Importancia de fomentar la seguridad en el smartphone

José Antonio-Navarrete Prieto, Hilda-Díaz Rincón, Iliana Gabriela-Laguna López de Nava

[a] Tecnológico Nacional de México/ Instituto Tecnológico de Tlalnepantla, Profesor de tiempo completo, Perfil Deseable, Responsable Cuerpo Académico" Ciencia, Tecnología Innovación y Sociedad", Doctor en Planeación Estratégica y Dirección de Tecnología, posgrado_ittla@yahoo.com.mx, Tlalnepantla de Baz, Edo. México, México
[b] Tecnológico Nacional de México/ Instituto Tecnológico de Tlalnepantla, Profesora de tiempo completo, Maestra en Planeación Estratégica y Dirección de Tecnología, Perfil Deseable, Jefa de Proyectos de Vinculación del Depto. de Sistemas y Computación, c_computo_sie@hotmail.com, Tlalnepantla de Baz, Edo. México, México
[c] Tecnológico Nacional de México/ Instituto Tecnológico de Tlalnepantla, Profesora de tiempo completo, Perfil Deseable, Coordinadora de Tutorías del Depto. De Sistemas y Computación, ilianaxim@hotmail.com, Tlalnepantla de Baz, Edo. México, México

Resumen

Actualmente el usuario utiliza en un 73% el smartphone para acceder a redes sociales y considerando el rápido crecimiento del ciberespacio constituido por el Internet y el elevado aumento de los delitos informáticos el cuerpo académico de "Ciencia, Tecnología, Innovación y Sociedad", realiza pláticas de principios básicos de ciberseguridad en el uso del smartphone dentro del Instituto Tecnológico de Tlalnepantla, durante los cuales los estudiantes muestran interés sobre el uso de herramientas de ciberseguridad, ya que se les indican las principales medidas de seguridad desde configuración de su smartphone, instalación de antivirus, como realizar una VPN (Virtual Private Network) y junto con ello se le fomenta la concientización del uso de este a través de mostrar casos y datos estadísticos actuales de los incidentes de seguridad más comunes en el uso del smartphone.

Palabras clave— ciberseguridad, concientizar, educación, Universidad

Abstract

Currently the user uses 73% of the smartphone to access social networks and considering the rapid growth of cyberspace constituted by the Internet and the high increase in computer crime, the academic body of "Science, Technology, Innovation and Society" conducts talks on basic principles of cybersecurity in the use of the smartphone within the Technological Institute of Tlalnepantla, during which students show interest in the use of cybersecurity tools, as they are told the main security measures from configuration of your smartphone, installation of antivirus, such as performing a VPN (Virtual Private Network) and together with it promotes awareness of the use of this through showing cases and current statistical data of the most common security incidents in the use of the smartphone..

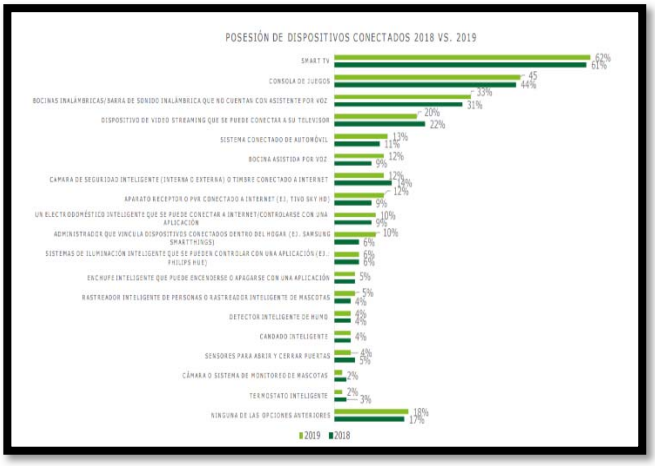
Keywords*— awareness, cybersecurity, education, University*

