

Universidad Autónoma del Estado  
de México

<https://recai.uaemex.mx>

ISSN: 2007-5278

Publicación cuatrimestral

Año: 7 No: 20

Septiembre / Diciembre 2018

## Artículo

---

### Autores:

Norma Martínez López\*

*Sistema de Universidades Estatales  
de Oaxaca*

Roselia Martínez López

*Instituto de Estudios de Bachillerato  
del Estado de Oaxaca*

### Fecha recepción:

22 de junio de 2018

### Fecha aceptación:

3 de diciembre de 2018

### Páginas:

14 – 35

\*nacademicoinv@hotmail.com

## Los jóvenes y la ciberseguridad en zonas rurales del estado de Oaxaca. Caso: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165.

Young people and cybersecurity in rural areas of the state of Oaxaca.  
The case of the State of Oaxaca Institute of Baccalaureate Studies  
(IEBO), campus 165.

### Resumen

Hoy en día cada, cada vez más jóvenes y niños están conectados a Internet exponiendo en línea su información y datos personales. Sin embargo, algunos jóvenes desconocen los riesgos que esto implica ya que no cuentan con información sobre ciberseguridad (p.ej. seguridad de la información y datos personales). Este fenómeno se agrava en las zonas rurales donde la tecnología aún es precaria y se desconocen los peligros y riesgos de Internet. Por ello, el objetivo de este estudio es dar a conocer los resultados sobre la información que tienen los jóvenes de educación media superior en zonas rurales del estado de Oaxaca con respecto a temas de ciberseguridad (p.ej. seguridad, privacidad y protección de la información y datos personales). La información se obtuvo mediante la aplicación de una encuesta sobre tales temas. Se sustenta la importancia de implementar un plan de estudios con una asignatura orientada a la seguridad informática..

### Palabras clave:

Seguridad de la información, privacidad de la información, jóvenes, plan educativo, zonas rurales.

### Abstract

Nowadays, an increasing number of youngsters and children are connected to the Internet, having their information and personal data exposed online. However, some of them are unaware of the risks that such practice implies, as they do not have information on cybersecurity matters (e.g. the security of the information and personal data). This situation is exacerbated in rural areas where technology is still precarious and the dangers and risks of the Internet are unknown. Because of this, the objective of this study is to expose some results about the information that young people from high school have in rural areas of the state of Oaxaca on cybersecurity issues (e.g. safety, privacy and protection of information, and personal data). The information was obtained by applying a survey on such topics. The importance of implementing a curriculum including a course on computer safety is posited.

### Keywords:

Information security, information privacy, youth people, educational plan, rural areas.

## 1. Introducción

La tecnología ha evolucionado y continuará su desarrollo, por lo que cada vez más jóvenes y niños usan Internet y tienen su información personal en línea. Sin embargo, algunos de estos usuarios aún desconocen los riesgos que esto implica, debido a que no se tiene una cultura de la seguridad y privacidad de la información. Por otra parte, algunos desconocen los derechos que tienen sobre sus datos personales, como: el derecho a la privacidad y seguridad de su información íntima. También existen algunos que desconocen cuáles son las leyes e instituciones que protegen sus datos personales. Esto se empeora en las zonas rurales donde aún la tecnología es escasa y el Internet es limitado, como el caso del Estado de Oaxaca.

Oaxaca es un Estado que se ubica en la región suroeste de los Estados Unidos Mexicanos y cuenta con un total de 570 municipios (Instituto Nacional para el Federalismo y el Desarrollo Municipal [INAFED], 2010). De acuerdo con el Censo de Población y Vivienda 2010 del Instituto Nacional de Estadística y Geografía (INEGI), cuenta con un total de población de 2,842, 808, de las cuales 1, 004,517 habla lengua indígena. El INEGI clasifica a las localidades en urbanas y rurales por la cantidad de habitantes, es decir, de 1000 a 2,499 habitantes se considera rural, y de 2,500 en adelante es urbana. Oaxaca es un Estado que cuenta con localidades y municipios rurales. El objeto de este estudio es la localidad de Río Anona perteneciente al Municipio de San Simón Almolongo, que tiene un total de 11 localidades, y cuenta con un total de población de 1,986, de los cuales 7 hablan lengua indígena (INEGI, 2010a), y además, es un municipio rural.

Ahora bien, en las zonas rurales del Estado el uso de la tecnología también está presente. Sobre la disponibilidad y uso de computadoras en áreas rurales, el Estado tiene una población total de 3, 657,437, de la cual se tiene un total de usuarios de computadora en áreas rurales de 1, 909,138, pero 432,768 si usa y 1, 476, 370 no la usa. En cuanto al uso de Internet, se tiene un total de usuarios de Internet en áreas rurales de 1, 909,138, de los cuales, los que usan Internet son un total de 689, 470, y un total de 1, 219, 668 no usan. En lo que respecta al uso del celular, hay un total de 1 909 138 usuarios en áreas rurales, de los cuales, 816, 784 si usa el celular, y 1,092, 354 no lo usa (INEGI, 2017).

Respecto a la tecnología, el Municipio de San Simón Almolongo tiene un total de 20 viviendas particulares habitadas que disponen de computadora, 156 de teléfono celular y 7 de Internet. La localidad de Río Anona tiene un total de 4 viviendas particulares habitadas que disponen de computadora, 20 de teléfono celular y 0 de Internet (INEGI, 2010b). De acuerdo a los datos presentados, se puede observar que en la entidad Oaxaqueña aun cuando el uso de la tecnología es precario, más aún, en sus áreas rurales, esta no está ausente. Por lo que es importante que estas áreas que se encuentran en desventaja tecnológica tengan acceso a la información sobre la ciberseguridad, puesto que no por ser zonas alejadas de la urbanización, no están

exentos de los peligros que representa el ciberespacio. Recalcando el uso indebido que hacen los jóvenes en Internet.

Los ciberdelincuentes cada día están buscando nuevas víctimas y formas de ocultar sus ataques. De acuerdo al artículo 6° de la constitución mexicana (Instituto Federal de Acceso a la Información Pública [IFAI], 2007), se considera necesario que los niveles educativos sean el pilar para empezar a contrarrestar los ataques de los piratas informáticos sobre los datos personales e íntimos y formar una cultura de la seguridad de la información. Aparte de esta necesidad, la privacidad de la información como un derecho de los ciudadanos debe ser una prioridad para los gobiernos y ciudadanos. El objetivo de este documento es dar un panorama sobre los conocimientos que tienen los jóvenes del Instituto de Estudios de Bachillerato del Estado de Oaxaca, plantel 165 ubicado en la comunidad de Río Anona, sobre el tema de la seguridad, privacidad y protección de la información enfocados a la ciberseguridad, y hacer ver la importancia de generar una cultura de la seguridad de la información. De igual forma, sustentar que en los diferentes niveles educativos aún falta implementar en el plan de estudios una asignatura enfocada a la seguridad de la información para proteger los datos personales e íntimos en Internet, de manera que los niños y jóvenes adquieran mejores prácticas para proteger sus datos personales digitales.

El artículo se desarrolla en los 5 apartados siguientes. 1) Introducción. 2) revisión de literatura. 3) metodología. 4) resultados. 5) por último se presentan las conclusiones del estudio.

## **2. Revisión de literatura**

### **2.1 Ciberseguridad**

Ciberseguridad es un concepto que aún se encuentra en desarrollo y no se tiene una definición única puesto que existen múltiples factores, perspectivas e intereses. Por ejemplo, se incorporan temas como: agendas políticas, estabilidad del Estado, seguridad de las aplicaciones y servicios, seguridad de los usuarios, seguridad de infraestructura nacional, infraestructura de Internet, entre otros (Tecnología y Comunicación, 2016). En los últimos años se ha generado un debate internacional sobre la seguridad cibernética, lo que refleja el deseo de las naciones de responder a las tendencias de los recursos mundiales cibernéticos (Observatorio de la ciberseguridad en América Latina y el Caribe, 2016).

Antes de llegar a la conceptualización de ciberseguridad, se hace referencia al término de “ciberespacio” que surge de la mano de la ciencia ficción. Fue William Gibson en su novela “Mona Lisa Acelerada” quien plantea por primera vez la idea de un “ciberespacio”, el cual se puede entender como un campo donde el ser humano puede construir un mundo donde realiza lo que desea, se proyecta de la manera que le plazca y obtiene aquello que el mundo físico le niega o le condena a no tener (Programa Sociedad de la Información y el Conocimiento [PROSIC], 2010, p. 27).

El mundo ahora está interconectado principalmente por la Internet, lo que conduce no solo a obtener ventajas, sino también estar en constante riesgo debido a las inseguridades del ciberespacio o mundo virtual. La ciberseguridad también es conocida como seguridad informática, cuya área se enfoca a la protección de la

infraestructura computacional y todo lo relacionado con esta, tal como a la seguridad de la información, protección de datos personales, seguridad física, por mencionar. La Unión Internacional de Telecomunicaciones [ITU] (2018, párr.1), la define como “el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno [...]”.

## 2.2 Datos personales

Hoy en día, Internet es una herramienta que más ciudadanos están utilizando. Los más jóvenes han crecido en un ambiente tecnologizado; se comunican a través de redes sociales como miembros de comunidades no geográficas y están conectados durante todo el día a través de dispositivos móviles (Ayala, 2015). Desde este punto, la hiperconectividad está ligada a todos los sistemas de comunicación digital que permiten que los individuos se conecten entre sí, bien porque poseen vínculos afectivos, comparten aficiones, actividades, creencias u objetivos comunes. La hiperconectividad se refiere a la gran cantidad de formas de comunicación intermediadas por la tecnología, o a la disponibilidad de las personas para comunicarse en cualquier lugar y en cualquier momento (Ayala, 2015), convirtiéndose así en hiperusuarios. Se entiende por hiperusuario a la categoría que abarca a todos esos usuarios que hacen un uso considerablemente intensivo de un producto o servicio, en este caso la tecnología la integran en sus vidas privadas o trabajos y han generado una relación casi de dependencia con ella (Lages, 2008).

Cabe mencionar que la hiperconectividad puede representar altos riesgos al almacenar información íntima en Internet de los hiperusuarios, y sobre todo con las constantes amenazas de los atacantes.

El IFAI<sup>1</sup> (2017) en la consulta de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) define los datos sensibles como:

Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para este. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales [INAI] (s.f.) en la guía práctica para ejercer el derecho a la protección de datos personales define a los datos personales como:

Cualquier información que refiera a una persona física que pueda ser identificada a través de los mismos, los cuales se pueden expresar en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, como, por ejemplo: nombre, apellidos, CURP, estado civil, lugar y fecha de

---

<sup>1</sup>En adelante será señalado como INAI. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), es un organismo que antes era conocido como Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), cambió de nombre en mayo de 2015 tras la aprobación de la Ley General de Transparencia y Acceso a la Información.

nacimiento, domicilio, número telefónico, correo electrónico, grado de estudios, sueldo, entre otros.

La protección tanto a los datos sensibles como personales se convierte en un reto para el derecho a la intimidad, que está cobrando gran importancia en la actualidad con el uso constante de las TIC que hacen cada vez más vulnerables a los individuos frente a las intromisiones a su vida privada.

El derecho a la intimidad se define como: “una facultad subjetiva reconocida a favor de la persona física, de no permitir la intromisión de extraños, en lo que respecta al ámbito de su reserva individual [...]” (Celis, 2006.p.74), y define dos tipos de amenaza contra la intimidad: la acción o intrusión en un espacio propio del individuo y, el conocimiento sobre los aspectos relacionados con la vida confidencial de una persona (Celis, 2006).

Relacionando el concepto anterior con las tecnologías de la información y la comunicación (TIC), podríamos decir que una computadora, un teléfono celular, un dispositivo de almacenamiento externo o una tableta, podría ser considerado como un espacio propio del individuo cuando contiene información privada. Por tanto, nadie debería tener la facultad de conocer esos datos sin su consentimiento, pero si un tercero intenta conocerla, esto se convertiría en una amenaza y una violación al derecho a la intimidad.

Los datos personales y la información privada de cada individuo, deberán ser protegidos de terceros que intenten darle un uso incorrecto. El artículo 06, apartado II de la Constitución Política de los Estados Unidos Mexicanos, establece que “la información privada y los datos personales será protegida en los términos y con las excepciones que fijen las Leyes” (IFAI, 2007, p.12).

Pese a la existencia de los derechos a la intimidad, es difícil cumplirlo por la omnipresencia de las TIC, por ello surge la importancia de instruir a los jóvenes en una educación que incluya medidas básicas de ciberseguridad.

### **2.3 Seguridad y privacidad de la información**

Frecuentemente los usuarios dejan sus datos personales y sensibles en la Internet la cual tiene el potencial de exponerlos y crear desafíos de privacidad a una escala mayor que nunca [...] (Internet Society, 2016). Nada garantiza que dicha información será privada, y estará fuera del alcance de terceros no autorizados. Los datos privados se han convertido en una mercancía rentable. Los individuos pueden ser víctimas de cualquier ataque cibernético como estafas, fraudes, robo de información, pedofilia, terrorismo, daños contra el honor o la imagen de una persona, robo de identidad o sencillamente con fines lucrativos. Una vez que los datos privados son dados de alta en Internet, son casi incontrolables, ya que los piratas informáticos pueden acceder a ellos. Un ejemplo de esto es la filtración de la red social más grande de Rusia conocida como VK.com (Vkontakte). La base de datos contenía información completa como: nombre y apellidos de los usuarios, correos electrónicos, ubicación, direcciones, números de teléfono, contraseñas en texto plano (Segu.info, 2016).

La seguridad de la información y la seguridad informática son conceptos que se vuelven confusos por la adopción de distinta tecnología con la que la información se puede acceder con un solo *click*, por ello es necesario aclararlos a continuación.

La seguridad de la información es definida como la protección de la información y sistemas de información de accesos, uso, divulgación, interrupción, modificación o destrucción no autorizada. En esencia, esto significa que queremos proteger nuestros datos y nuestros sistemas de aquellos que tratan de abusar de ella. En sentido general, significa proteger nuestros bienes. Esto significa principalmente protegerlos desde invasión de ataques a nuestras redes, desastres naturales, condiciones nocivas ambientales, apagones, robo o vandalismo u otros estados indeseables (Jason, 2011, p. 2).

Por otra parte, Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando, Saltos-Gómez (2017) afirman que la seguridad de la información incluye la protección de la información independientemente del medio en que se encuentre, mientras que la seguridad informática sólo atiende a la protección de las instalaciones informáticas y de la información en medios digitales.

Una vez explicado los conceptos, se aclara que en este estudio se usa el término de seguridad de la información, pero considerando únicamente la información digital. La rápida introducción de las TIC en la sociedad, exige que las personas dejen sus datos personales y sensibles en Internet. No obstante, los ciudadanos que pongan su información a disposición de los entes público o privado, tienen derecho a que esta permanezca fuera del alcance de terceros. Por tanto, estos son responsables de garantizar la seguridad y privacidad de la información de sus ciudadanos.

Es necesario promover leyes de privacidad de datos que sean fuertes e independientes de la tecnología, principios de privacidad por diseño y principios éticos en la recolección y tratamiento de los datos es un enfoque clave para proteger y fomentar la privacidad en línea. El Informe de la Internet Society del 2016, señala que la privacidad es el derecho de determinar cuándo, cómo y en qué medida los datos personales pueden ser compartidos con terceros (Internet Society, 2016).

Es posible que determinadas personas que se conectan a Internet y envían sus datos a través de formularios o redes sociales (fotografías o mensajes instantáneos) o de alguna otra forma, desconocen sobre el derecho a la protección de los datos personales, el cual permite a los individuos mantener mayor control sobre su información privada, y decidir quién los tendrá a su disposición y que ésta se trate de forma adecuada.

El sector gobierno debería generar leyes que garanticen la privacidad de la información ya sea en el mismo gobierno o en el sector privado, de manera que los datos de cualquier ciudadano estén disponibles únicamente para quienes deben utilizarlos. En un sentido optimista, debe haber estricto acuerdo entre empresas y gobierno para generar políticas y medidas de seguridad exigentes que mantengan a salvo los datos de los ciudadanos.

En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), señala según el Artículo 12, que:

El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. En caso de que el responsable pretenda tratar los datos para un fin que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular (Diario Oficial de la Federación, 2010).

