



Universidad
Internacional
de Valencia

Guía didáctica

ASIGNATURA: *Seguridad Informática*

Título: *Grado en Ingeniería Informática*

Materia: *Mención en Tecnologías de la Información*

Créditos: 6 ECTS

Código: 31GIIN

Índice

1. Organización general.....	3
1.1. Datos de la asignatura.....	3
1.2. Equipo docente	3
1.3. Introducción a la asignatura.....	3
1.4. Competencias y resultados de aprendizaje	3
2. Contenidos/temario	5
3. Metodología	7
4. Actividades formativas	8
5. Evaluación.....	9
5.1. Sistema de evaluación.....	9
5.2. Sistema de calificación	10
6. Bibliografía.....	10
6.1. Bibliografía de referencia.....	10

1. Organización general

1.1. Datos de la asignatura

MÓDULO	Menciones
MATERIA	Mención en Tecnologías de la Información
ASIGNATURA	<i>Seguridad Informática</i> 6 ECTS
Carácter	Optativa
Curso	Tercero
Cuatrimestre	Segundo
Idioma en que se imparte	Castellano
Requisitos previos	No existen
Dedicación al estudio por ECTS	25 horas

1.2. Equipo docente

Profesor	D. David Cereijo Grana dcereijog@professor.universidadviu.com
-----------------	---

1.3. Introducción a la asignatura

Esta asignatura contribuirá a que el graduado o graduada en ingeniería obtenga las competencias en la implementación y el uso de sistemas de cómputo, sistemas operativos, software y redes de telecomunicaciones de forma segura. Sin dejar de lado el desarrollo de software seguro, teniendo en cuenta desde la fase de diseño la seguridad como una prioridad (Security by Design & Secure by Default).

1.4. Competencias y resultados de aprendizaje

COMPETENCIAS GENERALES

CG.3.- Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

- CG.4.- Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos según lo establecido en la resolución.
- CG.5.- Capacidad para concebir, desarrollar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad, de acuerdo con los conocimientos adquiridos según lo establecido en la resolución.
- CG.6.- Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes de acuerdo con los conocimientos adquiridos según lo establecido en la resolución.
- CG.7.- Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento.
- CG8 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.
- CG9 - Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

COMPETENCIAS ESPECÍFICAS DE LA ASIGNATURA

- TI.1.- Demostrar comprensión del entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.
- TI.4.- Seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.
- TI.5.- Seleccionar, desplegar, integrar y gestionar sistemas de información que satisfagan las necesidades de la organización con los criterios de costo y calidad identificados.
- TI.6.- Concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación móvil

RESULTADOS DE APRENDIZAJE

Al finalizar esta asignatura se espera que el estudiante sea capaz de:

- RA.1.- Identificar las amenazas y los riesgos de seguridad de los Sistemas Informáticos
- RA.2.- Describir la problemática de seguridad de las redes de computadores con el fin de encontrar soluciones para protegerlas
- RA.3.- Explicar los mecanismos de protección y las políticas de seguridad
- RA.4.- Diseñar mecanismos de protección para aplicaciones distribuidas

2. Contenidos/temario

Tema 1. Introducción a la Seguridad

- 1.1. Introducción
 - 1.1.1. Objetivos
 - 1.1.2. La era de la información
- 1.2. Conceptos de Seguridad Informática
 - 1.2.1. Seguridad física
 - 1.2.2. Seguridad lógica
 - 1.2.3. Seguridad activa y pasiva
 - 1.2.4. Política de seguridad
 - 1.2.5. Dominios de la Seguridad Informática
- 1.3. Amenazas en un Sistema de Información
 - 1.3.1. Interrupción
 - 1.3.2. Intercepción
 - 1.3.3. Alteración
 - 1.3.4. Fabricación
- 1.4. Tipos y técnicas de ataque
 - 1.4.1. Ataques pasivos
 - 1.4.2. Ataques activos
 - 1.4.3. Técnicas de ataque
- 1.5. Ejemplos de la vida cotidiana
 - 1.5.1. Dispositivos móviles
 - 1.5.2. Correo electrónico
 - 1.5.3. Servicios online
 - 1.5.4. Página Web corporativa
 - 1.5.5. El usuario

Tema 2. Análisis de activos y riesgos

- 2.1. Fase 1. Definir el alcance
- 2.2. Fase 2. Identificar los activos
- 2.3. Fase 3. Identificar / seleccionar las amenazas
- 2.4. Fase 4. Identificar vulnerabilidades y salvaguardas
- 2.5. Fase 5. Evaluar el riesgo
 - 2.5.1. Cálculo del riesgo
- 2.6. Fase 6. Tratar el riesgo
- 2.7. Principales activos
 - 2.7.1. Equipos
 - 2.7.2. Software
 - 2.7.3. Datos o información
 - 2.7.4. Comunicaciones
- 2.8. Planes de riesgo

Tema 3. Seguridad pasiva

- 3.1. Elementos redundantes
- 3.2. Fuentes de alimentación
- 3.3. Sistemas de alimentación ininterrumpida
- 3.4. Discos
- 3.5. Sistemas RAID
- 3.6. Niveles RAID múltiple
- 3.7. Otras arquitecturas de almacenamiento
 - 3.7.1. Clúster de servidores
 - 3.7.2. Arquitecturas SAN, NAS y DAS
- 3.8. Copias de seguridad. Políticas.
 - 3.8.1. Política de copias de seguridad
 - 3.8.2. Consideraciones y tipos de copia de seguridad
 - 3.8.3. Copia completa
 - 3.8.4. Copia incremental
 - 3.8.5. Copia diferencial
 - 3.8.6. Copia espejo

Tema 4. Seguridad activa

- 4.1. Gestión de contraseñas
- 4.2. Control de acceso
- 4.3. Certificados y sistemas de clave pública y privada
- 4.4. Utilización de criptografía

Tema 5. Seguridad en profundidad. Análisis descendente

- 5.1. Seguridad por capas
- 5.2. Perímetro físico
- 5.3. Perímetro lógico o virtual
- 5.4. Red interna
- 5.5. Equipo. Aplicación. Datos.

Tema 6. Dentro de la red. Seguridad perimetral.

- 6.1. Segmentación de la red
- 6.2. VPN para conectar segmentos
- 6.3. Cortafuegos
 - 6.3.1. Filtrado de paquetes
 - 6.3.2. Pasarelas a nivel de aplicación
 - 6.3.3. Pasarelas a nivel de circuito
 - 6.3.4. Otros
- 6.4. NIDS (Network IDS)
 - 6.4.1. Intrusión
 - 6.4.2. Detección de intrusiones
 - 6.4.3. Primeros sistemas IDS
 - 6.4.4. Sistemas de detección de intrusos actuales
- 6.5. IPS (Intrusion Prevention Systems)
 - 6.5.1. Ejemplos

- 6.5.2. IPS en línea
- 6.5.3. IPS de nivel siete
- 6.5.4. IPS a nivel de aplicación
- 6.5.5. IPS híbridos

Tema 7. Dentro de la red II. Seguridad del sistema.

- 7.1. Hardening de Sistemas Operativos
- 7.2. Autenticación y Autorización
- 7.3. Cuotas
- 7.4. Actualizaciones críticas y parches de seguridad
- 7.5. Antivirus
- 7.6. Imágenes del Sistema
- 7.7. Puntos de restauración
- 7.8. Congelación
- 7.9. ACL
- 7.10. HIDS (Host IDS)

Tema 8. Mantenimiento del sistema

- 8.1. Actualizaciones
- 8.2. Automatización de tareas
- 8.3. Monitorización de la red y del sistema
- 8.4. SIEM
- 8.5. ELK
- 8.6. Monitorización de los registros de incidencias
- 8.7. Monitorización del rendimiento del sistema

3. Metodología

La metodología de la Universidad Internacional de Valencia (VIU) se caracteriza por una apuesta decidida en un modelo de carácter e-presencial. Así, siguiendo lo estipulado en el calendario de actividades docentes del Título, se impartirán en directo un conjunto de sesiones, que, además, quedarán grabadas para su posterior visionado por parte de aquellos estudiantes que lo necesitasen. En todo caso, se recomienda acudir, en la medida de lo posible, a dichas sesiones, facilitando así el intercambio de experiencias y dudas con el docente.