1. INTRODUCCIÓN

Dentro del Informe de ciberseguridad 2019 realizado por la Secretaría de Comunicaciones y Transportes (SCT), menciona que en la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la información en los Hogares [6] (ENDUTIH) 2017 indica que en México hay, al menos, 71.3 millones de usuarios de Internet, que representan el 63.9% de la población de seis años o más. El crecimiento total de usuarios en México, del 2015 al 2016, fue de 4.7% y, del 2016 al 2017, fue de 8.1%. De acuerdo con la tendencia creciente en el número de usuarios es preponderante una atención inmediata a los aspectos de ciberseguridad. Si a esto se agrega que, entre las principales actividades de los usuarios de Internet en México, de acuerdo con la ENDUTIH, se encuentran la obtención de información (96.9%), entretenimiento (91.4%), comunicación (90.0%), acceso a contenidos audiovisuales (78.1%) y acceso a redes sociales (76.6%) actividades en las cuales se puede intercambiar información sensible

Deloitte [2] muestra que actualmente el número de aparatos que pueden ser conectados a internet y manejados desde un dispositivo móvil va en aumento. La encuesta muestra que la adquisición de "dispositivos para el hogar que cuentan con conexión a internet" ha aumentado. El dispositivo "conectado" más utilizado es la Smart TV, ya que encontramos que 62% de los encuestados cuentan con una. Hay dispositivos con una penetración pequeña, pero que prometen crecer, como los rastreadores de mascotas y personas cuyo uso ha ido aumentando paulatinamente de 4% en 2018 a 5% en 2019, como se muestra en la Gráfico 1.

Gráfico.1 Posesión de dispositivos conectados 2018 vs 2019



Fuente: Estudio: Hábitos de los consumidores móviles en México, 2019 [2]

En el actual mundo globalizado cualquier persona desde un niño hasta un adulto, su mundo gira alrededor de las comunicaciones y en caso de las nuevas generaciones es el uso de teléfono móvil al cual se está conectado las 24 horas del día, utilizando casi la totalidad del tiempo el internet ya sea consultando redes sociales o haciendo uso de diversas aplicaciones las cuales que no siempre contienen información de valor y que en un momento dado pueden estar poniendo en riesgo su información que manejan.

Hoy en día en el smartphone se lleva todo tipo de información, tanto personal (fotos, conversaciones, datos bancarios, etc..) como de trabajo, información muy valiosa para el propietario del smartphone, pero mucho más para todo aquel que quiera infiltrarse dentro de su dispositivo, es por ello que el cuerpo Académico "Ciencia, Tecnología, Innovación y Sociedad" realiza pláticas de concientización que implica educar al recurso humano en torno a la seguridad del uso del smartphone como un primer acercamiento, debido a la moda actual de la utilización de estos dispositivos, la cual ha hecho que los ciberdelincuentes lo vean como un "nicho de mercado a explotar", ya que los dispositivos móviles se han convertido en uno de los focos principales para realizar ataques informáticos, debido a que el usuario al utilizarlo en la mayoría de los casos está regalando una gran cantidad de información a los gigantes de Internet, como Google y Facebook cediéndoles en todo momento además de información personal, la ubicación de los lugares que visita ya que al utilizar las aplicaciones y el navegador está cediendo la información a través del dispositivo.

[3] resaltan la importancia de la capacitación a los usuarios, pues sin importar sus buenas intenciones o las nuevas tecnologías que usen, los seres humanos siempre son el eslabón más débil en la cadena de protección a los datos. [2], además, considera que la concientización es clave en la batalla contra los intrusos y aconseja realizar evaluaciones periódicas entre los usuarios para determinar si reconocen vulnerabilidades potenciales, para de esta manera actuar en consecuencia y mejorar la seguridad informática de una organización. De acuerdo con [4], los programas de concientización en seguridad informática son herramientas útiles para educar a los usuarios de medios informáticos acerca de las conductas que se esperan de ellos, de las acciones que deben realizar en determinados escenarios y de las consecuencias de no seguir las reglas establecidas En INCIBE(2019) [7] indican que la tecnología asociada a dispositivos móviles, como smartphones, tabletas, relojes inteligentes u ordenadores portátiles, ha avanzado mucho en las últimas décadas. Teléfonos con pantallas plegables, flexibles o dobles, gran capacidad de almacenamiento, resoluciones de alta definición, cargas inalámbricas de la batería, procesadores, varias cámaras integradas, sensores faciales, etc., son características impensables hace tan solo unos pocos años.

En la nueva era digital, los Smartphones, las aplicaciones de mensajería y las redes sociales han ido creciendo en popularidad dentro de las aulas, ganando cada vez más adeptos y convirtiéndose en elementos imprescindibles para el día a día de los escolares. De acuerdo con un informe de McAfee, el 86% de los estudiantes utiliza su dispositivo móvil al menos una hora al día mientras están en clase. Además, el 45% de los alumnos consulta sus redes sociales en horas lectivas.

Para este trabajo se utilizó el método de investigación descriptiva, sin ninguna manipulación o modificación de los hechos y de la información investigada, basándose únicamente en la descripción de su ocurrencia, incluyendo la investigación documental. Como un estudio descriptivo se obtuvo información acerca del fenómeno objeto del estudio, describiendo la situación e identificando sus diferentes elementos [5].

También [3] Indica que hoy en día, la relación entre las personas y la tecnología es más intensa que nunca. Esta ha ido evolucionando a pasos agigantados y esto ha influido en el estilo de vida de los usuarios, quienes sienten la necesidad de estar "conectados" en todo momento, por lo que a muchos les resulta indispensable tener su dispositivo móvil a la mano. De acuerdo con la encuesta, el dispositivo que presenta mayor frecuencia de uso es el smartphone, con 96% de los encuestados, mostrando que es una herramienta para la comunicación personal, el trabajo, la escuela y la salud física, entre muchas otras actividades. El siguiente dispositivo con mayor frecuencia de uso es la laptop: 70% de los encuestados la usan diariamente, seguido de la computadora de escritorio con 62%. En el extremo, vemos que 19% de los consumidores que poseen lentes de realidad virtual los usan a diario. Por otro lado, el 5% de los usuarios que poseen una fitness band, nunca lo han utilizado. Los resultados sugieren una fuerte dependencia hacia los dispositivos tecnológicos.

2. CONTENIDO

Las pláticas de ciberseguridad se realizaron con estudiantes de segundo semestre de la carrera de Ingeniería en Tics (ITICS) y de Ingeniería en Gestión Empresarial (IGE), turno matutino, en el período correspondiente a Enero-Junio del 2019, se tuvo una participación 16 estudiantes de ITICS y 28 de IGE.

Estas primeras pláticas se llevaron a cabo con el apoyo de 2 docentes, teniendo estas una duración de 40 minutos, este fue un primer acercamiento para determinar ya un programa de capacitación de ciberseguridad, las presentaciones contenían temas como son: Principales amenazas en dispositivos móviles, Dispositivos no confiables, Aplicaciones maliciosas, Malware bancario, Ramsonware, ¿Cómo limpiar tu teléfono infectado?, ¿Como detectar un virus en el celular?, estos temas fueron para los estudiantes de IGE, para los de ITICS se agregaron otros temas como fueron: Creación de VPN, Phishing en dispositivos móviles, Seguridad en Android con herramientas especializadas (Passwordmeter, Clave Segura, Bit defender), se incluyó también la configuración básica de seguridad en Android.

Se tuvo la colaboración de 4 estudiantes de la carrera de Ingeniería en Tics, que estaban cursando la asignatura de Gestión y Seguridad en Tics, quienes participaron de forma voluntaria para la realización de estas, donde se les aplico una encuesta al inicio y otra al final, en donde la primera se realiza para establecer el nivel de conocimiento sobre ciberseguridad, conocer el sistema operativo que tiene su celular, si conocen de la existencia de ataques a los celulares y los riesgos de los mismos, dentro las preguntas esta la que se refiere al sistema operativo obteniendo como resultado que un total de 85% utilizan Android y el 15% utilizan IOS, en la pregunta que se refiere al sí poseen antivirus el 98% indico que no usa antivirus para su celular, siguiendo con la siguiente que pregunta con respecto a los ataques que han tenido en su smartphone, un 90% menciono malware y ransomware indicando que fue a través de instalar

aplicaciones y finalmente para los estudiantes de ITICS se les agrego una en especial con respecto a una VPN (Virtual Prívate Network), obteniendo que un 95% desconocían como realizar una VPN en su smartphone así como el uso que le podrían dar a la VPN.

Con respecto al uso que le dan el 90% indico que, para uso de redes sociales, un 100% para comunicarse con sus familiares y amigos y para uso de apoyo en la realización de tareas un 60% y lo que resulto notorio fuel el porcentaje para juegos el cual fue de un 80%., como se muestra en el gráfico 2.

