Libro blanco

La ciberseguridad de las mujeres durante la pandemia del COVID-19:

Experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital

OEA | Más derechos para más gente

Contenidos

Créditos

Luis Almagro
Secretario General
Organización de los Estados Americanos (OEA)

Arthur Weintraub
Secretario de Seguridad Multidimensional
Organización de los Estados Americanos (OEA)

Alison August Treppel
Secretaria Ejecutiva
Comité Interamericano contra el Terrorismo (CICTE)

Alejandra Mora Mora
Secretaria Ejecutiva
Comisión Interamericana de Mujeres (CIM)

Equipo Técnico de la OEA
Programa de Ciberseguridad
Kerry-Ann Barrett
Mariana Cardona
Mariana Jaramillo
Gabriela Montes de Oca Fehr

Comisión Interamericana de Mujeres /
Mecanismo de Seguimiento de la Convención de Belém do Pará
Luz Patricia Mejía Guerrero
Alejandra Negrete Morayta

Autora
Katya N. Vera Morales

Diseño y Diagramación
Michelle Felguérez

01 Objetivos

> *El incremento acelerado de los procesos de digitalización y transformación tecnológica ha sido una de las características más notables de la evolución de pandemia d el COVID-19, cuya gestión ha propiciado la construcción de un ecosistema digital en el que nuevas identidades, experiencias e interacciones están surgiendo, multiplicándose y transformándose a gran escala.*

Si bien es cierto que el cibercrimen, el abuso y la violencia digital significaban ya un problema mundial antes de la pandemia, estas nuevas condiciones han creado nuevas oportunidades para agresores y ciberdelincuentes, quienes durante esta etapa aumentaron en número y alcance sus ataques, replicando viejas técnicas y al mismo tiempo innovando en sus estrategias.

Desde marzo de 2020, diversos estudios a nivel global y regional se han dado a la tarea de identificar las tendencias y características de las amenazas en línea y los retos que se enfrentan en materia de ciberseguridad en el nuevo ecosistema digital. Un recorrido por tales estudios revela, sin embargo, que se ha colocado poca atención a las experiencias digitales de las mujeres en el marco de las crecientes vulnerabilidades un el espacio digital, persistiendo una falta de análisis con perspectiva de género sobre la gama de peligros cibernéticos que enfrentan y los impactos de la cibercriminalidad en sus vidas.

Esta falta de análisis de género ejemplifica lo que sucede a gran escala en el ámbito de la ciberseguridad, en donde prevalece aún un entendimiento de las tecnologías y los peligros cibernéticos como neutrales al género y, por tanto, sin impactos diferenciados en función de las identidades y expresiones de género de las personas (Millar et al, 2021: 8).

En este contexto, diversas voces en el ámbito de la academia, sociedad civil y foros multilaterales han iniciado a subrayar la necesidad de analizar las dimensiones de género de la ciberseguridad a fin de generar una mejor comprensión de las dinámicas que conforman la política y la práctica en este sector, surgiendo en años recientes declaraciones oficiales, estrategias para el desarrollo de capacidades e investigaciones que están abriendo camino en el tema.

Sumándose a estos signos de cambio, la presente publicación tiene por objeto contribuir al diálogo en torno a los vínculos entre la ciberseguridad y las normas y roles de género durante esta época crítica para el ciberespacio, presentando **un marco de análisis para la identificación de posibles vulnerabilidades y riesgos que enfrentan las mujeres**[1] en el nuevo ecosistema digital.

Para ello, se propone un **análisis del escenario de ciberataques** surgido a propósito de la crisis sanitaria **en conjunto con las dinámicas de acceso** y uso del internet por parte de las mujeres, así como de las **condiciones de desigualdad de género** sistémicas que inciden dentro y fuera de línea, a fin de identificar algunas **amenazas cibernéticas que les estarían afectando específicamente durante esta etapa.**

[1] Se destaca que, por cuestiones de espacio, el presente documento se enfoca únicamente en las experiencias diferenciadas de las mujeres en el ámbito de la ciberseguridad, si bien se reconoce la urgencia de traer a la conversación las experiencias en línea y los peligros cibernéticos que enfrentan actualmente otros colectivos marginados a partir de su identidad o expresión de género y sexual, así como impulsar el desarrollo de análisis que permitan revelar de forma detallada el impacto en la seguridad cibernética de la intersección entre el género y otros factores de discriminación y exclusión.

Este marco de análisis busca aportar elementos de utilidad para profesionales y responsables de políticas públicas de ciberseguridad en el contexto de las estrategias puestas en marcha para proteger a las personas en línea durante la crisis sanitaria. Asimismo, se ha utilizado como base para la delimitación de **un bloque de medidas básicas de seguridad digital cuya adopción es importante promover en la nueva normalidad digital.** Esto último bajo la premisa de que no basta con identificar posibles vulnerabilidades y peligros cibernéticos sino que, además, se requiere normalizar el autocuidado digital como parte de las estrategias para empoderar a las mujeres en el uso seguro de las nuevas tecnologías.

El estudio de las dimensiones de género de las normas, políticas y estrategias de ciberseguridad es un campo de exploración en plena transformación y cuyos avances indudablemente marcarán la pauta para un mejor entendimiento del ciberespacio. Con ello en mente, el presente documento busca contribuir con ideas para la reflexión que está en marcha, reconociendo el gran potencial que conlleva traer una mirada de género al sector y el impacto de fenómenos mundiales como la COVID-19 en aspectos puntuales de la industria.

02 Los impactos de la epidemia de COVID-19 en el ecosistema digital

La pandemia de COVID-19 ha significado un punto de inflexión en el uso del ciberespacio, el cual se ha convertido en el principal escenario común global. A partir de marzo de 2020, la crisis sanitaria conllevó la adopción de medidas de confinamiento para reducir la propagación del virus, manteniendo a una gran parte de la población mundial dentro de sus hogares y con reducida capacidad de desplazamiento físico. Ante este confinamiento forzado, de forma abrupta nos vimos en la necesidad de re-imaginar nuestras sociedades y modificar aspectos básicos de nuestras prácticas cotidianas, adoptando en la marcha nuevas estrategias individuales y colectivas para paliar los efectos de la crisis sanitaria.

Más que nunca, los gobiernos se han apoyado de las tecnologías para proteger y preservar la salud pública, mantener el funcionamiento de la economía y para acercar los servicios públicos a la ciudadanía, digitalizando aceleradamente sus procesos administrativos y de gestión, y brindando soluciones digitales en las áreas de salud, educación, comercio y trabajo. De igual forma, empresas, universidades, bancos, agencias internacionales, iglesias, organizaciones y grupos de todo tipo, naturaleza y tamaño han implementado herramientas y plataformas virtuales para migrar al ciberespacio sus actividades basadas previamente en la presencialidad física[2].

A nivel individual, nos hemos volcado también al ciberespacio en un esfuerzo por contrarrestar el aislamiento y mantener cercanía digital con familiares y amistades a pesar de la separación física, buscando preservar esa sensación de normalidad que desapareció con la llegada de la pandemia. Hasta la web hemos trasladado gran parte de nuestras actividades laborales, educativas, comerciales, de entretenimiento y relacionales[3], reforzando aún más aquella continuidad *online-offline* que ya se observaba en las interacciones humanas desde antes del advenimiento de la pandemia.

[2] De acuerdo con la Comisión Económica para América Latina y el Caribe (CEPAL), entre abril y marzo de 2020, el incremento del número de sitios web empresariales fue del 800% en Colombia y México, y alrededor del 360% en el Brasil y Chile. En México y Brasil el número de sitios nuevos de comercio electrónico aumentó en abril más del 450% en comparación con el mismo mes de 2019, y los sitios con presencia activa en Colombia y México aumentaron cerca del 500%. Véase: Comisión Económica para América Latina y el Caribe (CEPAL) (2020). Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19.

[3] En Europa, por ejemplo, el uso de internet para actividades de ocio, interacción en redes sociales o plataformas de televisión de paga se incrementó hasta tal punto que la Unión Europea solicitó a Netflix y HBO la reducción del bitraje de su contenido para evitar la saturación de la red. Véase: José García (12 marzo 2020). "Netflix reducirá la calidad del contenido para evitar saturar la red a petición de la Unión Europea". https://www.xataka.com/streaming/netflix-reducira-calidad-contenido-para-evitar-saturar-red-a-peticion-union-europea. Consultado el 1° de febrero de 2021.

Las tecnologías han permitido conectar a las personas afectadas con las autoridades y organismos de asistencia, actuando como un canal para la expresión de sus necesidades, preocupaciones y experiencias (UIT, 2020b: 17). Durante esta contingencia, ha quedado más claro que nunca que el acceso al internet ya no es un mero lujo, sino una línea de vida con el exterior y un derecho humano que habilita el ejercicio de otros derechos fundamentales como el derecho a la salud, educación, cultura y libertad de expresión (Agudelo et al, 2020: 3).

En el caso de mujeres y niñas, la acelerada digitalización durante la pandemia ha permitido romper con prejuicios y estereotipos en género que, por mucho tiempo, las han mantenido alejadas de las tecnologías digitales. Para una parte de ellas, esta ha sido una etapa en que la que por primera vez han explorado nuevas herramientas y plataformas de internet ante la necesidad de mantenerse conectadas, incursionando en el uso de servicios financieros digitales, compras por internet, procesos de escolarización a distancia y actividades empresariales en línea. El periodo de confinamiento ha motivado también su activa participación en debates digitales, la creación de lazos con nuevas comunidades de mujeres en línea, y les ha permitido implementar nuevas formas de teletrabajo para conciliar sus responsabilidades laborales y familiares.

En conjunto, este cambio de prácticas sociales durante la pandemia ha implicado modificaciones profundas en el ciberespacio. Desde marzo de 2020 se han registrado cifras récord del tráfico de internet a nivel mundial, alcanzando en ciertos países un incremento de entre 50% y 70%[4]. De acuerdo con la Comisión Económica para América Latina y el Caribe de las Naciones Unidas (CEPAL), en la región latinoamericana, durante el primer trimestre de 2020, el teletrabajo aumentó 324%, la educación en línea más del 60%, el comercio electrónico 157%, el *livestreaming* 12% y la banca electrónica 7% (CEPAL, 2020).

Al día de hoy no se tiene claridad sobre cuánto más durará la crisis sanitaria del COVID-19 y las medidas de distanciamiento físico, pero es claro que la digitalización llegó para quedarse y que será un elemento crucial de la 'nueva normalidad'. Durante esta etapa, el uso acelerado (y forzado en muchos casos) de herramientas digitales ha traído consigo una sensación de mayor comodidad en el uso de estas por parte de mujeres y hombres, y es de esperarse que una vez pasada la crisis las personas optarán por utilizar el internet para más cosas que antes.

A. Los riesgos en el nuevo ecosistema digital

> *El incremento exponencial a nivel mundial en el uso de la tecnología para mitigar el impacto de las medidas de combate de la crisis sanitaria ha significado también un gran desafío para el ecosistema digital, revelando fallas estructurales tanto en el acceso a internet como en la seguridad en línea.*

A medida que mujeres y hombres han volcado sus actividades al ciberespacio, se ha registrado un crecimiento exponencial del nivel de exposición a riesgos en línea debido a la falta de familiaridad con el uso a gran escala de las Tecnologías de la Información y la Comunicación (TIC) y a la carencia generalizada de conocimientos sobre ciberamenazas y herramientas de protección y seguridad digital.

[4] Mark Beech (25 marzo 2020). "COVID-19 Pushes up internet use 70% and streaming more than 12%, first figures reveal". https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=36a6e4ab3104. Consultado el 1° de febrero de 2021.

Más personas en línea con pocos conocimientos en ciberseguridad (y exponiéndose a más riesgos en línea de lo que lo harían usualmente en la escuela o en su centro de trabajo), ha configurado un escenario propicio para atacantes y ciberdelincuentes, quienes se han aprovechado rápidamente de esta 'nueva normalidad' digital explotando el miedo y la incertidumbre generadas por la pandemia y el deseo de información de la población (UNODC, 2020)[5].

Según lo han reportado diversas fuentes, los ciberdelitos han tenido un incremento directamente proporcional a la transformación digital iniciada en marzo de 2020, y para finales de ese mes todos los países habían recibido por lo menos un ciberataque temático de COVID-19[6]. La Organización de las Naciones Unidas (ONU) advirtió un aumento desde el inicio de la pandemia de 600% en los correos electrónicos maliciosos y 350% en los sitios electrónicos falsos, produciéndose un ciberataque aproximadamente cada 39 segundos[7]. En Estados Unidos, de acuerdo con información del Internet Complaint Centre (IC3) del FBI, se cuadruplicaron las quejas interpuestas sobre ciberdelitos[8], y en el caso de América Latina, se reportó un aumento de 74% de delitos cibernéticos durante la pandemia[9], más de 20.5 millones de ataques cibernéticos a personas usuarias en el hogar y 1.2 millones de ataques a dispositivos móviles entre enero y septiembre de 2020[10].

De acuerdo con análisis sobre las repercusiones del COVID-19 en la ciberdelincuencia realizados por agencias como la Oficina de Naciones Unidas contra las Drogas y el Delito (UNODC), la Organización Internacional de Policía Criminal (INTERPOL) y la Oficina Europea de Policía (EUROPOL), entre los ciberataques más comunes observados desde marzo de 2020 se encuentran el uso de métodos de ingeniería social, estafas por internet y campañas de *phishing*, la infiltración de malware en dispositivos electrónicos, la creación de sitios web falsos, sextorsión facilitada por las TIC, ataques a través de herramientas de trabajo remoto, la desinformación en línea y el uso del *Dark Web* para actividades criminales[11].

[5] Trend Micro (11 noviembre 2020). "Developing Story: COVID-19 Used in Malicious Campaigns". https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains. Consultado el 1° de febrero de 2021.

[6] News Center Microsoft Latinoamérica (16 junio 2020). "Explotar una crisis: Cómo se comportaron los cibercriminales durante el frote". https://news.microsoft.com/es-xl/explotar-una-crisis-como-se-comportaron-los-cibercriminales-durante-el-brote/. Consultado el 1° de febrero de 2021.

[7] Business Standard (7 agosto 2020). "UN reports sharp increase in cybercrime during coronavirus pandemic". https://www.business-standard.com/article/technology/un-reports-sharp-increase-in-cybercrime-during-coronavirus-pandemic-120080700289_1.html; Phil Muncaster (1° abril 2020). "Cyber-Attacks up 37% over past months as #COVID19 bites". https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/. Consultado el 1° de febrero de 2021.

[8] Maggie Miller (16 abril 2020). "FBI sees spike in cybercrime reports during coronavirus pandemic". The Hill. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cybercrime-reports-during-coronavirus-pandemic

[9] Unisys. Unisys Security Index. https://www.unisys.com/unisys-security-index; Mundo Contact (1° julio 2020). "Cibercrimen aumenta 74% en AL durante la pandemia". https://mundocontact.com/cibercrimen-aumenta-74-en-al-durante-pandemia/. Consultado el 1° de febrero de 2021.

[10] Para septiembre de 2020, se reportó un incremento exponencial de ciberataques en toda la región latinoamericana, con Argentina, Brasil y México como los países con mayor riesgo. Véase: Agencia EFE (30 septiembre 2020). "Argentina, Brasil y México, más vulnerables al cibercrimen en Latinoamérica". https://www.efe.com/efe/america/tecnologia/argentina-brasil-y-mexico-mas-vulnerables-al-cibercrimen-en-latinoamerica/20000036-4355566. Consultado el 1° de febrero de 2021.

[11] Para mayor detalle sobre las características de los ciberataques más comunes durante la pandemia de COVID-19 véase: Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) (2021), Twitter Alfabetismo y Seguridad Digital. Mejores prácticas en el uso de Twitter. https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-seguridad-digital-Twitter.pdf . Véase también: Oficina de Naciones Unidas para la Droga y el Delito (UNODC) (14 abril 2020). Cibercrime and Anti-Money Laundering Section. "Cybercrime and COVID19: Risks and Responses". https://www.unodc.org/documents/Advocacy-Section/EN_-UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf; INTERPOL (4 agosto 2020). "Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19". https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19; EUROPOL (5 octubre 2020). "Internet Organised Crime Threat Assessment (IOCTA)". https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020; Consejo de Europa (27 marzo 2020). "Cybercrime and COVID-19". https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19; INTERPOL, "COVID-1a Cyberthreat". https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats. Cibersecurity & Infraestructure Security Agency (8 abril 2020). "UK and US Security Agencies Issue COVID-19 Cyber Threat Update". https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update. Consultado el 1° de febrero de 2021. Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) (2021), Twitter es Alfabetismo y Seguridad Digital. Mejores prácticas en el uso de Twitter. https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-seguridad-digital-Twitter.pdf

Esta lista de ciberdelitos es, por supuesto, ejemplificativa de lo que está sucediendo en los espacios digitales y es previsible que las amenazas continúen evolucionando conforme se modifiquen las condiciones de la pandemia del COVID-19. Sin embargo, es importante notar que el incremento en el cibercrimen observado durante los últimos meses no es algo accidental. En muchos casos, **el COVID-19 ha simplemente intensificado los problemas preexistentes en materia de ciberseguridad,** dejando entrever el alto grado de vulnerabilidad y de exposición a riesgos en línea de las personas.

El nuevo contexto ha hecho evidente la paradoja tecnológica que enfrentamos desde hace unos años: **la gran mayoría de las personas están utilizando la tecnología sin tener plena conciencia de los riesgos y las consecuencias de su uso,** quienes para satisfacer sus necesidades de conectividad desestiman fácilmente que el internet puede ser un campo fértil para agresores y ciberdelincuentes.

B. Distintos contextos, distintos riesgos cibernéticos

> *Estar al tanto de las tendencias generales que ha adoptado la cibercriminalidad en tiempos del COVID-19 es crucial para conocer los potenciales riesgos y peligros cibernéticos que las personas enfrentan y enfrentarán en la nueva normalidad digital y las posibles medidas de seguridad digital a implementar.*

No obstante, al considerar esta radiografía del nuevo ecosistema digital es necesario también tener presente que las experiencias en línea de las personas, incluyendo su nivel de **exposición a amenazas y los ciberdelitos** que les afectan, no son uniformes o unívocas, sino que **varían dependiendo de los contextos personales y de factores sociales** tales como el género, la ubicación geográfica, la edad, el nivel educativo u origen étnico.

Si bien persiste aún cierto idealismo basado en la neutralidad de la web, lo cierto es que conforme avanza la digitalización es cada vez más claro que el ciberespacio no es el mismo para todas las personas ni está separado de los problemas sociales fuera de línea. La era tecnológica ha puesto de relieve que las personas no son seres unidimensionales, sino que existe una continuidad entre sus realidades *online-offline*. Esto cual implica que sus identidades y los roles sociales que desempeñan fuera de línea se trasladan también al ciberespacio, condicionando sus experiencias e interacciones digitales y, por tanto, los riesgos cibernéticos que enfrentan.

A partir de ello, un entendimiento integral de las necesidades de seguridad digital durante esta época de crisis conlleva necesariamente el reconocimiento de que el mundo *online* es un reflejo de las realidades *offline*, y que las tecnologías digitales replican (y potencialmente profundizan) el contexto en el que las personas viven fuera de línea.

Bajo esta premisa, y a fin de poder identificar los posibles riesgos cibernéticos que las mujeres están enfrentando durante esta época, en las siguientes líneas se abordará **cómo el género**[12] **de las personas condiciona los efectos de la pandemia del COVID-19 en el ciberespacio y la cibercriminalidad,** bajo el entendido de que incorporar esta perspectiva resulta una tarea ineludible para la conformación de estrategias de seguridad digital que resulten realmente efectivas durante esta época de cambios acelerados.

[12] El género se refiere a los roles, comportamientos, actividades, y atributos que una sociedad en una época determinada considera apropiados para hombres y mujeres, así como a las relaciones entre mujeres y hombres. Estos atributos, oportunidades y relaciones son construidos socialmente y aprendidos a través del proceso de socialización, y son específicas al contexto o época y cambiantes. El género determina qué se espera, qué se permite y qué se valora en una mujer o en un hombre en un contexto determinado. Véase: UN Women, Important Concepts Underlying Gender Mainstreaming. https://www.un.org/womenwatch/osagi/pdf/factsheet2.pdf

03 ¿Cómo habitan las mujeres la nueva normalidad digital? Un análisis bajo una perspectiva de género del ecosistema digital surgido a partir de la epidemia del COVID-19

> Se ha comprobado que existen **marcadas diferencias entre el tipo de ciberdelitos, abuso y violencia que se cometen en línea contra las mujeres en comparación con aquellos que afectan a los hombres,** cuyas manifestaciones adoptan formas específicas y generan impactos diversos en función de su género (Millar, Shires y Tropina, 2021; Brown y Pytlak, 2020).

Si bien el reconocimiento de estas diferencias ha ido ganando terreno en el ámbito de la ciberseguridad, a casi un año de iniciada la crisis sanitaria, **aún son escasos los análisis con una perspectiva de género sobre los impactos de la pandemia en la cibercriminalidad.** A la fecha, los estudios sobre las amenazas cibernéticas en contra de las mujeres se han concentrado en las distintas formas de violencia de género en línea que han surgido o aumentado durante la pandemia, dejando fuera los otros riesgos y ataques que estas enfrentan en el ciberespacio. Esta carencia de datos impide, desafortunadamente, conocer con certeza cómo están viviendo las mujeres y las niñas el incremento en los niveles del cibercrimen durante este periodo crítico.

En atención a este vacío, en este apartado se destacan algunos elementos a tomar en consideración al momento de desarrollar un análisis con una perspectiva de género sobre las amenazas cibernéticas que enfrentan las mujeres en la nueva normalidad digital, con lo cual se espera contribuir a un mejor entendimiento sobre lo que está ocurriendo en el ciberespacio.

En términos generales podemos decir que adoptar un enfoque o perspectiva de género implica analizar el impacto que tienen las características biológicas y de género de las personas en sus interacciones, oportunidades y roles sociales, y develar las dinámicas de desigualdad y diferencias de poder entre hombres y mujeres[13].

En consecuencia, traer esta **perspectiva al ámbito de la ciberseguridad permite revelar cómo las experiencias en línea de las personas y las amenazas cibernéticas y daños que enfrentan son distintos dependiendo de su identidad de género y orientación sexual.** Asimismo, también se expone **cómo las relaciones entre hombres y mujeres y la desigualdad de género pueden influir en cuestiones tales como los usos y riesgos en el internet.** Esta mirada de género implica formularse preguntas tales como:

[13] "El enfoque de género es una forma de mirar la realidad identificando los roles y tareas que realizan los hombres y las mujeres en una sociedad, así como las asimetrías, relaciones de poder e inequidades que se producen entre ellos. Permite conocer y explicar las causas que producen esas asimetrías y desigualdades, y a formular medidas (políticas, mecanismos, acciones afirmativas, normas, etc.) que contribuyan a superar las brechas sociales de género". Rworld. Glosario de términos relacionados al enfoque de igualdad de género. https://www.refworld.org.es/pdfid/5af1c8114.pdf

¿De qué forma habitan los hombres y las mujeres el ciberespacio y cuáles son los riesgos específicos que enfrentan?

¿Cuáles son las experiencias de las mujeres y niñas en el contexto actual de la cibercriminalidad?

¿Cuáles son los daños diferenciados que sufren las mujeres ante ciberataques?

Implementar esta perspectiva también devela un punto a considerar: las tecnologías digitales no son neutras, sino que, por el contrario, el género de las personas influye y condicionan el acceso, el uso que se le da al internet y los riesgos que se viven en él. Estas son diferencias que se mantienen a lo largo de las distintas etapas de vida y que interactúan con otras determinantes sociales tales como el grado educativo, la edad, ubicación, el nivel socioeconómico, la orientación sexual o el origen étnico de hombres y mujeres.

Como lo ha reconocido la Organización Mundial de la Salud (OMS), **los impactos de las pandemias nunca son neutrales al género de las personas** y, por tanto, los planes estratégicos mundiales y nacionales de preparación y respuesta frente al COVID-19 deben basarse en un sólido análisis de género y en la forma en que este interactúa con otras esferas desigualdad (OMS, 2020). Esta afirmación se extiende, por supuesto, a los impactos que la pandemia está teniendo en el ciberespacio, y a las políticas y medidas de ciberseguridad que deben adoptarse para frenar el actual surgimiento acelerado de amenazas en línea y ciberdelitos.

Consecuentemente, traer un análisis de género al nuevo ecosistema digital propiciado por la pandemia del COVID-19 permitirá identificar los diferentes patrones de exposición a ciberamenazas que están enfrentando hombres y mujeres y las medidas de seguridad digital más adecuadas para protegerles.

Con ello en mente, **en las siguientes líneas se propone un marco de análisis** conformado por tres componentes que permiten develar las experiencias diferenciadas de las mujeres en el internet así como sus necesidades especiales. Estos componentes son básicos para conocer el nivel de vulnerabilidad y los tipos de riesgos ante los cuales se podrían estar enfrentando en el nuevo ecosistema digital. Estos tres componentes son:

UNO — **Las condiciones en las que las mujeres acceden al ciberespacio.**

DOS — **La desigualdad de género y los impactos online-offline de la pandemia del COVID-19.**

TRES — **Los usos que las mujeres le dan al internet.**

A. ¿Qué obstáculos enfrentan las mujeres para habitar el ciberespacio? Las brechas digitales de género

> *El primer elemento a considerar al momento de analizar los impactos diferenciados de las ciberamenazas en las mujeres es el hecho de que* ***estas no gozan en pie de igualdad de un acceso pleno y de calidad al internet ni de los conocimientos necesarios*** *para protegerse y aprovechar todo lo que este puede ofrecerles.*

La pandemia del COVID-19 ha puesto en evidencia las consecuencias devastadoras que puede tener para las personas el contar con un inadecuado o nulo acceso a la red, quienes sin esta vía de contacto e información quedan más vulnerables al virus, desconectadas de sus seres queridos y segregadas de las estrategias gubernamentales para contrarrestar la crisis. Desafortunadamente, este es el escenario que enfrentan millones de mujeres y niñas en el mundo que aún no tienen un acceso adecuado a la web (Brown y Pytlak, 2020).

Si bien se ha reportado que las mujeres utilizan con cada vez más frecuencia el internet, las brechas digitales de género[14] persisten en múltiples niveles. De acuerdo con los últimos reportes de la Unión Internacional de Telecomunicaciones (UIT), 51% de la población a nivel mundial (aproximadamente 4 billones de personas) se encontraban en línea en 2019[15]. De ellas, solo **48% de las mujeres tenían acceso a internet en comparación con 55% de los hombres, lo cual en términos relativos significa que la brecha mundial de género es de 17% (UIT, 2020).** Además, la UIT informó que en países de renta baja y media, las mujeres tienen 10% menos probabilidades que los hombres de tener un teléfono móvil (UIT, 2020b), lo cual conlleva impactos importantes al ser este el medio más utilizado de acceso a internet[16].

[14] El término brecha de género se refiere a cualquier disparidad entre la condición o posición de los hombres y mujeres en la sociedad. Son las diferencias de oportunidades, acceso, control y uso de los recursos construidas con base en las diferencias biológicas, y producto histórico de actitudes y prácticas discriminatorias que obstaculizan el goce y ejercicio de los derechos por parte de hombres y mujeres.

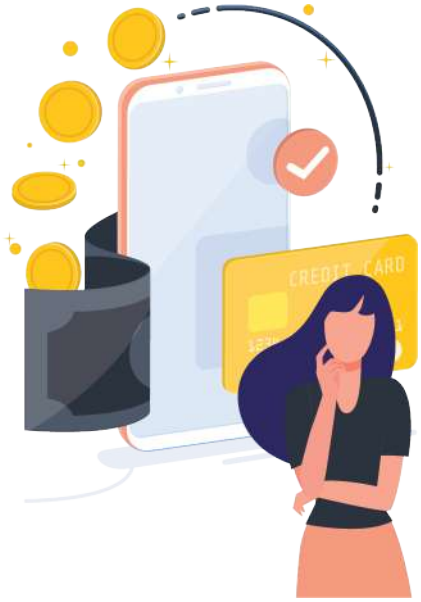
[15] La UIT identificó en 2020 importantes brechas de conectividad que persisten en las áreas rurales de los países en desarrollo. Globalmente, 72% de los hogares en áreas urbanas tienen internet frente al 38% en las áreas rurales.
En cuanto a la conectividad a nivel regional, la CEPAL indicó que en 2019 67% de los hogares urbanos estaban conectados a internet, mientras que sólo 23% de las zonas rurales estaban conectadas.
Por su parte, el Banco Interamericano de Desarrollo (BID) identificó que en el periodo comprendido entre 2017 y 2018, el porcentaje de acceso a internet en América Latina y el Caribe fue del 63% para los hombres y 57% para las mujeres, mientras que el uso del teléfono móvil fue del 80% para mujeres y 83% para hombres. La World Wide Web Foundation ha reportado también que los hombres tienen 21% más probabilidades de estar en línea que las mujeres, elevándose al 52% en los países menos desarrollados del mundo. Véase: World Wide Web Foundation (2020). The gender gap in internet access: using a women-centred method. https://webfoundation.org/2020/03/the-gender-gap-in-internet-access-using-a-women-centred-method/. Consultado el 1° de febrero de 2021; CEPAL (2020). Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19; BID (2020). ¿Desigualdades en el Mundo Digital? Brechas de Género en el Uso de las TIC.

[16] Se ha documentado también que los niños tienen 1.5 veces más probabilidades de tener un teléfono que las niñas. Véase: Jessica Posner Odede (2 agosto 2019). "Yes, technology can liberate girls around the world-but it must be managed properly". World Economic Forum. https://www.weforum.org/agenda/2019/08/getting-girls-online-first-step-achieving-gender-equality/. Consultado el 1° de febrero de 2021.

No debe perderse de vista que esta brecha de acceso básico a internet es parte de una brecha digital de género mucho mayor que involucra todas las formas en las que las mujeres son menos capaces de usar e influir en la tecnología, y que se ve agudizada por la conjunción con otros factores de exclusión como el nivel educativo, la ubicación geográfica, edad, nivel socioeconómico u origen étnico (Chair et al, 2020).

Se ha documentado que las mujeres y niñas no sólo sufren de una mayor desconexión del mundo digital sino que, cuando estas acceden a internet, no cuentan con una conectividad significativa[17] y alcanzan un mayor porcentaje de analfabetismo digital, lo cual implica que poseen menos habilidades para entender, controlar y generar vínculos de confianza con la tecnología[18]. Además, en comparación con los hombres, **las mujeres poseen un nivel más bajo de competencias en materia de seguridad digital,** lo cual impacta profundamente en el goce y ejercicio de sus derechos humanos en línea, y en su posibilidad de navegar con libertad y autonomía en la web (Chair et al, 2020).

Existen también **limitaciones de tiempo y contenido que las mujeres enfrentan al acceder a internet** (Brown y Pytlak, 2020). Por ejemplo, estudios indican que las mujeres tienen 25% menos probabilidades que los hombres de saber cómo aprovechar la tecnología digital para realizar tareas básicas (UIT, 2020b: 13)[19], y, en general, es exiguo su uso del internet con fines de empoderamiento económico o para el ejercicio de sus derechos (Chair et al, 2020). Las mujeres también permanecen ajenas al comercio en línea y al dinero móvil, estimándose que representan 56% de las personas excluidas financieramente de la economía digital[20]. Además, dado que estas tienen a su cargo la mayor parte del trabajo doméstico y de cuidados no remunerado, frecuentemente disponen de menos tiempo para explorar el ciberespacio y entrenarse para desarrollar nuevas habilidades digitales, y suelen ceder el uso de los dispositivos electrónicos a otros miembros de la familia cuando hay un número limitado en casa.



Estas brechas en el acceso y uso de internet y en el nivel de competencias y cultura digital propician la perpetuación de desigualdades de género, incluyendo desigualdades relacionadas con la pobreza informacional, puesto que **"coloca[n] a las mujeres en una posición desfavorable respecto a las oportunidades que ofrecen las nuevas herramientas digitales no sólo para el empleo sino para la participación política y social, y el ejercicio de los derechos de ciudadanía"** (Sainz et al, 2020).

[17] De acuerdo con Alliance for Affordable Internet, la conectividad significativa incluye contar con umbrales mínimos de acceso regular a internet, un dispositivo apropiado, datos suficientes y una conexión rápida. Véase: Alliance for Affordable Internet. "Meaningful Connectivity- unlocking the full power of internet access". https://a4ai.org/meaningful-connectivity/. Consultado el 1° de febrero de 2021.

[18] World Wide Web Foundation (agosto 2018), Advancing Women´s Rights Online: Gaps and Opportunities in Policy and Research. http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf; Organización para la Cooperación y el Desarrollo Económico (OCDE) (2018). Bridging the Digital Gender Divide: Include, Upskill, Innovate. http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf; Araba Sey y Nancy Hafkin (eds.) (2019). Taking Stock: Data and Evidence on Gender Digital Equality, United Nations University. https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf. Consultado el 1° de febrero de 2021.

[19] En la región, 35% de mujeres reportaron no saber cómo usar un teléfono móvil inteligente y un 40% señaló no saber cómo utilizar internet. Véase: BID (2020). ¿Desigualdades en el Mundo Digital? Brechas de Género en el Uso de las TIC.

[20] World Bank Group (2018), "La base de datos Global Findex 2017. Medición de la inclusión financiera y la revolución de la tecnología financiera. