INGENIUM ET POTENTIA
Revista Electrónica Multidisciplinaria de Ciencias Básicas, Ingeniería y Arquitectura
Año V. Vol V. N°1. Edición Especial 2023
Hecho el depósito de Ley: FA2019000052
FUNDACIÓN KOINONIA (F.K).
Santa Ana de Coro, Venezuela.

https://doi.org/10.35381/i.p.v5i1.2640

Vulnerabilidades y amenazas de la red en una unidad educativa

Network vulnerabilities and threats in an educational unit

Jorge Andrés Silva-Terán
pi.jorgeast38@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0002-7691-9959

Ariel José Romero-Fernández
ua.arielromero@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0002-1464-2587

Ana Lucia Sandoval-Pillajo
ui.anasandoval@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ibarra, Imbabura
Ecuador
https://orcid.org/0000-0003-1463-017X

Jorge Lenin Acosta-Espinoza
ui.jorgeacosta@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ibarra, Imbabura
Ecuador
https://orcid.org/0000-0003-4254-4228

Recibido: 15 de enero 2023
Revisado: 20 marzo 2023
Aprobado: 15 de abril 2023
Publicado: 01 de mayo 2023

INGENIUM ET POTENTIA
Revista Electrónica Multidisciplinaria de Ciencias Básicas, Ingeniería y Arquitectura
Año V. Vol V. N°1. Edición Especial 2023
Hecho el depósito de Ley: FA2019000052
FUNDACIÓN KOINONIA (F.K).
Santa Ana de Coro, Venezuela.

Jorge Andrés Silva-Terán; Ariel José Romero-Fernández; Ana Lucia Sandoval-Pillajo;
Jorge Lenin Acosta-Espinoza

RESUMEN

El objetivo principal fue la determinación de procedimientos que identifiquen vulnerabilidades y amenazas de la red en la institución. Según la finalidad, la investigación fue deductiva porque justificó el problema que es la inseguridad la red de la Unidad Educativa, enfocada en la identificación de vulnerabilidades y amenazas como una deducción de la existencia. Con la herramienta Power BI se efectuó informes obteniendo como resultado que el grado de vulnerabilidad que tiene la red de datos en las estaciones de trabajo que la componen es nivel medio, esto fue producto de software obsoleto o desactualizado; para que se impida la contaminación de los ordenadores con virus, troyanos, que generan intrusiones. En conclusión, con las medidas tomadas; se tiene la información académica de los estudiantes que reposa en la Unidad Educativa, estando protegida y es entregada a tiempo oportuno, sin novedades para el uso requerido, mediante solicitud y trámite personal.

Descriptores: Procedimiento de evaluación; herramienta; red de informática; unidad de información; ordenador. (Tesauro UNESCO).

ABSTRACT

The main objective was the determination of procedures that identify vulnerabilities and threats of the network in the institution. According to the purpose, the investigation was deductive because it justified the problem that is the insecurity of the network of the Educational Unit, focused on the identification of vulnerabilities and threats as a deduction of existence. With the Power BI tool, reports were made, obtaining as a result that the degree of vulnerability that the data network has in the workstations that compose it is medium level, this was a product of obsolete or outdated software; to prevent the contamination of computers with viruses, Trojans, which generate intrusions. In conclusion, with the measures taken; there is the academic information of the students that rests in the Educational Unit, being protected and delivered in a timely manner, without news for the required use, by request and personal process.

Descriptors: Evaluation procedure; tool; computer network; information unit; computer. (UNESCO thesaurus).

INTRODUCCIÓN

El presente artículo muestra resultados del proyecto que se desarrolló para tener una red segura, libre de piratas informáticos y mantener la información que posee la institución resguardada para que no tengan acceso personas no autorizadas. Se conoce que las tecnologías de la información y comunicación han ido evolucionando; esto ha causado que existan nuevos riesgos en la tecnología que si no se los detecta y depura pueden tener efectos en contra de la seguridad (Santiso , Koller, & Bisaro, 2016).

El desarrollo web ha facilitado las supuestas vulnerabilidades específicas de cualquier producto de tecnología. La cantidad de ataques va aumentando a diario; muchos se basan en amenazas, antes que tener causas como errores de configuración, errores de software, la inexperiencia del desarrollador, la falta de especialistas en seguridad de la información y falta de información sobre la seguridad de la información. (Bernardo, 2015)

En la práctica, han existido casos en que el programador web considera que el código solo puede ser conocido por personas escogidas, y él no da la atención necesaria a su seguridad, así las vulnerabilidades salen a flote; ha pasado en algunos sistemas de información grandes e importantes. Hay ocasiones en que ellos no conocen sobre estas vulnerabilidades y mientras no ocurra nada siguen con su aplicación. (Pîrnău, 2015).

