Apertura
ISSN: 1665-6180
apertura@udgvirtual.udg.mx
Universidad de Guadalajara
México

Castillejos López, Berenice; Torres Gastelú, Carlos Arturo; Lagunes Domínguez, Agustín
La seguridad en las competencias digitales de los millennials
Apertura, vol. 8, núm. 2, octubre, 2016, pp. 54-69
Universidad de Guadalajara
Guadalajara, México

apertura
Volumen 8, número 2, pp. 54-69 | Universidad de Guadalajara
doi: http://dx.doi.org/10.18381/Ap.v8n2.914

La **seguridad** en las **competencias digitales** de los *millennials*

Berenice Castillejos López *
Carlos Arturo Torres Gastelú **
Agustín Lagunes Domínguez ***

RESUMEN

Basados en un estudio mixto, en este documento valoramos la percepción del universitario sobre el tema de la seguridad en la Red, considerada una de las áreas de las competencias digitales. Apoyados en los descriptores del proyecto Ikanos del Instituto Vasco de Cualificaciones y Formación Profesional (2014), consideramos cuatro temas: la protección de los dispositivos, los datos personales, la salud y el uso sostenible de los recursos tecnológicos (INTEF, 2014). En la recolección de los datos, empleamos un cuestionario en línea y un guion de entrevista individual semiestructurado. Los resultados señalan que los *millennials* realizan prácticas básicas de seguridad, tales como el uso de antivirus, el manejo de contraseñas, ajustes en la configuración de las herramientas web, entre otros. Respecto a la identidad digital y la salud, es necesario promover el empleo adecuado de los datos personales, así como fomentar hábitos mediáticos saludables. En la protección del entorno natural identificamos la necesidad de crear conciencia sobre la adquisición de equipos, el manejo de los energéticos, el reciclaje y los desechos tecnológicos. Por último, este trabajo busca contribuir a la discusión sobre la seguridad y el consumo mediático dentro del marco de las competencias digitales.

Palabras clave:
Internet, *millennials*, competencias digitales, protección de datos, seguridad digital, TIC.

* Maestra en Gestión de la Calidad. Profesora-investigadora del Instituto de Turismo de la Universidad del Mar campus Huatulco, Oaxaca, México.
** Doctor en Ciencias de la Administración. Profesor de la Facultad de Administración de la Universidad Veracruzana, Veracruz, México.
*** Doctor en Sistemas y Ambientes Educativos. Profesor de la Facultad de Contaduría y Administración campus Ixtac de la Universidad Veracruzana, Veracruz, México.

Safety in the digital skills of millennials

Abstract

A mixed study research, this paper analyses the perception of the college students about online safety, considered one of the areas of digital skills. We rely on the Ikanos project descriptors of the Basque Institute of Professional Qualifications and Vocational Training (2014). We considered the four topics: protecting devices, protecting data and digital identity, protecting health and protecting the environment (INTEF, 2014). In collecting the data, we used an online survey and a semi-structured individual interview. From the results, millennials uses basic safety practices, such as using antivirus, password management, configuration settings in the Web tools, etc. Regarding the digital identity and health, it detected the need to promote the proper use of personal data and the media habits. For the environmental protection, it is essential promote awareness about the computers and electronic devices, energy management, recycling and technological waste. Finally, this research seeks to contribute to the discussion on safety and the media consumption within the framework for the development of digital skills.

Keywords:
Internet, millennials, digital skills, data protection, digital safety, ICT.

INTRODUCCIÓN

Cuando se aborda el tema del perfil del universitario, es primordial considerar sus actuaciones como gestor de información y conocimiento en la Red. Por tal hecho, resulta necesario identificar los factores que lo caracterizan como internauta. Hay clasificaciones tan básicas que van desde diferenciar a los usuarios novatos de los que ya manejan las tecnologías de la información y la comunicación (TIC), así como de aquellos que son expertos. Algunas tipologías más estructuradas se establecen en función del nivel de participación; otras se enfocan a la edad del usuario y marcan ciertos atributos sobre el uso tecnológico; algunas más refieren el tiempo de permanencia en la Red y los motivos que los llevan a navegar. Entre los términos más conocidos están los de generación net, definido en función del uso de internet; consumidores y productores, relacionado con la información y el desarrollo de contenidos; los nativos e inmigrantes digitales, categorizados en función de la edad; visitantes y residentes, clasificados de acuerdo con su motivación; y generaciones del cambio del milenio o *millennials*, que aluden a la era digital (Howe & Strauss, 2000; Pedró, 2006; Prensky, 2001; Tapscott, 1998; Tapscott & Williams, 2008; White & Le Cornu, 2011).

Los millennials, sujetos nacidos entre 1982 y 2000, también denominados generación Y,

aparecen en el tránsito del cambio del milenio y son contemporáneos de la revolución digital. Se trata de comunidades tecnosociales donde el uso de internet, los móviles y videojuegos son elementos clave en sus actividades cotidianas. Se encuentran sobreestimulados de información y de experiencias culturales multimediáticas (Area, Borrás y San Nicolás, 2015; Howe & Strauss, 2000; Pedró, 2006; Romo y Tarango, 2015). Este segmento no es homogéneo, ya que presenta una diversidad sobre el acceso a internet, las habilidades para emplear tecnología y el propósito de uso de la Red, es decir, si las actividades se desarrollan en contextos educativos formales o en el ambiente informal (Jones, Ramanau, Cross & Healing, 2010; Eynon & Malmberg, 2011). Tales referentes difieren de los argumentos de Prensky (2001) al identificar que no todas las personas nacidas después de 1980 tienen un alto nivel de uso de internet y poseen competencias digitales avanzadas (Akçayır, Dündar & Akçayır, 2016).

Los *milllennials* usan internet para comunicarse, entretenerse, buscar información, crear y participar en determinada actividad. Las experiencias de aprendizaje informal pueden surgir desde actividades como grabar videos, realizar trabajos artísticos, podcasts, escribir y compartir historias, hacer composiciones, entre otros. Es importante aclarar que la mayoría todavía continúa en su posición de consumidor y replicador de contenidos. En el plano académico, las actividades más comunes se relacionan con el compartir información de tareas o temas de aula y formar parte de grupos académicos en redes sociales sólo cuando éstos son creados por los docentes (Abel, Buff & Burr, 2016; Akçayır, Dündar & Akçayır, 2016; Domínguez y López, 2015; Garza, 2013; Jones, Ramanau, Cross & Healing, 2010; Eynon & Malmberg, 2011; Lee, 2014; Odabasi, Kusu & Gunuc, 2012; Pedró, 2006; Regil, 2014).

Los *milllennials* usan internet para comunicarse, entretenerse, buscar información, crear y participar en determinada actividad.

Esta generación frecuenta las redes sociales y las que más visita son Facebook, Twitter e Instagram. En el caso de Linkedin, sólo la usa con fines profesionales. Los dispositivos más utilizados son la laptop y el teléfono inteligente. Ante la alta propensión de uso de este último, también son llamados generación Smartphone. Estadísticas internacionales de 2013 revelaron que 76% de la población millennials contaba con un teléfono móvil. Respecto al periodo de conexión, se identificó que, en promedio, permanecían en línea seis horas diarias. Según datos por región, en Norteamérica y Latinoamérica se conectaron siete horas; seis horas en Asia y en Europa central y del Este; en tanto, en Europa Occidental, Oriente Medio y África, sólo cinco. Lo anterior indica que el continente americano es el que registró un mayor tiempo de conexión en el mundo (Abel, Buff & Burr, 2016; Johri, Teo, Lo, Dyfour & Schram, 2013; Lee, 2014; Telefónica, 2013).

