Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

https://doi.org/10.23913/ride.v12i23.980

Artículos científicos

Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios

Lack of Security of the Personal Information in Educational Digital Applications

Aplicações educacionais digitais e a falta de segurança dos dados pessoais de seus usuários

Paola Iliana de la Rosa Rodríguez
Universidad Autónoma de San Luis Potosí, México
paola.delarosa@uaslp.mx
https://orcid.org/0000-0001-6620-3589

Resumen

Este artículo analiza el uso de plataformas digitales en jóvenes universitarios y su conocimiento sobre los riesgos de exponer su información en estos espacios. Además, estudia el tratamiento de la información por diversas aplicaciones de uso didáctico. Para lograr lo anterior, se realizó un estudio exploratorio e inferencial y se aplicó una encuesta semiestructurada a alumnos de Criminología de la Universidad Autónoma de San Luis Potosí (UASLP). Asimismo, se eligieron 29 plataformas educativas y se analizó si protegen los datos de los usuarios, al igual que, en caso de hacerlo, el alcance de dicha protección. Los resultados evidenciaron que no existen mecanismos que protejan la privacidad y seguridad de la información que manejan las aplicaciones y que la responsabilidad por el mal uso de la información reside en los usuarios. También se encontró que el conocimiento y práctica de métodos para preservar la seguridad cibernética por parte de los internautas de las plataformas educativas tiene relación directa con dicha seguridad, por lo que hace falta un mayor conocimiento de herramientas para proteger los datos personales en el ciberespacio.

Palabras clave: ambientes educacionales, cibercrimen, plataformas virtuales, protección de datos, tecnología educativa.

Abstract

This article analyzes the use of digital platforms in young university students and their knowledge about the risks of exposing their information in these spaces. In addition, it studies the treatment of information by various applications for didactic use. To achieve this, an exploratory and inferential study was carried out and a semi-structured survey was applied to Criminology students from the Universidad Autónoma de San Luis Potosí (UASLP). Likewise, 29 educational platforms were chosen, and it was analyzed whether they protect user data, as well as, if they do, the scope of said protection. The results showed that there are no mechanisms to protect the privacy and security of the information handled by the applications and that the responsibility for the misuse of the information resides with the users. It was also found that the knowledge and practice of methods to preserve cyber security by Internet users of educational platforms is directly related to said security, which is why a greater knowledge of tools is needed to protect personal data in cyberspace.

Keywords: educational environment, cybercrime, virtual platforms, personal information protection, educational technology.

Resumo

Este artigo analisa o uso de plataformas digitais por jovens universitários e seus conhecimentos sobre os riscos de expor suas informações nesses espaços. Além disso, estuda o tratamento da informação por diversos aplicativos de uso didático. Para tanto, foi realizado um estudo exploratório e inferencial e aplicado um questionário semiestruturado a alunos de Criminologia da Universidade Autônoma de San Luis Potosí (UASLP). Da mesma forma, foram escolhidas 29 plataformas educacionais e foi analisado se protegem os dados dos usuários, bem como, caso o façam, o alcance dessa proteção. Os resultados mostraram que não existem mecanismos de proteção à privacidade e segurança das informações tratadas pelos aplicativos e que a responsabilidade pelo uso indevido das informações é dos usuários. Constatou-se também que o conhecimento e a prática de métodos de preservação da segurança cibernética pelos internautas de plataformas

educacionais está diretamente relacionado a essa segurança, razão pela qual é necessário um maior conhecimento das ferramentas de proteção de dados pessoais no ciberespaço.

Palavras-chave: ambientes educacionais, crimes cibernéticos, plataformas virtuais, proteção de dados, tecnologia educacional.

Fecha Recepción: Enero 2021 **Fecha Aceptación:** Julio 2021

Introducción

La pedagogía impartida a través de documentos impresos y de la pizarra está siendo sustituida hoy en día por entornos virtuales que se adecuan a los estilos de enseñanza-aprendizaje de profesores y alumnos y que favorecen el aprendizaje colaborativo, la interactividad y la interdisciplinariedad (Quintero, Munévar y Álvarez, 2009). Siguiendo a Gallado, Marqués y Bullen (2014), resulta ineludible transmutar las aulas en espacios de aprendizaje más atrayentes, participativos y productivos.

En el contexto educativo, los ambientes digitales son contemplados como medios masivos capaces de compartir un mensaje de manera casi inmediata y con una amplia capacidad de almacenar datos. A través de ellos se acortan distancias y se tiene disponible la información a cualquier hora, siempre y cuando se tenga acceso a un dispositivo electrónico conectado a la Red. De acuerdo con López (2007), fue a partir de la década de los 80 cuando en el ámbito universitario se comenzó a utilizar en mayor medida las tecnologías de la información y comunicación (TIC), lo cual ha originado la integración de las diversas herramientas por parte de docentes y estudiantes en los procesos de enseñanza-aprendizaje.

A partir de entonces, las tecnologías han ocasionado que las nuevas generaciones de alumnos adquieran conocimientos de forma distinta, pues su familiaridad con el mundo digital demanda nuevos métodos de enseñanza. En la primera década del siglo XXI, tal y como mencionan Conde y Boza (2019), comenzaron a formarse grupos de alumnos con roles más constructivos, propensos a desempeñarse más en modo virtual que presencial. Se trató de estudiantes pertenecientes a la denominada *generación red*, a quienes se les caracterizó por mostrar una relación cercana con las tecnologías digitales y las innovaciones educativas. El término *generación red* se debe a Don Tapscott (1998). En sus estudios sobre la revolución informática publicados en 1998, este autor refiere que los niños de esta generación han sido educados en la sociedad digital y que ahora, gran parte de ellos ya mayores de edad, se encuentran completamente inmersos en la era digital.

"La juventud se percibe así como un grupo social estrechamente ligado a la digitalización y a las redes" (Crovi, 2010, p. 122). Una generación caracterizada por utilizar equipos de cómputo portátiles con conexión a internet que aprenden a través de comunidades virtuales.

Para Cataldi y Dominighini (2015), las personas nacidas entre los años 1980 y 2000 se desarrollaron en contextos sociales con medios tecnológicos y ahora utilizan las TIC de forma productiva. Están familiarizados con el uso de correos electrónicos, videojuegos, redes sociales, cámaras digitales, buscadores en internet, videochats, geolocalizadores y sistemas inalámbricos. Los dispositivos electrónicos son una extensión de ellos e incluso tienen mayores capacidades tecnológicas que sus maestros. Negroponte (1995) especifica que cada generación ha sido más digital que la anterior.

Ahora bien, la creciente incorporación de espacios electrónicos en el área pedagógica, por un lado, y la utilización del ciberespacio por parte de la delincuencia, por otro, representan nuevos retos para las actuales generaciones de estudiantes. Hoy en día, la seguridad cibernética es un tema que alcanza no únicamente a quienes usan la Red con propósitos comerciales, sino a quienes abren cuentas en plataformas virtuales y utilizan programas educativos en estos espacios.

Teniendo como premisa los riesgos derivados de la exposición de los datos personales en la impartición de cursos con modalidades virtuales, este artículo examina si existe seguridad de la información en los entornos digitales educativos. Para conocer si los usuarios son conscientes de los riesgos en el ciberespacio y si adoptan mecanismos de seguridad en las cuentas que abren con fines educativos, se analizan plataformas y se conduce un estudio exploratorio

La hipótesis que plantea este trabajo es que estas herramientas educativas no ofrecen mecanismos de seguridad suficientes, por lo que ponen en peligro la identidad y privacidad de la información personal y vulneran la protección de los datos personales de los alumnos que se desenvuelven en comunidades virtuales de aprendizaje. No hay duda de que el desconocimiento de los mecanismos de seguridad expone de forma riesgosa la información de los cibernautas.

Materiales y métodos

Con el propósito de comprobar o descartar la hipótesis planteada, primeramente se llevó a cabo un estudio descriptivo-explicativo. Por consiguiente, se recogió y analizó la información obtenida de las herramientas digitales que se muestran en la tabla 1.

Tabla 1. Relación de plataformas objeto de estudio

Blogger	Kahoot	Tes
Calendario Google	Microsoft 365	Trello
Celebrity	Mindmeister	Tumblr
DidacTIC	OneDrive (Microsoft)	Tzaloa (Moodle)
Dropbox	Padlet	WeTransfer
Easybib	Quizizz	Wikia
Edmodo	Remind	WorkFlowy
Evernote	Schoology	Wordpress
Hangouts	Stormboard	Zoho
Jumpshare	Symbaloo	

Fuente: Elaboración propia

Se seleccionaron estas 29 plataformas educativas por ser las que más frecuentemente utilizan los alumnos de la licenciatura, de acuerdo con un sondeo, y con la intención de identificar el tratamiento de datos personales de los usuarios de dichos entornos digitales. Así pues, se analizaron las particularidades de estos espacios virtuales en lo referente a la protección de los datos proporcionados por los usuarios y respecto a si comparten dicha información con terceros. Asimismo, se indagó en quién recae la responsabilidad si hay un mal uso de estos datos personales.

Posteriormente, el mes de abril y mayo del año 2020, se llevó a cabo un estudio exploratorio e inferencial. Como parte de esta fase, se aplicó la encuesta que se incluye en la figura 7 a 155 alumnos de la licenciatura en Criminología de la Universidad Autónoma de San Luis Potosí (UASLP). La muestra incluía a estudiantes de segundo, cuarto, sexto y octavo semestre. Inicialmente, el número total de estudiantes era de 271; de ellos, 205 eran mujeres y 66 hombres, y estaban entre los 18 y 25 años de edad. De esta población, 155 contestaron la encuesta, la cual arrojó un nivel de confianza de 95 % y un margen de error de 5 %. La desviación estándar con respecto a la media es de 2.7.

El instrumento de investigación fue una encuesta semiestructurada (ver anexo) conformada por 14 planteamientos: seis preguntas abiertas y ocho ítems con escala tipo Likert, esto es, cuestionamientos con una gama de opciones de respuesta para que los encuestados puedan elegir. Gracias a estos ítems, se obtuvo información sobre la frecuencia del manejo de plataformas digitales, los propósitos de la utilización de programas o aulas virtuales dentro del curso, los dispositivos de seguridad que emplean, su conocimiento sobre el tratamiento que las plataformas hacen sobre los datos personales y su conocimiento sobre las políticas de privacidad de dichas aplicaciones, entre otros aspectos.

Ahora bien, respecto a la variable inobservable que se quiere medir, que en este caso es la seguridad de los datos personales que se suben a las plataformas, se incluyeron y midieron específicamente los siguientes variables independientes: *a)* la frecuencia con la que utilizan dispositivos de seguridad cibernética, *b)* su conocimiento sobre los avisos y políticas de privacidad de las plataformas, *c)* su conocimiento sobre el tratamiento de los datos personales de las plataformas y *d)* el semestre que cursa el alumno. Se eligieron estos ítems por ser los que se relacionan de manera positiva con la seguridad cibernética.

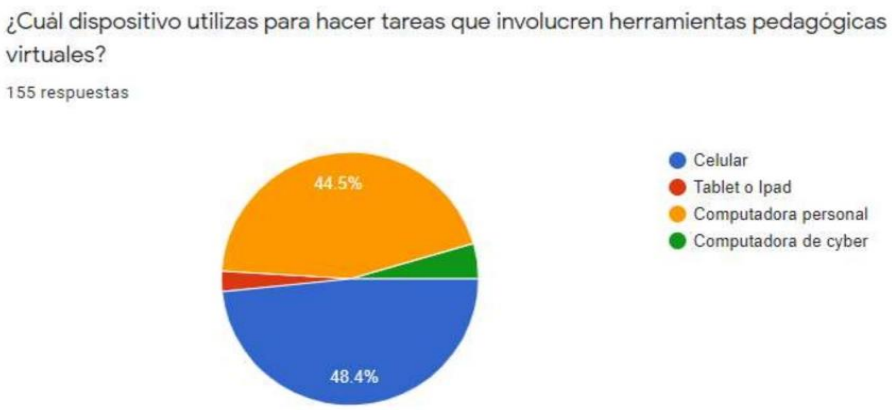
Para determinar la validez del estudio realizado, se utilizó el coeficiente alfa de Cronbach, el cual sirve para medir la fiabilidad de una escala de medida (Campo, 2006). Se calculó mediante la matriz de correlación utilizando Excel. Para ello, a las repuestas a las preguntas dicotómicas sobre el conocimiento de avisos y políticas, así como del tratamiento de sus datos en plataformas, se les asignó el valor de uno si eran negativa y dos si eran afirmativas. Para valorar la frecuencia de dispositivos de seguridad se asignaron los siguientes valores: *1* = Nunca, *2* = Muy rara vez y 3 = Casi siempre. Todos los valores fueron ordenados de menor a mayor. También se incluyó el semestre del alumno encuestado, con el fin de determinar si un semestre más bajo representa menor conocimiento sobre la seguridad cibernética.

Resultados

Uso de plataformas y seguridad cibernética de estudiantes universitarios

En cuanto al dispositivo que los estudiantes utilizan para hacer tareas que involucren herramientas tecnológicas virtuales, se encontró que 48.4 % de la población encuestada utiliza el celular, 44.5 % utiliza computadoras personales, 4 % renta computadoras y 3 % posee tabletas o iPad, tal como se aprecia en la figura 1.

Figura 1. Uso de dispositivos para realizar tareas



Fuente: Elaboración propia

La información que se obtuvo sobre las aplicaciones que utilizan los docentes está señalada en la Tabla 2.

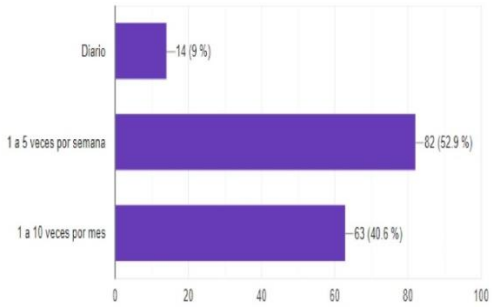
Tabla 2. Plataformas y aplicaciones que más utilizan sus profesores

Schoology	22.6 %
Tzaloa	18.7 %
DidacTIC	14.8 %
OneDrive	14.2 %
Kahoot!	11.6 %
Otras	18.1 %

Fuente: Elaboración propia

Además, 80 % de la población encuestada respondió que integran las plataformas para la realización de tareas y 20 % contestó que las utilizan para la elaboración de proyectos. La figura 2 muestra la frecuencia de uso de estas aplicaciones de la población encuestada.

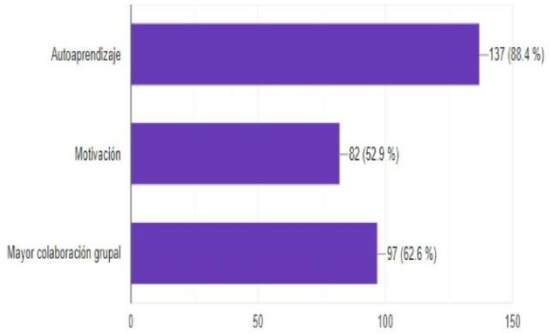
Figura 2. Frecuencia de uso de aplicaciones electrónicas



Fuente: Elaboración propia

Por su parte, la figura 3 muestra lo que buscan los alumnos al usar una herramienta digital.

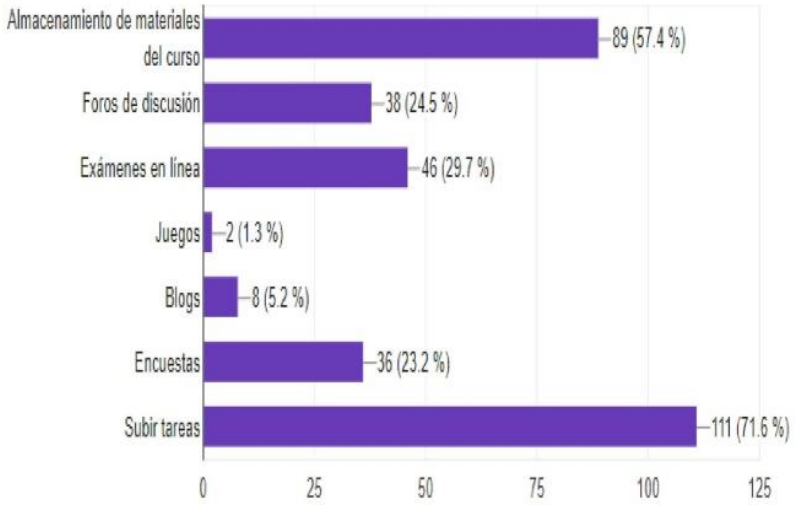
Figura 3. ¿Qué buscan obtener los alumnos al usar una herramienta digital?



