gran impacto en la comunidad académica y en la sociedad.

A parte de estas consideraciones generales sobre Seguridad Informática, hay otras cuestiones más específicas de la educación de la formación en seguridad que se presentan a continuación.

Crear un marco común para la definición de currículos

Las características inherentes de la Seguridad Informática requieren que, todos los actores y organizaciones que participan en el desarrollo de los currículos de seguridad, formen o utilicen a trabajadores cualificados y con amplia experiencia para realizar el desarrollo de estos currículos. Para poder identificar las necesidades en cuanto a los riesgos y amenazas de la Seguridad Informática con una amplia visión de futuro.

Por ello sería necesario crear un marco de trabajo común, para utilizarlo como referencia para ayudar tanto a las instituciones educativas, organizaciones profesionales o de certificación, profesores y alumnos para crear los currículos relativos a Seguridad Informática.

Este marco podría tener 3 características esenciales:

- Utilizar léxico, conceptos básicos y nomenclatura comunes para facilitar la comunicación entre los diferentes actores.

- Realizar un análisis y definición común de aquellos conocimientos, objetivos y habilidades que son críticas para la formación de los diferentes roles que pueden desempeñar los profesionales de Seguridad Informática.

- Desarrollar niveles de formación y profesionales para los diferentes roles de los profesionales que se desean formar en las conocimientos, objetivos y habilidades definidos anteriormente, que permita el análisis y refinamiento de las tareas, conocimiento, habilidades que conforman cada nivel o posición profesional.

Desarrollo de titulaciones y ciclos formativos específicos para Seguridad Informática

Uno de los objetivos de la FP es la formación de profesionales para cubrir la demanda por parte del mundo laboral y empresarial de empleo especializado y técnico para ocupar puestos para tareas específicas en las empresas, y por otro lado cubrir las necesidades socio-económicas de la sociedad. También tiene el enfoque de dar formación a aquellos jóvenes que no se sienten identificados con su desarrollo profesional y personal en un sistema educativo tradicional para obtener unos estudios superiores o universitarios.

De estas necesidades, tanto de los jóvenes como de la empresa, deberían surgir los títulos o familias de Formación Profesional que atiendan los requisitos de los puestos del trabajo del presente y del futuro.

Para ver si los títulos de FP se ajustan a las necesidades del mercado laboral, en el caso del sector de las Tecnologías de la Información, basta con buscar la lista de los empleos más demandados en los últimos años en el sector privado y empresarial. Sin necesidad de hacer una búsqueda específica orientada hacia los empleos demandados en el sector de la informática, se podría observar que los perfiles relacionados con la Seguridad Informática están incluidos en todas estas listas, incluso ocupando los primeros puestos por importancia o urgencia de la demanda de técnicos especialistas en este campo.

Por lo que se puede concluir que se debería desarrollar al menos un título orientado a formar profesionales en Seguridad Informática dentro de la FP en España.

Métodos de evaluación del currículo y de la actividad docente

Uno de los trabajos futuros o de ampliación que podría tener este TFM sería definir los métodos y herramientas para evaluar la actividad docente, definiendo cómo y cuándo sería recomendable evaluar la inclusión en el aula de las metodologías y herramientas propuestas en este trabajo. Para realizar una evaluación tanto cualitativa como cuantitativa de las innovaciones docentes introducidas en el aula. Se podría aplicar también una evaluación sobre a la aceptación y resultado de aprendizaje provocado sobre los alumnos.

Otro punto serían las evaluaciones y revisiones periódicas que deberían hacerse sobre el currículo de Seguridad Informática propuesto en este documento.

Propuesta de actividades relacionadas con las metodologías y herramientas propuestas

Otro trabajo futuro podría ser realizar propuestas de actividades, o unidades didácticas, desarrollando objetivos y contenidos, pero sólo utilizando metodologías y herramientas expuestas en este documento para el desarrollo completo del proceso de aprendizaje para los objetivos seleccionados.

Como, por ejemplo, desarrollar una unidad didáctica completa para la *"Configuración segura de redes cableadas e inalámbricas",* donde los alumnos organizados en grupos configuren unos router inalámbricos con los conocimientos obtenidos en una dinámica de Flipped Classroom, y posteriormente utilicen herramientas de auditoría y hacking ético para comprobar las vulnerabilidades e intentar acceder a los routers de otros grupos. Esta actividad podría estar también gamificada utilizando juegos basados en competiciones de captura la bandera (en inglés Capture de Flag, CTF)

13. Referencias

- BOE.es - Documento BOE-A-2015-8043. (s. f.). Recuperado 12 de marzo de 2018, de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-8043

- Portal de Educación de la Junta de Castilla y León - ORDEN EDU/362/2015, de 4 de mayo, por la que se establece el currículo y se regula la implantación, evaluación y desarrollo de la educación secundaria obligatoria en la Comunidad de Castilla y León. (s. f.). Recuperado 12 de marzo de 2018, de http://www.educa.jcyl.es/es/resumenbocyl/orden-edu-362-2015-4-mayo-establece-curriculo-regula-implan

- Portal de Educación de la Junta de Castilla y León - ORDEN EDU/363/2015, de 4 de mayo, por la que se establece el currículo y se regula la implantación, evaluación y desarrollo del bachillerato en la Comunidad de Castilla y León. (s. f.). Recuperado 12 de marzo de 2018, de http://www.educa.jcyl.es/es/resumenbocyl/orden-edu-363-2015-4-mayo-establece-curriculo-regula-implan

- Técnico en Sistemas Microinformáticos y Redes - TodoFP - Ministerio de Educación y Formación Profesional. (s. f.). Recuperado 12 de marzo de 2018, de http://www.todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe/informatica-comunicaciones/sistemas-microniformaticos-redes.html

- Técnico Superior en Administración de Sistemas Informáticos en Red. (s. f.). Recuperado 12 de marzo de 2018, de http://www.todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe/informatica-comunicaciones/admin-sist-informaticos-red.html

- Técnico Superior en Desarrollo de Aplicaciones Multiplataforma. (s. f.). Recuperado 12 de marzo de 2018, de http://www.todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe/informatica-comunicaciones/des-aplicaciones-multiplataforma.html

- Técnico Superior en Desarrollo de Aplicaciones Web. (s. f.). Recuperado 12 de marzo de 2018, de http://www.todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe/informatica-comunicaciones/des-aplicaciones-web.html

- Título Profesional Básico en Informática de Oficina - TodoFP - Ministerio de Educación y Formación Profesional. (s. f.). Recuperado 12 de marzo de 2018, de http://todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe/informatica-comunicaciones/informatica-oficina.html

- Título Profesional Básico en Informática y Comunicaciones - TodoFP - Ministerio de Educación y Formación Profesional. (s. f.). Recuperado 12 de marzo de 2018, de http://todofp.es/que-como-y-donde-estudiar/que-estudiar/familia/loe/informatica-comunicaciones/informatica-comunicaciones.html

- Defining Computer Science. (s. f.). Recuperado 11 de julio de 2019, de k12cs.org website: https://k12cs.org/defining-computer-science/

- Abler, R. T., Contis, D., Grizzard, J. B., & Owen, H. L. (2006). Georgia tech information security center hands-on network security laboratory. *IEEE Transactions on Education*, *49*(1), 82-87.

- Conklin, A. (2005). The Use of a Collegiate Cyber Defense Competition in Information Security Education. Proceedings of the 2Nd Annual Conference on Information Security Curriculum Development, 16–18. https://doi.org/10.1145/1107622.1107627

- Conti, G., Babbitt, T., & Nelson, J. (2011). Hacking competitions and their untapped potential for security education. *IEEE Security & Privacy*, *9*(3), 56-59.

- Du, W., & Wang, R. (2008). SEED: A Suite of Instructional Laboratories for Computer Security Education. *J. Educ. Resour. Comput.*, *8*(1), 3:1–3:24. https://doi.org/10.1145/1348713.1348716

- González Fernández, N. & Carrillo Jácome, G.A. (2016). El Aprendizaje Cooperativo y la Flipped Classroom: una pareja ideal mediada por las TIC. *Aularia: Revista Digital de Comunicación*, vol. 5 (número 2), pp. 43-48.

- Hamid, N. (2007). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. IGI Global.

- Hill, J. M. D., Carver, C. A., Jr., Humphries, J. W., & Pooch, U. W. (2001). Using an Isolated Network Laboratory to Teach Advanced Networks and Security. Proceedings of the Thirty-second SIGCSE Technical Symposium on Computer Science Education, 36–40. https://doi.org/10.1145/364447.364533

- Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical Hacking: Educating Future Cybersecurity Professionals. In *Proceedings of the EDSIG Conference ISSN* (Vol. 2473, p. 3857).

- Ibanez, M. B., Di-Serio, A., & Delgado-Kloos, C. (2014). Gamification for engaging computer science students in learning activities: A case study. *IEEE Transactions on learning technologies*, *7*(3), 291-301.

- Ko, S., & Rossen, S. (2017). *Teaching online: A practical guide*. Routledge.

- Korovessis, P., Furnell, S. M., Papadaki, M., & Haskell-Dowland, P. S. (2017). A toolkit approach to information security awareness and education.

- Logan, P. Y., & Clarkson, A. (2005). Teaching Students to Hack: Curriculum Issues in Information Security. Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education, 157–161. https://doi.org/10.1145/1047344.1047405

- M. Zhao, P. Chen, J. Wang and L. Yang, "The Practice of the Flipped Classroom Mode in the Information System Security Curriculum," *2018 9th International Conference on*

Information Technology in Medicine and Education (ITME), Hangzhou, 2018, pp. 669-672. doi: 10.1109/ITME.2018.00154

- Messeguer, P. y otros (2015) Enseñanza de la informática en primaria, secundaria y bachillerato: estado español, 2015. http://www.scie.es/wp-content/uploads/2015/05/Inform%C3%A1tica-Primaria-ESO-Bach.pdf

- Oriyano. (2016). CEH v9: Certified Ethical Hacker Version 9 Study Guide (Vol. 9). John Wiley & Sons.

- Pashel, B. A. (2006). Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level. Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, 197–200. https://doi.org/10.1145/1231047.1231088

- Riesco, M. y otros (julio 2014) La Informática como materia fundamental en un sistema educativo del siglo XXI. Actas de las XX JENUI.

- Schreuders, Z. C., & Butterfield, E. (2016). Gamification for teaching and learning computer security in higher education. In *2016 {USENIX} Workshop on Advances in Security Education ({ASE} 16)*.

- Seo, J. H., Bruner, M., Payne, A., Gober, N., & Chakravorty, D. K. (2019). Using Virtual Reality to Enforce Principles of Cybersecurity. *Journal of Computational Science*, *10*(1).

- Sheoran, P., & Singh, S. (2014). Applications of ethical hacking. International Journal of Enhanced Research in Science Technology & Engineering, ISSN, 2319-7463.

- Tourón, J. & Santiago, R. (2015). El modelo Flipped Learning y el desarrollo del talento en la escuela. *Revista de Educación*, 368 (abril-junio), pp. 196-231.

- Trabelsi, Z. (2014, October). Enhancing the comprehension of network sniffing attack in information security education using a hands-on lab approach. In *Proceedings of the 15th Annual Conference on Information technology education* (pp. 39-44). ACM.

- Trabelsi, Z., & McCoey, M. (2016). Ethical hacking in Information Security curricula. *International Journal of Information and Communication Technology Education (IJICTE)*, *12*(1), 1-10.

- Xu, L., Huang, D., & Tsai, W. T. (2013). Cloud-based virtual laboratory for network security education. *IEEE Transactions on Education*, *57*(3), 145-150.

- Yonemura, K., Sato, J., Takeichi, Y., Komura, R., & Yajima, K. (2018, July). Security Education Using Gamification Theory. In *2018 International Conference on Engineering, Applied Sciences, and Technology (ICEAST)* (pp. 1-4). IEEE.

- Zainuddin, Z., & Halili, S. (2016). Flipped classroom research and trends from different fields of study. *The international review of research in open and distributed learning*, *17*(3).