
Actas del Congreso Iberoamericano de Docentes

# Estado de la investigación sobre el análisis de vulnerabilidades en instituciones de educación superior en Colombia

Luis Eduardo Baquero Rey

Miguel Hernández Bejarano

ISBN: 978-84-948417-0-5 Artículo 1520

ISBN: 978-84-948417-0-5

Edita **Asociación Formación IB**.

Coordinación editorial: **Joaquín Asenjo Pérez, Óscar Macías Álvarez, Patricia Ávalo Ortega y Yoel Yucra Beisaga**

Año de edición: **2018**

Presidente del Comité Científico: **César Bernal.**

El I Congreso Iberoamericano de Docentes se ha celebrado organizado conjuntamente por la Universidad de Cádiz y la Asociación Formación IB con el apoyo del Ayuntamiento de Algeciras y la Asociación Diverciencia entre otras instituciones.

http://congreso.formacionib.org

red iberoamericana de docentes


formaciónib

# Estado de la investigación sobre el análisis de vulnerabilidades en instituciones de educación superior en Colombia

Luis Eduardo Baquero Rey[1], Miguel Hernández Bejarano[2]
Fundación Universitaria Los Libertadores
[1]lebaqueror@libertadores.edu.co, [2]mhernandezb@libertadores.edu.co

**RESUMEN**

Las Instituciones de Educación Superior (IES) son entidades que se organizan y conforman de características distintivas que entre ellas son similares, pero diferentes a las demás tipos de organizaciones; y también están expuestas a diferentes tipologías de amenazas cibernéticas. Este estudio hace parte integrante del desarrollo de un proyecto de investigación titulado "*Análisis de vulnerabilidades y hacking ético para la Fundación Universitaria Los Libertadores – Sede Bogotá, D.C.*" el cual pretende como uno de sus objetivos proponer un modelo de análisis de vulnerabilidades y hacking ético para IES y aplicarlo a las institución mencionada con el fin de validarlo y realizarle los ajustes correspondientes, de tal manera que pueda ser implementado en cualquier IES con el fin de mitigar de mejor manera los problemas relacionados con la seguridad informática. En este sentido, se pretende lograr consolidar el desarrollo del mismo, gracias a un proceso investigativo que involucra conceptos, descripción de herramientas software, artículos científicos, libros y documentos en general contenidos en fuentes de consulta especializada; con el ánimo de evaluar el estado actual de la investigación sobre el análisis de vulnerabilidades en los diferentes sistemas informáticos de las instituciones de educación superior en Colombia.

El objetivo principal de dicha indagación, es unificar los diferentes trabajos desarrollados por investigadores a nivel nacional, extraer el conocimiento de los mismos para finalmente obtener un artículo de revisión que logre mostrar de una manera clara y contundente como ha venido avanzando la investigación sobre el análisis de vulnerabilidades en las instituciones de educación superior en nuestro país. Además dicho documento servirá como referente a las siguientes generaciones que forman parte del semillero de investigación, para futuras investigaciones o proyectos de implementación de sistemas de análisis de vulnerabilidades a nivel académico.

Actualmente la investigación se encuentra en el proceso de obtención de artículos científicos para conformar el estado del arte, motivo por el cual no se encontrarán resultados cuantificados.

*Palabras clave*: Análisis de vulnerabilidades, instituciones de educación superior, seguridad informática.

## INTRODUCCIÓN

En Colombia, las Instituciones de Educación Superior (IES) son las entidades que cuentan, con arreglo a las normas legales, con el reconocimiento oficial como prestadoras del servicio público de la educación superior en el territorio colombiano. Los requisitos y trámites para constituir una institución del nivel superior están consignados en la Ley 30 de 1992. Las instituciones son fundamentalmente de dos clases u orígenes: públicas o privadas. Como entidades que son, al igual que otro tipo de organizaciones, eventualmente se ven enfrentadas a problemas de seguridad informática.

