

BIBLIOGRAFIA

[DRAG11] Dragonjar, (2011), “NETWORK AND SYSTEM SECURITY”, <http://www.dragonjar.org/101-libros-de-seguridad-informatica-gratis.xhtml>, editorial Sysgress.

[IMH14] Instituto Máquina Herramienta, (2013). “FIREWALL O CORTAFUEGOS”, <http://www.imh.eus/es/comunicacion/dokumentazio-irekia/manuales/seguridad-basica-en-internet/firewall-cortafuegos/referencemanual-all-pages>, <http://www.imh.eus>

[JAV10] Javajan, Webs for designers and you, (2010), “ARQUITECTURA DE UN SITIO WEB” http://www.guiadiseño.com/05_arquitectura.php

[KOOLE15] Dejan Kosutic, Oscar, Rhand Leal, (2015), “ ISO 27001 STANDARD”, <http://www.iso27001standard.com/es/que-es-iso-27001>

[KIO14] Kioskea.net, (2014). “SISTEMA DE DETECCIÓN DE INTRUSIONES”, <http://es.kioskea.net/contents/detection-171307462#162>, Kioskea.net.

[LOMAMOGL10] Iren Lorenzo-Fonseca, Francisco Maciá-Pérez, Francisco José Mora-Gimeno, Diego Marcos-Jorquera, Juan Antonio Gil-Martínez, Rogelio Lau-Fernández, (2010). “SISTEMA DE DETECCIÓN DE INTRUSIONES”, <https://www.dtic.ua.es/grupoM/recursos/articulos/JDARE-09-B.pdf>, Centro de Estudio de Ingeniería y Sistema – Instituto Superior Politécnico José Antonio Echevarría.

[MEA13] Rolling Meadows, (2013), “COBIT 5”, <http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-tiene-ya-disponible-la-version-en-espanol-de-COBIT-5.aspx>, <http://www.isaca.org>

[OWA14] owasp.org, (2010). “CROSS SITE SCRIPTING(XSS)”, https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29, owasp.org.

[PFC11] PFC Marisa, (2011), “INTRODUCCIÓN A LOS IDS”,
http://www.adminso.es/index.php/Archivo:Pfc_Marisa_Capitulo1.pdf

[ROM14] MSc. Romaniz C. Susana, (2014). “SEGURIDAD DE APLICACIONES WEB: VULNERABILIDADES EN LOS CONTROLES DE ACCESO”,

<http://sedici.unlp.edu.ar/bitstream/handle/10915/21581/1927+-+Seguridad+de+aplicaciones+web+vulnerabilidades+en+los+controles+de+acceso.pdf;jsessionid=8F904076D591AFBCFC689D7AF53F5169?sequen ce=1>, Facultad Regional Santa Fe - Universidad Tecnológica Nacional.

[SEIN15] Segu - Info, (2015). “SEGURIDAD INFORMÁTICA - IMPLICANCIAS E IMPLEMENTACIÓN”, <http://www.segu-info.com.ar/tesis/>, <http://www.segu-info.com.ar>

[NCA13] ncalculators, (2013), “CALCULATORS STATISTICS”,
<http://es.ncalculators.com/statistics/>

WEBGRAFIA

Angular - Seguridad, protegiendo vistas con guards (23/08/2018),
<https://codingpotions.com/angular-seguridad>

Evasión de autenticación con inyección SQL. (21/11/2013),
<https://www.securityartwork.es/2013/11/21/evasion-de-autenticacion-con-inyeccion-sql/>

Las 10 vulnerabilidades Web más explotadas. Open Security [10/01/2018],
<http://www.opensecurity.es/las-10-vulnerabilidades-web-mas-explotadas/>

Cross Site Scripting. SI4xUz (12/05/2018). <http://www.milw0rm.com/papers/207>

XSS: Cross Site Scripting – ¿Cómo evitarlo?. Stephen Reinhardt [29/10/2017],
<http://10typesofpeople.wordpress.com/2007/10/29/xss-cross-site-scripting-%C2%BFcomo-evitarlo/>

Code Injection Vulnerabilities Explained. The Server Pages [30/07/2014],
http://www.theserverpages.com/articles/webmasters/php/security/Code_Injection_Vulnerab

[ilities Explained.html](#)

Cross-Site Request Forgery. OWASP (23/10/2019), http://www.owasp.org/index.php/Cross-Site_Request_Forgery

Buffer Overflow. OWASP (21/02/2019), http://www.owasp.org/index.php/Buffer_Overflow

SQL Injection Attacks by Example. Steve Friedl (10/10/2017), <http://www.unixwiz.net/techtips/sql-injection.html>

Ataques mediante SQL Injection. Issel Guberna (2017), http://www.programacionphp.net/recursos-articulos/articulos-de-Vulnerabilidades/SQL-injection_0001601.html

Ataques XSS: Cross-Site Scripting en PHP (Copyright © Diego Lázaro 2018)
<https://diego.com.es/ataques-xss-cross-site-scripting-en-php>

Codificar los datos para evitar ataques XSS en una página web (Escrito por picodotdev el 29/03/2019)
<https://picodotdev.github.io/blog-bitix/2019/03/codificar-los-datos-para-evitar-ataques-xss-en-una-pagina-web/>