tecnología

Glosas de innovación aplicadas a la pyme

Edición 21

Vol. 6 N° 1 (2017)

Marzo - junio '17

ISSN: 2254 - 4143

Publicación trimestral

Depósito legal: A299-2012 Área de Innovación y Desarrollo, S.L

INDIZADO POR/ INDEXED BY

PLATAFORMA DE EVALUACIÓN DE REVISTAS

BASES DE DATOS INTERNACIONALES SELECTIVAS

DIRECTORIOS SELECTIVOS

HEMEROTECAS SELECTIVAS

BUSCADORES DE LITERATURA CIENTÍFICA EN ACCESO ABIERTO

OBJETIVO EDITORIAL

La Editorial científica 3Ciencias pretende transmitir a la sociedad ideas y proyectos innovadores, plasmados, o bien en artículos originales sometidos a revisión por expertos, o bien en los libros publicados con la más alta calidad científica y técnica.

NUESTRO PÚBLICO

- Personal investigador.
- Doctorandos.
- Profesores de universidad.
- Oficinas de transferencia de resultados de investigación (OTRI).
- Empresas que desarrollan labor investigadora y quieran publicar alguno de sus estudios.

COBERTURA TEMÁTICA

La Revista 3C Tecnología es una revista de carácter científico-social donde se difunden trabajos originales de investigación que abarcan diferentes temáticas relacionadas con la ingeniería y la tecnología.

INFORMACIÓN PARA AUTORES

Toda la información sobre el envío de originales se puede encontrar en el siguiente enlace:

<http://www.3ciencias.com/normas-de-publicacion/instrucciones-para-el-envio-de-articulos/>.

<p><i>3C Tecnología: Glosas de innovación aplicadas a la pyme</i></p> <p><i>Edición nº 21</i> <i>Volumen 6 número 1 (Marzo – junio '17)</i> DOI: http://dx.doi.org/10.17993/3ctecno.2017.v6n1e21</p> <p><u>Periodicidad trimestral</u> <i>Tirada nacional e internacional</i> <i>Artículos revisados por el método de evaluación por pares de doble ciego.</i> ISSN: 2254 - 4143 Nº de Depósito Legal: A 299 - 2012</p>	<p>Editorial: <i>Área de Innovación y Desarrollo, S.L.</i> Empresa de transferencia del conocimiento al sector empresarial.</p> <p>C/ Els Alzamora, 17 Alcoy, Alicante (España) Tel: 965030572</p> <p>E-mail editor: info@3ciencias.com</p> <p>Copyright © Área de Innovación y Desarrollo, S.L.</p>
---	--	--

PUBLISHING GOAL

3Cienicias wants to transmit to society innovative projects and ideas. This goal is reached through the publication of original articles which are subjected to peer review or through the publication of scientific books.

OUR PUBLIC

- Research staff.
- PhD students.
- Professors.
- Research Results Transfer Office.
- Companies that develop research and want to publish some of their works.

THEMATIC COVERAGE

3C Tecnología journal is a scientific-social journal, where original works are disseminated. These works cover different themes related to engineering and technology.

INSTRUCTIONS FOR AUTHORS

All information about sending originals can be found at the following link:
<http://www.3ciencias.com/normas-de-publicacion/instrucciones-para-el-envio-de-articulos/>

SUMARIO**INSTALACIONES SOLARES FOTOVOLTAICAS DE AUTOCONSUMO PARA PEQUEÑAS
INSTALACIONES. APLICACIÓN A UNA NAVE INDUSTRIAL 1**

*Self-consumption solar photovoltaic systems for small installations. industrial factory
application.....*

Paula Bastida Molina, Juan Ángel Saiz Jiménez, María Pilar Molina Palomares y
Bernardo Álvarez Valenzuela

**TRADUCTOR MÓVIL PARA ASISTENCIA MÉDICA A PACIENTES QUECHUA
HABLANTES 15**

Mobile translator for medical assistance for quechua speaking patients

Manuel Aveliono Lagos Barzola y Zuliana Villar Vila

¿POR QUÉ DESCONFIAR DE LOS DISPOSITIVOS DE ALMACENAMIENTO DIGITAL?... 35

Why you should not trust data storage devices?

Romel Vera Cadena

LA NECESIDAD Y LA OPORTUNIDAD DE LA INNOVACIÓN 47

The need and opportunity of innovation.....

Mónica García Cantó y Laura M^a Palacios Ruiz

**VULNERABILIDADES Y AMENAZAS A LOS SERVICIOS WEB DE LA INTRANET DE LA
UNIVERSIDAD TÉCNICA DE BABAHOYO 53**

Vulnerabilities and menaces to web services in intranet's technical university of babahoyo..

Geovanny Vega Villacís y Raúl Armando Ramos Morocho

tecnología

Recepción: 03 de enero de 2017

Aceptación: 23 de febrero de 2017

Publicación: 14 de marzo de 2017

INSTALACIONES SOLARES FOTOVOLTAICAS DE AUTOCONSUMO PARA PEQUEÑAS INSTALACIONES. APLICACIÓN A UNA NAVE INDUSTRIAL

SELF-CONSUMPTION SOLAR PHOTOVOLTAIC SYSTEMS FOR SMALL INSTALLATIONS. INDUSTRIAL FACTORY APPLICATION

Paula Bastida Molina¹

Juan Ángel Saiz Jiménez²

María Pilar Molina Palomares³

Bernardo Álvarez Valenzuela⁴

1. Graduada en Ingeniería Eléctrica. Universitat Politècnica de València. Departamento de Ingeniería Eléctrica. E-mail: paubasmo@etsid.upv.es
2. Profesor Universitat Politècnica de València. Departamento de Ingeniería Eléctrica. E-mail: jasaz@die.upv.es
3. Profesora Universitat Politècnica de València. Departamento de Ingeniería Eléctrica. E-mail: pimolina@die.upv.es
4. Profesor Universitat Politècnica de València. Departamento de Ingeniería Eléctrica. E-mail: balvarez@die.upv.es

Citación sugerida:

Bastida Molina, P., Saiz Jiménez, J.A., Molina Palomares, M.P. y Álvarez Valenzuela, B. (2017). Instalaciones solares fotovoltaicas de autoconsumo para pequeñas instalaciones. Aplicación a una nave industrial. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 6(1). 1-14. DOI: <http://dx.doi.org/10.17993/3ctecno.2017.v6n1e21.1-14/>.

RESUMEN

El autoconsumo fotovoltaico eléctrico permite producir energía eléctrica a partir de la radiación solar en el mismo lugar donde posteriormente se consumirá. La fuente de la que tomamos la energía es el sol, un recurso natural e ilimitado.

En los momentos en los que este tipo de alimentación no sea suficiente para cubrir los consumos eléctricos de las instalaciones receptoras, la diferencia se toma de la red eléctrica. Quedan así siempre cubiertas las necesidades eléctricas de los usuarios.

El uso de los sistemas de autoconsumo fotovoltaicos permite a los que los poseen reducir su facturación eléctrica, puesto que la energía autoproducida no se toma de la red eléctrica y no es, por tanto, facturada. Así, a partir del dinero que el usuario se ahorra de la facturación eléctrica, recupera el coste de la instalación en un plazo comprendido entre 5 y 10 años, dependiendo de la radiación solar y del lugar en el que está ubicada.

La legislación actual diferencia entre dos tipos de instalaciones fotovoltaicas para autoconsumo: mayores de 10 kW y menores de 10 kW. Resultan económicamente más rentables las instalaciones menores de 10 kW, puesto que las que tienen un valor mayor deben pagar por la energía autoconsumida.

Se analiza en este artículo el ejemplo de una instalación fotovoltaica para una nave industrial situada en Paiporta (Valencia-España) de 9,9 kW de potencia contratada.

ABSTRACT

Electrical self-consumption photovoltaic systems can produce electric power through the solar radiation in the same place where this energy will be consumed later. The electrical generation source is the sun, a natural and unlimited resource.

When this kind of generation is not enough to cover all the electrical consumption of the receiving installations, the difference is taken from the electrical grid. As a consequence, the needs of the customers are always covered.

The use of self-consumption photovoltaic systems allows their owners to reduce their electric billing, because self-produced power comes not from the electric grid, so it is not billed. Therefore, with the money that the customer can save from electric billing, the cost of the photovoltaic system is recovered in a period between 5 and 10 years, depending on the solar radiation and its location.

Current legislation distinguishes two self-consumption photovoltaic system types: higher than 10 kW and lower than 10 kW. Lower than 10 kW systems are economically more profitable, as in the other kind of photovoltaic system is compulsory to pay for the self-produced power.

An example of a photovoltaic system for an industrial factory placed in Paiporta (Valencia-Spain) with 9,9 kW of power is analyzed along this article.

PALABRAS CLAVE

Autoconsumo, Energía Solar, Fotovoltaica, Energías Renovables, Energía Eléctrica.

KEY WORDS

Self-consumption, Solar Power, Photovoltaic, Renewable Energies, Electric Power.

1. INTRODUCCIÓN

Las instalaciones solares fotovoltaicas de autoconsumo son aquellas que permiten al usuario generar su propia energía eléctrica. Es decir, el usuario produce la energía en el mismo lugar donde la consume, a partir de la radiación solar y de paneles fotovoltaicos. En los momentos en que el consumo eléctrico de la instalación es superior a la energía autoproducida por la instalación fotovoltaica, se toma la energía que falta de la red eléctrica [8].

Resultan un tipo de instalaciones muy interesantes: técnicamente porque se trata de una tecnología madura y suficientemente desarrollada, y económicamente porque el dinero que cuesta la instalación se recupera con facilidad en pocos años, a partir de la energía eléctrica ahorrada.

Desde un punto de vista técnico, se trata de instalaciones relativamente nuevas, aunque sus resultados han sido ampliamente contrastados a partir de instalaciones conectadas a la red en los últimos 15 años. Por ello, resultan instalaciones fiables y seguras, y además, tanto su dimensionado como su montaje son sencillos.

Desde un punto de vista económico, son instalaciones cuyo coste inicial se recupera en un plazo de tiempo razonable, de entre 5 y 10 años [4], dependiendo de la radiación solar y de la legislación. Cuanto mayor sea la radiación solar que incide sobre la instalación, más rápido se amortiza, este factor depende de la ubicación de la instalación. En cuanto a la legislación [2] [3], las instalaciones de menos de 10 kW son las que resultan a priori económicamente más rentables. Además, se permite también el uso de elementos de acumulación [9], que pueden utilizarse para recoger los excedentes que se produzcan, puesto que puede haber horas en las que la producción de la instalación fotovoltaica sea superior al consumo eléctrico que se esté produciendo.

Se analiza a lo largo de este artículo la implementación de una instalación solar fotovoltaica de autoconsumo para una nave industrial, situada en Paiporta (Valencia-España), cuya potencia contratada es de 9,9 kW. La radiación en Valencia, sin ser la más alta de España (es superior en zonas como Alicante o Murcia) es óptima para recuperar la inversión en la instalación fotovoltaica rápidamente. Además, la potencia contratada en la nave industrial va a permitir que esta tenga como máximo una potencia instalada fotovoltaica de 9,9 kW ya que la potencia instalada fotovoltaica no puede superar a la potencia contratada de la instalación receptora [2] [3]. Al ser una instalación fotovoltaica como máximo de 9,9 kW (inferior a 10 kW) optimizamos el tiempo para la recuperación de la inversión.

2. LEGISLACIÓN ACTUAL

El Real Decreto 2818/1998 fue el primero en España en realizar un tratamiento específico de las instalaciones solares fotovoltaicas conectadas a red. Dos años después, se publicó el Real Decreto 1663/2000, que supuso el inicio del despegue de la energía solar fotovoltaica en España.

Fueron finalmente los Reales Decretos 436/2004 y 661/2007 los que impulsaron el desarrollo de centrales solares fotovoltaicas conectadas a red en España, creando una prima por cada kWh producido.

A partir de 2008, con el Real Decreto 1578/2008 se limitó la cantidad de potencia fotovoltaica instalable anual. En 2011 se reguló inicialmente el régimen de autoconsumo, aunque con la publicación del Real Decreto 1/2012 se frenó la posibilidad de realizar instalaciones fotovoltaicas en España.

La legislación actual de las instalaciones solares fotovoltaicas para autoconsumo está regida por el Real Decreto 900/2015, aprobado el 9 de octubre de 2015. Este Real Decreto regula las condiciones administrativas, técnicas y económicas de las modalidades de suministro de energía eléctrica con autoconsumo y de producción con autoconsumo [2] [3].

Dicho Real Decreto establece dos tipos de autoconsumidores. La diferencia fundamental entre ambos tipos es que el consumidor de tipo 2 es un productor de energía eléctrica, mientras que el consumidor de tipo 1 no. El proceso necesario para darse de alta como instalación de producción eléctrica (consumidor de tipo 2) es un trámite complejo. Se encuentra aquí el primer factor legislativo que favorece las instalaciones de autoconsumo de pequeña potencia (tipo 1).

Dichas instalaciones cumplirán las siguientes características:

- La potencia instalada fotovoltaica no podrá superar nunca a la potencia contratada de la instalación receptora.
- Será necesario pagar un peaje por la potencia autoconsumida. Sin embargo, las instalaciones de hasta 10 kW de potencia instalada fotovoltaica estarán exentas de pagar este peaje. Este es otro de los factores legislativos que favorece las instalaciones de autoconsumo para instalaciones pequeñas.
- Los excesos de generación no serán remunerados. Es recomendable, por tanto, instalar un sistema de inyección 0, que evite que la energía autoproducida sea superior a la consumida [1].
- Es obligatorio instalar un contador homologado que mida la energía autoproducida.

El Real Decreto 900/2015 modifica el publicado en 2011 sobre autoconsumo, imponiendo peajes por la producción en régimen de autoconsumo, y poniendo impedimentos al balance neto. El balance neto consiste en permitir que los excedentes que se pudieran tener en una instalación fotovoltaica en las horas del día en las que se produce más de lo que se consume pudieran descontarse de la energía tomada de la red en las horas en las que se produce en la instalación fotovoltaica menos de lo que se consume.

Para la nave industrial analizada, la potencia instalada máxima podría ser de 9,9 kW, porque esta es su potencia contratada. Debido a ello estará exenta de pagar el peaje por la energía autoproducida (<10 kW). Además, dispondrá de un sistema de inyección 0 y de un contador de medida de la energía autoproducida.

3. CURVAS DE CONSUMO Y PRODUCCIÓN DIARIAS

El dimensionado de la instalación fotovoltaica va a depender del consumo de la instalación receptora y de la producción de la instalación fotovoltaica. Mediante la energía fotovoltaica generada se va a cubrir la mayor parte posible del consumo eléctrico, intentando que los excedentes fotovoltaicos no sean muy elevados [8], puesto que se van a perder y, por tanto, no van a contribuir a recuperar la inversión realizada.

Tanto la evolución del consumo eléctrico de la instalación receptora como la evolución de la producción de la instalación fotovoltaica se van a obtener de forma diaria, es decir, a partir de las curvas de consumo y producción diarias, estudiadas a lo largo de un año [4].

Para la obtención de las curvas de consumo diarias se eligen varios días tipo para cada mes del año. En cada uno de esos días tipo, se estudia como varía el consumo eléctrico de la nave industrial en períodos de quince en quince minutos. Para el caso de la nave industrial, los días tipo seleccionados serán días laborables, días no laborables y para los meses de verano también días de verano tipo [8], dado que en cada uno de ellos se producen condiciones de consumo diferentes.

Las curvas de producción diarias de la instalación solar fotovoltaica se obtienen a partir del producto de la radiación solar diaria y de la potencia instalada en las placas solares, representadas también en periodos de quince minutos, para cada uno de los meses del año. La radiación solar diaria se obtiene de la página web PVGIS, en la que tenemos la radiación diaria presentada respecto al horario internacional UTC. Para adaptar los horarios PVGIS al horario español se debe sumar una hora en los meses de invierno (enero, febrero, marzo, noviembre y diciembre) y dos horas en los meses de verano (abril, mayo, junio, julio, agosto, septiembre y octubre) [8].

Finalmente, para cada mes del año se superponen ambas curvas en una sola gráfica [4]. En el ejemplo estudiado de la nave industrial, se observa que hay periodos de tiempo en los que la producción supera al consumo, principalmente al mediodía, ya que en ese período de tiempo los trabajadores de la nave salen a comer, por lo que el consumo se reduce notablemente, y además, la producción aumenta porque la radiación solar en ese tiempo es mayor.

Como se ha dicho anteriormente, los excesos de generación fotovoltaicos no son económicamente remunerados [2] [3]. Por tanto, se va a instalar un sistema que evite los vertidos eléctricos a la red (sistema de inyección 0). La misión de este sistema de inyección 0 es regular el nivel de generación del inversor de la instalación fotovoltaica, en función del consumo del usuario, impidiendo la inyección de potencia a red cuando la energía generada

sea superior a la energía consumida. En esos momentos, desplaza el punto de funcionamiento del inversor, ajustándolo al nivel de consumo del usuario [1].

Utilizando el sistema de inyección 0, se observa que la energía fotovoltaica que se podría producir es superior a la que realmente se aprovecha [1]. Teniendo en cuenta esta consideración, observamos que va a resultar más rentable dimensionar la instalación fotovoltaica conforme a la energía realmente aprovechada y no conforme a la energía total que se podría producir. Así, la energía realmente aprovechada se obtiene multiplicando el valor de la energía total que se podría producir por el coeficiente de aprovechamiento. El valor de este coeficiente es el valor medio del cociente entre la energía generada real y la energía generada total para cada uno de los meses del año. En nuestro caso, el factor de aprovechamiento es de un 80% [4] [8]. El coeficiente se obtiene a partir del balance entre la energía que se podría producir y la que realmente se consume en cada uno de los meses del año.

En la figura 1 se muestran, como ejemplo, las curvas de producción y de consumo diarios para un día laborable del mes de abril. De la misma forma, se realizan estas curvas para cada uno de los meses del año, lo que nos permite obtener la energía que producimos y la que realmente autoconsumimos. La suma de las energías autoconsumidas en todos los meses del año nos proporciona la energía total ahorrada.

Figura 1: Curvas de consumo (roja) y producción (azul) diarias. Mes de abril.

Fuente: Elaboración propia.

4. ESQUEMA GENERAL

La instalación solar fotovoltaica para autoconsumo está conformada por placas solares fotovoltaicas y el inversor de conexión a red [4] [8].

Las placas solares fotovoltaicas son las encargadas de generar la energía eléctrica a partir de la radiación solar que incide sobre ellas. El número de placas necesario se calcula de acuerdo con lo explicado en el punto anterior, es decir, comparando el consumo de la nave con la producción de las placas, se coge el número de placas que nos haga perder la menor cantidad de energía posible.

El resultado que obtenemos es que necesitamos 20 placas de 255 W cada una (5,1 kW). La potencia de la instalación fotovoltaica será entonces de 5,1 kW, inferior a los 9,9 kW máximos que podías poner.

El inversor de conexión a red es el encargado de transformar la energía eléctrica que proporcionan las placas en corriente continua, en energía eléctrica en corriente alterna para la alimentación de los receptores de la nave industrial. La potencia de entrada del inversor debe coincidir con la potencia instalada en placas solares fotovoltaicas, que en este caso es de 5100 W.

Sin embargo, la instalación presentará unas pérdidas (caída de tensión en los cables, temperatura, punto de máxima potencia, etc.) de un 19%. Así, la potencia máxima que llegará al inversor serán los 5100 W menos estas pérdidas, por lo que el inversor deberá ser como mínimo de 4131 W. Se elige finalmente un inversor cuya potencia de entrada es de 4700 W.

El esquema de la instalación quedará tal como se puede ver en la figura 2.

Figura 2. Esquema general.
Fuente: Elaboración propia.

5. DISPOSICIÓN DE LAS PLACAS SOLARES FOTOVOLTAICAS

Es muy importante seleccionar una correcta disposición (lugar de ubicación, inclinación, orientación y distancia) de las placas solares fotovoltaicas para conseguir que la incidencia de la radiación solar sobre las mismas sea la mayor posible [8].

En cuanto al lugar de ubicación, se colocan preferentemente y si no hay ningún inconveniente técnico, en las cubiertas de las edificaciones puesto que son lugares desaprovechados, donde no suele haber nada construido. Además, al instalarse en lugares elevados se dificulta el robo de las mismas [10].

Por otro lado, el ángulo de inclinación de las placas se elige para que la radiación solar que incide sobre ellas sea la mayor posible de forma anual [10]. En nuestro caso y para Valencia, 30º respecto a la horizontal y con orientación sur [10].

Además, debe existir una distancia mínima entre cada una de las filas de placas y las siguientes, para evitar que cualquiera de las filas produzca sombra sobre las otras. Esa distancia mínima que debe existir entre filas es función de la altura relativa entre una fila y la siguiente (h) y la latitud del lugar donde está emplazada la instalación (k) [8] [10].

La nave industrial analizada presenta un tejado a dos aguas. Se decide instalar una estructura metálica de elevación sobre la cual se colocarán finalmente los soportes de placas. Esta estructura se instala para obtener una superficie plana horizontal, donde todos los soportes de las placas están a la misma altura

El ángulo de inclinación seleccionado para las placas de la nave industrial es de 30º, ángulo que permite obtener una mayor radiación solar anual (figura 3), en torno a 1550 horas/año efectivas. Además, las placas se orientan hacia el sur (figura 4).

Por último, teniendo en cuenta que la altura relativa es de 0,83 m y el factor k tiene un valor de 2,475 para la latitud correspondiente a España (39), la distancia mínima entre unas filas de placas debe ser 2,06 m. Finalmente, se decide dejar una distancia de 3 m entre cada una de ellas (figura 4), dado que tenemos suficiente espacio en la cubierta.

Figura 3. Ángulo de inclinación.

Fuente: Elaboración propia.

Figura 4. Distancia entre placas.

Fuente: Elaboración propia.

6. PRODUCCIÓN ELÉCTRICA Y RENTABILIDAD ECONÓMICA

Para instalaciones solares fotovoltaicas de autoconsumo, la producción teórica anual no coincide con la producción real anual [8].

La producción teórica anual se obtiene a partir del producto de la radiación solar total anual por la potencia instalada fotovoltaica. A partir de la página web PVGIS, ya citada, se obtienen las radiaciones solares para cada mes del año. La suma de estas radiaciones corresponde a la radiación solar anual, o las horas solares pico anuales (HSP) [4].

$$\text{Producción teórica anual (Wh/año)} = \text{HSP} \cdot \text{Potencia instalada (W}_{\text{pico}})$$

Sin embargo, se debe tener en cuenta que la instalación presenta una serie de pérdidas (por conexionado, por caídas de tensión, por polvo y suciedad, por temperatura...). Es difícil saber cuál es el valor de estas pérdidas puesto que las condiciones de funcionamiento son diferentes de unas instalaciones a otras y no hay posibilidad de establecer un criterio matemático único que recoja todas las circunstancias que se puedan producir. Sin embargo, a partir de la experiencia acumulada en el seguimiento de instalaciones fotovoltaicas conectadas a la red a lo largo de los últimos 15 años, hemos medido que las pérdidas obtenidas se sitúan por debajo del 19%. Por tanto, el rendimiento de la instalación que se ha utilizado en los cálculos es del 81%.

Además, el sistema de inyección 0 [1] regula el nivel de generación del inversor de la instalación fotovoltaica, en función del consumo del usuario, impidiendo la inyección de potencia a red cuando la energía generada es superior a la energía consumida. Por tanto, la energía generada real y aprovechada no es igual a la energía total que se podría generar.

Como se ha comentado anteriormente, la instalación se ha diseñado de forma que la energía real aprovechada corresponda aproximadamente al 80% de la energía total que se podría producir. Así, la producción real anual corresponde al producto de la producción teórica de la instalación por el rendimiento (81%) y por el coeficiente de aprovechamiento de la misma (80 %).

$$\begin{aligned} \text{Prod. real anual (kWh/año)} &= \\ &= \text{Prod. teórica anual (kWh/año)} \cdot \text{coef aprovechamiento} \cdot \eta \end{aligned}$$

Por otro lado, hay que tener en cuenta la disminución de aprovechamiento de la instalación debido a la pérdida de rendimiento de las placas con el tiempo. De forma lineal, se puede establecer que esa disminución es de aproximadamente un 0,5% por año. Así, la producción aprovechada real de la instalación del primer año se verá disminuida cada año.

$$\begin{aligned} \text{Coeficiente} &= (1 - 0.005 \cdot (\text{año} - 1)) \\ \text{Energía año } x &= \text{Energía primer año} \cdot (1 - 0.005 \cdot (\text{año} - 1)) \end{aligned}$$

La energía generada anualmente mediante la instalación fotovoltaica de autoconsumo se obtiene por tanto multiplicando la producción real anual por el coeficiente descrito en el párrafo anterior. Esta energía no tendrá que ser facturada por el usuario, ya que no la toma de la red eléctrica.

El dinero ahorrado anualmente se calcula multiplicando el precio del kWh por la energía producida y aprovechada real en la instalación fotovoltaica. El régimen tarifario de la nave industrial es 2.0 A, en el que el precio del kWh se mantiene constante, independientemente de la franja horaria del día en 0,1478 €/kWh, valor al que hay que añadir el impuesto de electricidad. Redondeando a la baja para situarnos en un valor más restrictivo, el coste energético utilizado para realizar los cálculos se toma de 0,15 €/kWh de forma constante [4][10].

A ese dinero, habrá que restarle el precio del seguro anual y el dinero reservado para mantenimiento de la instalación, también anual. La labor de mantenimiento de la instalación consiste en comprobar una vez al año el buen estado de la instalación y realizar la limpieza de los paneles. El precio del seguro, ya contratado en la nave antes de realizar la instalación fotovoltaica, se estima que tendrá un incremento de 50 €/año por incluir la instalación fotovoltaica. El dinero destinado a mantenimiento se estima en 150 €/año. En los cálculos realizados para los años sucesivos, se han mantenido estos valores constantes.

El coste total de la instalación solar fotovoltaica de autoconsumo objeto de estudio es de 6.402,77 €. De forma detallada, el coste de los paneles solares fotovoltaicos es de 2.906 €, el del inversor de conexión a red es de 1716,97€, el de la estructura soporte es de 1000 €, el del cableado y canalizaciones eléctricas es de 191,72 €, el de las protecciones eléctricas y puesta a tierra es de 348,08 € y el de la mano de obra es de 240 €.

Teniendo en cuenta el dinero que se ahorraría el usuario por la energía autoproducida, se obtiene que el período de amortización de la instalación se sitúa en menos de 8 años, tal y como se observa en la tabla 1 [4] [10].

RENTABILIDAD INSTALACIÓN SOLAR FOTOVOLTAICA PARA AUTOCONSUMO				
AÑO	COEFICIENTE	ENERGÍA ANUAL REAL PRODUCIDA Y APROVECHADA (kWh/año)	DINERO AHORRADO ANUAL (€)	DINERO AHORRADO ACUMULADO (€)
1	1	6.953,69	843,05	843,05
2	0,995	6.918,92	837,84	1.680,89
3	0,99	6.884,15	832,62	2.513,52
4	0,985	6.849,39	827,41	3.340,92
5	0,98	6.814,62	822,19	4.163,12
6	0,975	6.779,85	816,98	4.980,09
7	0,97	6.745,08	811,76	5.791,86
8	0,965	6.710,31	806,55	6.598,40

Tabla 1. Rentabilidad instalación solar fotovoltaica para autoconsumo.

Fuente: elaboración propia.

Es una cantidad de tiempo razonable, teniendo en cuenta la radiación solar de Valencia, que como hemos señalado no es la mayor de nuestro país, y que se trata de una instalación de pequeño tamaño, dado que solo tiene 5,1 kW en placas.

7. IMPACTO AMBIENTAL

Desde el punto de vista ambiental, la generación de energía eléctrica mediante instalaciones solares fotovoltaicas genera muchísimas menos emisiones de CO₂ que las tecnologías empleadas tradicionalmente, tales como el carbón, petróleo, ciclo combinado...

El mix de producción de la electricidad en España es variable de unos años a otros, por lo que las emisiones de CO₂/kWh también cambian cada año. En 2015 se ha situado en 302 g de CO₂/kWh, de acuerdo con los datos extraídos de La Oficina Catalana de Cambio Climático [5] [6].

Las emisiones de CO₂ producidas al generar energía eléctrica empleado instalaciones solares fotovoltaicas podrían considerarse nula, puesto que la producción directamente no genera emisiones. Sin embargo, se suelen asociar a la energía solar fotovoltaica las emisiones

debidas a las actividades necesarias para ponerla en marcha, como fabricación de los paneles o transporte de los mismos. Este valor asociado varía de unas fuentes a otras pero se sitúa en torno a los 35 g de CO₂/kWh [7].

En la nave industrial analizada, el empleo de la instalación solar fotovoltaica para autoconsumo supondría un ahorro en emisiones de CO₂ de un 88,41%, tal y como se muestra en la tabla 2.

IMPACTO AMBIENTAL		
FUENTE	EMISIONES CO ₂ (g/kWh)	EMISIONES CO ₂ ANUALES (g/año)
Mix eléctrico	302	2.100.014,95
Solar fotovoltaica	35	243.379,22

Tabla 2. Impacto ambiental.

Fuente: elaboración propia.

8. CONCLUSIONES

Las instalaciones solares fotovoltaicas son un tipo de instalaciones novedosas, pero suficientemente contrastadas a lo largo de los años como para considerarlas sistemas eléctricos seguros y fiables. Además, desde un punto de vista técnico, resultan muy sencillas de dimensionar y montar, y apenas necesitan mantenimiento.