Fuente: Elaboración propia

Los propósitos por los que los docentes utilizan las plataformas se enlistan en la figura 4.

Figura 4. Uso de las plataformas durante los cursos



Fuente: Elaboración propia

En materia de seguridad cibernética, 58.1 % de la población encuestada dice conocer de qué se trata, mientras que 41.9 % desconoce a qué se refiere.

Los métodos de seguridad que conocen la población encuestada se muestran en la tabla 3.

Tabla 3. Métodos de seguridad utilizados por los estudiantes

Antivirus	36.8 %
Contraseñas	20 %
Otras	20.6 %
No las conoce	22.6 %

Fuente: Elaboración propia

Las situaciones que ponen en riesgo o comprometen la seguridad de los datos de los alumnos figuran en la tabla 4.

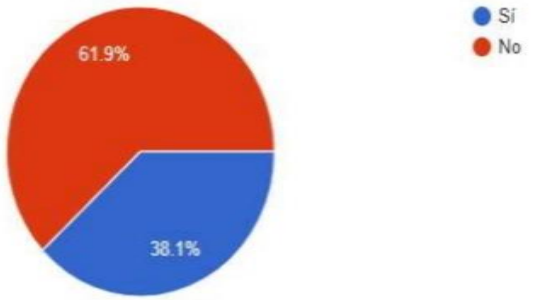
Tabla 4. Condiciones que arriesgan la seguridad de los datos personales

No cerrar apropiadamente su sesión	40.6%
Aceptar el uso de cookies	27.7%
Utilizar computadoras públicas	21.3%
Crear una cuenta	10.3%

Fuente: Elaboración propia

La mayoría de los alumnos manifiesta tener conocimiento sobre el tratamiento de sus datos personales en las plataformas educativas que utilizan (61.9 %) (ver figura 5).

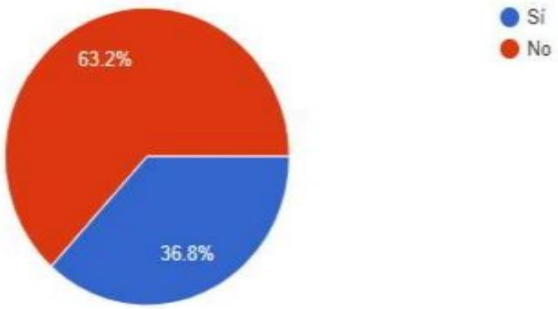
Figura 5. Estudiantes que conocen el tratamiento de las plataformas educativas hacia sus datos personales



Fuente: Elaboración propia

Respecto a los avisos y políticas de privacidad de las plataformas educativas, se obtuvo lo expuesto en la figura 6.

Figura 6. Estudiantes que conocen los avisos y políticas de privacidad de las plataformas educativas



Fuente: Elaboración propia

Más de la mitad de los estudiantes encuestados no lee los avisos y políticas de privacidad de los programas y aplicaciones y desconoce el manejo de la información personal que ingresan a las plataformas. Asimismo, 40 % de los estudiantes encuestados no hizo referencia a los métodos de seguridad utilizados, pues cerca de este mismo porcentaje desconoce el tema de la seguridad cibernética. Por lo tanto, el patrón conductual persistente en los alumnos es que no se informan sobre el destino de los datos personales que ingresan en la Red y tampoco existe una preocupación de estos por conocer y aplicar mecanismos de seguridad.

En cuanto a la variable inobservable, a saber, la seguridad cibernética, se empleó el alfa de Cronbach para los cuatro ítems que se consideraron en la encuesta: de una muestra de 155 sujetos resultó de 0.77. Este es un valor de grado alto, por lo que el instrumento de recolección de datos que se construyó presenta una alta fiabilidad (Celina y Campo, 2005). Se utilizó la siguiente fórmula:

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

Donde las variables representan lo siguiente:

α: Alfa de Cronbanch.

k: Número de ítems.

V_i: Varianza de cada ítem.

V_t: Varianza del total.

Tabla 5. Estadísticos de la escala

k	Vi	Vt	α
4	6.660	15.876	0.773966601

Fuente: Elaboración propia

La tabla 5 muestra los valores de las variables en este estudio. Los resultados arrojan que sí existe una correlación entre la seguridad cibernética de los alumnos encuestados, la cual depende tanto del número de semestres que han cursado como de la frecuencia de uso de sus dispositivos, de la verificación que hacen de los avisos y políticas de privacidad y del conocimiento del manejo de los datos personales por parte de las plataformas electrónicas. Estos últimos constituyen patrones de conducta que influyen en la

seguridad de los usuarios, pues tienen relación con la exposición arriesgada de su información a través de las plataformas.

Cabe mencionar que en la UASLP se han estado habilitando redes sociales como un medio de información y comunicación para sus programas educativos. A manera de ejemplo, en el año 2016 se incrementaron los cursos registrados que utilizan las plataformas Tzaloa (Moodle) y DidacTIC, lo cual puede repercutir en que más datos de alumnos queden expuestos a la inseguridad del ciberespacio. Aún más, a partir de la pandemia, se está utilizando Microsoft Teams, así como otras aplicaciones por las que optan los docentes.

Ahora bien, concatenando estos resultados y debido a que los docentes de la UASLP se apoyan de otras herramientas electrónicas para la impartición de sus cursos, este estudio pretende conocer los mecanismos de seguridad y el tratamiento que las plataformas educativas tienen para con sus usuarios.

Para este estudio, las aplicaciones educativas estudiadas se clasificaron de la siguiente forma:

- ocho herramientas que constituyen plataformas de trabajo,
- tres herramientas para almacenar datos,
- diez herramientas para debatir y colaborar,
- cinco herramientas para organizar trabajo y
- tres juegos.

Una vez que se recabó la información de cada una de las 29 aplicaciones o programas, se procedió a estudiar, cuantificar y analizar si estas páginas ofrecen mecanismos de seguridad. Después de examinar las políticas de privacidad de cada compañía y otros aspectos buscados en esta investigación, se obtuvieron los siguientes resultados (ver tabla 6).

Tabla 6. Concentrado sobre el tratamiento de datos personales en plataformas con fines educativos

	Plataformas de trabajo	Almacenamiento	Debate y colaboración	Organizadores de trabajo	Juegos	Total de plataformas
¿Comparte información de usuarios con terceros?	7	3	8	5	2	25
Requiere el consentimiento del usuario para permitir que terceras partes usen el contenido de sus datos pero lo hace a través del aviso privacidad (que pocas veces se lee).	8	2	6	4	0	20
La responsabilidad por el uso de los datos recae en el usuario o menciona que no se hace responsable	8	3	10	5	3	29
¿Regula la protección de los datos de menores de edad?	5	0	5	1	1	12

Fuente: Elaboración propia

Es de destacar que 25 de los sitios analizados señalan expresamente que sí comparten información del usuario con terceros, incluso establecen que no controlan ni responden cómo terceras partes puedan tener acceso a información de sus usuarios. No obstante lo anterior, los sitios utilizan *cookies* propias y aceptan *cookies* de terceras partes como proveedores, empresas de *marketing*, entre otras, que obtienen y analizan datos de los usuarios para adaptar contenidos, mejorar los servicios y mostrarles publicidad relacionada con sus preferencias mediante el análisis de los datos de navegación, pero con quienes el usuario de las plataformas educativas no abrió alguna cuenta personal y de quienes no sabe el destino y utilización que puedan ejercer sobre sus datos. Otro aspecto importante son las compañías que administran varios servicios en la Red; las empresas administradas por Google, por ejemplo, señalan que los servicios y aplicaciones que funcionan en un

dispositivo se comunican con otros servidores que ofrece la empresa y aclaran que pueden compartir entre sí la información del usuario. Además, las aplicaciones reciben un sinnúmero de visitantes desconocidos que pueden romper estos controles de seguridad.

Únicamente 68 % de las páginas analizadas requiere consentimiento para permitir que terceras partes usen el contenido de los datos y, como se analizó, lo hacen a través de la aceptación del aviso de privacidad, paso obligatorio para generar la cuenta electrónica que da acceso al sitio. Es una generalidad que las empresas administradoras de la plataforma compartan los datos o permitan a servidores tener acceso a estos; lo que las compañías señalan es que, en todo caso, si el usuario desea negar que se compartan sus datos personales, habrá que configurar la cuenta para este propósito, situación que solo es posible cuando la página tiene esta opción.

Todas las páginas analizadas se deslindan de la responsabilidad del mal uso de los datos que ingresan los usuarios. Específicamente, 20 transfieren al usuario la responsabilidad por el mal uso de los datos que ingresan los usuarios, 10 aplicaciones no señalan en quién recae la responsabilidad y se deslindan de ello. Se encontró que ciertas empresas transfieren dicha responsabilidad al controlador, que es "la persona física o moral, autoridad pública, dependencia u otro organismo que solo, o en conjunto con otros, determina la finalidad y los medios para procesar los datos personales".

Como se puede observar, el patrón general de las compañías que administran las plataformas es permitir que se compartan los datos del usuario y no hacerse responsable por los datos que ingresen los usuarios. Además, se advierte que cada país tiene sus políticas sobre privacidad, transferencia de datos y las aplicaciones tienen derechos distintos para usuarios americanos, europeos y latinoamericanos, lo que puede llegar a crear confusión al respecto.

Otro dato importante es que las generaciones más jóvenes son más propensas que las generaciones de adultos a proporcionar información personal sin mayores controles (Norton, 2018).

En cuanto a las plataformas utilizadas por la población encuestada, se registraron los resultados en la tabla 7.