Lo anterior manifiesta que se busca que la información este segura y se mantenga su privacidad. A pesar de ésta ley, esto ha sido poco relevante, tanto en el sector público como en el privado, ya que en muchas ocasiones esto se pasa por alto; revelando los datos de los ciudadanos a terceros. Tal es el caso del Instituto Nacional Electoral en México (INE), en el que se violó el derecho a la privacidad de la información de 87.4 millones de ciudadanos, ya que el padrón electoral correspondiente al 2015 (lista Nominal de Electores) se infiltró y fue puesto a disposición de cualquier tercero a través del servicio en la nube de Amazon, con sede en Estados Unidos (Chávez, 2016).

En el artículo 19 de la LFPDPPP establece “todo responsable que lleve a acabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado” (Poder Ejecutivo Secretaría de Gobernación, 2017, “Capítulo II”).

Aunque no existe una ley universal de privacidad o protección de datos que se aplique en toda la Internet (Internet Society, 2016), a nivel nacional si existe cierto marco de privacidad. Por ejemplo, en México, existen los derechos conocidos como ARCO que se encuentran en la guía práctica para la atención de las solicitudes de ejercicio de los derechos ARCO, que son los siguientes (INAI, 2013).

- Acceso: todo individuo tiene derecho a acceder a su información que este en posesión de particulares y que pueda verificar si se está usando correctamente.
- Rectificación: los titulares de los datos personales tienen el derecho de corregir su información en caso de que este incompleta o inexacta.
- Cancelación: los individuos tienen el derecho a borrar sus datos en caso de que no se estén usando debidamente.
- Oposición: el individuo tiene el derecho a oponerse al uso de su información personal o exigir la eliminación del mismo con el objetivo de evitar daños a su persona o simplemente porque no desea que sea usado por empresas, negocios, asociaciones o cualquier tercero.

Actualmente en México existen instituciones y normativas que se encargan de asegurar la protección de la información personal, como se muestra en la Tabla 1.

**Tabla 1:** Instituciones y normatividad que protegen la información personal en México.

| INSTITUCIÓN  | FUNCIÓN   | NORMATIVIDAD   |
|--|---|--|
| Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) | <ul style="list-style-type: none"><li>• Garantizar el derecho de acceso a la información pública gubernamental.</li><li>• Proteger los datos personales que estén en manos del gobierno federal.</li><li>• Resolver sobre las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado.</li></ul> | Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).<br><br>Reglamento para la Ley federal de Protección de Datos Personales en Posesión de Particulares (RLFPDPPP). |

**Fuente:** Poder Ejecutivo Secretaría de Gobernación (2010) y [www.mexicoabierto.org](http://www.mexicoabierto.org)

En México, el INAI es un organismo público que tiene la misión de proteger los datos personales de los ciudadanos. En caso de que ocurra una vulnerabilidad a la seguridad dichos datos, el INAI podrá tomar en cuenta el cumplimiento de sus consideraciones, en base al artículo 58 del reglamento de la LFPDPPP (Secretaría de Gobernación, 2013). La LFPDPPP es la legislación que permite proteger la información personal que pueda contenerse en las bases de datos de cualquier persona física o empresa. El INAI, pone a disposición de los ciudadanos una guía práctica para que conozcan los derechos que tienen los ciudadanos en relación a sus datos personales y cómo ejercerlos (INAI, s.f.: 3).

### 3. Metodología

En las comunidades rurales dónde el uso de las TIC como: teléfono celular, computadoras e Internet es limitado, los conocimientos sobre la seguridad de la información y el derecho sobre la protección de los datos personales es casi desconocida. Es posible que las personas que aún no tienen una cultura de la seguridad de la información, tiendan a estar más expuestas a que sus datos sean utilizados con distintos fines.

Tanto la protección legal de datos personales como el uso de mecanismos apropiados de seguridad son los modos que permiten proteger la privacidad de los usuarios y disminuir riesgos. Si bien los avances tecnológicos pueden requerir el manejo de nuestra información personal para el funcionamiento de un servicio, el estándar mínimo que se debe exigir es que tales datos sean debidamente resguardados, que es lo que espera una persona cuando confía información de este tipo a un órgano estatal (Hernández, Fernández yBaptista,2016) como municipal. De aquí la importancia de que los ciudadanos tengan una cultura sobre la seguridad y la privacidad de su información para minimizar los riesgos que ello conlleva.

El Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO) es un organismo público descentralizado que desde sus orígenes como Telebachillerato de Oaxaca imparte educación de nivel medio superior en comunidades de alta y muy alta marginación en la entidad, con resultados académicos destacados. En el IEBO existen más de 24 mil 100 estudiantes, distribuidos en 261 planteles, y se busca que reciban una educación de calidad, como derecho inalienable de cada ser humano. Los planteles se encuentran en diferentes regiones del Estado: Costa, Cañada, Istmo, Mixteca, Papaloapan, Sierra Norte, Sierra Sur y Valles Centrales (IEBO, 2016).

El caso del plantel 165 donde se realizó el estudio, está ubicado en la Región Sierra Sur, en la localidad Río Anona perteneciente al Municipio de San Simón Almolongas, del Distrito de Miahuatlán de Porfirio Díaz. En cuanto a su infraestructura, tiene cinco aulas construidas, una de ellas es la sala de cómputo o conocida como aula de medios con acceso a Internet, una dirección, una cafetería, sanitarios, una cancha de básquet bol. Por lo que respecta a las TIC, tiene computadoras, proyectores, copiadora e impresoras<sup>2</sup>. Debido a los costos elevados de la renta mensual de Internet, solo escasas computadoras tienen acceso a este. Por último, hay un total de 126 alumnos inscritos de diferentes comunidades incluyendo Simón Almolongas, Guixé, Santa María Velato, San José Llano Grande, el Zompantle, San Guillermo, San Nicolás, entre otras. Además, hay cinco profesores, uno de ellos tiene el cargo de Director (ver figuras 1,2 y 3).

**Figura 1:** Plantel 165 Río Anona.



Fuente: Archivo personal.

**Figura 2:** Estudiantes del Plantel



Fuente: Archivo personal.

**Figura 3:** Aula de medios del Plantel 165.



Fuente: Archivo personal.

### 3.1 Elaboración del instrumento de recolección de datos

Con el objetivo de conocer qué información tienen los estudiantes de este plantel sobre de la seguridad de la información, datos personales y de las leyes que existen respecto a la protección de datos personales, se diseñó una encuesta de preguntas cerradas con respuestas de “sí” y “no” con la ayuda de la herramienta de formularios de google para obtener resultados rápidos y fáciles, y se aplicó en el aula de medios.

<sup>2</sup>Por cuestiones de privacidad de la información, se omite el número de computadoras, proyectores, copiadoras e impresoras.

Se creó un total de 14 preguntas que miden las variables de estudio: protección de datos personales, seguridad de la información digital y legislación de datos personales. Se tiene 1 pregunta para conocer si los estudiantes consideran importante que dentro de su plan de estudios exista una materia donde se les enseñe como navegar de manera segura en Internet. También se agregó un apartado donde los encuestados escribieran ejemplos de contraseñas.

Las preguntas se eligieron para identificar si el alumno conoce: qué es la seguridad y privacidad de la información, controla su información que sube en internet, conoce los riesgos de su información en internet, conoce el derecho a la protección de sus datos personales y las leyes e instituciones que pueden protegerlos.

### **3.2 Determinación y tamaño de la muestra**

Para aplicar la encuesta, se tomó una muestra no probabilística por conveniencia. Este tipo de muestra se da “por los casos disponibles a los cuales tenemos acceso” (Hernández, Fernández y Baptista, 2014, p. 390) por lo que se aplicó a un total de 112 estudiantes presentes en el momento, el cual representa al 100% de encuestados.

### **3.3 Operacionalización de las variables**

Para la variable protección datos personales, se definió primero datos personales como toda aquella información que permita identificar a una persona física, por ejemplo: su domicilio, correo electrónico, nombre, edad. La protección de datos personales se definió como el control de la propia información frente al tratamiento automatizado o no. Para medir la protección de datos personales se pidió al encuestador indicar con respuestas de “sí” y “no” a preguntas sobre: es importante controlar la información que sube a internet, sabes que tu información privada está en internet, configuras tus redes sociales para tener mayor privacidad, conoces los riesgos de tu información personal en Internet.

Seguridad de la información se definió como la protección de la información digital de accesos, uso, divulgación, interrupción, modificación o destrucción no autorizada. En otras palabras, significa proteger nuestros datos de terceros no autorizados. Para su medición se preguntó con respuestas de “sí” y “no”, para conocer si el encuestado tenía o no conocimiento sobre: a qué se refiere la seguridad de la información, diferencia entre seguridad y privacidad de la información, medidas básicas de seguridad de la información, cómo se genera una contraseña segura.

Legislación de datos personales, se definió como el marco jurídico y regulatorio en materia de datos personales. Se midió con respuesta de “sí” y “no”, para identificar si tenían o no conocimiento sobre: derecho a la protección de los datos personales, leyes de protección de datos personales, derechos ARCO, derecho a la intimidad de datos personales, instituciones que protegen los datos personales.

## **4. Resultados**

Es importante mencionar que para la aplicación de las encuestas se hizo en más de un día, ya que solo algunas de las computadoras con las que cuenta la institución

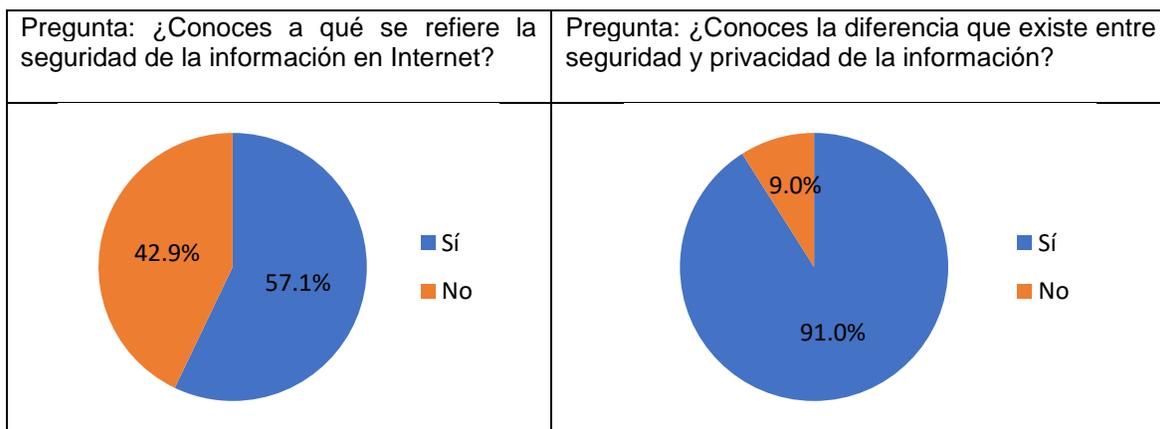
tienen acceso a Internet, por lo que los alumnos solo podían ocupar unas cuantas para tener acceso al formulario de google donde se encontraba la encuesta en línea. Algunos alumnos tuvieron problemas al momento de guardar sus respuestas por la lentitud de la red, y se vieron en la necesidad de volver a realizar su formulario. La Internet en ocasiones es inestable debido a problemas de red.

Una vez aplicada la encuesta, se clasificó la información por preguntas para su mayor facilidad de análisis. Las respuestas a cada pregunta se graficaron de forma circular y se presentan por temas clasificados en seguida:

#### 4.1 Seguridad de la información en Internet

El 57.1% de los jóvenes señalan que sí saben a qué se refiere la seguridad de la información en Internet, pero el 42.9% no lo sabe. Es decir, existe al menos la mitad de estos jóvenes que podrían ser vulnerables a que su información sea utilizada por terceros con fines ilícitos por la falta de conocimientos. Aun cuando la mitad de los encuestados saben a qué se refiere la seguridad de la información en Internet, el 91% no sabe la diferencia entre privacidad y seguridad de la información en Internet, y el 9% si lo conoce (ver figura 4). De aquí la importancia de fomentar una cultura se la seguridad de la información.

**Figura 4:** conocimientos sobre la seguridad de la información en internet de estudiantes de nivel medio superior.



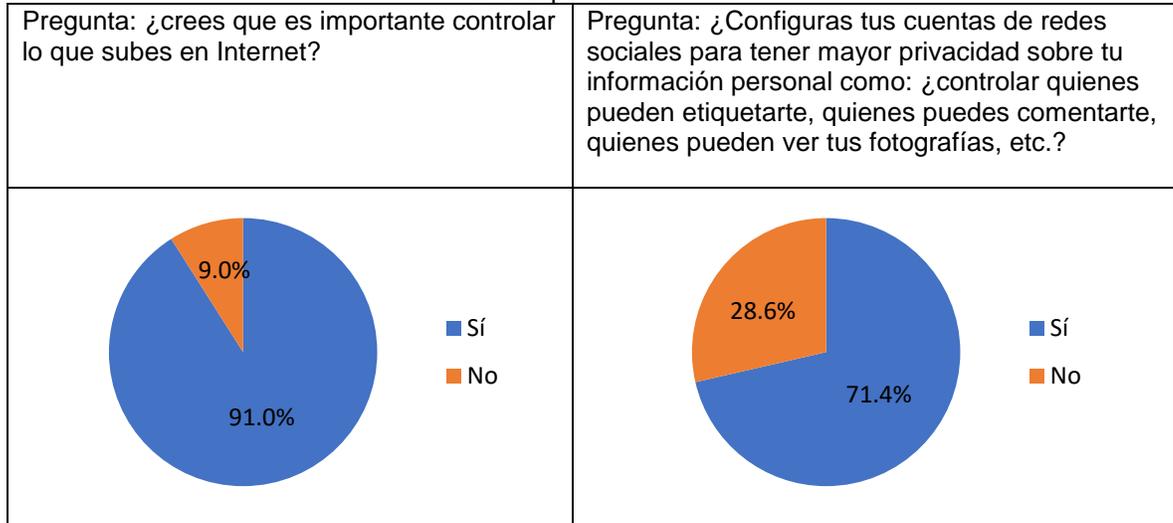
**Fuente:** Elaboración propia con base en Googleform.

En cuanto a la información que suben a Internet, un 91% considera que es importante controlarla y solo el 9% no lo considera importante. Por otra parte, el 71.4% configura sus cuentas sociales con parámetros de privacidad, lo que les permite hasta cierto punto mantener privada su información de terceros no autorizados, de modo que ellos deciden quién puede ver sus fotos, videos o publicaciones, mientras que el 28.6% no lo hace, lo que significa que es necesario darle a conocer a esta población la importancia de la seguridad y privacidad de su información (ver figura 5).

Respecto a los riesgos que corre su información personal en Internet, más de la mitad de los jóvenes sí lo sabe: el 86.6%, pero el 13.4% no. No obstante, más de la mitad, es decir, el 56.3% no conoce las medidas básicas de seguridad de la información y solo el 43.8% sí las sabe. De forma similar, un poco más de la mitad de los