Por lo antes expuesto, esta nueva era requiere individuos que posean competencias para la producción, difusión y consumo de información, de tal modo que puedan hacer frente a los retos del siglo XXI. Tal hecho da origen a la multialfabetización (planteamiento integrado de los distintos alfabetismos, debido a los diversos medios y lenguajes de la cultura de la sociedad actual), una condición necesaria para la construcción democrática de la ciudadanía, la cual implica desarrollar conocimientos y habilidades cognitivas e instrumentales, así como valores y actitudes de naturaleza social y política vinculadas al uso de las TIC, herramientas flexibles para actividades del aprendizaje permanente (Area,

2010; Chávez y Gutiérrez, 2015; Odabasi, Kusu & Gunuc, 2012).

LA SEGURIDAD EN LOS ENTORNOS DIGITALES

Abordar el tema de la seguridad en entornos digitales invita a reflexionar sobre los beneficios que aporta el uso de internet a la sociedad del siglo XXI. Sin embargo, es preciso tener en cuenta los riesgos que genera la navegación y, en algunos casos, la sobreexposición a los recursos mediáticos. Para atender las buenas prácticas en materia de seguridad, es conveniente mantener una postura neutral, sin caer en discursos tecnofóbicos, pero tampoco obviar los efectos físicos y psicológicos que producen las horas excesivas de uso de internet, así como el mal manejo de los dispositivos. Por este hecho, las TIC deben emplearse con inteligencia. Ante los posibles riesgos que implica tener presencia en la Red, es primordial tomar las medidas necesarias al momento de compartir información (Area, Borrás y San Nicolás, 2015).

Las competencias digitales no sólo deben concebirse desde el plano instrumental, sino han de estar relacionadas con aspectos psicológicos y sociales. La competencia digital resulta un aspecto clave y de carácter transversal que todo ciudadano digital debería desarrollar por la necesidad de aprovechar las tecnologías para incentivar la participación y el empoderamiento en la sociedad del siglo XXI. Promoverlas implica el uso crítico, creativo y seguro de las TIC, ya sea con fines laborales, escolares o actividades de la vida cotidiana (Instituto Vasco de Cualificaciones y Formación Profesional, 2014a). Aquino, Izquierdo, García y Valdés (2016) argumentan que la competencia digital facilita en los universitarios el desarrollo académico y abre posibilidades de participar en experiencias alternas de aprendizaje.

De acuerdo con Cabero y Gutiérrez (2015) y García-Aretio (2016), utilizar tecnologías para el aprendizaje es repensar la escuela y, además,

La competencia digital resulta un aspecto clave y de carácter transversal que todo ciudadano digital debería desarrollar por la necesidad de aprovechar las tecnologías para incentivar la participación y el empoderamiento en la sociedad del siglo XXI.

considerar ese equilibrio entre la dimensión individual y la social del sujeto que navega por la Red. Del mismo modo que en la presencialidad, en los espacios virtuales también se entretejen los valores de la persona y el comportamiento que adopta en comunidad.

Ferrari (2013), a través del proyecto DIGCOMP, propone un marco común de competencias digitales basado en conocimientos, habilidades y actitudes. Éste engloba cinco áreas: información, comunicación, creación de contenidos, seguridad y resolución de problemas. En lo referente a la seguridad, implica la protección de los dispositivos, los datos personales, la salud y el entorno o medio ambiente (INTEF, 2014) (ver tabla 1).

La competencia vinculada con la seguridad promueve la protección de los dispositivos, es decir, ser consciente de los riesgos y las amenazas que surgen en la Red; por ejemplo, virus, *malware* (programas y códigos maliciosos que buscan infiltrarse en un equipo), *spam* (correo electrónico no deseado), APT (del inglés *advanced persiten threat*), programas que restringen el acceso a determinadas partes o archivos del sistema infectado y cuyo propósito es bloquear el uso del dispositivo

Tabla 1. Seguridad, área de las competencias digitales.

Competencia	Descripción
Protección de los dispositivos	Proteger los dispositivos propios y comprender los riesgos y amenazas en red; conocer medidas de protección y seguridad.
Protección de datos personales	Entender los términos habituales de uso de los programas y servicios digitales; proteger activamente los datos personales; respetar la privacidad de los demás; protegerse a sí mismo de amenazas, fraudes y ciberacoso.
Protección de la salud	Evitar riesgos para la salud relacionados con el uso de la tecnología en cuanto a amenazas para la integridad física y el bienestar psicológico.
Protección del entorno	Tener en cuenta el impacto de las TIC sobre el medio ambiente.

Fuente: INTEF, 2014.

o parte de la información, así como los *phishing* o ataques que buscan engañar a los usuarios con falsos correos electrónicos o páginas web. Estos son sólo algunos de los riesgos a los que puede estar expuesto el internauta (IGF Spain, 2015; Chhikara, Dahiya, Garg & Rani, 2013; Hall, 2016).

En lo referente a la protección de datos personales, es importante considerar las condiciones y el término de uso de las páginas y herramientas digitales que circulan por la Red. Asimismo, la toma de conciencia sobre la protección de los datos (información textual, imágenes, videos, entre otros) para contrarrestar el riesgo de amenazas, fraudes y ciberacoso que se encuentran a la orden del día. De igual forma, este factor involucra el respeto a la privacidad de los demás, por ejemplo, en las redes sociales se observa con suma frecuencia la acción de etiquetar contactos en imágenes que se postean en el muro. En ocasiones, los usuarios de Facebook no conocen una quinta parte de las personas que se ubican en su lista de amistades. Estos contactos desconocidos tienen acceso a fotografías e información significativa que puede poner en riesgo su seguridad (Lee, 2014).

Atender el tema de la privacidad y los datos personales implica analizar la identidad digital. En un sentido estricto, la construcción de la identidad en línea no se basa en aspectos jurídicos o materiales, sino que surge de la expresión de la voluntad personal, desde un espectro flexible para ajustarse a los deseos de la persona (Martínez y Flores, 2016; Sullivan, 2016). Los millennials comparten información y transmiten conocimientos que inciden en la presentación y el desarrollo de su marca digital. A veces, el entusiasmo por tener presencia en la Red los lleva a comprometer su privacidad (Steijn & Vedder, 2015; Geller, 2016). Castañeda y Camacho (2012) señalan que, al valorar la identidad digital, se consideran dos aspectos: la parte personal, vinculada con lo que la persona hace de forma visible en internet y la parte social, que involucra a los que ejercen influencia (la red social de contactos o la red personal de aprendizaje) para generar tal identidad y también aquellas personas que se ven afectadas o influenciadas por el sujeto de referencia.

Reforzando lo expuesto en líneas anteriores, esta generación debe tener en cuenta que la sobreexposición de información personal en la Red atrae con facilidad a usuarios que navegan con otro perfil, cuyos fines, en ocasiones, tienen que ver con actos negativos (protestas, ciberacoso, agresiones, *hackeo*, espionaje, extorsión, entre otros). Beck (2015) señala que, para actividades escolares, se deberían crear identidades digitales invisibles, es decir, crear cuentas digitales anónimas o con seudónimos que protejan los datos oficiales de los estudiantes. Asimismo, el uso de redes virtuales privadas que no registren la dirección IP, así como emplear *browsers* y demás programas que eviten el rastreo de la huella digital.