En lo que se refiere a las metodologías específicas de enseñanza-aprendizaje, serán aplicadas por el docente en función de los contenidos de la asignatura y de las necesidades pedagógicas de los estudiantes. De manera general, se impartirán contenidos teóricos y, en el ámbito de las clases prácticas se podrá realizar la resolución de problemas, el estudio de casos y/o la simulación.

Por otro lado, la Universidad y sus docentes ofrecen un acompañamiento continuo al estudiante, poniendo a su disposición foros de dudas y tutorías para resolver las consultas de carácter académico que el estudiante pueda tener. Es importante señalar que resulta

fundamental el trabajo autónomo del estudiante para lograr una adecuada consecución de los objetivos formativos previstos para la asignatura.

4. Actividades formativas

Durante el desarrollo de cada una de las asignaturas se programan una serie de actividades de aprendizaje que ayudan a los estudiantes a consolidar los conocimientos trabajados.

A continuación, se relacionan las actividades que forman parte de la asignatura:

1. Actividades de carácter teórico

Se trata de un conjunto de actividades guiadas por el profesor de la asignatura destinadas a la adquisición por parte de los estudiantes de los contenidos teóricos de la misma. Estas actividades, diseñadas de manera integral, se complementan entre sí y están directamente relacionadas con los materiales teóricos que se ponen a disposición del estudiante (manual, SCORM y material complementario). Estas actividades se desglosan en las siguientes categorías:

- a. Clases expositivas
- b. Sesiones con expertos en el aula
- c. Observación y evaluación de recursos didácticos audiovisuales
- d. Estudio y seguimiento de material interactivo

2. Actividades de carácter práctico

Se trata de un conjunto de actividades guiadas y supervisadas por el profesor de la asignatura vinculadas con la adquisición por parte de los estudiantes de los resultados de aprendizaje y competencias de carácter más práctico. Estas actividades, diseñadas con visión de conjunto, están relacionadas entre sí para ofrecer al estudiante una formación completa e integral.

3. Tutorías

Se trata de sesiones, tanto de carácter síncrono como asíncrono (e-mail), individuales o colectivas, en las que el profesor comparte información sobre el progreso académico del estudiante y en las que se resuelven dudas y se dan orientaciones específicas ante dificultades concretas en el desarrollo de la asignatura.

4. Trabajo autónomo

Se trata de un conjunto de actividades que el estudiante desarrolla autónomamente y que están enfocadas a lograr un aprendizaje significativo y a superar la evaluación de la asignatura. La realización de estas actividades es indispensable para adquirir las competencias y se encuentran entroncadas en el aprendizaje autónomo que consagra la actual ordenación de enseñanzas universitarias. Esta actividad, por su definición, tiene carácter asíncrono.

5. Prueba objetiva final

Como parte de la evaluación de cada una de las asignaturas (a excepción de las prácticas y el Trabajo fin de título), se realiza una prueba (examen final). Esta prueba se realiza en tiempo real (con los medios de control antifraude especificados) y tiene como objetivo evidenciar el nivel de adquisición de conocimientos y desarrollo de competencias por parte de los estudiantes. Esta actividad, por su definición, tiene carácter síncrono.

5. Evaluación

5.1. Sistema de evaluación

El Modelo de Evaluación de estudiantes en la Universidad se sustenta en los principios del Espacio Europeo de Educación Superior (EEES), y está adaptado a la estructura de formación virtual propia de esta Universidad. De este modo, se dirige a la evaluación de competencias.