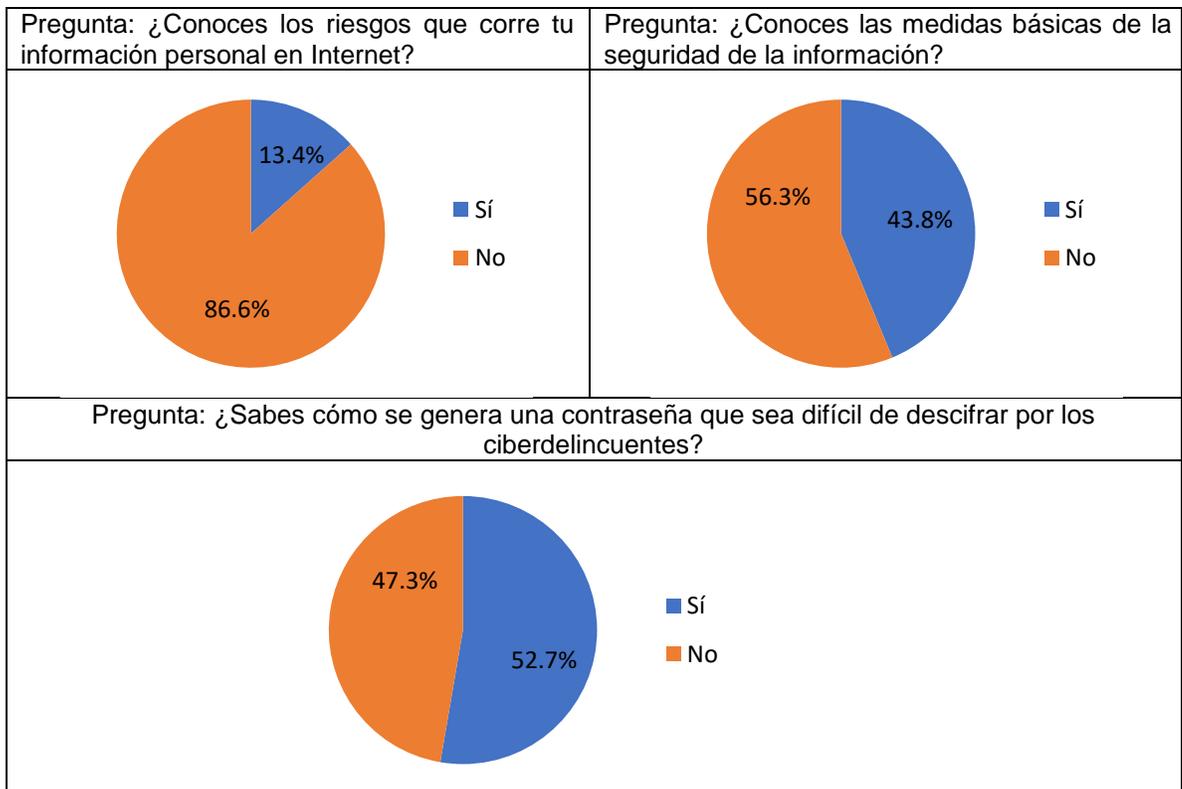
encuestados sabe cómo generar una contraseña hasta cierto punto segura, el 52.7%, y el 47.3% no lo sabe (ver figura 6). De acuerdo con los resultados arrojados en las gráficas, es recomendable que los jóvenes conozcan las medidas básicas de la seguridad informática, para generarles mayor protección cuando naveguen por Internet.

**Figura 5:** conocimientos sobre la seguridad de la información en internet de estudiantes de nivel medio superior.



**Fuente:** Elaboración propia con base en Googleform.

**Figura 6:** conocimientos sobre la seguridad de la información en internet de estudiantes de nivel medio superior.

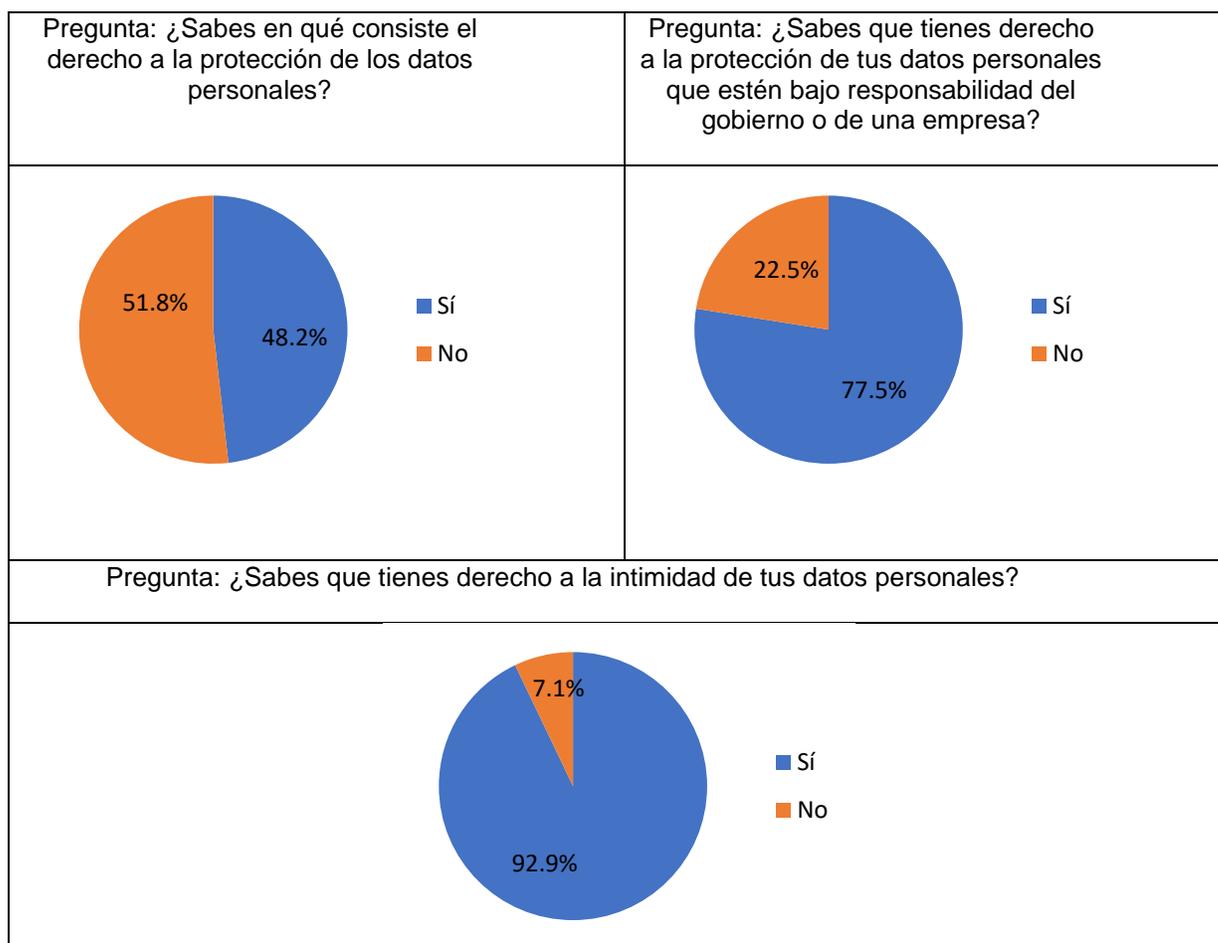


**Fuente:** Elaboración propia con base en Googleform.

## 4.2 Información y protección de datos personales en Internet.

En esta sección se evidencia que el 51.8% de los encuestados no sabe en qué consiste el derecho a la protección de datos personales, y menos de la mitad, el 48.2% sí lo sabe. Es claro que desconocen que tienen este derecho, pero el 77.5% reconoce que debe tener derecho a la protección de datos personales que estén en posesión del gobierno o de empresas privadas, y solo el 22% no lo sabe. De la misma forma, más de la mitad, el 92.9% sabe que tiene derecho a la intimidad de sus datos personales, y el 7.1% no (ver figura 7).