Para comprender el tema de análisis de vulnerabilidades, se debe tener plena claridad que este es uno solo de los componentes de la seguridad informática. Con el anterior pretexto, se puede entrar a definir la vulnerabilidad como una o varias debilidades que pueda llegar a tener un sistema en general y que permite a un atacante con cierto grado de conocimiento el acceso al mismo, con el objetivo de realizar funciones no permitidas dentro de él; dichas vulnerabilidades se generan debido a la flexibilidad o ausencia de controles o programas especializados y en la mayoría de casos fallas que son corregidas por los desarrolladores a medida que se van realizando los diferentes testeos. Así mismo, otro elemento importante es la amenaza, la cual hace referencia a cualquier tipo de peligro potencial ya sea de tipo humano o informático y que busca identificar las vulnerabilidades de un sistema para generar un daño u obtener información, existen dos tipos de amenazas: las no intencionales en las cuales se pueden encontrar los desastres naturales o los errores humanos, y las intencionales en donde se encuentran clasificados los hackers y sus programas maliciosos. Al identificar una vulnerabilidad a tiempo, y dimensionar el daño o impacto negativo que esta pueda producir al sistema, se habla entonces de la “exposición”, pero si no se toman las medidas adecuadas y este daño se materializa, entonces se habla de un “impacto”. Cuando se analiza la vulnerabilidad, la amenaza y la exposición, se logra identificar el “riesgo”, el cual se mitiga mediante “contramedidas” que no son otra cosa que controles, cuyo objetivo principal es el de eliminar las vulnerabilidades y los riesgos que van ligados a ellas y que en un momento dado puede llegar a utilizar un intruso para realizar un ataque. Dichas contramedidas pueden ser de origen software, dispositivos electrónicos o controles establecidos por los expertos en seguridad informática (Portantier, 2012).

En el propósito de diseñar e implementar una metodología de análisis de vulnerabilidades y hacking ético para la Fundación Universitaria Los Libertadores - Sede Bogotá que permita minimizar el impacto de las vulnerabilidades y mitigar los riesgos, y con el fin de definir un modelo de análisis de vulnerabilidades y hacking ético para una institución de educación superior, fue necesario primero realizar un estado de la investigación sobre el análisis de vulnerabilidades en IES en Colombia, para el cual es su intención este documento.

## METODOLOGÍA

La metodología utilizada se apoya en un cronograma de actividades en donde se decide colocar en un orden lógico el proceso para el levantamiento de información completo y que consta de cuatro partes:

Una primera que consta de una fundamentación de conceptos básicos sobre el análisis de vulnerabilidades.

La segunda parte se compone de una matriz comparativa de herramientas software que resalta las características de cada programa.

La tercera tiene como finalidad reunir un número considerable de revistas y artículos científicos, que servirán para fundamentar el estado del arte y que posteriormente se analizará para extraer la información más relevante sobre el análisis de vulnerabilidades en instituciones de educación superior.

Por último, se plantean unas recomendaciones y conclusiones al respecto.

## LAS VULNERABILIDADES INFORMÁTICAS Y SUS CAUSAS

Las vulnerabilidades se pueden agrupar en función de:

1. **Diseño:**

• Diseño de la seguridad perimetral: Forma parte de la seguridad de redes, tiene por objetivo el control total de la información que ingresa o sale de un sistema colocando una frontera entre la red interna y la externa (en este caso toda red que interactúe con la interna y no solo internet) (Fabuel, 2013).

• Debilidad en el diseño de los protocolos utilizados en las redes: Suele presentarse cuando se utilizan protocolos “no seguros” para el enlace entre las aplicaciones y las capas subyacentes según el modelo OSI. Para algunos expertos se clasifican los protocolos Telnet, SNMP y FTP (Herrera, Herrera, & perfil, 2017).

• Políticas de seguridad deficientes e inexistentes: Hoy en día las organizaciones en general buscan implementar políticas de seguridad, con el objetivo de documentar sus procesos y contar con un apoyo para atender problemas o situaciones que comprometan la información (Tutorial, 2017), pero de no existir, exponen al conjunto de información a peligros informáticos ya que no existe ni un orden lógico ni responsables por los diferentes componentes de los sistemas informáticos.

2. **Implementación**:

• Errores de programación: Por deducción, se generan por falta o bajo nivel en la calidad de las pruebas anteriores a la puesta en producción de un producto software, dejando ventanas de tiempo entre la detección y la posterior corrección de los fallos en la programación.

• Existencia de “puertas traseras” en los sistemas informáticos: A diferencia de los errores de programación, las puertas traseras en los algoritmos de programación pueden ser incluidas para un uso legítimo por parte de un programador, generando un alto riesgo al ser descubiertas por personal no idóneo o autorizado ("Cómo diferenciar una puerta trasera de una vulnerabilidad", 2017)

• Descuidos de los fabricantes: Directamente relacionado con los errores de programación y las puertas traseras, puede afectar un dispositivo físico, ya sea un router, un switch, un dispositivo electrónico, un servidor, etc., con el agravante de que si no se pueden distribuir a nivel masivo las actualizaciones necesarias para corregir la falla, puede llegar a generar grandes pérdidas económicas.

3. **Uso**:

• Configuración inadecuada de los sistemas informáticos: Muchos dispositivos “de fábrica” contienen una configuración básica, esto se observa frecuentemente en los celulares, los computadores, los modem, los switch; en donde por ejemplo las contraseñas siempre serán las mismas o inclusive llegan a ser inexistentes hasta que son configuradas, esto conlleva a un alto índice de vulnerabilidad si el dispositivo posterior a una configuración vuelve a su estado inicial y no existe un proceso que indique lo contrario (Informáticos, 2017).

• Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática: Una organización puede contar con los recursos económicos suficientes para adquirir medios tecnológicos de última generación, pero el personal a cargo del mantenimiento o uso en general puede no contar con la capacitación o conocimiento

suficiente para darle un uso adecuado a la infraestructura a cargo sumado a la falta de interés o seguimiento de los jefes en estos aspectos, genera un alto riesgo en la seguridad informática (Informáticos, 2017).

- Disponibilidad de herramientas que facilitan los ataques: A nivel general en internet se encuentra tanto información como herramientas ya desarrolladas con el ánimo de que cualquier persona con un mínimo de conocimiento informático pueda experimentar y en muchos casos acceder a sistemas informáticos vulnerables que no cuenten con las medidas de seguridad para identificar vacíos.

- Limitación gubernamental de tecnologías de seguridad: Muchas de las grandes potencias, tienen restringido el desarrollo de productos y algoritmos especializados en seguridad, tal vez porque los ven más como una amenaza que como una herramienta de protección no solo para su información sino también para sus ciudadanos. Para este fin se logró un tratado conocido como el "acuerdo de Wassenaar", el cual: "es un régimen internacional de control de exportaciones de armas convencionales, bienes y tecnologías de uso dual susceptibles de desvío para propósitos de proliferación y fortalecimiento de capacidades militares. Está compuesto por 40 países que adoptan las listas de bienes controlados y ponen en práctica de acuerdo a su legislación interna (es decir, cada país determina la forma de internalizar los controles de exportación). Los miembros del Acuerdo se reúnen en una sesión plenaria anual en Viena para actualizar las listas de bienes controlados y determinar las solicitudes de ingreso de nuevos miembros" ("Dirección de Control de Exportaciones México", 2017).

- Vulnerabilidad del día cero: Hace referencia al hecho de conocer una vulnerabilidad, contando con el suficiente conocimiento de cómo utilizarla y/o explotarla, pero desconocer por completo la manera de solucionarla (Ministerio de Educación, Cultura y Deporte de España, 2017).

## CLASIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades se clasifican en:

- Vulnerabilidades de desbordamiento de búfer: Se pueden considerar como programas que buscan activar la saturación de información en otros programas, para que ellos almacenen temporalmente esta información en los búfer, debido a que existen lenguajes que no permiten este desbordamiento, se produce el bloqueo del mismo y por lo tanto la ejecución de un código diseñado para ingresar al sistema ("Ataques por desbordamiento de búfer", 2017).

- Vulnerabilidades de condición de carrera: Ocurre cuando dos o más procesos de un sistema operativo utilizan un mismo sector para su ejecución, generando datos inconsistentes o un bloqueo momentáneo lo cual crea una ventana de tiempo para que un atacante obtenga privilegios de administrador (Lab, 2017)

- Vulnerabilidades de error de formato de cadena: Se presenta en programas desarrollados bajo funciones que permiten opciones de formato como ejemplo el printf(), al no ingresar el tipo de formato u opción ("%algo") más la cadena, se deja abierto para que el atacante parametrice dicha cadena con el formato deseado, introduciendo su propio código ("Errores en las cadenas con formato | Websecurity.es", 2017).

