Universidad Nacional Autónoma de México
Facultad de Filosofía y Letras
Colegio de Pedagogía

Propuesta pedagógica de alfabetización digital: MOOC dirigido a docentes de primaria para fomentar la Ciberseguridad dentro del aula

Tesina
que para obtener el título de
Licenciada en Pedagogía

P r e s e n t a
Marisol Sixto Marcos

Asesora
Dra. Itzel Casillas Avalos

Ciudad Universitaria, CDMX, 2023

Dedicatoria

A mi abuelita Ricarda y a mis abuelitos Pablo y Jacinto con mucho amor hasta el cielo.

Agradecimientos

A Dios por darme vida, salud y la oportunidad de reencontrarme con Él.

A mi papá y a mi mamá por su amor, consejos y todo el esfuerzo que han realizado a lo largo de estos años para que cada uno de nosotros, sus hijas e hijos, tuviéramos las herramientas suficientes para luchar por nuestras metas.

A mis hermanas y hermanos por el cariño, el apoyo, las risas, los chistes de mal gusto, las desveladas, los enojos y demás situaciones que nos ha tocado vivir, porque, aunque no lo crean, he aprendido mucho de ustedes.

A la Dra. Itzel Casillas por su apoyo, comprensión, paciencia y tiempo para construir el presente trabajo. Mi respeto y admiración total a su persona y a su labor como pedagoga y docente.

A mis sinodales, Angélica Silva, Miriam Carrillo, Miguel Ángel Pérez y Alejandro Román por el tiempo invertido para leer y enriquecer este trabajo con sus valiosas aportaciones.

A mis amigas, Arianna, Monse y Dany, porque a pesar de los años y las circunstancias siempre han estado ahí apoyándome. Gracias por su amistad incondicional.

A mis amigas de la universidad, Lore, Andy, Itzel, Gaby, Nath e Itzel, por cada uno de los momentos compartidos y por ser un gran pilar en mi vida.

Al Plan de becas TIC para la educación de la DGTIC por enriquecer mi formación profesional y porque en ese espacio logré forjar nuevas amistades y grandes colegas de la pedagogía (Lid, Trini, Day, Vivi y Fati).

Finalmente, a todas las personas que de manera directa o indirecta han contribuido en mi crecimiento personal y profesional.

Índice

Introducción

La ciberseguridad, el tema que motivó el presente trabajo, es de mi interés debido a que en algún momento fui víctima de *malware* dentro de Facebook y he conocido casos cercanos de amistades a quienes han amenazado con difundir fotos íntimas, a quienes les han suplantado su identidad o a quienes han sido víctimas de estafas en páginas de compra, por mencionar algunos.

A dichas experiencias se aunaron los conocimientos que adquirí en el marco del Taller de educación no formal 9, asignatura de la Licenciatura en Pedagogía, en el que se abordó el tema de alfabetización digital y en el cual pude vislumbrar un camino para afrontar y mitigar algunos de los problemas que se gestan dentro del entorno digital, específicamente de los referidos a la ciberseguridad.

Con el fin de tener un panorama general de la problemática, a continuación, se presenta una síntesis de las problemáticas y directrices a abordar en materia de ciberseguridad tomando como base dos estudios realizados en el país: *Hábitos de los usuarios en ciberseguridad México 2019* y el *17° Estudio sobre ciberseguridad en empresas, usuarios de Internet y padres de familia en México 2021*:

- Dispositivos.
- Uso de redes públicas.
- Instalación de aplicaciones.
- Privacidad en redes sociales.
- Robo de identidad.
- Acceso a contenido inapropiado (violencia, retos en línea, pornografía, drogas, armas, material racista, discriminatorio o de odio etc.).
- Contacto y comunicación arriesgada, en el que la persona es contactada por un desconocido y/o una persona mayor con fines de hostigamiento, seducción y/o abuso sexual (grooming, corrupción de menores, pornografía infantil, trata de personas, turismo sexual infantil, secuestro, etc.) o que intentan persuadirlos para participar en conductas poco saludables o peligrosas.

- Actividades en las que el individuo contribuye a que se produzca o reproduzca un contenido inapropiado o un contacto riesgoso (*cyberbullying*, *sexting*, sextorsión, etc.).
- Fraudes financieros.
- Poca o nula orientación (Información de los peligros en Internet, desconocimiento de las autoridades competentes en México en materia de ciberseguridad y desconocimiento sobre los sistemas de control parental).

Si bien todos estamos expuestos a algún riesgo dentro del ciberespacio, múltiples investigaciones coinciden en que son niñas y niños, los más vulnerables:

> el 52% de las niñas y los niños entre ocho y doce años, están expuestos a algún riesgo en Internet (*grooming*, *sextorsión*, *sexting*), el 41% han sido víctimas de ciberbullying, el 9% ha tenido interacción con desconocidos y el 18% se ha involucrado en algún tipo de comportamiento sexual (Park, 2019).

Tomando como base lo antes mencionado, arguyo que es necesario contribuir y "continuar con los esfuerzos para fomentar las capacidades digitales de los ciudadanos de forma integral, en donde se inculque el uso seguro y responsable de la tecnología" (SCT, 2019, p. 23), sobre todo en lo que refiere a la población infantil, ya que este sector accede a edades cada vez más tempranas y pueden no entender de manera automática su vulnerabilidad ante los riesgos en línea, de ahí la necesidad de iniciar su formación en competencias digitales desde edades tempranas.

En este contexto, nace la presente propuesta de alfabetización digital que tiene como objetivo diseñar un Curso Masivo Abierto en Línea (MOOC) para docentes de primaria alta en el que se ofrezcan orientaciones didácticas para que se promueva la ciberseguridad dentro del aula, de tal manera que los estudiantes puedan desarrollar las competencias necesarias para prevenir y hacer frente a los riesgos y amenazas que pudiesen encontrar al navegar dentro del ciberespacio.

Se retoma la alfabetización digital dentro de la propuesta, ya que dos medidas recomendadas por el Fondo de las Naciones Unidas para la Infancia (UNICEF) en materia educativa para proteger a niñas, niños y adolescentes de los peligros del mundo digital son:

- Enseñar alfabetización digital en las escuelas. Dado que los niños se conectan en línea a edades cada vez más tempranas, las escuelas, especialmente las públicas, deben incorporar programas de alfabetización digital.
- Apoyar la capacitación y alfabetización digital de los maestros. Los docentes deben ser capaces de desarrollar sus propias [competencias] para apoyar el uso de las TIC por parte de sus alumnos y ayudarlos a desarrollar una comprensión del uso seguro de Internet más allá del aula. (UNICEF, 2017, pp. 32-33).

El MOOC Ciberseguridad: prevención de riesgos desde el aula, tiene como uno de sus fines abonar a dichas medidas, ya que se plantea en un primer momento que las y los docentes identifiquen los riesgos más comunes a que se pueden enfrentar sus estudiantes al navegar en el ciberespacio, y en segundo lugar que conozcan algunas orientaciones didácticas que les permitan integrar y promover la ciberseguridad dentro de sus aulas.

A continuación, se describen los capítulos que integran la presente tesina:

En el capítulo 1 se hace una contextualización de los aspectos conceptuales y legales ligados a la ciberseguridad. En la primera parte del capítulo se presenta la definición y los componentes de la ciberseguridad, en la segunda parte se describen los principales riesgos a que están expuestas niñas y niños en su interacción con el ciberespacio; y finalmente, se abordan las acciones que se desarrollan a nivel nacional, regional e internacional para fomentar la ciberseguridad.

En el capítulo 2 se describen los elementos teóricos y conceptuales que dan sustento a la propuesta. Para comenzar, se aborda qué es la alfabetización digital, qué son las competencias digitales y cuál es su relación con la ciberseguridad; en segundo lugar, se plantea a grandes rasgos qué es la capacitación docente y cuál es su relación con la alfabetización digital y el desarrollo de competencias digitales; finalmente, se describen aspectos relevantes en torno a los MOOC y el por qué se proponen como medio para la capacitación docente.

En el capítulo 3, se desarrolla la propuesta del MOOC Ciberseguridad: prevención de riesgos desde el aula a través de un guion instruccional con tres apartados. En el primer apartado, se detallan los datos generales del curso (nombre, duración, objetivo general, programa del curso, metodología de trabajo y criterios de evaluación); en el segundo apartado se presentan

los elementos generales del módulo (nombre, objetivo particular y temario del módulo); y finalmente, se describen se describen con detalle los contenidos de cada tema, los recursos a utilizar, actividades y material extra para reforzar lo aprendido.

Capítulo 1. Ciberseguridad: una perspectiva teórica

En este primer capítulo, se presenta la definición y los componentes de la ciberseguridad, se describen los principales riesgos a que están expuestas niñas y niños en su interacción con el ciberespacio; y finalmente, se abordan las acciones que se desarrollan a nivel nacional, regional e internacional para fomentar la ciberseguridad.

1.1 Definición de ciberseguridad

Desde sus inicios Internet ha revolucionado el mundo, de tal manera que ahora es imposible imaginarse un mundo sin la red de redes, pues su uso se ha extendido e impregnado casi todos los ámbitos de la vida diaria.

La revolución que ha traído consigo Internet se encuentra vinculada con el surgimiento de una dimensión denominada ciberespacio (Machín, 2016). En términos generales, el ciberespacio refiere al lugar en el que se sitúan las cosas que suceden en la red, y de manera más específica, "es un entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet con el apoyo de dispositivos físicos (hardware), tecnologías de la información y la comunicación (TIC) y redes distribuidas mundialmente" (INN, 2015, p.7).

Los elementos mencionados en la definición posibilitan el procesamiento, almacenamiento y transmisión de datos e información; facilitan y aumentan la comunicación entre los individuos; y permiten la interacción entre las personas y la información a través de la infraestructura disponible (Machín, 2016). Dichas interacciones han desarrollado un escenario ideal para que organizaciones del sector público y privado potencien sus actividades dentro del mundo digital en ámbitos diversos, como la comunicación, el trabajo, la educación, la economía, la salud, el transporte, el ocio, la agilización de trámites entre gobierno y ciudadanos, entre otras.

Son innumerables los ejemplos que se podrían citar de los beneficios y oportunidades que la tecnología ofrece, sin embargo, también es necesario hablar y ser conscientes de los problemas relacionados con la seguridad que ha traído consigo, ya que, así como los usuarios y las organizaciones públicas y privadas desarrollan e incrementan su actividad digital también lo han hecho los delincuentes y organizaciones criminales, quienes han encontrado en el ciberespacio un lugar de bajo costo y riesgo mínimo para cometer actos delictivos que varían según su nivel y objetivo.

Para hacer frente a la diversidad de riesgos que suceden dentro del ciberespacio, surge y se desarrolla la ciberseguridad, la cual, de acuerdo con la Unión Internacional de Telecomunicaciones (UIT) se define, como:

> conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de la infraestructura conectada pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos; estos activos incluyen los dispositivos informáticos conectados, los usuarios, la infraestructura, las aplicaciones, los servicios, los sistemas de telecomunicaciones y los datos en el mundo cibernético (2018, p.13).

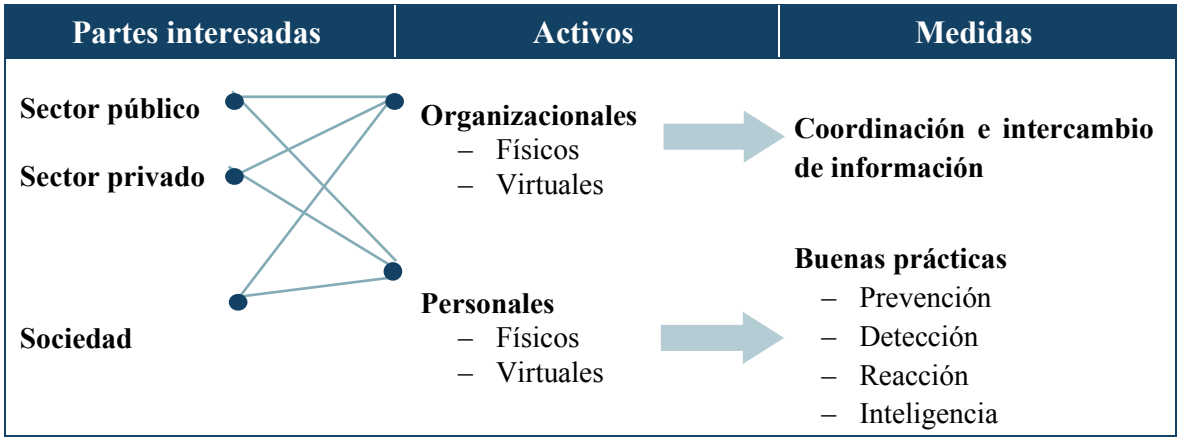
La razón por la cual se seleccionó esta definición es porque en ella es posible identificar los elementos clave que conforman y dan vida a la ciberseguridad: partes interesadas, activos y acciones para la gestión de riesgos y amenazas en el ciberespacio.

1.2 Componentes de la ciberseguridad

En la Figura 1, se presenta un esquema con los componentes de la ciberseguridad y sus interrelaciones, los cuales se describen con detalle en los siguientes subtemas.

Figura 1

Componentes de la ciberseguridad



Nota. Elaboración propia. Fuentes: INN. (2015). *ISO 27032* y COMEXI y McKinsey & Company. (2018). *Perspectiva de ciberseguridad en México.*

1.2.1 Partes interesadas

En el estándar 27032 sobre ciberseguridad de la Organización Internacional de Normalización (ISO),[1] se encuentran dos definiciones que aportan elementos relevantes para entender qué es una parte interesada y cuál es su relevancia para el tema que se desarrolla en el presente trabajo.

Desde la visión de sistema se define a las partes interesadas como un "individuo u organización que [tiene] un derecho, porción, reclamación o interés en un sistema […]" (INN, 2015, p.8), mientras que, desde la gestión de riesgos se les define como "individuo u organización que puede afectar o verse afectado por una decisión o actividad" (INN, 2015, p.8).

Tomando como base ambas definiciones, se tiene que el ciberespacio es un sistema que resulta de la interacción de múltiples elementos,[2] entre los que se encuentran las partes interesadas que son las personas u organizaciones que participan dentro de él y que tienen intereses diversos según el rol o los roles que desempeñan, ya sea como usuarios generales de aplicaciones, compradores, vendedores, desarrolladores de contenido, miembros de una organización u otros; y que al interactuar dentro del ciberespacio pueden verse afectados por las decisiones y actividades que dentro de él se gestan, incluyendo los riesgos y amenazas a que son susceptibles.

Las partes interesadas de acuerdo con el Consejo Mexicano de Asuntos Internacionales (COMEXI) se dividen en tres sectores: público, privado y sociedad. Dicha clasificación resulta relevante para los fines que competen a mi trabajo, ya que me centraré en los temas referentes al sector sociedad, debido a que los usuarios individuales suelen considerarse la parte más débil del ecosistema al no disponer de los conocimientos y recursos técnicos que tienen las organizaciones públicas y privadas para afrontar los retos del ciberespacio (Fundación Telefónica, 2016, p.10).

Si bien todos los usuarios individuales se consideran débiles en cuanto a las competencias para afrontar los retos del ciberespacio, múltiples investigaciones coinciden en que son niñas,

[1] Organización cuya principal actividad es la elaboración de normas técnicas internacionales que contribuyen a que el desarrollo, la producción y el suministro de bienes y servicios sean más eficaces, seguros y transparentes.
[2] Personas, softwares y servicios en Internet, dispositivos físicos (hardware), tecnologías de la información y la comunicación (TIC) y redes distribuidas mundialmente.

niños y adolescentes los sectores de la población más vulnerables, entre ellas, el Reporte de Impacto Global DQ 2019 en el que se estima que:

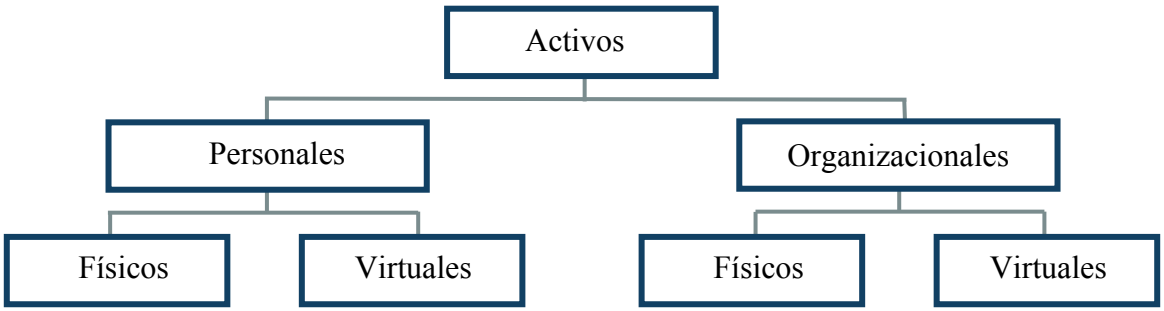
> el 52% de las niñas y los niños entre ocho y doce años, están expuestos a algún riesgo en Internet (*grooming*, *sextorsión*, *sexting*), el 41% han sido víctimas de *ciberbullying*, el 9% ha tenido interacción con desconocidos y el 18% se ha involucrado en algún tipo de comportamiento sexual (Park, 2019).

1.2.2 Activos en el ciberespacio

Un activo se define como "cualquier cosa que tenga valor para un individuo u organización" (INN, 2015, p.18). Los activos, como se menciona en la definición pueden pertenecer o ser de valor para un individuo u organización, de manera que se clasifican en dos grandes grupos: activos personales y activos organizacionales, los cuales, se subdividen a su vez en físicos[3] y virtuales[4], como se muestra en la Figura 2.

Figura 2

Clasificación de los activos



Nota. Fuente: Elaboración propia INN. (2015). ISO 27032 (p.19).

Tanto los activos físicos como los virtuales son de suma relevancia y resulta fundamental no minimizarlos por su naturaleza de estar o no visibles en el mundo real, ya que ambos son susceptibles de riesgos y amenazas que pueden afectar gravemente a los individuos, a su información, a su patrimonio, a su reputación e incluso a su dignidad, tanto en la vida en línea como fuera de ella.

[3] Existen en el mundo real (dispositivos digitales, personas, etc.).

[4] Solo existen en el ciberespacio y no se pueden ver o tocar en el mundo real (identidad digital, información crediticia en línea, monedas virtuales, software, etc.).

De acuerdo con el estándar 27032 sobre ciberseguridad de la ISO (2015, p.19), existen muchos activos, entre los que se encuentran:

- Datos e información
- Software (Programas y aplicaciones)
- Hardware (Dispositivos digitales)
- Servicios (Internet, aplicaciones, etc.)
- Personas
- Activos intangibles (identidad en línea, imagen, reputación, etc.)

A continuación, se describen los riesgos más frecuentes que pueden afectar a los activos de los usuarios dentro del ciberespacio, refiriéndose principalmente a aquellos que pueden afectar a niñas, niños y adolescentes.

1.2.2.1 Riesgos para los dispositivos

Uno de los riesgos más frecuentes que pueden afectar a los dispositivos de los usuarios a nivel de software y hardware son los programas maliciosos (*malware),* los cuales refieren a la "variedad de programas dañinos para los ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles (*adware*[5], *spyware*[6], virus[7], gusanos[8], troyanos[9], *ransomware*[10], *rootkit*[11], *cryptojacking*[12], *exploits*[13], etc.) que son utilizados para robar, cifrar o borrar datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad sin el conocimiento o consentimiento del propietario del equipo" (Malwarebytes, s/f).

Algunas de las acciones que pueden promover que los dispositivos se infecten de programas maliciosos son:

[5] Muestra publicidad en las computadoras, redirige las solicitudes de búsqueda a sitios web de publicidad y recopila datos comerciales sobre el usuario (Universidad Veracruzana, 2015).
[6] Accede a los datos de una computadora y los envía a otros dispositivos sin que el usuario lo advierta (Kaspersky, s/f).
[7] Altera el funcionamiento normal de cualquier dispositivo (GFC Global, s/f).
[8] Se propaga a través de varios dispositivos mientras permanece activo en todos ellos (Avast, 2016).
[9] Espía a las víctimas o roba datos (Avast, 2021).
[10] Restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esa restricción (Malwarebytes, s/f).
[11] Permite a un usuario no autorizado obtener el control de un sistema informático sin ser detectado (Avast, 2021).
[12] Usa de manera subrepticia la potencia de los ordenadores para generar criptomonedas (Interpol, s/f).
[13] Cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware (Avast, 2020).

- Descargar programas gratuitos de Internet.
- Dar clic en mensajes de supuestos premios, errores falsos o en ventanas emergentes.
- No actualizar los programas instalados en los dispositivos digitales.
- Visitar sitios web infectados.
- Conectarse a redes públicas que tengan como fin esparcir programas maliciosos.
- Abrir archivos adjuntos de un correo electrónico.
- No utilizar programas antivirus.
- Utilizar contraseñas débiles.

Entre las afecciones que pueden generar los programas maliciosos a los activos de los usuarios, se encuentran:

- Filtración o robo de datos personales.
- Disminución gradual de la velocidad del ordenador o dispositivos móviles.
- Envío de mensajes o correos electrónicos sin el conocimiento del propietario.
- Robo de dinero, recursos de computación u algún otro objetivo[14].

Como vimos en este apartado, existen varias acciones que pueden aumentar la posibilidad de infectar nuestros dispositivos y provocar daños a los activos de los usuarios, los cuales pueden ir desde la disminución gradual de la velocidad del ordenador o dispositivos móviles hasta la filtración o robo de datos personales. Por lo anterior, resulta fundamental conocer las principales medidas de seguridad, con el fin de proteger la disponibilidad, integridad y confidencialidad de la información resguardada en nuestros dispositivos, así como aumentar su esperanza de vida.

1.2.2.2 Riesgos de contenido y manipulación

En el ciberespacio se puede acceder a un sinfín de contenidos, muchos de ellos explícitos, dado que no existe una regulación de todo lo que se publican y transmite en la red; bajo esta condición niñas, niños y adolescentes están expuestas y expuestos a encontrar o acceder a contenido no deseado, inapropiado y/o delicado durante su interacción dentro del mundo digital (UNICEF, s/f).

Tomando como referentes los informes *Estado mundial de la infancia 2017- Niños en un*

[14] Infectar la mayor cantidad de computadoras posibles con sus credenciales de hurto, construir botnets, u otros programas maliciosos (Malwarebytes, s/f).

mundo digital (UNICEF), Seguridad de los niños en línea: Minimizando el riesgo de la violencia, el abuso y la explotación en línea 2019 (UNESCO-UIT), Directrices sobre la protección de la infancia en línea para los encargados de formular políticas 2020 (UIT) y *Protección de la infancia en línea: Guía para padres y educadores 2020 (UIT)*, los contenidos que se pueden considerar de riesgo son:

- Contenido agresivo que pueda llegar a ser perturbador, que incentive a cometer actos específicos de violencia en contra de una persona o grupo; y aquellos que promuevan la ideología de grupos terroristas.
- Contenido de tipo sexual, el cual puede incluir material explícito de desnudos, actos sexuales gráficos y/o material pornográfico.
- Material que promueva contenido racista, discriminatorio o de odio en el que se justifique la violencia hacia a una persona o un grupo, debido a su origen étnico o raza, orientación sexual, género, identidad de género, religión, discapacidad, entre otras.
- Formas de publicidad que tengan como fin crear un apego temprano de niñas, niños y adolescentes a determinadas marcas o productos.
- Páginas que promueven prácticas perjudiciales a nivel físico y psicológico, como autolesiones, anorexia, suicidio, entre otras.
- Contenido engañoso o manipulativo que tenga como fin promover determinados puntos de vista político, comerciales o de otro tipo.

En resumen, podemos ver en este apartado como la falta de regulación en la red, expone a niñas, niños y adolescentes a un sinfín de contenidos no deseados y riesgosos como los mencionados con antelación, por ello resulta fundamental promover el desarrollo de competencias entre esta población a fin de afianzar un comportamiento seguro y responsable en su interacción con el ciberespacio.

1.2.2.3 Riesgos de contacto

Sin lugar a duda, Internet y el ciberespacio han marcado un antes y un después en el área de la comunicación, ya que además de acortar las distancias, han configurado la manera en que se entienden y se gestan las relaciones interpersonales, la expresión personal y la privacidad.

Las redes sociales como uno de los principales canales de comunicación han sido utilizadas por niñas y niños como un medio de ocio para chatear con sus amigas y amigos, visualizar y

publicar fotografías, videos, entre muchas otras actividades, descuidando en ocasiones su privacidad y omitiendo la regla de tener trece años como mínimo para tener cuentas o perfiles dentro de las principales plataformas, como TikTok, Facebook, Instagram, YouTube, Snapchat, etc.

No disponer de los conocimientos necesarios para gestionar la privacidad y las relaciones interpersonales, a través de medios como redes sociales puede exponer a niñas y niños a ser contactados por extraños (generalmente adultos) y establecer comunicaciones que los pueden exponer a riesgos.

A continuación, se describen los riesgos de contacto (UNICEF, 2017; UNESCO-UIT, 2019; UIT, 2020):

- Ciberacoso, refiere a las acciones ejecutadas de manera reiterada (intimidación, acoso, exclusión, discriminación, etc.) a través de medios digitales por parte de una persona o un grupo de ellas con la intención deliberada de provocar daños a un tercero. Este ciberacoso puede ser la prolongación de un acoso realizado en la vida fuera de línea, y con ello, la víctima es invadida a cualquier hora y en espacios que ella podría considerar como seguros.
- *Grooming*, situación en la que un niño es acosado sexualmente por un adulto a través de medios digitales. *Grosso modo*, el *grooming* se ejecuta a través de una serie de fases: 1. Contacto y acercamiento, el adulto adopta una identidad falsa, con el fin de mostrarse como un coetáneo de la víctima y así entablar una relación de amistad; 2. Generación de confianza y obtención del material, el acosador genera un vínculo de confianza (secretismo e intimidad) con la víctima a fin de obtener el material; 3. Chantaje y acoso, una vez que la víctima ha enviado material se vuelve objeto de chantaje, ya sea para que entregue nuevo material o bien, para lograr un encuentro presencial. Una segunda forma de ejecutar el grooming es cuando el acosador obtiene material de la niña, niño o adolescente mediante la obtención de contraseñas o el hackeo de cuentas y utilizando dicho material para chantajear a la víctima para que produzca más material u obtener un encuentro físico.
- Niñas, niños y adolescentes pueden ser contactados, radicalizados y reclutados por grupos extremistas (Talibán, Al Shabab, neonazis, defensores de la supremacía blanca, entre otros).

- La explotación y uso de datos personales obtenidos a través de publicidad no deseada (spam), es un tema que ha planteado problemas con relación al consentimiento y la transacción de datos.
- Ser sometidos a presión, engañados o coaccionados para realizar compras con la autorización de quien las paga o sin ella.

Los riesgos mencionados en este apartado pueden derivarse del poco o nulo conocimiento de niñas y niños para gestionar su privacidad y relaciones interpersonales, lo cual, los expone a ser contactados por extraños con fines diversos que van desde la intimidación hasta el acoso sexual, por mencionar algunos.

1.2.2.4 Riesgos de conducta

En los riesgos de conducta, las niñas, niños y adolescentes pueden ser perpetradores o víctimas, es decir, pueden ser ellas o ellos quienes escriban o elaboren materiales que tengan como fin dañar a un coetáneo suyo, dichas acciones muchas veces son incentivadas por determinadas características que ofrece el ciberespacio, como el anonimato y la viralidad. Las niñas, niños y adolescentes se sienten protegidos y con la libertad de hacer comentarios hirientes o cometer agresiones sin ningún límite, porque su identidad está protegida por el anonimato y la facilidad con que se puede crear cuentas y perfiles falsos. Con respecto a la viralidad, ésta puede ser particularmente perturbadora y dañina, ya que los materiales (imágenes o mensajes hirientes) se pueden comunicar a terceras personas de manera rápida y tener un alcance inimaginable, por lo que la víctima podría tener mayor dificultad para poner fin al incidente.

A continuación, se describen los riesgos de contacto (UNICEF, 2017; UNESCO-UIT, 2019; UIT, 2020):

- *Ciberbullying*, son actividades hostiles (provocación, hostigamiento, denigración, suplantación de la identidad, violación de la identidad, exclusión, *fraping*, troleo, etc.) practicadas entre pares a través de medios digitales, con el fin de dañar, acosar o intimidar.
- Sextear es una práctica usada principalmente entre adolescentes a través de la cual se ejecuta el intercambio de contenido de tipo sexual (imágenes o videos) producido por los remitentes de manera voluntaria. El riesgo comienza con la divulgación del material

entre personas que no eran los destinatarios, lo cual, puede provocar daños a la identidad y reputación digital e incentivar otros riesgos, como el ciberbullying, chantaje o extorsión, etc.

- Divulgación de información personal, la cual, puede suponer riesgos de daño físico.
- El abuso físico y sexual son posibles riesgos dentro de encuentros en la vida real con personas que se conocieron en línea.
- Contenido potencialmente dañino generado por el usuario a través del cual se promueve contenido agresivo, sexual, racista, discriminatorio o de odio.
- Infracción de los derechos de autor a través de la descarga de música, películas, programas de televisión u otros contenidos que son de pago.
- Dentro de esta categoría, se encuentran también aquellas conductas que conllevan riesgos para la salud, como el tiempo excesivo en pantalla, el uso excesivo y compulsivo de internet y/o de los juegos en línea.

Resulta fundamental mencionar que aun cuando las niñas, niños y adolescentes están expuestos a riesgos y amenazas en línea, éstos "no siempre se traducen en daños […] si se tienen los conocimientos y la capacidad de reacción necesarios para sobrellevar la experiencia (UIT, 2020 b, p.15). Lo mencionado con antelación resume en gran parte la razón de ser de la propuesta de alfabetización digital a la que arguyo en este trabajo, ya que expone la necesidad de iniciar la formación en competencias digitales desde edades tempranas para prevenir y hacer frente a los riesgos y amenazas que pudiesen encontrar niñas, niños y adolescentes al navegar dentro del ciberespacio.

1.2.3 Acciones para la gestión de riesgos y amenazas en el ciberespacio

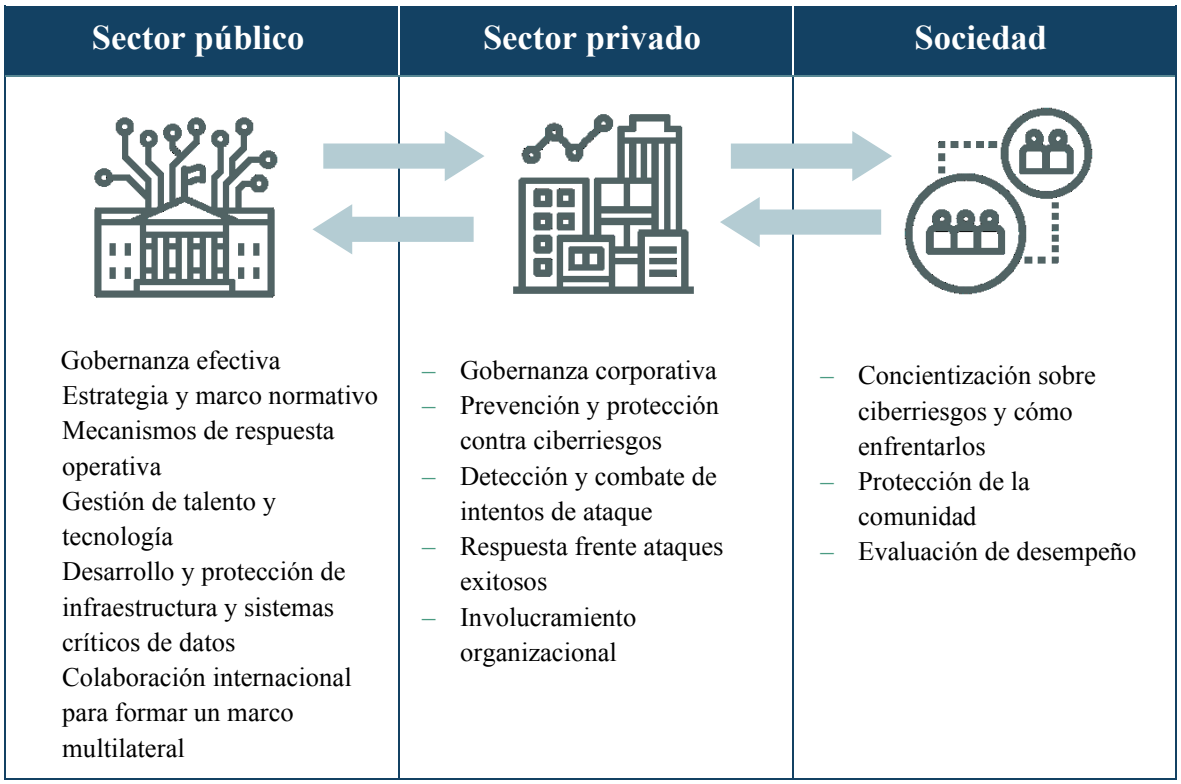
Las acciones para la gestión de riesgos y amenazas son todas aquellas que se dirigen a mitigar y/o mantener en niveles aceptables los riesgos a que son susceptibles las partes interesadas y sus activos en el ciberespacio; y entre las que se incluyen: políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías.

De acuerdo con su nivel de actuación y las capacidades (técnicas y operativas) que tengan las partes interesadas, éstas determinarán el enfoque y la metodología bajo las cuales se regirán para mantener los riesgos en niveles aceptables. En la Figura 3, se describen grosso modo las acciones que competen trabajar a cada una de las partes interesadas.

Es importante mencionar que, aunque existe esta categorización el trabajo de cada uno de ellos no es aislado uno respecto del otro, debido a que existen y se deben desarrollar nuevas oportunidades para el trabajo conjunto, por ejemplo, los tres sectores (sector público, privado y sociedad civil) pueden trabajar para desarrollar campañas específicas que doten de herramientas para prevenir y enfrentar incidentes a los usuarios individuales que son quienes están más expuestos.

Figura 3

Agenda por sector en materia de ciberseguridad



Nota. Fuente: COMEXI y McKinsey & Company. (2018). *Perspectiva de ciberseguridad en México* (p.6).

Como se ha mencionado con antelación, los usuarios individuales se consideran la parte más débil del ecosistema al no disponer de las capacidades ni de los expertos en tecnología con que cuentan las instituciones públicas y privadas, por ello, resulta fundamental trabajar en la formación de los usuarios en materia de ciberseguridad, pues "el 80% de los ciberdelitos podrían evitarse con medidas básicas de prevención" (Policía Federal, 2018, p. 32).

En la ISO 27032 (2015) se describen algunos aspectos a considerar al momento de definir una estrategia para la gestión de riesgos y amenazas en el ciberespacio para los usuarios:

- Aprender y entender las políticas de seguridad y privacidad del sitio y aplicación que les interesa, tal y como fueran publicadas por el sitio.
- Aprender y entender los riesgos de seguridad y privacidad involucrados; y determinar los controles aplicables apropiados.
- Establecer y aplicar una política de privacidad personal para la protección de la identidad.
- Gestionar la identidad en línea.
- Informar eventos o encuentros sospechosos a las autoridades respectivas.
- Como comprador o vendedor, se debe leer y entender la política de seguridad y privacidad de los sitios de compra en línea y realizar los pasos para verificar la autenticidad de las partes involucradas. No compartir datos personales, a menos que se establezca un interés genuino de vender o comprar. Usar un mecanismo de pago confiable.

Por su parte, Fundación Telefónica en el libro Ciberseguridad, la protección de la información en un mundo digital (2016), describe un ciclo de vida de la ciberseguridad que se compone de las siguientes etapas:

- Prevención. Es fundamentalmente una etapa de carácter formativo, con el fin de inculcar las mejores prácticas y debe ser abordada por el usuario desde varias perspectivas, entre las que se incluyen:
  - Informarse sobre la evolución de los riesgos y amenazas; y qué posibles soluciones existen contra ellas.
  - Conocer el funcionamiento de las herramientas o productos de seguridad, sus características y su forma de actuar para obtener la protección más efectiva.
  - Protección física de los dispositivos para garantizar que nadie sin autorización pueda manipularlos o conectar dispositivos no autorizados.
- Detección. La detección puede ocurrir mientras se está produciendo un incidente o pasado un tiempo desde que comenzó a desarrollarse éste. Es importante recordar que entre más tiempo transcurra desde el inicio del incidente hasta su detección los

problemas pueden ser mayores, debido a que los perpetradores han podido actuar libremente durante un largo período de tiempo.

- Reacción. Si desafortunadamente se ha producido un ataque es importante actuar en varios campos. Por un lado, dar una respuesta técnica y, si finalmente se ha producido un robo de identidad, robo de datos u otro ciberdelito, acudir a las fuerzas y cuerpos de seguridad del Estado e iniciar acciones legales para que los delitos que se hayan podido cometer no queden impunes.
- Inteligencia. El carácter dinámico y cambiante de los riesgos y amenazas cibernéticas obliga a la constante actualización y revisión de los sistemas de seguridad, compartir información y analizarla de forma eficiente puede ayudar a mejorar los niveles de seguridad, lo cual, requiere de una mayor colaboración entre todas las partes interesadas.

El ciclo de buenas prácticas de Fundación Telefónica aporta elementos fundamentales para considerarse dentro del curso que se desarrollará, ya que brinda las fases y algunos de los elementos que deben abordarse para fomentar la ciberseguridad.

1.3 Acciones nacionales e internacionales de ciberseguridad

El asunto del ciberespacio ha ido cobrando mayor relevancia, dada la tendencia que indica que los incidentes y ataques cibernéticos aumentan en frecuencia, grado de afectación y sofisticación, por lo que gobiernos y empresas reconocen la necesidad de sumar esfuerzos y fortalecer las capacidades en materia de ciberseguridad a fin de atenuar la problemática de la ciberdelincuencia que afecta los ámbitos económicos, jurídicos, políticos, militares y sociales a nivel global (Gobierno de México, 2017).

En los siguientes apartados se describen algunas de las acciones desarrolladas en materia de ciberseguridad a nivel nacional, regional e internacional.

1.3.1 Acciones internacionales y regionales de ciberseguridad

A continuación, se describen algunas de las alianzas, espacios y mecanismos en los que México participa a nivel internacional y regional para el intercambio de información y mejores prácticas en materia de ciberseguridad.

La Organización de las Naciones Unidas (ONU) como uno de los principales organismos para promover la cooperación internacional, ha desarrollado diferentes actividades, con el fin de garantizar la seguridad en el ciberespacio, entre las que se encuentran:

- Cumbre Mundial sobre la Sociedad de la Información (CMSI), 2003.
- Foro para la Gobernanza de Internet (FGI), 2022,
- Grupo de Expertos Gubernamentales (GEG), 2022.
- Comisión de Prevención del Delito y Justicia Penal (CCPCJ), 2022.
- Unión Internacional de Telecomunicaciones (UIT), organismo especializado en las Tecnologías de la Información y la Comunicación y cuyos proyectos en materia de ciberseguridad son:
  a. Desarrollo de estrategias de ciberseguridad a través de la publicación de informes, guías, artículos, cursos, talleres, entre otros.
  b. Creación de Equipos de Respuestas a Incidentes Informáticos (CSIRT), para ayudar a los Estados Miembros a crear capacidades a nivel nacional y regional.
  c. Realizar una encuesta para medir el compromiso y desarrollo de los Estados Miembros, la cual, deriva en el Índice Global de Ciberseguridad (IGC). En el informe del IGC, México se sitúa como un país en desarrollo en cuanto a capacidades en materia de ciberseguridad. En la Tabla 1 se muestran las puntuaciones que obtuvo en el IGC:

Tabla 1

Puntuaciones de México en el índice Global de Ciberseguridad (IGC).

1. Medidas legales. Leyes y reglamentos sobre ciberdelincuencia y ciberseguridad.	15.61
2. Medidas técnicas. Implementación de capacidades técnicas a través de agencias nacionales y sectoriales.	17.90
3. Medidas organizativas. Estrategias y organizaciones nacionales que implementan la ciberseguridad.	14.70
4. Medidas de desarrollo de capacidades. Campañas de concientización, capacitación, educación e incentivos para el desarrollo de capacidades en seguridad cibernética.	16.13

5. Medidas de cooperación. Alianzas entre agencias, empresas y países.		17.34
	Total	81.68

Nota: Elaboración propia. Fuente: Unión Internacional de Telecomunicaciones. (2022). *Índice Global de Ciberseguridad* 2020. (p.65)

De acuerdo con el informe y con los datos que se muestran en la Tabla 1, las áreas de fuerza relativa son las medidas técnicas y de cooperación con una puntuación de 17.90 y 17.34, respectivamente; y las áreas de crecimiento potencial son las medidas organizativas, legales y las de desarrollo de capacidades. A nivel regional, México se encuentra en la posición 4 y a nivel internacional ocupa el lugar 52.

Con base en los datos del ICG, podemos ver que México a nivel regional es uno de los países que más avances ha tenido en cuanto al desarrollo de capacidades en materia de ciberseguridad, sin embargo, a nivel internacional sus capacidades están aún en un nivel incipiente respecto a países más desarrollados, lo que nos indica que aún hay mucho trabajo por hacer.

En el marco de la Organización para la Cooperación y Desarrollo Económicos (OCDE), México, junto con otros 40 países suscribieron los siguientes tres factores en materia de ciberseguridad durante la Reunión Ministerial de Economía Digital de 2016 (Gobierno de México, 2017, p.10):

1. Reducir barreras para el comercio electrónico nacional e internacional.
2. Desarrollar estándares técnicos globales que permitan la interoperabilidad y un Internet seguro, estable, abierto y accesible.
3. Desarrollar con los tomadores de decisiones, estrategias para la privacidad y protección de datos enfatizando la transparencia en el sector público.

El Foro Económico Mundial (FEM), en el Informe de Riesgos Globales 2022, identificó que las amenazas de ciberseguridad cibernética están creciendo y están superando la capacidad de las sociedades para prevenirlas o responder a ellas de manera eficaz, que la prevención inevitablemente implicará costos más altos; y que los riesgos intangibles, como la desinformación, el fraude y la falta de seguridad digital afectarán la confianza pública en los sistemas digitales (FEM, 2022).

A nivel regional, el Banco Interamericano de Desarrollo (BID) en colaboración con la Organización de los Estados Americanos (OEA) publicó el *Reporte de Ciberseguridad 2020-Riesgos, avances y el camino a seguir en América Latina y el Caribe*, con el fin de medir el crecimiento y desarrollo de las capacidades de los Estados Miembros para hacer frente a los crecientes riesgos y amenazas del ciberespacio a través del Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), el cual, evalúa las capacidades de los países mediante las siguientes etapas de maduración: Inicial, Formativa, Consolidada, Estratégica y Dinámica. En la Tabla 2, se muestran las puntuaciones que México obtuvo en el CMM.

Tabla 2

Niveles de madurez de México en el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)

1. Política y estrategia de seguridad cibernética.	Consolidada
2. Cultura cibernética y sociedad.	Consolidada
3. Formación, capacitación y habilidades cibernéticas.	Consolidada
4. Marcos legales y regulatorios.	Consolidada
5. Estándares, organizaciones y tecnologías.	Formativa

Nota: Fuente: Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA). (2020). *Reporte de Ciberseguridad 2020. Riesgos, avances y el camino a seguir en América Latina y el Caribe* (pp.126-127).

En dicho estudio, México se sitúa como uno de los países que ha aumentado sus niveles de madurez en materia de cultura y formación dentro de la región; y que tiene como área de oportunidad incrementar las medidas que tengan como fin aminorar los ataques a empresas y gobiernos.

La Alianza del Pacifico, conformada por México, Chile, Perú y Colombia en la XX reunión de Ministros de Finanzas se comprometieron al establecimiento de mecanismos conjuntos para el intercambio de amenazas e incidentes cibernéticos que afecten al sistema financiero y el mercado de capitales. Además de lo anterior, aprobaron una guía de buenas prácticas con

métodos alternativos para las micro, pequeñas y medianas empresas (MiPyMEs) del sector financiero (Flores, 2019).

Con lo anteriormente desarrollado, es posible vislumbrar que México mantiene múltiples alianzas, espacios y mecanismos a nivel regional e internacional para intercambiar información y mejores prácticas con respecto a la ciberseguridad. En algunos casos se abordan aspectos integrales (marcos legales, marcos operativos, cooperación internacional,

cultura, educación, etc.); y en algunos otros, áreas específicas (comercio, financieras, legales, entre otras); pero todas, con el fin de contribuir al desarrollo de un ciberespacio seguro.

1.3.2 Acciones nacionales de ciberseguridad

En este apartado se describen las acciones que se han desarrollado en materia de ciberseguridad en México. Para comenzar, se hace referencia a algunos de los estudios realizados por instancias gubernamentales y asociaciones civiles; en un segundo momento, se hace alusión a las disposiciones legales que contemplan algunos incidentes cibernéticos; en un tercer momento, se mencionan cuáles son las instancias que operan en el país para atender, prevenir y mitigar amenazas cibernéticas; y finalmente, se mencionan algunas de las acciones en materia de formación que se promueven para fomentar la ciberseguridad entre la población mexicana.

1.3.2.1 Estudios en materia de ciberseguridad

A continuación, se presentan algunos de los estudios realizados por instituciones gubernamentales y de la sociedad civil en el país, con el fin de tener un panorama general de las problemáticas que afectan a la sociedad en el ciberespacio.

En el estudio Hábitos de los usuarios en ciberseguridad México 2019 de la Secretaria de Comunicaciones y Transportes (SCT) con apoyo de la Organización de Estados Americanos (OEA) destacan las siguientes conclusiones:

- En muchas ocasiones, los usuarios utilizan conexiones públicas sin detenerse a pensar en las consecuencias que esto pueda tener, ya que, aunque no todas estas redes son maliciosas, existe el riesgo de que los usuarios se conecten a puntos que tengan como finalidad esparcir códigos maliciosos o robar información.

- La mayoría de los participantes no cuida el tipo de aplicaciones que instala en sus dispositivos móviles.
- Los participantes no tienen una conciencia clara acerca de la privacidad en el uso de las redes sociales e Internet lo que puede exponerlos a delitos como robo de identidad, secuestro, trata de personas y corrupción de menores.
- El acceso libre que tienen los menores de edad a la tecnología se convierte en un problema, debido a que pueden verse expuestos a contenidos no adecuados para su edad.
- El 34% de los participantes ha sufrido algún tipo de acoso, de los cuales dos terceras partes son menores de edad.
- El 27% de los participantes ha sufrido de robo de identidad, de los cuales sólo una tercera parte son adultos.
- El 21% de los adultos participantes ha sufrido fraudes financieros a través de medios digitales.
- El 17% de los adultos participantes ha sufrido extorsión por el envío de fotografías con poca o nula ropa.

En el Módulo de Ciberacoso (MOCIBA) 2021 que realiza el Instituto Nacional de Estadística y Geografía (INEGI) como un apartado de la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH), destacan las siguientes conclusiones:

- Entre las medidas de seguridad tomadas para proteger dispositivos (computadora, tableta electrónica, teléfono celular) o cuentas de internet, destacan: crear o poner contraseñas (claves, huella digital, patrón, etcétera) con el 95.3%; seguida de instalar o actualizar programas antivirus, cortafuegos y antiespías con 28.4%.
- De la población usuaria de Internet, 21.7% vivió alguna situación de acoso cibernético.
- Las situaciones experimentadas con mayor frecuencia por parte de la población de mujeres que ha vivido ciberacoso fueron: contacto mediante identidades falsas (36.7%), recibir mensajes ofensivos (32.9%) y recibir insinuaciones o propuestas sexuales (32.3%); mientras que para la población de hombres que han vivido

ciberacoso fueron: contacto mediante identidades falsas (37.1%), recibir mensajes ofensivos (36.9%) y llamadas ofensivas (23.7%).

- De las víctimas que lograron identificar el sexo del agresor, el 62.1 % de hombres fueron agredidos por hombres y 55.3 % de las mujeres fueron agredidas por hombres.
- Los principales medios a través de los cuales las personas sufrieron ciberacoso, fueron: Facebook, Whatsapp y Twitter.

En el Estudio sobre ciberseguridad en empresas, usuarios de Internet y padres de familia en México 2021 de la Asociación de Internet MX, destacan las siguientes conclusiones:

- El 47% de los padres no usa o no sabe qué es un sistema de control parental y su principal problema es el establecimiento de límites para el uso de los dispositivos.
- La mayor preocupación sobre los riesgos en Internet para niñas, niños y adolescentes es sufrir acoso por parte de los adultos.
- El 15% de los padres manifestaron que sus hijos han tenido acceso a material inapropiado y el 2% compartió imágenes íntimas con extraños.
- De los encuestados, el 26% no sabe cuál es la autoridad competente para reportar problemas de ciberseguridad.
- Sólo el 4% de las personas encuestadas que tuvieron experiencias negativas con sus hijas o hijos, lo reportaron a las autoridades.
- El 33% de las niñas, niños y adolescentes no recibe orientación en la escuela sobre los peligros de Internet.

A manera de resumen, y tomado como base los datos de los estudios mencionados anteriormente, los principales problemas y directrices a abordar en materia de ciberseguridad en México son:

- Dispositivos (uso de redes públicas e instalación de aplicaciones).
- Privacidad en redes sociales.
- Robo de identidad.
- Acceso a contenido inapropiado (violencia, retos en línea, pornografía, drogas, armas, material racista, discriminatorio o de odio etc.).

- Contacto y comunicación arriesgada, en el que la persona es contactada por un desconocido y/o una persona mayor con fines de hostigamiento, seducción y/o abuso sexual (grooming, corrupción de menores, pornografía infantil, trata de personas, turismo sexual infantil, secuestro, etc.) o que intentan persuadirlos para participar en conductas poco saludables o peligrosas.
- Actividades en las que el individuo contribuye a que se produzca o reproduzca un contenido inapropiado o un contacto riesgoso (*cyberbullying, sexting*, sextorsión, etc.).
- Fraudes financieros.
- Poca o nula orientación (Información de los peligros en Internet, desconocimiento de las autoridades competentes en México en materia de ciberseguridad y desconocimiento sobre los sistemas de control parental).

El objetivo de este apartado, fue presentar los principales problemas y directrices a abordar en materia de ciberseguridad en México, a través de estudios realizados por instituciones gubernamentales y de la sociedad civil, los cuales nos sugieren que la falta de conciencia y conocimientos sobre los riesgos que implica el uso de Internet y las redes sociales dentro del ciberespacio puede derivar en situaciones de acoso cibernético, exposición a contenidos inapropiados y/o a delitos como el robo de identidad y la corrupción de menores.

1.3.2.2 Disposiciones legales en materia de ciberseguridad

A la fecha, México no cuenta con una ley operando en materia de ciberseguridad. En 2017, durante la administración de Enrique Peña Nieto se lanzó una Estrategia Nacional de Ciberseguridad[15], sin embargo, dicha estrategia no trascendió del papel y una de las posibles causas es que estuvo marcada por el cambio de administración, ya que en 2018 se llevaron a cabo las elecciones federales para renovar cargos mediante elección popular (presidente de la república, senadores y diputados federales).

[15] La Estrategia Nacional de Ciberseguridad se publicó en 2017 y en ella se contemplaron cinco objetivos estratégicos (Sociedad y derechos, Economía e innovación, Instituciones públicas, Seguridad pública y Seguridad nacional), tres principios rectores (Perspectiva de derechos humanos, Enfoque basado en gestión de riesgos, Colaboración multidisciplinaria y de múltiples actores) y ocho ejes transversales (Cultura de ciberseguridad, Desarrollo de capacidades, Coordinación y colaboración, Investigación, desarrollo e innovación TIC, Estándares y criterios técnicos, Infraestructuras críticas, Marco jurídico y autorregulación; y Medición y seguimiento).

Durante la administración actual, específicamente entre 2019 y 2020 se presentaron algunas iniciativas ante el Congreso, unas con el fin de actualizar la Estrategia Nacional de Ciberseguridad desarrollada en el sexenio anterior; y otras con el fin de que se expida una ley en ciberseguridad y de que ésta adquiera obligatoriedad en el territorio nacional. Sin embargo, a la fecha no se ha consolidado ninguna de las propuestas.

Algunas de las disposiciones legales vigentes que prevén algunos incidentes cibernéticos y/o buscan la protección y privacidad de los datos personales son:

- Título noveno del Código Penal Federal "Revelación de secretos y acceso ilícito a sistemas y equipos de informática".

  En el Capítulo I Revelación de secretos, se establecen las multas a quien "sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto" (p.171).

  En el Capítulo II Acceso ilícito a sistemas y equipos informáticos, se establecen las multas a quien incurra en alguna de las siguientes acciones (estando o no autorizado), dentro del sector industrial, sistema financiero, Estado o seguridad pública:

  1. Modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.
  2. Conozca, obtenga, copie o utilice información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.
  3. Si bien, este artículo tipifica el acceso ilícito a sistemas y equipos de informática como un delito, dichas "disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen" (BID-OEA, 2020, p.125).

- En lo que refiere a la protección de datos personales y la privacidad, existen dos leyes:
  1. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (organismos gubernamentales).
  2. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (organismos no gubernamentales).

El principal objetivo de las leyes antes mencionadas es proteger la información personal contra daño, pérdida, destrucción, uso, acceso o tratamiento no autorizado en soportes físicos

o electrónicos; y es una obligación de toda entidad (gubernamental o no gubernamental) que maneja datos personales establecer y mantener los mecanismos de seguridad que eviten que los datos sean utilizados indebidamente, que se respeten los derechos de los titulares y se garantice una expectativa razonable de privacidad. El organismo encargado de velar por la privacidad y protección de datos personales es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

- La Ley Olimpia como comúnmente es conocida, no refiere específicamente a una ley, sino a un conjunto de reformas al Código Penal Federal (Artículo 199 Octies) y a los códigos penales de las entidades[16] mediante las cuales se reconoce la violencia digital[17] como un tipo de delito.

  En el Código Penal Federal (2022), además de tipificar la violencia digital como un delito, se establecen sanciones económicas y penas de cárcel para quien:

  1. Divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona sin su consentimiento, su aprobación o su autorización.
  1. A quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.
  2. Se impondrán las mismas sanciones a quien divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual que no correspondan con la persona que es señalada o identificada en los mismos.

Si bien la Ley Olimpia ha representado un avance significativo en los años recientes para luchar en contra de algunos incidentes cibernéticos, queda mucho camino por recorrer en material legal para que se tipifiquen y castiguen los distintos tipos de delincuencia que suceden dentro del ciberespacio.

[16] Son 29 entidades en México que han aprobado normas relativas a la Ley Olimpia.

[17] Son actos de acoso, hostigamiento, amenazas, insultos, mensajes de odio, vulneración de datos o información privada realizados mediante el uso de tecnologías. Además de la difusión de imágenes, audios o videos —reales o simulados— del contenido íntimo sexual de una persona sin su consentimiento o mediante engaño. (Procuraduría Federal del Consumidor, 2021).

1.3.2.3 Autoridades de respuesta a incidentes cibernéticos

En México y en el mundo existen unidades especializadas para atender, prevenir y mitigar amenazas cibernéticas que operan bajo el nombre de Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) o Equipo de Respuesta ante Emergencias Informáticas (CERT).

A nivel nacional actúa el Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional (CERT-MX), el cual, tiene como misión "brindar servicios de apoyo en la respuesta a incidentes cibernéticos a través de la identificación de amenazas y del modus operandi de la ciberdelincuencia para el alertamiento a la ciudadanía" (Gobierno de México, s/f). Cabe mencionar, que aun cuando en el país operan otros CSIRT y CERT que ofrecen servicios para entidades académicas (UNAM CERT, CERT UACH, UV CSIRT, etc.) y organizaciones del sector público y privado (CSIRT Marina, Axtel CSIRT, CERT-ATTMX, etc.); el CERT-MX, es el único punto de contacto y coordinación dentro y fuera del territorio nacional.

En el sitio web del CERT-MX (https://www.gob.mx/gncertmx), es posible localizar materiales sobre ciberseguridad (guías, alertas, boletines y recomendaciones), así como dos formularios de atención para reportar incidentes, uno exclusivo para la ciudadanía y otro para instituciones públicas y privadas. El formulario para la ciudadanía, que es el tema que compete a este trabajo, se compone de tres apartados: datos de contacto, descripción de los hechos y un espacio para adjuntar evidencia digital.

Además del CERT-MX que es operado por la Dirección General Científica de la Guardia Nacional, en los estados de la República existen Unidades de Policía Cibernética, las cuales se encargan de "realizar actividades de prevención, vigilancia, identificación, monitoreo y rastreo en la red pública de Internet, con la finalidad de prevenir cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y patrimonial de los habitantes" (IFT, 2015). Dichas Unidades son operadas por la Secretaría de Seguridad Pública (SSP), la Fiscalía General del Estado (FGE) o la Fiscalía General de Justicia (FGJ), según sea la organización de cada estado de la república mexicana.

1.3.2.4 Acciones para fomentar la ciberseguridad en México

Algunas de las iniciativas que se han desarrollado dentro del sector público, privado y de la sociedad civil que sean desarrollado para fomentar la ciberseguridad entre la población mexicana, se encuentran:

Semana Nacional de Ciberseguridad, iniciativa de la Guardia Nacional que tiene como fin generar un espacio colaborativo de expertos nacionales e internacionales de los diversos sectores con el objetivo de preservar un entorno digital seguro. Entre las temáticas que se abordan, se encuentran: seguridad ciudadana en el ciberespacio, protección de infraestructuras críticas, economía digital para MiPyMEs, legislación en ciberdelitos y ciberseguridad niñas, niños y adolescentes (Guardia Nacional CERT-MX, 2021).

La *Jornada Internet seguro para todas y todos,* es una iniciativa de la Guardia Nacional que tiene como fin informar a la sociedad, sobre la importancia del uso responsable de las nuevas tecnologías, a través de la difusión de medidas preventivas, y la sensibilización sobre los riesgos en el internet. Los temas en que se centra dicha jornada son: Niñas, niños y adolescentes, Ciberseguridad ciudadana, Civismo digital, Ciberseguridad financiera y perspectiva de género en el ciberespacio (Guardia Nacional, 2022).

Sé Genial en Internet, es una iniciativa de Google para enseñar a las niñas y los niños de 8 a 12 años las habilidades que necesitan para preservar su seguridad y actuar con inteligencia en línea. La Coordinación General @prende.mx de la Secretaría de Educación Pública, en conjunto con Google y Robotix, llevaron a cabo una capacitación en materia de Ciudadanía Digital, con el objetivo de brindar a las y los docentes de México las "herramientas y métodos necesarios para enseñar en el aula los conceptos básicos de ciudadanía y seguridad digital" (Coordinación General @prende.mx, 2020). La capacitación consistió en una conferencia de una hora y quince minutos en YouTube, en la cual, se presentaron de manera somera los antecedentes de la iniciativa, los componentes que integran el programa y los materiales que se pueden descargar desde su sitio web.

A favor de TIC, es un proyecto educativo de la asociación civil *A favor de lo mejor* que a través de diversas herramientas (artículos, talleres y programas, tutoriales y materiales descargables sobre los riesgos en Internet) acompaña a los padres de familia y educadores para formar a niñas, niños y adolescentes en el uso, aprovechamiento y generación adecuada de los contenidos de internet (A favor de TIC, 2016).

Se genera la propuesta del MOOC para los docentes de primaria para que desde la escuela se promuevan estas competencias con un mayor alcance dentro de la población, ya que las estrategias que se han desarrollado, como las mencionadas tienen un alcance limitado de tiempo y espacio.

A través de este capítulo, se planteó la problemática que dió origen a este trabajo a fin de tener un panorama claro de los principales riesgos a que están expuestas niñas y niños en su interacción en el ciberespacio, lo cual, nos insta a intervenir sobre dicha realidad a fin de buscar los medios que permitan a los usuarios tomar conciencia de los riesgos y la responsabilidad que se debe asumir al navegar en el ciberespacio.

Capítulo 2. La alfabetización digital: un camino

En este segundo capítulo, se aborda de manera teórica la alfabetización digital, las competencias digitales y su relación con la ciberseguridad; se describe a grandes rasgos la capacitación docente y su relación con la alfabetización digital y el desarrollo de competencias digitales; finalmente, se describen aspectos relevantes en torno a los MOOC y el por qué se propone como medio para la capacitación docente.

2.1 Alfabetización digital y competencias digitales: una relación indisociable

En este apartado, se define qué es la Alfabetización digital, qué son las competencias digitales y algunas clasificaciones existentes; finalmente, se describe la relación entre alfabetización digital, competencias digitales y ciberseguridad.

2.1.1 Definición de Alfabetización digital

Cuando se escucha o lee el término alfabetización, comúnmente se piensa en la noción que la relaciona con la adquisición de las competencias básicas para leer y escribir, sin embargo, dicha noción resulta restringida si se parte de la idea que, "la alfabetización es un concepto polisémico y cambiante que se redefine en función del contexto histórico" (Núñez y Rodríguez, s/f, p.140).

Para reforzar la idea anterior, a continuación, se describen las tres dimensiones de la alfabetización que Núñez y Rodríguez (s/f, p.146) utilizan para proyectar la idea de la alfabetización dentro del ámbito social; y que, a su vez, sirven de referencia para caracterizar a la Alfabetización digital.

1. *Participar de forma activa dentro de la sociedad.* Se considera que la alfabetización promoverá la actuación eficaz de la persona dentro del grupo o comunidad, desempeñando con dignidad su papel de ciudadano y haciendo un buen uso de los derechos que le corresponden en su calidad de tal.

   Bajo esta primera dimensión, los cambios vertiginosos de la tecnología y su uso cada vez más extensivo impactan de manera directa en la sociedad y exigen que las personas desarrollen los conocimientos, habilidades y actitudes necesarias para desenvolverse de forma adecuada en un mundo que tiende cada vez más a la digitalización.