Tabla 7. Tratamiento de datos en las plataformas usadas por alumnos de Criminología de la UASLP

	Tzaloa	DidacTIC	Schoology	OneDrive
¿Comparte información de usuarios con terceros?	Sí	Sí	Sí	Sí
Requiere el consentimiento del usuario para permitir que terceras partes usen el contenido de sus datos pero lo hace a través del aviso de privacidad.	Sí	Sí	Sí	Sí
La responsabilidad por el uso de los datos recae en el usuario o menciona que no se hace responsable.	Sí	Sí	Sí	Sí

Fuente: Elaboración propia

El número de usuarios de dispositivos tecnológicos e Internet va en aumento. Y según lo detectado aquí, los índices de inseguridad de datos personales pueden crecer conforme el número de internautas vaya creciendo. La Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares Mexicanos (Endutih) (Instituto Nacional de Estadística y Geografía [Inegi], 2018) documentó que en el 2018 existieron 50 845 170 usuarios de computadora, 74 325 379 usuarios de Internet y 83 079 732 usuarios de teléfono móvil. Según los grupos de edad, 9 226 846, esto es, 18.1 % del total de cibernautas del país, fueron usuarios de entre 18 a 24 años. Aunado a ello, documentó que 23 757 297 personas fueron usuarios de computadoras para labores escolares. La computadora fue utilizada en ese año por 18 620 599 estudiantes con grado de licenciatura. Finalmente, 13 201590 de los usuarios de telefonía celular tenían de 18 a 24 años.

Con la información anterior se infiere que vivimos en un mundo digital en donde recolectar y almacenar datos de personas es más la norma que la excepción. Si bien es un hecho que las empresas recolectan información personal con fines de analítica, investigación, publicidad o *marketing*, muchas veces no sabemos en dónde termina esa información. Hoy en día la cibercriminalidad es un fenómeno creciente en el planeta y estos criminales se valen precisamente de la información que ingresan los internautas para llevar

a cabo robos de identidad, usurpación de identidad, robos y crímenes contra la propiedad intelectual, entre otros.

Discusión

¿Se puede hablar de privacidad digital en los entornos digitales?

En primer término, los métodos de enseñanza han incorporado herramientas didácticas que se apoyan de dispositivos electrónicos y de Internet. Los estudiantes observan, buscan, transforman información y realizan actividades académicas a través de diversas aplicaciones. Los profesores han implementado libros o textos digitales, portales de búsqueda, sistemas de archivo y almacenamiento de contenidos, e-portafolios, juegos educativos, discusiones en foros digitales o chats y otras herramientas de colaboración en línea. Dichos docentes guían a sus estudiantes para que se autodescubran y puedan formular sus propias ideas y realizar interconexiones para alcanzar sus metas (Amaya, Zúñiga, Salazar y Ávila, 2018).

Con la finalidad de utilizar estos recursos, los docentes y alumnos ingresan y confían datos personales y otros productos de nuestra creatividad a los sitios e interfaces, desconociendo el buen o mal uso que puedan hacer de estos. Por lo general, estas aplicaciones y programas requieren que el usuario genere una cuenta y proporcionen datos personales tales como el nombre, edad, día, mes y año de nacimiento, apodo, nombre de usuario, contraseña, algunos otros solicitan foto, ocupación y los sitios que son de paga tendrán los datos de la tarjeta de crédito y dirección para facturación.

Además, tal como dijeran Rallo y Martínez (2011), todos, de manera inconsciente, al buscar o realizar una compra en Internet, vamos dejando una huella sobre lo que nos interesa, lo que abre la posibilidad de que extraños puedan conocer nuestras actividades y preferencias. En otras palabras, el internauta va dejando rastros valiosos de su identidad que se traducen en información personal, la cual llega a tener un valor que depende de los propósitos del que la obtenga.

Mucha de la información que subimos a estas plataformas queda a la vista de todos los cibernautas; otros datos, a pesar de no quedar expuestos, pueden ser hackeados por técnicos informáticos que obtienen acceso no autorizado a estas aplicaciones y páginas.

Aunado a lo anterior, derivado de las *cookies*,[1] se puede obtener información sobre hábitos, intereses, lo cual puede ser utilizado en perjuicio del internauta (Norton, 2018). Surge, entonces, el consecuente planteamiento sobre la privacidad que se tiene sobre la información que ingresamos en los ambientes virtuales: ¿existen datos personales en ambientes virtuales y redes sociales?

Hay que tomar en cuenta que las redes informáticas que usan docentes y alumnos son lugares intangibles y que, si bien es cierto que no podemos decir que una injerencia en las comunicaciones o en la compartición de información personal en el terreno digital es una violación a la privacidad del domicilio,[2] sí podemos demandar que los espacios o medios a través de los cuales se almacena o comparte nuestra información sean protegidos, así como se protege el domicilio de las personas, pues existe una expectativa de privacidad en un gran número de operaciones y actividades que llevamos a cabo en sitios electrónicos. Entonces, lo que se debe de considerar para que la norma jurídica proteja esta información, es la expectativa de intimidad que tiene un individuo con respecto a los lugares a los que ingresa, independientemente de que sean físicos o virtuales.

Si alguien ingresa sin nuestro consentimiento y altera, hace uso o se apodera de esos datos, viola nuestro derecho a la privacidad y, por ende, comete una acción ilícita que merece ser sancionada. Por ello, la garantía de privacidad en las comunicaciones debe alcanzar la información compartida y las actividades llevadas a cabo en estos terrenos. Los correos electrónicos y la información personal quedan comprendidos en dicha protección.