- Vulnerabilidades de Cross Site Scripting (XSS) Existen dos tipos de XSS, la reflejada, que trata de modificar variables de intercambio entre dos páginas web con el ánimo de obtener las cookies para posteriormente "robar la identidad". Almacenada que es cuando se inyecta código HTML en la página web para capturar tráfico e información (Pérez, 2017).

• Vulnerabilidades de inyección SQL: Básicamente este ataque pretende insertar código SQL por medio de los datos de estrada del cliente hacia la aplicación, buscando modificar las consultas originales, por consultas que traerán otros datos como los son usuarios, etc., ("Ataques de inyección SQL: qué son y cómo protegerse - Pressroom Hostalia", 2017).

• Vulnerabilidades de denegación de servicio: Este tipo de ataque normalmente se dirige hacia los servidores de una organización con el ánimo de causar inhabilidad por un tiempo específico, a diferencia de las anteriores clasificaciones de vulnerabilidades esta o tiene por objetivo acceder a la información, sino causar pérdidas de tiempo que se traducen a pérdidas económicas de las organizaciones ("Ataque por denegación de servicio", 2017).

• Vulnerabilidades de ventanas engañosas: Este tipo de vulnerabilidad está presente generalmente en internet y tiene por objetivo mostrar algún tipo de información relevante a la víctima para que ella posteriormente acceda a un sitio que ya tiene parametrizado obtener información de forma directa que es cuando se digitan datos en formularios o indirecta que es cuando se realiza la instalación de programas que permiten el acceso a los dispositivos (acceso a la información almacenada) ("Seguridad informática", 2013)

## TIPOS DE VULNERABILIDADES

Las vulnerabilidades pueden ser:

• Vulnerabilidades que afectan equipos tecnológicos: Se clasifican tanto dispositivos finales (celulares, computadores), dispositivos de almacenamiento (servidores, dispositivos USB) como dispositivos de interconexión (switch, modem)

• Vulnerabilidades que afectan programas y aplicaciones: Incluyen sistemas operativos, aplicaciones (ofimáticas, juegos, navegadores)

## CASOS REPORTADOS EN INSTITUCIONES DE EDUCACIÓN SUPERIOR EN COLOMBIA

A medida que las IES utilizan recursos tecnológicos para facilitar el acceso a la información por parte de funcionarios administrativos, cuerpo docente, estudiantes y público en general, aumenta la posibilidad de que estos sistemas reciban ataques cibernéticos desde cualquier sitio y sea realizado por cualquier individuo; encontrándose Colombia en el año 2017 en la sexta posición a nivel mundial según la firma Symantec. (El Colombiano, 2018, p. 1)

La Universidad del Tolima fue víctima de un acceso no autorizado a sus sistemas de calificación, viéndose afectada por la modificación de las notas de alrededor de 18.000 estudiantes, según la fuente consultada los hackers lograron ingresar desde computadores externos aprovechando la época de vacaciones. Es de destacar dos puntos: como primera medida las autoridades mencionaron la posibilidad de que el autor del ataque conociera con anterioridad el sistema junto con su estructura; y como segundo punto importante la generación de backup al sistema lo que permitió la restauración de la información original. (El Tiempo, 2018, p. 4)

Sobre el mismo caso la firma Marrugo Rivera y Asociados (empresa especializada en Derecho y que ofrece servicios de asesoramiento en el impacto de la tecnología y el cumplimiento normativo), manifiesta: “es importante indagar cual ha sido la gestión en materia de seguridad informática en la institución educativa en el pasado” y va más allá

al afirmar que: “es necesario no solo emprender acciones para la remediación en este caso puntual, se deben establecer verdaderos programas que aseguren la continuidad y la posibilidad de aprender de los errores en estos casos” (Admin, 2018, p. 2). Y concluye diciendo: “Preocupa de sobremanera, que información personal de estudiantes, docentes y personal administrativo quede expuesta por falta de inversión en plataformas y programas que aseguren los activos en las instituciones tanto públicas como privadas en el país” (Admin, 2018, p. 3).

En el año 2015 un estudiante de ingeniería industrial de la Universidad de Los Andes utilizó key loggers, que es un programa del tipo Malware utilizado para capturar las pulsaciones en un teclado (Malenkovich, 2013, p. 2), con el objetivo de obtener las contraseñas de los docentes para modificar sus notas; al lograr su objetivo procedió a ofrecer este servicio vía email a estudiantes de la misma universidad y otra IES, lo cual condujo a su posterior captura por parte de la unidad de delitos informáticos de la Dijín. Claramente se observa en este caso como una persona sin los estudios técnicos necesarios y con el manejo de una herramienta software especializado, aprovecha vulnerabilidades de un sistema para acceder y realizar acciones no permitidas. (Obando, 2015, p. 3).

Hacia el año 2016 el grupo denominado “Anonimous” realizó un ataque a la página web de la Universidad de Los Andes, logrando modificar contenido y bloqueando el acceso a varios sitios de dicho portal, en su momento la respuesta al ataque por parte de la IES fue suspender el servicio de la página mientras lograban resolver las vulnerabilidades presentadas; en su defensa voceros de la IES argumentaron la constante inversión en equipos e infraestructura tecnológica al igual que la capacitación en temas de seguridad informática, y mencionaron: “Sin embargo, como la comunidad lo ha visto en los medios de comunicación, no es posible lograr el completo blindaje a este tipo de ataques”. (El Espectador, 2016, p. 3).

Según informe presentado por la Policía Nacional de Colombia y su división de control de Cibercrimen, para el año 2017 el sector de educación se ubicó en el tercer lugar en cuanto a ciberincidentes (Caivirtual, 2018, p. 9), encontrando los siguientes delitos informáticos según el código penal Colombiano:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación
- Interceptación de datos informáticos
- Daño informático
- Uso de software malicioso

## HERRAMIENTAS INFORMÁTICAS

Para hacerle frente a esta problemática es necesario la adopción de una buena práctica y utilizar las herramientas o herramientas apropiadas para cada caso. En este sentido, se estudiaron un total de 13 herramientas de software presentes en el mercado, utilizando para ellos una matriz comparativa indicando su desarrollador, distribuciones, algunas características especiales, medios soportados, compatibilidad, si es monousuario o multiusuario, el tipo de licenciamiento y el enlace oficial de información y descarga.

## RECOMENDACIONES

- Contar con un área específica de seguridad y defensa informática que cuente con personal idóneo para identificar, resolver y contrarrestar cualquier amenaza y así

mismo recibir reportes de incidencias por parte de usuarios de los diferentes sistemas.

- Estructurar una política de seguridad informática que cuente con controles adecuados sobre todos los sistemas informáticos de las IES, la cual debe ser de pleno conocimiento y aplicación por parte de los usuarios de los diferentes sistemas
- Generar una cultura de protección de la información enfocada al usuario interno a través de capacitaciones, sentido de pertenencia y una adecuada utilización de los recursos informáticos con el fin de evitar consecuencias legales.
- Diseñar, desarrollar y ejecutar planes de seguridad tecnológicos óptimos para cada tipo de sistema informático, que cuenten con seguimiento, revisión y ajustes periódicos.
- Realizar pruebas de intrusión controladas con el objetivo de identificar vulnerabilidades en los sistemas informáticos, realizando la documentación minuciosa para posteriormente efectuar análisis obteniendo así oportunidades de mejora.
- Destinar un porcentaje del ingreso de la IES al sistema de seguridad informática, teniendo en cuenta que la información es el recurso más valioso para cualquier tipo de entidad; resaltando que las IES cuentan no solo con datos de personas, sino también con aportes científicos de docentes y estudiantes.
- Mantener correctamente actualizados los diferentes sistemas informáticos según las recomendaciones de los desarrolladores.

## CONCLUSIONES

Una gran fortaleza de la investigación realizada hasta el momento es su marco teórico lo cual ayudara a entender el lenguaje que normalmente se utiliza en las revistas y artículos científicos, y que para muchos investigadores que no contamos con amplia experiencia o destreza en el mismo puede llegar a ser una dificultad en el desarrollo del proceso.

Como se menciona en la introducción, actualmente el proceso de investigación se encuentra en la etapa número tres que corresponde a la recopilación de artículos científicos relacionados con el análisis de vulnerabilidades en instituciones de educación superior en Colombia, a este punto no se han encontrado documentos que se centren puntualmente en el tema en mención, por lo tanto se están buscando artículos que se relacionen con seguridad informática y hacking ético en este tipo de instituciones.

Al ser un tema poco abordado no se logrará contar con suficientes datos como para poder generar graficas con tendencias o mediciones, personalmente considero que las mismas no generaran un gran aporte para el artículo de revisión, motivo por el cual la investigación se centrara en las investigaciones existentes y su respectivo aporte académico

El resultado de este trabajo será de gran utilidad para el semillero de seguridad informática de la Fundación Universitaria Los Libertadores, ya que podrá ser utilizado por estudiantes y académicos para implementar programas de identificación de vulnerabilidades que hoy en día afectan constantemente todo tipo de sistemas a nivel mundial.

## REFERENCIAS BIBLIOGRÁFICAS

Portantier, F. (2012). Seguridad informática 1era edición. Buenos Aires. Fox Andina.

Pérez, J., Bolaño López, F., & Rincón Mosquera, N. (2016). Arquitectura de seguridad de un entorno computacional para eCiencia en la nube (3rd ed.). Bogotá: Universidad

Distrital Francisco José de Caldas. Retrieved from http://revistas.udistrital.edu.co/ojs/index.php/revcie/article/view/11091/11933.

Vulnerabilidades de un sistema informático | Seguridad Informática. (2017). Descargas.pntic.mec.es. Retrieved 21 March 2017, from http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

Díaz, C. (2013). Implantación de un sistema de seguridad perimetral (1st ed., pp. 7, 8, 9, 10). Madrid: Universidad Politécnica de Madrid. Retrieved from http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf.

Herrera, s., Herrera, s., & perfil, V. (2017). VULNERABILIDAD DE LOS SISTEMAS INFORMÀTICOS. Vulnerabilidadtisg.blogspot.com.co. Retrieved 21 March 2017, from http://vulnerabilidadtisg.blogspot.com.co/

Tutorial. (2017). Redyseguridad.fi-p.unam.mx. Retrieved 21 March 2017, from http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html.

Cómo diferenciar una puerta trasera de una vulnerabilidad. (2017). SearchDataCenter en Español. Retrieved 31 March 2017, from http://searchdatacenter.techtarget.com/es/consejo/Como-diferenciar-una-puerta-trasera-de-una-vulnerabilidad

Informáticos, V. (2017). Vulnerabilidades de los Sistemas Informáticos. Inf-tres-quince.blogspot.com.co. Retrieved 22 March 2017, from http://inf-tres-quince.blogspot.com.co/2011/04/vulnerabilidades-de-los-sistemas.html

Dirección de Control de Exportaciones. (2017). Siicex.gob.mx. Retrieved 21 March 2017, from http://www.siicex.gob.mx/portalSiicex/CONTROL%20DE%20EXPORTACIONES/Preguntas%20frecuentes.html

Ataques por desbordamiento de búfer. (2017). CCM. Retrieved 22 March 2017, from http://es.ccm.net/contents/19-ataques-por-desbordamiento-de-bufer

Lab, I. (2017). La condición de carrera - internetlab.es. internetlab.es. Retrieved 22 March 2017, from http://www.internetlab.es/post/2548/condicion-de-carrera/

Errores en las cadenas con formato | Websecurity.es. (2017). Websecurity.es. Retrieved 22 March 2017, from http://www.websecurity.es/errores-las-cadenas-formato

Pérez, I. (2017). Comprendiendo la vulnerabilidad XSS (Cross-site Scripting) en sitios web. WeLiveSecurity. Retrieved 23 March 2017, from https://www.welivesecurity.com/la-es/2015/04/29/vulnerabilidad-xss-cross-site-scripting-sitios-web/

Ataques de inyección SQL: qué son y cómo protegerse - Pressroom Hostalia. (2017). Pressroom Hostalia. Retrieved 22 March 2017, from https://pressroom.hostalia.com/white-papers/ataques-inyeccion-sql

Ataque por denegación de servicio. (2017). CCM. Retrieved 23 March 2017, from http://es.ccm.net/contents/22-ataque-por-denegacion-de-servicio

SEGURIDAD INFORMATICA. (2013). Mrcdsq.blogspot.com.co. Retrieved 23 March 2017, from http://mrcdsq.blogspot.com.co/2013/04/normal-0-21-false-false-false-es-ec-x.html

El Colombiano. (2018). Colombia, el sexto país con más ciberataques en 2017. El Colombiano. Recuperado de http://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174

El Tiempo. (2018). Hacker mejoró notas de los estudiantes de la Universidad del Tolima. Noticias El tiempo. Recuperado de http://www.eltiempo.com/colombia/otras-ciudades/hacker-mejoro-las-notas-de-todos-estudiantes-de-la-universidad-del-tolima-177850.

Marrugo Rivera & Asociados. (2018). La Seguridad de la Información en las Universidades en Colombia. Marrugo Rivera & Asociados. Recuperado de https://www.marrugorivera.com/blog/2018/02/01/la-seguridad-de-la-informacion-en-las-universidades-en-colombia/

Malenkovich, S. (2013). Qué es un keylogger?. Karpersky Lab Daily. Recuperado de https://latam.kaspersky.com/blog/que-es-un-keylogger-2/453/

Obando, V. (2015). Universidades, víctimas de “hackers”. El Espectador. Recuperado de https://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884

El Espectador. (2016). Anonymous ataca el sitio web de la Universidad de los Andes. El Espectador. Recuperado de https://www.elespectador.com/noticias/actualidad/anonymous-ataca-el-sitio-web-de-universidad-de-los-ande-articulo-620617

Caivirtual. (2018). Informe: Balance Cibercrimen en Colombia 2017. Caivirtual. Recuperado de https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf.

Caivirtual. (2017). Ciberincidentes tiempo real histórico [Figura]. Recuperado de https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico.

Tenable. (2017). Nessus Vulnerability Scanner. [online] Available at: https://www.tenable.com/products/nessus-vulnerability-scanner# [Accessed 1 May 2017].

Netsparker.com. (2017). Windows Based Netsparker Website Vulnerability Scanner. [online] Available at: https://www.netsparker.com/web-vulnerability-scanner/ [Accessed 1 May 2017].

Sqlmap.org. (2017). sqlmap: automatic SQL injection and database takeover tool. [online] Available at: http://sqlmap.org/ [Accessed 1 May 2017].

Anon, (2017). [online] Available at: https://www.coresecurity.com/core-impact [Accessed 1 May 2017].

Owasp.org. (2017). OWASP. [online] Available at: https://www.owasp.org/index.php/Main_Page [Accessed 1 May 2017].

Saas.hpe.com. (2017). Software Solutions Designed to Scale | HPE Software. [online] Available at: https://saas.hpe.com/es-es/home [Accessed 1 May 2017].

Www-03.ibm.com. (2017). IBM - Productos - IBM Security AppScan. [online] Available at: http://www-03.ibm.com/software/products/es/appscan [Accessed 1 May 2017].

Acunetix. (2017). Website security - keep in check with Acunetix. [online] Available at: https://www.acunetix.com/ [Accessed 1 May 2017].

Rapid7. (2017). Accelerate Security, Vuln Management, Compliance | Rapid7. [online] Available at: https://www.rapid7.com/ [Accessed 1 May 2017].

CS, R. (2017). Retina CS Network Vulnerability Assessment Software - BeyondTrust. [online] BeyondTrust. Available at: https://www.beyondtrust.com/products/retina-cs/ [Accessed 1 May 2017].

Wireshark.org. (2017). Wireshark · Go Deep. [online] Available at: https://www.wireshark.org/ [Accessed 1 May 2017].

Snort.org. (2017). Snort - Network Intrusion Detection & Prevention System. [online] Available at: https://www.snort.org/ [Accessed 1 May 2017].

Mcafee.com. (2017). Productos de seguridad | McAfee. [online] Available at: https://www.mcafee.com/es/products.aspx [Accessed 1 May 2017].

Admin. (17 de Agosto de 2018). La Seguridad de la Información en las Universidades en Colombia. Bogotá D. C.: Marrugo Rivera & Asociados. https://www.marrugorivera.com/blog/2018/02/01/la-seguridad-de-la-informacion-en-las-universidades-en-colombia/.