Los piratas informáticos utilizan cada vez más el encubrimiento técnico, inventan códigos difíciles con complejidad de análisis. La solución del antivirus de contrarrestar el código de malware es demorosa y complicada según el tipo, así los hackers tienen mayor cantidad de tiempo para robar más dinero a los afectados. Los procedimientos utilizados para infectar a un dispositivo móvil han aumentado, así como la expansión de programas de malware por medio de tiendas en línea; los robots priorizan el envío de mensajes de texto con malware a contactos de la víctima. (Iovan & Ramona, 2018). Es muy importante la protección de datos y privacidad como herramienta primordial en la defensa de los individuos y sus relaciones con las empresas: Amazon, Apple, Facebook, Google y

Microsoft; que han evolucionado y alcanzado una expansión y un poder realmente desmedido creando monopolios (Morte, 2017).

La evolución del desarrollo de software, los inventos y las publicaciones desmedidas, generan la aparición de aplicaciones nuevas en las tiendas, generando el rompimiento de la información y el problema para descubrir aplicaciones necesarias, por lo que es prudente que los programadores desarrollen las apps o módulos requeridos. Existe la falta de profesionales idóneos, lo que crea que el contenido venga de una fuente dudosa (Martínez, Martínez, Mud-Castelló, Mud-Castelló, & Moreno, 2015).

Se ha demostrado que la utilidad de las pruebas de inteligencia y valoraciones de vulnerabilidades no son tan eficientes, hay que seguir con el avance de la tecnología y las herramientas para detección y su funcionalidad evolucionan; los usuarios tomarán en cuenta la importancia, previniendo que los sistemas sean más complicados en las tecnologías de la información. (Mckinnel, Dargahi, Dehghantanha, & Choo, 2019)

Las vulnerabilidades y ataques encontrados en la red se establecen por medio de observación directa, estudios de evaluaciones con herramientas de búsqueda de tráfico de red, de envío y recepción de paquetes, y encuestas a usuarios que se encuentran en la red. Se prosigue con el bajo nivel de preparación en seguridad de la información y errores sin control, intrusiones y ataques; culminando con el diseño de un programa que detecte problemas para resolver las amenazas existentes (Vega & Ramos, 2017).

La gestión de riesgos en la actualidad se ha convertido en un elemento vital para todo, por lo que ahora las actividades que se realicen tienen que estar bajo control. Dependiendo de los objetivos estratégicos, la ventaja competitiva en el mercado, las regulaciones o restricciones de cumplimiento, las empresas de Tecnología de información o los departamentos tecnológicos pueden ser certificados en cuanto a estándares de sistemas de gestión con normas ISO (Barafort, Mesquida , & Mas, 2016).

La utilización de normas ISO como la 27001-2015 del Sistema de Gestión de la Seguridad de la información son una ventaja competitiva y ayudan con el buen manejo de la información basados en sus ejes principales como la confidencialidad, integridad y disponibilidad de la información.

La ingeniería social es ahora una vulnerabilidad existente, debido a que, mediante engaños a las personas; los atacantes que, generalmente están encubiertos y con perfiles falsos, encuentran y reciben información suministrada por redes sociales con la finalidad de realizar delitos informáticos, causados por exceso de confianza por parte de las víctimas. La Unidad Educativa “Gonzalo Zaldumbide” es una institución fiscal, la cual posee una red que se encuentra vulnerable, sin un firewall externo disponible; lo que dificulta la restricción desde y hacia algunos sitios no permitidos e inseguros y genera un riesgo para los usuarios. También se encontró algunos dispositivos que son miembros de la red con antivirus, anti-spyware, filtro anti-spam, anti-malware sin instalar y desactualizados.