Sistema de Evaluación	Ponderación
Portafolio*	40 %
<i>Entrega de informes de problemas y ejercicios</i>	10%
<i>Planteamiento, estudio, análisis y resolución de casos</i>	10%
<i>Informes o memorias de prácticas de laboratorio</i>	15%
<i>Participación activa en los debates, foros y otros medios</i>	5%.
Sistema de Evaluación	Ponderación
Prueba final*	60 %
<i>La prueba final consistirá en un examen en línea, el cual incluirá preguntas de tipo teóricas, así como resolución de ejercicios y/o problemas. Esto permitirá que el estudiante demuestre que ha alcanzado las competencias y resultados de aprendizaje esperados en cada una de las unidades competenciales.</i>	

***Es requisito indispensable para superar la asignatura aprobar cada apartado (portafolio y prueba final) con un mínimo de 5 para ponderar las calificaciones.**

Los enunciados y especificaciones propias de las distintas actividades serán aportados por el docente, a través del Campus Virtual, a lo largo de la impartición de la asignatura.

Atendiendo a la Normativa de Evaluación de la Universidad, se tendrá en cuenta que la utilización de **contenido de autoría ajena** al propio estudiante debe ser citada adecuadamente en los trabajos entregados. Los casos de plagio serán sancionados con suspenso (0) de la actividad en la que se detecte. Asimismo, el uso de **medios fraudulentos durante las pruebas de evaluación** implicará un suspenso (0) y podrá implicar la apertura de un expediente disciplinario.

5.2. Sistema de calificación

La calificación de la asignatura se establecerá en los siguientes cálculos y términos:

Nivel de aprendizaje	Calificación numérica	Calificación cualitativa
Muy competente	9,0 - 10	Sobresaliente
Competente	7,0 - 8,9	Notable
Aceptable	5,0 -6,9	Aprobado
Aún no competente	0,0 -4,9	Suspenso

Sin detrimento de lo anterior, el estudiante dispondrá de una **rúbrica simplificada** en el aula que mostrará los aspectos que valorará el docente, como así también los **niveles de desempeño que tendrá en cuenta para calificar las actividades vinculadas a cada resultado de aprendizaje**.

La mención de «**Matrícula de Honor**» podrá ser otorgada a estudiantes que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los estudiantes matriculados en una materia en el correspondiente curso académico, salvo que el número de estudiantes matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

6. Bibliografía

6.1. Bibliografía de referencia

- Blanco, J. (2019, 8 de septiembre). Manual de la asignatura. Seguridad Informática.
- Ablon, L.; Bogart, A. (2017). Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits. Santa Monica, California: RAND Corporation. ISBN: 978-0-8330-9761-3
- Ali, B., Awad, A.I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors, 18(3), 817. doi: 10.3390/s18030817
- Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. Procedia Computer Science, 124, 691-697. doi: 10.1016/j.procs.2017.12.206
- Arriols, E. (2018). Chief Information Security Office: El Red Team de la empresa. Madrid: OXWORD Computing. ISBN: 978-84-09-01497-2
- Barman, S.; Samanta, D.; Chattopadhyay, S. (2015). Fingerprint-based crypto-biometric system for network security. EURASIP Journal on Information Security. 3. doi: 10.1186/s13635-015-0020-1

Blanco, J. (2018a, 22 de junio). El RGPD cumple 2 años. [universidadviu.es](https://www.universidadviu.es/el-rgpd-cumple-2-anos/). Recuperado de <https://www.universidadviu.es/el-rgpd-cumple-2-anos/> (último acceso: 30 de septiembre 2019)

Blanco, J. (2018b, 15 de septiembre). Tu propia VPN con una Raspberry Pi. Sospedia.net. Recuperado de <https://sospedia.net/tu-propia-vpn-con-una-raspberry-pi/> (último acceso: 28 de septiembre 2019)

Blanco, J. (2019, 8 de septiembre). Tareas programadas en Linux. Sospedia.net. Recuperado de <https://sospedia.net/tareas-programadas-en-linux/> (último acceso: 28 de septiembre 2019)