Específicamente, la expectativa de privacidad de las plataformas educativas radica en que para acceder a la información se requiere de un proveedor de acceso al servicio, nombre de usuario y clave de acceso, y debido a que solo el destinatario es el que cuenta con su clave personal, solo él tiene la posibilidad de conocer su contenido. Ahora, está la posibilidad técnica de tener acceso al contenido, sin embargo, esta no implica tener la posibilidad jurídica. Y ante la posibilidad técnica de terceras personas de acceder a nuestros contenidos, debe surgir el derecho a la protección de nuestra información, la cual debe de estar respaldada tanto por mecanismos rigurosos de seguridad de los proveedores

[1] Una *cookie* es un archivo que contiene cantidades de datos que se envían entre un emisor, que es el servidor donde está alojada la página web, y un receptor, que es el navegador que se usa para visitar cualquier página web, con el objetivo de identificar el historial de actividad de los internautas, recabar direcciones y contraseñas del correo electrónico, teléfono y dirección, dirección de IP, el sistema operativo de nuestra computadora, el navegador que utilizamos y las páginas que hemos visitado anteriormente, entre otra información.

[2] Puesto que se dificulta asimilar el espacio cibernético al domicilio tradicional.

o administradores del servicio como por regulaciones jurídicas que penalicen injerencias a nuestra privacidad.

En esta misma línea, el respeto a la protección de la privacidad de la información se debe extender a y debe contemplar las "nuevas" formas de comunicación a través de internet. Además, habrá de tomarse en consideración que lo que se protege es el carácter privado de las comunicaciones independientemente del contenido de estas.

Además, como se dijo anteriormente, el acceso a estos sitios de Internet permite que otras compañías tengan acceso a nuestra navegación, tendencias y preferencias, y con ello a nuestra información personal. Surge entonces la vinculación del uso de tecnología educativa con la protección de la privacidad de la información y con la seguridad cibernética.

De acuerdo con un reporte publicado en el año 2016 por Norton, entre los mayores riesgos que toman los cibernautas se encuentran:

- 34 % no protege los dispositivos que tienen en sus hogares.
- 66 % no protege la red wifi en sus casas.
- 61 % ingresó información financiera en la Red cuando estaban conectados en lugares públicos.

La seguridad cibernética o informática está formada por aquellas medidas de seguridad o barreras tanto físicas (contando entre ellas a puertas y cerraduras) como lógicas (como las contraseñas) que los usuarios ponemos a fin de proteger nuestros bienes informáticos y nuestra información, considerada como un bien jurídico tutelado.

El informe de Norton (2016) señala que 76 % de los usuarios sabe que debe de proteger su información, sin embargo, llega a compartir sus contraseñas o llevan a cabo acciones riesgosas al estar usando la Red. De acuerdo con sus estimaciones, 35 % de los internautas tienen al menos un dispositivo sin controles de seguridad, por lo que quedan desprotegidos ante las habilidades de los ciberdelincuentes.

Conclusiones

La hipótesis de este trabajo plantea que las plataformas educativas no proveen mecanismos de seguridad. De acuerdo con la exhaustiva revisión en los sitios elegidos, 86 % de ellos comparte información del usuario con terceros y no controla el acceso que terceras partes puedan tener a la información de sus usuarios. El total de las plataformas transfiere al usuario la responsabilidad por el uso de los datos o no se hace responsable del tratamiento de los datos. Además, 68 % de los sitios permite que terceras partes usen el contenido de los datos del usuario.

En cuanto al conocimiento que los usuarios tienen sobre la seguridad cibernética, de una muestra con 95 % de nivel de confianza, 58.1 % de la población encuestada conoce de qué se trata, mientras que 41.9 % no sabe a qué se refiere. Aunado a ello, 40 % de los alumnos encuestados manifiesta no cerrar apropiadamente su sesión y 27.7 % señala aceptar el uso de cookies en sus dispositivos.

En esa misma línea, 62 % de la muestra encuestada no conoce el tratamiento de las plataformas educativas hacia sus datos personales; únicamente 38 % manifiesta conocerlo. Por si fuera poco, tan solo 36.8 % de la población encuestada conoce los avisos y políticas de privacidad de las plataformas educativas, el resto, 63.2 %, no conoce su contenido.

Finalmente, 40 % de los estudiantes encuestados no hizo referencia a los métodos de seguridad utilizados, pues cerca de este mismo porcentaje desconoce el tema de la seguridad cibernética. Por lo tanto, el patrón conductual persistente en los alumnos es que no se informan sobre el destino de los datos personales que ingresan en la Red y tampoco muestran interés por conocer y aplicar mecanismos de seguridad en su información.

Ahora bien, siendo la variable dependiente la seguridad cibernética de los usuarios de plataformas educativas, se encontró que la frecuencia de uso de sus dispositivos, la verificación que hacen de los avisos y políticas de privacidad, así como el conocimiento del manejo de los datos personales por parte de las plataformas electrónicas, tienen una relación directa con la seguridad de la información de los cibernautas. Estos últimos constituyen patrones de conducta que influyen en la seguridad de los usuarios, pues tienen relación con la exposición arriesgada de su información a través de las plataformas. La fiabilidad del estudio se obtuvo mediante el coeficiente alfa de Cronbach. El coeficiente que se obtuvo del estudio fue 0.77, resultando válido el estudio.

Con este estudio se advierte que no existen mecanismos plenos seguridad por parte de los proveedores de servicios de internet en lo que a la privacidad de los datos personales

se refiere y que este fenómeno impone mayores retos al usuario. Por último, los gobiernos deben promover la cultura de la seguridad cibernética e impulsar acciones para proteger a los cibernautas proporcionándoles el conocimiento necesario para proteger la información que ingresen en la red.

Futuras líneas de investigación

Una vez descubierto que los datos de los usuarios de la red no gozan de una plena protección, un sendero de interrogantes se abrió ante nosotros: ¿quiénes recopilan nuestra información?, ¿tienen derecho a obtenerla?, ¿cómo la recopilan?, ¿qué hacen con nuestra información? y ¿cómo la utilizan? El estudio del tratamiento de los datos y rastros que dejamos en las plataformas digitales puede dar origen a trabajos que analicen y colmen estas inquietudes.