Gráfico 2. Hábitos del uso del Smartphone

Fuente: Elaboración Propia

Dentro de las preguntas está la de: ¿Cuál es el principal uso que le das a tu smartphone? (Obligatorio) min=1 max=3

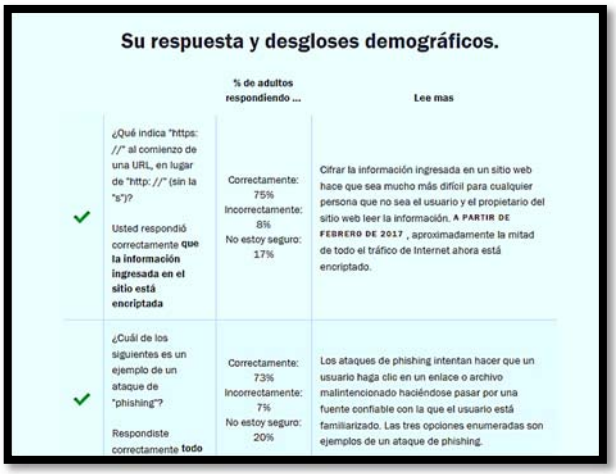
Redes Sociales, Leer las noticias, Bajar Aplicaciones, Jugar, Consultar portales especializados, Buscar información para tareas, Consultar correo electrónico, Comunicarse con familiares y amigos.

Otra de las preguntas fue: ¿Utiliza algún software antivirus? Si, cuál, No, por qué. En esta pregunta se le indican al participante algunos de los softwares antivirus más comunes y comerciales que utilizan., la mayoría indico que no utiliza ninguno siendo este un total del Y cuando se les pregunto que, si utilizan 82% y un 18% si, posterior a esta se le pregunta que si utiliza algún antispyware, el 90% contesto que no y el 10% si, siendo la razón que desconocen que es un antispyware. Continuando con las preguntas estas fueron: ¿Has tenido alguna mala experiencia visitando algún sitio desde tu smartphone?, ¿Cuál de las siguientes afirmaciones describe mejor cómo te sentiste al tener una mala experiencia visitando un sitio de Internet a través del móvil? Es importante resaltar que la amenaza en lo smartphone está al orden del día, por lo que la instalación de un cortafuegos es un paso en la dirección correcta para proteger el equipo, ya que con eso tendrá un elemento más de protección para que las entidades no autorizadas no pueden acceder al equipo, lo que reduce las posibilidades amenazas a la seguridad.

Este primer diagnóstico permite resaltar la importancia de crear un programa de concientización en todos los niveles para los estudiantes.

Y posteriormente se les aplico otra encuesta con respecto a los temas de ciberseguridad como se muestra a continuación, pero la estrategia fue no solo realizar la encuesta y generar estadísticos, si no que estos se le mostraran al encuestado y además se le diera información complementaria al respecto de la pregunta, como se muestra en la figura 1.

Fig. 1. Encuesta realizada a estudiantes.

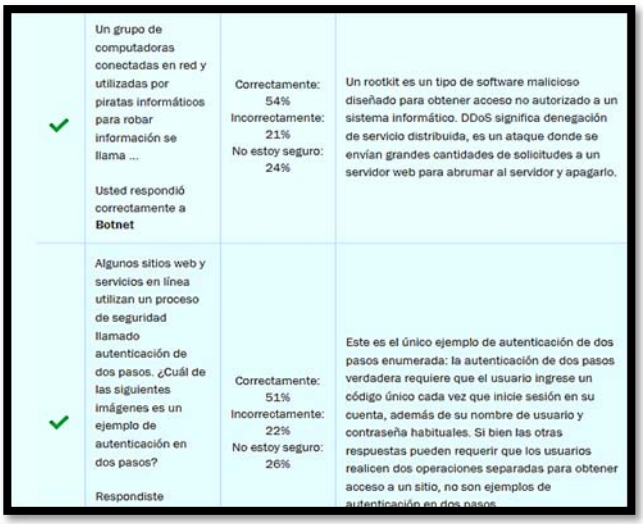


Fuente: Elaboración Propia como resultado de la encuesta realizada

Con lo que aquí se muestra, se puede visualizar el resultado de la respuesta, además de que se le da información complementaria con referencia a la pregunta realizada, también se les indica la información con respecto a las respuestas de los participantes y puede ver en donde se ubica con respecto a la certeza de su respuesta.