Centro Criptológico Nacional (2019). PILAR. Metodología. Recuperado de <https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/metodologia.html> (último acceso: 15 de septiembre 2019)

Denning, D. E., Neumann, P. G. (1985). Requirements and Model for IDIS - A Real-Time Intrusion Detection Expert System. Technical Report, Computer Science Laboratory, SRI International, Menlo Park, California

DNSstuff (2019, 24 de mayo). 5 Best Free and Open-Source SIEM Tools in 2019. Recuperado de <https://www.dnsstuff.com/free-siem-tools> (último acceso: 17 de septiembre 2019)

FNMT (2019). Una solución con solera: la criptografía. Recuperado de https://www.cert.fnmt.es/content/pages_std/html/tutoriales/tuto3.htm (último acceso: 16 de septiembre 2019)

FreeNAS (2019). FreeNAS features. Recuperado de <https://www.freenas.org/about/features/> (último acceso: 22 de septiembre 2019)

Gartner (2019a). Reviews for Intrusion Detection and Prevention Systems. Recuperado de <https://www.gartner.com/reviews/market/intrusion-prevention-systems> (último acceso: 16 de septiembre 2019)

Gartner (2019b). Unified Threat Management (UTM). IT Glossary. Recuperado de <https://www.gartner.com/it-glossary/unified-threat-management-utm> (último acceso: 16 de septiembre 2019)

Gil, Ana María (2017, 9 de octubre). ¿Qué es la Seguridad por Capas? CyberSecurityNews. Recuperado de <https://cybersecuritynews.es/que-es-la-seguridad-por-capas-2/> (último acceso: 22 de septiembre 2019)

Huang, D.Y.; Matthaios Aliapoulios, M.; Li, V.G.; Invernizzi, L.; McRoberts, K.; Bursztein, E.; Levin, J.; Levchenko, K.; Snoeren, A. C.; Damon McCoy, D. (2018). Tracking Ransomware End-to-end.

2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 618-631. doi: 10.1109/SP.2018.00047

INCIBE (2015, 9 de septiembre). Insistimos: ¡Haz copias de seguridad! (1/2). Recuperado de <https://www.incibe.es/protege-tu-empresa/blog/copias-seguridad-01> (último acceso: 22 de septiembre 2019)

INCIBE (2017a, 16 de enero). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. Recuperado de <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo> (último acceso: 15 de septiembre 2019)

INCIBE (2017b, 10 de febrero). Analizadores de red en sistemas de control. Recuperado de <https://www.incibe-cert.es/blog/analizadores-red-sistemas-control> (último acceso: 15 de septiembre 2019)

INCIBE (2018). Políticas de seguridad para la pyme: copias de seguridad. Recuperado de <https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/copias-seguridad.pdf> (último acceso: 22 de septiembre 2019)

INCIBE (2019). Políticas de seguridad para la pyme: contraseñas. Recuperado de <https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf> (último acceso: 18 de septiembre 2019)

Internet Engineering Task Force (IETF) (1996). Address Allocation for Private Internets. Request for Comments (RFC): 1918. Recuperado de <https://tools.ietf.org/html/rfc1918> (último acceso: 20 de septiembre 2019)

Internet Engineering Task Force (IETF) (1998). Security Architecture for the Internet Protocol. Request for Comments (RFC): 2401. Recuperado de <https://tools.ietf.org/html/rfc2401> (último acceso: 20 de septiembre 2019)

Internet Engineering Task Force (IETF) (2007). Internet Security Glossary, Version 2. Request for Comments (RFC): 4949. Recuperado de <https://tools.ietf.org/html/rfc4949> (último acceso: 20 de septiembre 2019)

Jang-Jaccard, J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993. ISSN 0022-0000. doi: 10.1016/j.jcss.2014.02.005

Jouini, M.; Rabai, L.B.A.; Aissa, A.B. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, 32, 489-496. ISSN 1877-0509. doi: 10.1016/j.procs.2014.05.452

Kereki, F. (2008, 7 de febrero). Sudo, or Not Sudo: That Is The Question. Recuperado de <https://www.linux.com/news/sudo-or-not-sudo-question/> (último acceso: 25 de septiembre 2019)

Lewis, K. (2017). Chapter 78. Endpoint Security. En J. R. Vacca (Ed.). *Computer and Information Security Handbook (Third Edition)* (pp. 1049-1055). Morgan Kaufmann. ISBN 9780128038437. doi: 10.1016/b978-0-12-803843-7.00078-8

Lundgren, B.; Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, 25(2), 419–441. doi: 10.1007/s11948-017-9992-1

Ministerio de Hacienda y Administraciones Públicas (Ed.) (2012a). *MAGERIT v.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Octubre 2012. NIPO: 630-12-171-8. Recuperado de

https://www.administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html (último acceso: 28 de septiembre 2019)

Ministerio de Hacienda y Administraciones Públicas (Ed.) (2012b). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método*. Centro de Publicaciones del Ministerio de Hacienda y Administraciones Públicas. Secretaría General Técnica. Subdirección General de Información, Documentación y Publicaciones.

Colección: administración electrónica. NIPO: 630-12-171-8. Recuperado de <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html> (último acceso: 15 de septiembre 2019)

Mitra, A., Najjar, W.A., & Bhuyan, L.N. (2007). Compiling PCRE to FPGA for accelerating SNORT IDS. ANCS. 07. Proceedings of the 3rd ACM/IEEE Symposium on Architecture for networking and communications systems, 127-136. doi: 10.1145/1323548.1323571

National Institute of Standards and Technology (NIST) (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-94*. Recuperado de <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf> (último acceso: 20 de septiembre 2019)

National Institute of Standards and Technology (NIST) (2012). *BIOS Protection Guidelines for Servers (Draft). Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-147B (Draft)*. Recuperado de https://csrc.nist.gov/csrc/media/publications/sp/800-147b/final/documents/draft-sp800-147b_july2012.pdf (último acceso: 28 de septiembre 2019)

National Institute of Standards and Technology (NIST) (2018a). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. NIST Special Publication 800-160, 1, pp. 172*. doi: 10.6028/NIST.SP.800-160v1

Noriega, S. (2014). *5 Elementos De Seguridad De Tu Página Web Que Debes Conocer*. CertStopShop. Recuperado de <https://www.certstopshop.com/blog/5-elementos-de-seguridad-de-tu-pagina-web-que-debes-conocer> (último acceso: 22 de septiembre 2019)

Sebring, M. M., Sellhouse, E., Hanna, M. E., Whitehurst, R. A. (1988). Expert system in intrusion detection: A case study. In Proceedings of the 11th National Computer Security Conference, pp. 74-81, Baltimore, Maryland.

Sneha, M. (2015). Performance Analysis of RAIDs in Storage Area Network. *International Journal of Computer Applications*, 126(13), 26-31. doi: 10.5120/ijca2015906231

Spafford, E. H. (1989). Crisis and aftermath. *Communications of the ACM*. 32(6), 678-687 doi: 10.1145/63526.63527

SRI International Computer Science Laboratory (2019). *History*. Recuperado de <http://www.csl.sri.com/programs/intrusion/history.html> (último acceso: 16 de septiembre 2019)

Tener W. T. (1989). Discovery: An expert system in the commercial data security environment. In Proceedings of the 4th IFIP TC11 International Conference on Security, pages 261-268, 1989. Recuperado de https://www.cerias.purdue.edu/about/history/coast_resources/idcontent/ids.html

UNE (2017). UNE-EN ISO 27002:2017. Recuperado de <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0058429> (último acceso: 15 de septiembre 2019)

Zhao, Y.; Li, S.; Jiang, L. (2018). Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment. Security and Communication Networks, 2018(9178941), 13 pp. doi: 10.1155/2018/9178941