Por tal hecho, uno de los retos del gobierno, en conjunto con los centros educativos y la sociedad civil, es concientizar sobre el impacto de la identidad digital y la educación en valores.

Por otro lado, la protección de la salud toma en consideración los riesgos físicos y emocionales a los que se expone el usuario ante el uso excesivo de la tecnología. Las conductas adictivas a internet, aunadas a los trastornos de sueño y atención, así como los malestares corporales que acarrea la larga exposición a estos medios electrónicos, inciden de cierta manera en la calidad de vida del usuario (IGF Spain, 2015; Wąsiński & Tomczyk, 2015).

Los jóvenes con comportamientos adictivos pueden llegar a considerar la conectividad permanente como algo intrínseco por la forma en que establecen sus relaciones de amistad y su vida social. Cabe mencionar que, durante 2012, Reino Unido realizó un estudio en el cual identificó que dos terceras partes de los cibernautas presentaban nomofobia, es decir, el temor a estar sin el teléfono móvil. Otro aspecto encontrado fue el gran interés por saber de los otros y, en cierto grado, la creencia de que, al dejar de revisar sus dispositivos y enviar mensajes, se corre el riesgo de quedar en la invisibilidad. Tal acto desencadena el síndrome FOMO (*fear of missing out*), el miedo a perderse de algo por abstenerse a usar internet. Aunado a esto, se reconoce la infoxicación digital (sobresaturación de información) y los distractores que circulan por la Red (Abel, Buff & Burr, 2016; Lee, 2014; Serrano-Puche, 2012).

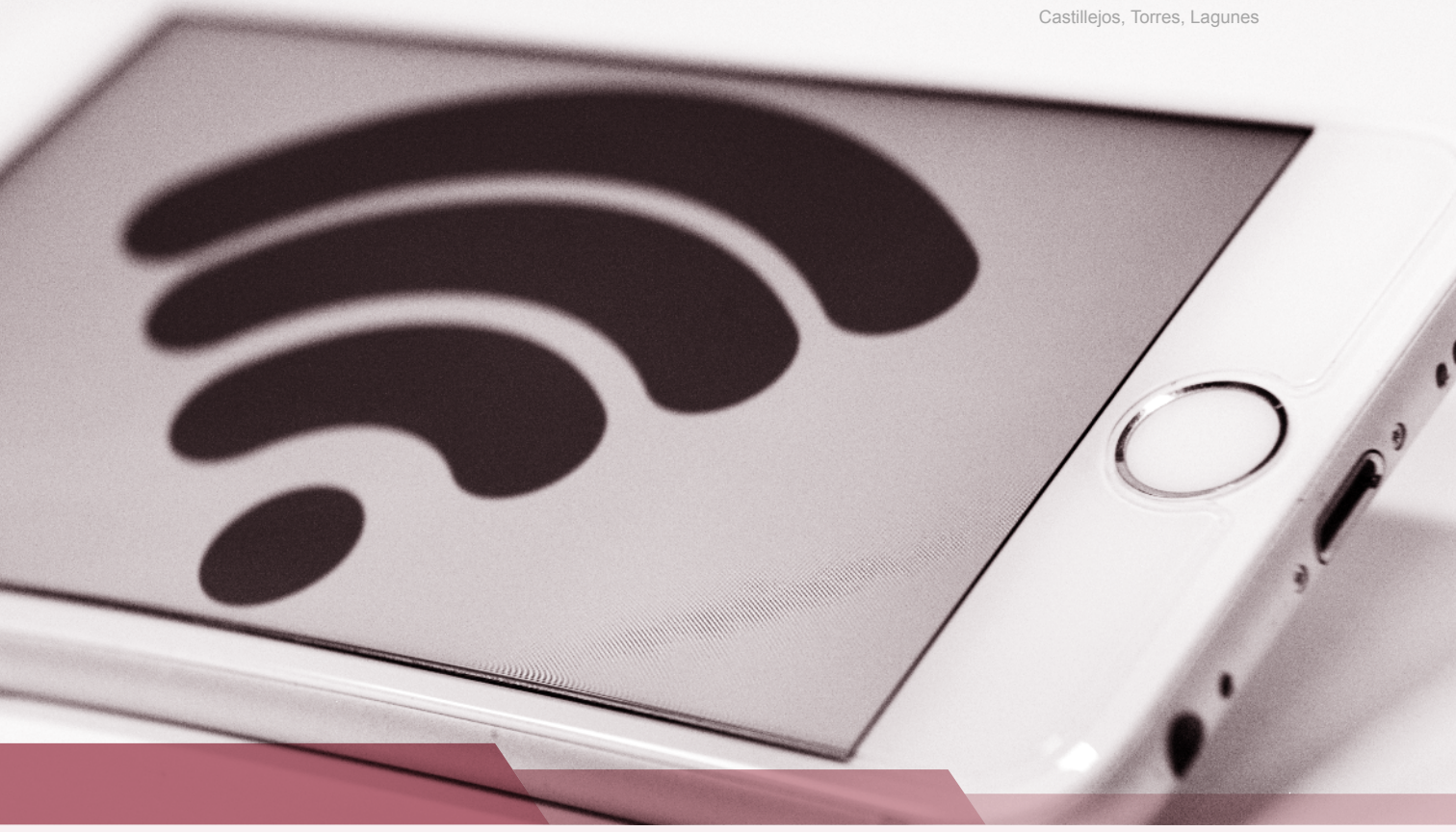
Para contrarrestar los efectos mencionados, se promueven hábitos mediáticos saludables, traducidos en una dieta digital que implica la valoración del tiempo empleado en la navegación por internet, acción que invita a desarrollar una agenda de actividades con espacios de desconexión y buscar un equilibrio entre las actividades que involucren el uso de la tecnología y las relaciones interpersonales directas (Aguaded y Romero, 2015; Sieberg, 2011).

... Reino Unido realizó un estudio en el cual identificó que dos terceras partes de los cibernautas presentaban nomofobia, es decir, el temor a estar sin el teléfono móvil.

La protección del entorno involucra la toma de conciencia sobre el impacto que generan las TIC en el medio ambiente. Esto lleva a adoptar una postura informada para considerar aspectos positivos y negativos. Integra, además, la aplicación de buenas prácticas para el uso de la tecnología en la vida diaria, como tomar medidas en el ahorro de energéticos y optimizar los tiempos de consumo en línea. El manejo de los dispositivos electrónicos y consumibles van desde la toma de decisiones de compra hasta las acciones de desecho y reciclaje (Bekaroo, Bokhoree & Pattinson, 2016).

METODOLOGÍA

Se trata de un estudio mixto apoyado en un cuestionario en línea y entrevistas semiestructuradas a 62 estudiantes universitarios (74% mujeres y 26% hombres, de los cuales 97% tenían una edad que oscilaba entre los dieciocho a veinticinco años) ubicados en la región costa del estado de Oaxaca. Para la elaboración del cuestionario, tomamos como base el test de autodiagnóstico de IKANOS, un proyecto sobre competencias digitales del Instituto Vasco de Cualificaciones y Formación Profesional (2014), que, a su vez, se deriva del Marco Común de Competencias Digitales, que engloba cinco áreas: información, comunicación, creación de contenidos, seguridad y resolución de problemas (Ferrari, 2013; INTEF, 2014). Es importante



aclarar que para el desarrollo de este documento, sólo consideramos los resultados de la cuarta área de competencia digital, la de seguridad.