Continuando con las preguntas realizadas en la encuesta se presenta la figura 2.

Fig.2 Encuesta de ciberseguridad



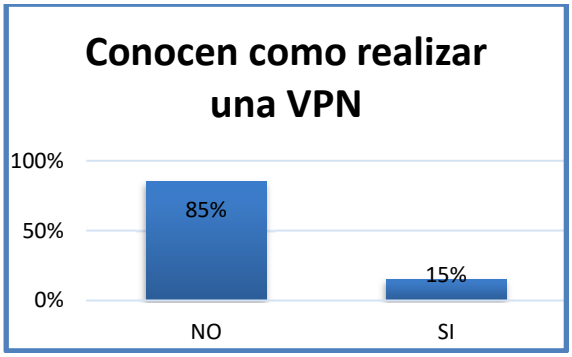
Fuente: Elaboración Propia como resultado de la encuesta realizada

Esta pregunta se refiere sobre el conocimiento de las posibles amenazas que el usuario puede tener en sus dispositivos, para lo cual se le dan opciones de recomendación dentro de la pregunta esta encuesta fue realizada en línea y desde ahí comenzó la concientización al usuario al incluirle información complementaria en la misma, además de que fomentar la autorreflexión al mostrarle los datos de las respuestas de los participantes

Dentro de la asignatura de Gestión y Seguridad se preguntó en forma directa a los estudiantes si habían creado VPN y si utilizan herramientas de seguridad en sus smartphones a la

cual se obtuvo un resultado de desconocimiento crear una VPN de un 85% (ver gráfico 3).

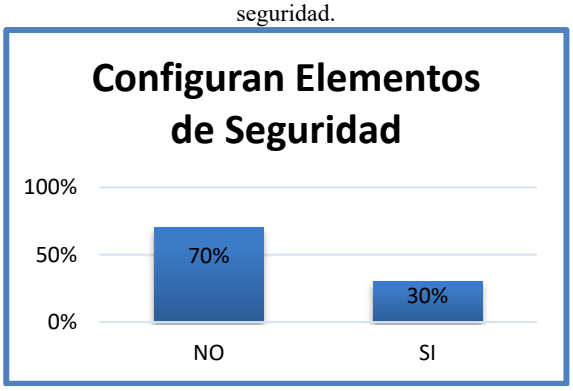
Gráfico 3. Resultado de realizar una VPN



Fuente: Elaboración Propia

En lo que respecta a estudiantes de séptimo-octavo semestre, un 70% no configuran elementos de seguridad tal y como lo muestra el gráfico 4.

Gráfico 4. Resultado con respecto a configuración de elementos de seguridad.



Fuente: Elaboración Propia

Además, los encuestados desconocen en un 70% herramientas técnicas para proteger su smartphone estos datos fueron obtenidos de un total de 35 estudiantes que cursaban la asignatura en el mismo periodo indicado.

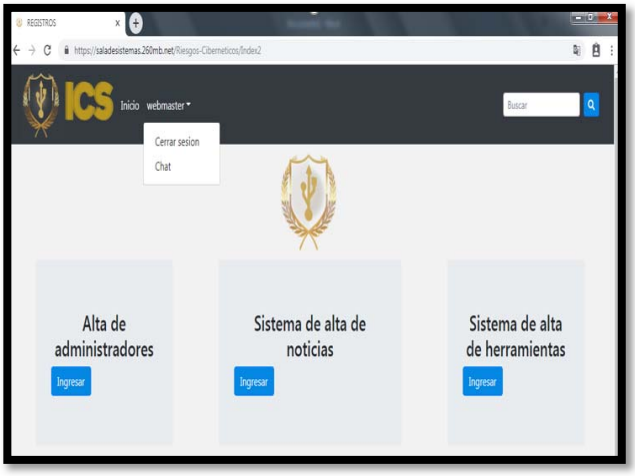
Como se puede observar en los resultados existe un alto grado de desconocimiento de establecer medidas de seguridad en lo smartphone.

En los últimos años, cada vez más centros educativos están llevando a cabo políticas de sensibilización y educación entre los menores acerca de la importancia de la ciberseguridad.

Es importante indicar que el portal web que se desarrolló se encuentra en una fase de prueba y que este incluye elementos tales como sistema de clasificador de noticias, sistema de integración de herramientas de protección, las cuales permiten integran información referente a la ciberseguridad la cual podrán localizar a través de acceder al portal toda vez que ya se encuentre liberado.

La información que se incluye en el portal se encuentra clasificada en orden cronológico, continuando con una subclasificación por (noticias, defensas, ataques, historias, visitas y normas). Dentro del mismo, integra herramientas para la protección del usuario y un chat para estar en continua comunicación con los visitantes.

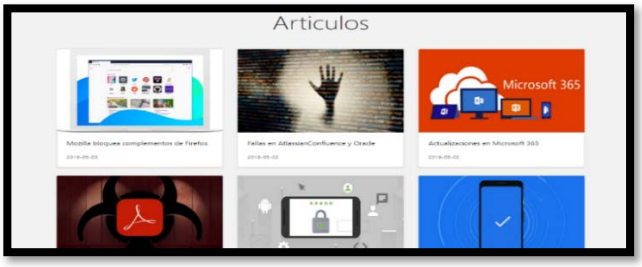
Fig.1. Sistemas integradores de la administración del portal



Fuente. Elaboración Propia

En la figura 2 se muestra el contenido del portal como es el control de artículos, herramientas, infografías, etc.

Fig. 1. Sección de Artículos del Portal



Fuente: Elaboración Propia

El portal muestra el contenido de noticias y artículos ilustrando el mismo con una imagen e incluyendo un texto breve para que se interese el usuario.

Fig. 3. Elemento de Apoyo al usuario, contenidos dentro del portal

Fuente. Elaboración Propia

El portal cuenta con un registro de control de noticias, usuarios registrados y visitantes, este incluye también un chat que le permitira estar en contacto constante con el visitante y apoyarlo en su dudas al respecto de los temas que se incluyen en el mismo.

Fig. 4. Registro de Control y Collage de Infografias

Fuente: Elaboración Propia

Según McAfee, el 80% de los estudiantes afirma que su colegio toma las medidas necesarias para asegurar que los dispositivos que usan en la escuela están protegidos contra cualquier ataque. Además, el 86% de los alumnos señala que se sienten informados respecto a la educación en ciberseguridad. Así McAfee propone que se debe realizar la educación digital desde edades tempranas además de sensibilizar a los más jóvenes de la importancia de la seguridad online desde la infancia, es esencial para prevenir y hacer frente a posibles amenazas potenciales a las que se exponen los menores cuando hacen uso de Internet, aplicaciones de mensajerías o redes sociales. El reducir los riesgos al limitar el tipo y la cantidad de datos personales que comparten los niños en Internet ayudará a minimizar las probabilidades de sufrir un ataque además de establecer el control parental en sus dispositivos evitará que los menores accedan a sitios potencialmente peligrosos y webs no autorizadas por los padres.

La ciberseguridad es uno de los retos que se enfrenta en el desarrollo de servicios y plataformas educativas, al mismo nivel de importancia que la capacitación, la adaptación a tecnologías no alineadas con la estrategia de la institución y a los riesgos externos del entorno, aseguró José Valdez Cotera, CIO de la Red de Universidades Anáhuac.

Inculcar estas habilidades fundamentales en los jóvenes garantiza menos lagunas de conocimiento que nos hacen menos vulnerables cuando nos protegemos de los posibles atacantes. Los talleres sobre programa maligno, codificación y cifrado deberían incluirse como estándar para que los jóvenes tengan una amplia gama de conocimientos y comprensión.

"La formación del profesorado en ciberseguridad es fundamental para sensibilizar a padres y a alumnos de la importancia de proteger sus dispositivos, así como de las amenazas online a las que se enfrentan y sus consecuencias. Por ello, es muy importante que los centros educativos apuesten por la implementación de campañas de educación en ciberseguridad que permita a los docentes informar tanto a padres como a alumnos sobre cómo hacer un uso responsable de sus dispositivos y exponerse lo menos posible a potenciales amenazas", señala Francisco Sancho, product partner manager consumer and mobile de McAfee España.

En el sitio web de Innovación Educativa que es una iniciativa de la Universidad Peruana de Ciencias Aplicadas, publica en su artículo "La importancia de la ciberseguridad en las universidades" de junio 15 del 2019, que de acuerdo con el Center for Digital Education, los retos son los siguientes:

Phishing: Un tercio de los usuarios que reciben correos electrónicos diseñados para obtener datos los abren según un informe de Verizon 2016, que analizó 2,260 violaciones y cubrió más de 100,000 incidentes.

Educación del usuario: Los estudiantes, docentes y personal administrativo de las universidades están muy ocupados con actividades académicas y tienen muy poco tiempo para preocuparse por la ciberseguridad.

Seguridad en la nube: La computación en la nube funciona bien para el lado de TI de la universidad, pero también presenta desafíos para la seguridad dado que la institución no tiene completamente el control de todo el proceso.

Compromiso de las autoridades con la Estrategias de Seguridad: La seguridad no siempre encabeza la lista de prioridades de los líderes universitarios. Pero a medida que aumentan los riesgos y las consecuencias, es importante poner la seguridad en el radar a nivel ejecutivo.

Inversión en tecnologías de seguridad de última generación. Como si se tratara de una carrera armamentista, los altos costos de tecnologías de última generación plantean retos importantes en la priorización de presupuestos de las universidades.

Gestión de la identidad y acceso. El desafío de las universidades está en implementar sistemas que controlen quién puede acceder a diferentes aplicaciones y qué nivel de acceso necesitan.

Gobernanza de la seguridad de datos. Muchas universidades no cuentan con gestión centralizada, en esos casos es más difícil gobernar la seguridad de los datos.

Dispositivos personales. Con docentes y estudiantes que traen tantos dispositivos al campus, los miembros del personal de seguridad no tienen la oportunidad de asegurarse de que esos dispositivos estén seguros y estos equipos contribuyen a ampliar las brechas de seguridad.

Finalmente, el realizar este tipo de actividad como parte del servicio a la sociedad cubre los siguientes objetivos como son:

- Sensibilizar acerca del uso inseguro de las nuevas tecnologías y las consecuencias derivadas, prevenir que las TIC se utilicen para realizar actividades como el ciberbulling, ciberacoso.
- Desarrollar competencias profesionales, emocionales, sociales y cognitivas, además del fomento de valores como el respeto, igualdad, solidaridad, cooperación y empatía y como una parte importante está el de promover su implicación como agente participativo y de cambio de la nueva sociedad en Red,

fomentando el ejercicio de la ciudadanía digital activa y responsable

Finalmente se observó que los participantes, a pesar de ser estudiantes de una carrera profesional de tecnologías y de otras carreras a nivel de ingeniería, desconocen las herramientas tecnológicas de protección para proporcionar mejor nivel de seguridad en sus actividades cotidianas del uso del smartphone y de la serie de riesgos que conlleva el utilizar internet, el instalar aplicaciones, el uso de las redes sociales. El conocer la serie de amenazas que se encuentran latentes permitió iniciar una primera campaña de concientización además de que se observó el interés por conocer herramientas y que fue del agrado de los mismos por lo que solicitaron que se les invitara a pequeños talleres donde se les mostrara como utilizar herramientas de protección del smartphone y de su pc, por lo que se puede interpretar como un efecto positivo que debe fortalecerse constantemente con actividades orientadas a mejorar la seguridad de los estudiantes y de la información que manejan en sus diversos dispositivos.

Como parte de la información que se les dio a conocer que existe en México la [8] AMECI que es la Asociación Mexicana de Ciberseguridad, la cual es una organización que apoya el fomento a la Ciberseguridad.

3. CONCLUSIONES Y RECOMENDACIONES

Finalmente el realizar este tipo de actividad por parte del cuerpo académico, permitió prestar un servicio a la sociedad cubriendo siguientes objetivos como son: Sensibilizar acerca del uso inseguro de las nuevas tecnologías y las consecuencias derivadas, desarrollar competencias profesionales, emocionales, sociales y cognitivas, además del fomento de valores como el respeto, igualdad, solidaridad, cooperación y empatía y como una parte importante está el de promover su implicación como agente participativo y de cambio de la nueva sociedad en Red, fomentando el ejercicio de la ciudadanía digital activa y responsable

Actualmente se está desarrollando un sitio web de ciberseguridad que pretende ir creciendo además de ir incluyendo más servicios para la comunidad para apoyar la concientización de la ciberseguridad tanto a nivel institución como a nivel empresa.