Numerosas empresas han trabajado desde hace años en mejorar el funcionamiento de los componentes de estas instalaciones. Por ejemplo, la vida útil de los inversores ha aumentado desde 15 hasta 20 años, mientras que la duración en el tiempo de una instalación solar fotovoltaica de autoconsumo se sitúa en más de 40 años.

Esta mejora del rendimiento ha ido acompañada además de una reducción de los precios de los componentes de las instalaciones solares fotovoltaicas, haciendo que su coste final sea cada vez más barato. Además, el uso de estas instalaciones permite al usuario reducir su facturación eléctrica notablemente, como anteriormente se ha mostrado. Con el dinero ahorrado, se amortiza la instalación en un plazo de tiempo razonable.

Finalmente, suponen también un tipo de instalaciones respetuosas con el medio ambiente. La fuente de energía principal es el sol, un recurso limpio e ilimitado, a partir del cual se consigue generar energía eléctrica y cubrir las necesidades de los usuarios.

9. REFERENCIAS BIBLIOGRÁFICAS

- [1] Andrés, A. (2015). ¿Cuál es la mejor solución para el autoconsumo con inyección 0? *El blog de la energía fotovoltaica*.
- [2] Andreu, F. (2015). 10 claves para entender el Real Decreto de Autoconsumo. *Solartradex*.
- [3] Calvo, D. (2015). Real decreto de autoconsumo: ¿cómo sacarle provecho?. *El blog de la energía fotovoltaica*.
- [4] García, D. (2015). Reinventando el autoconsumo. *Revista SMA*.
- [5] Instituto para la Diversificación y Ahorro de la Energía (2012). Factores de Conversión Energía Final-Energía Primaria y Factores de Emisión de CO₂-2011. Recuperado de: http://www.idae.es/uploads/documentos/documentos_Factores_Conversion_Energia_y_CO2_2011_0a9cb734.pdf.
- [6] Oficina Catalana del Cambio Climático. (2016). Factor de emisión asociado a la energía eléctrica: el mix eléctrico. Recuperado de: http://canviclimatic.gencat.cat/es/reduex_emissions/factors_demissio_associats_a_lenergia/.
- [7] Resch, R. Kaye, N. (2007). La promesa de la energía solar: Estrategia energética para reducir las emisiones de carbono en el siglo XXI. *Crónica ONU. Vol XLIV. Nº 2*.
- [8] Saiz Jiménez, JA. (2016). Apuntes Energías Renovables. *Energías Renovables*.
- [9] Salas, V. (2016). Autoconsumo fotovoltaico trifásico con almacenamiento de energía. *Solarnews*, 62.
- [10] Sofos Energía. (2016). Diez casos de éxito de autoconsumo fotovoltaico para empresas. *Energética XXI*.

Recepción: 10 de enero de 2017**Aceptación:** 28 de febrero de 2017**Publicación:** 14 de marzo de 2017

TRADUCTOR MÓVIL PARA ASISTENCIA MÉDICA A PACIENTES QUECHUA HABLANTES

MOBILE TRANSLATOR FOR MEDICAL ASSISTANCE FOR QUECHUA SPEAKING PATIENTS

Manuel Avelino Lagos Barzola¹Zuliana Villar Vila²

1. Profesor del Dpto. de Matemática y Física, Área de Informática. Universidad Nacional de San Cristóbal de Huamanga, Ayacucho (Perú). E-mail: manuel.lagos@unsch.edu.pe
2. Bióloga por la Universidad Nacional de San Cristóbal de Huamanga, Ayacucho. Médico por la Universidad Científica del Sur, Lima (Perú). E-mail: zvillarv@hotmail.com

Citación sugerida:

Lagos Barzola, M.A. y Villar Vila, Z. (2017). Traductor móvil para asistencia médica a pacientes quechua hablantes. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 6(1), 15-34. DOI: <http://dx.doi.org/10.17993/3ctecno.2017.v6n1e21.15-34/>.

RESUMEN

El propósito del trabajo es desarrollar un software traductor móvil que permita realizar un diagnóstico adecuado a pacientes quechua hablantes a través de una comunicación fluida, en las instituciones de salud de la región Ayacucho. El caso de estudio se desarrolló en el Centro de Salud de Carmen Alto de Ayacucho, y el software fue diseñado para ser utilizado en atención de consultorio de medicina general.

Para el desarrollo del traductor móvil se utilizó el proceso ágil de desarrollo de Software de Programación Extrema. Para determinar la validez del instrumento desarrollado, se utilizó el diseño de validación y confiabilidad del instrumento. La validez del *software* se sustenta en que en su desarrollo se tuvo la participación de expertos en salud.

El trabajo de investigación se realizó en dos etapas tras la construcción del software. En la primera se realizó un análisis de fiabilidad del *software* y se determinó si el software permitía al médico realizar preguntas y registrar los síntomas de los pacientes quechua hablantes. En la segunda etapa se determinó el resultado del nivel de concordancia entre el diagnóstico de dichos pacientes con la colaboración de dos médicos: uno con dominio y fluidez del quechua, mientras que el segundo no. Se debe tener en cuenta que para este último se usó la herramienta desarrollada.

Finalmente, con un alto nivel de confianza, se colige que el traductor móvil para asistencia médica a pacientes quechua hablantes permite al médico general realizar preguntas satisfactoriamente y registrar los síntomas de sus pacientes. Además, con un índice de Kappa de Cohen de 0,804, se precisa que la herramienta es altamente confiable para el diagnóstico de los pacientes con la característica idiomática requerida.

ABSTRACT

The purpose of this research is the development of a mobile translator software that allows a medical diagnosis to Quechua speaking patients, through a fluently communication in the health institutions of the region of Ayacucho. The case of study was developed at Carmen Alto Health Center in Ayacucho, and the software was designed to be used just in general medicine.

To create the mobile translator, it was used the agile process of extreme programming software development. On the other hand, in order to determine the validity of the developed instrument, it was used the validation and reliability design of the instrument. The validity of the software is based on the fact that its development has involved the participation of health experts.

The application work was taken place in two stages. In the first stage, a reliability analysis of the software was performed and it was determined if the software allowed the doctor to ask the questions and record the symptoms of the Quechua speaking patients. In the second stage, the result of the level of concordance between the diagnosis of the patients was held with the help of two doctors: one who mastered Quechua, while the second one did not. It should be taken into account that the second doctor used the developed tool. Finally, through a high level of trust, it is concluded that the mobile translator for medical care to Quechua speaking patients allows the general practitioner to ask questions satisfactorily and record the symptoms of their patients. In addition, with a Cohen Kappa index of 0.804, it is specified that the tool is highly reliable for the diagnosis of patients with the required idiomatic feature.

PALABRAS CLAVE

Traductor móvil, asistencia médica, paciente quechua hablante, medicina general.

KEY WORDS

Mobile translator, medical assistance, quechua speaking patient, general medicine.

1. INTRODUCCIÓN

Con respecto a la calidad de la atención médica, Donabedian, (1984) refiere que es “el grado en que los medios más deseables se utilizan para alcanzar las mayores mejoras posibles en la salud”. Propone tres dimensiones involucradas para lograr la calidad de la atención médica: la dimensión estructura, la dimensión proceso y la dimensión resultados. En la segunda dimensión, como componente importante, menciona el proceso de comunicación.

El tema de investigación es el desarrollo de un traductor móvil para asistencia médica a pacientes quechua hablantes. El fundamento para realizar esta investigación fue la problemática que sufre la comunidad de quechua hablantes de la región de Ayacucho, ya que la asistencia médica es deficiente en zonas rurales o de bajos recursos, la cual se plasma en inadecuados diagnósticos y comunicación entre el médico hispanohablante y el paciente quechua hablante. Cabe resaltar que esta problemática es poco conocida por la falta de denuncias de estos pacientes.

Se desarrolla el traductor móvil de asistencia médica con el objetivo principal de brindar una herramienta al sector salud, en especial los médicos para que puedan realizar un diagnóstico adecuado a pacientes quechua hablantes, a través de una comunicación fluida.

Se desarrolló el traductor móvil bajo el proceso ágil de Programación Extrema y, finalmente, se validó la confiabilidad del *software* para el diagnóstico de los pacientes por parte de los médicos no quechua hablantes.

2. METODOLOGÍA

2.1. DISEÑO DE LA INVESTIGACIÓN

Según Carrasco, (2005) el diseño de investigación no experimental de tipo transversal se emplea para analizar y conocer las características, rasgos, propiedades y cualidades de un hecho realizado en un momento determinado de tiempo.

Según el punto anterior, el diseño de investigación para el trabajo de tesis es no experimental de tipo transversal, debido a que se busca recoger la información de forma directa en un momento determinado. Se tiene como objetivo básicamente el de precisar y describir de manera pertinente el *software* traductor de asistencia médica para pacientes quechua hablantes, así como verificar su confiabilidad en el diagnóstico médico. Por otro lado, para determinar la validez del instrumento tipo *software* desarrollado se utilizó el diseño de validación y confiabilidad del instrumento.

2.2. POBLACIÓN

Pacientes que acuden al Centro de Salud de Carmen Alto, Ayacucho y quienes padecen de enfermedades comunes como faringitis aguda, amigdalitis aguda, bronquiolitis y neumonía.

2.3. POBLACIÓN MUESTRAL

Son los resultados de los diagnósticos obtenidos a partir de la evaluación con el *software* usado por el médico no quechua hablante y sin el *software*, pero con la presencia de un médico quechua hablante a los pacientes mencionados con antelación.

2.4. MUESTRA

Primero, para saber si el *software* permitía realizar preguntas satisfactoriamente a pacientes quechua hablantes para así registrar sus síntomas, se hizo la prueba en una muestra intencionada de setenta y cinco pacientes que asistieron al Centro de Salud de Carmen Alto, Ayacucho.

Segundo, para ver si el *software* demostraba efectividad en el diagnóstico de los pacientes, se hizo la prueba en una muestra intencionada de noventa y seis pacientes en el Centro de Salud ya mencionado.

2.5. TÉCNICAS E INSTRUMENTOS

Las técnicas utilizadas para el estudio fueron:

- a) Lista de cotejo
- b) Análisis documental

Los instrumentos utilizados fueron:

- a) Lista de cotejo
- b) Ficha de historia clínica

3. RESULTADOS Y ANÁLISIS DE RESULTADOS

3.1. DESARROLLO DEL SOFTWARE

Proceso de atención de pacientes en consultorio de medicina general

Regularmente en un consultorio de medicina general el proceso de atención a pacientes por parte del médico sigue el siguiente flujograma:

Gráfico 1. Flujograma del proceso de atención en consultorio de medicina general.

Fuente: Elaboración propia.

La aplicación móvil de asistencia médica para pacientes quechua hablantes se construyó como herramienta de apoyo para el proceso de comunicación en estas actividades.

Sobre la elección del proceso de desarrollo de Software para el traductor móvil

Si tuviésemos que responder a la pregunta: ¿por qué elegir un proceso de desarrollo de software ágil?

Nuestra respuesta está muy de acuerdo con lo que manifestó Jacobson (2002) y que Pressman (2010) hace referencia, respecto a la agilidad:

La agilidad se ha convertido en la palabra mágica de hoy día para describir un proceso del software moderno. Todos son ágiles. Un equipo ágil es diestro y capaz de responder de manera apropiada a los cambios. El cambio es de lo que trata el software en gran medida. Hay cambios en el Software que se construyen en los miembros del equipo debidos a las nuevas tecnologías, de todas clases y que tienen un efecto en el producto que se elabora o en el proyecto que lo crea. Deben introducirse apoyos para el cambio en todo lo que se haga en el software y en ocasiones se hace porque es alma y corazón de éste. Un equipo ágil reconoce que el software es desarrollado por individuos que trabajan en equipo, y que su capacidad, su habilidad para colaborar, es el fundamento para el éxito del proyecto (p. 88). Y por otro lado, es imperiosa la necesidad de abordar temas como el que precisó Fowler, que recoge también Pressman (2010):

- a) Es difícil predecir qué requerimientos de software persistirán y cuáles cambiarán. También es difícil pronosticar cómo cambiarán las prioridades del cliente a medida que avanza el proyecto.
- b) Para muchos tipos de software, el diseño y la construcción están imbricados. Es decir, ambas actividades deben ejecutarse en forma simultánea, de modo que los modelos de diseño se prueban a medida que se crean. Es difícil predecir cuánto diseño se necesita antes de que se use la construcción para probar el diseño.
- c) En análisis, el diseño, la construcción y las pruebas no son tan predecibles como nos gustaría (desde el punto de vista de planeación).

Así mismo, se buscó alcanzar principios de agilidad como: que nuestra prioridad fue la de satisfacer al cliente a través de entregas prontas del software. Fueron bienvenidos los requerimientos cambiantes, se entregó con frecuencia software funcional, se trabajó junto con los clientes (médicos) y la conversación fue cara a cara.

Finalmente, y con respecto a la elección del proceso de desarrollo de software de Programación Extrema se dio gracias a las siguientes razones:

- a) En primer lugar, cumple con las expectativas de agilidad de un proceso ágil de desarrollo de Software requeridos en este proyecto.
- b) Pressman, (2010) afirma que es el enfoque más utilizado del desarrollo de software ágil. Consultada otras fuentes Scrum/XP Hybrid es la segunda más utilizada, frente a Scrum que es la más utilizada (<http://bspin.org/>, 2012).
- c) Y el volumen promedio de bibliografía del uso de la Programación Extrema, frente a SCRUM y otros procesos ágiles.

Desarrollo de la implementación del Software

La implementación del software siguió las etapas del proceso de desarrollo de software de Programación Extrema: exploración, planeación, iteraciones a la primera versión y puesta en producción.

Las historias de usuario obtenidas por parte del personal médico fueron:

Tabla 1. Historia de usuario realizar preguntas al paciente en quechua.

Historia de usuario	
Número: 1	Nombre: Realizar preguntas al paciente en quechua.
Usuario: Médico	
Modificación de Historia N°: NA	Iteración asignada: 1
Prioridad de negocio: Alta	Riesgo en desarrollo: Media
Descripción: Como médico quiero realizar preguntas y/o decir órdenes en quechua al paciente quechua hablante acerca de sus síntomas, con el objetivo de obtener información crítica a ser analizada para realizar su diagnóstico.	

Fuente: elaboración propia.

Tabla 2. Dar alternativas de respuesta en quechua al paciente.

Historia de usuario	
Número: 2	Nombre: Dar alternativas de respuesta en quechua al paciente.
Usuario: Médico	
Modificación de Historia N°: NA	Iteración asignada: 1
Prioridad de negocio: Alta	Riesgo en desarrollo: Media
Descripción: Como médico quiero brindar información sobre las alternativas de respuesta de cada pregunta realizada al paciente quechua hablante, con el objetivo de dar al paciente sólo alternativas fijas de respuesta.	

Fuente: elaboración propia.

Tabla 3. Resumen de respuestas del paciente

Historia de usuario	
Número: 3	Nombre: Resumen de respuestas del paciente
Usuario: Médico	
Modificación de Historia N°: NA	Iteración asignada: 1
Prioridad de negocio: Alta	Riesgo en desarrollo: Media
Descripción: Como médico quiero un resumen de todas las respuestas dadas por el paciente quechua hablante, con el objetivo de tener un reporte resumido de toda la información brindada por el paciente acerca de sus síntomas.	

Fuente: elaboración propia.

Tabla 4. Diagnosticar al paciente en quechua.

Historia de usuario	
Número:4	Nombre: Diagnosticar al paciente en quechua.
Usuario: Médico	
Modificación de Historia N°: NA	Iteración asignada: 1
Prioridad de negocio: Alta	Riesgo en desarrollo: Media
Descripción: Como médico quiero comunicar el diagnóstico de la enfermedad al paciente en quechua, con el objetivo de que el paciente quechua hablante entienda qué enfermedad padece.	

Fuente: elaboración propia.

Tabla 5. Dar tratamiento farmacológico en quechua al paciente.

Historia de usuario	
Número:5	Nombre: Dar tratamiento farmacológico en quechua al paciente.
Usuario: Médico	
Modificación de Historia N°: NA	Iteración asignada: 1
Prioridad de negocio: Alta	Riesgo en desarrollo: Media
Descripción: Como médico quiero comunicar el tratamiento farmacológico al paciente en quechua, con el objetivo de que el paciente quechua hablante entienda qué medicamentos tomar, así como la duración y frecuencia del mismo.	

Fuente: elaboración propia.

Tabla 6. Dar tratamiento preventivo en quechua al paciente.

Historia de usuario	
Número:6	Nombre: Dar tratamiento preventivo en quechua al paciente.
Usuario: Médico	
Modificación de Historia N°: NA	Iteración asignada: 1
Prioridad de negocio: Alta	Riesgo en desarrollo: Media
Descripción: Como médico quiero comunicar el tratamiento preventivo al paciente en quechua, con el objetivo de que el paciente quechua hablante entienda qué acciones preventivas realizar para su diagnóstico.	

Fuente: elaboración propia.

Tecnologías utilizadas para el desarrollo del software traductor móvil

Las herramientas tecnológicas que se utilizaron, son en gran parte de software libre, fueron seleccionadas en función a las necesidades y limitaciones como recursos económicos, humanos y el tipo de aplicación que es el software traductor móvil de asistencia médica.

Tabla 7. Herramientas de desarrollo del traductor móvil de asistencia médica.

Herramientas de desarrollo		
SOFTWARE	FABRICANTE	DESCRIPCIÓN
MICROSOFT WINDOWS 8.1	Microsoft	Sistema Operativo
JAVA JDK	Desarrollado por Sun Microsystems originalmente	Java es un lenguaje de programación orientado a objetos, desarrollado por Sun Microsystems originalmente, que posee un sistema que interpreta y ejecuta los archivos para ser compilados en tiempo real.
ANDROID SDK	Google.	El SDK (Software Development Kit) de Android, incluye un conjunto de herramientas de desarrollo. Comprende un depurador de código, biblioteca, un simulador de teléfono basado en QEMU, documentación, ejemplos de código y tutoriales. Las plataformas de desarrollo soportadas incluyen GNU/Linux, Mac OS X 10.5.8 o posterior, y Windows XP o posterior.
ANDROID STUDIO	Google.	Entorno de desarrollo integrado para la plataforma Android. Está basado en el software IntelliJ IDEA de JetBrains, y es publicado de forma gratuita a través de la Licencia Apache 2.0. Está disponible para las plataformas Microsoft Windows, Mac OS X y GNU/Linux.
SQLite	D. Richard Hipp.	Sistema de gestión de bases de datos relacional compatible con ACID, contenida en una relativamente pequeña (~275 kB) biblioteca escrita en C. SQLite es un proyecto de dominio público.
https://www.materialpalette.com/	-	Herramienta en línea para trabajar combinaciones de colores basados Google Material Design.
https://www.fluid.com	-	Herramienta en línea para elaboración de prototipos de aplicaciones móviles así como el flujograma de la aplicación.
https://icons8.com/	-	Herramienta en línea que brinda un conjunto rico de íconos.

Fuente: elaboración propia.

Herramientas para la ejecución del software traductor móvil de asistencia médica

Son necesarias las siguientes herramientas para que el usuario pueda ejecutar la aplicación móvil.

Tabla 8. Herramientas para la ejecución del traductor móvil de asistencia médica.

Herramientas para ejecución		
SOFTWARE	FABRICANTE	DESCRIPCIÓN
SISTEMA OPERATIVO ANDROID	Google.	Sistema operativo basado en el núcleo Linux. Fue diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tablets o tabléfonos; y también para relojes inteligentes, televisores y automóviles
SQLITE	D. Richard Hipp.	Sistema de gestión de bases de datos relacional compatible con ACID, contenida en una relativamente pequeña (~275 kB) biblioteca escrita en C. SQLite es un proyecto de dominio público.

Fuente: elaboración propia.

Interfaz gráfica de usuario (GUI)

La interfaz gráfica del usuario está distribuida bajo la siguiente estructura:

1. **Interfaz principal.** A partir de esta interfaz se pueden acceder a las diferentes categorías de la aplicación web, como son:
 - a. **Antecedentes.** Categoría que permitirá al médico obtener información acerca de los antecedentes del paciente.
 - b. **Síntomas.** Categoría que permitirá al médico obtener información de los síntomas del paciente.
 - c. **Examen físico.** Categoría que permitirá al médico dar indicaciones para realizar el examen físico correspondiente al paciente.
 - d. **Examen laboratorio.** Categoría que permitirá al médico solicitar exámenes de laboratorio al paciente.
 - e. **Examen de imagen.** Categoría que permitirá al médico solicitar exámenes de tipo imagen al paciente.
 - f. **Diagnóstico.** Categoría que permitirá al médico precisar el diagnóstico del paciente.
 - g. **Tratamiento.** Categoría que permitirá al médico precisar el tratamiento farmacológico y preventivo al paciente.

- h. **Preguntas comprobación.** Categoría que permitirá al médico realizar algunas preguntas que le permita saber si el paciente entendió su diagnóstico y/o tratamiento.
 - i. **Personal.** Categoría orientada a que el usuario pueda crear sus propias preguntas, así como grabar sus propios audios.
 - j. **Reporte.** Categoría en la que el usuario podrá generar un reporte de las preguntas realizadas con las respectivas respuestas del paciente, registradas por el médico.
2. **Interfaz categoría.** Es la interfaz que nos muestra las subcategorías de la categoría seleccionada previamente, así, se muestran a continuación las subcategorías por cada categoría respectivamente:
- a. Antecedentes
 - i. Antecedentes generales
 - ii. Antecedentes gineco - obstétrico
 - iii. Aparato cardiovascular
 - iv. Aparato respiratorio
 - v. Aparato urogenital
 - vi. Aparato digestivo
 - vii. Hematología y oncología
 - viii. Endocrinología
 - ix. Aparato locomotor
 - x. Neurológicas
 - xi. Infecciones
 - xii. Salud mental
 - xiii. Cabeza y cuello
 - xiv. Antecedentes quirúrgicos
 - xv. Antecedente de vacunación
 - b. Síntomas
 - i. Síntomas generales
 - ii. Oído
 - iii. Buco-dental
 - iv. Ojo
 - v. Nariz
 - vi. Aparato respiratorio
 - vii. Aparato cardiovascular
 - viii. Aparato digestivo
 - ix. Aparato urinario
 - x. Aparato genital
 - xi. Mama
 - xii. Sistema nervioso
 - xiii. Piel
 - xiv. Salud mental
 - c. Examen físico
 - i. No presenta sub categorías

- d. Examen laboratorio
 - i. No presenta sub categorías
- e. Examen de imagen
 - i. No presenta sub categorías
- f. Diagnóstico
 - i. Oído
 - ii. Vista
 - iii. Piel
 - iv. Aparato cardiovascular
 - v. Aparato respiratorio
 - vi. Aparato digestivo
 - vii. Aparato locomotor
 - viii. Sistema nervioso
 - ix. Endocrinológicos
 - x. Salud mental
 - xi. Sangre
 - xii. Infecciones
- g. Tratamiento
 - i. Tratamiento farmacológico
 - ii. Tratamiento preventivo
 - iii. Curaciones
 - iv. Duracion
 - v. Frecuencia
- h. Preguntas comprobación
 - i. No presenta sub categorías
- i. Personal
- j. Reporte
 - i. No presenta sub categorías

3.2. VALIDEZ DE CONTENIDO DEL SOFTWARE

Se garantiza la validez de contenido del *software* para el diagnóstico médico a pacientes quechua hablantes, ya que sus requisitos funcionales fueron trabajados con expertos en el sector salud. Cabe precisar que el *software* está orientado a las consultas de medicina general.

3.3. ANÁLISIS DE FIABILIDAD DEL SOFTWARE

Los resultados del análisis de fiabilidad del *software* se basan en dos etapas y dos muestras intencionadas.

Primero: resultados de pruebas realizadas en pacientes para determinar si el *software* permitió realizar preguntas y registrar los síntomas de los pacientes

Para saber si el *software* permitió realizar preguntas a pacientes, se hizo la prueba en una muestra intencionada de 75 pacientes y se obtuvo los resultados siguientes.

Tabla 9. Resultados de pruebas realizadas en pacientes para determinar si el software permitió realizar preguntas en el Centro de Salud de Carmen Alto.

		Frecuencia	Porcentaje
Válido	No	2	2,7
	Sí	73	97,3
	Total	75	100,0

Fuente: elaboración propia.

Gráfico 2. Resultados de pruebas realizadas en pacientes para determinar si el software permitió realizar preguntas en el Centro de Salud de Carmen Alto.

Fuente: elaboración propia.

Se observa que en el 97.3 % de los pacientes, el *software* permitió realizar preguntas satisfactoriamente, hecho que indica que existe un alto nivel de confianza para poder efectuar preguntas a los pacientes.

Asimismo, para determinar si el *software* permite registrar los síntomas de los pacientes, se utilizó la misma muestra de la prueba anterior.

Tabla 10. Resultados de pruebas realizadas en pacientes para determinar si el software permitió realizar preguntas en el Centro de Salud de Carmen Alto.

		Frecuencia	Porcentaje
Válido	No	2	2,7
	Sí	73	97,3
	Total	75	100,0

Fuente: elaboración propia.

Gráfico 3. Resultados de pruebas realizadas en pacientes para determinar si el software permitió realizar preguntas en el Centro de Salud de Carmen Alto.

Fuente: elaboración propia.

Se observa que en el 97.3 % de los pacientes, el *software* traductor permitió registrar los síntomas de los pacientes, lo que demuestra ser un buen indicador para afirmar que sí permite registrar los síntomas de los pacientes.

Segundo: resultado del diagnóstico de pacientes de acuerdo al médico quechua hablante y al médico no quechua hablante

Para determinar si el *software* determinaba efectividad en el diagnóstico de los pacientes, se hizo la prueba en una muestra intencionada de 96 pacientes en el Centro de Salud de Carmen Alto, Ayacucho.

La prueba consistió en medir el nivel de concordancia entre los diagnósticos de los pacientes elaborados por dos médicos: uno que es quechua hablante (sin *software*) y otro no quechua hablante (con el *software*). Para medir dicha concordancia se hizo uso del estadístico de índice de Kappa de Cohen.

Para ello se planteó las siguientes hipótesis estadísticas:

Ho: No existe concordancia entre el diagnóstico del médico quechua hablante y el diagnóstico del médico no quechua hablante.

H1: Existe concordancia entre el diagnóstico del médico quechua hablante y el diagnóstico del médico no quechua hablante.

Tabla 11. Resultado de diagnóstico de pacientes de acuerdo al médico quechua hablante y no quechua hablante.

		Médico con <i>software</i> (no quechua hablante)				Total	
		Faringitis aguda	Amigdalitis aguda	Bronqui olitis	Neumonía		
Médico quechua hablante	Faringitis aguda	N	18	1	1	21	
		%	18,8 %	1,0 %	1,0 %	21,9 %	
	Amigdalitis aguda	N	2	21	1	25	
		%	2,1 %	21,9 %	1,0 %	1,0 %	26,0 %
	Bronquiolitidis	N	2	1	26	1	30
		%	2,1 %	1,0 %	27,1 %	1,0 %	31,3 %
	Neumonía	N	1	1	1	17	20
		%	1,0 %	1,0 %	1,0 %	17,7 %	20,8 %
	Total	N	23	24	29	20	96
		%	24,0 %	25,0 %	30,2 %	20,8 %	100,0 %

Fuente: elaboración propia.

Tabla 12. Medidas simétricas.

		Valor	Error estándar asintótico ^a	Aprox. S ^b	Aprox. Sig.
Medida de acuerdo	Kappa	,804	,048	13,563	,000
N de casos válidos		96			
a. No se supone la hipótesis nula.					
b. Utilización del error estándar asintótico que asume la hipótesis nula.					

Fuente: elaboración propia.

En la tabla de resultado del diagnóstico de pacientes de acuerdo al médico quechua hablante y no quechua hablante, se puede apreciar que en el 27,1 % de los diagnósticos los médicos coincidieron que dichos pacientes tienen bronquiolitis. En el 18.8 % de los casos coinciden y diagnostican faringitis aguda, mientras que en 2.1 % de los casos no coincidieron, ya que el médico quechua hablante diagnosticó amigdalitis aguda y el médico no quechua hablante diagnosticó faringitis aguda.

A continuación, aparecen los resultados propios del análisis de la prueba del índice de Kappa para datos pareados (datos que corresponden al mismo individuo, pero observados por 2 médicos diferentes) en el número de pacientes diagnosticados (96), y finalmente, la probabilidad de error tipo I (P-valor = 0,000) asociada al índice de Kappa de Cohen (0,804).

Decisión:

Como el P-valor es menor de 0,05 entonces se rechaza la H_0 , lo cual indica que podemos afirmar a un nivel de confianza al 95% que existe concordancia casi perfecta (de acuerdo a la valoración del coeficiente de Kappa de acuerdo a Landis y Koch (1997) entre el médico quechua hablante y el médico no quechua hablante.

La prueba de concordancia o armonía entre jueces se encuentra en el protocolo de las características psicométricas de la fiabilidad de un instrumento de medida, y de acuerdo a la existencia de una concordancia casi perfecta entre los médicos, se puede indicar que el *software* traductor móvil es altamente confiable (buena, de acuerdo a la valoración del índice de Kappa) para el uso en el diagnóstico de los pacientes por parte de los médicos no quechua hablantes.

4. CONCLUSIONES

- a) Con un alto nivel de confianza, se precisa que el traductor móvil para asistencia médica a pacientes quechua hablantes permite realizar preguntas satisfactoriamente.
- b) Con un alto nivel de confianza, se demuestra que el traductor móvil para asistencia médica a pacientes quechua hablantes permite el registro de síntomas de pacientes satisfactoriamente.
- c) Con el índice de Kappa de Cohen de 0,804, se determina que el traductor móvil para asistencia médica es altamente confiable (buena, de acuerdo a la valoración del índice de Kappa) para el diagnóstico de los pacientes por parte de los médicos no quechua hablantes, con un nivel de confianza al 95 %.
- d) Finalmente, se afirma que es posible desarrollar un *software* traductor móvil para realizar un diagnóstico adecuado a pacientes quechua hablantes a través de una comunicación fluida.

5. REFERENCIAS BIBLIOGRÁFICAS

- Baird, S. (2002). *Teach Yourself Extreme Programming in 24 Hours*. Primera edición. Estados Unidos.
- Beck, K. (1999). *Extreme programins Explained*. Primera Edición. USA. Addison-Wesley urb Co.
- Bernal C. (2010). *Metodología de la investigación*. Tercera Edición. Pearson Educación, Colombia.
- Cárdenas A.M, Godoy D.D. (2008). *Estrategias de comunicación*. Pontificia Universidad Javeriana. Colombia.
- Carrasco D. S. (2005). *Metodología de la investigación científica*. Primera edición. Editorial San Marcos. Lima, Perú.
- Computerhope. (2016). Recuperado de: <http://www.computerhope.com/jargon/t/translator.htm/>.
- Date, C.J. (2001). *An Introduction to Database Systems*. Séptima edición. México. Pearson Educación.
- De la Cruz, T. M. (2003). *La traducción de textos turísticos: propuesta de clasificación y análisis de muestras*. Recuperado de: http://apps.who.int/iris/bitstream/10665/37500/1/WHO_TRS_176_spa.pdf/.
- DSIIC-Universidad Politécnica de Valencia. (2006). *Metodologías Agiles para el Desarrollo de Software: Extreme Programming (XP)*. Valencia, España.
- Huayhua, M. (2006). *Discriminación y exclusión: políticas públicas de salud y poblaciones indígenas*. Disponible: <http://archivo.iep.pe/textos/DDT/DDT147.pdf/>. [05 de marzo del 2016].
- Donabedian, A. (1966). *Evaluating the quality of medical care*. *The Milbank Memorial Fund Quarterly*, 44 (3), 166-203. Publicado nuevamente en junio 2005, 83 (4), 691-729.

- Donabedian, A. (1984). *La Calidad de la atención médica, definición y métodos de evaluación*. Editorial La Prensa Médica Mexicana.
- Jeffries, R., Anderson, A. y C. Hendricksopn. (2001). *Extreme programming Installed. Primera Edición*. Usa. Addison-Wesley urb Co.
- Joyanes, L. (1996). *Programación orientada a objetos*. Madrid, España: McGraw – Hill Interamericana de España S.A.U.
- Joyanes, L. y Zahonero, I. (2002). *Programación en Java 2: Algoritmos, estructuras de datos y Programación orientada a objetos*. Madrid, España: McGraw – Hill Interamericana de España S.A.U.
- Lopera, Q. J. (2008). *Manual de semiología en quechua*. Recuperado de: <http://cmp.org.pe/documentos/librosLibres/manualSemiologiaQuechua/>.
- Mobile Marketing Asociation. (2011). *Libro Blanco de Apps / Guía de apps móviles*. Mobile Marketing Asociation.
- Organización Mundial de la salud (1959). *Segundo informe del comité de Expertos de Organización de la Asistencia Médic*. Ginebra.
- Pizzolante N. I. (2004). *El Poder de la Comunicación Estratégica*. Editorial Pontificia Universidad Javeriana. Bogotá.
- Pressman, R. (2002). *Ingeniería de software: Un enfoque práctico (5ª Ed.)*. Madrid, España: McGraw – Hill Interamericana S.A.
- Priolo, S. (2007). *Programación extrema*.
- Sánchez, C.G. (2006), *Seminario de Etnolingüística, un estudio de tres lenguas amerindias: Natuatl, quechua y aimara. Informe Final de Seminario de Grado, Universidad de Chile*, Chile. Recuprado de: http://repositorio.uchile.cl/tesis/uchile/2006/gomez_m2/sources/gomez_m2.pdf. [02 de febrero del 2016].
- Schmuller, J. (1997). *Aprendiendo UML en 24 horas*. Naucalpan de Juárez, Mexico: Editorial División Computación.
- Servicio Canario de la Salud – España. (2015). Recuperado de: <http://www3.gobiernodecanarias.org/>.
- Solis, F.G. (2011). *Quechua: una síntesis. Revista cultural electrónica Construyendo nuestra Interculturalidad*. Recuperado de: http://www.interculturalidad.org/numero06-07/attachments/article/89/Solis_Quechua-Una-sintesis.pdf. [20 de enero del 2016].
- Tur, J. (1974). *Sobre la teoría de la traducción*. Centro Virtual Cervantes. Recuperado de: http://www.colegiotraductores.org.uy/Jaume_Tur_Sobre_teoria_de_la%20traduccion.pdf. [10 de enero del 2016].
- Universal Doctor (2016). Recuperado de: <http://www.universaldactor.com/>.

Valdivia. (2010). <<http://alertacontraelracismo.pe/wp-content/uploads/2013/01/Ladiscriminaci%C3%B3nenelper%C3%BAyelcaso-de-la-salud.pdf>>.

Wasserman, A.I. (2010). *Software engineering issues for mobile application development. Proceedings of the FSE/SDP workshop on future of software engineering research*, 7-8 de noviembre de 2010.

Weitzenfeld, A. (2005). *Ingeniería de Software Orientado a Objetos con UML, Java e Internet*. México, D.F., México: Thomson.

Zurita, B. (1966). *Anales de la Facultad de Medicina: Calidad de la Atención de la Salud*. Universidad Nacional Mayor de San Marcos. ISSN 1025 – 5583, 57(4). Perú. 199.

Recepción: 23 de enero de 2017**Aceptación:** 10 de marzo de 2017**Publicación:** 14 de marzo de 2017

¿POR QUÉ DESCONFIAR DE LOS DISPOSITIVOS DE ALMACENAMIENTO DIGITAL?

WHY YOU SHOULD NOT TRUST DATA STORAGE DEVICES?

Romel Vera Cadena¹

1. Consultor de Seguridad Informática. (Ecuador). E-mail: romel.vera.cadena@gmail.com

Citación sugerida:

Vera Cadena, R. (2017). ¿Por qué desconfiar de los dispositivos de almacenamiento digital?. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 6(1), 35-46. DOI: <http://dx.doi.org/10.17993/3ctecno.2017.v6n1e21.35-46/>.

RESUMEN

Los dispositivos de almacenamiento digital pueden no ser tan seguros como se pensaba. Mediante un pendrive se puede pasar *malware* al computador y esto sucede por *software* o *hardware*, siendo éste último abusado por fallas de diseño en la implementación del USB para pasar desapercibido por *software* de seguridad debido a que no existen parches para este tipo de problemas.

ABSTRACT

Data storage devices may not be as safe as previously thought. A pendrive can be used to infect a computer with malware and this can be achieved by software or hardware, the latter being abused by design flaws in the implementation of USB, and cannot be detected by security software because there are no patches for this type of problem.

PALABRAS CLAVE

Malware, Pendrive, USB, Seguridad Informática, badUSB.

KEY WORDS

Malware, Pendrive, USB, Information Security, badUSB.

1. INTRODUCCIÓN

Los usuarios de computadoras intercambian *pendrives* regularmente para poder transmitir información relevante en una empresa o para algo trivial en el hogar. La mayoría conoce que por el uso constante de estos dispositivos se van a encontrar *malwares* y normalmente depende del antivirus evitar que el *malware* infecte al equipo, pero los problemas de seguridad en éstos dispositivos de almacenamiento portátiles no son tan sencillos como se pensaba (Tischer, 2016).

Varios especialistas de seguridad como Karsten Nohl y Jakob Lell han demostrado que los dispositivos USB pueden ser usados para infectar un computador con *malware* sin ser detectado y éste *malware* podría interceptar el uso de internet del usuario o instalar *software* no deseado en el equipo. Esto ocurre porque el problema no radica en la memoria del dispositivo o del computador sino en el *firmware* que controla las funciones básicas del dispositivo USB. Por ejemplo, un dispositivo USB como en el caso de un pendrive contiene un pequeño computador y un *firmware* que es esencialmente un *software* especial o un pequeño sistema operativo que hace que el dispositivo funcione correctamente (Nohl, 2014).

Este *firmware* funciona a bajo nivel y es usualmente programado de fábrica y al momento en que se adquiere un *pendrive* básicamente se estaría haciendo un acto de fe porque se confía que el *firmware* del *pendrive* funciona tal y como fue diseñado por el fabricante (Greenberg, 2014).

En muchos de los dispositivos USB los *firmwares* pueden ser reprogramados al momento de ser insertados en un computador desconocido o de poca confianza. Esto es posible porque algunos de los fabricantes no diseñaron seguridades que eviten la reprogramación del *firmware* (Han, 2016) (Schumilo, 2014).

Como consecuencia, estos dispositivos podrían ser usados para transmitir *malware* o realizar bromas pesadas, como transmitir virus o troyanos, convertir un teclado en un teclado espía haciendo uso de un registro interno de lo que se escribe, enviar imágenes de una webcam a otro computador, etc. (Nasution, 2014) (Stoffregen, 2014).

El presente artículo tiene como propósito concientizar a las personas en cuanto al riesgo que existe cuando se usan dispositivos USB de desconocidos, sean de almacenamiento o no y también demostrar mediante un experimento de laboratorio cómo se construye un dispositivo que pudiese presentarse como un *pendrive*, pero que en realidad funciona como un teclado y que realice acciones en el ordenador.

2. METODOLOGÍA

Desarrollando el laboratorio práctico se contestará la siguiente pregunta:

- ¿Es posible burlar software de seguridad utilizando dispositivos de almacenamiento modificados?

Para contestar esta interrogante se realizará un laboratorio práctico en el que se construirá un dispositivo USB modificado y, posteriormente, se ejecutarán pruebas en 10 computadoras diferentes que tengan instalado software de seguridad con la finalidad de poder reflejar los resultados obtenidos en una tabla.

Para corroborar el éxito de la prueba, el dispositivo USB deberá realizar las siguientes acciones visibles en el computador:

1. Esperar 11 segundos después de que el dispositivo haya sido conectado al computador
2. Abrir la ventana “ejecutar” del Windows
3. Abrir el editor de texto del Windows (Notepad)
4. Escribir 2 líneas en el Notepad:
 - “Prueba de dispositivo Teensy.”
 - “Completa!”

El sistema operativo seleccionado para realizar éstas pruebas es Windows 10 de Microsoft por tratarse de un sistema operativo en el mercado con un mayor porcentaje de adopción (SpiceWorks, 2016).

Figura 1. Porcentaje de adopción de Windows 10 en compañías después de 6 meses de su lanzamiento.

Fuente: [Spiceworks 2016](#).

Y para la selección del software de seguridad se han tenido en cuenta las evaluaciones del mejor software de seguridad de AVTEST del mes de diciembre del 2016 (AVTEST, 2017).

2.1. MATERIALES

1. Teensy++ 2.0

El material principal es un hardware que básicamente es una placa de circuito impreso con un microcontrolador programable y en este caso será un Atmel AVR.

Si posee conocimientos básicos de electrónica puede comprar los componentes individualmente en:

<https://www.sparkfun.com>

<https://www.adafruit.com>

O puede comprar la unidad lista para usar en:

<https://www.pjrc.com>

En el caso de comprar un Teensy es aconsejable adquirir cualquier unidad desde la versión 2.0 en adelante.

Figura 2. Teensy++ 2.0

Fuente: [PJRC](http://www.pjrc.com)

Teensy++ 2.0 es una placa de desarrollo USB que viene con un microcontrolador AVR de la firma Atmel AT90USB1286, y se puede programar con el lenguaje Arduino o C.

El Teensy++ 2.0 está diseñado para realizar rápidamente proyectos teniendo poca base en electrónica y programación. Su diseño está pensado para proyectos que se desarrollan en protoboards o en un tablero de pruebas.

2. Cable USB Mini-B

Para conectar el Teensy++ 2.0 al computador es necesario contar con un cable USB Mini-B.

Figura 3. Cable USB Mini-B

Fuente: [PJRC](http://www.pjrc.com)

3. Un computador con sistema operativo Windows

2.2. SOFTWARE REQUERIDO

Para poder programar el Teensy++ 2.0 es necesario instalar:

1. Arduino IDE 1.8.1

<https://www.arduino.cc/en/Main/Software>

2. Teensyduino 1.35

https://www.pjrc.com/teensy/td_download.html

Deberá instalarlos en el orden indicado arriba.

El Arduino IDE es un entorno de programación y el Teensyduino contiene librerías para poder usar efectivamente el Teensy.

2.3. LABORATORIO

Para realizar el laboratorio práctico con éxito siga los siguientes 6 pasos:

1. Iniciar el entorno de programación.

Deberá conectar el Teensy al iniciar el entorno de programación para que el Windows instale los Drivers automáticamente.

Figura 4. Inicio del software Arduino IDE versión 1.8.1.

Fuente: elaboración propia.

2. Seleccionar el board que se está usando.

Click en Tools -> Board -> Teensy++ 2.0

Figura 5. Selección del board Teensy++ 2.0.

Fuente: elaboración propia.

3. Seleccionar el modo de operación.

Click en Tools -> USB Type -> Keyboard + Mouse + Joystick

Figura 6. Selección del modo de operación.

Fuente: elaboración propia.

4. Escribir el código en la ventana de texto del entorno de programación:

```
void setup() {
  Serial.begin(9600);
  delay(11000);

  appRun("notepad");
  delay(1000);

  Keyboard.println("Prueba de dispositivo Teensy.");
  delay(1000);
  Keyboard.println("Completa!");
}
void loop() {
}
void appRun(char *SomeCommand)
{
  Keyboard.set_modifier(128);
  Keyboard.set_key1(KEY_R);
  Keyboard.send_now();
  Keyboard.set_modifier(0);
  Keyboard.set_key1(0);
  Keyboard.send_now();
  delay(1500);
  Keyboard.print(SomeCommand);
  Keyboard.set_key1(KEY_ENTER);
  Keyboard.send_now();
  Keyboard.set_key1(0);
  Keyboard.send_now();
}
```

Código 1. Código fuente de las funciones que ejecutará el Teensy++ 2.0.

Fuente: elaboración propia.

5. Compilar el código.

Click en Sketch -> Verify/Compile

Figura 7. Compilar código fuente.

Fuente: elaboración propia.

6. Subir el código compilado al Teensy.

Si ha desconectado el Teensy en este paso deberá conectarlo nuevamente para poder continuar.

Figura 8. Código compilado y listo para subir al Teensy.

Fuente: elaboración propia.

Para poder subir el código al Teensy es necesario presionar el botón de programación del Teensy.

Figura 9. Ubicación del botón de programación del Teensy++ 2.0.

Fuente: elaboración propia, basada en gráfico de [PJRC](#).

Finalmente, el código hará que el Teensy se comporte como un teclado y enviará los comandos programados a la computadora.

Lo puede probar desconectándolo y volviéndolo a conectar al mismo PC, o a otro PC.

3. RESULTADOS

Se realizaron pruebas a 10 computadoras diferentes que contaban con software de seguridad.

Los *softwares* de seguridad fueron descargados de sus sitios web oficiales y sus versiones corresponden a versiones de pruebas (trial) descargados el día sábado 7 de enero del 2017.

Tabla 1. Resultado de pruebas usando el Teensy++ 2.0.

Prueba	Sistema Operativo	Software de Seguridad	Teensy ejecución de código	Detectado
1	Windows 10 Pro v1607	Windows Defender	100%	No
2	Windows 10 Home v1607	Windows Defender	100%	No
3	Windows 10 Home v1511	ESET Smart Security	100%	No
4	Windows 10 Pro v1607	Kaspersky Total Security	100%	No
5	Windows 10 Pro v1607	Avast Premier	100%	No
6	Windows 10 Home v1511	AVG Ultimate	100%	No
7	Windows 10 Pro v1607	Norton Security Premium	100%	No
8	Windows 10 Pro v1607	Avira Antivirus	100%	No
9	Windows 10 Pro v1607	Panda Global Protection	100%	No
10	Windows 10 Home v1607	McAfee LiveSafe	100%	No

Fuente: Elaboración propia.

En la tabla de resultados se observa que ningún software de seguridad pudo detectar las acciones programadas que realizó el Teensy++ 2.0 en el computador.

El Teensy++ 2.0 realizó todas las acciones visuales que se programaron usando el código fuente del laboratorio.

4. CONCLUSIONES Y RECOMENDACIONES

Al comienzo del presente artículo se indagó en el tema del uso de dispositivos USB tomando en consideración especial los de almacenamiento al tratarse de dispositivos de uso diario para transferir información, y posteriormente se planteó la interrogante “¿Es posible burlar software de seguridad utilizando dispositivos de almacenamiento modificados?”.

Los resultados del laboratorio práctico reflejan que sí es posible burlar software de seguridad mediante la programación o reprogramación de dispositivos USB.

Por lo tanto, es posible que un delincuente informático o una persona maliciosa pueda infectar equipos informáticos, interceptar contraseñas que se registren en el teclado, exfiltrar información, etc. logrando causar daños y pérdidas financieras a una empresa o individuo.

Como medidas cautelares se sugiere que las personas se aseguren de que todos los dispositivos USB que se vayan a conectar en un computador provengan de fuentes fiables.

De sospechar de un dispositivo USB lo recomendable es avisar a un técnico de confianza para que le realice pruebas al dispositivo en un ambiente seguro.

En las empresas es posible realizar pruebas de seguridad usando estos dispositivos que aparentan ser *pendrives* normales con la finalidad de demostrar lo inseguro que es confiar en dispositivos USB desconocidos.

En el hogar se debe educar a los miembros de la familia para evitar ser víctimas de delincuentes informáticos ya que estos dispositivos son cada vez más asequibles, fáciles de usar y fáciles de programar.

5. FUTURAS INVESTIGACIONES

Es posible crear dispositivos más elaborados, por ejemplo:

- Disfrazar el Teensy como un pendrive mediante el uso de una impresora 3D o desmantelando otro dispositivo y adaptando el conector USB tipo A.

Figura 10. Teensy 3.2 con adaptación USB del tipo A.

Fuente: Elie.net.

- Se puede analizar otros dispositivos de similar función como el USB Rubber Ducky de Hak5 el cual viene armado, listo para usar y es fácil de programar.

El USB Rubber Ducky se puede conseguir en:

<https://hakshop.com/products/usb-rubber-ducky-deluxe>

Figura 11. USB Rubber Ducky de la empresa Hak5.

Fuente: [Hak5 HakShop](https://hakshop.com/products/usb-rubber-ducky-deluxe).

6. REFERENCIAS BIBLIOGRÁFICAS

- AVTEST. (2017). *The best antivirus software*. Retrieved from AVTEST: <<https://www.av-test.org/>>.
- Greenberg, A. (2014). *Why the Security of USB Is Fundamentally Broken*. Retrieved from Wired: <<https://www.wired.com/2014/07/usb-security/>>.
- Han, S. S. (2016). *IRON-HID: Create your own bad USB*.
- Nasution, S. M. (2014). Integration of kleptware as keyboard keylogger for input recorder using teensy USB development board. *IEEE*, 1-5.
- Nohl, K. (2014). *BadUSB—On accessories that turn evil*. Black Hat USA.
- Schumilo, S. S. (2014). *Don't trust your USB! How to find bugs in USB device drivers*. Blackhat Europe.
- SpiceWorks. (2016). *Windows 10 Adoption: Sprinting out the Gate*. Retrieved from SpiceWorks: <<https://www.spiceworks.com/it-articles/windows-10-adoption/>>.
- Stoffregen, P. J. (2014). *Teensy usb development board*.
- Tischer, M. D. (2016). Users really do plug in USB drives they find. *IEEE Symposium* (pp. 306-319). IEEE.

Recepción: 15 de noviembre de 2016**Aceptación:** 06 de febrero de 2017**Publicación:** 14 de febrero de 2017

LA NECESIDAD Y LA OPORTUNIDAD DE LA INNOVACIÓN

THE NEED AND OPPORTUNITY OF INNOVATION

Mónica García Cantó¹Laura M^a Palacios Ruiz²

1. Consultora especialista en el área de innovación y financiación. Executive Máster en Innovación (EOI). Ingeniera de Organización Industrial e Ingeniera Técnica especializada en Química por la Universidad de Valencia (EPSA). E-mail: monigc22@hotmail.com
2. Consultora especialista en el área de innovación y organización industrial. Grado de Ingeniería Civil e Ingeniería Técnica de Obras Públicas. Máster Universitario en Organización Industrial y Logística por la Universidad de Valencia (EPSA). E-mail: lpalaciosr@gmail.com

Citación sugerida:

García Cantó, M. y Palacios Ruiz, L.M. (2017). La necesidad y la oportunidad de la innovación. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 6(1), 47-52. DOI: <http://dx.doi.org/10.17993/3ctecno.2017.v6n1e21.47-52/>.

RESUMEN

Se realiza un análisis de la necesidad y oportunidad de la innovación como opción de supervivencia. Así mismo, se estudian los diferentes conceptos de innovación, tecnología y su importancia para el desarrollo empresarial, se exponen sus fases y alcance. Se realiza un análisis pormenorizado de las dificultades de la función innovación en la pyme. Se incorpora una descripción de aquellas herramientas consideradas básicas para poder gestionar con éxito la innovación, acabando con un apartado de conclusiones.

ABSTRACT

In this research, an analysis of the necessity and opportunity of the innovation as an option of survival is realized. Besides, the different concepts of innovation, technology and its importance for the enterprise development are studied, its phases and reach are exposed. It is performed a detailed analysis of the difficulties of innovation in SMEs function. It is incorporated a description of those basic tools to successfully manage innovation, ending with a section of conclusions.

PALABRAS CLAVE

Innovación tecnológica, investigación y desarrollo, gestión de la innovación, herramientas para la innovación.

KEY WORDS

Technological innovation, research and development, management of innovation, tools for innovation.

1. INTRODUCCIÓN

La historia nos ha revelado en reiteradas ocasiones que la mayoría de las innovaciones aparecen ante períodos críticos que desencadenan problemáticas que necesitan ser resueltas de forma efectiva.

En estos momentos de crisis, en los que la economía española y europea se encuentran debilitadas y disminuidas, aparece el factor o función innovación como elemento que jugará un papel fundamental en su reactivación.

Por otra parte, el entorno empresarial, la globalización y la extraordinaria capacidad de la sociedad para crear conocimiento abren un enorme abanico de oportunidades para innovar. En cuanto a la sociedad, cada vez más exigente, impulsa cambios en el entorno empresarial próximo, siendo una fuente constante de retos que inducen cambios en la oferta de las empresas y en la forma de llevarla al mercado.

La globalización convierte en accesibles mercados algunos antes descartados, así como abre también los habituales a nuevos competidores que pueden tener otras ventajas. Sólo con cambios, es decir, con innovaciones, será posible hacer frente a las nuevas situaciones, sean estas oportunidades o amenazas para la empresa.

Estas son sólo algunas de las razones que hacen que las innovaciones sean las que marcan el camino para asegurar la permanencia de la empresa y para aprovechar oportunidades que distingan su oferta.

2. ¿QUÉ ES LA INNOVACIÓN Y EN QUÉ CONSISTE?

En ocasiones se asocia la innovación exclusivamente con la Investigación y Desarrollo, I+D. Si bien el factor tecnológico está presente en gran parte de la actividad innovadora de las empresas, la función innovación incluye otras actividades no necesariamente basadas en la tecnología.

Desde un punto de vista más amplio, podríamos definir la Innovación como el arte de convertir las ideas y el conocimiento en productos, procesos o servicios nuevos, significativamente mejores que los existentes, y sobre todo, así sean valorados o reconocidos por el mercado, sin excluir nuevos enfoques de marketing, nuevas formas de distribución, cambios en la organización,...

Por lo tanto, Innovación no solo es añadir mayor sofisticación técnica o tecnológica a los productos o servicios, sino que estos se adapten mejor a las necesidades del cliente o usuario final. Así pues, los tres principios básicos que debe cumplir toda innovación o desarrollo son fundamentalmente tres [1], [2], [3]:

1. Debe cubrir alguna necesidad, ser útil.
2. Se tiene que poder repetir y continuar con ello.
3. Debe poder ser asumida y gestionada y soportada por la organización o empresa que la desarrolla.

Aunque existen diferentes tipos de clasificaciones de la innovación, la mayoría suelen basarse en el siguiente esquema [1], [3], [4]:

- Innovación tecnológica.
- Innovación de producto.
- Innovación de servicio.
- Innovación de proceso.
- Innovación en la gestión de las relaciones con el cliente.
- Innovación organizacional.

Desde un punto de vista estratégico, la innovación no es una alternativa de negocio, tampoco es solo cosa de empresas con mucho nombre y tamaño, es una necesidad, quizás la única opción de supervivencia para las pymes, dado que la competencia de mercado global no nos permite hacer las cosas como hasta ahora.

Desde esta perspectiva la innovación en la pyme será aquello que nos da la oportunidad de diferenciarnos, ser muy buenos en algunos aspectos en los que otras empresas no operan.

3. DIFICULTADES EN LA GESTIÓN DE LA INNOVACIÓN EN LA PYME

En general, la dificultad real para la adopción de innovaciones no está en la propia innovación, sino en su implantación práctica, siendo necesario contemplar los siguientes factores clave para que una innovación se implante con éxito [4], [6]:

- Falta de tiempo. La gerencia y directivos de la empresa no tienen tiempo para desarrollar con éxito la función innovación.
- No adecuación de la estructura de la empresa. Las estructuras verticales, departamentales o jerárquicas conllevan falta de fluidez de los procesos, caracterizándose por ser “reinos de taifas” o compartimentos estancos, mientras que las estructuras horizontales o por proyectos conllevan la no dependencia temporal de los participantes, mientras dura el proyecto, de sus departamentos o secciones. Las estructuras matriciales son sin ninguna duda una solución óptima, aunque no es fácil ni inmediata su diseño e implantación.
- Inexistencia o no adecuación de la estructura organizativa de la innovación. Comité de innovación, director de proyecto, director funcional, administrador del proyecto, ...
- Carencias formativas, relativas a los mecanismos y herramientas para innovar, del personal clave de la empresa. La orientación hacia el aprendizaje es necesaria para que los colaboradores estén dispuestos a experimentar y a asumir los riesgos de aprender algo nuevo.
- Falta de cultura, incentivación, motivación hacia la innovación. La percepción de los miembros del equipo sobre la importancia y necesidad de implantar la innovación, lo que supone una resistencia al cambio y una visión cortoplacista,
- Enorme distanciamiento enorme entre universidades, centros de investigación y empresas.

4. HERRAMIENTAS BÁSICAS PARA LA GESTIÓN DE LA INNOVACIÓN

En este apartado pretendemos enumerar y realizar una pequeña descripción de las metodologías y herramientas que deben ser puestas en práctica por una organización de cualquier tipo o tamaño para implementar con éxito la función innovación [5], [6], [7].

- Técnicas de creatividad que permiten el entrenamiento creativo. Como se fomentan las ideas y como éstas se convierten en innovación.
- Evaluación y selección de las ideas o proyectos. Análisis de viabilidad técnica y de mercado.
- Estado del arte, estudio de la técnica, antecedentes a la innovación.
- Vigilancia tecnológica e inteligencia competitiva como proceso organizado, selectivo y permanente de captar información del exterior y de la propia organización sobre ciencia, tecnología y mercados, seleccionarla, analizarla, difundirla y comunicarla, para convertirla en conocimiento para tomar decisiones con menor riesgo y poder anticiparse a los cambios
- Generación y selección de proyectos. Creación del mapa de proyectos, indicación de dificultad, impactos, costes, recursos, etc. con indicación de zonas de ausencia, análisis y diversificación de riesgos.
- Selección, propiamente dicha, a partir de los proyectos presentados según los pasos anteriores.
- Especificación, planificación, control y seguimiento de proyectos: determinación y control de objetivos, hitos, actividades, recursos necesarios, responsabilidades, entregables, tiempos,...
- Revisión y cierre de proyectos: cierre administrativo, cuentas, contratos con proveedores, recogida y archivo de información. Se incluirá en esta fase la revisión y extracción de conclusiones para el desarrollo de nuevos proyectos, en base a la consecución de los objetivos, el cumplimiento de los plazos, el uso de recursos, costes, etc.

5. CONCLUSIONES

Si bien es cierto que la innovación es fundamental para el éxito y supervivencia de las organizaciones, también es cierto que la mayoría de gerentes y directores no están satisfechos con la capacidad innovadora de sus empresas.

Se equivocan aquellos que entienden la “innovación” como un factor espontáneo, no estructurado, ligado a la “prueba y error”, suerte o azar. La innovación, como cualquier otra función y subsistema de la empresa, es sistemática, está basada en el conocimiento y solo tendrá éxito si tiene una orientación de proceso, si se la destina de recursos suficientes y de herramientas y mecanismos específicos que garanticen su consecución.

6. REFERENCIAS BIBLIOGRÁFICAS

- [1] Florángel Ortiz. (2006). Gestión de innovación tecnológica en PYMES manufactureras. México.
- [2] Cluster Audiovisual Galego (2011). El sistema de gestión de la innovación. Milladoiro, A Coruña.
- [3] Martínez García, F.J. (2007). Estrategia e innovación de la pyme industrial en la comunidad de Cantabria, Santander.
- [4] Robotiker. (2001). Guía Tecnopyme.
- [5] CEM. (2009). Guía práctica de innovación para pymes.
- [6] Ramis Pujol, J. (2009). Guía práctica de la innovación para PYMES.
- [7] Fundación Cotec. (2010). La innovación en un sentido amplio. Análisis conceptual y empírico.

Recepción: 17 de enero de 2017

Aceptación: 10 de marzo de 2017

Publicación: 14 de marzo de 2017

VULNERABILIDADES Y AMENAZAS A LOS SERVICIOS WEB DE LA INTRANET DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO

VULNERABILITIES AND MENACES TO WEB SERVICES IN INTRANET'S TECHNICAL UNIVERSITY OF BABAHOYO

Geovanny Vega Villacís¹

Raúl Armando Ramos Morocho²

1. Universidad Técnica de Babahoyo. Facultad de Administración, Finanzas e Informática. Babahoyo, Los Ríos (Ecuador). E-mail: pvega@utb.edu.ec

2. Universidad Técnica de Babahoyo. Facultad de Administración, Finanzas e Informática. Babahoyo, Los Ríos (Ecuador). E-mail: rmos@utb.edu.ec

Citación sugerida:

Vega Villacís, G. y Ramos Morocho, R.A. (2017). Vulnerabilidades y amenazas a los servicios web de la intranet de la Universidad Técnica de Babahoyo. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 6(1), 53-66. DOI: <http://dx.doi.org/10.17993/3ctecno.2017.v6n1e21.53-66/>.

RESUMEN

Hoy en día el recurso sustancial a proteger, es sin duda la información. El objetivo de la investigación es demostrar las vulnerabilidades y amenazas que presentan los servicios WEB en la intranet de la Universidad Técnica de Babahoyo. Se determinó las debilidades y ataques presentes en la red; a través de, análisis por observación directa con pruebas de tráfico de paquetes y encuestas a usuarios de red. Se concluye en la falta de procedimientos en seguridad informática y errores no controlados por ataques y perpetraciones. Finalizando con el diseño de un Sistema de Detección de Intrusos (NDIS).

ABSTRACT

Today the substantial resource to protect, is certainly THE INFORMATION. The objective of the research is to demonstrate the vulnerabilities and threats presented by WEB services in the intranet of the Technical University of Babahoyo. We determined the weaknesses and attacks present in the network; through direct observation analysis with tests of packet traffic and surveys to network users. It concludes in the lack of procedures in computer security and errors not controlled by attacks and perpetrations. Finishing with the design of an Intrusion Detection System (NDIS).

PALABRAS CLAVE

Seguridad Informática, Amenazas y Ataques de Red, Sistemas de Detección de Intrusos.

KEY WORDS

Computer Security, Network's Menaces and Attacks, Intrusion Detection Systems.

1. INTRODUCCIÓN

Hoy en día, teniendo en cuenta el avanzado ritmo de la tecnología, las empresas e instituciones sean públicas o privadas adoptan medidas de protección y seguridad para preservar su bien más preciado, la información, ya que del mismo modo se han hecho presentes los ataques informáticos e infiltraciones no autorizadas de personal ajeno o mal intencionado para cometer acciones ilícitas o sacar ventaja competitiva.

Es así que las empresas invierten sin escatimar recursos en asesorías y capacitaciones, equipos informáticos, personal preparado y entrenado para afrontar dicho reto y mermar cualquier tipo de irrupción a sus sistemas informáticos. Según (Symantec Corporation, 2015) el 55% de las empresas están reclutando personal en áreas de seguridad informática, un 42% han aumentado los presupuestos de prevención en pérdida de datos y el 45% están aumentando los presupuestos en seguridad Web, redes y puntos finales.

No muy ajena a esta realidad, la Universidad Técnica de Babahoyo (UTB) presenta inconvenientes en su infraestructura tanto al interior como hacia la WAN en materia de seguridad informática. Uno de los aspectos objeto de estudio son las vulnerabilidades y amenazas presentes en la intranet de la institución, orientados a los servicios WEB, siendo necesario evidenciar el uso libre e ilimitado del Internet con acceso a cualquier página web, red social, aplicaciones y sitios de baja confianza, factores que toleran un fácil ingreso e infiltración de personas no autorizadas al interior de la red.

El presente caso de estudio se enfoca en aspectos de seguridad LÓGICA y ACTIVA para la intranet de la universidad, permitiendo evidenciar las falencias en materia de seguridad informática y poner a prueba dichas vulnerabilidades con testeos simples de infiltración a puertos sobre los servicios WEB no controlados de la red TCP/IP, y recomendar un plan de mejora a través del diseño elemental de un Sistema de Detección de Intrusos (NDIS).

2. LA SEGURIDAD INFORMÁTICA

La seguridad informática en la actualidad ya no es una ventaja competitiva entre una empresa y otra, es una necesidad, ya que el avance tecnológico ha permitido también el aumento de la delincuencia informática produciendo perjuicios en las organizaciones por pérdida o mala manipulación de la información.

Según (Symantec Corporation, 2015) “el 95% de empresas sufrió pérdidas debido a ciberataques incluyendo tiempo de inactividad, robo de identidad de clientes y empleados y robo de propiedad intelectual; el 86% de estas pérdidas se traduce en costos reales. Y el 20% de los negocios perdió por lo menos USD \$181,220 como resultado de ciberataques.”

Para evitar y en el mejor escenario minimizar los ataques e infiltraciones no deseadas, es indispensable implementar medidas de protección y seguridad a la infraestructura tecnológica. Adoptar políticas de seguridad informática y diseñar una intranet segura. Solo

es posible, a través de un análisis detallado de los distintos protocolos de seguridad, herramientas tecnológicas y aplicaciones informáticas.

La Universidad Técnica de Babahoyo cuenta con una intranet poco segura, provocando poner en alto riesgo las actividades y procesos informáticos de la institución. Es evidente apreciar la facilidad de acceso para cualquier usuario a la red, poder conectarse al internet y acceder en forma libre e ilimitada a cualquier sitio WEB. Por otro lado, las redes sociales están constantemente disponibles y no existe restricción alguna para ejecutar aplicaciones que puedan conectarse fuera de la red.

Parte del gran problema de accesibilidad y control en la red de la institución radica en la falta de gestión y monitoreo a los diferentes puertos y servicios de la red; ya que no cuenta con una red segura efectiva y protegida contra amenazas y ataques perpetrados al interior como hacia afuera, perjudicando casi en un 80% su infraestructura tecnológica para cualquier incidente.

Los equipos de comunicación se encuentran sobredimensionados y mal configurados, y específicamente el equipo proxy (SOPHOS SG330) no actúa efectivamente sobre la seguridad y protección controlando los puertos de entrada y salida de la intranet.

El propósito del presente Caso de Estudio está orientado a:

Demostrar las vulnerabilidades y amenazas que presentan los servicios WEB en la intranet de la Universidad Técnica de Babahoyo, como factor endeble en materia de seguridad informática.

Las preguntas de reflexión para determinar los problemas de investigación son:

- ¿Cuáles son las medidas de seguridad informática implementadas en la intranet de la UTB para un correcto uso del Internet?
- ¿Qué estados de seguridad presentan los puertos TCP/IP con análisis de tráfico de paquetes usando servicios WEB?

La investigación se desarrolla en el perímetro que conforma la Universidad Técnica de Babahoyo, misma que se encuentra situada en el cantón Babahoyo dentro de la zona urbana. Al ser una entidad del estado ecuatoriano, está sujeta a varias obligaciones y regulaciones, entre una de ellas dicta lo siguiente:

Ley Orgánica de Telecomunicaciones. - Artículo 61. Competencias del Órgano Rector - Corresponde a la Institución de Educación Superior:

9. Formular las políticas y planes para la creación, regulación y supervisión de la central de datos de la institución, intercambio de información por medios electrónicos, seguridad en materia de información e informática, así como evaluación de su ejecución. (ARCOTEL, 2015)

Seguridad Lógica. - La seguridad lógica complementa a la seguridad física, protegiendo el software y los equipos informáticos. Es decir, las aplicaciones y datos de usuarios de robos, pérdida de datos, modificaciones no autorizadas, etc. A continuación, se enumera las principales amenazas y mecanismos para defenderse (Seoane, César & et al., 2013):

Tabla 1. Amenazas y mecanismos de defensa en seguridad Lógica.

AMENAZAS	MECANISMOS DE DEFENSA
ROBOS	<ul style="list-style-type: none"> • Cifrar la información almacenada en los soportes para que en caso de robo no sea legible. • Utilizar contraseñas para evitar el acceso a la información. • Sistemas biométricos (uso de huella dactilar, tarjetas identificadoras, caligrafía).
PÉRDIDA DE INFORMACIÓN	<ul style="list-style-type: none"> • Realizar copias de seguridad para poder restaurar la información perdida. • Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado. • Uso de conjunto de discos redundantes, protege contra la pérdida de datos y proporciona la recuperación de los datos en tiempo real.
PÉRDIDA DE INTEGRIDAD EN LA INFORMACIÓN	<ul style="list-style-type: none"> • Uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp, etc. • Mediante la firma digital en el envío de información a través de mensajes enviados por la red. • Uso de la instrucción del sistema operativo Windows, sfc (system file checker).
ENTRADA DE VIRUS	Uso de antivirus, que evite que se infecten los equipos con programas malintencionados.
ATAQUES DESDE LA RED	<ul style="list-style-type: none"> • Firewall, autorizando y auditando las conexiones permitidas. • Programas de monitorización • Servidores Proxys, autorizando y auditando las conexiones permitidas.
MODIFICACIONES NO AUTORIZADAS	<ul style="list-style-type: none"> • Uso de contraseñas que no permitan el acceso a la información. • Uso de listas de control de acceso. • Cifrar documentos.

Fuente: Seoane, César; et al. 2013.

Seguridad Activa. - La seguridad activa la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos. A continuación, se enumeran las principales técnicas de seguridad activa (Seoane, César & et al., 2013):

Tabla 2. Técnicas de seguridad activa.

TÉCNICA	¿QUÉ PREVIENE?
USO DE CONTRASEÑAS	Previene el acceso a recursos por parte de personas no autorizadas.
LISTAS CONTROL DE ACCESO	Previene el acceso a los Ficheros por parte de personal no autorizado.
ENCRIPCIÓN	Evita que personas sin autorización puedan interpretar la información.
USO DE SOFTWARE DE SEGURIDAD INFORMÁTICA	Previene de virus informáticos y de entradas indeseadas al sistema informático.
FIRMAS Y CERTIFICADOS DIGITALES	Permite comprobar la procedencia, autenticidad e integridad de los mensajes
SISTEMAS DE FICHEROS CON TOLERANCIA A FALLOS	Previene fallos de integridad en caso de apagones de sincronización o comunicación
CUOTAS DE DISCO	Previene que ciertos usuarios hagan un uso indebido de la capacidad de disco

Fuente: Seoane, César; et al. 2013.

2.1. ELEMENTOS QUE ATENTAN LA SEGURIDAD INFORMÁTICA

Entre los elementos que atentan contra la seguridad de las redes de cómputo encontramos las amenazas físicas y lógicas, catástrofes naturales, acciones humanas, entre otras. Un informe de seguridad de Cisco revela que el 77% de los trabajadores desconoce las principales amenazas de seguridad, poniendo en peligro los datos de sus compañías. El empleado resulta ser el eslabón más débil de la cadena por falta de conciencia y desconocimiento (Casas, 2014).

Por otro lado, durante el desarrollo de aplicaciones los programadores suelen dejar puertas abiertas originadas en ocasiones por errores de programación. Si dicha vulnerabilidad se descubriera o filtrara por cualquier intruso, éste puede hacer uso de ella para violar la integridad del sistema. Empresas de seguridad a nivel mundial reportan que los ataques a datos confidenciales mediante el uso de puertas abiertas durante el primer semestre del 2014, aumentó en un 113% (Symantec Corporation, 2015).

2.2. AMENAZAS LÓGICAS

Las amenazas lógicas son todos los programas que de una forma u otra pueden dañar el sistema informático. Se les conoce con el nombre de *malware*, *bugs* o agujeros. Son errores de programación software que pueden comprometer el sistema operativo. A estos errores se les conoce como *bugs* y los programas que aprovechan de estas vulnerabilidades, *exploits*. Estos últimos son muy peligrosos ya que no se necesita de mucho conocimiento para utilizarlos y comprometer un servidor (Ludwin, 2006).

Las bombas lógicas son partes de código de algún programa que permanecen pasivas hasta que son activadas en un determinado momento y ejecutan su tarea destructiva, y los detonadores suelen ser presencia o ausencia de un fichero específico, una fecha concreta, una combinación de teclas, y otras variantes (Ludwin, 2006). Los VIRUS son también secuencias de códigos que se insertan en un fichero ejecutable denominado huésped, de manera que cuando se active el fichero el virus también lo hará, insertándose a sí mismo en otros programas para asegurar su procreación y diseminación. A estos se le unen los caballos de troya, los cuales son instrucciones escondidas en programas de manera que este parezca realizar las tareas que el usuario espera de él, pero en realidad ejecuta funciones ocultas que atentan contra la seguridad. Los caballos de Troya ocultan su intención real bajo la apariencia de un programa inofensivo (Villalón, 2002).

Ataques por envenenamiento IP O ARP (SPOOFING), las relaciones de confianza basadas en direcciones IP pueden ser burladas por *spoofing*, mediante el cual se suplanta la identidad de la máquina en la que se confía. El *spoofing* puede ser IP o ARP cuando el envenenamiento es ARP es más difícil de detectar porque la máquina del intruso funciona de puente entre las estaciones y no se interrumpe la comunicación (Villalón, 2002). El escaneo de puertos funciona a partir de las respuestas de los protocolos (TCP o UDP) como resultado a los intentos de conexión en determinados puertos, pudiendo obtener información acerca de los servicios ofrecidos por los sistemas operativos y las aplicaciones. Una vez conocida la versión de la aplicación, se consiguen sus vulnerabilidades. Casi la totalidad de los sistemas de detección de intrusos son capaces de detectar los escaneos de puertos, el cual no llega a ser un ataque, pero es sin duda la antesala. Como Sistema de Detección de Intrusos basado en Red (NIDS) se recomienda el SNORT, en su versión para Linux. (Villalón, 2002).

3. METODOLOGÍA

Para el presente trabajo las metodologías de investigación que más se articulan son la descriptiva y de campo. Definiendo la problemática que presenta la Universidad Técnica de Babahoyo, en: ¿Qué tipos de vulnerabilidades y amenazas presentan los servicios WEB a la intranet de la Universidad Técnica de Babahoyo en materia de seguridad informática?

Estas metodologías permitirán recolectar información y evidenciar los problemas que presenta la Universidad en materia de seguridad informática, identificando sus vulnerabilidades y amenazas perpetradas a la intranet, emplear las técnicas y herramientas necesarias para comprobar el acceso y conectividad que ejecutan los usuarios de la red, y, adicionalmente, dirigir las guías de observación para el testeo de los puertos TCP/IP.

Para la recolección de la información, los instrumentos más adecuados para llevar a cabo la investigación son: Las encuestas y fichas de observación de campo, los mismos que fueron realizados al personal que trabaja en la Universidad. Para llevar a cabo dichos instrumentos fue necesario calcular la muestra simple de la población total de usuarios en la red matriz de la UTB, según se detalla en la siguiente tabla:

Tabla 3. Cuadro distribución de la población (universo).

Nro.	Descripción	Lugar	Población
1	Usuarios de Red	Campus matriz UTB	406
2	Administradores y Operadores red	Dirección de Sistemas, DataCenter de las facultades	10
3	Autoridades inmediatas	Edif. Administrativo y facultades	4
		TOTAL	420

Fuente: elaboración propia.

La fórmula estadística para el tamaño de la muestra es la aleatoria simple no estratificada, que al emplear permite calcular el tamaño de la muestra simple del universo. Para calcular el tamaño de la muestra suele utilizarse la siguiente fórmula:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Hallando el valor de n:

$$n = \frac{420(0,5)^2(1,96)^2}{(420-1)(0,07)^2 + (0,5)^2(1,96)^2}$$

n = 104 usuarios de red

4. RESULTADOS

Seguidamente, se procede a realizar 104 encuestas en forma aleatoria a docentes y empleados de la Universidad de distintas unidades y facultades, obteniendo en resumen los siguientes resultados:

- 1) ¿Usted como usuario de la red universitaria, trabaja en base a normas y reglamentos en políticas de seguridad informática?

Tabla 4. Respuestas pregunta n. 1.

Indicador	Valor	Porcentaje
Sí	0	0%
No	100	100%

Fuente: elaboración propia.

Gráfico 1. Respuestas pregunta n. 1.
Elaborado por: elaboración propia.

Para la pregunta n. 1 el total de encuestados (usuarios de red) que representa el 100%, afirman no seguir una política de seguridad, ya que la misma no existe.

- 2) ¿Su equipo informático ha tenido ataques de virus?

Tabla 5. Respuestas pregunta n. 2.

Indicador	Valor	Porcentaje
Siempre	19	19%
Casi siempre	43	43%
Rara vez	32	32%
Nunca	6	6%

Fuente: elaboración propia.

Gráfico 2. Respuestas pregunta n. 2.
Elaborado por: elaboración propia.

En la pregunta n. 2, un 43% de usuarios casi siempre tienen ataques de virus, un 32% rara vez y el 19% de usuarios siempre padecen de ataques de virus. Teniendo apenas un 6% nunca han sufrido de ataques siendo la minoría. En consecuencia, tenemos ataques frecuentes de virus y malwares en la red e internet.

- 3) ¿Cuándo hace uso del internet con qué frecuencia se le aparecen ventanas emergentes en el navegador que afectan a su equipo?

Tabla 6. Respuestas pregunta n. 3.

Indicador	Valor	Porcentaje
Siempre	17	17,3%
Casi siempre	71	72,4%
Rara vez	10	10,3%
Nunca	0	0%

Fuente: elaboración propia.

Gráfico 3. Respuestas pregunta n. 3.
Elaborado por: elaboración propia.

En la pregunta n. 3, un 72,4% indican que casi siempre hay presencia de ventanas emergentes, el 17,3% se manifiesta que siempre, y un 10,3% rara vez. En consecuencia, solo pocos usuarios expresan estar conformes con el servicio y la manera de prevenir la presencia de Windows Pop-up's.

- 4) ¿Existe un software especial que gestione la seguridad informática de la red, equipos, sistemas y aplicaciones?

Tabla 7. Respuestas pregunta n. 4.

Indicador	Valor	Porcentaje
Sí	5	50%
No	5	50%

Fuente: elaboración propia.

Gráfico 4. Respuestas pregunta n. 4.
Elaborado por: elaboración propia.

En la pregunta n. 4, la mitad de administradores y operadores de red (50%) emplea algún tipo software que gestione la seguridad y protección de la red; mientras que el otro 50% no lo emplea o desconocen.

- 5) ¿Cuentan con alguna aplicación que monitoree la cantidad de perpetraciones, ataques mal intencionados y errores en la red?

Tabla 8. Respuestas pregunta n. 5.

Indicador	Valor	Porcentaje
Sí	5	55.6%
No	4	44.4%

Fuente: elaboración propia.

Gráfico 5. Respuestas pregunta n. 5.
Elaborado por: elaboración propia.

Para la pregunta n. 5, un 55,6% manifiesta que si tienen una aplicación para monitorear y controlar la red en criterios de seguridad, ataques y perpetraciones, mientras que el otro 44,4% no lo tiene configurado. Por tal razón, se deduce que la red no está totalmente monitoreada y supervisada, dejando todo este ejercicio al departamento de informática de la institución.

4.1. ANÁLISIS DEL TRÁFICO DE PAQUETES PARA COMPROBAR LAS AMENAZAS PRESENTES EN LA INTRANET DE LA UTB

Para proceder con la comprobación de las vulnerabilidades y amenazas que sufre la intranet de la Universidad, se ejecuta el formulario de observación de campo y pruebas in situ. Comenzando por identificar la puerta de enlace que permite la Entrada/Salida de paquetes a la intranet universitaria, para ello se ubica la dirección privada y pública del *gateway* que permite tal tarea siendo en el caso de la UTB, el firewall SOPHOS SG330. Esto se procede realizando una simple consulta de traza y se logra establecer que la IP privada está en el segmento 192.168.0.0/28, mientras que la IP pública asignada es: 181.198.25.129/26.

4.1.1. Análisis de seguridad con inyección de paquetes y puertos no controlados

Para llevar a efecto la ficha de observación y responder las preguntas se ejecutaron programas testeadores de red e inyectores de paquetes para analizar los tipos, tamaños y calidad de los paquetes. Se emplearon los siguientes programas:

- a) **ZenMap GUI:** Es una herramienta gráfica muy amigable que se puede instalar tanto en Linux como en Windows muy fácilmente, ofrece una serie de opciones ya pre configuradas de escaneo, sobre el que únicamente se selecciona el *target* sobre el que se lanzará el escaneo (Corletti E., 2011).

Para esta actividad se utilizará el escaneo de topología y puertos para identificar los puertos de red hábiles y controlados (ver gráfico 7).

Gráfico 7. Testeo al Firewall SOPHOS. ZenMap 6.4.

Elaborado por: elaboración propia.

- b) **Nemesis 1.4.:** Es una herramienta de línea de comandos utilizada para crear aplicaciones personalizadas de IP. Paquetes similares a hping. Puede ser utilizado para crear paquetes TCP y UDP también, pero también ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF y RIP también; ósea permite inyectar gran cantidad de paquetes a una red determinada (Andy Wood, 2013).

```
dolavinus:src/projects/nemesis/nemesis-1.4beta2/src$ ./nemesis tcp -vv
(dolavinus):nemesis/nemesis-1.4beta2/src$ 77: ./nemesis tcp -vv 16:48:30

TCP Packet Injection -- The NEMESIS Project Version 1.4beta2 (Build 14)

      [IP] 18.198.226.12 > 36.204.185.43
      [IP ID] 14570
      [IP Proto] TCP (6)
      [IP TTL] 255
      [IP TOS] 0x00
      [IP Frag offset] 0x0000

      [TCP Ports] 27744 > 53
      [TCP Flags] SYN
      [TCP Urgent Pointer] 0
      [TCP Window Size] 4096
      [TCP Seq number] 1662480531

      [Hexdump]
      45 00 00 28 38 EA 00 00 FF 06 00 00 12 C6 E2 0C E..(88..ü....kâ.
      24 CC B9 2B 6C 60 00 35 63 17 70 93 58 02 11 74 $i^+l`.5c.p.X..t
      50 02 10 00 23 62 00 00 P...#b..

Wrote 40 byte TCP packet.

TCP Packet Injected
(dolavinus):nemesis/nemesis-1.4beta2/src$ 78: 16:48:36
```

Gráfico 8. Inyección de Paquetes con Nemesis 1,4.

Elaborado por: elaboración propia.

- c) **SmartSniff:** Es una herramienta de análisis de redes / dignostic que le permite capturar paquetes TCP / IP que pasan a través de su adaptador de red. Puede ver los datos capturados como secuencia de conversaciones entre clientes y servidores en modo ASCII (para protocolos basados en texto, como HTTP, SMTP, POP3 y FTP) o como volcado hexadecimal (para protocolos no basados en texto, como DNS) (portablefreeware, 2017).

Gráfico 9. Prueba de Ataques y Perpetraciones a la RED-UTB. ZenMap 6.4.

Elaborado por: elaboración propia.

El Gráfico 9, visualiza el reporte del análisis de ataques y perpetraciones de paquetes de prueba desde una IP pública 18.198.226.12, usando el programa NEMESIS 1,4. Obteniendo los siguientes resultados (Vega, 2015):

- 36 paquetes peligrosos de 2044 enviados.
- 4 puertos no controlados y cerrados por el firewall SOPHOS.
- No hay control de paquetes por http, no existe aplicaciones.
- No existen puertos seguros controlados para https, ftps, etc.
- No hay resolución de nombres a direcciones IP's privadas establecidas.
- Ausencia de DNS, no existe control de dominio.

4.2. DISEÑO DE UN SISTEMA DE DETECCIÓN DE INTRUSOS

Para proteger la infraestructura informática de la UTB, se puede acoger al siguiente diseño de Detección de Intrusos a la intranet universitaria.

Para proteger los sistemas informáticos se debe realizar un análisis de las amenazas potenciales, pérdidas que se podrían generar y probabilidad de ocurrencia. A partir de este análisis se diseñan políticas de seguridad que defina reglas y responsabilidades para evitar amenazas y minimizar sus efectos los mismos que se dividen en tres grandes grupos, Prevención, Detección Y Recuperación (Villalón, 2002).

El NIDS (Gráfico 10), debe ser implementado en un punto donde sea capaz de analizar todo el tráfico de la red y equipos que se desea proteger. En la situación de la Universidad caso de estudio, es necesario implementar el equipo servidor NDIS junto al proxy SOPHOS (firewall de la gráfica) de la institución. Tal como detalla la gráfica 10, vendría a ubicarse en la zona verde de protección tanto de entrada como salida de la intranet.

Gráfico 10. Zonas de un IDS dentro de una organización.

Fuente: elaboración propia.

5. CONCLUSIONES

- Se determinó que en la intranet de la Universidad Técnica de Babahoyo existen debilidades e incoherencias en las configuraciones de red, ya que no todos los puertos TCP/IP están controlados, no existe un monitoreo detallado de cada una de las subredes y el tráfico de red que hay en cada una de ellas.
- No existe un software específico que gestione las actividades de seguridad informática y gestione eficientemente las conexiones de usuarios de red y monitoree los accesos y usos de internet; provocando que exista libre acceso a sitios no seguros.
- Con la recolección de información de los usuarios y administradores de red, se pudo evidenciar la falta de procedimientos de seguridad en sus equipos informáticos, la carencia de herramientas que ayuden a controlar y supervisar el acceso a los servicios de la intranet, presencia de malwares y ataques constantes de virus, e información basura no deseada para los usuarios.
- No existe una adecuada administración en la infraestructura tecnológica confinando el trabajo al Firewall de Hardware, **SOPHOS** para la interceptación de intrusos y control de accesos; misma que se encuentra parcialmente operativa al estar bloqueada por la falta de licenciamiento y el no poder acceder a él para ser configurado adecuadamente.
- Se recomienda tomar en cuenta las observaciones y tomar las medidas necesarias en materia de seguridad informática, implementar una aplicación NDIS (Sistemas de Red para Detección de Intrusos) y un portal cautivo para acceso de usuarios a los servicios WEB.

5. REFERENCIAS BIBLIOGRÁFICAS

- Andy Wood. (Enero de 2013). *ANDY WOOD | Security Professional*. Obtenido de Auditing Firewalls via Packet Crafting with HPing and Nemesis: <<https://entsecarch.files.wordpress.com/2014/05/auditing-firewalls-via-packet-crafting-with-nemesis-and-hping-public.pdf/>>.
- ARCOTEL, A. d. (2015). *Ley Organica de Telecomunicaciones*. Quito: Registro Oficial Suplemento 439.
- Casas, A. (30 de octubre de 2014). *Revista Digital CSO Computerworld*. Recuperado el 15 de abril de 2015, de CSO Computerworld: <<http://cso.computerworld.es/seguridad-en-cifras/>>.
- Corletti E., A. (2011). *Seguridad por Niveles*. Madrid: DarFE Learning Consulting .
- Ludwin, M. (2006). *The Little Black Book of Computer Virus*. Arizona, American: Eagle publications, Inc.
- portablefreeware. (6 de marzo de 2017). *PORTABLEFREWARE*. Obtenido de SmartSniff v2.27: <<https://www.portablefreeware.com/?id=781/>>.
- Ramos, R. & Gallegos, E. (2016). Infección con ransomware en el servidor de base de datos del sistema Onsysytec ERP. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 5(4), 56-76. DOI: <<http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.56-76/>>
- Seoane, C. & et al. (2013). *Seguridad informática*. Madrid: McGraw-Hill.
- Symantec Corporation. (20 de enero de 2015). *Symantec Internet Security Corporation*. Recuperado el 20 de abril de 2015, de Symantec Internet Security Threat Report: <http://www.symantec.com/security_response/publications/threatreport.jsp/>.
- Vega, G. (2015). *Seguridad informática y métodos de protección en infraestructuras tecnológicas y su incidencia en la intranet de la Universidad Técnica de Babahoyo, año 2015". Diseño de una infraestructura tecnológica segura*. Quevedo: UTEQ.
- Villalón, A. (2002). *Seguridad en Unix y Redes*. Valencia: Universidad Politécnica de Valencia.

CONSEJO EDITORIAL

COMPONENTES	
Director	Víctor Gisbert Soler
Editores adjuntos	María J. Vilaplana Aparicio
	Inés Poveda Pastor
	Vicente Sánchis Rico
Editores asociados	David Juárez Varón
	F. Javier Cárcel Carrasco

COMITÉ CIENTÍFICO TÉCNICO

ÁREA TEXTIL	Prof. Dr. Josep Valldeperas Morell Universidad Politécnica de Cataluña España
ÁREA FINANCIERA	Prof. Dr. Juan Ángel Lafuente Luengo Universidad Jaume I; Castellón de la Plana España
ORGANIZACIÓN DE EMPRESAS Y RRHH	Prof. Dr. Francisco Llopis Vañó Universidad de Alicante España
ESTADÍSTICA; INVESTIGACIÓN OPERATIVA	Prof. Dra. Elena Pérez Bernabéu Universidad Politécnica de Valencia España
DERECHO	Prof. Dra. María del Carmen Pastor Sempere Universidad de Alicante España
INGENIERÍA Y TECNOLOGÍA	Prof. Dr. David Juárez Varón Universidad Politécnica de Valencia España
TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN	Prof. Dr. Manuel Llorca Alcón Universidad Politécnica de Valencia España

tecnología