**Figura 7:** conocimientos sobre protección de datos personales de estudiantes de nivel medio superior.



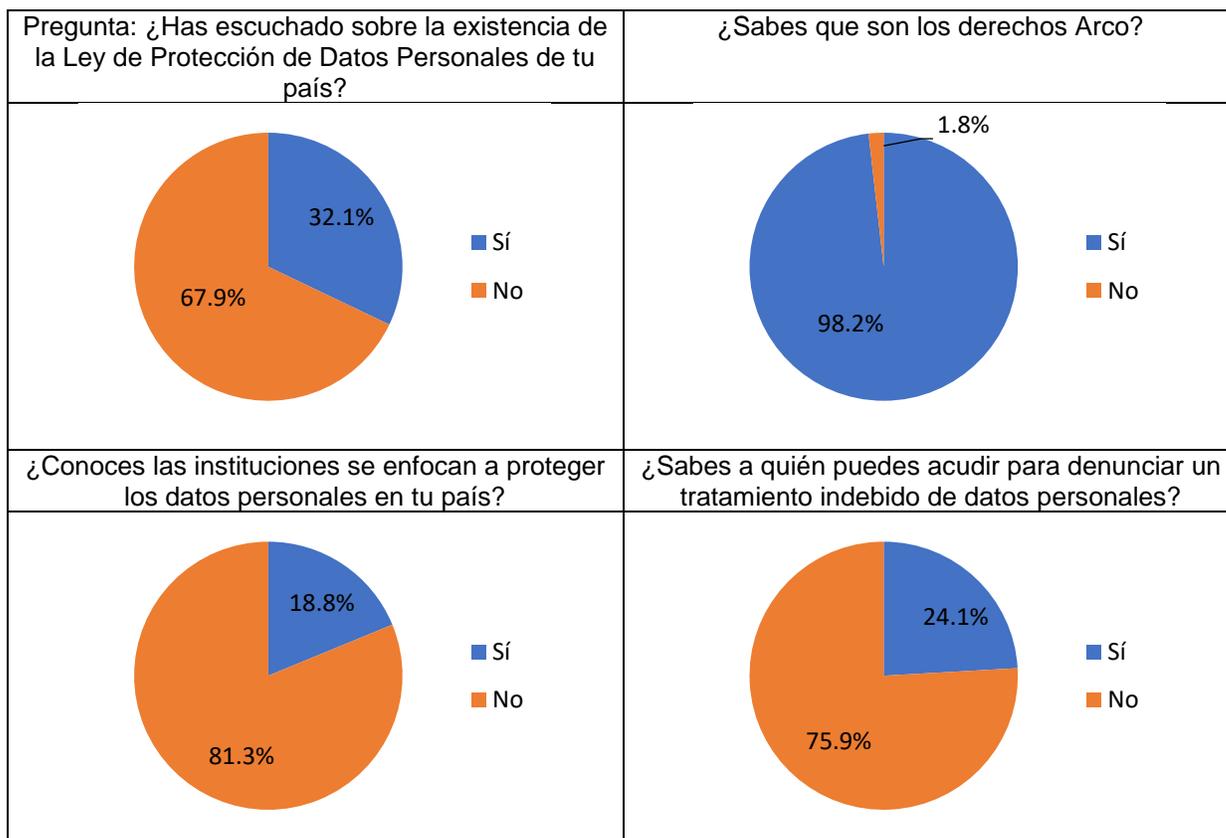
Fuente: Elaboración propia con base en Googleform.

## 4.3 Legislación de protección de datos personales.

Más de la mitad de los estudiantes encuestados no saben que en México existe una Ley que protege sus datos personales; el 67.9%, y sólo el 32% sí lo sabe. Aunado a esto, el 98.2% de los alumnos del plantel 165 no sabe qué son los derechos ARCO, es decir, es claro que saben que su información debe ser privada, pero desconocen sus derechos al acceso, rectificación, cancelación y oposición de sus datos

personales. Asimismo, el 81.3% desconoce las instituciones que se enfocan a proteger sus datos personales, y solo el 18.8% sí lo sabe. Por otra parte, el 75.9% no tiene el conocimiento sobre a quién acudir para denunciar un tratamiento indebido de datos personales, y solo el 24.1% lo sabe (ver figura 8). Así que, estos datos demuestran la importancia de conocer los derechos ARCO para ejercerlos ya que se trata de la protección de los datos personales.

**Figura 8:** conocimientos sobre legislación de datos personales de estudiantes de nivel medio superior.

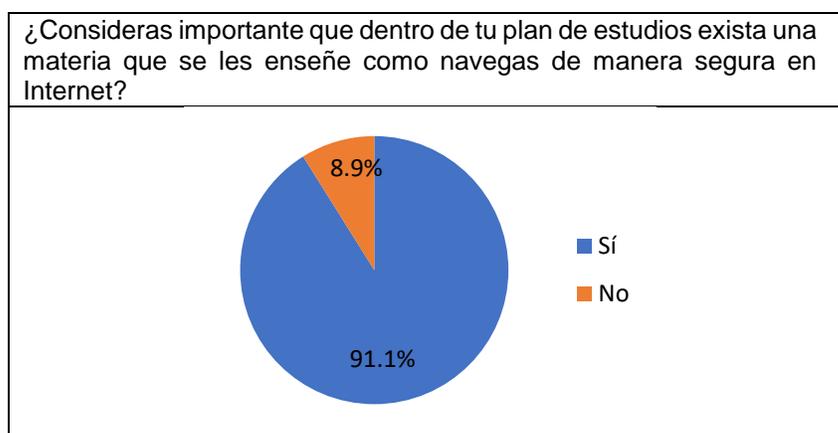


Fuente: Elaboración propia con base en Googleform.

#### 4.4 Asignatura orientada a la seguridad de la información

Respecto a la necesidad de que el plan de estudio del IEBO cuente con una materia orientada a la seguridad de la información, el 91.1 % contesto que sí lo considera importante que exista una asignatura en esta área en donde se le enseñe las medidas básicas de la seguridad de la información. Solo el 8.9 % señalaro que no. Ver Figura 9.

**Figura 9:** asignatura sobre la seguridad de la información en estudiantes de nivel medio



Fuente: Elaboración propia con base en Googleform.

#### **4.4 El Plan de estudios del Instituto de Bachilleratos del Estado de Oaxaca y la ausencia de asignaturas enfocadas a la seguridad informática.**

Es claro que Internet brinda numerosas oportunidades y beneficios para los niños y niñas, y los jóvenes, dada la influencia que ejerce sobre su nivel educativo y su inclusión social. Sin embargo, también existen peligros que trascienden los límites de edad, la localización geográfica y las fronteras más claramente delineadas del mundo real, por lo que este sector de la sociedad corre el riesgo de encontrar en Internet aspectos que vulneran su derecho a la seguridad y privacidad de la información (Fondo de las Naciones Unidas para la Infancia [UNICEF], 2012).

El objetivo de los responsables de trazar políticas destinadas a incrementar las oportunidades de los niños, niñas y jóvenes, también son responsables del desarrollo de un acceso más seguro a Internet. Cabe señalar, que no solo el gobierno tiene la responsabilidad, sino también el sector privado en Internet, ya que según la concepción actual de la responsabilidad corporativa sobre el respeto a los derechos humanos, establecida a nivel internacional en el informe titulado “Principios rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para ‘proteger, respetar y remediar’”, las empresas están obligadas a respetar los derechos humanos y a tratar de prevenir o mitigar las consecuencias negativas sobre estos directamente relacionadas con sus actividades, productos y servicios (UNICEF, 2012).

Desde nuestro punto de vista, se considera que la educación es el factor clave para iniciar con una cultura de la protección de la información, ya que la falta de seguridad digital implica que estemos expuestos a ataques de ciberdelincuentes y espionaje.

Como parte de un derecho humano a la privacidad de la información, se propone que los funcionarios públicos al frente de la educación de México incorporen a los programas de estudio en los niveles de educación primaria, secundaria y bachillerato una asignatura enfocada a la “seguridad de la información” debido a la incorporación y necesidad de las TIC en la sociedad; que permita que los estudiantes conozcan los riesgos que conlleva el no hacer un buen uso de la información personal en Internet y

como protegerse frente a los criminales en la red. Además de cómo ejercer sus derechos sobre la protección de la información personal.

Con base en los resultados obtenidos de la encuesta, es necesario mencionar que existen estudiantes sobre todo en las zonas rurales que desconocen qué es la seguridad de la información, cómo proteger sus datos personales y a que instituciones acudir en caso de ser necesario para garantizar sus derechos a la privacidad y seguridad de su información. De aquí la importancia de un plan de estudios en los bachilleratos rurales que contemple una asignatura acerca de la seguridad informática para contribuir a que los jóvenes tengan noción acerca de cómo protegerse en Internet, en cuanto a la seguridad y privacidad de su información. De la misma manera, que tengan información acerca de la protección de datos personales.

En este documento debido a que el estudio se enfoca a zonas rurales, y se toma como caso de estudio el bachillerato: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO) del plantel 165 “Río Anona”, en la Tabla 2 se presenta su plan de estudios al ciclo escolar 2017-B.