El cuerpo académico ha establecido de manera ya formal un grupo de estudiantes investigadores para la ciberseguridad, además de que para el año 2020 realizara videos y platicas virtuales para fomentar la ciberseguridad con la integración de un programa que se propondrá a la Institución para continuar con esta labor social tan importante de "fomentar la ciberseguridad".

[9] Indica que tal como señala InfoWorld, todos los smartphones tienen tres elementos básicos de seguridad. La primera gran tarea como usuario móvil es ser consciente de estos niveles y activarlos en los dispositivos:

Protección para dispositivos: permitir el "borrado" de datos remoto si pierdes o te roban el dispositivo.

Protección de datos: evitar que se transfieran datos corporativos a aplicaciones personales que se ejecutan en el mismo dispositivo o en la red personal

Seguridad para la gestión de aplicaciones: impedir que tu información en las aplicaciones se vea comprometida.

Es por ello por lo que la seguridad para smartphones no solo depende de los teléfonos, sino también de la tecnología de gestión de dispositivos móviles (MDM) instalada en los servidores de la empresa, que controla y gestiona la seguridad de los dispositivos. Ambas deben funcionar juntas para proporcionar una buena seguridad. Debes analizar todo el panorama de las herramientas necesarias para controlar las aplicaciones instaladas, están también permiten limitar las fugas de información originadas en aplicaciones de terceros como las de almacenamiento en la nube. MAM permite a los administradores aplicar políticas específicas en aquellas aplicaciones que son de uso laboral, dejando exentas del control aquellas de uso personal. Gracias a esta tecnología las empresas que permiten el uso de dispositivos personales para trabajar el Bring Your Own Device (BYOD) para llevar un control de las aplicaciones empresariales y la información que gestionan sin interceder en la parte personal del dispositivo.

Al analizar la vulnerabilidad y la escasa cultura de ciberseguridad es una motivación para lograr establecer programas de ciberseguridad a todos los niveles ya que los usuarios de los smartphones son de cualquier edad por lo que se deben generar programas en forma continua por parte de las instituciones educativas y del gobierno para el fomento de la protección al usuario en cuestiones de ciberseguridad. Por lo que al crear el portal web es una estrategia, pero no lo es todo ya que al usuario al que motivarlo a utilizar herramientas de seguridad y prevenir así los delitos informáticos y de ciberseguridad que van en aumento por uso de estos dispositivos.

4. REFERENCIAS

[1] Subsecretaría de Comunicaciones de la Secretaría de. Comunicaciones y Transportes (SCT) (2019). Estudio de Hábitos de los usuarios en ciberseguridad en México, Obtenido https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

[2] Global Mobile Consumer Survey (GMCS), (2019), Estudio: Hábitos de los consumidores móviles en México, 2019, Obtenido de https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/technology/Global-Mobile-Consumer-Survey.pdf

[3] Juárez, C. M., Ventura, R. (2018), Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios, Paakat: Revista de Tecnología y Sociedad ISSN: 2007-3607 Universidad de Guadalajara Sistema de Universidad Virtual México suv.paakat@redudg.udg.mx

[4] Wiseman, C. (2017). Accounting Firm Cybersecurity: Training Your Staff and Protecting Your Business. CPA Practice Advisor, 27.

[5] Rhodes-Ousley, M. (2013). Information Security - The Complete Reference. USA: McGraw-Hill.

[6] INEGI. (2017). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, Obtenido de https://www.inegi.org.mx/programas/dutih/2017/
[7] INCIBE (2019). INSTITUTO NACIONAL DE CIBERSEGURIDAD. Obtenido de https://www.incibe.es/que-es-incibe
[8] AMECI. (2019) Asociación Mexicana de Ciberseguridad, Obtenido de https://www.ameci.org/index.php/servicios-seguridad/generales/seguridad-prevencion-escuelas
[9] Kaspersky Lab (2019) , Seguridad para smartphones, Obtenido de https://www.kaspersky.es/resource-center/threats/smartphones