Se definió que el acceso a la red de la Unidad Educativa “Gonzalo Zaldumbide” por personas no autorizadas es identificado; y solventan las dudas por el desconocimiento de políticas de seguridad, para que no generen inseguridad de los docentes y personal administrativo al ingresar en la red institucional. La seguridad de la red se convierte en una necesidad en la Unidad Educativa “Gonzalo Zaldumbide” como los puertos abiertos, el acceso de personal no autorizado y el desinterés existente por revisar habitualmente las estaciones de trabajo de la red, han permitido buscar soluciones; porque trata de no poner en riesgo la integridad de la información y estabilidad de los sistemas que son utilizados por los miembros que laboran en la misma para determinar procedimientos que identifiquen vulnerabilidades y amenazas de la red en la institución.

En el laboratorio de la red de la unidad cada año se realizan las pruebas de Ser Bachiller, donde la mayoría de las estaciones de trabajo no se encuentran en óptimas condiciones;

tienen virus y malware que dificultan la extracción de datos realizada con dispositivos externos, resultando infectados y con la posibilidad de expandirse en todo este espacio.

En la investigación se diagnosticó la vulnerabilidad de la infraestructura de telecomunicaciones de la facultad de Ingeniería Industrial de la Universidad de Guayaquil, y se describe el conocimiento de las vulnerabilidades en la seguridad, donde se pueden obtener mejoras en los servicios ofertados, fortificar la seguridad de la red y evitar el acceso de personas que no tengan permisos.

Usando Kali Linux se facilita la inspección por el alcance de sus herramientas para análisis de la red, al hacer correr este programa se puede identificar las amenazas existentes (González, y otros, 2018). Existen herramientas para mapeo y revisión de puertos como Network Mapper (Nmap), Deepmagic Information Gathering Tool (Dmitry) y (Zmap); con Nmap se pueden analizar múltiples puertos y detectar vulnerabilidades con los diferentes scripts que al actualizar se obtiene, con Dmitry se puede obtener la información sobre un host objetivo y hasta reportes de su tiempo de funcionamiento o para realizar un escaneo de puertos TCP; con Zmap se pueden analizar de forma sistemática todas las direcciones IP versión 4 que se encuentran valederas en la web. (Paluch & Wünderlich, 2016)

En la parte de sniffer existen herramientas como Wireshark que es para capturar el tráfico de la red y análisis, tiene interfaz gráfica integrada y los resultados se los puede exportar en algunos formatos; otra herramienta es TCPdump que es un analizador de paquetes en el nivel de línea de comando. Para la detección de vulnerabilidades y la topología de la red se tiene herramientas como Open Vulnerability Assessment System (openVAS) que es un framework con la finalidad de escanear las vulnerabilidades de la red y su base de datos está actualizada regularmente en Network Vulnerability Tests (NVT), con más de 50000 tipos de vulnerabilidades; además de la consola tiene su interfaz gráfica Greenbone para facilidad de uso y mejor entendimiento de los reportes; otra herramienta

que se tiene es Nessus que es un escáner de redes que detecta posibles vulnerabilidades que se basan en una lista de fallas conocidas; las dos son gratuitas y de código abierto. (Revay, 2019)

MÉTODO

Según la finalidad, la investigación fue deductiva porque justificó el problema que es la inseguridad la red de la Unidad Educativa, enfocada en la identificación de vulnerabilidades y amenazas como una deducción de la existencia, para buscar la resolución de esta problemática usando los resultados para mitigar la vulnerabilidad de la red. La encuesta generada se la realizó a los 36 docentes que laboran en la institución para determinar el grado de inseguridad que tienen los docentes al ingresar a la red de la institución y no se aplicó un muestreo ni un método muestral porque el universo es menor a 100; ellos usan con frecuencia los dispositivos conectados a la red, donde tres de los encuestados cumplen con las actividades del área administrativa, y la entrevista directa que se hizo al Licenciado Jorge Chapi, rector de la Unidad; estas técnicas fueron utilizadas para la recopilación de la información.

La herramienta para la encuesta fue un cuestionario con preguntas que ayudaron a conocer la frecuencia y uso de los ordenadores, la existencia de problemas que hayan tenido con el ingreso a la red y las restricciones de acceso a sitios con riesgos. Según el alcance la investigación que se realizó fue descriptiva porque caracteriza la existencia de una problemática que es la inseguridad la red de la institución y existe la necesidad de evitar que piratas informáticos puedan acceder y robar la información usando pruebas de penetración en ambientes virtuales.