Referencias

Amaya, A., Zúñiga, E., Salazar, M., y Ávila, A. (2018). Empoderar a los profesores en su quehacer académico a través de certificaciones internacionales en competencias digitales. *Apertura. Revista de Innovación Educativa*, *10*(1), 104-115. Recuperado de http://www.scielo.org.mx/scielo.php?pid=S1665-61802018000100104&script=sci_arttext&tlng=pt.

Campo, A. (2006). Usos del coeficiente de alfa de Cronbach. *Biomédica*, *26*(4), 585-588.

Cataldi, Z. y Dominighini, C. (2015). La generación millennial y la educación superior. Los retos de un nuevo paradigma. Revista de Informática Educativa y Medios Audiovisuales, 12(19), 14-21.

Celina, H. y Campo, A. (2005). Aproximación al uso del coeficiente alfa de Cronbach. *Revista Colombiana de Psiquiatría*, *34*(4), 572-580.

Conde, S. y Boza, A. (2019). La educación del futuro: perspectiva del alumnado. Validación de una escala. *Apertura. Revista de Innovación Educativa*, *11*(2), 86-103. Recuperado de http://www.udgvirtual.udg.mx/apertura/index.php/apertura/article/view/1518.

Crovi, D. (2010). Jóvenes, migraciones digitales y brecha tecnológica. *Revista Mexicana de Ciencias Políticas y Sociales*, *52*(209), 119-133.

Gallado, E., Marqués, L. y Bullen, M. (2014). Usos académicos y sociales de las tecnologías digitales del estudiante universitario de primer año. *Tendencias Pedagógicas*, *23*, 191-204. Recuperado de https://revistas.uam.es/tendenciaspedagogicas/article/view/2079.

Instituto Nacional de Estadística y Geografía [Inegi]. (2018). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (Endutih) 2018. México: Instituto Nacional de Estadística y Geografía. Recuperado de https://www.inegi.org.mx/programas/dutih/2018/default.html.

López, M. C. (2007). Uso de las TIC en la educación superior de México. Un estudio de caso. *Apertura. Revista de Innovación Educativa*, *7*(7), 63-81. Recuperado de http://www.udgvirtual.udg.mx/apertura/index.php/apertura4/article/view/94/105.

Negroponte, N. (1995). *Being Digital*. United States: New York: Knopf.

Norton. (2016). *Norton Cyber Security. Insights Report*. United States: Norton. Retrieved from https://us.norton.com/cyber- security-insights.

Norton. (2018). Norton LifeLock Cyber Safety. Insights Report. United States: Norton. Retrieved from https://us.norton.com/cyber-security-insights-2018.

Quintero, J., Munévar, F. y Álvarez, D. (2009). Ambientes naturales y ambientes virtuales de aprendizaje. *Revista Colombiana de Educación*, (56), 12-37.

Rallo, A. y Martínez, R. (2011). Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. *Quaderns del CAC*, *14*(2), 41-52. Recuperado https://www.cac.cat/sites/default/files/2019-01/Q37_Rallo_Martinez_ES.pdf.

Tapscott, D. (1998). *Growing Up Digital: The Rise of the Net Generation*. New York, United States: McGraw-Hill.

Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

Anexo

Figura 7. Encuesta realizada a estudiantes de Criminología de la UASLP

AGRADECEMOS TUS RESPUESTAS A LA SIGUIENTE ENCUESTA. Semestre:_____

¿Cuántos docentes de este semestre incluyen tecnología en la enseñanza? _____

¿Cuáles son los dispositivos más usados por el profesor en su enseñanza? _____

¿Qué plataforma(s) didáctica(s) utilizan en sus cursos? _____

¿Con qué frecuencia usan plataformas virtuales en general? a) diario, b) ___ veces por semana, c)___ veces por mes

¿Con qué propósito las(os) utilizan? a) Almacenamiento de materiales del curso e) juegos
b) Foros de discusión f) blogs
c) Exámenes en línea g) encuestas
d) Otro? Cuál? O cuáles?_____

¿Cómo las integran al desarrollo del curso? a) tareas, b) proyectos, c) otro: cuál?_____

¿Que buscan los alumnos de un recurso virtual?

a) autoaprendizaje b) motivación c) mayor colaboración grupal d) otra:_____

¿Cuál dispositivo utilizas para hacer tareas que involucran herramientas pedadógicas virtuales?

a) Celular
b) Tableta o ipad
c) Computadora personal
d) Computadora de cyber

¿Sabes que es la seguridad cibernética? Si. No. Explica._____

_____

En tu opinión, en cuál de las siguientes puedes poner en riesgo (comprometer) la seguridad de tus datos?
a) Al crear una cuenta
b) Al aceptar el uso de cookies
c) Al no cerrar propiamente una sesión
d) Al utilizar computadoras públicas

Nombra 3 sistemas de seguridad digitales que conozcas _____

¿Con qué frecuencia utilizas dispositivos de seguridad cibernética?
a) Nunca
b) Muy rara vez
c) Casi siempre
d) Siempre

¿Cómo te proteges ante la inseguridad cibernética?

_____

¿Conoces los avisos y políticas de privacidad (+) así como el tratamiento de los datos personales (++) de las plataformas educativas que utilizas?(+) _____ (++) _____

Fuente: Elaboración propia