De acuerdo con Robles (2011, p.55) para desarrollarse como un ciudadano digital, es necesario el cumplimiento de al menos tres condiciones: acceso a Internet, el cual, posibilita el acceso de los ciudadanos a las interacciones que suceden dentro del ciberespacio entre personas, información, software y servicios; habilidades digitales, referidas a las capacidades de nivel medio alto para involucrarse en diversas actividades del mundo digital; y percepción de la utilidad de las tecnologías, referida a la capacidad de percatarse y hacer uso de los beneficios que éstas aportan a la vida cotidiana, académica y laboral.

2. *Aprender a lo largo de toda la vida.* La alfabetización se puede entender como un aprendizaje permanente que posibilita acceder continuamente al conocimiento y que puede ser adquirida por las personas en diferentes niveles o grados.

   Bajo esta segunda dimensión, la Alfabetización digital, insta a una preparación urgente de todos, de aquellos que no nacieron ni crecieron con las TIC y también de aquellos que aun cuando les ha sido fácil integrarlas, muchas veces carecen de las competencias para usarlas de forma crítica y segura.

3. *Ser crítico en el entorno.* La alfabetización se ha relacionado con el pensamiento crítico y reflexivo, hasta el punto de que se le ha considerado como el conjunto de competencias críticas que permite a los individuos comunicar y comprender la circulación de las ideas entre los individuos y grupos.

   La Alfabetización digital, se puede relacionar con esta tercera dimensión, en tanto que busca un uso crítico y reflexivo del uso y manejo de las TIC para transformarlas en conocimiento que sirva para la transformación personal y social.

Con base en las dimensiones antes mencionadas, la Alfabetización digital está íntimamente relacionada con el desarrollo de las competencias necesarias para desarrollarse en una sociedad que tiende cada vez más a lo digital, que deben y pueden ser adquiridas por todos en diferentes grados y niveles, con el fin de avanzar a competencias de nivel medio y alto que permitan convertirse en ciudadanos digitales que usan de forma crítica las tecnologías en pro de su vida personal, académica y/o laboral.

En lo que refiere propiamente a qué es la Alfabetización digital, en el presente trabajo se retoman dos definiciones: en la primera, en la que se le define, como "acciones formativas dirigidas al desarrollo de habilidades técnicas, sociales y éticas relativas al uso de las TIC,

organizadas por instituciones, asociaciones, ONG, etc." (Travieso y Planella, 2008, p.3) y, en la segunda, como el "conjunto de conocimientos, habilidades y actitudes para resolver eficazmente problemas con herramientas digitales y/o en contextos digitales" (Matamala, 2018, p.69).

Ambas definiciones son relevantes en la presente propuesta, ya que se busca diseñar una acción formativa en la que se desarrollen los conocimientos, habilidades y actitudes relativas a la ciberseguridad para prevenir y hacer frente a los riesgos y amenazas que pueden encontrar niñas, niños y adolescentes al navegar en el ciberespacio.

2.1.2 Definición y clasificaciones de competencias digitales

Las competencias digitales son definidas por la UNESCO, como "una serie de capacidades para utilizar dispositivos digitales, aplicaciones de comunicación y redes a fin de acceder a la información, gestionarla, comprenderla, integrarla, comunicarla, evaluarla y crearla de forma segura y adecuada" (2021, p.2).

Las competencias digitales son múltiples y existen diversas propuestas a través de las cuales se ha buscado categorizarlas, por un lado, se encuentran aquellas propuestas que las categorizan a través de dimensiones, como las que se mencionan a continuación:

Modelo de tres dimensiones (Matamala, 2018):

1. Dimensión técnica, referida a las habilidades operativas de uso de TIC.
2. Habilidades cognitivas, referidas a la capacidad crítica de búsqueda, evaluación y selección de información.
3. Habilidades socioemocionales, referidas al uso responsable de Internet.

Modelo de cinco dimensiones (García, 2017):

1. Instrumental. Capacidad para usar software y hardware.
2. Cognitivo-intelectual. Capacidad para buscar, seleccionar, analizar, interpretar y recrear la información.

3. Sociocomunicacional. Capacidad para comunicarse eficazmente a través de las TIC.
4. Axiológica. Capacidad para adquirir valores éticos y democráticos con relación al uso de la información.
5. Emocional. Referida a la capacidad para regular las emociones provocadas por la experiencia en los entornos digitales.

Por otro lado, se encuentran los marcos de competencias digitales, los cuales además de las dimensiones, muestran los niveles de dominio a través de los cuales las personas pueden medir su nivel de competencia, entre los que destacan:

DigComp

Es un marco desarrollado por la Unión Europea para su población en general, en el que se plantean cinco áreas de competencia: información, comunicación, creación de contenidos, seguridad y resolución de problemas.

Marco de Inteligencia Digital (DQ)

Fue desarrollado por la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Asociación de Estándares IEEE (IEEE SA) y el Instituto DQ en asociación con el Foro Económico Mundial (WEF), el cual, se integra de tres niveles de madurez (ciudadanía digital, creatividad digital y competitividad digital) y ocho áreas de la vida digital (identidad digital, uso digital, protección digital, seguridad digital, inteligencia emocional digital, comunicación digital, alfabetización digital y derechos digitales), las cuales derivan en un marco de veinticuatro competencias digitales.

Resulta imprescindible hablar de estas categorizaciones, ya que a partir de su estudio será posible identificar los conocimientos, habilidades y actitudes que se deben desarrollar en materia de ciberseguridad, y que servirán de base para seleccionar y organizar los contenidos que sean pertinentes para el diseño del MOOC.

2.1.3 Alfabetización digital, competencias digitales y ciberseguridad

En el título de este apartado se arguye a una relación indisociable entre alfabetización digital y competencias digitales, debido a que "[…] las competencias digitales, forman parte de las competencias de alfabetización […] varios aspectos de las competencias digitales resultan cada vez más indispensables para estar alfabetizado" (UNESCO, 2021, p.3).

Con base en lo anterior, las competencias digitales refieren propiamente al conjunto de conocimientos, habilidades y actitudes que las personas deben desarrollar y adquirir para desenvolverse de manera eficiente dentro de la sociedad, mientras que la alfabetización digital, refiere principalmente al proceso o la acción formativa, a través de la cual se adquieren y desarrollan dichas competencias.

En lo que refiere a la idea de que las competencias resultan cada vez más indispensables para estar alfabetizado, es fundamental comprender que los avances tecnológicos exigen de la sociedad cambios para hacer frente y adaptarse a los desafíos y demandas derivadas de dichos avances. En este sentido, las competencias digitales, en gran medida, se orientan a definir las áreas, criterios y niveles de dominio para que las personas puedan prepararse para hacer un uso seguro y eficiente de las tecnologías con las que se relacionan en el día a día y de aquellas que van emergiendo.

Finalmente, la relación entre los términos: alfabetización digital, competencias digitales y ciberseguridad, es que, tanto en los criterios como en los marcos de competencias digitales se definen aspectos referentes a los conocimientos, habilidades y actitudes en materia de seguridad digital, las cuales, abonan elementos indispensables para la propuesta formativa de alfabetización digital en materia de ciberseguridad.

2.2 Capacitación docente

En este apartado se define qué es la capacitación docente, cuáles son sus objetivos, cuáles son las modalidades de capacitación y se describe la relación de la capacitación docente con la alfabetización digital y el desarrollo de competencias digitales.

2.2.1 Definición y objetivos

La capacitación, refiere al "proceso educativo de corto plazo, aplicado de manera sistemática y organizada, por medio del cual las personas adquieren conocimientos, desarrollan habilidades y competencias en función de objetivos definidos" (Chiavenato, 2011, p. 322). Con base en el último punto de la definición y en relación con la capacitación docente, ésta se encamina a lograr "aptitudes, conocimientos, capacidades o habilidades complementarias para el desempeño del servicio" (Ley General del Servicio Profesional Docente, p.2).

Como ya se ha mencionado, el objetivo de la capacitación docente se focaliza en el desarrollo de competencias complementarias para el desarrollo de su servicio, pero, cuáles son esas

competencias a que refiere la Ley, de acuerdo con el Instituto Nacional para la Evaluación de la Educación (INEE, 2017, p.40), el contenido de la formación continua de los docentes se apega a los siguientes siete perfiles genéricos:

1. Programas de desarrollo en la función, basados en Perfiles, Parámetros e Indicadores y en los resultados de la evaluación.
2. Programas para el desarrollo de uso de las Tecnologías de la Información y la Comunicación (TIC).
3. Programas de formación de figuras del Servicio de Asistencia Técnica a la Escuela (SATE)[18].
4. Programas para fortalecer habilidades para la evaluación de los aprendizajes en el aula.
5. Programas de actualización en cambios, innovación y temas socialmente prioritarios.
6. Programas para el desarrollo de la gestión escolar y la gestión institucional.
7. Programas de atención y fortalecimiento del dominio de los contenidos disciplinarios.

La propuesta que se plantea en el presente trabajo se relaciona con el perfil 2, en tanto que la alfabetización digital y las competencias digitales se inscriben dentro del área de las TIC.

En lo que concierne a los objetivos que persigue la capacitación docente, de acuerdo con Vázquez y Cotto (2017) son:

- Desarrollar una actitud de compromiso con el mejoramiento de la educación.
- Utilizar de manera adecuada y creativa los instrumentos curriculares, materiales y recursos de apoyo.
- Intercambiar experiencias que contribuyan al mejoramiento de la calidad de vida de los estudiantes y de su aprendizaje.
- Cumplir con eficiencia el rol protagónico de agentes del proceso de transformación educativa.

[18] Ahora denominado Sistema de Asesoría y Acompañamiento a las Escuelas (SISAAE).

2.2.2 Modalidades de capacitación

Las modalidades de capacitación se pueden clasificar en función de la presencia en tiempo y espacio (presencial, a distancia y mixta) o por el tipo de propuesta (curso, taller, seminario, estancias, especializaciones, etc.).

En función de la presencia en tiempo y espacio

La capacitación al igual que otros ámbitos de la vida cotidiana se ha visto permeada por los cambios tecnológicos, posibilitando el desarrollo de modalidades alternas a la capacitación presencial que rompen con las barreras de tiempo y espacio.

De acuerdo con la Estrategia Nacional de Formación Continua, las modalidades de implementación de las ofertas formativas para los docentes son: presencial, en línea, bimodal y autogestiva, como se muestra en la Figura 4.

Figura 4

Modalidades de implementación de la oferta de formación

Presencial	Se organiza de manera directa entre una persona facilitadora y un grupo de participantes en un mismo horario y espacio físico.
En línea	Se vale de los medios tecnológicos para propiciar experiencias de aprendizaje a partir de la interacción y comunicación de manera síncrona y asíncrona entre quienes participan, y se realiza a través de plataformas de gestión del aprendizaje. Requiere la participación de una persona facilitadora, tutora o asesora, que brinde acompañamiento, retroalimentación y seguimiento puntual y oportuno a quienes estén participando.
Bimodal	Combina los encuentros presenciales y en línea para la interacción didáctica entre personas facilitadoras y participantes. También considera las sesiones de acompañamiento (presenciales o en línea) con el estudio que realizan de manera autónoma quienes participan.
Autogestiva	Es una forma de organizar el aprendizaje en la que quienes participan administran sus propias estrategias para lograr el objetivo de la oferta de formación, sin contar con el apoyo de una persona facilitadora. Requiere de medios que conduzcan la experiencia de aprendizaje *a partir* del trabajo autónomo, que pueden ser materiales didácticos o plataformas de aprendizaje.

Nota. Fuente: Dirección General de Formación Continua a Docentes y Directivos –SEP. Estrategia Nacional de Formación Continua. (p.33).

Con base en este criterio, la propuesta a la que arguyo en el presente trabajo se inserta dentro de la modalidad autogestiva, en tanto que los MOOC se valen de un diseño tecnológico de una o varias plataformas para generar experiencias de aprendizaje autónomo en las que los participantes gestionan sus propios recursos (tiempo, estrategias de aprendizaje, etc.) para lograr el objetivo de la oferta de formación, sin contar con el apoyo de una persona facilitadora.

Cabe mencionar, que la existencia o no de una persona facilitadora está en función del tipo de MOOC, ya que como veremos más adelante, existe una amplia gama de cursos que según su diseño y recursos (sobre todo, económicos y tecnológicos) puedan tener o no este perfil operando durante el desarrollo del curso.

En función del tipo de propuesta de formación

La modalidad de capacitación en función del tipo de propuesta de formación se basa en dos criterios: objetivo que se pretende alcanzar y duración de la propuesta. Con base en estos criterios, las propuestas formativas para los docentes, de acuerdo con la Estrategia Nacional de Formación Continua (2022, p. 34-35), son:

- Taller. Propuesta conformada por sesiones de estudio planificadas y estructuradas metodológicamente que fortalecen el saber hacer y el desarrollo de habilidades y actitudes con base en la integración sistemática de conocimientos teórico-metodológicos. Suelen durar un mínimo de 20 horas y un máximo de 120.
- Curso. Propuesta pedagógica estructurada metodológicamente con la finalidad de construir un marco referencial a partir de la revisión de contenidos teórico-conceptuales, orientados a promover la reflexión, que den pauta a la construcción de conocimientos complejos. Suelen durar un mínimo de 20 horas y un máximo de 120.
- Diplomado. Es un programa académico que ofrece a las y los participantes formación especializada con la finalidad de actualizar o profundizar en algún tema, abordando aspectos de orden teórico. En este tipo de formación, el valor curricular habrá de contemplarse en una duración mínima de 120 horas.
- Intervención formativa. Es un conjunto de actividades formativas secuenciadas, que consideran esquemas, como el seminario, la tertulia pedagógica, el grupo de análisis

de la práctica o encuentro y la conferencia magistral, las cuales son articuladas por un propósito formativo. Estos tipos de formación deberán desarrollarse en un mínimo de 20 horas y el máximo de carga horaria será de 200 horas.

En función de esta tipología, la propuesta a la que se arguye en el presente trabajo es un curso orientado a la reflexión, en torno a los problemas relativos a la ciberseguridad y a brindar herramientas que posibiliten que los docentes promuevan la ciberseguridad en sus aulas, a través de la revisión de los contenidos teóricos y de las actividades que se desarrollen en el curso. La extensión que se estima tendrá como mínimo 20 horas y como máximo 40, las cuales entran dentro del rango propuesto para cursos y talleres.

2.2.3 La capacitación docente para el desarrollo de competencias digitales

La incursión de las TIC en la educación ha abierto grandes posibilidades para mejorar los procesos de enseñanza y aprendizaje, pero también ha representado nuevos desafíos dentro de las instituciones educativas, como lo son el diseño, mantenimiento y gestión de la infraestructura tecnológica, las competencias docentes que se requieren para la integración de las TIC y la provisión de recursos y contenidos digitales que favorezcan el uso e integración pedagógica (Martínez, 2021).

Respecto a estos tres desafíos para la integración de las TIC planteadas por Martínez, me centraré de manera específica en el de competencias digitales docentes. Las competencias digitales docentes se definen como el conjunto de "conocimientos, actitudes y habilidades que el profesorado necesita poseer para la adecuada utilización de los medios digitales y las TIC como recursos educativos integrados a su práctica docente (Suárez, Almerich, Diaz & Fernández, 2011, p. 294, como se citó en Arcos, 2019).

En la definición antes mencionada, es posible visualizar los niveles en que el docente debe dominar las competencias digitales, por un lado, a las competencias técnicas, relativas al saber usar los medios y herramientas digitales; y por el otro lado, a las competencias pedagógicas que posibiliten integrar las TIC de manera efectiva dentro de su práctica docente dentro de cualquier situación educativa.

Como se vio en el primer apartado de este segundo capítulo, las competencias digitales son diversas y se ha buscado clasificarlas a través de criterios y marcos de competencia digital; y la formación de los docentes no es la excepción, ya que a través diversos proyectos se han

definido estándares para competencias TIC orientados a mejorar la práctica de los docentes en todas las áreas de su desempeño profesional, entre los que se encuentran:

- Marco de Competencias de los Docentes en materia de TIC de la UNESCO (ICT-CFT)

  Se compone de seis aspectos prioritarios para la labor pedagógica de los docentes (Comprensión del papel de las TIC en la educación, currículo y evaluación, pedagogía, aplicación de competencias digitales, organización y administración y aprendizaje profesional de los docentes) y de tres niveles de conocimientos (adquisición, profundización y creación).
- *DigCompEdu*

  Es un marco de competencias digitales, diseñado específicamente para los educadores de todos los niveles educativos de la Unión Europea. En este marco se plantean seis áreas: compromiso profesional, recursos digitales, enseñanza y aprendizaje, evaluación y retroalimentación, empoderar a los participantes y facilitar la competencia digital de los estudiantes.

Se retoma la alfabetización digital dentro de la propuesta, ya que dos medidas recomendadas por el Fondo de las Naciones Unidas para la Infancia (UNICEF) en materia educativa para proteger a niñas, niños y adolescentes de los peligros del mundo digital son:

- Enseñar alfabetización digital en las escuelas. Dado que los niños se conectan en línea a edades cada vez más tempranas, las escuelas, especialmente las públicas, deben incorporar programas de alfabetización digital.
- Apoyar la capacitación y alfabetización digital de los maestros. Los docentes deben ser capaces de desarrollar sus propias [competencias] para apoyar el uso de las TIC por parte de sus alumnos y ayudarlos a desarrollar una comprensión del uso seguro de Internet más allá del aula. (UNICEF, 2017, pp. 32-33).

Tomando como base lo anterior, la propuesta que se presenta en este documento tiene como unos de sus fines abonar a esas dos medidas, por un lado, apoyar en la capacitación de competencias digitales en materia de ciberseguridad entre los docentes de primaria alta a través del curso MOOC, y por el otro, ofrecer orientaciones didácticas dentro del curso que les permitan integrar y promover la ciberseguridad dentro de sus respectivas aulas.

2.3 MOOC

En este apartado se define qué son los MOOC, cuáles son sus orígenes, qué tipos de MOOC existen, cuál es el proceso para elaborar un MOOC, que plataformas los ofertan y el por qué se proponen los MOOC como medio para la capacitación docente.

2.3.1 Orígenes y definición de los MOOC

MOOC es el acrónimo en inglés de *Massive Online Open Courses*, "el término fue utilizado por primera vez en 2008 para el curso *Connectivism and Connective Knowledge* diseñado por George Siemens, Stephen Downes y Dave Cormier y ofrecido por la División de Extensión Universitaria de la Universidad de Manitoba, en Canadá" (Mercado, 2016, p.54). En este curso de 12 semanas de duración se inscribieron aproximadamente unos 2.300 estudiantes de diferentes partes del mundo.

Si bien dicho curso no tuvo el impacto de los MOOC actuales, abrió el camino para el desarrollo que han tenido en la década reciente, ya que incluso, el 2012, fue bautizado como "el año del MOOC" ante las altas expectativas que se generaron en torno a estos cursos.

Ahora que ya se ha hecho un panorama muy sintético en torno a los orígenes de estos cursos, en la Figura 5, se define qué son los *Massive Online Open Courses* tomando como base sus principales características, las cuales derivan del acrónimo MOOC. Cabe mencionar que dicho acrónimo es utilizado comúnmente para referirse a este tipo de cursos, debido a que no existe un término en español que sea aceptado ampliamente para referirse a ellos.

Figura 5

Acrónimo en inglés de Massive Open Online Course (MOOC)

M	Massive	Son masivos, ya que atienden a un gran número de participantes dadas las posibilidades que ofrecen los medios tecnológicos que se utilizan para hospedarlos y distribuirlos.
O	Open	Son abiertos, esta característica hace referencia a su carácter de gratuidad. Cabe mencionar que dependiendo de las entidades que los ofertan, éstos pueden ser totalmente gratuitos, requerir de una cuota de acceso o pagar únicamente para obtener un certificado de acreditación.

O	Online	Su forma de distribución es en línea, de manera que, para acceder a ellos es necesaria una conexión a Internet.
C	Course	Son cursos, y, por tanto, tienen una estructura similar, es decir, poseen objetivos de aprendizaje, unidades o módulos, actividades de aprendizaje, actividades de evaluación, etc.

Nota. Fuente: Adaptado de Mercado, R. (2016). *Cursos masivos abiertos en línea: oportunidad o amenaza.* Universidades, Núm. 70, (pp. 55-56).

2.3.2 Tipos de MOOC

Los MOOC pueden adoptar diversas formas, en función de criterios, como el fundamento pedagógico bajo el cual se sustentan, el grado de escala o masividad y su nivel de apertura, entre otros. A continuación, se describen algunas de las tipologías que se han utilizado para clasificar a los MOOC.

Figura 6

Tipología de MOOC propuesta por Clark.

TransferMOOCs	Se trasladan los cursos en línea elaborados por las universidades a plataformas MOOC. Las actividades se caracterizan por buscar la transferencia de contenido por parte de un docente a un grupo de alumnos.
MadeMOOCs	Incorpora elementos de vídeo, hace énfasis en la creación de tareas que deben realizar los estudiantes (actividades retadoras, como la solución de problemas); y potencia el trabajo y la evaluación entre pares.
SynchMOOCs	Se establecen fechas específicas de inicio y fin del curso, así como de las actividades y evaluaciones a realizar durante su desarrollo.
AsynchMOOCs	No se establecen fechas límites para la inscripción al curso, ni para la realización de actividades.
AdaptativeMOOCs	En este tipo de cursos, se emplean algoritmos para presentar experiencias personalizadas de aprendizaje basadas en evaluaciones dinámicas y en la recopilación de datos del desempeño en el curso.
GroupMOOCs	Son cursos elaborados para grupos específicos.
ConnectivistMOOCs	Se basan en el enfoque teórico del conectivismo propuesto por George Siemens y Stephen Downes.

MiniMOOCs	Son cursos intensivos que se trabajan en plazos cortos (horas o días) en lugar de semanas como comúnmente se trabajan.

Nota: Fuente: Cabero, J., Llorente, M. y Vázquez, A. (2014). *Las tipologías de MOOC: Su diseño e implicaciones educativas.* (p.17).

Figura 7

Tipología de MOOC propuesta por el Observatorio de Innovación Educativa

xMOOC	Es el modelo más común. La "x" indica que se trata de MOOC comerciales, es decir, aquellos que se ofertan en plataformas comerciales o semicomerciales, como Coursera, edX y Udacity. Se centra en el aprendizaje tradicional: visualización de videos y la realización de cuestionarios (tipo examen). El curso se desarrolla en torno a un profesor titular y un plan de estudios básico.
cMOOC *Connectivist Massive Online Open Courses*	La "c" indica que se trata de un MOOC conectivista. Su énfasis está en la creación de conocimiento por parte de los estudiantes, en la creatividad, la autonomía; y el aprendizaje social y colaborativo. El desarrollo del curso es similar a un seminario, ya que los materiales se utilizan únicamente como punto de partida para entablar discusiones entre los participantes.
DOOC *Distributed Open Collaborative Course*	Los Cursos Colaborativos Distribuidos en Línea (DOOC), constan de materiales que se distribuyen entre estudiantes de diferentes instituciones. La administración del curso varía, ya que no se centra en un experto o institución en particular, sino en la experiencia de participantes provenientes de diversos contextos institucionales.
BOOC *Big Open Online Course*	Los Cursos Abiertos en Línea a Gran Escala (BOOC) son similares a los xMOOC, con la diferencia de que en estos cursos se limita el número de participantes (comúnmente no más de 50).
SMOC *Synchronous Massive Online Open Courses*	En los Cursos en Línea Masivos y Simultáneos (SMOC), las clases se transmiten en vivo, por lo cual, los estudiantes se conectan en línea de manera simultánea.
SPOC *Small Private Online Course*	Los Pequeños Cursos en Línea y Privados (SPOC), utilizan la misma infraestructura que los xMOOC, aunque su alcance no es masivo y pueden incluir elementos cerrados en sus contenidos. Son cursos con un grupo limitado de participantes y con

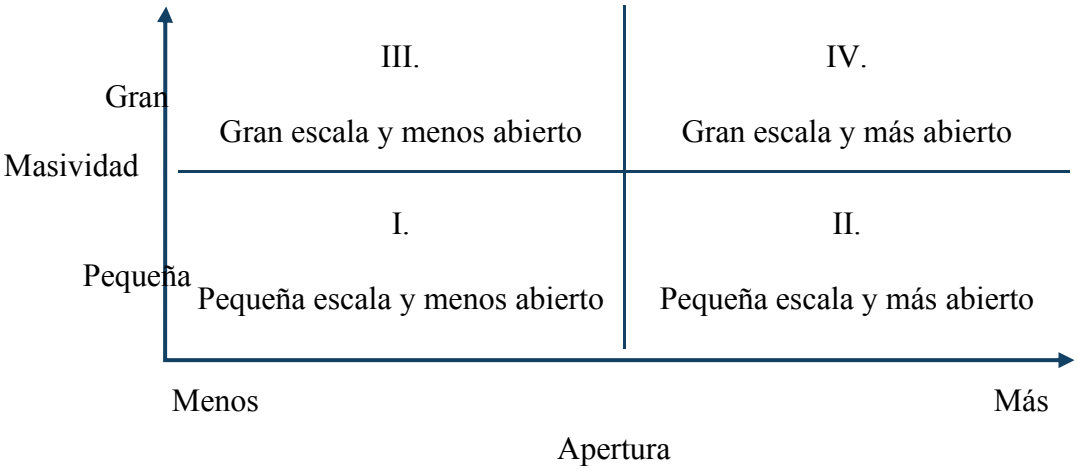
	interacciones estudiantes-profesor/a basadas en el modelo convencional del aula.

Nota: Fuente: Observatorio de Innovación Educativa del Tecnológico de Monterrey. (2014). Reporte EduTrends. MOOC. (p.5).

Pilli y Admiraal (2016) proponen una nueva taxonomía para clasificar los MOOC tomando como base dos dimensiones: masividad y apertura. La taxonomía se sintetiza en una matriz bidimensional compuesta de cuatro categorías, las cuales se muestran en la Figura 8.

Figura 8

Matriz bidimensional para clasificar MOOC.



Nota. Fuente: Pilli, O. y Admiraal, W. (2016). *A Taxonomy of Massive Open Online Courses*. (p.226).

Con base en esta taxonomía, los MOOC se clasifican de la siguiente manera:

- Primer cuadrante. Son los MOOC de pequeña escala y menos abiertos. Tienen un número de participantes limitado, es decir, de 200 a 500 participantes en lugar de miles. En cuanto a la apertura también está limitado, ya puede necesitar de una cuota para acceder a algunas partes del curso. En este cuadrante, se encuentran los SPOC y groupMOOC.
- Segundo cuadrante. Refiere a los MOOC de pequeña escala y más abiertos. En tanto al número de participantes está limitado, tal y como en los del primer cuadrante. Se considera abierto, en tanto que los materiales del curso y/o los exámenes son gratuitos

para todos los participantes. En este cuadrante, se sitúan los cMOOC, BOOC, DOOC, POOC, Adaptive MOOC, etc.

- Tercer cuadrante. Son los MOOC de gran escala y menos abiertos. En estos cursos se permite la participación ilimitada con contenido restringido de forma gratuita. En él se encuentran los cursos a distancia tradicionales, como los SMOC y miniMOOC, entre otros.
- Cuarto cuadrante. Refiere a los MOOC con escala y participación ilimitados. En este cuadrante se encuentran los cursos en los que los expertos expresan sus conocimientos e ideas a través de videos y contenidos dentro del curso, como los xMOOC, transferMOOC, madeMOOC, asynchMOOC, SPOC, etc.

Son diversas las categorías utilizadas para clasificar los MOOC, sin embargo, resulta factible no casarse con ninguna de las clasificaciones, debido a que no hay una teoría que las sustente, ni un consenso con respecto a los criterios que se usan para categorizarlas. Lo más factible es guiarse de las necesidades que se buscan satisfacer y de los criterios y recursos con que se cuenta para llevar a cabo la implementación.

2.3.3 Proceso para la elaboración de un MOOC

Los MOOC, como se mencionó en el apartado de definición y orígenes, son cursos, y, por tanto, tienen una estructura similar, es decir, poseen objetivos de aprendizaje, unidades o módulos, actividades de aprendizaje, actividades de evaluación, etc., con sus debidas variantes y características, las cuales se delinean en el presente apartado.

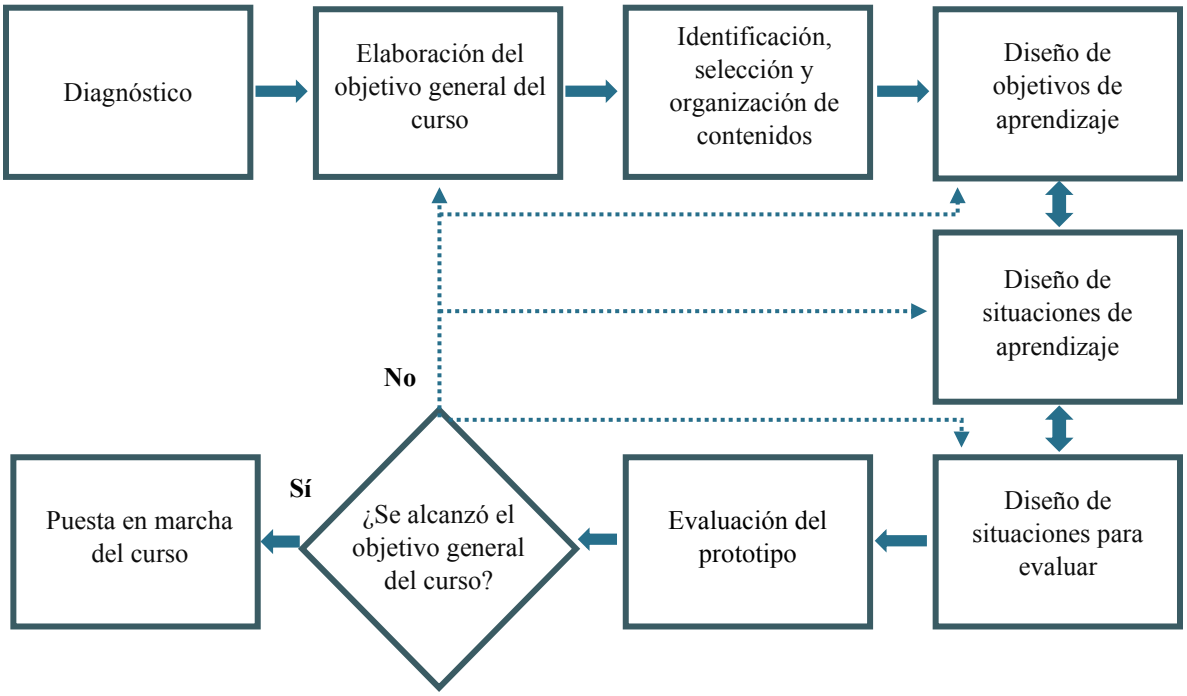
Uno de los factores clave para asegurar el éxito y la calidad de un proyecto formativo, independientemente de la modalidad en que se lleve a cabo, (presencial, en línea, híbrida, etc.) es el diseño instruccional. El diseño instruccional, *grosso modo* es el "esquema que ubica los diferentes procesos involucrados en la elaboración de programas educativos" (Gil, 2004, p.95), y que tiene como fin, generar un ambiente propicio en donde se desarrollen los procesos de enseñanza y aprendizaje.

Existen múltiples modelos de diseño instruccional, a través de los cuales se organiza una propuesta formativa, como el modelo ADDIE, el modelo de Dick y Carey, el modelo ASSURE entre otros. En la Figura 9, se presenta el modelo de diseño instruccional que propone María del Carmen Gil Rivera, el cual, se utilizará como base para describir el

proceso de elaboración de un MOOC y como guía para la elaboración de la propuesta pedagógica de alfabetización digital a la que arguyo en este trabajo.

Figura 9

Modelo de diseño instruccional para programas educativos a distancia



Nota. Fuente: Adaptado de Gil, M. (2004). *Modelo de diseño instruccional para programas educativos a distancia.* Horizontes, vol. XXVI, núm. 104, (p.95).

Diagnóstico

Antes de comenzar propiamente con el diseño, es necesario realizar un diagnóstico, con el fin de identificar: las necesidades educativas, las características de los estudiantes, la infraestructura tecnológica y los recursos humanos disponibles.

Identificación de necesidades educativas

La identificación de las metas educativas permite establecer las metas y objetivos De acuerdo con Bradshaw (citado por Gil, 2004), existen cinco tipos de necesidades.

- Normativas: refieren a la falta de conocimientos que tiene un sujeto o grupo de personas con relación a un estándar de conocimientos.
- Sentidas. Expresan el interés de una persona por aprender algo, ya sea por necesidad o porque genuinamente le gustaría saber.

- Por demanda. Se hacen evidentes cuando la solicitud de algo es muy frecuente.
- Comparativas: hacen referencia a los beneficios o conocimientos que tiene un determinado grupo en comparación con otro.
- Prospectivas o anticipadas: refieren a aquellas que seguramente se necesitarán o se presentarán en el futuro.

Características del público al que se dirige el programa educativo

En el caso de los MOOC es muy importante recordar que el público al que se dirige puede llegar a ser muy amplio y con características muy heterogéneas. Entre las cuestiones más relevantes a considerar con respecto a este punto, se encuentran:

- Edad. Estimar una edad promedio.
- Conocimientos. Las personas interesadas o quienes se inscriben al curso, pueden tener un conocimiento mínimo del tema o tener mucha experiencia, por ello, resulta de suma relevancia, publicar en la oferta del MOOC, el alcance, el perfil de los participantes, los prerrequisitos del área de conocimiento y los aspectos tecnológicos que deben saber o tener para participar en él.
- Ubicación geográfica. Los MOOC, como se ha visto anteriormente, rompen con la barrera del espacio, razón por la cual, en el curso puede haber personas de países diversos con idiomas y culturas distintas, por lo que es recomendable utilizar un lenguaje sencillo y evitar el uso excesivo de modismos propios de la región, para que el curso sea comprensivo a la mayoría.

Identificación de infraestructura tecnológica

Resulta fundamental identificar la infraestructura tecnológica, ya que la descripción de ésta permite tomar decisiones que influyen en el diseño de las situaciones de aprendizaje y de evaluación como se verá con detalle en los siguientes apartados.

Entre los principales aspectos tecnológicos a considerar en el desarrollo de un MOOC se encuentran: plataforma que se utilizará para implementar el curso, herramientas para el diseño de materiales (videos, infografías, test, etc.) y los canales de comunicación disponibles (síncronos y asíncronos).

Identificación de recursos humanos

En el diseño, desarrollo y ejecución de un MOOC, se requiere de un equipo multidisciplinario; y es importante determinar desde el inicio del proyecto quiénes serán los profesionales que intervendrán. El equipo multidisciplinario que se contempla como indispensable para el desarrollo de un MOOC, de acuerdo con la *Guía práctica para hacer un MOOC* (Lladós, s/f, pp.23-50) son:

Coordinador/a o responsable del programa educativo

- Diseño el proyecto junto con las personas interesadas, lo cual, implica decidir una meta, identificar una pregunta que el proyecto buscará responder, y definir los datos necesarios para ser recopilados y utilizados dentro del proyecto.
- Se encarga de la gestión institucional, administrativa, pedagógica y comunicacional.
- Crea un ambiente en el que todas las personas se sientan dispuestas a participar.
- Dirige retrospectivas para reflexionar sobre el trabajo realizado y las lecciones aprendidas.
- Informa el estado y los resultados del MOOC a los interesados.

Experto/a en el contenido del programa educativo

- Selecciona y organiza los contenidos a través de un esquema o gráfico que dé cuenta de sus relaciones.
- Selecciona, ordena y jerarquiza los contenidos en materiales didácticos con asesoría pedagógica y tomando en cuenta las posibilidades multimedia.
- Redacta recursos y estrategias que favorezcan la reflexión acerca de lo que se leerá: acciones tendientes a mantener la atención, la participación y a generar debate (controversias, preguntas, ejemplos, relatos, metáforas, simulaciones y analogías).
- Define la naturaleza de las actividades, buscando que favorezcan el desarrollo de procesos cognitivos y socioafectivos que posibiliten la formación integral.
- En el desarrollo de las actividades explicita y detalla el nombre, objetivos, la o las acciones a realizar (consignas, con especificación de los tipos de producción que se deben desarrollar, los recursos y elementos a utilizar, y si son obligatorios u opcionales), la modalidad individual o colectiva de trabajo, el espacio de entrega de la tarea, los criterios de evaluación y el tiempo disponible para la realización de la tarea o la fecha límite de entrega.

- Brinda tutoriales de uso cuando proponga producir con ciertas aplicaciones o herramientas, además del enlace para acceder a ellas.

Diseñador/a instruccional o pedagogo/a

- Brinda orientaciones sobre estrategias didácticas, elaboración y selección de materiales educativos, bibliografía actualizada del campo educativo, perspectivas pedagógicas actuales e inclusión de TIC.
- Colabora en la planificación general del curso y su práctica es transversal.
- Acompaña y asesora al experto en contenido en el proceso de planificación, producción y revisión del material.
- Sugiere materiales para integrar en los módulos que faciliten diferentes usos y propósitos, tales como la interacción con la realidad, la experimentación, la sensibilización, la reflexión, y no convertirse sólo en complementos o extensiones de la exposición de quien enseña.
- Asegura la coherencia entre el contenido, las actividades y los criterios de evaluación de la propuesta analizando el modo en que se presentan.

Experto/a en el uso de medios

- Se encarga de la planificación, realización y posproducción de los contenidos audiovisuales, gráficos e interactivos.
- Desarrolla la propuesta estética (paletas de colores, tipografías, formas predominantes y estilos de maquetación).
- Acompaña en el proceso de estructuración de contenidos para ayudar a definir qué contenidos son más adecuados para ser abordados de manera audiovisual, gráfica o interactiva y cuáles de manera escrita.
- Define en conjunto con el equipo y dependiendo de los recursos económicos y materiales disponibles los formatos a utilizar, cantidad de videos, ubicación en la estructura del curso y guionado de las piezas a producir.
- Establece un plan con base en el cronograma para ejecutar y coordinar los procesos de grabación, edición, corrección y subtitulado de los materiales.

Corrector/a de estilo

- Interviene lingüísticamente en los textos de los diferentes elementos del curso para que los futuros lectores puedan entenderlos.

– Revisa y corrige la estructura general de los textos (orden, coherencia, extensión, etc.) y después en la ortotipografía.

Diseñador/a de sitios web

– Analiza y comprende la estructura del documento a maquetar.
– Identifica incongruencias en el documento a maquetar, tomando como base las posibilidades de la plataforma y propone alternativas.
– Integra los contenidos de texto, multimedia y de diseño gráfico en la estructura HTML del curso.
– Comprueba el maquetado en diferentes navegadores web.
– Informa al equipo la finalización del trabajo para que pueda ser revisado.
– Realiza las modificaciones y/o correcciones.

Docente-asesor/a

– Es especialista en el tema del MOOC y si no participó en la producción de contenidos, deberá conocerlos y estudiar el modo en que fueron estructurados dentro de la propuesta de enseñanza.
– Apoya y alienta al grupo de participantes a avanzar en el MOOC.
– Profundiza los contenidos y promueve la participación dentro de los espacios de interacción.
– Realiza el seguimiento y evaluación de las actividades.
– Elabora un informe de evaluación que incluya sugerencias de mejora.

Además de definir qué roles trabajarán en el diseño del MOOC, resulta indispensable elaborar un plan de trabajo que incluya los procesos, los responsables y las fechas de inicio y fin de cada una de las actividades que se ejecutarán, con el fin de conocer el tiempo total requerido para poner en marcha el programa que se está diseñando.

Elaboración del objetivo general del programa

El objetivo general, señala lo que los participantes deben saber en términos de conocimientos, habilidades y actitudes, al finalizar el proceso formativo (curso, taller, diplomado, etc.). Parte de las necesidades identificadas en el diagnóstico y responde a la pregunta: qué necesita conocer y/o qué debe saber hacer el participante.

Los objetivos generales son de suma relevancia, ya que son "el punto de partida y de llegada […], pues la selección de los contenidos, las situaciones de aprendizaje y de evaluación son diseñadas para alcanzar esos objetivos" (Gil, 2004, p.98).

Identificación selección y organización de contenido

En función del objetivo general se define "qué es lo que van a aprender los participantes en el curso, es decir, qué contenidos van a ser organizados de manera didáctica para que los participantes construyan su propio conocimiento" (Gil, 2004, p.99).

Para identificar y seleccionar los contenidos de un programa educativo es necesario ubicar qué tipo de contenidos se van a enseñar:

- Contenidos conceptuales. Refiere a los procesos mentales o intelectuales del participante en torno a hechos, conceptos y principios., que van desde la memorización (orden inferior) hasta la aplicación de criterios y elaboración de juicios que requieren de una actividad intelectual compleja (orden superior)
- Contenidos procedimentales. Hacen referencia a las acciones o formas de actuar para resolver problemas. En este tipo de contenido se localizan las habilidades (disposición para realizar algo), las técnicas (habilidades para hacer uso de procedimientos) y estrategias (actividades destinadas a conseguir un objetivo específico).
- Contenidos actitudinales. Refieren a los patrones y principios de conducta (actitudes y valores) que posibilitan que la persona se desarrolle de manera armónica dentro de la sociedad.

Es fundamental identificar y determinar qué tipo de contenidos se abordarán, en qué cantidad y con qué profundidad a fin de balancearlos y que no se carguen hacia un solo tipo. Además, sirven de referencia para determinar a través de qué recursos se presentará la información y a través de qué actividades de aprendizaje se afianzarán dichos contenidos.

Diseño de objetivos de aprendizaje

En estos objetivos, se describen y especifican con mayor precisión los conocimientos, habilidades y las actitudes que se espera que el participante alcance al término de un tema, actividad de aprendizaje, unidad o módulo. Son el punto de partida de las situaciones de aprendizaje y de evaluación, la selección de los materiales didácticos y los medios de comunicación (Gil, 2004).

Diseño de situaciones de aprendizaje

En esta fase debe explicarse de manera clara las acciones individuales o colectivas que los participantes realizarán. También se deben definir los materiales didácticos que se utilizarán para organizar y representar el conocimiento; y los medios de comunicación síncronos o asíncronos (Gil,2004).

Diseño de situaciones para evaluar

El diseño de las actividades para evaluar los aprendizajes se determina en función de los objetivos y de las actividades de aprendizaje planeadas y diseñadas con antelación. Gil (2004, pp.108-109) identifica cinco tipos de actividades para evaluar los aprendizajes, en función del objetivo y del momento en que aparecen dentro del curso:

- Actividades de evaluación inicial. Sirven para identificar si el participante cuenta con los requisitos de conocimientos previos relacionados con el programa educativo.
- Actividades de evaluación formativa. Sirven para identificar si las situaciones de aprendizaje están propiciando que el participante construya y reconstruya sus conocimientos. Son útiles para que el participante pueda identificar los logros obtenidos y/o las dificultades que se le presentan para apropiarse de ese conocimiento.
- Actividades de evaluación integradoras. Permiten cerrar la unidad o módulo de conocimientos que se esté abordando.
- Actividades de evaluación sumativa. Proporcionan información sobre los resultados finales, es decir, evidencian y valoran los resultados o productos alcanzados por el estudiante.
- Actividades de autoevaluación. Proporcionan información sobre el propio aprendizaje, en el caso de que se respondan de manera correcta podrían convertirse en aprendizajes significativos, en caso contrario, pueden motivar para que estudie nuevamente el tema o busque información complementaria.

En los MOOC, las actividades de evaluación más frecuentes se encuentran:

- Cuestionarios. Se presentan regularmente entre 5 o 10 preguntas por video, material o módulo, según se plantee en el diseño y la secuencia de actividades. Proporcionan una evaluación y retroalimentación inmediata y de manera automática. Este tipo de actividad puede desarrollarse como actividad de evaluación inicial, formativa, integradora, sumativa o de autoevaluación.

- Actividades por pares. Son actividades que se pueden desarrollar al final de un módulo o como actividad de cierre del curso. Suelen ser proyectos, ensayos u otros relacionados con los contenidos del curso, en las que los estudiantes cargan un trabajo y revisan los trabajos de sus compañeros tomando como base una rúbrica en la que se debe establecer, de manera muy detallada, los criterios de evaluación.

2.3.4 Plataformas que ofertan MOOC

En la actualidad existen múltiples plataformas que ofertan MOOC, entre las más reconocidas se encuentran: Udacity, Coursera, edX, MiriadaX, FutureLearn, Canvas Network y Khan Academy.

Las primeras plataformas MOOC que comenzaron a desarrollarse fueron Udacity y Coursera, las cuales mediante la alianza entre universidades de prestigio y el cobro por el uso de dichas plataformas iniciaron este modelo educativo. Udacity y Coursera se constituyeron como empresas con fines de lucro, siendo apoyadas por inversionistas que ven en estos medios educativos oportunidades de negocio. Poco tiempo después, se aliaron la Universidad de Harvard y el Instituto Tecnológico de Massachussets (MIT) para comenzar a operar edX, una plataforma MOOC que a diferencia de las antes mencionadas se constituyó como una empresa sin fines de lucro, posibilitando así el acceso de hospedaje a un gran número de instituciones que, de otra forma, no hubieran podido sumarse a este creciente movimiento educativo (Mercado, R., 2016).

Figura 10

Plataformas MOOC

Udacity http://www.udacity.com/	Fue creada por Sebastián Thrun en 2012. Se estima que el número de usuarios registrados es de 400, 000. Sus cursos se especializan en nueve áreas: inteligencia artificial, sistemas autónomos, negocio, computación en la nube, seguridad cibernética, ciencia de datos, gestión de productos, programación, desarrollo y carrera profesional. Aunque la mayoría de sus cursos tienen costo, cuenta con cursos abiertos.

Coursera https://www.coursera.org/	Fue fundada en 2012 por los doctores Andrew Ng y Daphne Koller. De acuerdo con su *Reporte de impacto-Sirviendo al mundo a través del aprendizaje 2021*, la plataforma cuenta con 92 millones de estudiantes inscritos y más de 250 socios en todo el mundo.
edX https://www.edx.org/	Fue lanzada en 2012 por la Universidad de Harvard y el MIT. De acuerdo con su página oficial, la plataforma tiene 42 millones de usuarios inscritos, más de 160 socios y más de 3 600 cursos.

Nota: Elaboración propia. Fuente: Mercado, R., (2016). Cursos masivos abiertos en línea: oportunidad o amenaza. (p.54).

Entre las plataformas MOOC desarrolladas en Europa, se encuentran las que se muestran en la siguiente figura:

Figura 11

Iniciativas de plataformas MOOC en Europa.

FutureLearn	En Reino Unido, mediante la Open University. De acuerdo con su página oficial, la plataforma cuenta con más de 80 socios.
Miriada X	España mediante el apoyo de la asociación UNIVERSIA y el Banco Santander desarrollaron Miríada X
FUN MOOC https://www.fun-mooc.fr/fr/	Fue fundada en 2013 por el Ministerio de Educación Superior e Investigación de Francia y es operada por la France Université Numérique. Cuenta con más de 160 socios, quienes crean y ofrecen MOOC y SPOC.

Nota: Elaboración propia. Fuente: Mercado, R., (2016). Cursos masivos abiertos en línea: oportunidad o amenaza. (p.54).

La incursión de los cursos MOOC en latinoamericana tuvo lugar a través de las plataformas de Coursera, edX y Miríada X, aunque dentro de la región ya existen desarrollos propios, como los que se encuentran en la Figura 12.

Figura 12

Iniciativas de plataformas MOOC en Latinoamérica.

Veduca https://veduca.org/	Es una plataforma desarrollada en Brasil. Cuenta con más de 3 millones de usuarios inscritos.
México X https://mexicox.gob.mx/	Fue lanzada en 2015 por la Secretaría de Educación Pública (SEP) a través de la Dirección General de Televisión Educativa. Con base en los datos de su página oficial, la plataforma cuenta con 2.6 millones de usuarios inscritos y más de 70 instituciones aliadas.

Nota: Elaboración propia. Fuente: Mercado, R., (2016). Cursos masivos abiertos en línea: oportunidad o amenaza. (p.54).

2.3.5 ¿Por qué un MOOC para la capacitación docente?

Se plantea el diseño de un curso MOOC, porque la considero una alternativa viable para la capacitación docente al ofrecer los siguientes beneficios:

- Promover el autoaprendizaje de los participantes.
- Gestionar su ritmo de aprendizaje.
- Flexibilidad en cuanto a tiempo y espacio, ya que se puede estudiar desde cualquier lugar y horario sin la necesidad de desplazarse.
- Reducción de costos, tanto para la persona o institución que oferta el programa educativo como para los participantes.
- Masividad. Se busca que la información llegue a miles de personas, refiriendo de manera específica a docentes.

En este segundo capítulo, se trató de hacer evidente el papel fundamental de la alfabetización digital como el camino a través del cual las y los usuarios pueden desarrollar los conocimientos, habilidades y actitudes básicas para hacer frente a los riesgos del ciberespacio. Bajo esta perspectiva, la formación en competencias digitales es considerada como la principal herramienta con la que contamos para protegernos y hacer un uso eficiente de las TIC.

Con base en lo anterior, en el siguiente capítulo, se desarrolla la planeación de un MOOC como medio para la capacitación docente en competencias digitales, a fin de emprender acciones desde el ámbito formal qué promuevan competencias digitales en materia de ciberseguridad desde el aula.

Capítulo 3. MOOC. Ciberseguridad: prevención de riesgos desde el aula

En este tercer capítulo se presenta el guion instruccional que contiene la planeación del MOOC Ciberseguridad: prevención de riesgos desde el aula, el cual tiene como objetivo que las y los docentes identifiquen los riesgos más comunes a que se pueden enfrentar sus estudiantes al navegar en el ciberespacio, así como las medidas preventivas que desde el aula se pueden implementar para mitigarlos.

El guion instruccional se integra de los siguientes tres apartados:

1. Datos generales del curso. Se detallan aspectos relativos al nombre, duración, objetivo general, programa del curso, metodología de trabajo y criterios de evaluación.
2. Elementos generales del módulo. Se presenta el nombre, objetivo particular y temario del módulo.
3. Elementos de desarrollo del módulo. Se describen con detalle los contenidos de cada tema, los recursos a utilizar, actividades y material extra para reforzar lo aprendido.

3.1 Datos generales del curso

Nombre del curso:	Ciberseguridad: prevención de riesgos desde el aula	**Duración:**	15 horas
Diseñadora:	Marisol Sixto Marcos		
Público objetivo:	Docentes de educación básica de nivel primaria		
Requerimientos:	— Conocimientos básicos de TIC: - Usar navegadores y buscadores para realizar investigaciones - Comunicarse en entornos digitales - Manipular y crear archivos multimedia — Experiencia docente mínima de un año.		
Idioma:	Español		

<table>
<tr><td>Introducción general o presentación:</td><td colspan="2">Resulta innegable que el ciberespacio ha creado un escenario de múltiples oportunidades para todos, ya que nos permite comunicarnos, interactuar, acceder e intercambiar información, expresar opiniones, realizar compras, entre muchas otras. Sin embargo, también ha traído consigo retos en torno a la seguridad y el bienestar de la vida en línea y fuera de ella, sobre todo en lo que refiere a la población infantil, ya que este sector accede a edades cada vez más tempranas y pueden no entender de manera automática su vulnerabilidad ante los riesgos en línea, de ahí la necesidad de iniciar su formación en competencias digitales desde edades tempranas como factor de prevención.

En este curso conocerás los principales riesgos a que se enfrentan niñas y niños al navegar en el ciberespacio, con el fin de que conozcas y/o refuerces tus competencias digitales en materia de ciberseguridad y cuentes con las herramientas que te permitan integrar y promoverla dentro del aula, de esta forma tus estudiantes podrán aprovechar al máximo los beneficios de la tecnología.</td></tr>
<tr><td>Objetivo general:</td><td colspan="2">Al finalizar el MOOC, las y los docentes:
Identificarán los riesgos más comunes a que se pueden enfrentar sus estudiantes al navegar en el ciberespacio, así como las medidas preventivas que desde el aula se pueden implementar para mitigarlos.</td></tr>
<tr><td rowspan="3">Programa del curso:</td><td>Módulos</td><td>Temas</td></tr>
<tr><td>1. Explorando el ciberespacio</td><td>1.1 Introducción
1.2 Retos y oportunidades del ciberespacio para niñas y niños.
1.3 Principales conceptos de ciberseguridad.</td></tr>
<tr><td>2. Riesgos para los dispositivos</td><td>2.1 Introducción
2.2 ¿Cuáles son los riesgos más comunes y cómo prevenirlos?
2.2.1 Malware
2.2.2 Estafas</td></tr>
</table>

	3. Riesgos de contenido y manipulación	3.1 Introducción 3.2 ¿Cuáles son los riesgos más comunes y cómo prevenirlos? 3.2.1 Contenido agresivo, de odio y sexual 3.2.2 Salud, retos y actividades peligrosas 3.2.3 Noticias falsas
	4. Riesgos de contacto	4.1 Introducción 4.2 ¿Cuáles son los riesgos más comunes y cómo prevenirlos? 4.2.1 Grooming
	5. Riegos de conducta	5.1 Introducción 5.2 ¿Cuáles son los riesgos más comunes y cómo prevenirlos? 5.2.1 Cyberbullying 5.2.2 Sexting 5.2.3 Ciberdependencia
Metodología de trabajo:	A través de los cinco módulos que integran el curso, desarrollarás las siguientes actividades: — Lecturas breves — Videos con una duración de entre 2 y 10 minutos — Participación en foros — Revisión de materiales en enlaces externos — Cuestionarios de opción múltiple al finalizar cada módulo — Evaluación entre pares	
Criterios de evaluación:	Para acreditar el curso deberás realizar todas las actividades establecidas en la plataforma.	

3.1.1 Elementos generales del módulo 1

Título:	**1. Explorando el ciberespacio...**
Objetivo particular:	Identificar los principales conceptos relacionados con el ciberespacio y la ciberseguridad.
Temario:	1.1 ¿Qué es el ciberespacio? 1.2 Retos y oportunidades del ciberespacio para niñas y niños. 1.3 Principales conceptos de ciberseguridad.

3.1.2 Elementos de desarrollo del módulo 1

Temas	Recurso	Contenido
Introducción	*Video*	¿Sabías que todas las actividades que desarrollamos con el uso de Internet suceden dentro del ciberespacio? Pero, ¿sabes cuál es la diferencia entre estos dos términos o qué relaciones existen entre ellos? Para iniciar a explorar el ciberespacio, observaremos el siguiente video, en el cual podremos reconocer los principales elementos que nos permiten conectarnos e interactuar a través de este espacio virtual: https://www.youtube.com/watch?v=AIYtgDOjQX8
	Infografía	Como vimos en el video anterior, el ciberespacio es un concepto en el que se integran tecnologías, servicios, datos y usuarios, los cuales en interacción han generado un escenario que facilita el desarrollo de un sinfín de actividades en el mundo digital. Con el fin de tener una idea más clara de los elementos que integran el ciberespacio, observemos la siguiente infografía: https://i0.wp.com/informacionytic.com/wp-content/uploads/2019/03/ciberespacio.png?resize=670%2C415&ssl=1

Oportunidades y retos del ciberespacio	*Video*	Para iniciar con el tema observaremos el siguiente video que presenta las posibilidades y desafíos del ciberespacio para niñas y niños, desde la perspectiva de Mateo, un niño de 6 años: https://www.youtube.com/watch?v=C89i0rLuz34
	Texto	De acuerdo con el Global Kids Online (2019), las principales actividades que desarrollan niñas y niños en el ciberespacio, son: — Ver videos — Jugar en línea — Mantener contacto a través de redes sociales con amigas, amigos, familiares y con otras niñas o niños con los que tienen intereses comunes. — Crear contenidos (música, videos, blogs, páginas web, etc.) — Buscar información Si bien son muchas las oportunidades que el ciberespacio ofrece para que niñas y niños desarrollen nuevas habilidades dentro del mundo digital, también ha traído consigo retos en torno a la seguridad y el bienestar de la vida en línea y fuera de ella, ya que niñas y niños están expuestos a diversos riesgos que pueden afectarles, los cuales abordaremos con detalle en los siguientes módulos.
Principales conceptos de ciberseguridad	*Texto*	Para hacer frente a la diversidad de riesgos que suceden dentro del ciberespacio, surge y se desarrolla la ciberseguridad, la cual en términos generales refiere al conjunto de herramientas, tecnologías y acciones que se pueden utilizar para proteger las pertenencias o cosas de valor (activos) de las personas u organizaciones dentro del ciberespacio, tales como datos e información, identidad y reputación digital, programas y aplicaciones, hardware, etc. Si bien el término podría resultarnos complejo y lejano a nuestra realidad, la ciberseguridad está al alcance de todos y no requiere de grandes conocimientos técnicos, sino de un interés genuino para saber cómo protegernos y/o actuar frente a los riesgos que podemos encontrarnos al navegar por el ciberespacio. En el siguiente video podemos observar algunos conceptos y prácticas básicas relacionadas con la ciberseguridad para dar nuestros primeros pasos en el tema: https://www.youtube.com/watch?v=bv-h_omPJog&t=185s
	Texto	Con el fin de reforzar y de aprender nuevos conceptos relacionados con la ciberseguridad, revisaremos juntos el siguiente glosario: — Ciberseguridad

		— Dispositivos — Actualización — Software — Vulnerabilidad — Permisos — Contraseñas y bloqueo de pantalla — Información sensible o privada — Copia de seguridad — Antivirus — HTTPS

Actividad de evaluación integradora	*Cuestionario*	1. ¿Cuál de las siguientes opciones corresponde a la URL de una web segura? a. http://paginaweb.com b. https://paginaweb.com c. segura.paginaweb.com 2. Firefox, Google Chrome, Internet Explorer o Microsoft Edge son programas que tenemos instalados en nuestros dispositivos para acceder a Internet, pero ¿cómo se llaman estos programas? a. Buscadores b. Navegadores c. Antivirus 3. Si tenemos la sospecha de que nuestro ordenador está infectado y queremos arreglarlo, ¿qué debemos hacer? a. Analizarlo con un antivirus b. Reiniciarlo c. Dar clic en la advertencia que aparece en pantalla para descargar un antivirus y recuperar mi información. 4. Mecanismo para bloquear el acceso a los dispositivos que utiliza para verlo. algún elemento de nuestro cuerpo, como la huella dactilar o nuestro rostro. a. Contraseña b. Biometría c. PIN 5. Fallo de seguridad que sufre un programa informático y que puede ser aprovechado por los ciberdelincuentes. a. Infección b. Vulnerabilidad c. Smishing

3.1.3 Elementos generales del módulo 2

Título:	**2. Riesgos para los dispositivos y cómo prevenirlos**
Objetivo particular:	Identificar los principales riesgos para los dispositivos y las medidas básicas de prevención que se enfrentan niñas y niños en el ciberespacio.
Temario:	**2.1** Introducción **2.2** ¿Cuáles son los riesgos más comunes y cómo prevenirlos? 2.2.1 Malware 2.2.2 Estafas

3.1.4 Elementos de desarrollo del módulo 2

Temas	Recurso	Contenido
Introducción	*Texto*	¿Te ha pasado que tus dispositivos (celular, tablet o computadora) estén súper lentos, aparezcan recuadros negros en la pantalla, publicidad no deseada o que se abran múltiples ventanas en el navegador? Si tu respuesta al planteamiento anterior es sí, existe la posibilidad de que tus dispositivos hayan sido infectados por algún tipo de malware, los cuales tienen como fin robar, cifrar, borrar datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad sin el conocimiento o consentimiento del propietario. Quizá te preguntes, ¿cómo es que mi dispositivo se puede infectar o qué puedo hacer para evitar que esto ocurra? En este módulo, identificaremos todas aquellas actividades que pueden afectar la integridad de nuestros dispositivos y las buenas prácticas para mantenerlos en buen estado.

<table>
<tr>
<td></td>
<td>Test</td>
<td>¡Se ha detectado una amenaza!
Instrucciones:
Lee con atención cada una de las siguientes preguntas y responde sí o no, según tus prácticas en el uso y mantenimiento de tus dispositivos. Recuerda que no hay respuestas correctas o incorrectas.

<table>
<tr><th>Preguntas</th><th>Sí</th><th>No</th></tr>
<tr><td>1. ¿Tienes instalado algún antivirus en tus dispositivos?</td><td></td><td></td></tr>
<tr><td>2. ¿Revisas de manera periódica que todos tus dispositivos, aplicaciones y programas estén actualizados?</td><td></td><td></td></tr>
<tr><td>3. ¿Has descargado algún programa o aplicación ilegítima (pirata) alguna vez?</td><td></td><td></td></tr>
<tr><td>4. ¿Analizas con antivirus los programas antes de instalarlos en tus dispositivos?</td><td></td><td></td></tr>
<tr><td>5. ¿Al instalar una aplicación revisas atentamente los permisos que le concedes?</td><td></td><td></td></tr>
<tr><td>6. ¿Tienes activado algún mecanismo de bloqueo en tus dispositivos (contraseña, PIN, huella dactilar, etc.)?</td><td></td><td></td></tr>
<tr><td>7. ¿Las contraseñas que utilizas para tus cuentas están personalizadas para cada servicio y hacen uso alternado de mayúsculas, minúsculas, letras y caracteres especiales?</td><td></td><td></td></tr>
<tr><td>8. ¿Te has conectado a alguna red pública en el metro, parques, etc.?</td><td></td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td>Malware</td>
<td>Video</td>
<td>¿Qué es malware y qué tipos existen?
https://www.youtube.com/watch?v=HuasitV4lcw</td>
</tr>
</table>

	Texto	¿Qué acciones pueden promover que los dispositivos se infecten de programas maliciosos? - Descargar programas gratuitos de Internet - No actualizar los dispositivos digitales y los programas instalados en ellos - Visitar sitios web infectados - Conectarse a redes públicas - Dar clic en mensajes de error falsos o en ventanas emergentes - Abrir archivos adjuntos de un correo electrónico - No utilizar y/o actualizar nuestros programas antivirus - Utilizar contraseñas débiles
	Texto	¿Cómo proteger mis dispositivos? Te invitamos a visitar los siguientes enlaces en los que descubrirás buenas prácticas y tutoriales para proteger tus dispositivos de programas maliciosos. — Descargar programas y aplicaciones sin riesgo https://www.osi.es/es/actualidad/blog/2021/07/28/descargando-aplicaciones-sin-riesgos — Actualización de dispositivos, programas y aplicaciones https://www.osi.es/es/actualidad/blog/2021/07/28/aprende-mantener-actualizados-tus-dispositivos-programas-y-aplicaciones — Antivirus https://www.osi.es/es/actualidad/blog/2021/07/28/el-antivirus-es-necesario-pero-lo-tienes-funcionando — Contraseñas y seguridad en las cuentas https://www.osi.es/es/actualidad/blog/2021/07/28/bloqueo-de-dispositivos-por-que-es-importante En la siguiente infografía encontrarás los mejores tips para crear contraseñas seguras: https://www.osi.es/es/campanas/crea-tu-contrasena-segura

	Texto	¡Extra, extra! Para conocer más del tema y acceder a materiales que puedes utilizar para trabajar en el aula te recomendamos visitar los siguientes enlaces: — Contraseñas y seguridad en las cuentas https://www.osi.es/es/campanas/contrasenas-seguras
	Video	¿Qué es el phishing, smishing y vishing? https://www.youtube.com/watch?v=dQQHBMbKSAM
Estafa	*Texto*	¡Extra, extra! Para saber más acerca de este tipo de estafas, te invitamos a consultar los siguientes blogs con información más detallada de cómo identificarlos: — Phishing https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-phishing — Smishing https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-smishing — Vishing https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-vishing — Recursos para trabajar en el aula: https://www.schoolofsocialnetworks.org/es/proteger-tus-datos-y-dispositivos-profes/ https://n9.cl/cacef
	Texto	¿Qué hacer si eres víctima de una estafa? Recuerda que tienes a tu disposición los seguimientos mecanismos de atención: — Unidades de Policía Cibernética: https://ciberseguridad.ift.org.mx/reporte_ciudadano.php

		— Formulario de atención a la ciudadanía (Reportar incidentes cibernéticos): https://www.gob.mx/gncertmx?tab=Reporta%20un%20delito%20cibern%C3%A9tico
Actividad de evaluación integradora	*Cuestionario*	1. Luis está por comenzar sus clases en línea y requiere descargar la aplicación de Zoom, ¿cuál de las siguientes afirmaciones es la más segura para instalar dicha aplicación en su celular? a. Descargarla del primer sitio web de descargas gratuitas que aparezca en su búsqueda. b. Buscarla en la tienda oficial de su dispositivo móvil y descargar la primera opción. c. Buscarla en la tienda oficial de su dispositivo móvil y descargar la opción que corresponda con el fabricante original. 2. Mediante las actualizaciones nuestros dispositivos y los programas instalados en ellos, se actualizan a una mejor versión (sin fallos y más segura). Con base en lo anterior ¿cuál de las siguientes afirmaciones es correcta? a. No todas las actualizaciones son buenas. b. Debemos asegurarnos de disponer siempre de la última versión. c. Se actualizan automáticamente y no tenemos que preocuparnos. 3. De acuerdo con las buenas prácticas para generar contraseñas, ¿cuál de las siguientes cumple con los criterios de seguridad? a. 1234567890 b. IP3rr0grande11m% c. MS2005VHA0 4. Un correo ha llegado a tu bandeja de entrada. En el mensaje dice que es tu banco y que debido a una actividad sospechosa necesitas dar clic a un enlace que te direccionará a un formulario que deberás llenar para recuperar tu cuenta. ¿Qué harías? a. Haría clic en el enlace y seguiría los pasos. b. Ignoraría el mensaje. c. Llamaría a mi banco para comprobar el mensaje. 5. Imagina que te encuentras en una cafetería después de tu jornada laboral y, mientras esperas lo que ordenaste, recuerdas que no enviaste un correo urgente que contiene información confidencial de tu trabajo. ¿Qué harías? a. Conectarme a la red de la cafetería para enviar el correo urgente. b. Conectarme a una red gratuita para enviar solo el correo urgente.

		c. Utilizar mis datos móviles o esperar y usar la red de casa.

3.1.5 Elementos generales del módulo 3

Título:	**3. Riesgos de contenido y manipulación**
Objetivo particular:	Reconocer los principales riesgos a que son asequibles niñas y niños ante la diversidad y no regulación de todos los contenidos que circulan por el ciberespacio, así como las medidas que se pueden utilizar para evitar ser consumidores de contenido no deseado.
Temario:	**3.1** Introducción **3.2** ¿Cuáles son los riesgos más comunes y cómo prevenirlos? **3.2.1** Agresivo, racista y de odio. **3.2.2** Sexual **3.2.3** Salud **3.2.4** Noticias falsas

3.1.6 Elementos de desarrollo del módulo 3

Temas	Recurso	Contenido

Introducción	*Texto*	En el ciberespacio se puede acceder a un sinfín de contenidos, muchos de ellos explícitos, dado que no existe una regulación de todo lo que se publica y transmite en la red; bajo esta condición niñas y niños están expuestos a encontrar o acceder a contenido no deseado, inapropiado y/o delicado durante su interacción con el mundo digital. A lo anterior se suma el hecho de que no todo lo que vemos y leemos es 100% real, confiable o seguro, por ello, es relevante que niñas y niños aprendan a buscar información y entender la diferencia entre una opinión y un hecho contrastado. En este módulo, identificaremos aquellos contenidos que se consideran de riesgo, así como las medidas que se pueden utilizar para evitar ser consumidores de contenido no deseado.
Contenido agresivo, de odio y sexual	*Foro*	Observa con detalle los siguientes videos y responde: https://www.youtube.com/watch?v=sE-a_hAQmug https://www.youtube.com/watch?v=6K0wtyDl2u4 — ¿Consideras que es frecuente encontrar en redes sociales publicaciones o comentarios en que se burlen de una persona o grupo por su apariencia física, origen étnico, raza, orientación sexual, género, identidad de género, religión, discapacidad, etc.? — Sabías que Facebook sanciona a los usuarios que violan las normas de la comunidad, perdiendo la capacidad de comentar y publicar en periodos de tiempo que van de las 24 horas a los 30 días o, en casos más serios, perder sus cuentas de manera indefinida. ¿Consideras que medidas como las antes mencionadas ayudan a mitigar el problema? Si tu respuesta es no, ¿qué otras medidas consideras que son necesarias adoptar?

A continuación, encontrarás la breve descripción de algunos contenidos que se consideran inapropiados y/o delicados:

Contenido	Agresivo	Racista y de odio	Sexual
¿Qué es?	Material perturbador, que incentive a cometer actos específicos de violencia en contra de una persona o grupo; y aquellos que promuevan la ideología de grupos terroristas	Material que tiene como fin humillar, agredir o violentar a una persona o grupo, debido a su origen étnico o raza, orientación sexual, género, identidad de género, religión, discapacidad, entre otras.	Material explícito de desnudos, actos sexuales gráficos y/o material pornográfico.

Para saber más sobre estos tipos de contenidos y de aquello que se puede publicar o no en las plataformas, te invitamos a leer las Normas de comunidad aplicables a cada una de ellas, a través de los siguientes enlaces:

- TikTok:https://www.tiktok.com/community-guidelines?lang=es#34
- Facebook:https://transparency.fb.com/es-la/policies/community-standards/?source=https%3A%2F%2Fes-la.facebook.com%2Fcommunitystandards
- YouTube: https://support.google.com/youtube/answer/2801939?hl=es-419&ref_topic=9282436

	Texto	Si bien no podemos tener control sobre todos los contenidos que se transmiten en la red, podemos tomar determinadas medidas para mitigarlos. En el siguiente video encontrarás algunas medidas que, aunque se enmarcan en los contenidos de odio pueden aplicarse a otros contenidos de riesgo: https://www.youtube.com/watch?v=NmYkbdmOpuA * Evita la apología de cualquier tipo de violencia (publicar o compartir contenido que promueva el consumo de drogas y/o alcohol, imágenes de contenido sexual o poco apropiadas, etc.), discriminación o discursos de odio (hacia personas o grupos por razones de género, orientación sexual, raza, color de piel, etc.) en redes sociales, recuerda que todas nuestras interacciones dejan huella e influyen en nuestra identidad y reputación digital.
	Video	Si bien no podemos tener control sobre todos los contenidos que se transmiten en la red, podemos tomar determinadas medidas para mitigarlos. En el siguiente video encontrarás algunas medidas que, aunque se enmarcan en los contenidos de odio pueden aplicarse a otros contenidos de riesgo: https://www.youtube.com/watch?v=NmYkbdmOpuA * Evita la apología de cualquier tipo de violencia (publicar o compartir contenido que promueva el consumo de drogas y/o alcohol, imágenes de contenido sexual o poco apropiadas, etc.), discriminación o discursos de odio (hacia personas o grupos por razones de género, orientación sexual, raza, color de piel, etc.) en redes sociales, recuerda que todas nuestras interacciones dejan huella e influyen en nuestra identidad y reputación digital.

Salud, retos y actividades peligrosas	*Foro*	Observa con detalle los siguientes videos y responde: https://www.youtube.com/watch?v=WHoXAw5_gcw https://www.youtube.com/watch?v=clHZtWVVGZI — ¿Has visto materiales que promueven o inciten a prácticas de autolesión, suicidio y trastornos alimenticios en redes sociales? — ¿Consideras que las advertencias utilizadas en redes sociales sobre que determinadas prácticas están hechas por profesionales y que no debes intentarlas son suficientes para que niñas y niños desistan de intentarlas?
	Texto	¡Extra. extra! Para conocer más del tipo de contenido que se puede publicar o no en las plataformas, te invitamos a leer las Normas de comunidad aplicables a cada una de ellas. A continuación, te dejamos tres de las más utilizadas: — TikTok:https://www.tiktok.com/community-guidelines?lang=es#34 — Facebook:https://transparency.fb.com/es-la/policies/community-standards/?source=https%3A%2F%2Fes-la.facebook.com%2Fcommunitystandards — YouTube: https://support.google.com/youtube/answer/2801939?hl=es-419&ref_topic=9282436
Noticias falsas	*Video*	Recurres a alguna de las siguientes prácticas cuando navegas por el ciberespacio: ¿Al buscar información utilizas la que aparece en el primer sitio web de tu buscador sin contrastarla con otras fuentes? ¿Al navegar por redes sociales o internet lees solo los encabezados de las noticias o artículos periodísticos y generas opiniones sin conocer de fondo el contexto? En los siguientes videos, encontrarás algunos tips para no caer en el anzuelo de la desinformación y de las noticias falsas (también conocidas como *fake news*): https://www.youtube.com/watch?v=71FwZ5OQaw8 https://www.youtube.com/watch?v=7YkD8jwdU-M
	Texto	¡Extra. extra! Para conocer más del tema y acceder a materiales que puedes utilizar para trabajar en el aula te recomendamos visitar los siguientes enlaces:

		— https://storage.googleapis.com/gweb-interland.appspot.com/es-419-all/hub/pdfs/Google_SeGenialEnInternet_ElPlanDeEstudios2019.pdf (pp.50-56) — https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/como-combatir-las-fake-news-2022-02-28_es

3.1.7 Elementos generales del módulo 4

Título:	**4. Riesgos de contacto**
Objetivo particular:	Identificar los principales riesgos de contacto y las medidas de prevención.
Temario:	**4.1** Introducción **4.2** ¿Cuáles son los riesgos más comunes y cómo prevenirlos? **4.2.1** Ciberacoso **4.2.2** Grooming **4.2.3** Otros… (grupos extremistas/publicidad/compras)

3.1.8 Elementos de desarrollo del módulo 4

Temas	Recurso	Contenido
Introducción	*Texto*	Internet y el ciberespacio han configurado la manera en que se entienden y se gestan las relaciones interpersonales, la expresión personal y la privacidad. Las redes sociales como uno de los principales canales de comunicación han sido utilizadas por niñas y niños como un medio de ocio para chatear con sus amigas y amigos, visualizar y publicar fotografías,

		videos, entre muchas otras actividades benéficas para su desarrollo personal y social, sin embargo, no disponer de los conocimientos necesarios para gestionar la privacidad y las relaciones interpersonales, a través de estos medios, pueden exponerlos a ser contactados por extraños (generalmente adultos) y establecer comunicaciones de riesgo.
Grooming	*Foro*	**¿Quién está detrás de la pantalla?** Observa con detalle los siguientes videos y responde: https://youtu.be/QcChhpy-KzM https://www.youtube.com/watch?v=pAohWiuNPYo — ¿Conoces en persona a todos los contactos que agregas en redes sociales?, ¿crees que tus estudiantes tomen sus precauciones y eviten el contacto con desconocidos en redes sociales? — ¿A que riesgos se exponen niñas y niños al entrar en contacto con un desconocido?
	Video	Exposición temática — ¿Qué es grooming? https://www.youtube.com/watch?v=QgDh0ukHjoQ
	Infografía	Componentes y fases del grooming: https://farodigital.org/wp-content/uploads/2019/10/Guia-Provincia.pdf (p.40)
	Video	¿Qué hacer ante un caso de grooming? https://www.youtube.com/watch?v=zTFhSsR74Qs
	Texto	¡Extra. extra! Para conocer más del tema y acceder a materiales que puedes utilizar para trabajar en el aula te recomendamos visitar los siguientes enlaces: — https://farodigital.org/wp-content/uploads/2019/10/Guia-Provincia.pdf (pp.37-47)

Actividad de evaluación integradora	*Análisis de casos*	Lee con atención los siguientes casos y con base en las medidas de prevención que vimos en el módulo responde a los planteamientos: Caso 1. María recibe un mensaje directo en IG de @chicovoley12, alguien a quien no sigue y con quien tiene solamente dos contactos en común. "¡Hola! Me encantan tus publicaciones. ¡Eres SÚPER divertida! ¿Me das tu número de teléfono para que podamos conversar?" ¿Qué recomendaciones o consejo le darías? Caso 2. Isabel, una chica de 13 años, mantenía conversaciones con un chico que conoció por IG. Pasados tres meses del primer contacto, ella comenzó a recibir fotos del chico desnudo (que en realidad era un hombre mayor) e instigaciones para que ella le enviará fotos desnuda. ¿Qué debería hacer Isabel?

3.1.9 Elementos generales del módulo 5

Título:	**5. Riesgos de conducta**
Objetivo particular:	Identificar los principales riesgos de conducta en los que niñas y niños se pueden ver inmiscuidos como víctimas o perpetradores dentro del ciberespacio.
Temario:	5.1 Introducción 5.2 ¿Cuáles son los riesgos más comunes y cómo prevenirlos? 5.2.1 Cyberbullying 5.2.2 Sexting 5.3.2 Ciberdependencia

3.1.10 Elementos de desarrollo del módulo 5

Temas	Recurso	Contenido
Introducción	*Texto*	El anonimato y la viralidad son dos de las características del ciberespacio que han incentivado a niñas y niños a perpetrar actos que tienen como fin dañar a coetáneos suyos. Con respecto al anonimato, niñas y niños se sienten protegidos y con la libertad de hacer comentarios hirientes o cometer agresiones sin ningún límite, ya que su identidad está oculta detrás de una pantalla y por la facilidad con que se puede crear cuentas y perfiles falsos. En lo que refiere a la viralidad, ésta puede ser particularmente perturbadora y dañina, ya que los materiales (imágenes, videos o mensajes hirientes o de carácter sexual) se pueden comunicar a terceras personas de manera instantánea y tener un alcance inimaginable. En este módulo, identificaremos algunas de las actividades de riesgo en que se pueden ver inmiscuidas niñas y niños, así como las medidas preventivas y de acción para mitigarlos.
Ciberbullying	*Foro*	Observa con detalle el video y responde a los planteamientos que aparecen a continuación: https://www.youtube.com/watch?v=Ds3GP7ypzes — ¿Consideras que debe existir un marco de actuación para las y los docentes dentro de las instituciones educativas para atender casos de esta índole? — ¿Qué actividades consideras que como docente puedes realizar para prevenir y/o afrontar situaciones de ciberbullying dentro del salón de clases o de la institución en que laboras?
	Video	¿Qué es el cyberbullying? https://www.youtube.com/watch?v=GRfQnuDKRsA ¿Qué tipos existen? https://www.youtube.com/watch?v=C3iugyohGmk
	Video	¿Cómo prevenir el ciberbullying? https://www.youtube.com/watch?v=ZHQ03fSn9J0

	Infografía	¿Qué hacer en caso de ciberbullying? https://www.afavordetic.com/_files/ugd/b73e04_7d96759a486c45f380d3eb01b71e9c7a.pdf A continuación, encontrarás un directorio con los teléfonos, sitios web y redes sociales de las Unidades de Policía Cibernética de cada estado. Si requieres de asesoría o reportar un incidente cibernético, comunícate con la Unidad que corresponda a tu localidad: https://ciberseguridad.ift.org.mx/reporte_ciudadano.php
	Texto	¡Extra, extra! Para conocer más del tema y acceder a materiales que puedes utilizar para trabajar en el aula te recomendamos visitar los siguientes sitios web: — https://www.afavordetic.com/ciberbullying — https://www.youtube.com/watch?v=g19n5WA2cfw — https://farodigital.org/wp-content/uploads/2019/10/Guia-Provincia.pdf (pp. 16-27)
Sexting	*Foro*	La imagen se vuelve contra ti Lee con atención la noticia y observa el video para responder a los siguientes planteamientos: https://www.afavordetic.com/_files/ugd/b73e04_28d996a3adab4e8e805d141d2f04965a.pdf https://www.youtube.com/watch?v=TqRbo9JzaLY — ¿Te suenan familiares las historias presentadas? ¿Conoces algún caso como estos? — ¿Consideras que el sexting es un problema grave? Argumenta tu respuesta.
	Video	¿Qué es sexting y cuáles son sus consecuencias? https://www.youtube.com/watch?v=7mZp2OI9hgo

	Infografía	¿Cómo prevenir el sexting? — No te tomes fotos provocativas. ¡Cuida tu intimidad! ¿Has decidido sextear? Toma en cuenta las siguientes recomendaciones: https://www.sextingseguro.com/consejos-sextear-nudes-con-menos-riesgos/ — En caso de acoso, guarda evidencias y denuncia. Recuerda que tienes a tu disposición los seguimientos mecanismos de atención: Unidades de Policía Cibernética: https://ciberseguridad.ift.org.mx/reporte_ciudadano.php Formulario de atención a la ciudadanía (Reportar incidentes cibernéticos): https://www.gob.mx/gncertmx?tab=Reporta%20un%20delito%20cibern%C3%A9tico — Configura tu privacidad en redes sociales y evita contactar con desconocidos. En el siguiente documento, encontrarás una guía con pasos detallados para configurar tus cuentas en Instagram, Facebook, WhatsApp y TikTok: https://www.argentina.gob.ar/sites/default/files/configuracion_de_privacidad_en_redes_sociales.pdf — Si recibes fotos o videos con imágenes sexuales de niñas, niños y adolescentes, no los difundas y reportalos. Recuerda que, en redes sociales, sitios de videos o blogs, existen opciones de denuncia y bloqueo de imágenes. — No incites, ni presiones a otros a crear contenido de este tipo.
	Texto	¡Extra. extra! Para conocer más del tema y acceder a materiales que puedes utilizar para trabajar en el aula te recomendamos visitar los siguientes enlaces: — https://www.afavordetic.com/sexting — https://farodigital.org/wp-content/uploads/2019/10/Guia-Provincia.pdf (pp. 28-36)
Ciberdependencia	*Test*	**¿Qué tan dependiente soy de la tecnología?** **Instrucciones:** Lee con atención cada una de las siguientes preguntas y selecciona el inciso que más se acerque a tu respuesta. Recuerda que no hay respuestas correctas o incorrectas. 1. ¿Te regresas a casa si dejas el celular, aunque ya hayas salido y estés lejos?

a. Siempre
b. A veces
c. Nunca

2. ¿Si llega una notificación la atiendes inmediatamente?
    a. Siempre
    b. A veces
    c. Nunca
3. ¿Pasas más tiempo frente a las pantallas que haciendo deporte, tocando algún instrumento, jugando con hermanos o amigos?
    a. Siempre
    b. A veces
    c. Nunca
4. ¿Si no tienes una pantalla en tus manos, no sabes cómo entretenerte? ¿Sientes que te aburres?
    a. Siempre
    b. A veces
    c. Nunca
5. ¿Tienes siempre contigo un cargador por si se te acaba la batería?
    a. Siempre
    b. A veces
    c. Nunca
6. ¿Al despertar lo primero que haces es ver tu celular?
    a. Siempre
    b. A veces
    c. Nunca
7. ¿Mientras te bañas, usas los dispositivos para ver videos, películas, series o simplemente escuchar música?
    a. Siempre
    b. A veces
    c. Nunca
8. ¿Llevas tu celular contigo para ir al baño, sino que vas a hacer mientras haces del baño?
    a. Siempre

		b. A veces c. Nunca 9. ¿Lo último que haces antes de dormir es ver el celular? a. Siempre b. A veces c. Nunca
	Video	¿Qué es ciberdependencia? https://www.youtube.com/watch?v=jxmIF1KZdc4 Riesgos de la ciberdependencia https://www.afavordetic.com/_files/ugd/b73e04_fea6c56d7bb84ffe8124997395137c63.pdf
	Texto	Consecuencias 1.Falta de concentración 2.Fracaso escolar o laboral 3. Aislamiento o pérdida de las relaciones sociales 4. Alteraciones en la conducta (agresividad, rompimiento de normas y mentiras) 5. Sensación de abstinencia cuando no se está conectado (irritabilidad y ansiedad) 6. Disminución de las horas de hábitos saludables diarios, como dormir, comer, higiene, etc. 7. Baja calidad de vida
	Texto	Prevenir la ciberdependencia, ¿aceptas el reto? https://docs.google.com/document/d/1sVf-JPQp-FQRv0-qL7wgWXjJOI3aG9mwQZAxOYSgJao/edit?usp=sharing
	Texto	¡Extra, extra! Para conocer más del tema y acceder a materiales que puedes utilizar para trabajar en el aula te recomendamos visitar los siguientes enlaces: — https://www.afavordetic.com/ciberdependencia

	Cuestionario	1. Carlos constantemente mira las redes sociales y siente insatisfacción al comparar sus logros con los de sus contactos. ¿A qué riesgo de la ciberdependencia corresponde este síntoma? a. Nomofobia b. Editiovultafobia c. Taxiedad 2. ¿Cuál de las siguientes no es una buena práctica para practicar sexting? a. Evitar el uso de redes públicas para el envío o recepción de imágenes. b. Excluir de la imagen o video partes que puedan ayudar a reconocer tu identidad (rostro, marcas corporales, objeto, etc.). c. Evitar guardar las imágenes en el dispositivo y subirlas a la nube para mayor seguridad. 3. El sexting puede derivar en otros riesgos, como: a. Cyberbullying, sextorsión, grooming, daños a la huella digital, etc. b. Chantaje, bullying, ciberdependencia, etc. c. Grooming, sextorsión, malware, daños a la huella digital, etc. 4. ¿Cuáles de las siguientes características definen el cyberbullying? a. Son comportamientos agresivos practicados entre iguales a través de medios digitales b. Tiene como fin dañar a otro y se vale de prácticas, como humillación, insultos, amenazas, denigración, suplantación de identidad, etc. c. Todas las anteriores 5. La profesora de civismo creó un blog sobre la clase y otorgó permiso a los estudiantes para que escribieran, editarán y publicarán comentarios. Al día siguiente, la profesora se ausenta y el suplente no se da cuenta de que hay un conflicto en el blog, ya que alguien está publicando comentarios muy

		agresivos sobre uno de los estudiantes de la clase. ¿Cuál de las siguientes acciones es la más acertada para que los estudiantes afronten la situación? a. Responder a los comentarios con frases como: "Esto no es correcto". "Yo soy amigo de _____y eso no es verdad". b. Ignorar el conflicto hasta que regrese la profesora. c. Pedir a los demás estudiantes que publiquen comentarios agradables y elogios sobre la víctima. d. Avisar al suplente que alguien se está comportando de forma agresiva en el blog, y debería informarle a la profesora.
Mensaje de finalización del curso	*Texto*	¡Felicidades por concluir el curso Ciberseguridad: prevención de riesgos desde el aula! Ahora está en ti dar el siguiente paso para concientizar a tus estudiantes o el ignorar lo que has aprendido y permitir que tus estudiantes sigan expuestos a numerosas situaciones de riesgo en el ciberespacio. Aventúrate y comienza a desarrollar esta experiencia desde el aula, ayuda a tus estudiantes a conocer las bases de la ciberseguridad, a informarse y llevar a cabo las mejores prácticas para que puedan aprovechar al máximo las ventajas de la tecnología.

Conclusiones

La propuesta aquí desarrollada pretende contribuir a los esfuerzos que se han desarrollado a nivel nacional para fomentar el uso seguro y responsable de la tecnología entre la población infantil, partiendo del supuesto que, "el 80% de los ciberdelitos podrían evitarse con medidas básicas de prevención" (Policía Federal, 2018, p. 32). Lo anterior desde el papel fundamental que para ello pueden tener los docentes.

En el primer capítulo se planteó la problemática que dio origen a este trabajo. Se presentaron los principales riesgos a que están expuestas las personas, especialmente niñas y niños, se definió qué es y cuáles son los elementos que integran la ciberseguridad; y se describieron las acciones que se han desarrollado a nivel nacional, regional e internacional para contribuir al desarrollo de un ciberespacio seguro ante el crecimiento exponencial de los riesgos, amenazas y delitos, en relación con el uso cada vez más extensivo de la tecnología.

Si bien creemos que la ciberseguridad es un tema complejo y muy distante de nuestra realidad, ésta se pone en juego en muchas de las actividades que realizamos cotidianamente de manera consciente o inconsciente al hacer uso de nuestros dispositivos e internet, las cuales pueden ir desde descargar aplicaciones piratas, hasta tener encuentros con personas de redes sociales que quizá no conocemos en persona y que pueden derivar en una amenaza a nuestra integridad física y mental, entre muchas otras.

La situación antes descrita, nos insta a intervenir sobre dicha realidad a fin de buscar los medios que permitan a los usuarios tomar conciencia de los riesgos y la responsabilidad que se debe asumir al navegar en el ciberespacio, sobre todo en lo que refiere a la población infantil, ya que este sector accede a edades cada vez más tempranas y pueden no entender de manera automática su vulnerabilidad ante los riesgos de la vida digital.

En el segundo capítulo se trató de hacer evidente el papel fundamental de la alfabetización digital como el camino a través del cual las y los usuarios pueden desarrollar los conocimientos, habilidades y actitudes básicas para hacer frente a dichos riesgos. Bajo esta perspectiva, la formación en competencias digitales es considerada como la principal herramienta con la que contamos para protegernos y hacer un uso eficiente de las TIC.

Si bien esta formación puede resultar nueva para algunos, no se trata de haber descubierto el hilo negro, sino el de desarrollar nuevas propuestas a través de las cuales se sistematice el trabajo que se ha venido realizando y buscando los medios y espacios para hacerlas posibles, de ahí que en el presente trabajo se haya plateado un MOOC como medio para la capacitación docente en competencias digitales y como espacio de actuación el ámbito formal de la educación, ya que como se vio durante el primer capítulo muchas de las acciones que se han desarrollado a nivel nacional, se han gestado desde el ámbito no formal.

Lo anterior respondió a una de las recomendaciones de la UNICEF de que los "docentes deben ser capaces de desarrollar sus propias [competencias] para apoyar el uso de las TIC por parte de sus alumnos y ayudarlos a desarrollar una comprensión del uso seguro de Internet más allá del aula" (2017, pp.32-33). Bajo esta perspectiva, las y los docentes tienen como misión ayudar y acompañar a sus estudiantes para que entiendan cómo funciona el ciberespacio, cuáles son los riesgos a que están expuestos y fomentar entre ellos buenas prácticas para hacer un uso responsable y eficiente de las TIC.

Considero importante resaltar que la ciberseguridad está al alcance de todos y no requiere de grandes conocimientos técnicos, sino de un interés genuino para saber cómo protegerse y/o actuar frente a los riesgos del ciberespacio.

En el tercer capítulo, se presentó la planeación del MOOC a través de un guion instruccional, en el que se concretó la propuesta del curso, el cual tiene como objetivo que las y los docentes identifiquen los principales riesgos a que se pueden enfrentar sus estudiantes al navegar por el ciberespacio y las medidas que desde el aula se pueden implementar para mitigarlos.

Con lo antes descrito, es posible denotar que el curso tiene un carácter primordialmente preventivo, sin embargo, también es posible localizar en él elementos para la detección de riesgos y medidas de reacción para saber cómo actuar en caso de ser víctima. Es importante mencionar que aun cuando los riesgos y amenazas se buscan mitigar a través de medidas como a la argüida en este trabajo, no es una solución total y definitiva, ya que éstos siguen creciendo en sofisticación y a mayor velocidad que las soluciones que se intentan desde los diversos niveles de la sociedad (políticas, leyes, programas de educación y/o capacitación, etc.).

Construir esta propuesta me permitió como pedagoga identificar los retos que supone la integración de una intervención educativa a través del uso de las TIC, las cuales van desde la capacidad para detectar una necesidad, investigar sobre ella y buscar alternativas de solución, hasta la capacidad creativa y de planeación que se requiere para diseñar ambientes virtuales de aprendizaje que faciliten y promuevan los procesos de enseñanza y aprendizaje.

Como pedagogas y pedagogos es fundamental desarrollar un sentido crítico que nos posibilite identificar las diversas problemáticas que afectan a nuestra sociedad, a fin de buscar soluciones coherentes y viables desde nuestro campo de actuación. Respecto a este último punto, la pedagogía nos permite incidir en muchos otros campos, como la tecnología, la salud, la ecología y la economía por mencionar algunos.

En el caso específico de este trabajo, me centré en el sector tecnológico, un ámbito que crece y envuelve nuestra realidad, diluyendo cada vez más la línea entre nuestra vida *online* y *offline*. Son múltiples los retos que la tecnología nos plantea en la actualidad, los cuales hacen patente la necesidad urgente de que las personas adquiramos a través de la educación y/o capacitación las competencias digitales que nos ayuden a prepararnos para afrontar los desafíos actuales y los venideros que se derivaran de los avances tecnológicos que están emergiendo.

Referencias

A favor de TIC. (2016). *Conócenos*. Recuperado de: https://www.afavordetic.com/about

Arcos, R. (2019). *Elaboración de un MOOC para el desarrollo de la competencia digital en docentes de matemáticas*. http://dspace.casagrande.edu.ec:8080/bitstream/ucasagrande/1823/1/Tesis1999ARCe.pdf

Asociación de Internet MX. (2021). *17° Estudio sobre ciberseguridad en empresas, usuarios de Internet y padres de familia en México 2021.* Recuperado de: https://www.asociaciondeinternet.mx/estudios/habitos-de-internet

Avast. (2016). ¿Qué es un gusano informático? Recuperado de: https://www.avast.com/es-es/c-computer-worm

Avast. (2020). Exploits: todo lo que debe saber. Recuperado de: https://www.avast.com/es-es/c-exploits

Avast. (2021). ¿Qué es un malware troyano? Guía definitiva. Recuperado de: https://www.avast.com/es-es/c-trojan

Avast. (2021). ¿Qué es un rootkit y cómo se elimina? Recuperado de: https://www.avast.com/es-es/c-rootkit

Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA). (2020). *Reporte de Ciberseguridad 2020. Riesgos, avances y el camino a seguir en América Latina y el Caribe.* Recuperado de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Cabero, J., Llorente, M. y Vázquez, A. (2014). *Las tipologías de MOOC: Su diseño e implicaciones educativas.* Profesorado-Revista de curriculum y formación del profesorado, Vol. 18, núm.1, pp. 13-26. https://www.redalyc.org/pdf/567/56730662002.pdf

Chiavenato, I. (2011). *Administración de recursos humanos. El capital humano de las organizaciones.* McGrawHill Educación. https://www.sijufor.org/uploads/1/2/0/5/120589378/administracion_de_recursos_humanos_-_chiavenato.pdf

Código Penal Federal. (2021). Diario Oficial de la Federación, México. Última reforma 12-11-2021. Recuperado de: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

COMEXI y McKinsey & Company. (2018). *Perspectiva de ciberseguridad en México.* Recuperado de: https://consejomexicano.org/multimedia/1528987628-817.pdf

Congreso de los Estados Unidos Mexicanos (2019). *Ley General del Servicio Profesional Docente*. https://legislacion.scjn.gob.mx/buscador/paginas/wfArticuladoFast.aspx?q=O2BTSgJ7ydpYoSMwf6C6nuROYaIRPS/czg0HvmTWsdRtAIAMbR29BK+OrfQgFtntDwOueWRTx0uuC5L/jiDbpg

Coordinación General @prende.mx. (2020). *3,000 docentes serán capacitados en materia de 'Ciudadanía Digital', a través del programa Sé Genial en Internet*. Recuperado de: https://www.gob.mx/aprendemx/articulos/la-coordinacion-general-prende-mx-google-y-robotix-suman-esfuerzos-para-promover-la-ciudadania-digital-responsable-y-segura?idiom=es

Dirección General de Formación Continua a Docentes y Directivos –SEP. (20229. *Estrategia Nacional de Formación Continua 2022.* Recuperado de: http://dgfc.basica.sep.gob.mx/multimedia/2022/Docs/ENFC_2022.pdf

Flores, L. (2019). *Alianza del Pacífico se compromete a fortalecer la ciberseguridad.* El Universal. Recuperado de: https://www.eluniversal.com.mx/cartera/alianza-del-pacifico-se-compromete-fortalecer-la-ciberseguridad

Fondo de las Naciones Unidas para la Infancia (UNICEF). (2017). *Estado mundial de la infancia 2017-Niños en un mundo digital.* Recuperado de: https://www.unicef.org/sowc2017/

Fondo de las Naciones Unidas para la Infancia (UNICEF). (s/f). *Conoce los distintos tipos de riesgos en línea*. Recuperado de: https://ciberconscientes.com/identifica-los-distintos-tipos-de-riesgos-en-linea/#:~:text=Los%20riesgos%20de%20contacto%20y,riesgos%2C%20con%C3%B3celos%20a%20detalle%20aqu%C3%AD.

Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en un mundo digital*. Editorial: Ariel. Recuperado de: https://www.fundaciontelefonica.com/cultura-digital/publicaciones/531/#close

García, S. (2017). Alfabetización Digital. Nuevos escenarios de la comunidad educativa Razón y Palabra, Vol.21, Núm. 98, pp. 66-81. https://1library.co/document/zxv40x4y-alfabetizacion-digital.html.

GFC Global (s/f). Virus informáticos y antivirus. Recuperado de: https://edu.gcfglobal.org/es/virus-informaticos-y-antivirus/que-es-un-virus-informatico/1/#

Gil, M. (2004). Modelo de diseño instruccional para programas educativos a distancia. Horizontes, vol. XXVI, núm. 104, pp. 93-114.: http://www.scielo.org.mx/pdf/peredu/v26n104/v26n104a6.pdf

Guardia Nacional. (2022). *Guardia Nacional inicia la jornada 2022. Internet seguro para todas y todos.* Recuperado de: https://www.gob.mx/guardianacional/prensa/guardia-nacional-inicia-la-jornada-2022-internet-seguro-para-todas-y-todos

Guardia Nacional-CERT-MX (2021). *7a. Semana Nacional de la Ciberseguridad de la GN.* Recuperado de: https://www.gob.mx/gncertmx/articulos/114554

Instituto Federal de Telecomunicaciones (IFT). (2015). *Ciberseguridad*. Recuperado de: https://ciberseguridad.ift.org.mx/reporte_ciudadano.php

Instituto Nacional de Estadística y Geografía (INEGI). (2022). Módulo sobre ciberacoso 2021. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/mociba/MOCIBA2021.pdf

Instituto Nacional de Normalización (INN). (2015). *ISO 27032-Tecnologías de la información-Técnicas de seguridad- Directrices para la ciberprotección.* Recuperado de: https://www.trusttech.cl/docs/nch.27032.pdf

Instituto Nacional para la Evaluación de la Educación. (INEE). (2018). *Formación continua de docentes: política actual en*

Interpol (s/f). Criptojacking, Recuperado de: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Cryptojacking

Lladós, G., Cargnelutti, J. y Oviedo, M. (s/f). *Guía práctica para hacer un MOOC.* https://rdu.unc.edu.ar/bitstream/handle/11086/16169/Guia%20MOOC%209%20%281%29.pdf?sequence=1&isAllowed=y.

Machín, N y Gazapo, M. (2016). *La ciberseguridad como factor crítico en la seguridad de la Unión Europea.* UNISCI, Núm. 42, pp. 47-68. Recuperado de: https://www.redalyc.org/articulo.oa?id=76747805002.

Malwarebytes (s/f). Ransomware. Recuperado de: https://es.malwarebytes.com/ransomware/

Malwarebytes. (s/f). *Malware*. Recuperado de: https://es.malwarebytes.com/malware/

Martínez, H. (2021). La integración de las TIC en instituciones educativas en Carneiro, R., Toscano, J. y Díaz, T. Los desafíos de las TIC para el cambio educativo. Fundación Santillana. https://www.oei.es/uploads/files/microsites/28/140/lastic2.pdf

Matamala, C. (2018). *Desarrollo de alfabetización digital ¿Cuáles son las estrategias de los profesores para enseñar habilidades de información?* Perfiles Educativos, Vol. 40 Núm. 162, pp. 68-85.: https://perfileseducativos.unam.mx/iisue_pe/index.php/perfiles/article/view/58846/52079.

Mercado, R. (2016). *Cursos masivos abiertos en línea: oportunidad o amenaza.* Universidades, Núm. 70, pp. 53-68. http://www.redalyc.org/articulo.oa?id=37348529005.

México y buenas prácticas nacionales e internacionales. https://www.inee.edu.mx/wp-content/uploads/2018/12/P1F226.pdf

Núñez, J. y Rodríguez, M. (s/f). *El desafío de alfabetizar en el siglo XXI: dimensiones y propuestas en torno a la alfabetización.* https://journals.ucjc.edu/VREF/article/view/4094/3007.

Observatorio de Innovación Educativa del Tecnológico de Monterrey. (2014). *Reporte EduTrends. MOOC.* https://observatorio.tec.mx/edutrendsmooc

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) y Unión Internacional de Telecomunicaciones (UIT). (2019). *Seguridad de los niños en línea: Minimizando el riesgo de la violencia, el abuso y la explotación en línea 2019*. Recuperado de: https://unesdoc.unesco.org/ark:/48223/pf0000374580

Park, Y. (2019). *DQ Global Standards Report 2019. Common Framework for Digital Literacy, Skills and Readiness*. Recuperado de: https://www.dqinstitute.org/wp-content/uploads/2019/11/DQGlobalStandardsReport2019.pdf

Pilli, O. y Admiraal, W. (2016). *A Taxonomy of Massive Open Online Courses.* Contemporary Educational Technology, 7(3), pp. 223-240. https://www.cedtech.net/download/a-taxonomy-of-massive-open-online-courses-6174.pdf.

Policía Federal. (2018). *Prevención del delito cibernético*. Recuperado de: https://www.infosecuritymexico.com/content/dam/sitebuilder/rxmx/intra-logistics/PDF/presentacione_2018/infosecurity2018_ArturoGome_PF.pdf

Procuraduría Federal del Consumidor. (2021). *La "Ley Olimpia" y el combate a la violencia digital.* Recuperado de: https://www.gob.mx/profeco/es/articulos/la-ley-olimpia-y-el-combate-a-la-violencia-digital?idiom=es

Robles, J. (2011). Ciudadanía digital: Una introducción al nuevo concepto de ciudadano. Barcelona: UOC.

Secretaría de Comunicaciones y Transportes (SCT). (2019). *Hábitos de los usuarios en ciberseguridad México 2019*. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

Travieso, J. y Planella, J. (2008). *La alfabetización digital como factor de inclusión social: una mirada crítica.* UOC Papers-Revista sobre la sociedad del conocimiento. https://www.uoc.edu/uocpapers/6/dt/esp/travieso_planella.pdf.

UNESCO. (2021). *Día Internacional de la Alfabetización. Seminario web-Alfabetización para una recuperación centrada en las personas: reducir la brecha digital*. https://en.unesco.org/sites/default/files/ild-2021-concept-note-agenda-es.pdf.

UNICEF. (2017). *Estado mundial de la infancia 2017-Niños en un mundo digital.* https://www.unicef.org/sowc2017/

Unión Internacional de Telecomunicaciones (UIT). (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad.* Recuperado de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

Unión Internacional de Telecomunicaciones (UIT). (2020) a. *Directrices sobre la protección de la infancia en línea para los encargados de formular políticas 2020.* Recuperado de: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-S.pdf

Unión Internacional de Telecomunicaciones (UIT). (2020) b. *Protección de la infancia en línea: Guía para padres y educadores 2020.* Recuperado de: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.EDUC-2020-PDF-S.pdf

Universidad Veracruzana (2015). ¿Qué es un Adware y cómo se pasa a nuestros equipos de cómputo y móviles? Recuperado de: https://www.uv.mx/infosegura/general/noti_adware/

Vázquez, R. y Cotto, J. (2017). *La importancia de la capacitación docente. Centro de Excelencia Académica.* https://cea.uprrp.edu/la-capacitacion-docente-y-su-importancia/