RESULTADOS

En la investigación se buscó la mejor alternativa para determinar las vulnerabilidades de la red de la institución; usando una máquina virtual de Oracle Virtual Box Versión 6.0.8 r130520 donde se instaló Kali-Linux 4.19.0 por ser usada para auditoría y seguridad informática, y por tener más de 600 programas preinstalados; se ha tomado en cuenta a las herramientas Nmap para el escaneo de puertos y vulnerabilidades, Open VAS para la detección de vulnerabilidades y Wireshark para la revisión de tráfico de red; porque son utilizables en los distintos sistemas operativos (Windows, Linux, IOS, Android), y son de código abierto y gratuitas. (Narayan & Mehtre, 2015) dicen que existen muchas herramientas de código abierto, de alta calidad para evaluación de vulnerabilidades y herramientas de prueba de penetración disponibles en el mercado con su propia experiencia y limitación y realizan una tabla para su elección en una de sus publicaciones.

Herramientas para la revisión de puertos

Entre las herramientas para mapeo y revisión de puertos se revisó tres con licencia free que son: Nmap Versión 7.70, que permitió ver los equipos que se encontraron activos en la red, los puertos abiertos vulnerables para realizar ataques y las aplicaciones ejecutadas; además ayudó a encontrar vulnerabilidades explotables en con los scripts asociados a la herramienta con ingresos ocultos a otras estaciones de trabajo; Zmap posee características parecidas para escaneo de un puerto, utiliza grupos multiplicativos cíclicos, lo que permite el escaneo del mismo espacio más rápido que Nmap; con DMitry se puede recopilar mayor cantidad de información posible sobre un host, reunir posibles subdominios, escaneo del puerto TCP, direcciones de correo electrónico, información sobre el tiempo de actividad, y búsquedas de IP con whois.

Tabla 1.
Análisis de las herramientas de test o escaneo.

N°	Nombre de la herramienta	Tipo de licencia	Escaneo	Modo Grafico
1	Nmap	Libre	Multipuerto	Zenmap
2	Zmap	Libre	Un Puerto	No posee
3	Dmitry	Libre	TCP	Si

Fuente: Los autores.

Para la decisión de uso de la herramienta Nmap en escaneo de puertos se analizó la Tabla 1. y se comparó con Zmap y Dmitry tomando en consideración los parámetros tipo de licencia, escaneo y modo gráfico; las tres herramientas son de software libre y la licencia es gratuita, se especifica que Dmitry y Nmap poseen modo gráfico para mejor visualización, así mismo en escaneo Nmap tiene la opción de realizar por multipuerto por lo que se puede ocultar el ingreso a otras estaciones de trabajo, y en las otras pueden ser descubiertos.

Herramientas para la verificación del tráfico de red

Entre las herramientas de verificación de tráfico de red se revisaron 2, la primera es Wireshark versión 2.6.6 que es muy reconocida por ser un analizador de protocolos en tiempo real y con modo gráfico, con ella se realizó un monitoreo de paquetes enviados y recibidos, mediante un filtro se especificó los hosts que tenían problemas en la transmisión y se realizó una prueba de intrusión, en la cual se observó el puerto por donde se ingresó denominado puerta trasera, también posee un modo consola para su revisión que no es muy detallada; la segunda es TCPDump en la que se hizo un análisis mediante

comandos y sin poder observar gráficamente el tráfico, también el fue revisado en tiempo real con menor entendimiento, también se utiliza esta herramienta para rastrear problemas y actividades de la red y tiene una versión para Windows conocida como WinDump que posee iguales características como el modo consola con lenguaje de código del Sistema Operativo.

Tabla 2.
Análisis de las herramientas de tráfico de red.

N°	Nombre de la herramienta	Tipo de licencia	Librería	Modo Grafico
1	Wireshark	Libre	Libpcap	Incluido
2	TCPDump	Libre	Libpcap	No

Fuente: Los autores.

Para la decisión de uso de la herramienta WireShark en revisión de transferencia de paquetes se analizó en la Tabla 3 teniendo en consideración los parámetros tipo de licencia, librerías y modo gráfico; con características iguales, pero WireShark posee su interfaz gráfica y TCPDump es un analizador de paquetes en el nivel de línea de comando.

Herramientas para la búsqueda de vulnerabilidades

Entre las herramientas para la búsqueda de vulnerabilidadesse hizo la revisión de 2 que son: OpenVAS 9.0 con una interfaz web Greenbone Security Assistant versión 7.0.3, se trata de un framework que tiene como base servicios y herramientas para la evaluación de vulnerabilidades y puede utilizarse de forma individual o como parte del conjunto de

herramientas de seguridad, también puede utilizarse desde Metasploit, el framework para la explotación de vulnerabilidades, el gestor es el servicio que lleva a cabo tareas como el filtrado o clasificación de los resultados del análisis, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios, incluyendo grupos y roles.