**Tabla 2:** Plan de estudios del IEBO al ciclo escolar 2017-B.

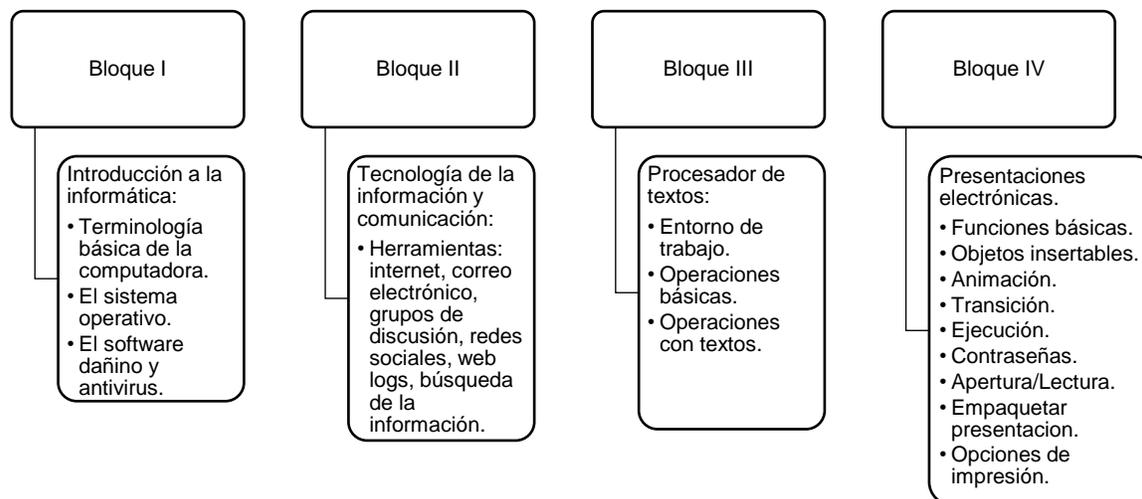
| <b>Primer Semestre</b>  | <b>Segundo Semestre</b>   |
|---|---|
| Matemáticas I<br>Química I<br>Ética y Valores I<br>Introducción a las Ciencias Sociales<br>Taller de Lectura y Redacción I<br>Lengua Adicional al Español I (Inglés)<br>Informática I<br>Orientación Escolar<br>Actividades Paraescolares   | Matemáticas II<br>Química II<br>Ética y Valores II<br>Historia de México I<br>Taller de Lectura y Redacción II<br>Lengua Adicional al Español II (Inglés)<br>Informática II<br>Orientación Escolar<br>Actividades Paraescolares   |
| <b>Tercer Semestre</b>  | <b>Cuarto Semestre</b>  |
| Matemáticas III<br>Física I<br>Biología I<br>Historia de México II<br>Literatura I<br>Lengua Adicional al Español III (Inglés)<br>Orientación Vocacional<br>Actividades Paraescolares<br>Módulo I:<br>Administración Municipal<br>» Elementos de la Administración Municipal<br>» Fundamentos de Diseño Gráfico | Matemáticas IV<br>Física II<br>Biología II<br>Estructura Socioeconómica de México<br>Literatura II<br>Lengua Adicional al Español IV (Inglés)<br>Orientación Vocacional<br>Actividades Paraescolares<br>Módulo II:<br>Planeación del Desarrollo<br>» Métodos y Herramientas de Planeación<br>» Diseño Interactivo |

| Quinto Semestre   | Sexto Semestre   |
|---|--|
| Geografía<br>Historia Universal Contemporánea<br>Orientación Profesiográfica<br>Actividades Paraescolares<br>Cálculo Diferencial<br>Temas Selectos de Ciencias de la Salud I<br>Administración I<br><br>Ciencias de la Comunicación I<br>Módulo III:<br>Proyectos de Desarrollo local<br>» Elaboración de Proyectos Sociales<br>» Gestión de Bases de Datos | Ecología y Medio Ambiente<br>Filosofía<br>Metodología de la Investigación<br>Actividades Paraescolares<br>Orientación Profesiográfica<br>Cálculo Integra<br><br>Temas Selectos de Ciencias de la Salud II<br>Administración II<br>Ciencias de la Comunicación II<br>Módulo IV:<br>Proyectos de Inversión<br><br>» Elaboración de Proyectos Productivos<br>» Diseño Web |

Fuente: [http://www.iebo.edu.mx/index.php?option=com\\_content&view=article&id=352&Itemid=472](http://www.iebo.edu.mx/index.php?option=com_content&view=article&id=352&Itemid=472)

En la Tabla 2, se puede observar que en ningún semestre se le imparte al alumno alguna asignatura denominada seguridad de la información. También se puede ver que Informática I es la única asignatura que contiene un sólo tema ligado (ver figura 9).

**Figura 10:** contenido disciplinar la asignatura Informática del IEBOI.



Fuente: Elaboración propia con base en IEBO (2013).

En la figura 10 se puede observar que en el bloque I del programa de estudios de Informática I de agosto del 2013, hay un tema relacionado con la seguridad de la información: el software dañino y antivirus, y el bloque II, está vinculado a que los estudiantes aprendan los conceptos sobre las herramientas de Internet, a pesar que no se focaliza directamente con el tema de la seguridad de la información, se puede tomar ventaja de los temas vistos para abordar cuestiones relacionadas, sin embargo, por falta de tiempo y el cumplimiento que se debe dar a los contenidos definidos, se

vuelve complicado tratar de forma amplia sobre lo que respeta a la ciberseguridad, por ello se considera relevante agregar una asignatura que considere directamente las temáticas. El programa de estudios de informática I se ha utilizado hasta el ciclo escolar 2017-B.

Por su parte Informática II, trata sobre el uso de las hojas de cálculo (Excel), publisher y algoritmos. El resto de las materias del área de informática se vinculan con diseño gráfico (CorelDraw 12), diseño interactivo (Flash 8), gestión de base de datos (MySQL) y diseño web (Dreamweaver 8, PHP, servidor WAMP).

Por tanto, al conocer reducidamente acerca de estos temas al igual que en otros niveles educativos, se vuelven blancos vulnerables para los atacantes o para aquellos que se dedican a realizar actos ilícitos en Internet. De aquí, la importancia de que desde el nivel primaria conozcan cómo hacer frente a estos nuevos cambios en la era de la tecnología. Ya que, además, con ello, se ayudaría también a brindarles información que los oriente a no revelar su información personal en páginas de Internet y redes sociales tales como: Facebook, WhatsApp, YouTube, Instagram, Twitter, Snapchat, que puedan ser usados por terceros. “Proporcionar un entorno seguro exige una comprensión profunda de los tipos y la prevalencia de los riesgos online que los jóvenes cibernautas enfrentan, así como de las soluciones más eficaces para mitigar esos riesgos” (Farrukh, Sadwick y Villasenor, 2014).

## **5. Conclusiones**

La seguridad informática en el área digital y la protección de la información privada, son temas que actualmente están cobrando mayor importancia, y diferentes sectores, tanta sociedad civil, academia, sector público y privado, se están interesando por buscar nuevas formas para hacer frente a este nuevo reto que involucra a todos, puesto que la mayoría de las personas tiene acceso a Internet, y por tanto, cualquier acceso a la red deja rastros de la información personal. Ahora bien, es común que los usuarios jóvenes se muestren más interesados por usar la tecnología. Para el caso de Oaxaca, algunas de sus comunidades aún no cuentan totalmente con internet, y de la experiencia vivida se sabe que en ocasiones los jóvenes sólo tienen acceso cuando asisten a la escuela o en los cibercafé pero de forma restringida porque por ejemplo, en el plantel 165 no existe señal de Wifi para los dispositivos móviles, aunque existen algunas zonas de la escuela donde hay cobertura de la red datos Telcel. Es en estas zonas donde los celulares pueden tener señal y los alumnos pueden ocupar datos para usar internet.

En cuanto a los conocimientos que estos jóvenes puedan tener acerca de los peligros que corre su información en Internet, la seguridad de su información y protección de datos personales, existen algunos que carecen de ello. Para el caso de estudio se obtuvo que del total de jóvenes encuestados (112 alumnos) sólo el 57.1% conoce a qué se refiere la seguridad de la información en Internet. Cabe mencionar que es necesario hacer saber a los jóvenes la importancia de controlar la información que suben en Internet, ya que, aunque es una mínima cantidad, se obtuvo que el nueve por ciento no lo considera así. Relacionado a esto, el 28.6 por ciento no configura sus redes sociales para tener mayor privacidad de su información.

En los resultados se obtuvo que el 13.4 por ciento de los jóvenes del IEBO desconocen los riesgos que corre su información personal en internet, lo que los vuelve blancos fáciles para los delincuentes. Otro punto preocupante es que el 56.3 por ciento desconoce las medidas básicas de la seguridad de la información.

Ahora bien, en cuanto a la legislación de datos personales, se obtuvo que más de la mitad, el 67.9 por ciento desconoce la Ley de Protección de Datos Personales que existe en México, y el 98.2% desconoce que son los derechos ARCO. El 81.3 por ciento no conoce a las instituciones que protegen sus datos personales, y derivado de esto el 75.9 por ciento no sabe a quién acudir en caso de que terceros hagan mal uso de sus datos personales.

