



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE FILOSOFÍA Y LETRAS
COLEGIO DE PEDAGOGÍA

Importancia de la ciberseguridad en la escuela:
recomendaciones para alumnos de nivel secundaria.

TESINA

QUE PARA OBTENER EL TÍTULO DE

LICENCIADA EN PEDAGOGÍA

PRESENTA:

MAYRA JACQUELINE RATIA GALINDO

Asesora: MTRA. CLAUDIA ELENA LUGO VÁZQUEZ



Ciudad Universitaria, CDMX, 2022.



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

A mi mamá, por siempre estar, por sacarnos adelante y ser un ejemplo de valentía y fortaleza, porque sin tu insistencia no podría haber logrado esto. Este trabajo es para ti. Te amo.

A mi hermana, por ser mi cómplice en la vida, por apoyarme y escucharme, por volverme a poner en mi carril cuando pierdo el rumbo. 사랑해요 Baby.

A mi papá por haber sido el mejor, por enseñarme a ser una princesa con espada y porque a pesar de que ya no estás físicamente siempre estarás en mi corazón y en cada uno de mis logros. Te abrazo hasta cielo.

A Toño, porque siempre me motivas a ser mejor, porque en cada paso que doy me has acompañado, por celebrar cada logro junto a mí y sobre todo por no dejar de insistir con tener mi título. Te amo mimor.

A Mimi, por siempre apoyarme, cuidarme y motivarme a lograr mis metas, por ser parte de esta etapa y festejar conmigo cada capítulo finalizado.

A Saraí, por todas las locuras que la vida nos ha permitido compartir, por siempre estar presente y por ser un ejemplo de perseverancia. Te quiero queso.

A Anita Y Bere por hacer de la universidad una etapa genial, por ser un ejemplo y motivación para poder concluir este trabajo.

A Adri y Javi, por siempre apoyarnos, por ser parte del clan y por escucharme en mis momentos de crisis con la tesina. Los quiero.

A la Mtra. Claudia, por ser una excelente asesora, siempre compartir sus conocimientos y consejos para que este trabajo tomara forma.

A mis sinodales, la Lic. Esther Hirsch, la Mtra. Laura Márquez, la Lic. Roxana Velasco y el Dr. Roberto Villamil, por sus aportes en el trabajo que ayudaron a enriquecerlo.

A la UNAM, por albergarme en sus aulas y brindarme grandes experiencias.

Y en general a todos los que de alguna u otra manera fueron parte de mi vida y de este proceso.

Infinitas gracias a todos por poner su granito de arena en mi vida.

Índice:

Introducción.....	5
1. Los adolescentes y el nivel secundaria de escuelas privadas en México.....	9
1.1. La educación privada en México.....	10
1.1.1. La educación privada en tiempos de COVID en México.....	12
1.2. Los adolescentes de secundaria y su rango de edad.....	14
1.3. El desarrollo psico-social de los adolescentes de secundaria.....	16
1.4. La madurez cognitiva de los adolescentes en edad correspondiente a nivel secundaria.....	17
1.5. Uso de dispositivos tecnológicos en adolescentes de secundaria en México.....	19
2. Ciberseguridad y educación.....	22
2.1. ¿Qué es la ciberseguridad?	23
2.2. La ciberseguridad en México.....	26
2.3. Identificación de los diversos ataques cibernéticos.....	29
2.4. Ciudadanía digital.....	33
2.5. Importancia de la ciberseguridad y la ciudadanía digital en la educación	37
3. Recomendaciones para que los alumnos de secundaria eviten ser víctimas de ciberataques.....	39
3.1. Recomendaciones para la comunidad escolar.....	41
3.1.1. Recomendaciones para alumnos.....	48
3.1.2. Recomendaciones para docentes y personal administrativo.....	58
Conclusiones.....	66
Anexos.....	69
Gráfico 1.....	69
Gráfico 2.....	70
Gráfico 3.....	71
Fuentes consultadas.....	72

Introducción

El presente trabajo tiene la intención de exponer algunas recomendaciones sobre el reconocimiento y prevención de la ciberseguridad, así como de la ciudadanía digital dentro de la comunidad escolar, haciendo énfasis en porqué es importante hablar de estos temas dentro de la escuela y sobre todo con los adolescentes que cursan la secundaria en una escuela privada.

Debido a la reciente pandemia por la COVID-19, toda la educación tuvo que migrar a modalidad virtual, por lo que muchas escuelas privadas decidieron optar por dar las clases desde alguna herramienta de videoconferencia, así como implementar plataformas educativas que les ayudara a llevar un control de tareas, actividades de clase, contenidos digitales, etc., por lo que, al pasar al ambiente digital, surgieron diversas cuestiones relacionadas con la seguridad.

La ciberseguridad y educación deben ser temas de interés general actual para todos los pedagogos, sin embargo, en mi caso surgió debido a la labor que desempeño como Implementadora de Soluciones Educativas dentro de Sistema UNOi.

En este cargo tengo contacto directo con las escuelas privadas que han contratado dicho sistema, en el cual pueden ingresar a una plataforma educativa que les permite tener un censo de alumnos y profesores, consultar contenidos y materiales que abarcan los aprendizajes esperados por la SEP, así como generar actividades para el reforzamiento de los temas y tener un registro de asistencias, calificaciones y boletas.

De igual forma, les permite agendar sesiones virtuales desde alguna de las herramientas como Zoom, Microsoft Teams y Google Meets; por lo que, con la pandemia, muchas de las escuelas que contrataron la plataforma, empezaron a utilizarla de forma mucho más constante y migraron sus clases y actividades a esta herramienta digital.

Dentro de mis funciones como Implementadora de Soluciones Educativas, se encuentra la capacitación a los docentes que se encargan de la configuración de la plataforma, la cual les permite a todos los alumnos y profesores ingresar a los beneficios antes mencionados; además, realizo apoyo técnico a estos colegios, debido a esto, al inicio de la pandemia empezamos a recibir muchos reportes de escuelas que tenían incidencias con alumnos que habían copiado tareas, perdido su información o enviado mensajes sugestivos o agresivos a compañeros y/o maestros, por lo que, además de buscar una solución técnica, como pedagoga mi interés fue más allá y quise saber cómo podríamos apoyar a esas escuelas.

Esto me llevó a decidir que era importante hablar de ciberseguridad, pues en los primeros casos, el punto crítico se encontraba en que los alumnos tenían contraseñas asignadas de fácil acceso como abc123, 123456, etc, lo que las hace sumamente vulnerables; en el segundo caso, encontramos que no solo era un tema de ciberseguridad, sino de reglas de uso de la tecnología y es por eso que noté la relevancia de conocer más sobre ciudadanía digital.

En todos los casos, tanto la ciudadanía digital como la ciberseguridad iban de la mano y era necesario hacer del conocimiento de las escuelas que debían tener información al respecto y poder compartirlo con su comunidad, es así como decidí que podía plasmar dentro de la tesina algunos ejemplos de cómo se puede poner al alcance de todos una información tan técnica como lo es la ciberseguridad.

Dentro del primer capítulo se abordará el tema de la educación privada en México, así como el desarrollo psico-social de los adolescentes y el uso de la tecnología de este sector poblacional. Todo esto planteado desde la educación privada, por lo que se abordará también la parte legal, pues es necesario entender cómo es que estas escuelas tuvieron su auge y por qué se les permite cambiar, de cierta forma, el plan de estudios para impartir asignaturas que no forman parte de lo que estipula la Secretaría de Educación Pública.

Lo anterior se basa en la educación en tiempos de COVID-19, pues fue el parteaguas para pasar de lo convencional a lo digital dentro de las aulas, que si bien, por el creciente desarrollo tecnológico se han empezado a incluir dentro de las clases diferentes dispositivos, no habíamos dimensionado qué tan preparados estábamos todos para poder realizar clases 100% virtuales.

En el segundo capítulo se centrará en la ciudadanía digital y por qué es importante hablar de ella junto al tema de ciberseguridad, ya que a pesar de ser conceptos diferentes uno ayuda al otro a que se cumplan ciertas reglas dentro de la vida digital, las cuales lograrán que los ciudadanos digitales sean personas críticas de sus acciones.

En este capítulo también se abordarán ambos temas desde la perspectiva del país, que si bien, aún nos encontramos en vías de desarrollo con ambos, si se han realizado acciones para poder establecerlos y dar pie a mejoras, las cuales en su mayoría se encuentran estipuladas dentro de acuerdos firmados por México con organismos internacionales a los cuales pertenecen y responden a proyectos de crecimiento en temas digitales.

El punto central de este capítulo es la ciberseguridad, el cual se escucha más a menudo, pero que aparentemente carece de difusión y sobre todo en el área educativa, por lo que, se presentarán los diferentes tipos de riesgos cibernéticos a los que estamos expuestos y las recomendaciones de cuidado que marcan las principales empresas de tecnología y ciberseguridad del mundo.

Con la información de los dos capítulos anteriores se llegará al tercer y último capítulo, en el cual se mostrarán los diferentes materiales que se elaborarán como infografías, juegos y retos que se diseñarán para que se puedan usar dentro de las escuelas, tanto con los alumnos como con el personal docente y administrativo.

Dicho material se tiene pensado hacer para uso individual y no es necesario que todos sean aplicados en las escuelas, pues dependerá de las necesidades de cada centro educativo.

El objetivo principal de ese material es poder poner al alcance de todos la información de la ciberseguridad y la ciudadanía digital, pues muchas veces el desconocimiento de esto no se debe a la falta de información, sino a que ésta es demasiado técnica y de difícil comprensión, por lo que como pedagoga puedo apoyar a la población y ponerla a su alcance, haciéndola mucho más entendible y de fácil acceso.

Como bien sabemos, la vida digital ya es algo cotidiano, pero no por eso somos expertos en los temas de buenas prácticas, así como de seguridad dentro de internet, por lo que hablar de ello se considera de suma importancia para evitar un impacto negativo dentro de la educación, sobre todo en las clases virtuales.

1. Los adolescentes y el nivel secundaria de escuelas privadas en México.

Para poder hablar de los estudiantes de secundaria pertenecientes a escuelas privadas, es importante profundizar sobre este tipo de educación en el país, explicar la legislación que la rige, ya que, a pesar de que tienen cierta libertad para poder establecer horarios de asistencia a la escuela y de contenidos brindados, hay algunos que deben ser impartidos de forma obligatoria para cubrir con los aprendizajes esperados indicados por la Secretaría de Educación Pública.

Otro punto importante de cubrir es el de la educación en tiempos de COVID 19, ya que, al no poder estar de forma presencial en las aulas, muchas de las instituciones privadas de México decidieron contratar diferentes herramientas tecnológicas para poder llevar a cabo las clases de manera remota; grandes empresas como Google decidieron poner de forma gratuita el acceso a su conjunto de aplicaciones como apoyo a la educación, siendo de las herramientas con mayor demanda dentro de las instituciones.

También se explicará porqué la edad de los alumnos que cursan el nivel secundaria los convierte en un sector vulnerable en el tema de ciberseguridad basándonos en estudios de psicólogos que explican el desarrollo psicosocial, y madurez cognitiva, por medio de etapas según la edad del individuo.

Cabe mencionar que, no se toma a los adolescentes como sujetos iguales en comportamiento, desarrollo, habilidades, etc., sino que es un individuo completamente diferente a los demás, cada uno posee su propia personalidad, habilidades, madurez, etc.

El último punto para tratar es acerca las investigaciones de uso de la tecnología en adolescentes, lo que nos ayudará a dar pie al segundo capítulo de la tesina.

Estos últimos años ha ido evolucionando mucho la tecnología y prácticamente en todos los hogares se cuenta con al menos 1 dispositivo de computo y acceso a internet, y en la mayoría de los casos cada integrante de las familias cuenta con un teléfono celular que se conecta a la red y tiene acceso a la descarga de aplicaciones que ayudan a los estudiantes con la educación a distancia.

1.1. La educación privada en México.

Hablar de educación privada en México puede ser un tema controversial, ya que por años se ha estigmatizado a este sector, se le ha señalado de elitista y clasista debido a que no todos pueden tener acceso a este tipo de escuelas, por lo mismo, se ha llegado a mencionar que cobran por permitir ingresar a ellas y que los niños reciban educación, no son más que un negocio en dónde el dueño es el único ganador.

En 1940 Jaime Torres Bodet siendo secretario de educación impulsó la creación de escuelas privadas en el país, invitando a particulares a crear centros de estudios para cubrir la demanda de acceso a la educación¹; esto, aunado a la tan marcada diferencia de clases sociales, impulsó que los centros educativos privados fueran estereotipados como clasistas y elitistas, pues el acceso a ellos dejaba muy en claro que quién podía pagar por la educación era porque tenía ingresos económicos elevados o eran líderes nacionales, además de que para ingresar, los aspirantes de alumnado debían pasar exámenes de admisión, emulando a colegios jesuitas o maristas, lo que aseguraba que ingresaran alumnos “sin problemas.”²

¹ Torres Septián, Valentina. 1984. *Algunos Aspectos De Las Escuelas Particulares En El Siglo XX.. Historia Mexicana*. Página 350. Disponible en línea: <https://historiamexicana.colmex.mx/index.php/RHM/article/view/2588/2099> (consultado el 28 de enero 2022)

² *Ibid.* Pag. 352

Actualmente, la educación privada en el país se rige por el artículo 3º de la Constitución Política de los Estados Unidos Mexicanos, la cual, en el párrafo IV indica que:

*Los particulares podrán impartir educación en todos sus tipos y modalidades. En los términos que establezca la ley, el Estado otorgará y retirará el reconocimiento de validez oficial a los estudios que se realicen en planteles particulares.*³

Por lo que, la educación privada, puede impartir clases de acuerdo con lo que mejor convenga siempre y cuando cumpla con el plan de estudios establecido por la Secretaría de Educación Pública (SEP).

Entonces ¿qué cosas deben impartir de forma obligatoria las escuelas secundarias privadas?

De acuerdo con el mapa curricular establecido por la SEP en su portal de internet, en nivel secundaria los contenidos se encuentran divididos en tres componentes curriculares (Ver gráfico 1 y 2 en anexos):

- Formación académica
- Desarrollo personal y social
- Autonomía curricular

Estos componentes se dividen en las asignaturas a impartir dentro de las escuelas, siendo el componente Formación académica en donde la SEP indica las asignaturas obligatorias para toda la secundaria, ya sea pública o privada.

En el caso de las áreas de Desarrollo Personal y Social, en la asignatura de artes, se sugieren 4 opciones para que la escuela las imparta:

- Artes visuales
- Danza
- Música
- Teatro

³ Constitución Política de los Estados Unidos Mexicanos.
<https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf> (consultado el 2 febrero 2022)

El componente autonomía curricular, es en donde las escuelas privadas pueden realizar algunos cambios pero es de suma importancia que brinden los contenidos de los componentes de Formación académica y Desarrollo Personal y Social.

Es importante mencionar que no toda sede que se haga llamar escuela y cobre por brindar educación se encuentra avalada por la SEP, pues se requiere de una autorización que brinda esta dependencia por medio del acuerdo 255, por el que se establecen los trámites y procedimientos relacionados con la autorización para impartir educación secundaria, para que dichos estudios sean válidos ante el organismo encargado de regular la educación básica del país.

Como podemos ver, las escuelas privadas actualmente responden a una demanda en el acceso a la educación, misma que, para poder brindar un plus a las familias mexicanas, optan por adaptar el mapa curricular e impartir clases extras como idiomas o talleres; también hay otras que, deciden incorporarse a algún grupo religioso y a pesar de que la educación debe ser laica, en el ámbito privado se permite impartir este tipo de contenidos mientras no se descuide lo ya indicado por la SEP.

1.1.1. La educación privada en tiempos de COVID en México

Estos años han sido bastante inestables para la mayoría de los habitantes del país, pero uno de los sectores que se vio más afectado, fue el de la educación privada, pues muchos padres de familia prefirieron dejar de gastar dinero en altas colegiaturas para invertirlo en otras necesidades.

La pérdida de empleos, la falta de infraestructuras tecnológicas y el desconocimiento de herramientas tecnológicas, ayudó a que muchos centros de estudios privados perdieran alumnado, aunque muchos otros tomaron esto como

un reto para salir de lo convencional y optaron por aprender a usar la tecnología y de esta forma llevar hasta el hogar de cada alumno la enseñanza a través de una pantalla.

Muchas empresas dedicadas a la tecnología abrieron de forma gratuita el uso de sus herramientas para apoyar el desarrollo de la educación, como lo realizó Google, por lo que las escuelas aprovecharon y decidieron convertirse en expertos de las herramientas, tratar de darles a los alumnos sus clases como merecen para que pudieran seguir aprendiendo.

Otros colegios, no tan apegados a la tecnología, solamente optaron por utilizar las herramientas de videoconferencia que también se ofrecieron de forma gratuita como Zoom y Webex.

A pesar de que actualmente se están retomando las clases presenciales, no todos los alumnos han regresado a las aulas, por lo que muchas escuelas privadas tienen la opción de las aulas híbridas, donde una parte de los alumnos está en la escuela en clase presencial y la otra parte en casa desde su dispositivo y conectado a una sesión remota.

Otras escuelas privadas, optaron por contratar plataformas educativas, qué, además de brindarles el acceso a dicha herramienta, les diera opciones de equipamiento para sus aulas, por ejemplo, Sistema UNOi, Santillana Compartir, Knotion y AMCO.

La pandemia ha generado crisis en el ámbito educativo, pero también ha permitido ver que se requiere una actualización de los métodos que se estaban utilizando para la impartición de clases, ha dejado al descubierto que no todos estamos listos para dejar lo ya conocido para adaptarnos a las tecnologías y, lo más importante, ha dejado en claro que, a pesar de todo, siempre vamos a encontrar la forma de salir adelante para lograr formar a los alumnos.

1.2. Los adolescentes de secundaria y su rango de edad

Para empezar a hablar de este sector poblacional, es importante definir lo que entendemos por adolescencia, la cual, de acuerdo con la UNICEF es una etapa necesaria e importante para hacernos adultos. Esencialmente es una etapa con valor y riqueza en sí misma, que brinda infinitas posibilidades para el aprendizaje y el desarrollo de fortalezas. Es una etapa desafiante, de muchos cambios e interrogantes para los adolescentes, pero también para sus padres y adultos cercanos.⁴

De acuerdo con la Organización Mundial de la Salud, la adolescencia abarca de los 10 a los 19 años, la cual se divide en 3 etapas:

Etapa	Características	Rango de edad
Temprana	Las hormonas sexuales comienzan a estar presentes y por esto se dan cambios físicos, cambia la voz, aparece vello púbico y en axilas, olor corporal, aumento de sudoración y con esto surge el acné. Comienzan a buscar cada vez más a los amigos.	Entre los 10 y los 13
Media	Comienzan a evidenciarse cambios a nivel psicológico y en la construcción de su identidad, cómo se ven y cómo quieren que los vean. La independencia de sus padres es casi obligatoria y es la etapa en la que pueden caer fácilmente en situaciones de riesgo.	Entre los 14 y los 16

⁴ UNICEF. ¿Qué es la adolescencia? <https://www.unicef.org/uruguay/que-es-la-adolescencia> (Consultado el 5 de febrero de 2022)

Tardía	Comienzan a sentirse más cómodos con su cuerpo, buscando la aceptación para definir así su identidad. Se preocupan cada vez más por su futuro y sus decisiones están en concordancia con ello. Los grupos ya no son lo más importante y comienzan a elegir relaciones individuales o grupos más pequeños.	De los 17 y puede extenderse hasta los 21
--------	---	---

Tabla realizada con información de la UNICEF.⁵

Según datos estadísticos del Instituto Nacional para la Evaluación de la Educación (INEE), en sus indicadores educativos del ciclo escolar 2017-2018, tan solo en la Ciudad de México la población de entre 12 y 14 años, considerada como la ideal para cursar secundaria era de 380,019 alumnos, de los cuales 72,279 estaban inscritos en una de las 540 escuelas secundarias privadas.⁶

De acuerdo con las estimaciones de la Secretaría de Educación Pública (SEP) en el ciclo 2020-2021 la población perteneciente a nivel secundaria en el sector privado era de 68,680 alumnos inscritos en alguna de las 622 escuelas.⁷

Basándonos en el rango de edad ideal para cursar la secundaria en México indicado por el INEE, los alumnos se encuentran entre los 12 y los 14 años, pero de acuerdo con la experiencia personal, en el último grado de secundaria están entre los 14 y 15 años, por lo que el límite del rango de edad que estaremos contemplando en el trabajo para poder brindar más detalles sobre estos adolescentes serán los 15 años.

⁵ *Idem*

⁶ INEE. *Principales cifras Educación básica y media superior Inicio del ciclo escolar 2017-2018*. <https://www.inee.edu.mx/wp-content/uploads/2019/08/P2M111.pdf> (Consultado el 25 de enero de 2022)

⁷ SEP. *Estadística educativa México. Ciclo escolar 2020-2021*. http://planeacion.sep.gob.mx/Doc/estadistica_e_indicadores/estadistica_e_indicadores_entidad_federativa/estadistica_e_indicadores_educativos_15MEX.pdf (Consultado el 25 de enero de 2022)

Como lo indica la OMS, en la adolescencia media comienzan los cambios psicológicos, la construcción de la identidad y la idea de la independencia de sus padres, lo que hace que esta edad sea estigmatizada como una de las etapas más difíciles, se les denomina como conflictivos y se les trata desde el prejuicio, sin tomar en cuenta que es la etapa donde se forma la autoestima y la confianza.

1.3. El desarrollo psicosocial de los adolescentes de secundaria

Para poder dar pie a la explicación del desarrollo psico-social, es importante partir de lo que entendemos por el término. Según el diccionario médico de la Universidad de Navarra es el proceso de interacción progresiva entre el niño y su ambiente por el que va adquiriendo las capacidades, y especialmente los conocimientos, que le convierten en miembro adulto de su sociedad.⁸

Existen autores que explican este desarrollo por etapas, llegando hasta la adolescencia, la cual, es la que nos interesa en nuestro trabajo.

Entre los autores más destacados en este tema, hay 2 que nos apoyarán a dar bases en lo que se quiere explicar; el primero es Erikson, un psicoanalista estadounidense, cuyo principal trabajo fue el de extender el estudio del psicoanálisis del desarrollo psicosexual hacía lo psicosocial.

La perspectiva de Erikson fue organizar una visión del desarrollo del ciclo completo de la vida de la persona humana, extendiéndolo en el tiempo, de la infancia a la vejez.⁹ (Ver Anexos, gráfico 3)

En este trabajo tomaremos como referencia el estadio V – Adolescencia (12 a 20 años), en esta etapa la principal tarea es la de buscar la identidad del individuo, los adolescentes se centran en responder la pregunta ¿Quién soy?; también

⁸ Clínica Universidad de Navarra. *Diccionario médico* <https://www.cun.es/diccionario-medico/terminos/desarrollo-psicosocial> (Consultado el 27 de enero de 2022)

⁹ Redalyc. *El desarrollo psicosocial de Eric Erikson. El diagrama epigenético del adulto* <https://www.redalyc.org/pdf/695/69520210.pdf> . (Consultado el 5 febrero de 2022)

comenzarán a buscar la aprobación social, es decir, comenzarán a tener grupos de amigos con los que se identifique y sienta que tiene afinidad.

El segundo autor es Vygotsky, psicólogo ruso que estudió el desarrollo sociocultural, el cual, pone atención en la participación proactiva de los menores con el entorno que les rodea, siendo el desarrollo cognoscitivo fruto de un proceso colaborativo con su contexto social.¹⁰

Vygotsky menciona que los niños desarrollan su aprendizaje por medio de la interacción social.

De acuerdo con lo anterior, podemos decir que el individuo aprende de acuerdo con el entorno social que lo rodea como la familia, amigos, compañeros de clase, etc.

A mí parecer, ambas teorías son parte importante del desarrollo, pues los adolescentes son muy diversos y no existe un patrón de comportamiento, como bien lo indica Vygotsky, la parte social influye mucho, pues el adolescente tomará parte de lo que su familia le brinde como los valores, pero también lo complementará con lo que descubra de forma individual, como el saber quién es sin lo que se le ha impuesto en la familia, qué cree, qué le gusta, qué piensa y de esta forma irá conformando su YO.

1.4. La madurez cognitiva de los adolescentes en edad correspondiente a nivel secundaria

Si bien, según las teorías del desarrollo vamos alcanzando ciertas metas en el ámbito cultural, social, y biológico, la madurez cognitiva también juega un papel importante, pues puede que tenga desarrollada de forma correcta su parte psicosocial, pero sus actitudes aún son muy infantiles, o al revés, todo esto depende de qué tanto se ha desarrollado la parte cognitiva; por lo que, aquí abordaremos

¹⁰ Eduimpulsa. La teoría sociocultural de L. Vygotsky. <https://eduimpulsa.com/la-teoria-sociocultural-de-vigotsky/> (Consultado el 5 de febrero de 2022)

desde esa perspectiva el porqué los adolescentes de 12-15 años aún suelen ser impulsivos en sus decisiones.

Según la organización Stanford Children's Health, el desarrollo cognitivo significa el crecimiento de la capacidad de un niño de pensar y razonar.¹¹

Este proceso se presenta entre los 6 y los 18 años, por lo que, la edad en la que se encuentran los alumnos de secundaria están casi finalizando su adolescencia, pasan de un pensamiento concreto a tener operaciones lógicas formales. Es importante notar que:

- Cada niño progresa a su propio ritmo respecto a la capacidad de pensar de maneras más complejas.
- Cada niño desarrolla su propia visión del mundo.
- Algunos niños son capaces de utilizar operaciones lógicas en las tareas escolares mucho antes de que pueden utilizarlas para resolver sus problemas personales.
- Cuando surgen los problemas emocionales, estos pueden interferir con la capacidad de pensar de maneras complejas.
- La posibilidad de considerar posibilidades y realidades puede afectar la toma de decisiones. Esto puede ocurrir de maneras positivas o negativas.¹²

Se puede decir que, la madurez cognitiva nos ayudará a tomar decisiones, pero se apoyará de lo que el adolescente es, es decir, dependerá de los valores que tenga, de las creencias y de la personalidad.

¹¹ Stanford Children's Health. *Desarrollo cognitivo*.

<https://www.stanfordchildrens.org/es/topic/default?id=desarrollocognitivo-90-P04694> (Consultado el 28 de enero de 2022)

¹² *Idem*

1.5. Uso de dispositivos tecnológicos en adolescentes de secundaria en México

Los adolescentes están muy familiarizados con el uso de dispositivos tecnológicos como el celular, computadoras, tabletas, etc. Por lo que, podemos suponer que el uso de herramientas de comunicación como mensajería instantánea, redes sociales, correo electrónico, entre otros, son de su completo manejo.

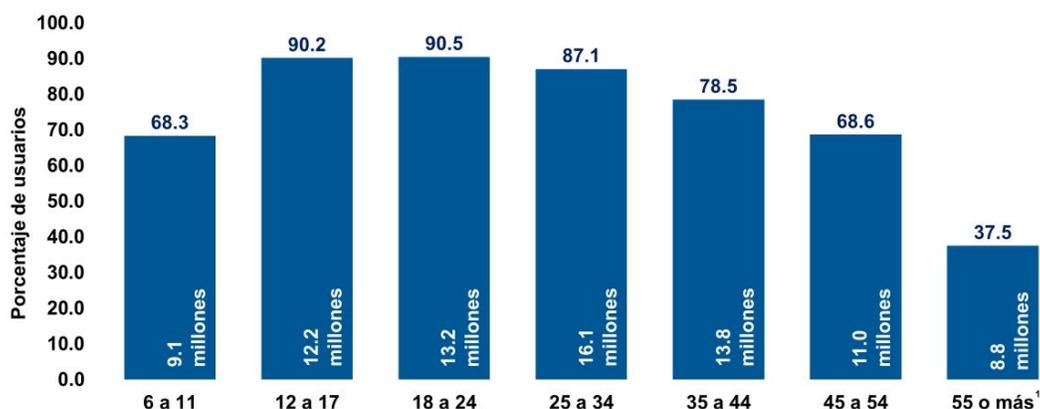
Marc Prensky, escritor y conferencista estadounidense, indicó en 2001 que los adolescentes actuales ya no pueden aprender como los de antes, pues sus cerebros y culturas son completamente diferentes. Esto lo explica mediante su término “nativo digital”, el cual indica que las generaciones que nacieron y han crecido con las tecnologías los convierte en nativos digitales, pues toda su vida la han tenido y no ha sido necesario aprender a incorporarla a su rutina diaria, por el contrario, solamente van actualizando lo que ya saben.

De acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020, en México 84.1 millones de personas son usuarios de internet, que representan 72% de la población de seis años o más. Esta cifra revela un aumento de 1.9 puntos porcentuales respecto a la registrada en 2019 (70.1%).¹³

El grupo de edad que más utiliza el internet es el de 18 a 25 años, seguido del grupo de 12 a 17, esto de acuerdo con la Encuesta ENDUTIH 2020.

¹³ Comunicado de Prensa. *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2020*. https://www.gob.mx/cms/uploads/attachment/file/647466/ENDUTIH_2020_co.pdf (Consultado el 5 de febrero de 2022)

Distribución de los usuarios de Internet por grupos de edad, 2020



Nota: Porcentajes calculados respecto de la población total de seis años o más por grupo de edad.
¹ Incluye a las personas que no supieron especificar la edad.

Fuente: Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020.

Gráfico tomado de Twitter. <https://twitter.com/SantaellaJulio/status/1407424267910844421/photo/1>

Los tres principales medios para la conexión de usuarios a internet en 2020 fueron: celular inteligente (Smartphone) con 96.0%, computadora portátil con 33.7% y televisor con acceso a internet 22.2%¹⁴

De acuerdo a lo anterior, los adolescentes que cursan el nivel secundaria ya son considerados nativos digitales, pues toda su vida han estado cerca de la tecnología, lo que los hace interactuar de forma más directa por medio de las redes sociales y aplicaciones de mensajería instantánea. También se encuentran en el segundo grupo de edad con más uso de internet desde cualquier dispositivo.

Actualmente, debido a la COVID 19, las clases tuvieron que migrar a espacios tecnológicos, por lo que el uso de herramientas de videoconferencias se han convertido en la principal fuente de conexión entre las escuelas y los alumnos, provocando que pasen más tiempo frente a los dispositivos y hagan mayor uso de aplicaciones de mensajería, correo o alguna plataforma educativa.

¹⁴ *Idem*

Debemos entender que las cosas cambian, que la tecnología avanza y que la podemos aprovechar en el ámbito educativo, mejorando los planes de estudio, reforzando los aprendizajes y llamando la atención de nuestros alumnos con temas de su interés. Como padres de familia, docentes o personas enfocadas en el ámbito educativo tenemos la obligación de abrir nuestro panorama y no quedarnos en lo que conocemos, debemos aprender a llevar la tecnología a las aulas y que nuestros alumnos se apropien de ella sabiendo decidir qué sirve y qué no.

Es por todo lo anterior que podemos decir que el tema de la ciberseguridad y el reforzamiento de la ciudadanía digital es de suma importancia para poder ayudar a nuestros adolescentes a cuidarse dentro de las tecnologías, así como dar pauta a que no todo lo que hagan en internet o con tecnologías como los videojuegos se estigmatice y se denomine como una pérdida de tiempo; es por esto, que en el siguiente capítulo podremos comprender qué es la ciberseguridad y cuál es el impacto dentro de la educación.

2. Ciberseguridad y Educación.

La reciente pandemia mundial debido a la COVID-19 ha obligado a los centros escolares a mudarse a las aulas virtuales, haciendo que los alumnos utilicen plataformas educativas, así como otras herramientas tecnológicas dentro de la red para poder tener acceso a sus clases.

Debido a esto, es que se plantea una de las principales cuestiones ¿Qué tanto conocimiento de seguridad tenemos en torno al uso de todas estas herramientas que nos brindan acceso a información en internet? Si nos ponemos a analizar la pregunta, varios podrían afirmar que lo manejan, otros podrían indicar que no al grado que les gustaría, pero sin importar cuál sea la respuesta a dicha cuestión, todas nos llevarán a la pregunta: ¿qué tanto nos impacta dentro de la educación el desconocimiento de la ciberseguridad?

Así mismo, otro punto importante de revisar es el comportamiento dentro del internet, pues muchas veces creemos que por estar tras un monitor, somos anónimos y podemos hacer lo que queramos, pero no es así, pues parte de las iniciativas de los principales organismos sobre el desarrollo de la educación y la infancia ha determinado ciertos puntos de comportamiento, los cuales se utilizan de manera global, haciendo que no se presenten límites geográficos, pero sí permitiendo que cada país actúe de acuerdo a sus leyes establecidas por el uso indebido de esta herramienta.

Actualmente, las escuelas se han tenido que acercar al mundo de las tecnologías, muchos sin antes haberlo hecho y sin siquiera tener un conocimiento previo de cómo manejarlas, pero ante la demanda, decidieron aventurarse y hacer lo mejor posible, pero a todo esto ¿qué es la ciberseguridad, por qué es tan importante conocerla para tener en cuenta el impacto dentro de la educación, existen reglas dentro del mundo cibernético? ¿Existe algún código de conducta dentro de internet? En este capítulo podremos comprender estos conceptos.

2.1 ¿Qué es la ciberseguridad?

Para poder hablar de la ciberseguridad recurriré a citar a 3 de las empresas más importantes tanto en el tema de protección digital como en el ámbito de fabricación de dispositivos y desarrollo de software

Según Kaspersky, empresa de ciberseguridad, es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.¹⁵

De acuerdo con CISCO, empresa dedicada a fabricar dispositivos para redes locales y externas, indica que, la ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales.¹⁶

Para Microsoft, empresa dedicada a fabricar dispositivos y software, indica que la ciberseguridad es la práctica de proteger su información digital, dispositivos y activos. Esto incluye información personal, cuentas, archivos, fotos e incluso el dinero.¹⁷

De acuerdo a las tres definiciones citadas, podemos decir que la ciberseguridad nos ayuda a tener protegida nuestra información digital y forma parte de las buenas prácticas para el correcto uso de la tecnología.

Pero... ¿qué es lo que debemos cuidar? ¿cuáles son los aspectos que la escuela debe tomar en cuenta para que su ciberseguridad no sea vulnerada tan fácilmente?

¹⁵ Kaspersky. ¿Qué es la ciberseguridad? <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security> (consultado el 27 de enero de 2022)

¹⁶ CISCO. ¿Qué es la ciberseguridad? https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html (consultado el 27 de enero de 2022)

¹⁷ Microsoft ¿Qué es la ciberseguridad? <https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390> (Consultado el 15 de marzo de 2022)

De acuerdo a CISCO, lo que debemos tomar en cuenta para protegernos son tres entidades:

1. Los dispositivos Endpoints (como computadoras, dispositivos inteligentes y routers)
2. Las redes
3. La nube

La tecnología común que se usa para proteger estas entidades incluye firewalls, filtrado de DNS, protección contra malware, software antivirus y soluciones de seguridad de correo electrónico¹⁸.

De acuerdo con Microsoft, el cuidar solamente los dispositivos no nos mantiene protegidos, pues indica que la seguridad digital también requiere que se establezca un conjunto de procesos y procedimientos adecuados, como lo son:

- Copias de seguridad de datos: los datos importantes deberían almacenarse en una ubicación segura y debería poder restaurar una copia correcta y probada de los datos en caso de que algo malo le suceda al archivo.
- Buenos hábitos cibernéticos: no abra vínculos o datos adjuntos inesperados que pueda recibir en correo electrónico o mensajes de texto, aunque parezcan proceder de un remitente de confianza.
- Mantener el software actualizado: los sistemas operativos como Windows, MacOS, iOS o Android, así como las aplicaciones y exploradores deben mantenerse actualizados con las revisiones y correcciones más recientes del fabricante.
- Usar contraseñas seguras, únicas: las contraseñas buenas deben tener al menos 14 caracteres, no deben ser palabras en inglés y no se deben volver a usar en varias cuentas.
- Usar la autenticación multifactor: siempre que sea posible, tanto en casa como en el trabajo, habilite la autenticación multifactor para mantener sus cuentas más seguras.

¹⁸ CISCO. *¿Qué es la ciberseguridad?* https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html (consultado el 27 de enero de 2022)

- Bloquear los dispositivos: asegúrese de que sus dispositivos requieren una contraseña, PIN o autenticación biométrica como una huella digital o un reconocimiento facial para poder iniciar sesión en ellos. Los dispositivos perdidos o robados pueden ser una mina de oro para criminales si pueden acceder fácilmente a los datos de un dispositivo desbloqueado.¹⁹

También indica que, la ciberseguridad debe contemplar 3 puntos muy importantes para todos los usuarios:

- Confidencialidad: mantener los secretos y garantizar que solo los usuarios autorizados puedan obtener acceso a sus archivos y cuentas.
- Integridad: garantizar que su información es la que debe ser y de que nadie ha insertado, modificado o eliminado cosas sin su permiso. Por ejemplo, cambiar malintencionadamente un número en una hoja de cálculo.
- Acceso: garantizar que puede tener acceso a su información y sistemas cuando lo necesite. Un ejemplo de un problema de acceso sería una denegación de servicio, donde los atacantes desbordan el sistema con tráfico de red para hacer que el acceso sea casi imposible; o ransomware que cifra el sistema e impide que lo use.²⁰

Ahora bien, si enfocamos la ciberseguridad en la educación y en específico en la escuela, se podría decir que ésta abarca los temas de administración de redes, acceso o bloqueo de ciertas páginas en internet, permitir la conexión a internet desde diversos dispositivos, administración de cuentas ya sean correos institucionales, datos de acceso por usuarios a plataformas, etc.

La ciberseguridad entonces, no se trata solo de decidir qué página visito, abarca todo nuestro entorno digital y sus componentes, se trata de hacer nuestra comunidad educativa un entorno más seguro dentro de la vida tecnológica, por lo que, no solo es un tema de atención dentro de las escuelas, sino que esta

¹⁹ Microsoft *¿Qué es la ciberseguridad?* <https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390> (Consultado el 15 de marzo de 2022)

²⁰ *Idem*

información se puede ampliar para que se lleve a casa y hagamos una comunidad más segura dentro y fuera de las aulas.

2.2. La ciberseguridad en México

En la Ciudad de México la ciberseguridad está a cargo de la policía cibernética, la cual fue fundada en abril del 2013 con la finalidad de prevenir, por medio del monitoreo y patrullaje en la red pública, cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y patrimonial de los habitantes de la Ciudad de México [...] y busca, con estrategias de prevención, inculcar entre los cibernautas una cultura de respeto y “Civismo Digital”.²¹

Durante el año 2017 en México se llevaron a cabo varios foros, talleres y espacios de debate, los cuales concluyeron con la realización de La Estrategia Nacional de Ciberseguridad (ENCS) cuyo objetivo era identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.²²

Dicha Estrategia Nacional se mantuvo durante el mandato de Enrique Peña Nieto (2012-2018), pero al momento de ingresar el gobierno a cargo de Andrés Manuel López Obrador (2018 – actual), la Estrategia del gobierno anterior se dejó de lado, dando paso a una Estrategia de Ciberseguridad a cargo de la Secretaría de Marina, así como algunos manuales de mejores prácticas para la ciberseguridad orientadas

²¹ Policía Cibernética. *¿Quiénes somos?* <https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica> (Consultado el 10 marzo de 2022)

²² *Estrategia Nacional de Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (Consultado 15 de marzo de 2022)

al sector privado, a cargo de la Secretaría de la Defensa Nacional (Sedena) y el Centro de Respuesta a Incidentes de la Guardia Nacional (CSIRT-MX)²³

Actualmente la Secretaría de Marina se encuentra a cargo de la Unidad de Ciberseguridad, la cual tiene como misión planear, conducir y ejecutar las actividades de seguridad de la información, ciberseguridad y ciberdefensa para la protección de la infraestructura crítica de la Secretaría de Marina - Armada de México y coadyuvar en el esfuerzo nacional para el mantenimiento de la integridad, estabilidad y permanencia del Estado mexicano.²⁴

La Secretaría de Marina realizó la Estrategia Institucional para el Ciberespacio, en la cual puntualizan 4 acciones específicas:



Gráfico tomado del documento de la Estrategia Institucional para el Ciberespacio pág. 8 https://www.gob.mx/cms/uploads/attachment/file/661788/Estrategia_Institucional_Ciberespacio_SM.pdf

²³ El economista. *Las estrategias nacionales de ciberseguridad deben tener un enfoque civil: MITRE.* <https://www.economista.com.mx/tecnologia/Las-estrategias-nacionales-de-ciberseguridad-deben-tener-un-enfoque-civil-MITRE-20210921-0088.html> (consultado 15 de marzo de 2022)

²⁴ Unidad de Ciberseguridad. *Seguridad y Defensa en el Ciberespacio.* <https://www.gob.mx/semar/articulos/unidad-de-ciberseguridad-279197?idiom=es> (Consultado el 15 de marzo de 2022)

México pertenece a diferentes Organismos internacionales, por lo que debe atender ciertas actividades en pro del desarrollo del país; una de esas actividades es justamente la ciberseguridad, tema que tiene en desarrollo junto a la Organización de Estados Americanos (OEA), quien creó el Programa de Ciberseguridad, el cual tiene como objetivos:

- Apoyar a los Estados Miembros de la OEA en el desarrollo de capacidades técnicas y políticas para prevenir, identificar, responder y recuperarse exitosamente de incidentes cibernéticos.
- Mejorar el intercambio de información, la cooperación y la coordinación sólidas, efectivas y oportunas entre las partes interesadas en seguridad cibernética a nivel nacional, regional e internacional.
- Aumentar el acceso al conocimiento e información sobre amenazas y riesgos cibernéticos por parte de los interesados públicos, privados y de la sociedad civil, así como los usuarios de Internet.²⁵

Los esfuerzos regionales del Programa de Ciberseguridad son multifacéticos y se centran en (I) el desarrollo de políticas, (II) la creación de capacidad (incluida la capacitación y los ejercicios) y (III) la investigación y la divulgación.²⁶

Entrando a temas educativos, dentro de la ciberseguridad se tienen planes de acción mediante pláticas informativas enfocadas al acoso escolar, acoso por parte de otras personas fuera del entorno escolar, robo de identidad y Sexting. También han empezado a difundir información sobre recomendaciones para llevar a cabo clases virtuales de forma segura, dividiendo en recomendaciones para alumnos, para maestros y para padres de familia.

²⁵ OEA. *Programa de Ciberseguridad*. <https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp>
(Consultado 15 de marzo de 2022)

²⁶ *Idem*

Con toda esta información en mente, podemos darnos cuenta que México aún se encuentra en vías de desarrollo respecto a la ciberseguridad, pues no tenemos una continuidad sobre las estrategias planteadas, además de que no se contempla en ningún momento a la educación dentro de los sectores vulnerables, que si bien, se ha avanzado en informar sobre algunos temas en el ámbito educativo, la ciberseguridad no solo se centra en eso y es necesario darlo a conocer.

Como lo hemos visto a lo largo de esta investigación, la educación inmersa en la virtualidad también es un tema que se ha venido desarrollando poco a poco y es justo por esto que debemos tener en cuenta la importancia de estos temas como profesionales de la educación.

2.3. Identificación de los diversos ataques cibernéticos

Dentro del mundo de las ciberamenazas, se tienen identificados varios tipos de ellas, por lo que diversas instituciones se han dado a la tarea de organizarlos e identificarlos para poder darlos a conocer, haciendo que, los principales consumidores de la tecnología estén alerta y eviten caer en ellas.

Para Kaspersky, existen 3 tipos de ciberamenazas

1. El delito cibernético incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.
2. Los ciberataques a menudo involucran la recopilación de información con fines políticos.
3. El ciberterrorismo tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor.²⁷

De acuerdo a este listado, los ciberdelicuentes se valen de diferentes métodos para lograr su cometido, siendo estos los principales:

²⁷ Kaspersky. ¿Qué es la ciberseguridad? <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security> (consultado el 27 de enero de 2022)

Tipo de amenaza ²⁸	Descripción
Suplantación de identidad (phishing)	Es la práctica de enviar correos electrónicos fraudulentos que se asemejan a correos electrónicos de fuentes de buena reputación. El objetivo es robar datos sensibles, como números de tarjetas de crédito e información de inicio de sesión. Es uno de los más comunes de ciberataque.
Ransomware	Es un tipo de software malicioso. Está diseñado para exigir dinero mediante el bloqueo del acceso a los archivos o el sistema informático hasta que se pague un rescate. El pago del rescate no garantiza que se recuperen los archivos o se restaure el sistema.
Malware	Es un tipo de software diseñado para obtener acceso no autorizado o causar daños en una computadora. Es una de las ciberamenazas más comunes.
Ingeniería social	Es una táctica que los adversarios usan para engañar a fin de que se revele información confidencial. Pueden solicitarle un pago monetario u obtener acceso a sus datos confidenciales. Puede combinarse con cualquiera de las amenazas listadas anteriormente para predisponerlo a hacer clic en un enlace, descargar malware o confiar en una fuente maliciosa.

²⁸ CISCO. ¿Qué es la ciberseguridad? https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html (consultado el 27 de enero de 2022)

En el caso del Malware, se divide en tipos, donde cada uno ataca de forma diferente.

Tipo de Malware ²⁹	Descripción
Virus	Es un programa capaz de reproducirse, que se incrusta en un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
Troyanos	Es un tipo de malware que se disfraza como software legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan datos
Spyware	Es un programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información.
Adware	Software de publicidad que puede utilizarse para difundir malware
Botnets	Son redes de computadoras con infección de malware que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario.

Estos listados no indican que no haya más o que en un futuro no puedan encontrarse otros tipos, pero las instituciones han realizado estas divisiones para que sea más fácil su identificación, así como la difusión de la información entre los usuarios y eviten caer en las trampas.

²⁹ Kaspersky. ¿Qué es la ciberseguridad? <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security> (consultado el 27 de enero de 2022)

Ahora, aterrizando a temas educativos, ¿en qué nos puede ayudar saber o contar con esta información? Pues justamente para poder educarnos en el uso del entorno tecnológico, que si bien ya tiene bastante tiempo estando a la mano de muchos pobladores de todo el mundo, no se había notado tanto la falta de información al respecto como en los últimos años, en donde hemos tenido que basar prácticamente todas nuestras actividades cotidianas en el uso de dispositivos con acceso a internet.

Planteando una situación meramente escolar, muchas escuelas decidieron migrar sus clases presenciales a la virtual mediante herramientas de videoconferencia, y supongamos que una escuela decidió que la forma en la que enviaría la información de las sesiones sería por correo electrónico, compartiendo una liga de acceso a dicha sesión virtual en un hilo de correos en donde, muchas veces, los maestros no ponían los destinatarios de forma oculta; en el cuerpo del mismo venía un enlace que, al dar clic dirigía a la sesión... ¿Cuántos riesgos de ser víctimas de un ciberataque se localizan en el caso? Al menos encontramos 3:

- 1- Correos masivos que pueden reenviarse logrando que caiga en manos de personas que no son de la escuela.
- 2- Robo de información, ya que al no tener un listado oculto, todos podemos consultar la información de los destinatarios
- 3- Ir a sitios no seguros al dar clic en una liga sin realmente verificar la fuente.

Es por esto, que queremos lograr que nuestras entidades educativas tengan la información mucho más a la mano, de forma entendible y así puedan hacer una comunidad escolar en línea mucho más segura para todos.

2.4. Ciudadanía digital

Para empezar a hablar de ciudadanía digital, es necesario comenzar por entender qué es ser ciudadano y podemos definirlo como:

*[...] ser miembro pleno de una comunidad, tener los mismos derechos que los demás y las mismas oportunidades de influir en el destino de la comunidad. También supone el cumplimiento de una serie de deberes y obligaciones vinculados a esos derechos.*³⁰

A nivel global, la ciudadanía digital se refiere principalmente a nuestras actitudes en los espacios digitales, y al mismo tiempo a nuestros derechos y obligaciones.³¹

Hace referencia a lo tecnológico, pero también a lo social y por lo tanto el concepto se encuentra en constante cambio, pues nos da la pauta de lo que puedo hacer y hasta qué punto está permitido.

En México, la ciudadanía digital se definió dentro del Cuaderno de Investigación No. 72 del Senado de la República como:

*Un conjunto de derechos y obligaciones que permiten la participación libre y responsable en una sociedad en línea, esto es, en una caracterizada por la mediación de las TIC. En este sentido, se propone abordar la ciudadanía digital como un concepto multidimensional en el cual se identifican al menos tres ejes analíticos: la accesibilidad, las habilidades y la participación política.*³²

³⁰ Faro democrático. ¿Qué es ser ciudadano? <https://farodemocratico.juridicas.unam.mx/que-es-ser-ciudadano-y-que-es-ser-ciudadana/> (Consultado el 18 de marzo de 2022)

³¹ UNICEF. *Guía de sensibilización sobre convivencia digital*. <https://www.unicef.org/argentina/media/9481/file/Gu%C3%ADa%20sobre%20Convivencia%20Digital-2020.pdf> (Consultado el 22 de febrero de 2022)

³² Zamora Saenz, Itzkuauhtli. (2020). *Una aproximación a la ciudadanía digital en México: acceso, habilidades y participación política*. Cuaderno de investigación No. 72, Instituto Belisario Domínguez, Senado de la República, Ciudad de México. http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5094/CI_72.pdf?sequence=1&isAllowed=y (Consultado el 16 de marzo de 2022)

Anteriormente, se tenían registros de comportamientos no debidos hacia otras personas dentro del mundo del internet, mismos que no estarían bien vistos hacerlos de manera presencial, pero todo era posible debido a que una pantalla y el anonimato nos respaldaba, por lo que se empezó a hablar sobre dar pautas de comportamiento, tratar de comprender que la vida en la tecnología es una extensión más de nuestro día a día y no un punto y aparte.

Dentro de la ciudadanía digital, a comparación con la definición de ciudadanía por sí sola, no existe un límite territorial geográfico, por lo que, al estar dentro de las redes de internet, debes hacer uso de las reglas sociales digitales, las cuales te permitirán poseer *un conjunto de competencias que faculta a los ciudadanos a acceder, recuperar, comprender, evaluar y utilizar, para crear, así como compartir información y contenidos de los medios en todos los formatos, utilizando diversas herramientas, de manera crítica, ética y eficaz con el fin de participar y comprometerse en actividades personales, profesionales y sociales.*³³

La UNESCO propone pensar la ciudadanía en ámbitos digitales desde tres niveles: el sujeto como receptor, como participante y como actor activo [...] Por lo tanto, podemos sostener que para avanzar en la búsqueda de una ciudadanía digital es necesario fomentar que las personas-usuarios de tecnologías digitales sean sujetos críticos, proactivos y conscientes de las oportunidades y riesgos que existen en las Tecnologías de la Información y la Comunicación (TIC).³⁴

Tal como lo indica el Ministerio de Educación en Chile, se deben cumplir ciertos lineamientos para cubrir con el objetivo de ser el ideal de ciudadano digital

³³ *Idem*

³⁴ *Idem*

Actitudes de un buen ciudadano en la era digital

- 1** Promueve un uso de los dispositivos adecuado a la edad, considerando los riesgos de su uso en la infancia
SALUD Y BIENESTAR DIGITAL
- 2** Aprovecha las posibilidades que otorga internet para aprender y adquirir competencias útiles para el mundo laboral
ALFABETIZACIÓN DIGITAL
- 3** Toma medidas de seguridad en los dispositivos personales como uso de antivirus y contraseñas
SEGURIDAD DIGITAL
- 4** Respeta la diversidad de opiniones comprendiendo que todas tienen el mismo valor, sin "enganchar" ni promover comentarios negativos o agresivos
ETIQUETA DIGITAL
- 5** Recuerda que todos tenemos derecho a acceder a internet, sin importar sexo, cultura o nivel socioeconómico
ACCESO DIGITAL
- 6** Se informa de manera responsable y verifica la información antes de compartirla
COMUNICACIÓN DIGITAL
- 7** Aprovecha los espacios de participación y creación de comunidad con ideas u objetivos que te representen
RESPONSABILIDAD Y DERECHOS DIGITALES
- 8** Cumple las normas de comportamiento y leyes asociadas a los sitios web y redes que utilizas
LEYES DIGITALES
- 9** Lee los términos y condiciones cuando compres un producto o des tus datos en un sitio web
COMERCIO DIGITAL

Gráfico tomado del cuadernillo de Ciudadanía Digital. Pág. 10

<https://formacionciudadana.mineduc.cl/wp-content/uploads/sites/46/2019/06/CiudadaniaDigital-Cuadernillo.pdf>

Actualmente en México se cuenta con un Plan de Ciudadanía Digital, el cual está a cargo de la Agencia Digital de Innovación Pública y se publicó en el 2019, en dicho plan se habla sobre el cómo el gobierno de la Ciudad de México empezará a hacer los trámites de forma virtual, facilitando la vida de la ciudadanía a partir del uso de la tecnología, pero promoviendo las leyes para la protección y resguardo de datos personales.

La COVID-19 nos ayudó a dar paso a una educación virtual y, aunque muchos espacios escolares ya estaban buscando las herramientas para innovar la educación, nadie estaba preparado para dar un salto tan grande como lo fue el hecho de tener un resguardo obligado en casa, no poder tener un contacto humano más allá de tu núcleo familiar, sin embargo, esta situación nos ayudó a crecer como profesionistas de la educación, haciendo que salieramos del confort y buscáramos opciones de acercamiento con los alumnos y, a pesar de que realmente aún hay brechas de accesibilidad y este tipo de acercamiento virtual solamente beneficia a un sector poblacional, podemos empezar a educar a esos alumnos como ciudadanos digitales y poco a poco ir rompiendo brechas para dar paso a asegurar el acceso a internet como el derecho básico universal que garantiza que todos seamos unos verdaderos ciudadanos digitales.

En México, se sigue trabajando para poder puntualizar sobre ellos y, al igual que la ciberseguridad, la ciudadanía digital es un tema que no se ha profundizado y no se ha tomado con la seriedad que debería, pues a pesar de que ya hay un avance en la implementación de estos términos, aún estamos en proceso de desarrollarlos y llevarlos a cabo de manera plena.

Brindar la importancia necesaria a este tema nos permitirá, junto a la ciberseguridad, formar personas críticas, que sepan realizar búsquedas seguras, capaces de analizar información y ser cautelosos ante las situaciones de riesgo en las que puedan encontrarse para saber cómo actuar ante ellas.

Es de suma importancia poder establecer lineamientos que nos permitan fomentar las buenas prácticas, que nos aseguren el acceso y sobre todo, poder contar con ellas dentro del ambiente escolar virtual.

2.5. La importancia de la ciberseguridad y la ciudadanía digital en la educación

En un mundo que vive conectado y prácticamente basa su vida en los dispositivos, es importante cuidar toda la información que se guarda o se comparte ya que se tiene el riesgo de sufrir ataques que lleven a la pérdida de datos o ser víctimas de fraudes y extorsiones.

Enfocando nuestro tema en los centros escolares, podemos decir que las escuelas guardan información sensible, como datos personales de familias, datos bancarios tanto de la misma escuela como de los padres de familia, información general de la escuela, así como toda la información que los alumnos van generando si se usan las plataformas educativas para impartir clases.

Justamente, por las condiciones actuales en donde nueva información y parte de nuestra vida la extendimos a un espacio tecnológico, que nos permite tenerla a la mano en cualquier lugar y convivir con más personas por todas las herramientas que se han desarrollado para poder estar conectados con terceros, es necesario hablar de cuáles son los riesgos, que se deben cuidar y qué se debe hacer dentro del mundo tecnológico, apoyar a los alumnos a desarrollar esa consciencia crítica y que sean ciudadanos ejemplares tanto en la vida presencial como en la online.

Es importante puntualizar que la ciberseguridad y la ciudadanía digital van de la mano, pues mientras una nos ayuda a protegernos y evitar ser víctimas de algún ciberataque, la otra nos va a decir cómo actuar dentro del mundo virtual, me va a formar como un ser crítico y así evitar que caiga en manos de los ciberdelincuentes; aquí podemos pensar ¿Y estos temas en qué ayudan o perjudican a la educación? La respuesta puede ser muy sencilla, pues en la educación constantemente se trabaja con información que llega a ser confidencial, que si bien no forma parte de un secreto de Estado, si es importante mantener una privacidad de todo, pues no sería agradable que la escuela sufriera un ataque cibernético y salieran a la luz las

respuestas de todos los exámenes, o que los datos bancarios de los padres de familia fueran robados.

Como vemos, estos temas pueden ser puntos que las soluciones sean sencillas y otros donde realmente no habrá solución y es ahí donde entra nuestra preocupación y es lo que queremos evitar.

Como adultos tenemos una conciencia más desarrollada que nos permite tener un sentido de prevención y cuando no conocemos algo, le tememos y tratamos de no “arruinarlo” y esto no nos excluye de ser víctimas de ataques cibernéticos.

Estamos seguros de que, si no sabemos buscaremos apoyo en los que sí saben, que son lo jóvenes y este es el punto al que quería llegar, pues como lo mencioné en el capítulo 1, los adolescentes pueden llegar a ser personas con poco criterio y que actúan de forma impulsiva, sin generalizar el comportamiento, pues habrá adolescentes que sean mucho más críticos y tratarán de evitar situaciones de peligro; en esta situación, nos acercamos a ellos y nada nos garantiza que ellos sepan más de lo que uno sabe, salvo nuestra creencia de que ellos son nativos digitales y por ende entienden mejor la tecnología.

Basándonos en la situación anterior, es que llegó mi motivación de hacer este trabajo, pues es necesario poder puntualizar con los alumnos la importancia de saber sobre ciberseguridad y ciudadanía digital, así mismo, tener en mente siempre que estos temas impactan de manera directa a la educación, que aunque es uno de los ámbitos que casi nadie toca a la hora de exponer los temas, sabemos que siempre es de los más afectados.

Como profesionalista de la educación, me preocupa que sigamos avanzando en temas tecnológicos, que sigamos innovando en la educación, que queramos meter nuevas herramientas de enseñanza – aprendizaje, pero que dejemos de lado los temas de ciberseguridad y ciudadanía digital, ya que nos van a llevar de la mano en dichos avances haciendo de nuestros desarrollos mejores planteamientos y con ello

lograremos acercar a México a la altura de los países más desarrollados en estos temas.

Es debido a esta preocupación que en el siguiente capítulo presentaré materiales de apoyo para que la información aquí presentada se encuentre al alcance de los alumnos y de la comunidad escolar en general.

3. Recomendaciones para que los alumnos de secundaria eviten ser víctimas de ciberataques

Para iniciar con este capítulo es importante brindar un poco del contexto y los motivos que me orillaron a decidir trabajar sobre el tema; y se debe a mi labor pedagógica dentro de Sistema UNOi, en donde me desempeño como Implementadora de Soluciones Educativas (Asesor digital), mis funciones principales son capacitar a los docentes que estarán encargados de configurar la plataforma educativa, es decir, les brindamos la información de todo el aspecto tecnológico para que puedan acoplarla a las necesidades de la escuela.

El hecho de que yo trabaje con docentes hace que sea evidente que en muchas escuelas les hace falta hablar sobre los temas de ciberseguridad y ciudadanía digital dentro de la comunidad escolar, pues al ser el área de capacitación tecnológica, también fungimos como soporte técnico y al recibir correos o llamadas solicitando ayuda porque algún alumno envió mensajes agresivos a otros compañeros o están acosando a una maestra, como pedagoga lo primero que me salta es la pregunta ¿Qué podemos hacer para evitar estas situaciones? Si bien, podemos recomendarle cuestiones técnicas en cuanto a configuración, también debemos abarcar el educar al usuario sobre la sana convivencia en el entorno digital.

Con lo anterior en mente, decidí que quería investigar más a fondo sobre la problemática, entender un poco más este tema y tratar de ayudar a las escuelas,

pero sin tener que aplicar un taller obligatorio, sino que sea más de poder proporcionarles la información puntualizada y lista para su uso, logrando que cada escuela tenga acceso a ella y la puedan aplicar dependiendo de las necesidades que se han detectado en la comunidad escolar, fue así como llegué a la conclusión de hacer material informativo.

Para empezar a diseñar este material debo tener en cuenta que los adolescentes pueden ser personas impulsivas, que no suelen revisar a detalle la información que reciben, pero también ya son nativos digitales, lo que los hace ser, hasta cierto nivel, expertos en el uso de las herramientas tecnológicas, pero esto no implica que estén exentos de caer en los peligros de la ciberdelincuencia, por lo que, elaboraré materiales a manera de recomendación para que los alumnos de secundaria eviten ser víctimas de ciberataques y que también cumplan con las normas de ser ciudadanos digitales.

Dicho material lo propongo para su difusión, ya que se quiere lograr que la información sea difundida de forma masiva y de alguna manera hacerla viral, como todos los videos, retos, juegos, etc. que actualmente están de moda, por lo que se recurrirá a las diferentes plataformas y redes sociales que usan los adolescentes, como Instagram. La propuesta será a través de infografías, juegos y retos que los ayuden a crear una consciencia en el uso de la tecnología, así como de la ciudadanía digital.

Es importante mencionar que estas recomendaciones no estarán solamente ligadas a la escuela, pues los adolescentes viven conectados a la tecnología tanto dentro como fuera de las aulas, por lo que, deben conocer las reglas y los peligros que esto conlleva. Empezar por concientizar a los alumnos sobre las buenas prácticas dentro del mundo digital, así como de los riesgos que conlleva, ayudará a formar personas mucho más capaces de tener una vida digital plena.

Este material estará creado para los alumnos, pero deberá ser aplicado por los docentes o el personal administrativo del Colegio, incluyendo a los padres de familia, pues nuestra población objetivo aún necesita la guía de alguien que les permita acercarse de forma responsable a la información.

Debemos comprender que ambos temas, ciberseguridad y ciudadanía digital, actualmente son de importancia para integrar en la vida escolar debido a las nuevas estrategias que se están aplicando para la impartición de clases, que si bien, no se espera que la virtualidad o las clases híbridas duren por siempre, si nos dejan una pauta para que sean opciones en casos necesarios, además de que, el internet ya se ha vuelto parte fundamental de la vida diaria y todos debemos aprender a usarlo de forma responsable.

3.1. Recomendaciones para la comunidad escolar

Las acciones que se deben tomar como comunidad escolar no dependen del todo de los alumnos, por lo que es importante que empecemos por un sector poblacional usuario, lo ideal sería tratar de vincular profesores, alumnos y personal administrativo sobre el uso de las herramientas tecnológicas y orientarlos en ciberseguridad y ciudadanía digital.

Si bien, estos 3 grupos están conformados por personas de diferentes rangos de edad, así como de diversos conocimientos en cuanto a la tecnología, dentro de la escuela todos hacen uso de ella y llega a ser responsabilidad del colegio capacitar a su personal en el uso de todo lo que se implementa, pero tomando en cuenta que actualmente las escuelas privadas están incluyendo el uso de tecnología en sus actividades diarias, es de suma importancia poder brindarles información que les ayude a no ser víctimas de la ciberdelincuencia y que los usuarios principales sepan utilizar de manera objetiva dichas herramientas.

Probablemente dentro de la escuela la información que se pretende difundir como recomendaciones a los alumnos, sea de gran apoyo también para los demás participantes de la comunidad escolar, logrando así, que poco a poco tanto los nativos digitales como los no nativos sean usuarios ejemplares y compartan sus conocimientos con otras personas.

De manera general, se recomienda difundir información sobre qué es la ciberseguridad y la ciudadanía digital, esto mediante infografías que pueden ser colocadas dentro de la escuela, en los murales de anuncios, así como ser enviadas de manera electrónica como correos o por medio de chats de alguna aplicación de mensajería instantánea.

Si el colegio cuenta con una plataforma educativa, puede colocarse dentro de la información de consulta, es decir, el poseer la información de manera física o virtual, nos permite que todos nuestros alumnos y personal de la escuela tengan acceso a ella, logrando que la conozcan y la entiendan.

Como mencioné anteriormente, un material que se puede utilizar y con el que se puede informar a todos los actores de la comunidad escolar son las infografías, las cuales no solamente se pueden usar de forma impresa, pues al contar con el archivo digital, se puede enviar por correo, mensajería instantánea o compartir por redes sociales de la escuela.

Por lo que diseñé estas opciones de infografía:

¿Malware?

Malware o "software malicioso" es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.
Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente.

¿CÓMO FUNCIONA?

DESCARGA O INSTALACIÓN INVOLUNTARIA

La mayoría de las infecciones se producen cuando realiza, sin saberlo, una acción que provoca la descarga del malware.



TIPOS COMUNES



- Ransomware: Bloquea el acceso a la información hasta que se pague un rescate
- Spyware: recaba información sobre un dispositivo o red
- Adware: Muestra publicidad sin parar
- Gusanos: infecta un equipo y después se replica a otros dispositivos.
- Troyano: Introduce Malware
- Botnets: Convierten los equipos en "zombies"

SINTOMAS

PUEDA MANIFESTARSE A TRAVÉS DE VARIOS COMPORTAMIENTOS

- El dispositivo empieza a funcionar más lento de lo normal.
- Nota que le falta espacio de almacenamiento
- En su dispositivo aparecen ventanas emergentes y programas no deseados



¿CÓMO ME PROTEJO?



El malware no solo supone una amenaza para los PC, Mac y dispositivos móviles también pueden ser su objetivo. La mejor protección contra el malware es un potente programa antivirus de un proveedor de confianza.



FUENTES:

<https://www.avast.com/es-es/c-malware>
<https://es.malwarebytes.com/malware/>

Diseño propio elaborado con información de Avast y Alwarebytes obtenida de:
<https://www.avast.com/es-es/c-malware> y <https://es.malwarebytes.com/malware/>

PROTÉGETE DE LOS VIRUS



Muchos tipos de virus y malware en general pueden afectar al buen funcionamiento de nuestros dispositivos y comprometer nuestra privacidad.

1

Mantener los sistemas actualizados

2

Usar herramientas de seguridad

3

Cuidado con los enlaces que visitamos

4

Descargar solo de fuentes fiables

5

Controlar lo que compartimos y a quienes aceptamos en redes sociales



Estos son algunos consejos básicos que podemos aplicar para proteger nuestra seguridad frente al malware.

Diseño propio con información obtenida de Alwarebytes: <https://es.malwarebytes.com/malware/>

5 actitudes de un buen ciudadano digital



Toma medidas de seguridad
Hace uso de antivirus y contraseñas

Respeta la diversidad de opiniones
Comprende que toda opinión importa y no promueve las agresiones



Se informa de manera responsable
Antes de compartir información, la verifica

Cumple las normas de comportamiento
Sabe que tanto los sitios web como las redes que utiliza tienen normas y leyes



Lee los términos y condiciones
Cada que ingresa datos personales en un sitio web, sabe qué alcances tendrán con su información

Diseño propio con información obtenida del Ministerio de Educación de Chile:
<https://formacionciudadana.mineduc.cl/wp-content/uploads/sites/46/2019/06/CiudadaniaDigital-Cuadernillo.pdf>

También realicé una infografía sobre el uso de iPads dentro del aula, pues algunas escuelas privadas cuentan con estos dispositivos, sobre todo en las que tienen alguna plataforma educativa que incluya equipamiento digital, les brindan estos equipos como herramientas de trabajo y son parte del inventario, por lo que se recomienda tener reglas de uso como las siguientes:

Cuidado del iPad

Aquí podrás encontrar información que te ayudará con el cuidado de tu dispositivo

1



Mantenlo siempre actualizado

Si te pide alguna actualización de Software, instálala, si tienes dudas, recuerda que puedes acudir con el encargado de sistemas

2

No cambies el Apple ID

Recuerda que el dispositivo es propiedad del Colegio, por lo que debes evitar poner cuentas personales



3



No descargues aplicaciones sin autorización

Evita descargar aplicaciones que no sean educativas, esto evitará que se llene la memoria del dispositivo



Recuerda que el iPad es parte de tu equipo de trabajo, cuidarlo es responsabilidad de todos

Si tienes dudas o necesitas apoyo con el uso del dispositivo, no dudes en acercarte al encargado de sistemas

Si tu dispositivo no funciona

Es muy importante que lo lleves con el encargado de sistemas y cuentes lo que sucedió, entre más detalles proporciones será más fácil poder ayudarte.

Elaboración propia

3.1.1. Recomendaciones para alumnos

Para dar inicio a este apartado es importante dejar en claro que todas las escuelas deben hablar sobre los diversos riesgos que existen en internet, que si bien es un tema que probablemente tenga fastidiados a los adolescentes, jamás está de más tener la información fresca y así evitar ser víctimas, además, se pueden incluir temas de ciudadanía digital, el cual no está tan explotado por los centros educativos.

Pensando en lo anterior, una actividad que diseñé para brindar recomendaciones para los alumnos y aplicarlas tanto dentro de las actividades escolares como en la vida diaria, consta de una plantilla, en la cual los alumnos deberán ir marcando lo que han realizado dentro de internet:



Checklist

Ciberseguridad

Marca todas las acciones que realizas en internet

<input type="checkbox"/>	Mis contraseñas no se repiten	<input type="checkbox"/>	Tengo al menos 2 cuentas de correo	<input type="checkbox"/>	Hago respaldos en la nube
<input type="checkbox"/>	Comparto archivos con diferentes permisos en la nube.	<input type="checkbox"/>	Cierro las sesiones en los dispositivos que no uso	<input type="checkbox"/>	Tengo activa la verificación de 2 pasos en mis cuentas
<input type="checkbox"/>	Agrego personas que no conozco a mis redes sociales	<input type="checkbox"/>	Abro enlaces sin verificar	<input type="checkbox"/>	Reenvío ofertas o concursos sin verificar
<input type="checkbox"/>	Me conecto a redes públicas	<input type="checkbox"/>	Uso mi tarjeta digital para hacer compras en línea	<input type="checkbox"/>	Verifico que las páginas tengan HTTPS
<input type="checkbox"/>	Mis dispositivos tienen instalado antivirus	<input type="checkbox"/>	Mantengo mis dispositivos actualizados	<input type="checkbox"/>	Sé distinguir las Fakenews
<input type="checkbox"/>	Acepto las cookies de todos los sitios	<input type="checkbox"/>	Tengo instalado un bloqueador de anuncios en mi navegador	<input type="checkbox"/>	Todas mis redes sociales son públicas
<input type="checkbox"/>	Sé administrar las redes de mi modem	<input type="checkbox"/>	Comparto mi ubicación en tiempo real en mis redes sociales	<input type="checkbox"/>	Comparto información delicada en mis redes sociales
<input type="checkbox"/>	Tengo fotos íntimas en mi celular	<input type="checkbox"/>	He compartido fotos íntimas	<input type="checkbox"/>	Veó películas desde páginas ilegales

De acuerdo a mis resultados... ¿Qué tan riesgosa es mi actividad en internet?

Elaboración propia

Una vez realizada, tenemos la oportunidad de hacer una discusión sobre los riesgos que cada alumno ve en su actuar diario en internet, sin necesidad de mostrar a los demás compañeros cuáles son las actividades que realizan, pues debemos estar conscientes que estos alumnos se encuentran en la adolescencia y están formando su autoestima, por lo que, no debemos exponerlos a situaciones bochornosas o que les causen algún tipo de incomodidad.

Este ejercicio es más bien de autorreflexión, pero guiado por un docente que ayude a entender por qué ciertas actividades ponen en riesgo la seguridad de los alumnos. Esta plantilla también la pueden compartir los docentes con los alumnos para que, si los alumnos lo desean, la compartan en las historias de Instagram y se haga un tipo reto del famoso juego “Yo nunca, nunca”.

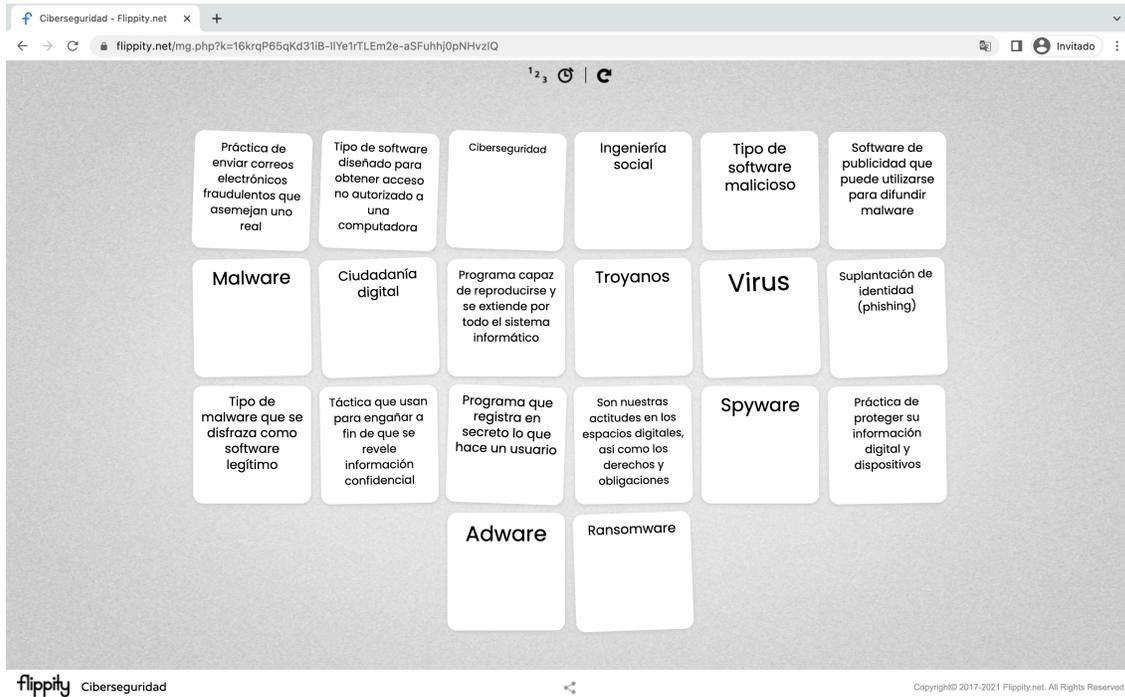
Pensando en actividades que realicen dentro de la escuela apoyados por un docente, realicé 2 juegos con ayuda de la plataforma Flippity, la cual permite que, mediante plantillas, se creen diversos juegos que se llevan a cabo en línea.

La primera actividad guiada es sobre emparejamiento de cartas y lo que deben hacer los alumnos es seguir estos pasos:

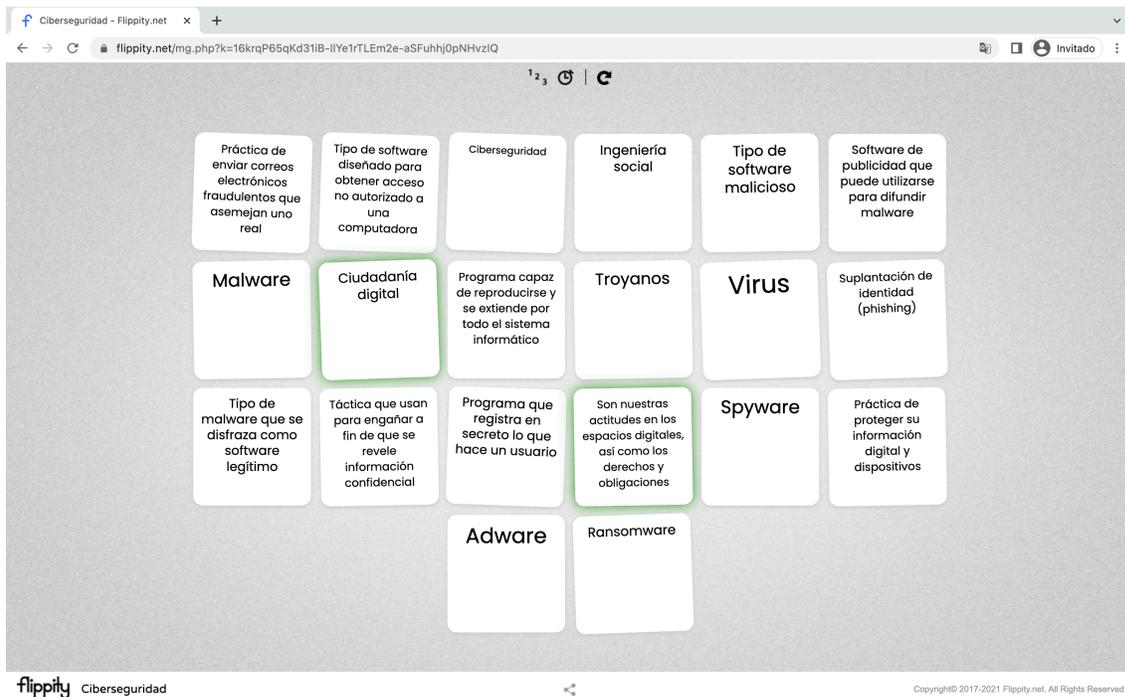
1. Ingresar al enlace

<https://www.flippity.net/mg.php?k=16krqP65qKd31iB-IIYe1rTLEm2e-aSFuhhj0pNHvzIQ>

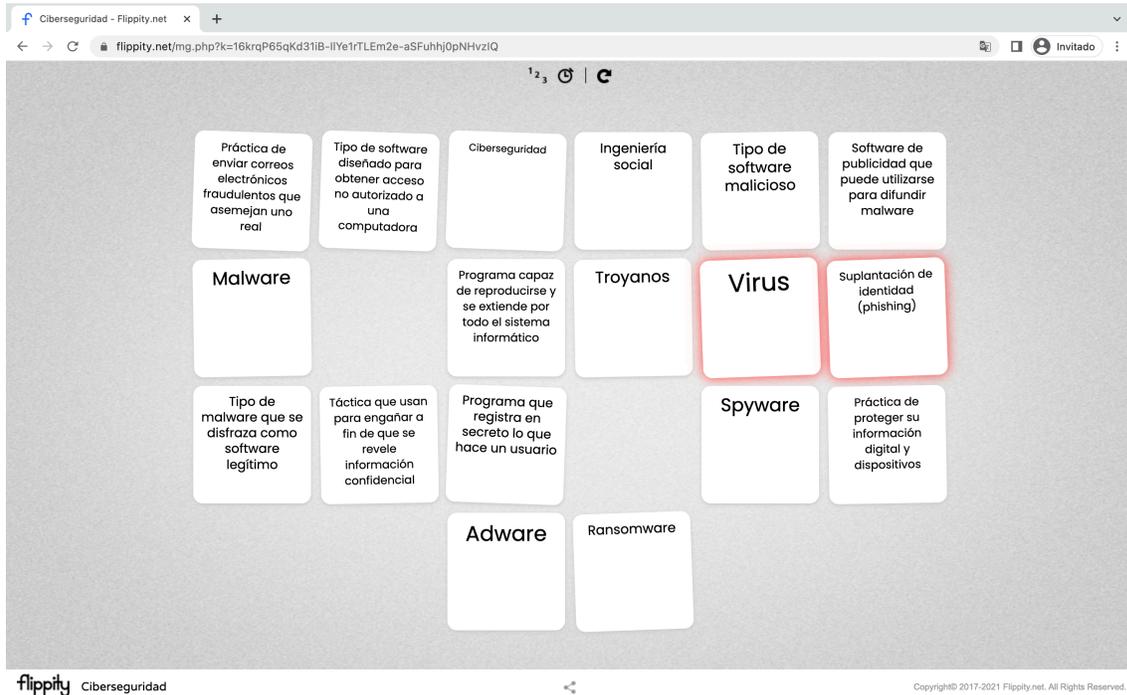
2. Una vez dentro del sitio, se mostrarán varias tarjetas con frases o palabras:



3. Deben seleccionar 2 tarjetas para formar la pareja de concepto y definición.
Si la selección es correcta, se pondrá el contorno en color verde



4. En caso de que las tarjetas no coincidan, se marcará el contorno en color rojo.



Cabe mencionar que, para lograr este ejercicio, es necesario que los alumnos hayan leído las infografías mostradas anteriormente, así como haber tenido pláticas sobre los temas con sus profesores.

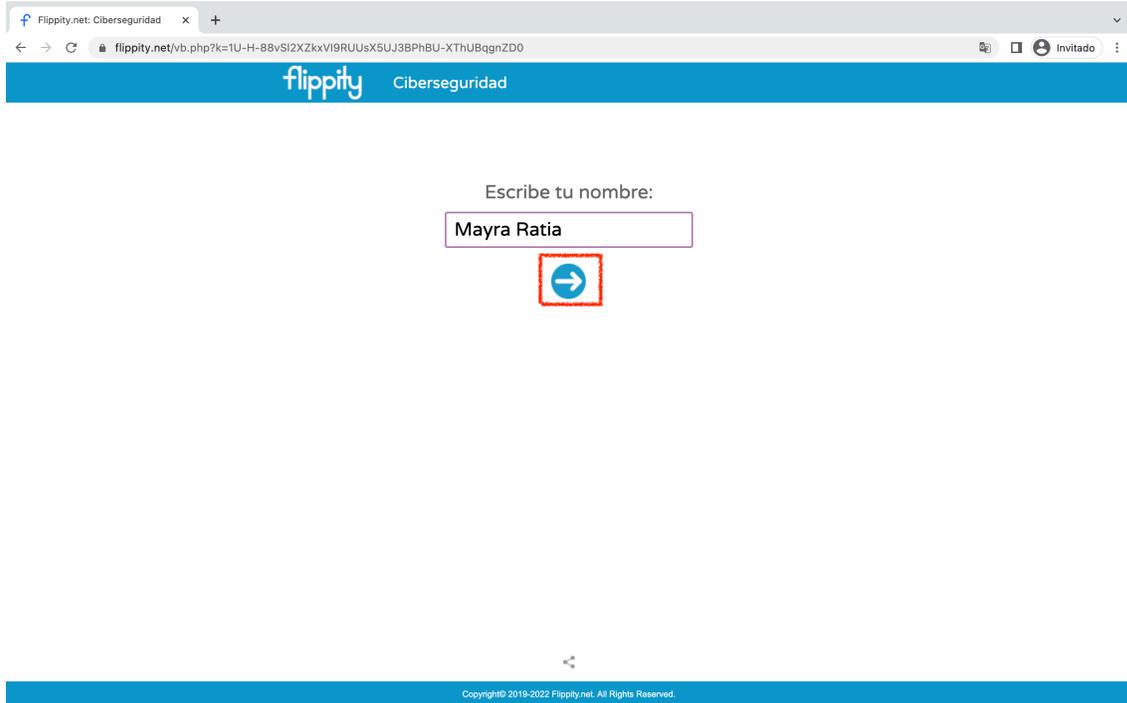
La segunda actividad que diseñé con la misma plataforma tiene la opción de que al finalizar envía las respuestas al correo del profesor. La actividad consta de 8 preguntas, en las cuales al responder de forma correcta vas desbloqueando la siguiente, son preguntas sobre ciberseguridad y resolución de casos.

Las instrucciones son las siguientes:

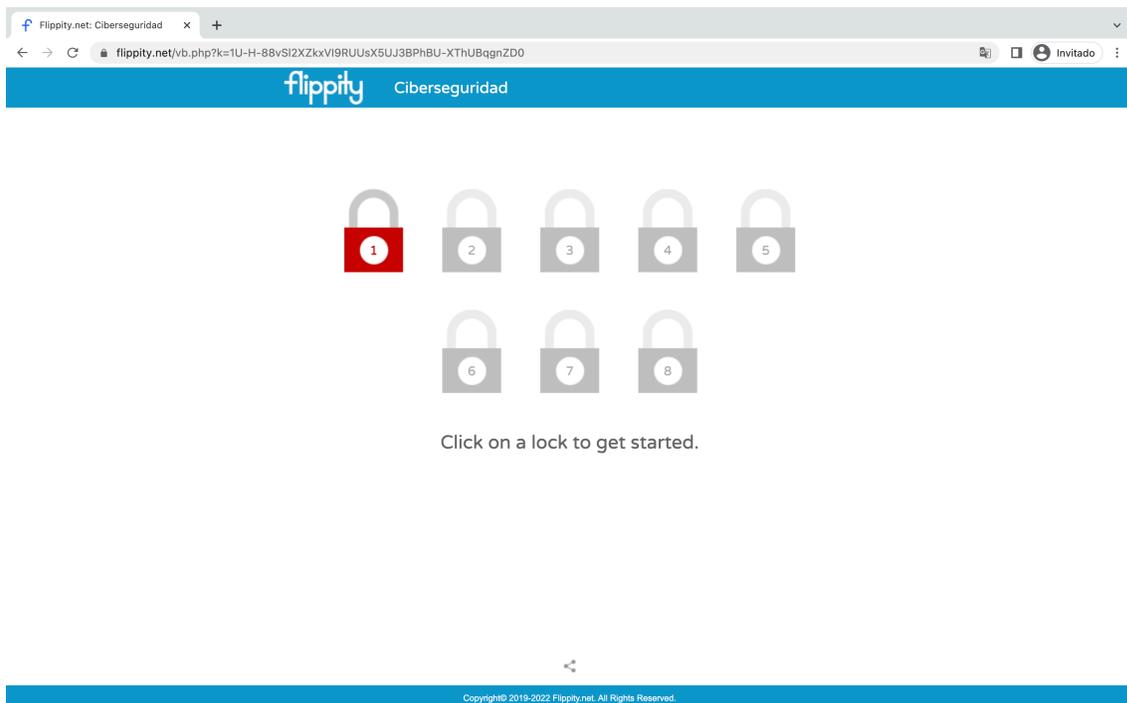
1. Para ingresar, deben visitar el siguiente enlace:

<https://www.flippity.net/vb.php?k=1U-H-88vSI2XZkxVI9RUUsX5UJ3BPhBU-XThUBqgnZD0>

- Una vez que se encuentren dentro del sitio, les pedirá que ingresen su nombre y dar clic en la flecha azul debajo del espacio para el nombre.



- Deberán seleccionar el primer candado, dando clic sobre él para abrir la pregunta que al responder de forma correcta les desbloqueará la siguiente.



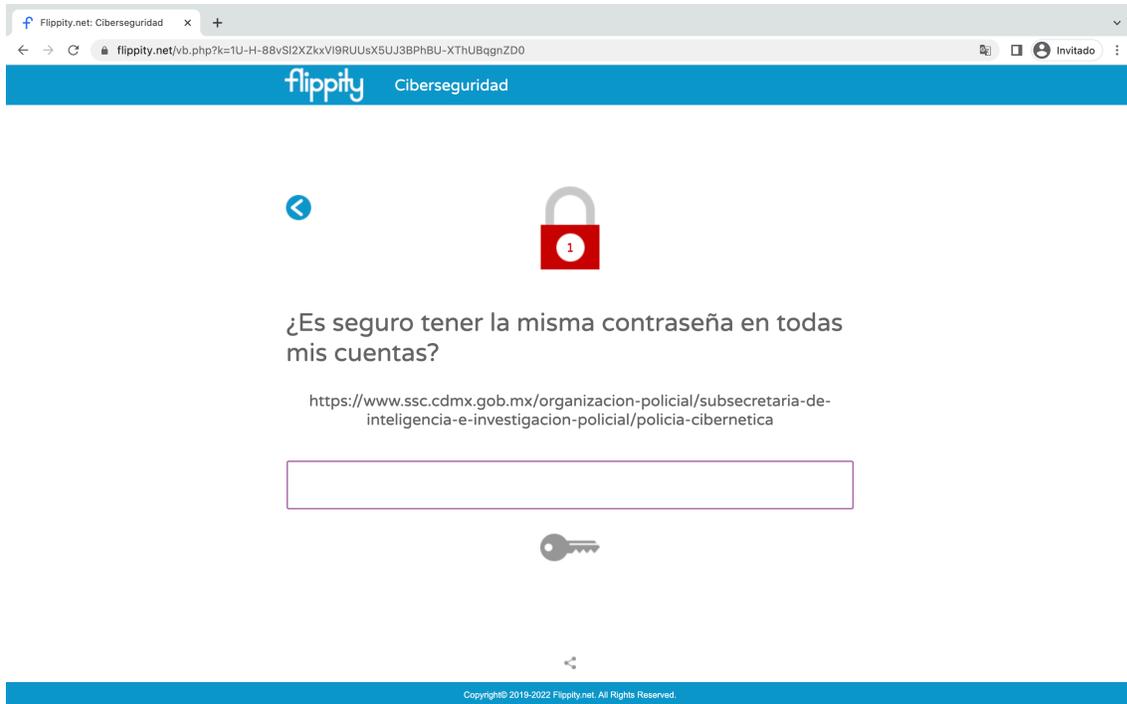
4. Dentro de las preguntas, pueden encontrar la opción de pista, la cual se activa dando clic en el foco.



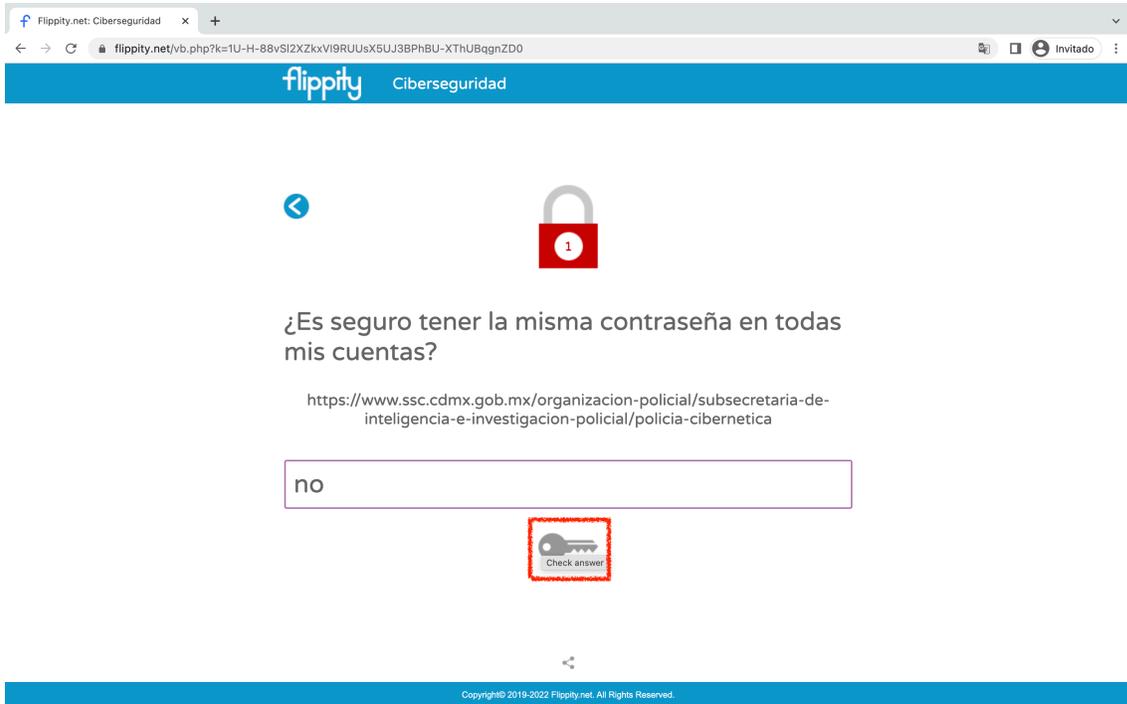
5. Saldrá un mensaje en una ventana flotante y solo deben dar clic en aceptar



6. Les mostrará la pista, la cual consta de un enlace a un sitio donde podrán localizar la respuesta, solo deben copiar el texto y pegarlo en una pestaña del navegador



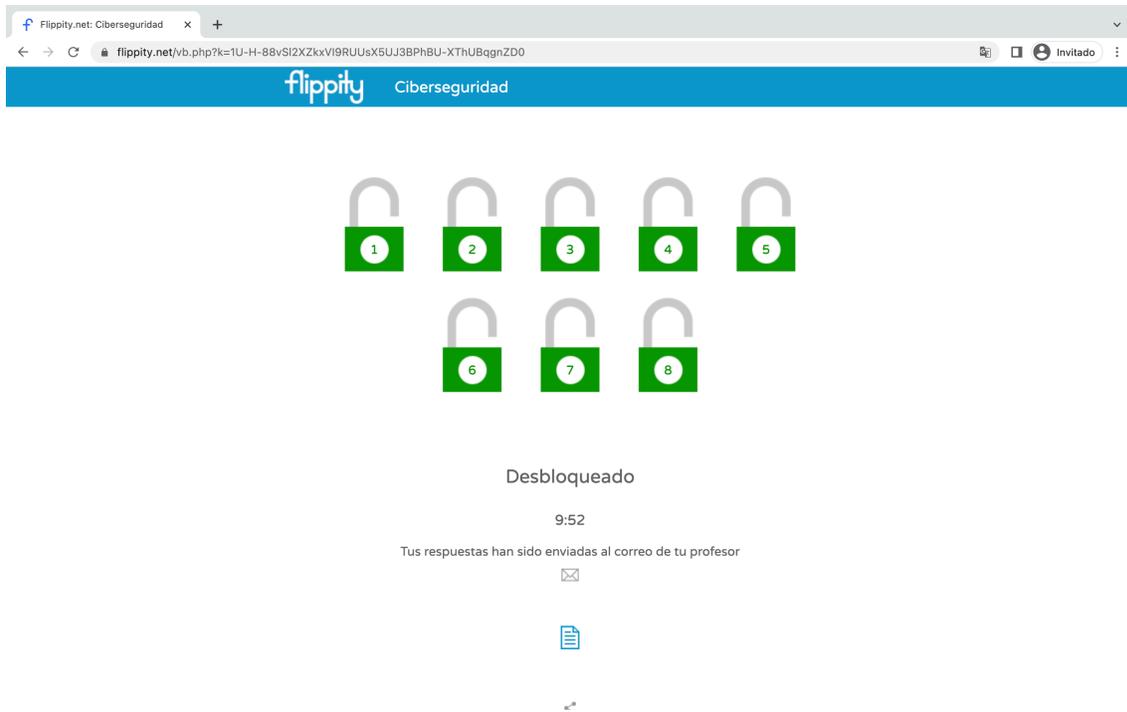
7. Una vez que tengan la respuesta deben escribirla y dar clic en la llave debajo del espacio de respuesta. Deben tener cuidado con la ortografía y la redacción



8. Si la respuesta es correcta, el candado se pondrá de color verde y se mostrará abierto. Posteriormente, deben dar clic en la flecha debajo de la respuesta para regresar al panel principal



9. Si la respuesta es incorrecta, la actividad emitirá un sonido de bloqueo y deben revisar que todo esté escrito de forma correcta o bien, revisar la respuesta.
10. Al finalizar la actividad, todos los candados estarán de color verde, se visualizará el tiempo que tardaron en responder y mostrará un aviso de que las respuestas fueron enviadas al correo del profesor.



Es importante comprender que las actividades escolares de los alumnos no solo se quedan en las aulas, pues fuera de ellas se siguen realizando ciertas actividades complementarias como las tareas.

Sin embargo, también es cierto que al estar fuera ya no existe la seguridad que la institución les puede brindar sobre la tecnología, por lo que debemos puntualizar que al salir de la escuela cambia completamente la rutina de los alumnos, el apoyo que pueden tener por parte de los profesores y sobre todo la vigilancia.

Mientras en la escuela las redes y los equipos pueden estar administrados para que no permitan conectarse a ciertos sitios o que los dispositivos personales no

detecten las señales de WiFi, en casa, prácticamente todo es de acceso libre y a menos de que tengan a papá y/o mamá a un lado, o con conocimientos de sistemas, los adolescentes tienen un mundo de información disponible y a su alcance, pueden buscar “n” cantidad de información y hacer infinidad de cosas, por lo que, este es el lugar donde los adolescentes deben poner en práctica los conocimientos adquiridos sobre ciberseguridad y ciudadanía digital que se les brindó como recomendación en la escuela.

3.1.2. Recomendaciones para docentes y personal administrativo

Como lo mencioné al inicio del capítulo, dentro de la comunidad escolar no solamente los alumnos son los que están en riesgo de ser víctimas de ataques cibernéticos y tampoco son completamente responsables de las acciones que se deben tomar para evitar ser el blanco de la delincuencia, por lo que en este apartado estableceré algunas recomendaciones para que el cuerpo docente y administrativo pueda tomar en cuenta y así crear una comunidad escolar mucho más segura.

Para empezar, trabajaremos con el personal de sistemas, que, si bien no es una figura recurrente en las escuelas, debería ser indispensable, pues es el experto en estos temas, por lo que podemos decir que ésta sería una primera recomendación, tener al menos una persona encargada de sistemas.

La segunda recomendación va encaminada al uso de las cuentas institucionales, es decir las cuentas de correo, accesos a plataformas, etc.

Por lo que, pensando en que cada mes las escuelas deben hacer una reunión de consejo técnico, es el lugar perfecto para que puedan abarcar estos temas y poder hacer actividades que ayuden a los docentes y personal administrativo a entender el por qué deben estar involucrados.

Por esto, es que decidí crear una actividad de retos que pueden cumplir todos los docentes y personal administrativo:

PROTEGER LA SEGURIDAD

Es todo el conjunto de técnicas y acciones que se implementan para controlar y mantener la privacidad de la información y datos de una institución; y asegurarnos que esa información no salga del sistema de la escuela y caigan en las manos equivocadas.

Objetivo: Fomentar una ciudadanía digital mediante retos que ayuden al cuidado de nuestra seguridad en internet.

Instrucciones: Deberán cumplir los 5 retos de seguridad en un máximo de 30 días. Puede acudir con el departamento de sistemas en caso de dudas.

RETO 1

Cambia tu contraseña del correo institucional.

No uses la misma que tienes en otro lugar

Usa al menos 8 caracteres, incluye letras, números y caracteres especiales

RETO 2

Mantén actualizados tus equipos

No postergues las actualizaciones, actualízala al primer aviso

RETO 3

Usa la nube del Colegio

Guarda algunos de los archivos más importantes en la nube que te proporciona el Colegio

Trabaja desde la nube tus archivos

RETO 4

No abras correos dudosos

Si recibes correos con ligas extrañas, no los abras

No compartas spam dentro del Colegio.

RETO 5

Elimina el rastreo de cookies

Descarga un bloqueador de cookies y anuncios

Cambia tu navegador a Brave o safari

Elaboración propia

Como recomendaciones para desarrollar la ciudadanía digital entre el cuerpo docente y el personal administrativo, decidí que pueden enfocarse en las buenas

prácticas con el equipo o herramientas digitales de apoyo para las clases, por lo que, al enfocarnos en escuelas privadas, muchas de ellas cuentan con instalación de las llamadas aulas digitales, que incluyen al menos un proyector y un dispositivo como iPad o Tablet, por lo que diseñé una infografía que pueden colocar en los salones.

Cuidados del equipo digital del aula

Aquí encontrarás información sobre qué sí y que no debes hacer cuando usas el equipo digital de las aulas (proyector y iPad)

SÍ HACER

Encender y apagar el proyector con el botón desde el mismo dispositivo o con el control

Espera a que encienda el proyector, no desesperes

Si el proyector no da imagen, selecciona el botón source search, si no funciona llama a sistemas

Bloquear tu iPad cuando no esté en uso

NO HACER

Cerrar la tapa del proyector sin apagarlo antes, así evitarás fundir la lámpara

Presionar el botón de encendido varias veces, deja que el proyector termine el proceso de encendido

No jales los cables o los muebles de manera brusca, así evitarás que se dañen

Dejarla sin bloquear, a parte de que es riesgoso para tu seguridad, gasta batería

¿Dudas?

Acercarte all área de sistemas del Colegio, es la persona indicada para ayudarte a resolverlas.

Elaboración propia

Dos recomendaciones que pueden llevar a cabo siempre y cuando el cuerpo directivo lo decida es la gestión de contraseñas y el filtrado web, las cuales les ayudará a que puedan tener contraseñas variadas para todas las cuentas institucionales, que sean seguras y que se les reporte en caso de que hayan sido vulneradas y que, dentro de la red de la escuela, no se visiten sitios de riesgo, respectivamente.

Por lo que, para dar a conocer la información sobre cada una de las recomendaciones, creé 2 infografías con las que los directores junto a su responsable de sistemas puedan decidir cuál de todas las ofertas del mercado les beneficia.

Existe un programa que te permite guardar contraseñas para utilizarlas siempre que quieras pudiendo cumplir así con el consejo de que en cada servicio tengas una contraseña diferente.

GESTORES DE CONTRASEÑAS

Es un programa diseñado para almacenar credenciales de acceso en una bóveda cifrada.

Almacenamiento

Además de almacenar tus contraseñas, también te enseñan a cuidarlas y gestionarlas.

Seguridad

Algunos gestores pueden incluir un sistema para crear contraseñas fuertes, así como alertas que te avisan cuándo tienes contraseñas débiles o excesivamente repetidas en varios servicios

Análisis

Otros de los servicios que pueden incluir algunos de estos gestores son los análisis periódicos de tus correos en la Dark Web para ver si se ha filtrado alguna de tu contraseñas.

Prevención

Recuerda que los datos se almacenan en un servidor, pero los datos están cifrados, es decir, no están a la mano de las personas que intenten robar dicha información

Referencias

<https://www.youtube.com/watch?v=xHSnHj-zKF4>
<https://www.xataka.com/basics/gestores-contrasenas-que-cuales-populares-como-utilizarlos>

Diseño propio con información obtenida de <https://www.youtube.com/watch?v=xHSnHj-zKF4> y <https://www.xataka.com/basics/gestores-contrasenas-que-cuales-populares-como-utilizarlos>

Filtrado Web



Es un software diseñado para restringir los sitios web que un usuario puede visitar en su equipo.



Estos filtros pueden funcionar con una whitelist o una blacklist: las whitelists solo permiten el acceso a sitios elegidos específicamente por quien configura el filtro; las blacklists restringen el acceso a sitios no deseados según lo determinado por las normas instaladas en el filtro.

Prevención

se utilizan a menudo como herramienta para la prevención de malware



¡Ojo!

Existen diferentes formas de evitar el software de filtrado web, por lo que los administradores de redes deben asegurarse de que el filtro ofrezca otras funciones además de bloquear o permitir ciertos sitios web.

Bonus

Los filtros más avanzados pueden incluso bloquear la información que se envía por Internet para evitar que se divulguen datos confidenciales.

Fuentes:

<https://latam.kaspersky.com/resource-center/definitions/web-filter>

Como podemos ver, para llevar a cabo reglas de ciberseguridad e implementar la ciudadanía digital, necesitamos de toda la comunidad escolar y, aunque en este caso nuestra población objetivo son los alumnos de secundaria, debemos dejar en claro que sin el apoyo de los docentes, los padres de familia, los directivos y personal administrativo, ellos por sí mismos se enfrentan a diferentes retos y bloqueos por el hecho de ser menores de edad y porque a veces la información no es tan clara o simplemente no se les ha proporcionado.

Es importante que le demos el peso necesario a estos temas, que como hemos ido revisando en el transcurso del trabajo, son importantes debido a los avances tecnológicos y que el día de mañana podamos evitar muchos incidentes que dejen en vulnerabilidad tanto a los alumnos como a la escuela en general.

La idea de hacer solamente recomendaciones, se basa en el contexto escolar, ya que, aunque hablamos de escuelas privadas, no todas son iguales y de esta forma, las escuelas pueden ajustar la información de acuerdo a las necesidades que tengan.

Como pedagogos no somos expertos en muchos temas, pero es la gran maravilla del área, pues podemos trabajar junto a otras profesiones como los ingenieros en sistemas, psicólogos y programadores, para poder aterrizar esos temas importantes, que muchas veces están en términos muy técnicos, logrando así, que la población en general tenga acceso a esa información, ya que recordemos, el conocimiento es poder.

Considero que estos son los puntos más relevantes para que los adolescentes cuenten con el acceso a la información dentro de las escuelas y que éstas como institución puedan tomar las decisiones más acertadas ante sus necesidades, pues a pesar de que las actividades presenciales se están retomando, no debemos retroceder los avances que, forzosamente, se realizaron en la educación, es mejor

mantenerlos y mejorarlos para que podamos seguir avanzando en temas de innovación educativa.

Conclusiones

Los temas de ciberseguridad y ciudadanía digital van de la mano, por lo que, al hablar de la ciudadanía digital, nos permite educar a los usuarios digitales sobre los temas de ciberseguridad y cómo sentar las bases para evitar estar expuestos a los riesgos que por desgracia, nos dejan vulnerables tanto a nivel personal, así como a nivel institucional.

Como pudimos ver en nuestros capítulos, los adolescentes, que a pesar de ser nativos digitales y por ende entender la tecnología mucho más que un adulto, por su naturaleza psico social, a veces no le permite visualizar por completo los riesgos que conlleva el hecho de llevar una vida dentro del internet, compartir fotos, información y muchos más datos en las redes sociales; hasta el recibir un correo puede poner en riesgo su seguridad.

Hablar de estos riesgos es parte importante de entablar desde la educación formal, es decir, desde las escuelas y es aquí donde puntualizamos y englobamos el tema central de este trabajo, pues como se mencionó, debido a la COVID 19, muchas escuelas se vieron en la necesidad de cambiar las aulas presenciales por aulas virtuales, cada alumno y cada profesor desde su casa conectados por medio de un dispositivo, ya sea celular o computadora y con ayuda de alguna herramienta de videoconferencia.

Todo eso nos dejó ver que, aunque por los avances tecnológicos hayamos ido adaptandonos al uso cotidiano de diferentes dispositivos y herramientas tecnológicas, jamás nos habíamos sentido tan expuestos como en estos años de

pandemia, pues permitimos que nuestros compañeros conocieran un espacio de nuestra casa.

En otros casos, las escuelas les brindaron a los alumnos usuarios y contraseñas para usar plataformas educativas en donde podrían ver los materiales de clase, así como las tareas asignadas y en estos casos, fue donde no solo como individuos podría haber vulnerabilidad, sino también como institución, pues si en la escuela no seguían ciertas recomendaciones de seguridad, por ejemplo en contraseñas, éstas podrían ser descifradas y por ende expuestas para que cualquier persona pudiera ingresar a las plataformas y consultar cualquier información tanto de la escuela en general como de los alumnos.

Con esto en mente, es que se llegó a la conclusión de que era un tema relevante y que afecta a la educación de manera directa, pues al trabajar en una empresa que se dedica a temas de educación mediante plataformas escolares y enfocarme en el área técnica, pude ver cómo es que día a día se presentaban infinidad de incidencias referentes a la vulnerabilidad de la seguridad y fue cuando decidí que como pedagoga, además de poder brindar los conocimientos mediante la capacitación sobre el uso de dicha plataforma, también podía hacer algo más poniendo a su disposición información que les ayudara a entender la importancia de conocer sobre la ciberseguridad.

Ahora bien, es importante mencionar que así como cada persona es un mundo, también cada escuela lo es, por lo que, el hecho de que no diseñara un taller va enfocado a esta cuestión y es que, cada escuela es diferente en la cuestión de la infraestructura tecnológica, pues podemos encontrar desde la que está completamente equipada y sabe mucho sobre el tema de ciberseguridad y por ende los alumnos cuentan con mucha seguridad dentro de las aulas virtuales y las plataformas educativas, como el colegio que apenas se acercó a estas plataformas y no entiende por completo de lo que se habla y cómo es que debería manejar los temas de seguridad para todos en el uso de la tecnología.

Considero que aún nos falta mucho más por recorrer en estos temas de forma general, pues al buscar información de lo que hace México para poner sobre la mesa estos temas y que se adapten a diferentes ámbitos, se encontró que sí se está llevando a cabo, pero no en el ámbito educativo y es lo que deja tan vulnerable a la educación en estos tiempos de pandemia.

Debemos empezar a enfocarnos más en las necesidades educativas y si yo como profesionista de la educación puedo poner un granito de arena, aunque parezca poco, sé que será un parteaguas para las próximas generaciones y poco a poco se lograrán más cosas.

Anexos

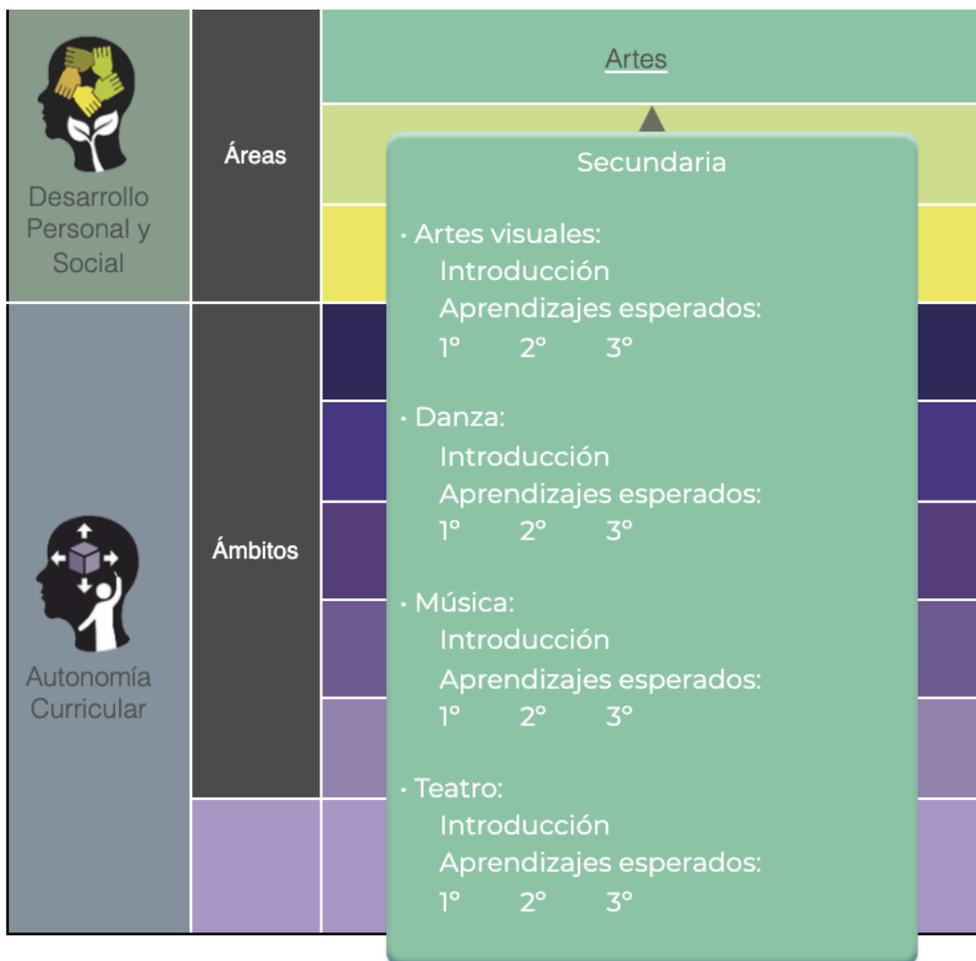
Gráfico 1

Componente curricular		Nivel educativo		
		Secundaria		
		Grado escolar		
		1°	2°	3°
 Formación Académica	Campos y Asignaturas	Lengua Materna (Español)		
		Lengua Extranjera (Inglés)		
		Matemáticas		
		Ciencias		
		Biología	Física	Química
		Historia		
		Geografía		
		Formación Cívica y Ética		
		Tecnología		
 Desarrollo Personal y Social	Áreas	Artes		
		Tutoría y Educación Socioemocional		
		Educación Física		
 Autonomía Curricular	Ámbitos	Ampliar la formación académica		
		Potenciar el desarrollo personal y social		
		Nuevos contenidos relevantes		
		Conocimientos regionales		
		Proyectos de impacto social		
		Profundización		

Tomado del portal de la SEP. Mapa Curricular

<https://www.planprogramasdestudio.sep.gob.mx/index-mapa-curricular2019.html#>

Gráfico 2



Tomado del portal de la SEP. Mapa Curricular

<https://www.planyprogramasdestudio.sep.gob.mx/index-mapa-curricular2019.html#>

ESTADIO	A Estadios y modos psicosexuales	B Crisis psicosociales Sintónica y distónica	C Relaciones sociales significativas	D Fuerzas básicas Virtudes y fuerzas sincrónicas	E Patologías básicas Antipatía y fuerza distónica	F Principios relacionados de orden social	G Ritualizaciones vinculantes - Integrantes (Institución)	H Ritualizaciones Desvinculantes- Desintegrantes (Sistemas Sociales)
I - INFANTE (1 año)	SENSORIO MOTOR - ORAL - RESPIRATORIO	CONFIANZA VS. DESCONFIANZA BÁSICA	PERSONA MA- TERNA Diada	ESPERANZA "Yo soy la esperanza de tener y dar."	DESCONFIANZA Retraimiento	ORDEN CÓSMICO Universo (Religión)	TRASCENDENTE (Religión - Iglesia)	IDOLATRÍA
II - INFANCIA (2 a 3 años)	MUSCULAR - ANAL ENTRENAMIEN- TO HIGIÉNICO	AUTONOMÍA VS. VERGÜENZA Y DUDA	PADRES	VOLUNTAD "Yo soy lo que puedo querer libremente."	VERGÜENZA Y DUDA	LEY Y ORDEN (Legal)	JUDICIALES Ley y consciencia (Judiciario)	LEGALISMO
III - PREES- COLAR EDAD DEL JUEGO (3 a 5 años)	INFANTIL Genital - loco- motor. Aprendi- zaje sexual	INICIATIVA VS. CULPA Y MIE- DOS	FAMILIA BÁSICA Triada	PROPÓSITO "Yo soy lo que puedo imaginar que seré."	SENTIMIENTO DE CULPA Y MIEDOS Inhibición	PROTOTIPOS IDEALES (Artes)	DRAMÁTICAS Artes, teatro, cine, Mitología (Artes dramáticas)	MORALISMO
IV - EDAD ESCOLAR (6 a 12 años)	LATENCIA	LABORIOSIDAD VS. INFERIORI- DAD	VECINDARIO Y ESCUELA	COMPETENCIA "Yo soy lo que puedo aprender para realizar en el trabajo."	INFERIORIDAD Inercia	ORDEN TECNOLÓGICO (Tecnología)	FORMALES Técnicas (Tecnología)	FORMALISMO
V - ADO- LESCENCIA (12 a 20 años)	PUBERTAD	IDENTIDAD VS. CONFUSIÓN DE IDENTIDAD	GRUPO DE IGUALES Y otros grupos Modelo de liderazgo	FIDELIDAD - FE "Yo soy lo que puedo creer fielmente":	CONFUSIÓN DE IDENTIDAD Postergar valo- res. Moratoria psicosocial	VISIÓN DEL MUNDO IDEOLOGÍA (Cosmovisión)	IDEOLÓGICAS (Orden ideológico)	TOTALITARISMO (Fanatismo)
VI - ADULTO JOVEN (20 a 30 años)	GENITALIDAD	INTIMIDAD VS. AISLAMIENTO	COMPAÑEROS de amor y traba- jo. Competencia Cooperación	AMOR "Nosotros somos lo que amamos"	AISLAMIENTO Exclusividad Narcisismo	PATRONES DE COOPERACIÓN Sentido Ético (Asociaciones)	ASOCIATIVAS Solidariedad (Asociaciones abiertas el cerradas)	ELITISMO Clase
VII - ADULTO (30 a 50 años)	PRODUCTIVI- DAD	GENERATIVIDAD VS. ESTANCA- MIENTO	TRABAJO DIVI- DIDO Familia y hogar compartidos	CUIDADO - CELO: Caridad "Yo soy lo que cuido y celo"	ESTANCA- MIENTO Rechazo	CORRIENTES DE EDUCACIÓN Y TRADICIÓN (Asociaciones)	GENERACIO- NALES Productividad y Creatividad (Familia)	AUTORITARISMO (Poder degenerado)
VIII - VIEJO (Después de los 50 años)	GENERALIZA- CIÓN de los modos sensuales	INTEGRIDAD VS. DESESPERANZA	GÉNERO HUMA- NO "Mi género"	SABIDURÍA "Yo soy lo que sobrevive en mí."	DESESPERA- NZA Desdén	SABIDURÍA (Síntesis existencial)	FILOSÓFICAS (Teorías Filosóficas)	DOGMATISMO (Ritualismo)

Tomado de Redalyc. El desarrollo psicosocial de Eric Erikson. El diagrama epigenético del adulto

<https://www.redalyc.org/pdf/695/69520210.pdf>

Fuentes consultadas

Avast. *¿Qué es el malware?* Consultado el 28 de marzo de 2022. Disponible en: <https://www.avast.com/es-es/c-malware>

Boeree, C. George. 12 marzo del 2019. *Teorías de Personalidad en Psicología: Erik Erikson*. Consultado el 5 de febrero del 2022. Disponible en: <https://www.psicologia-online.com/teorias-de-personalidad-en-psicologia-erik-erikson-683.html>

Bordignon, Nelso Antonio. *El desarrollo psicosocial de Eric Erikson. El diagrama epigenético del adulto*. Revista Lasallista de Investigación 2, no. 2 (2005):50-63. Redalyc. Consultado el 5 de febrero del 2022. Disponible en: <https://www.redalyc.org/pdf/695/69520210.pdf>

CISCO. *¿Qué es la ciberseguridad?* Consultado el 27 de enero del 2022. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Clínica Universidad de Navarra, *Desarrollo psicosocial*. Consultado el 27 de enero del 2022. Disponible en: <https://www.cun.es/diccionario-medico/terminos/desarrollo-psicosocial>

CNN en español. *Nativos digitales ¿quiénes son y qué significa?* Consultado el 5 de febrero del 2022. Disponible en: <https://cnnespanol.cnn.com/2013/01/25/nativos-digitales-quienes-son-y-que-significa/>

Constitución Política de los Estados Unidos Mexicanos. Consultado el 2 de febrero del 2022. Disponible en: <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>

Cruz Valencia, Galvy Ilvey. "ciberseguridad para la educación online." *Universidad Nacional Autónoma de México. Revista Seguridad*. No. 22. Consultado el 15 de marzo del 2022. Disponible en: <https://revista.seguridad.unam.mx/numero22/ciber-seguridad-para-la-educacion-online>

Delgado, Paulette. 22 Septiembre del 2020. "¿Somos o no ciudadanos digitales? La realidad de la conectividad en la pandemia," *Instituto para el Futuro de la Educación. Observatorio*. Tecnológico de Monterrey. Consultado el 20 de marzo del 2022. Disponible en: <https://observatorio.tec.mx/edu-news/ciudadania-digital-pandemia>

EDUIMPULSA. *La teoría sociocultural de L. Vigotsky*. Consultado el 5 de febrero de 2022. Disponible en: <https://eduimpulsa.com/la-teoria-sociocultural-de-vigotsky/>

Fondo de las Naciones Unidas para la Infancia. Gobierno de la Provincia de Buenos Aires. 2020. *Guía de sensibilización sobre convivencia digital*. Consultado el 22 de febrero del 2022. Disponible en: <https://www.unicef.org/argentina/media/9481/file/Gu%C3%ADa%20sobre%20Convivencia%20Digital-2020.pdf>

Fondo de las Naciones Unidas para la Infancia. Uruguay. *¿Qué es la adolescencia?* Consultado el 5 de febrero del 2022. Disponible en: <https://www.unicef.org/uruguay/que-es-la-adolescencia>

Gobierno de la Ciudad de México. Agencia Digital de Innovación Pública. *Presentación del Plan de Ciudadanía Digital*. Consultado el 14 de marzo de 2022 Disponible en: <https://adip.cdmx.gob.mx/comunicacion/nota/presentacion-del-plan-de-ciudadania-digital>

Gobierno de la Ciudad de México. Secretaría de Seguridad Ciudadana. *Policía Cibernética*. Consultado el 10 de marzo del 2022. Disponible en: <https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica>

Gobierno de México. *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares*. Consultado el 5 de febrero del 2022. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/647466/ENDUTIH_2020_co.pdf

Gobierno de México. *Estrategía Nacional de Ciberseguridad*. Consultado el 15 de marzo del 2022. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Gobierno de México. Procuraduría Federal del Consumidor. *Escuelas particulares, lo que debes saber*. Consultado el 2 de febrero del 2022. Disponible en: <https://www.gob.mx/profeco/es/articulos/escuelas-particulares-lo-que-debes-saber?idiom=es>

Gobierno de México. Secretaría de Educación Pública. *Mapa Curricular*. Consultado el 3 de febrero del 2022. Disponible en: <https://www.planyprogramasdestudio.sep.gob.mx/index-mapa-curricular2019.html>

Gobierno de México. Secretaría de Marina. *Estrategia Institucional de Ciberespacio*. Consultado el 11 de marzo del 2022. Disponible en: <https://www.gob.mx/semar/documentos/unidad-de-ciberseguridad-278750?state=published>

Google. 2022. “Ayuda de cuenta de Google.” Consultado el 18 de abril del 2022. Disponible en: <https://support.google.com/accounts/answer/32040?hl=es-419#zippy=>

Instituto Nacional Electoral. *Ciudadanía y Participación*. Consultado el 18 de marzo del 2022. Disponible en: <https://farodemocratico.juridicas.unam.mx/que-es-ser-ciudadano-y-que-es-ser-ciudadana/>

Instituto Nacional para la Evaluación de la Educación. *La educación obligatoria en México, informe 2019*. Consultado el 25 de enero del 2022. Disponible en: [https://www.inee.edu.mx/medios/informe2019/stage_01/cap_0102.html#:~:text=2%20Los%20grupos%20poblacionales%20que,17%20a%C3%B1os%20\(media%20superior\).](https://www.inee.edu.mx/medios/informe2019/stage_01/cap_0102.html#:~:text=2%20Los%20grupos%20poblacionales%20que,17%20a%C3%B1os%20(media%20superior).)

Instituto Nacional para la Evaluación de la Educación. *Principales cifras. Educación básica y media superior. Inicio del ciclo escolar 2017-2018*. Consultado el 25 de enero del 2022. Disponible en: <https://www.inee.edu.mx/wp-content/uploads/2019/08/P2M111.pdf>

“Jóvenes, el sector con más acceso a internet y tecnología.” 2021. *Reporte Índigo*. 23 de junio. Consultado el 5 de febrero del 2022. Disponible en: <https://www.reporteindigo.com/indigonomics/jovenes-el-sector-con-mas-acceso-a-internet-y-tecnologia/>

Kaspersky. *¿Qué es la ciberseguridad?* Consultado el 27 de enero del 2022. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

Malwarebytes. *Malware*. Consultado el 28 de marzo del 2022. Disponible en: <https://es.malwarebytes.com/malware/>

Microsoft Corporation. “¿Qué es la ciberseguridad?” Consultado el 15 de marzo del 2022. Disponible en: <https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390>

Ministerio de Educación. Gobierno de Chile. *Ciudadanía digital*. Consultado el 16 de marzo del 2022. Disponible en: <https://formacionciudadana.mineduc.cl/wp-content/uploads/sites/46/2019/06/CiudadaniaDigital-Cuadernillo.pdf>

Organización de Estados Americanos. *Programa de ciberseguridad*. Consultado el 15 de marzo del 2022. Disponible en: <https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp>

Prensky, Mark. *Nativos e Inmigrantes Digitales*. Consultado el 5 de febrero del 2022. Disponible en: [https://marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20\(SEK\).pdf](https://marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20(SEK).pdf)

Riquelme, Rodrigo. 2021. “Las estrategias nacionales de ciberseguridad deben tener un enfoque civil: MITRE.” *El economista*, 21 de septiembre. Consultado el: 15 de marzo del 2022. Disponible en: <https://www.eleconomista.com.mx/tecnologia/Las-estrategias-nacionales-de-ciberseguridad-deben-tener-un-enfoque-civil-MITRE-20210921-0088.html>

Santaella, Julio (@SantaellaJulio), “#ENDUTIH2020 la penetración del internet supera el 90% de la población para el rango entre 12 y 24 años de edad...” Twitter. 22 junio del 2021, https://twitter.com/SantaellaJulio/status/1407424267910844421?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1407424267910844421%7Ctwgr%5E%7Ctwcon%5Es1&ref_url=https%3A%2F%2Fwww.reporteindigo.com%2Fin digonomics%2Fjovenes-el-sector-con-mas-acceso-a-internet-y-tecnologia%2F

Secretaría de Educación Pública. *ACUERDO número 255, por el que se establecen los trámites y procedimientos relacionados con la autorización para impartir educación secundaria*. Consultado el 10 febrero del 2022. Disponible en: <http://sep.gob.mx/work/models/sep1/Resource/fe27ab92-1e15-4cc0-b36b-1eb2af344f06/a255.pdf>

Secretaría de Educación Pública. *Ley Organica De Educación*. Consultado el 2 de febrero del 2022 Disponible en: https://www.sep.gob.mx/work/models/sep1/Resource/3f9a47cc-efd9-4724-83e4-0bb4884af388/ley_03021940.pdf

Secretaría de Educación Pública. Dirección General de Planeación, Programación y Estadística Educativa. *Estadística Educativa México. Ciclo Escolar 2020 – 2021*. Consultado el 25 de enero del 2022. Disponible en: http://planeacion.sep.gob.mx/Doc/estadistica_e_indicadores/estadistica_e_indicadores_entidad_federativa/estadistica_e_indicadores_educativos_15MEX.pdf

Stanford Children´s Health. *Desarrollo congntivo en la adolescencia*. Consultado el 28 de enero del 2022. Disponible en: <https://www.stanfordchildrens.org/es/topic/default?id=desarrollocognitivo-90-P04694>

Torres Septién, Valentina. *Algunos Aspectos De Las Escuelas Particulares En El Siglo XX*. Historia Mexicana. 1984. 33p. Consultado el 28 de enero del 2022. Disponible en: <https://historiamexicana.colmex.mx/index.php/RHM/article/view/2588/2099>

Zamora Saenz, Itzkuauhtli. *Una aproximación a la ciudadanía digital en México: acceso, habilidades y participación política*. Cuaderno de investigación No. 72, Instituto Belisario Domínguez, Senado de la República, Ciudad de México, 2020, 27p. Consultado el 16 de marzo del 2022. Disponible en:

[http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5094/CI_72.pdf?
sequence=1&isAllowed=y](http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5094/CI_72.pdf?sequence=1&isAllowed=y)