En lo que refiere al análisis e interpretación de los resultados del cuestionario, las preguntas sobre competencia y protección de los dispositivos y de datos personales fueron planteadas con opciones de respuesta dicotómicas, con un carácter de variable nominal. Esto llevó a determinar frecuencias porcentuales. En tanto que en el tema de la salud y protección del entorno, trabajamos con variables escala. Esto desencadenó el cálculo de las medias de once ítems, precedidos del análisis de confiabilidad alfa de Cronbach, el cual reportó un buen nivel de confiabilidad (.927). La escala de respuesta fue de 10 grados, donde 1 significó desconocer o no ser capaz de desarrollar la acción que describe el ítem y 10, tener conocimiento o ser capaz de desarrollar la acción.

Para el análisis y la interpretación de los datos, aplicamos estadística descriptiva, apoyados en el software SPSS versión 22. Es importante resaltar que, con la finalidad de enriquecer los resultados de la encuesta, efectuamos entrevistas individuales semiestructuradas, con una muestra por conveniencia de treinta informantes que antes habían respondido el cuestionario en línea. Para esto, diseñamos un guion de preguntas, cuyas respuestas fueron procesadas en el software Atlas.ti, versión 7, e identificamos los aspectos clave del tema de seguridad como resultado de la codificación de la información.

RESULTADOS

Para analizar las prácticas de seguridad, fue necesario conocer los hábitos de uso de los universitarios. Respecto a los dispositivos, emplean la

computadora de escritorio y portátil (94%), seguido del teléfono móvil inteligente o Smartphone (77%) y la tableta (18%). Algunos no disponen de internet en el hogar (29%). Una gran proporción se conecta a diario (74%) y acceden, principalmente, desde una computadora personal (PC) o portátil (63%); otros señalan que dependiendo del momento y la situación eligen el equipo (19%), en ciertos casos desde el Smartphone (13%) o tableta (5%). El lugar de conexión más frecuente es la casa (63%), seguido de los cibercafés o espacios públicos (19%). Entre los tipos de usos de internet, destacan la búsqueda de información para uso personal o profesional (98%); las redes sociales con fines personales o profesionales (84%); el envío y la recepción de correos (81%); escuchar música y ver películas en línea (74%), así como la mensajería instantánea (71%).

Protección de los dispositivos

En el uso de internet y dispositivos digitales, argumentan que actúan con prudencia cuando reciben mensajes cuyo remitente, contenido o archivo adjunto desconocen (*spam*) (84%). Manifiestan que si la información resulta nueva o dudosa, se debe proceder a su verificación. Recurren al bloqueo de páginas sospechosas o la instalación de programas que contrarresten el riesgo del ciberespionaje, aspecto que menciona IGF Spain (2015). En su mayoría, tienen instalado un antivirus que ejecutan y actualizan de manera regular (77%). Una menor proporción (69%) emplea diferentes contraseñas para acceder a los dispositivos y servicios digitales, y éstas son modificadas en forma periódica mediante estrategias para su administración.

Asimismo, una proporción revisa a menudo la configuración y los sistemas de seguridad de sus dispositivos y las aplicaciones (58%). Debido al empleo de dispositivos externos, como la memoria extraíble, identifican el escaneo de estos instrumentos para evitar contaminar el equipo de trabajo; aunado a esto, se encuentra la cultura del respaldo de información y el empleo de extensiones cuando navegan por internet, tal y como se aprecia en la siguiente declaración: "Hago uso de programas antivirus, así como también verifico la información y las memorias que he de ingresar a mi dispositivo electrónico en uso". En tanto, otro participante mencionó: "Cuento con un respaldo de todo y protejo mis dispositivos, de igual forma no dejo registradas mis contraseñas". Algunos cambian, con la periodicidad que estiman oportuna, el código de seguridad de la red inalámbrica o la clave de acceso a la estación de red Wifi que tienen instalada (39%); son minoría los que conocen y hacen uso de sistemas de protección de conexiones inalámbricas ante escuchas o accesos clandestinos (29%) (ver tabla 2).

Tabla 2. Escala sobre la protección de dispositivos.

Ítem	Porcentaje
Actuar con prudencia cuando se reciben mensajes cuyo remitente, contenido o archivo adjunto desconoce (spam).	84
Instalación de un programa antivirus, el cual se ejecuta y actualiza de manera regular.	77
Utilización de diferentes contraseñas para acceder a los equipos, dispositivos y servicios digitales y la modificación periódica.	69
Revisión de la configuración y los sistemas de seguridad de los dispositivos o las aplicaciones utilizadas.	58
Cambios periódicos del código de seguridad de la red inalámbrica o la clave de acceso a la estación de red Wifi que se tiene instalada en el hogar, trabajo o escuela.	39
Conocimiento y uso de sistemas de protección de conexiones inalámbricas ante escuchas o accesos clandestinos.	29

De acuerdo con Hall (2016), observamos conocimientos básicos sobre los mecanismos de protección, como la activación de antivirus en el equipo empleado, el manejo de correos no deseados, así como la administración de contraseñas para los dispositivos y herramientas digitales. Es innegable que existan campañas para sensibilizar a la población sobre los protocolos de seguridad informática, pero, en ocasiones, la falta de interés o desconocimiento puede llevar a no poner atención en la configuración de los dispositivos y en aquellas actividades sospechosas que se observan en la Red.

Por otro lado, la cultura por la aplicación de códigos de seguridad y sistemas de protección en las redes inalámbricas es mínima, lo que implica trabajar más en aspectos sobre ciberseguridad. Atender este tema es más complejo cuando la conexión Wifi se realiza fuera del hogar, sobre todo en los espacios públicos, donde queda totalmente vulnerable la información personal. Esto llevaría a tomar decisiones acerca de la conveniencia de conectarse fuera del hogar, aun cuando se traten de redes privadas. Ahora bien, las medidas de seguridad en casa deben estar orientadas a identificar las mejores prácticas que mantengan a salvo la privacidad y la optimización del ancho de banda ante cualquier persona que intente unirse sin autorización.

Es innegable que existan campañas para sensibilizar a la población sobre los protocolos de seguridad informática, pero, en ocasiones, la falta de interés o desconocimiento puede llevar a no poner atención en la configuración de los dispositivos y en aquellas actividades sospechosas que se observan en la Red.

Protección de los datos personales

Los estudiantes utilizan las funciones de privacidad disponibles en las aplicaciones para aprobar o rechazar quién puede acceder a su perfil (95%). Sólo comparten su perfil con su lista de contactos/amigos (92%). Son conscientes de la forma en que la información de su identidad digital puede o no ser utilizada por terceros y de los riesgos que implica (90%). En la interacción a través de la Red, expresaron que nunca revelan información privada (90%). Establecen que se debe mantener un cierto nivel de privacidad, al argumentar que no todo lo contenido en internet debe estar expuesto, principalmente en redes sociales. Conocen y tienen en cuenta los peligros y consecuencias de que alguien suplante su identidad en internet, ya sea por estafas, robo de identidad o algún otro acto indebido (89%). Algunos estudiantes optan por dos o más identidades digitales, de tal forma que puedan tener un mejor manejo de la información que gestionan. Extreman sus precauciones antes de dar o recibir información personal, como la dirección, edad, teléfono, datos bancarios/tarjetas de crédito, fotos personales, entre otros (86%), salvo que la aplicación o página en la que naveguen solicite tal información.

En el uso de las redes sociales, únicamente agregan como amigos a personas que en realidad conocen (86%). Algunos dijeron ser capaces de identificar aquellas páginas web o mensajes de correo con los que puedan ser estafados (65%). Otros suelen modificar la configuración básica de privacidad que por defecto ofrecen los servicios en línea que utilizan para mejorar su protección (65%). Uno de los estudiantes declaró: “Bloqueo ciertos contenidos, pongo filtros para verificar antes información y me limito a proporcionar datos personales”. Lo antes descrito coincide con los argumentos

Tabla 3. Escala sobre la protección de datos personales.

Ítem	Porcentaje
Utilización de las funciones de privacidad disponibles en las aplicaciones para aprobar o rechazar quién puede acceder a su perfil.	95
Acción de compartir el perfil con su lista de contactos/amigos.	92
Conciencia sobre la forma en que la información de su identidad digital puede o no ser utilizado por terceros.	90
No revelar información privada.	90
Conocimiento y consideración de los peligros y consecuencias que alguien suplante su identidad en internet (estafas por robo de identidad o de otras credenciales).	89
Extremar precauciones antes de dar o recibir información personal (DNI, dirección, edad, teléfono, datos bancarios/tarjetas de crédito, fotos personales, etcétera).	86
En el uso de las redes sociales se agrega únicamente a amigos y personas conocidas.	86
Capacidad de identificar aquellas páginas web o mensajes de correo con los que puedan ser estafados.	65
Modificación de la configuración básica de privacidad que por defecto ofrecen los servicios en línea para mejorar la protección.	61
En las transacciones por internet se comprueba que, al transmitir datos sensibles, la conexión es segura y que la página en la que se efectúa la operación cuente con un certificado de seguridad, emitido por una autoridad certificadora de confianza.	58
Solicitar a los proveedores de servicios en línea información sobre el proceso de conservación y tratamiento de los datos personales, así como sobre sus políticas de privacidad.	42
Conocimiento y consideración de los aspectos básicos que establecen las normativas en materia de seguridad informática para regular la protección de datos personales.	26

de Geller (2016), Lee (2014), así como lo expuesto por Martínez y Flores (2016) (ver tabla 3).

En contraparte, cuando realizan transacciones a través de internet, una menor proporción comprueba que, al transmitir datos sensibles, la conexión sea segura y que la página en la que efectuaron la operación cuente con un certificado de seguridad y que éste sea emitido por una autoridad certificadora de confianza (58%). Algunos solicitan a los proveedores de servicios en línea información sobre el proceso de conservación y tratamiento de sus datos personales, así como de sus políticas de privacidad (42%). Además, muy pocos conocen y consideran los aspectos básicos que establecen las normativas en materia de seguridad informática para regular la protección de datos personales en el ámbito de internet (26%). Un entrevistado reflexionó sobre el escaso nivel de protección que adopta al navegar por la Red: "No facilito mis datos personales, pero a veces, para que te otorguen información se proporciona un número de teléfono; en este caso, no sé qué tanto protegen mi identidad en la Web. Desconozco esta parte".

Percibimos un nivel de conciencia sobre los riesgos a los que pueden estar sujetos por compartir información personal. Los resultados muestran que falta fomentar una cultura de protección de datos; a pesar de que existe una serie de normativas que regulan las actividades en la Red, se necesitaría difundirlas un poco más. Es posible considerar que, ante los eventos de inseguridad que se viven en la actualidad, aunados a los delitos que se cometen en la Red, la gran mayoría extreme precauciones en la utilización de los datos personales, debido a que sus tres principales usos de internet

se centran en la búsqueda de información, las redes sociales y el envío, y recepción de correos. Si a lo anterior se le agrega el desconocimiento sobre protocolos de seguridad en transacciones electrónicas, no sólo se ponen en riesgo los datos personales, sino también la situación económica. En virtud de las diversas estrategias de los ciberdelincuentes, es necesario tener identificados los espacios donde se reportan tales actos indebidos. Es innegable que el gobierno ha emprendido campañas de seguridad, pero éstas todavía no tienen el impacto que se requiere.

Identificamos un interés por la protección de los datos personales; los jóvenes procuran cuidar su información personal en la Red, pero una gran proporción desconoce las políticas de los proveedores de servicios en línea en lo referente al tratamiento de sus datos personales y el manejo de su privacidad. Respecto a la configuración y los sistemas de seguridad en dispositivos y aplicaciones, desarrollan actividades básicas, como la modificación de la configuración que por defecto los servicios en línea establecen (Lee, 2014; Martínez y Flores, 2016).

Protección de la salud

En este aspecto, identificamos que todas las valoraciones se ubicaron por arriba de la media de la escala de respuesta. La calificación más alta refiere al conocimiento acerca de los riesgos y las consecuencias que implica el ciberacoso (8.08), seguido de la adopción de mecanismos de prevención para evitar el acoso a través de la Red (*ciberbulling*) (7.39); posteriormente, el conocimiento sobre los riesgos que implica el uso inadecuado de tecnologías en los aspectos ergonómicos y adictivos (7.06); en cuarta posición, la adopción de medidas preventivas para proteger la salud (6.55); por último, mantenerse informado y actualizado sobre los riesgos de salud que el uso de las TIC puede generar en el bienestar físico o psicológico y abordar este tema con otras personas (6.05).

En algunos casos se afirmó que se estaba combatiendo la adicción: "Realmente estoy consciente de la adicción al uso de redes sociales, pero aún me cuesta superarlo, y lo que hago para obstruir este mal hábito es reflexionar en que hay cosas más importantes que hacer o que tengo alguna otra tarea". Otros comentaron que se debe tener un control de los tiempos, prescindir de comprar y usar dispositivos innecesarios, así como evitar los distractores de la Red; no preocuparse por no tener señal y realizar actividades sin uso de tecnología. Una declaración que vale la pena resaltar es la siguiente: "Evito comprar aparatos electrónicos innecesarios, limitándome sólo al que utilice; trato de utilizar lo menos posible los dispositivos para evitar cansancio o enfermedades" (ver tabla 4).

Tabla 4. Escala sobre la protección de la salud.

Ítems	Media	Desviación estándar
Conocimiento sobre los riesgos y consecuencias que puede implicar el ciberacoso.	8.08	1.876
Adopción de mecanismos de prevención para evitar el acoso a través de la Red (ciberbulling).	7.39	2.425
Conocimiento sobre los riesgos de salud que implica el uso inadecuado de las tecnologías (aspectos ergonómicos, adictivos, etcétera).	7.06	2.318
En el uso de las TIC, la adopción de medidas preventivas para la protección de la propia salud y de las que es responsable.	6.55	2.500
Mantenerse informado y actualizado sobre los riesgos de salud que el uso de las TIC puede generar en el bienestar físico o psicológico y abordar este tema con otras personas.	6.05	2.551

En lo concerniente a la salud física, algunos emplean protectores visuales, practican algún tipo de ejercicio, anteponen las necesidades fisiológicas en periodos de uso, cuidan la higiene personal, así como las posiciones corporales. Otros consideran contar con equipo y mobiliario cómodo: "Uso lentes cuando trabajo en la computadora, tengo una silla de escritorio que me permite permanecer cómoda por varias horas, no dejo de lado mis necesidades fisiológicas mientras estoy trabajando en la computadora. Organizo mi tiempo conforme a las actividades con mayor prioridad en el día". En casos extremos, hay algunos testimonios que sostuvieron no proteger su salud de forma adecuada. Los resultados obtenidos demuestran que los estudiantes son conscientes del impacto que tienen las TIC en la salud, pero falta trabajar con los hábitos mediáticos.

El tema de la salud integra diversas vertientes: por un lado, hace mención del ciberacoso, pero también atiende lo vinculado a la adicción al internet y los problemas físicos que desencadena el uso excesivo de las TIC. Estos dos últimos puntos llaman más la atención del adulto joven cuando se le cuestiona sobre su salud y reflexionan sobre las enfermedades físicas que puede ocasionar la sobreexposición de medios electrónicos, tales como molestias y dolores musculares, daños en audición, problemas de sobrepeso u obesidad por el sedentarismo, afectaciones al sistema nervioso, enfermedades oculares, entre otras. Por otro, la nomofobia y el síndrome FOMO, dos factores que se relacionan con el uso de la Web social e invitan a cuestionar las experiencias que les deja a los millennials mantenerse en el ciberespacio. Por lo tanto, considerar hábitos mediáticos implica la adopción de prácticas periódicas de desconexión, acción necesaria en el desarrollo de competencias digitales. Por último, el valor utilitario que tiene un dispositivo con internet no debería estar vinculado a estrategias de mercadotecnia que incitan a crear dependencia con la tecnología (Abel, Buff & Burr, 2016; Sieberg, 2011; Serrano-Puche, 2012; Wąsiński & Tomczyk, 2015).

Protección del entorno

Ahora bien, en cuanto a la protección del entorno, los aspectos con mayor puntuación fueron: la aplicación sistemática de medidas básicas para ahorrar energía (7.66); el conocimiento sobre el impacto que las TIC tienen en la vida diaria, en el consumo en línea y en el medio ambiente (6.94). Entre las valoraciones más bajas se ubicó el reciclaje de

Tabla 5. Escala sobre la protección del entorno.

Ítems	Media	Desviación estándar
Aplicación sistemática de medidas básicas para ahorrar energía.	7.66	2.032
Conocimiento sobre el impacto que las TIC tienen en la vida diaria, en el consumo en línea y en el medio ambiente.	6.94	2.469
Comprensión a lo que se refiere y engloba el concepto de Green IT (tecnologías verdes).	5.48	2.616
Utilización de sistemas remotos/virtuales de comunicación/colaboración (videoconferencia, telerreuniones, etcétera) para evitar los costos de desplazamiento, combustible, etcétera, inherentes a la comunicación presencial.	5.16	2.753
Reciclaje de los elementos TIC obsoletos o gastados (componentes electrónicos o informáticos, tóneres, etcétera) depositándolos en los sitios adecuados.	4.87	2.831
Participación en grupos de trabajo en la Red o utilizando las redes sociales para actuar, movilizar, protestar, informar, concienciar, así como para compartir y aportar ideas sobre la mejora de la sostenibilidad (*crowdsourcing*).	4.81	2.874

los elementos TIC obsoletos o gastados (4.87), así como la participación en grupos de trabajo en la Red o utilizando las redes sociales para actuar, movilizar, protestar, informar, concienciar, así como compartir y aportar ideas sobre sostenibilidad (4.81) (ver tabla 5).

En la protección del entorno se observan vacíos de esta competencia. Algunos millennials aseguraron que tenían pocas nociones o desconocían la problemática: "Sé muy poco del tema, pero aun así sí estoy muy consciente [de] que al usar una simple computadora hago un gran daño". Existe la conciencia sobre el uso de la tecnología, principalmente sobre el ahorro de los energéticos. Un entrevistado comentó: "Desconozco si afectan de manera directa, pero soy consciente del uso de la energía eléctrica". Otra de las declaraciones que vale la pena resaltar es:

> Todo tipo de tecnología afecta en mayor o menor medida el medio ambiente, por ejemplo, en la fabricación de éstos, se hace uso de materiales que después de terminar su ciclo de vida y ser desechados, contaminan con las sustancias o químicos que lo componen, pero, también las TIC sirven para transmitir información acerca del cuidado y protección que debemos hacer al medio que nos rodea.

Algunos recomiendan sólo usar la tecnología necesaria. De los temas que faltaría fortalecer está el del reciclaje de tecnología y las tecnologías verdes. Un estudiante afirmó que "pocas veces me pongo a pensar en ese aspecto".

El desconocimiento y la falta de motivación sobre temas medioambientales son factores determinantes en la protección del entorno. Cuando se atiende este tipo de temas, las acciones que se observan tienen que ver más con la reducción del consumo de energéticos. Hacer conciencia sobre las tecnologías verdes conlleva educar a los jóvenes sobre el impacto que tienen las TIC en el ecosistema. Relacionar la sustentabilidad dentro de la competencia seguridad resulta muchas veces ser poco usual, pero al momento de dimensionar lo que implica estar y convivir en espacios seguros, esto va más allá del individuo; involucra también el lugar donde se desarrolla (Bekaroo, Bokhoree & Pattinson, 2016; Suryawanshi & Narkhede, 2015).

DISCUSIÓN Y CONCLUSIONES

Analizar la seguridad informática a través de las cuatro competencias (protección de dispositivos, datos personales, salud y entorno) lleva a reflexionar sobre los hábitos de uso de la tecnología, principalmente lo relacionado con internet. Con la irrupción de la Web social, con suma frecuencia aparecen herramientas digitales que atienden determinadas necesidades del internauta y que pueden ser instaladas en diferentes dispositivos. Esto, aunado a las estrategias de mercadotecnia para comercializar equipos que revolucionan el uso. Toda esta atmósfera digital incita, en especial a los jóvenes, a estar a la vanguardia. Valorar el impacto de la tecnología en la vida cotidiana invita a considerar la multialfabetización, es decir, perfilar conocimientos, habilidades y actitudes que encaminen al empoderamiento y la participación de la sociedad en aspectos que contribuyan a desarrollar prácticas más sostenibles (Area, 2010).

Las estadísticas sobre hábitos de consumo de internet deberían dejar de centrarse en el ocio y la comunicación; es necesario promover nuevas formas de aprender en la Red; esto invita a replantear los principales motivos que llevan a conectarse. No hay que satanizar al internet como un espacio que genera adicción, sino valorar la frecuencia en que se usa y el para qué se utiliza; eso es lo que determina su aprovechamiento.

Las buenas prácticas sobre seguridad deberían partir de la toma de decisiones en la adquisición de equipos, de tal forma que se cuente con lo necesario y no dejarse llevar por la mercadotecnia. Además, prever el empleo de programas para proteger los dispositivos, aunado a la configuración y administración de contraseñas. En el caso

de las herramientas digitales, hay que considerar las políticas de uso de los datos personales y la privacidad, además de la gestión responsable de la identidad digital (INTEF, 2014).

Por otro lado, es importante tomar en cuenta lo relacionado con las políticas de privacidad y manejo de datos personales que emplean las empresas de servicios tecnológicos. Hoy en día, cada vez que revolucionan las herramientas digitales, se establecen nuevos criterios de registro para el usuario. Esto lleva a cuestionar en qué medida las compañías protegen la identidad digital del internauta o es sólo una utopía del mercado tecnológico (Lee, 2014).

En el plano de la salud surge una pregunta fundamental: ¿qué motiva a estar conectado(a)? Ésta, aunada a la posición que guarda el tema de las redes sociales, espacios donde los jóvenes destinan un mayor tiempo de uso, debido a lo práctico que puede ser ingresar desde el teléfono móvil, además de la necesidad del individuo por acceder y participar en la redes sociales. Es indispensable valorar las redes sociales desde dos espectros: un entorno que promueve la participación y el empoderamiento de la sociedad y el espacio para socializar que trae encubierto vacíos de soledad y necesidades de reconocimiento personal. Formar parte de lo que sucede en la Red puede ser una de las condicionantes que ponga en riesgo no sólo la salud emocional, sino también la física.

Lo anterior invitar a reflexionar sobre los argumentos de Bauman (2005) relacionados con la incertidumbre y el sentimiento creciente de inseguridad que desencadena la modernización. Es importante cuestionar si tal proceso de transformación de la sociedad se está dando de forma voluntaria o bajo presión. Las habilidades sociales desde la presencialidad revisten un debilitamiento en las interacciones con personas reales. En el mundo virtual se busca crear mecanismos que promuevan ambientes saludables para la convivencia. Tal es el caso de las netiquetas o códigos de conducta que aparecen en la Red.

Por lo anterior, las relaciones interpersonales directas no deberían ser sustituidas por la virtualidad. A pesar de que la generación de los millennials nació en un mundo de tecnología, han de cubrir necesidades sociales de carácter presencial. Entre los retos del siglo XXI también debería estar prevista la cultura de hábitos mediáticos saludables. Tal es el impacto de empleo de internet a través del teléfono móvil que algunos espacios de convivencia presencial han comenzado a restringir su uso (Aguaded y Romero, 2015; Serrano-Puche, 2012; Sieberg, 2011).

Cabe señalar que el tema de la seguridad no sólo se centra en proteger al usuario y a sus dispositivos, sino también aborda lo relativo a la protección del entorno natural. Da apertura a tomar conciencia sobre la adquisición de equipos, el manejo de los energéticos, el reciclaje y los desechos de los dispositivos, así como la pertinencia de las herramientas digitales para promover el cuidado del medio ambiente y uso de las tecnologías verdes.

Por último, abordar el tema de la seguridad digital es muy amplio; no sólo intervienen factores instrumentales que indiquen buenas prácticas de uso de la TIC, sino también psicológicos y sociales. Tal hecho invita a identificar futuras líneas de investigación, como profundizar en el equilibrio que debe existir entre el uso de la Web social y la aplicación de hábitos mediáticos saludables en millennials. Asimismo, valorar el fenómeno *big data* en la protección de datos personales.

REFERENCIAS BIBLIOGRÁFICAS

Abel, Jessica P.; Buff, Cheryl L.; Burr, Sarah .A. (2016). Social media and the fear of missing out: Scale development and assessment. *Journal of Business & Economics Research*, vol. 14, núm. 1, pp. 33-44. doi: http://dx.doi.org/10.19030/jber.v14i1.9554

Aguaded, Ignacio y Romero Rodríguez, Luis M. (2015). Mediamorfosis y desinformación en la infoesfera: alfabetización mediática, digital e informacional ante los cambios de hábitos de consumo informativo. *Education in the Knowledge Society (EKS)*, vol. 16, núm. 1, pp. 44-57. doi: http://dx.doi.org/10.14201/eks20151614457

Akçayır, Murat; Dündar, Hakan; Akçayır, Gokçe. (2016) What makes you a digital native? Is it enough to be born after 1980?

Computers in Human Behavior, vol. 60, pp. 435-440. doi: http://dx.doi.org/10.1016/j.chb.2016.02.089

Aquino Zúñiga, Silvia Patricia; Izquierdo Sandoval, Manuel Jesús; García Martínez, Verónica; Valdés Cuervo, Ángel Alberto. (2016). Percepción de estudiantes con discapacidad visual sobre sus competencias digitales en una universidad pública del sureste de México. *Apertura, Revista de Innovación Educativa,* vol. 8, núm. 1, Recuperado de http://www.udgvirtual.udg.mx/apertura/index.php/apertura/article/view/788.

Area Moreira, Manuel. (2010). Tecnologías digitales, multialfabetización y bibliotecas en la escuela del siglo XXI. *Boletín de la Asociación Andaluza de Bibliotecarios*, año 25, núm. 98-99, pp. 39-52. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3616424

Area Moreira, Manuel; Borrás Machado, José F.; San Nicolás Santos, Belén. (2015). Educar a la generación de los *millennials* como ciudadanos cultos del ciberespacio. Apuntes para la alfabetización digital. *Revista de Estudios de Juventud,* núm. 109, pp. 13-32. Recuperado de http://www.injuve.es/sites/default/files/2016/05/publicaciones/cap1_109.pdf

Bauman, Zygmunt. (2005). *Modernidad y ambivalencia*. España: Anthropos Editorial.

Beck, Estee N. (2015). The invisible digital identity: Assemblages in digital networks. *Computers and Composition*, vol. 35, pp. 125-140. doi: http://dx.doi.org/10.1016/j.compcom.2015.01.005

Bekaroo, Girish; Bokhoree, Chandradeo; Pattinson, Colin. (2016). Impacts of ICT on the natural ecosystem: A grassroot analysis for promoting socio-environmental sustainabilitiy. *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 1580-1595. doi: http://dx.doi.org/10.1016/j.rser.2015.12.147

Cabero Almenara, Julio y Gutiérrez Castillo, Juan Jesús. (2015). La producción de materiales TIC como desarrollo de las competencias del estudiante universitario. *Aula de Encuentro*, vol. 2, núm. 17, pp. 5-32. Recuperado de https://idus.us.es/xmlui/handle/11441/32243

Castañeda, Linda y Camacho, Mar. (2012). Desvelando nuestra identidad digital. *El Profesional de la Información*, vol. 21, núm. 4, pp. 354-360. doi: http://dx.doi.org/10.3145/epi.2012.jul.04

Chávez Márquez, Irma Leticia y Gutiérrez Diez, María del Carmen. (2015). Redes sociales como facilitadoras del aprendizaje de ciencias exactas en la educación superior. *Apertura, Revista de Innovación Educativa*, vol. 7, núm. 2. Recuperado de http://www.udgvirtual.udg.mx/apertura/index.php/apertura/article/view/698

Chhikara, Jyoti; Dahiya, Ritu; Garg, Neha; Rani, Monika. (2013). Phishing & anti-phishing techniques: Case study. *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, núm. 5, pp. 458-465. Recuperado de http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I3-0315.pdf

Domínguez Pozos, Fernando de Jesús y López González, Rocío. (2015). Uso de las redes sociales digitales entre los jóvenes universitarios en México. Hacia la construcción de un estado del conocimiento (2004-2014). *Revista de Comunicación*, núm. 14, pp. 48-69. Recuperado de http://udep.edu.pe/comunicacion/rcom/pdf/2015/Art048-069.pdf

Eynon, Rebecca & Malmberg, Lars Erik. (2011). A typology of young people's internet use: Implications for education. *Computers & Education*, vol. 56, núm. 3, pp. 585–595. doi: http://dx.doi.org/10.1016/j.compedu.2010.09.020

Ferrari, Anusca. (2013). *DIGCOMP: A framework for developing and understanding digital competence in Europe*. Recuperado de http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=6359

García-Aretio, Lorenzo. (2016). El juego y otros principios pedagógicos. Su pervivencia en la educación a distancia y virtual. *RIED. Revista Iberoamericana de Educación a Distancia*, vol. 19, núm. 2, pp. 9-23. Recuperado de http://revistas.uned.es/index.php/ried/article/view/16175

Garza Mejía, Enrique. (2013). *Uso y consumo de internet en jóvenes estudiantes: análisis del estado de Tamaulipas.* Tesis doctoral. Recuperado de https://dspace.usc.es/bitstream/10347/7511/1/rep_388.pdf

Geller, Tom. (2016). In privacy law, it's the U.S. vs. the world. *Communications of the ACM*, vol. 59, núm. 2, pp. 21-23. doi: http://dx.doi.org/10.1145/2852233

Hall, Mark. (2016).Why people are key to cyber-security. *Network Security*, vol. 2016, núm. 6, pp. 9-10. doi: http://dx.doi.org/10.1016/S1353-4858(16)30057-5

Howe, Neil & Strauss, William. (2000). *Millennials rising: The next great generation*. Nueva York: Vintage.

IGF Spain (2015). *La gobernanza de internet en España*. Presentado en el Foro de la Gobernanza de Internet en España. Recuperado de http://www.igfspain.com/doc/archivos/Gobernanza_Internet_Spain_2015.pdf

Instituto Vasco de Cualificaciones y Formación Profesional. (2014a). Descriptores de competencias digitales del proyecto IKANOS. Recuperado de http://ikanos.blog.euskadi.net/wp-content/uploads/2014/05/IVAC.pdf

Instituto Vasco de Cualificaciones y Formación Profesional. (2014b). Test de autodiagnóstico de competencias digitales. IKANOS. Recuperado de http://ikanos.encuesta.euskadi.net/index.php/566697/lang-es

INTEF (2014). Marco Común de Competencia Digital Docente. Recuperado de http://educalab.es/documents/10180/12809/Marco-ComunCompeDigiDoceV2.pdf

Johri, Aditya; Teo, Hon Jie; Lo, Jenny; Dufour, Monique; Schram, Asta (2013). Millennial engineers: Digital media and information ecology of engineering students. *Computers in Human Behavior*, vol. 33, pp. 286–301. doi: http://dx.doi.org/10.1016/j.chb.2013.01.048

Jones, Chris; Ramanau, Ruslan; Cross, Simon; Healing, Graham. (2010). Net generation or digital natives: Is there a distinct new generation entering university? *Computers & Education*, vol. 54, núm. 3, pp. 722–732. doi: http://dx.doi.org/10.1016/j.compedu.2009.09.022

Lee, Newton. (2014). *Facebook nation. Total information awareness*. Nueva York: Springer.

Martínez Velázquez, Antonio y Flores Sosa, José. (2016). En defensa del anonimato. En J. Lara (ed.). *Internet en México. Derechos humanos en el entorno digital. México: derechos digitales* (pp. 19-55). Recuperado de https://www.derechosdigitales.org/wp-content/uploads/Internet-en-Mx-2016.pdf

Odabasi, Ferhan; Kusu, Abdullah; Gunuc, Selim. (2012). Characteristics of lifelong learner. En P. Resta (ed.). *Proceedings of Society for Information Technology & Teacher Education International Conference 2012* (pp. 4037-4039). Chesapeake, VA: Association for the Advancement of Computing in Education.

Pedró, Francesc. (2006). *The new millennium learners: Challenging our views on ICT and learning.* París: OECD-CERI. Recuperado de http://www.oecd.org/edu/ceri/38358359.pdf

Prensky, Marc. (2001). Digital natives, digital immigrants. *On the Horizon*, vol. 9, núm. 5, pp. 1-6. Recuperado de http://marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

Regil Vargas, Laura. (2014). *Cultura digital universitaria*. Tesis doctoral. Recuperado de http://www.tesisenred.net/bitstream/handle/10803/283956/lrv1de1.pdf?sequence=1

Romo González, José Refugio y Tarango, Javier. (2015). Factores sociodemográficos, educativos y tecnológicos en estadios iniciales de cibercultura en comunidades universitarias. *Apertura, Revista de Innovación Educativa*, vol. 7, núm. 2. Recuperado de http://www.udgvirtual.udg.mx/apertura/index.php/apertura/article/view/626

Serrano Puche, Javier. (2012). *La desconexión digital periódica como parte de la alfabetización mediática.* Presentado en Las Media Enterprises y las Industrias Culturales, Investigar la Comunicación y los Nuevos Medios. III Congreso Internacional Comunicación 3.0. 10 y 11 octubre, Salamanca. Recuperado de http://campus.usal.es/~comunicacion3punto0/comunicaciones /2012/606.pdf

Sieberg, Daniel. (2011). *Digital diet: The 4-step plan to break your addiction and regain balance in your life*. Nueva York: Three River Press.

Steijn, Wouter M. P. & Vedder, Anton. (2015). Privacy concerns, dead or misunderstood? The perceptions of privacy amongst the young and old. *Information Polity*, vol. 20, núm. 4, pp. 299-311. doi: http://dx.doi.org/10.3233/IP-150374

Sullivan, Clare. (2016). Digital citizenship and the right to digital identity under international law. *Computer Law & Security Review*, vol. 32, núm. 3, pp. 474-481. Recuperado de http://dx.doi.org/10.1016/j.clsr.2016.02.001

Suryawanshi, Kavita & Narkhede, Sameer. (2015). Green ICT for sustainable development: A higher education perspective. *Procedia Computer Science*, vol. 70, pp. 701-707. Recuperado de http://dx.doi.org/10.1016/j.procs.2015.10.107

Tapscott, Don (1998). *Growing up digital: The rise of the net generation*. Nueva York: McGraw-Hill.

Tapscott, Don & Williams, Anthony, D. (2008). *Wikinomics: How mass collaboration changes everything.* Nueva York: Atlantic.

Telefónica (2013). Telefónica Global Millennial Survey: Global results. Recuperado de http://survey.telefonica.com/globalreports/

Wąsiński, Arkadiusz & Tomczyk, Łukasz. (2015). Factors reducing the risk of internet addiction in young people in their home environment. *Children and Youth Services Review*, vol. 57, pp. 68-74. doi: http://dx.doi.org/10.1016/j.childyouth.2015.07.022

White, David; David, S.; Le Cornu, Alison. (2011). Visitors and residents: A new typology for online engagement. *First Monday*, vol. 16, núm. 9. Recuperado de http://firstmonday.org/article/view/3171/3049

CÓMO CITAR ESTE ARTÍCULO:

Castillejos, B., Torres, C. y Lagunes, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura, 8,* (2). pp. 54-69. doi: http://dx.doi.org/10.18381/Ap.v8n2.914

Recepción del artículo: 21/05/2016 | Aceptación para publicación: 05/07/2016 | Publicación: 30/10/2016