El proyecto OpenVAS mantiene una colección de NVT (OpenVAS NVT Feed) que crece constantemente y que actualiza los registros semanalmente. Los equipos instalados con OpenVAS se sincronizan con los servidores para actualizar las pruebas de vulnerabilidades y Nessus es una herramienta de seguridad de código abierto basado en plugins, tiene una interfaz basada en la biblioteca de componentes gráficos GIMP Toolkit (GTK), y realiza más de 1200 pruebas de seguridad remotas en su versión pagada; en la versión gratuita se pudo realizar un test a 16 estaciones de trabajo por una sola ocasión en la misma red.

Tabla 3.
Análisis de las herramientas de búsqueda de vulnerabilidades.

N°	Nombre de la herramienta	Tipo de licencia	Modo Grafico
1	OpenVAS	Libre	Greenbone
2	Nessus	Libre / pagada	Incluído

Fuente: Los autores.

Para la decisión de uso de la herramienta OpenVAS en análisis de vulnerabilidades se analizó la Tabla 4. y se comparó con Nessus teniendo en cuenta los parámetros tipo de licencia y modo gráfico; donde OpenVas fue designada porque es gratuita y Nessus tiene su versión free para una revisión de máximo 16 hosts y de solo una red y no tiene activadas todas sus características.

Herramientas de análisis e inteligencia de negocio

Entre las herramientas de bussiness intelligence se tiene a Power BI es un servicio de análisis de negocios de Microsoft que tiene gran afinidad con sus productos, es pagada y con el directorio activo y los correos institucionales otorgados por el Ministerio de Educación se la utiliza con esa licencia; con su uso se proporcionó visualizaciones interactivas y capacidades de inteligencia empresarial con una interfaz entendible para todo el personal administrativo de la institución; Tableau es otra de las herramientas de Business Intelligence que, también tiene buenas características, pero al ser pagada y como las instituciones fiscales no poseen recursos ha sido descartado en el uso de este proyecto.

Método de Deming

A continuación, se aplicó el método de Deming Plan-Do-Check-Act (PDCA o PHVA) para encontrar las vulnerabilidades y mitigarlas; este ciclo repetitivo está basado en la norma ISO/IEC 27001 y consta de 4 fases que son:

Fase 1: Plan (Planificar): En esta fase se realiza la topología de la red, colocando los hosts con sus respectivas direcciones IP.

Fase 2: Do (Hacer): En esta fase se escanean puertos abiertos y sus servicios, sistemas operativos, firewall, el tráfico de red diario, por cada host y se hace la constatación de que todos los equipos que se definieron en la fase 1 se encuentren en la red.
Fase 3: Check (verificar): En esta fase se realiza la detección y evaluación de vulnerabilidades y la verificación de la topología de la red expuesta.
Fase 4: Act (actuar): En esta fase se realiza un informe del análisis efectuado para poder mitigar las vulnerabilidades.

DISCUSIÓN

De los dispositivos que tenían uno o varios puertos abiertos se tenía que el 68,75% tenían esta vulnerabilidad; el cambio que se ha producido es la revisión de puertos que se pueden quedar abiertos sin que tengan ningún problema y los que solo se requiera para accesos predeterminados se abren cuando sea necesario y así mismo se cierran cuando ya se haya ejecutado el proceso o transferencia. Se mejoró la seguridad de la red con revisiones periódicas y mitigando las vulnerabilidades, antes del proyecto los ordenadores y programas que se encuentran instalados no se encontraban actualizados, había un 25% de estaciones de trabajo en donde el Sistema Operativo se encontraba sin el parche de seguridad lo que generaba que los datos e información pueda ser interceptada.
Otra de las mejorías con el proyecto es la instalación de un firewall a todos los hosts para protección contra el acceso a sitios web no permitidos, y las posibles intrusiones de hackers, el porcentaje de hosts sin instalarlo estaba en un 81,25%; y en la nueva medición tiene un 0%. Las vulnerabilidades siempre van a existir, por lo tanto, se debe realizar una revisión periódica de los ordenadores.

CONCLUSIONES

Las vulnerabilidades con esta identificación y análisis se han podido mitigar con la actualización de Sistemas Operativos y software, cierre de puertos, uso de antivirus, instalación de antimalware y revisión periódica de los dispositivos conectados a la red.

Con la herramienta Power BI se efectuó informes obteniendo como resultado que el grado de vulnerabilidad que tiene la red de datos en las estaciones de trabajo que la componen es nivel medio, esto fue producto de software obsoleto o desactualizado; para que se impida la contaminación de los ordenadores con virus, troyanos, que generan intrusiones.

El beneficiario directo es toda la Comunidad Educativa, porque se ofrece seguridades en la red para el uso del personal Administrativo, Docentes, Estudiantes y Padres de Familia; así no serán víctimas de intrusiones y robo de información.

Docentes, Estudiantes y Padres de Familia pueden navegar con resguardo por las redes sociales, así como el envío y recepción de correos; porque la solución presentada evita técnicas de hackeo como pishing, pharming y punycode; estableciendo medidas que permitan disminuir el porcentaje del riesgo. Con los resultados obtenidos y las medidas tomadas; la información académica de los estudiantes que reposa en la Unidad Educativa “Gonzalo Zaldumbide” está protegida y es entregada a tiempo, sin novedades para el uso requerido, mediante solicitud y trámite personal.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A los docentes, trabajadores y estudiantes de La Unidad Educativa “Gonzalo Zaldumbide”. Ecuador.

REFERENCIAS CONSULTADAS

Barafort, B., Mesquida , A., & Mas, A. (2016). Integrating Risk Management in IT settings from ISO Standards and Management Systems Perspectives. *Computer Standards & Interfaces*, 38-64. doi:http://dx.doi.org/10.1016/j.csi.2016.11.010

Bernardo, D. (2015). Clear and present danger: Interventive and retaliatory approaches to cyber threats. *Applied Computing and Informatics, 11*(2), 144-157. doi:https://doi.org/10.1016/j.aci.2014.11.002

Gonzalez, G., Dubus, S., Motzek, A., García, J., Alvarez, E., Merialdo, M., . . . Debar, H. (2018). Dynamic risk management response system to handle cyber threats. *Future Generation Computer Systems, 83*, 535-552. https://n9.cl/sh24a

Iovan, S., & Ramona, M. (2018). MALWARE FOR MOBILE DEVICES AND THEIR SECURITY. *Fiabilitate şi Durabilitate*, 267-272. https://n9.cl/pf0crg

Martinez, J., Martinez, O., Mud-Castelló, S., Mud-Castelló, F., & Moreno, L. (2015). Análisis de la calidad y seguridad de la información de aplicaciones móviles en prevención terciaria. [Analysis of the quality and security of the information of mobile applications in tertiary prevention]. *Farmaceúticos Comunitarios, 7*(4), 23-27. https://n9.cl/04nz3v

Mckinnel, T., Dargahi, T., Dehghantanha, A., & Choo, K.-K. (2019). A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. Computers and Electrical Engineering, 75, 175-188. https://n9.cl/xedj9

Morte, R. (2017). ¿Protección de datos/privacidad en la época del Big Data, IoT, wearables…? Sí, más que nunca. [Data protection/privacy in the era of Big Data, IoT, wearables…? yes more than ever]. *Dilemata*, 219-233. https://n9.cl/6sdrm

Narayan, J., & Mehtre, B. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science 5, 57*, 710-715. https://n9.cl/95p7t

Paluch, S., & Wünderlich, N. (2016). Contrasting risk perceptions of technology-based service innovations in inter-organizational settings. *Journal of business research*, 2424-2431. https://n9.cl/qjk23

Pîrnău, M. (2015). General Aspects of some Causes of Web Application Vulnerabilities. Memoirs of the Scientific Sections of the Romanian Academy, 55-66. https://n9.cl/ffniy

Revay, L. (2019). From Malware Testing to Virtualization. Procedia Computer Science, 150, 751-756. https://n9.cl/pf0crg

Santiso , H., Koller, J. M., & Bisaro, M. (2016). Seguridad en entornos de educación virtual. *Memoria Investigaciones en Ingeniería, 14*, 67-88. https://n9.cl/6cqfz

Vega, G., & Ramos, R. (2017). Vulnerabilidades y amenazas a los servicios web de la intranet de la Universidad Técnica de Babahoyo. [Vulnerabilities and threats to the web services of the intranet of the Technical University of Babahoyo]. *3c Tecnología, 6*, 53-66. https://n9.cl/89ak2