Finalmente se puede observar que existen jóvenes que desconocen cómo protegerse de los peligros de Internet, las leyes que velan por la privacidad de la información, sus derechos personales, por lo que se ven expuestos a distintos problemas relacionados al Internet, ya sea que se vuelvan vulnerables para los atacantes, usurpación de identidad, secuestros, fraudes, entre otros, de aquí la necesidad de que en los planes de estudios exista una asignatura que abarque ampliamente el tema acerca de los peligros que se pueden encontrar en Internet, cómo proteger sus datos e información personal, así como sus derechos ARCO en México.

Asimismo, es claro decir que una de las desventajas que se presentaría en los alumnos y profesor al momento de llevar a cabo las prácticas de la seguridad de la información en teléfonos celulares, computadoras u otras TIC, es el restringido acceso a Internet, pero los conocimientos aprendidos podrían aplicarse en otros contextos donde el estudiante tenga mayor acceso a dicha red.

## Referencias

- Ayala, T.C. (noviembre, 2015). Redes sociales e hiperconectividad en futuros profesores de la generación digital. *Ciencia, Docencia y Tecnología*, 26 (51), 224-270. Recuperado de: [www.pcient.uner.edu.ar/index.php/cdyt/article/download/58/153](http://www.pcient.uner.edu.ar/index.php/cdyt/article/download/58/153)
- Celis, M. A. (2006). La protección de la intimidad como derecho fundamental de los mexicanos. En Universidad Nacional Autónoma de México (Ed.), *Estudios en homenaje a Marcia Muñoz de Alba Medrano*, México (pp. 71-108). España. Recuperado de: <https://archivos.juridicas.unam.mx/www/bjv/libros/5/2253/9.pdf>
- Chávez, V. (22 de abril de 2016). Filtran lista nominal de electores en Amazon; INE interpone denuncia.El Financiero. Recuperado de: <http://www.elfinanciero.com.mx/nacional/lista-nominal-de-electores-disponible-en-amazon-ine-interpone-denuncia.html>
- Farrukh, A., Sadwick, R. y Villasenor, J. (octubre, 2014). Seguridad de los jóvenes en Internet: Riesgos, Respuestas y Recomendaciones para la Investigación. Center for Technology Innovation at Brookings. Recuperado

de:<http://www.brookings.edu/~media/research/files/papers/2014/10/21-youth-internet-safety-farrukh-sadwick-villasenor/brookingsyouthinternetsafetyspanish.pdf>

Figueroa-Suárez, J.A., Rodríguez-Andrade, R.F., Bone-Obando, C.C. y Saltos-Gómez, J.A. (diciembre, 2017). Seguridad informática y seguridad de la información. Polo del conocimiento, 2 (12), pp.145-155. Recuperado de: <https://polodelconocimiento.com/ojs/index.php/es/article/download/420/pdf>

Fondo de las Naciones Unidas para la Infancia (UNICEF). (2012). La seguridad de los niños en línea: Retos y estrategias mundiales. Recuperado de:<http://www.unicef.org/panama/spanish/Seguridad-en-Internet-Informe-Inocenti.pdf>

Hernández, R., Fernández, C. y Baptista, M. (2014). Selección de la muestra. En Autor (Eds.), Metodología de la investigación (pp. 170-195). México, D.F.: Mc Graw Gill/ Interamericana Editores.

Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO). (2013). 1er. Semestre comunicación: un enfoque basado en competencias. Manuscrito disponible en archivo electrónico, IEBO, Oaxaca, Oax.

Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO). (2016). Planteles del IEBO. Oaxaca: Autor. Recuperado de: [http://www.iebo.edu.mx/interno/?option=com\\_planteles](http://www.iebo.edu.mx/interno/?option=com_planteles)

Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO). (2017). Nosotros. Oaxaca: Autor. Recuperado de: <http://www.iebo.edu.mx/>

Instituto Federal de Acceso a la Información Pública (IFAI). (2007). Reforma al artículo 6° constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos. Recuperado de: <http://inicio.ifai.org.mx/Publicaciones/ModificacionArt6.pdf>

Instituto Nacional de Estadística y Geografía. (INEGI). (2010a). Censo de Población y vivienda 2010. Conjunto de datos de población de 12 años y más. Recuperado de: [http://www.inegi.org.mx/sistemas/olap/Proyectos/bd/censos/cpv2010/P12Mas.asp?s=est&c=27823&proy=cpv10\\_p12mas](http://www.inegi.org.mx/sistemas/olap/Proyectos/bd/censos/cpv2010/P12Mas.asp?s=est&c=27823&proy=cpv10_p12mas)

Instituto Nacional de Estadística y Geografía. (INEGI). (2010b). Censo de Población y vivienda 2010. Recuperado de: <http://www3.inegi.org.mx/sistemas/SCITEL/default?ev=5>

Instituto Nacional de Estadística y Geografía. (INEGI). (2017). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), 2017. Recuperado de:<http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2017/>

- Instituto Nacional de Transparencia y Acceso a la Información y Protección de Datos Personales (INAI). (s.f.). Guía práctica para ejercer el derecho a la protección de datos personales. Recuperado de:  
<http://www.periodistasdeapie.org.mx/documentos/01GuiaPracticaEjercerelDer echo.pdf>
- Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales (INAI). (2013). Guía práctica para la atención de las solicitudes de Ejercicio de los derechos ARCO. Recuperado de:  
<http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf>
- Instituto Nacional para el Federalismo y el Desarrollo Municipal (INAFED). (2010). SNIM Sistema Nacional de Información Municipal. México, D.F. Recuperado de:  
<http://www.snim.rami.gob.mx/>
- Internet Society.(2016). Informe de la Internet Society, Introducción a la privacidad en Internet. Recuperado de:  
<http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-Privacy-20151030-es.pdf>
- Jason, A. (2011). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. USA: Elsevier Inc. Recuperado de:  
[http://index-of.es/Hack/The.Basics.of.Information.Security\\_Understanding.the.Fundamentals.pdf](http://index-of.es/Hack/The.Basics.of.Information.Security_Understanding.the.Fundamentals.pdf)
- Lages, V. (2008). La inserción de las Pymes en cadena de valor global. En Sistema Económico Latinoamericano y del Caribe [SELA]. (Ed.), Pymes: Una visión estratégica para el desarrollo económico y social(185-194). Venezuela: Horizonte. Recuperado de:  
<http://www.sela.org/media/2464236/pymes-una-vision-estrategica-para-el-desarrollo.pdf>
- Observatorio de la ciberseguridad en América Latina y el Caribe. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Recuperado de:  
<http://gobernanza.udg.mx/sites/default/files/Ciberseguridad.pdf>
- Poder Ejecutivo Secretaría de Gobernación. (2010). Diario Oficial. Recuperado de:  
<http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/LFPDPPP.pdf>
- Programa Sociedad de la Información y el Conocimiento (PROSIC). (2010). Ciberseguridad en Costa Rica. Costa Rica: Universidad de Costa Rica. Recuperado de:  
<http://www.kerwa.ucr.ac.cr/bitstream/handle/10669/500/libro%20completo%20Ciber.pdf?sequence=1&isAllowed=y>
- Secretaría de Gobernación. (2013). Recomendaciones de seguridad en materia de datos personales. México: Diario Oficial de la Federación. Recuperado

de:[http://www.dof.gob.mx/nota\\_detalle.php?codigo=5320179&fecha=30/10/2013](http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013)

Segu.info (06 de junio de 2016). 190 de cuentas comprometidas en Vk.com. Autor. Recuperado de <http://blog.segu-info.com.ar/2016/06/190-millones-de-cuentas-comprometidas.html>

Tecnología y Comunicación- TEDIC. (2016). Comentarios al Borrador del plan de ciberseguridad 2016. Recuperado de: [https://www.tedic.org/wp-content/uploads/sites/4/2016/06/observaciones-sobre-el-plan-de-ciberseguridad\\_v14jun-.pdf](https://www.tedic.org/wp-content/uploads/sites/4/2016/06/observaciones-sobre-el-plan-de-ciberseguridad_v14jun-.pdf)

Unión Internacional de Telecomunicaciones (ITU). (2018). Ciberseguridad. Autor. Recuperado de: <http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx>