

Brindar soluciones tecnológicas personales y empresariales como una necesidad para incrementar la Cultura de Seguridad Informática

Provide personal and business technology solutions as a need to increase the Information Security Culture

BARROSO-BARAJAS, Alfonso José†*, VILLAGRAN-VIZCARRA, Dafnis Cain, RAMÍREZ-OCHOA, Dynhora Danheyda y CÓRDOVA-VILLEGAS, Perla Cristina

Universidad Tecnológica de Chihuahua

ID 1^{er} Autor: *Alfonso José, Barroso-Barajas* / ORC ID: 0000-0002-5353-5987, Researcher ID Thomson: 3133-2018, CVU CONACYT ID: 521749

ID 1^{er} Coautor: *Dafnis Cain, Villagran-Vizcarra* / ORC ID: 0000-0001-5611-9834, Researcher ID Thomson: 3134-2018, CVU CONACYT ID: 953360

ID 2^{do} Coautor: *Dynhora Danheyda, Ramírez-Ochoa* / ORC ID: 0000-0002-1326-908X, Researcher ID Thomson: 3130-2018, CVU CONACYT ID: 521748

ID 3^{er} Coautor: *Perla Cristina, Córdoba-Villegas* / ORC ID: 0000-0002-0527-4831, Researcher ID Thomson: 3091-668, CVU CONACYT ID: 171313

DOI: 10.35429/JCT.2019.8.3.1.5

Recibido 10 de Enero, 2019, Aceptado, 30 de Marzo, 2019

Resumen

En la actualidad la cantidad de ataques cibernéticos van en aumento siendo la carencia de la cultura de la seguridad informática la causa principal de ellos, así como la dificultad de encontrar información centralizada, clara y práctica para el personal, generando que se ponga en riesgo los controles de accesos y se creen vulnerabilidades y se exponga información de relevancia, tanto personal como de la compañía. Es por ello la importancia de tener un lugar en el que se brinde apoyo, se encuentre la información concentrada y ofrezcan respuestas para incrementar la seguridad informática, utilizando un formato que sea digerible para todas las personas que accedan a dicha información. Así como una herramienta empresarial en la que detecte las vulnerabilidades y amenazas, brindando propuestas de soluciones tecnológicas. Objetivos: Reducir los riesgos de inseguridad impulsados mediante una cultura de seguridad informática para garantizar la confidencialidad, integridad, rapidez y disponibilidad de la información. Analizar vulnerabilidades de seguridad que pudiesen existir en el manejo de la información y sistemas que afecten de manera personal o profesional. Establecer mecanismos de sensibilización para el personal sobre temas de seguridad informática. Centralizar la información del tema de seguridad informática a través de un sitio web que sirva para la difusión de las técnicas de prevención de ataques y posibles soluciones a vulnerabilidades de seguridad informática. Agilizar la aplicación de encuestas a través de una app que sirva para brindar soluciones tecnológicas a las instituciones que se encuesten. Metodología: El proyecto está basado en la investigación comprensiva, ya que se explican las vulnerabilidades y amenazas que puedan ocurrir, predicen el riesgo e impacto que generará y proponen una solución para elevar el grado de seguridad informática. Realizando una investigación hipotético-deductiva en la cual se describen los procesos administrativos que se llevan a cabo dentro de las empresas y aquellos que son planeados en el objetivo de estudio se pretende demostrar que una cultura informática puede reducir los riesgos de seguridad en una empresa y en la sociedad. Las técnicas de investigación que se utilizan son las de cuestionarios, para ello se diseñó una serie de preguntas para determinar la seguridad informática a nivel usuario. Contribución: Se desarrolla una aplicación móvil para realizar las encuestas mostrando estadísticas en gráficas para poder así brindar soluciones tecnológicas a las empresas con las que se trabaje, de tal forma que los datos estadísticos se vean reflejados en una de las secciones del sitio web desarrollado, que además cuenta con tips, técnicas y metodologías para incrementar la seguridad en los hogares y en las empresas.

Seguridad Informática, Cultura Informática, Tecnologías

Abstract

Currently, the number of cyber-attacks is increasing because of the lack of culture of computer security. This is the main cause of this problem. Apart from this, there is a difficulty of finding centralized, clear and practical information for the staff, thus it generates the risk of access controls and vulnerabilities so personal data and company's information is exposed. That is why it is important to have a place where support is provided, the information is concentrated and offers answers to increase computer security, using a format that is clear enough for all people who access to such information. This is also a business tool that detects vulnerabilities and threats, offering proposals for technological solutions. Objectives: To reduce the risks of insecurity through a Culture of Information Security to guarantee the confidentiality, integrity, speed and availability of information. To analyze security vulnerabilities that may exist in the management of information and systems that affect personally or professionally. To establish awareness mechanisms for staff on IT security issues. To centralize information on the topic of computer security through a website that serves to disseminate attack prevention techniques and possible solutions to computer security vulnerabilities. To streamline the application of surveys through an app that serves to provide technological solutions to the institutions that are surveyed. Methodology: The project is based on comprehensive research, since it explains the vulnerabilities and threats that may occur, predicting the risk and impact that it might generate as well as proposing a solution to increase the degree of computer security. Carrying out a hypothetical-deductive research describing the processes performed and those that are planned in the objective of study, it is pretended to demonstrate that a computer culture can reduce the risks of security in a company and in the society. The type of research techniques used are questionnaires, for this reason series of questions are designed to determine the computer security at the user level. Contribution: A mobile application is developed to carry out the surveys showing statistics in graphs in order to provide technological solutions for the companies. Therefore, the statistical data is reflected on one of the sections of the website developed, where also shows tips, techniques and methodologies to increase security in homes and businesses.

Computer security, Computer Culture, Technologies

Citación: BARROSO-BARAJAS, Alfonso José, VILLAGRAN-VIZCARRA, Dafnis Cain, RAMÍREZ-OCHOA, Dynhora Danheyda y CÓRDOVA-VILLEGAS, Perla Cristina. Brindar soluciones tecnológicas personales y empresariales como una necesidad para incrementar la Cultura de Seguridad Informática. Revista de Tecnología Informática. 2019. 3-8: 1-5

* Correspondencia del Autor (Correo electrónico: abarroso@utch.edu.mx)

† Investigador contribuyendo como primer autor.

Introducción

El siguiente artículo expone la necesidad de contar con herramientas tecnológicas que brinden soluciones que impacten en la vida de las personas y de las instituciones, incrementando su cultura en seguridad informática y de esta manera reducir los riesgos y vulnerabilidades a los que nos enfrentamos día con día debido a la creciente inseguridad cibernética.

El siguiente trabajo presenta los resultados de la tercera etapa del proyecto, el cual tiene como objetivo el desarrollar dos aplicaciones que ayuden a detectar y analizar ataques así como vulnerabilidades de seguridad, resolviendo y proporcionando soluciones tecnológicas de lo detectado por nuestras herramientas o por otras externas.

Este trabajo es producto de dos etapas anteriores en la que se realizó un análisis de seguridad en los procesos críticos de unas empresas, en la que se identificaron riesgos y se determinó las acciones que deben llevarse a cabo para mejorar la seguridad informática de las instituciones (Ramírez Ochoa, Barroso Barajas, Siqueiros García, & Villagran Vizcarra, 2017). Y en la etapa en la que se elaboró el contenido de las capacitaciones para el personal para el manejo de la información y de esta manera reducir los riesgos de seguridad (Villagran Vizcarra, Ramírez Ochoa, Barba Martínez, & Barroso Barajas, 2018).

Justificación

En el 2018 en México se recibieron 1.5 millones de ataques cibernéticos al día (Forbes Staff, 2018) y se considera que el año 2019 puede ser pronosticado como el “año del ciberataque” donde 9 de cada 10 empresas en el mundo serán presa de los ataques cibernéticos (RealNet, 2019). Por lo que estar protegido debe ser una prioridad para las empresas y no es una tarea sólo de ellas, sino para todas las personas que utilicen alguna tecnología digital.

Algunas empresas se protegen con equipo especializados, las cuales se vuelven inútiles con la falta de una cultura de seguridad informática del personal, poniendo en riesgo su información y la de la empresa.

La falta de una cultura de seguridad informática se debe a que los contenidos de seguridad no tiene niveles o clasificaciones por lo que para algunos usuarios son muy especializados y les resultan difíciles de interpretar o muy básicos (para los expertos) que les resultan aburridos. Además de que la información se encuentra distribuida en varios sitios web y en algunos casos se encuentra desactualizada, algunas de las páginas de seguridad mencionan los ataques y vulnerabilidades a los que se encuentran expuestos los usuarios con una solución casi insignificante o muy poca información de las herramientas que se deben de tener (sin explicar los beneficios de usarlo y desventajas por no tenerlo).

Equipamientos, metodologías y herramientas utilizadas

Metodología del desarrollo de software

Para la realización del proyecto se utiliza la metodología ágil *Scrum* la cual se emplea para administrar las actividades que cada miembro del equipo debe realizar y establecer los límites de tiempos de las entregas; esto se logra debido a las categorías que se manejan: Por hacer, haciendo y hecho.

Para poder implementar esta metodología se hace uso de la herramienta llamada *Trello*, la cual apoya el trabajo colaborativo, llevando un seguimiento del proyecto de manera virtual, haciendo que todos los integrantes del equipo tengan acceso por diversas herramientas tecnológicas a las actividades asignadas, teniendo recordatorios de las metas a lograr y porcentajes de actividades terminadas (Atlassian, 2019).

Aplicación móvil y sitio web

Para el desarrollo de la aplicación móvil se requiere del uso del entorno de desarrollo *Android Studio*, por ser una herramienta rápida y el IDE oficial de Google para la creación de aplicaciones en Android empleando el lenguaje de programación JAVA (Developers, 2019), así como se emplea el framework *Bootstrap* para desarrollar con HTML, CSS y JS componentes front-end (Bootstrap, 2019) y se usa *JSON* para el intercambio de datos entre los lenguajes (JSON, 2019).

En la realización del sitio web se optó por utilizar *HTML* y *PHP* por ser una multiplataforma de código abierto para el desarrollo de páginas dinámicas. Donde *PHP* es el lenguaje del servidor y envía el resultado al cliente en formato *HTML* que permite estructurar la información en el navegador (*PHP*, 2019) y se maneja un servidor web *Apache HTTP server* que es gratuito y confiable (*Apache Software Foundation*, 2019).

Para almacenar la información se emplea el sistema de gestión de base de datos *MySQL* (*MySQL*, 2019) y *Firebase* para las funciones de estadísticas y evitar fallas en la comunicación (*Firebase*, 2019).

El uso de la herramienta *GIT HUB* fue fundamental para el trabajo en equipo debido a que es una herramienta *SaaS* (*Software as a Services*) el cual ayuda a llevar un registro y control de los cambios que se realizan sobre el código de los proyectos (*github*, 2019).

Y se utiliza como servidor físico un sistema operativo *CentOS ver7* por su elevado nivel de seguridad que maneja en la detección de vulnerabilidades (*IONOS*, 2017).

Aplicación móvil y sitio web

El sitio web final cuenta con un menú con cinco opciones para navegar por él:

1. Inicio: donde se encuentra la descripción del sitio web.
2. Nosotros: contiene la planeación normativa, historia y organigrama de del comité de seguridad informática.
3. Incidentes: contiene las noticias más relevantes de seguridad informática y las estadísticas generales que arroja la aplicación móvil.
4. Amenazas: Apartado en el que se explican algunas de las amenazas que se pueden evitar y herramientas que ayudarán evitar, corregir o incrementar la seguridad de la información y/o equipo.
5. Divulgación: sección de libros, artículos, infografías y videos acerca de la seguridad informática.

Además el sitio web cuenta con un inicio de sesión para os administradores que serán los que editen y alimentan las secciones.

La aplicación móvil cuenta con un diseño simple, que principia con inicio de sesión para acceder a las funciones de la aplicación (acceso o registro), una vez ya dentro de la aplicación aparece la sección de cuestionarios (crear, borrar o modificar) y posterior se encuentra la sección para crear las preguntas que contendrá el cuestionario.

Una vez creadas los cuestionarios se tendrá listo para poder realizar la recolección de información en las empresas o instituciones que se visitan.

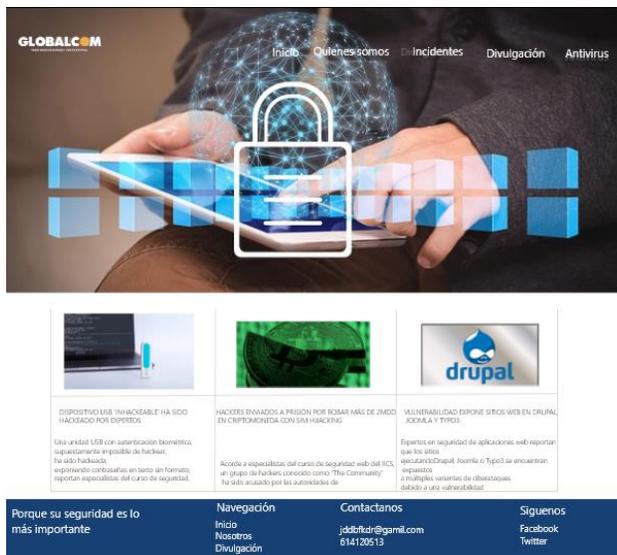


Figura 1 Pantalla del sitio web y Autor Naylea Tinajero (documento de estadías may-ago 2019, UTCH)

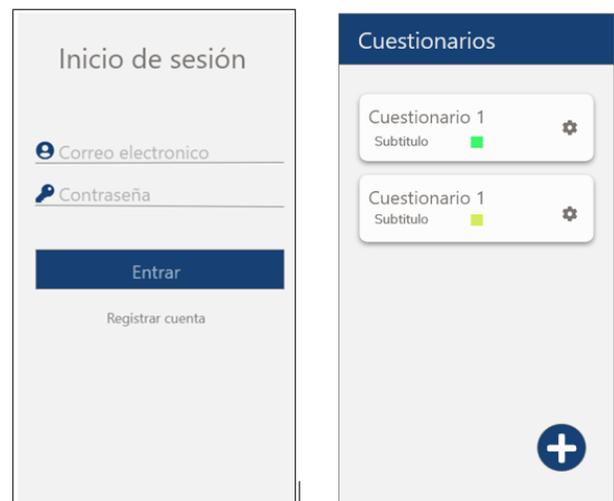


Figura 1 Pantallas de la app móvil y Autor Alejandro Delgado (documento de estadías may-ago 2019, UTCH)

Teniendo la información recolectada y almacenada en la base de datos, se podrá realizar de manera más rápida y eficiente los reportes que se entregarán a cada una de las empresas encuestadas, los cuales contienen las soluciones tecnológicas para las vulnerabilidades y amenazas que se encuentren.

Así mismo se generan estadísticas generales para que estas sean visualizadas en el sitio web, manteniendo la confidencialidad de la información proporcionada por las empresas encuestadas.

Resultados

En esta parte del proyecto se ha desarrollado una aplicación móvil la cual agilizará la recolección de información de las vulnerabilidades y amenazas de las empresas e instituciones en la cual podemos realizar la recolección de la información de manera más rápida, confiable y eficiente.

Y al mismo tiempo podemos ayudar a la sociedad en general a través del sitio web se muestran estadísticas generales del levantamiento de información que se tiene, así como tips, noticias, capacitaciones y consultorías de herramientas y metodologías de seguridad informática que ayudarán a fortalecer una cultura de seguridad informática.

Agradecimiento

Agradecemos al Ing. Ernesto García Cota dueño de la empresa «Globalcom Internacional, S.A. de C.V.» por su apoyo para la realización de este proyecto, ya que durante estos dos años nos ha ayudado con conocimiento, instalaciones y equipamiento para la publicación de las aplicaciones.

Al cuerpo académico «Servicios integrales para el desarrollo empresarial» que nos han ayudado con la realización de la planeación normativa del comité que se está creando.

También agradecemos a los maestros Ivonne Siqueiros y Daniel León que han sido colaboradores y parte importante de este proyecto.

Así mismo agradecemos la ayuda de los alumnos Naylea Tinajero y Alejandro Rocha, los cuales ayudaron en la base para el desarrollo de las aplicaciones.

Y la Universidad Tecnológica de Chihuahua por el apoyo para la realización de las diversas fases y actividades del proyecto por medio del cuerpo académico «Tecnologías de seguridad Informática».

Conclusiones

En esta etapa del proyecto se han logrado desarrollar las herramientas que nos ayudarán a automatizar procesos y así brindar de manera más rápida la información a las empresas. Pero aún se tiene planes para continuar con este trabajo el cual incluye la formalización del comité de seguridad informática el cual tiene como base al cuerpo académico «Tecnologías de seguridad informática» y la empresa «Globalcom Internacional, S.A. de C.V.».

La misión de este comité será “ayudar a las organizaciones a proteger la información para la sistematización de procesos mediante la capacitación, asesoría e implementación de herramientas que favorezcan su permanencia en el mercado”.

Referencias

Apache Software Foundation. (2019). *APACHE*. Obtenido de HTTP Server Project: <https://httpd.apache.org/>

Atlassian. (30 de Abril de 2019). *Trello*. Obtenido de Trello le permite trabajar de forma más colaborativa y ser más productivo: https://trello.com/es/?&aceid=&adposition=1t4&adgroup=66473930365&campaign=1740089219&creative=338995137250&device=c&keyword=trello%20com&matchtype=b&network=g&placement=&ds_kids=p42165194695&ds_e=GOOGLE&ds_eid=700000001550057&ds_e1=GOOGLE&gclid=EA1aIQobCh

Bootstrap. (2019). *Bootstrap*. Obtenido de <https://getbootstrap.com/>

Developers. (2019). *Developers*. Obtenido de Android Studio: <https://developer.android.com/studio>

Firestore. (2019). *Firestore*. Obtenido de <https://firebase.google.com/>

Forbes Staff. (16 de abril de 2018). *Forbes*. Obtenido de Mexicanos reciben 1.5 millones de ataques cibernéticos al día: <https://www.forbes.com.mx/mexicanos-reciben-1-5-millones-de-ataques-ciberneticos-al-dia/>

github. (2019). *github*. Obtenido de Built for developers: <https://github.com/>

IONOS. (21 de noviembre de 2017). *Digital Guide*. Obtenido de ¿Qué es CentOS? Versiones CentOS y requisitos del sistema: <https://www.ionos.mx/digitalguide/servidores/known-how/que-es-centos-versiones-y-requisitos-del-sistema/>

JSON. (2019). *Introducing JSON*. Obtenido de <https://www.json.org/>

MySQL. (2019). *MySQL*. Obtenido de 1.3.1 What is MySQL?: <https://dev.mysql.com/doc/refman/5.5/en/what-is-mysql.html>

PHP. (2019). *PHP y HTML*. Obtenido de <https://www.php.net/manual/es/faq.html.php>

Ramírez Ochoa, D. D., Barroso Barajas, A. J., Siqueiros García, M. I., & Villagran Vizcarra, D. C. (Diciembre de 2017). The computer security culture reduces the risk of information loss and leakage. *Journal-Schools of economic thought and Methology*, 1(1), 29-35. Recuperado el Julio de 2019, de http://www.rinoc.org/revistas/Journal_Schools%20of_economic_thought_and_Methology/vol1num1/Journal_Schools%20of_economic_thought_and_Methology_V1_N1_4.pdf

RealNet. (2019). *RealNet*. Obtenido de 2019 el año de los ciberataques: <https://www.realnet.com.mx/noticias/notas/nota.php?t=2019-el-ao-de-los-ciberataques&id=1652>

Villagran Vizcarra, D. C., Ramírez Ochoa, D. D., Barba Martínez, C., & Barroso Barajas, A. J. (Diciembre de 2018). Importancia de la capacitación del personal a través de una cultura de seguridad informática. *Revista de Tecnologías de la Información y Comunicaciones*, 2(5), 11-5. Recuperado el Julio de 2019, de http://www.ecorfan.org/spain/researchjournals/Tecnologias_de_la_Informacion_y_Comunicaciones/vol2num5/Revista_de_Tecnologia_de_la_Informacion_y_Comunicaciones_V2_N5_3.pdf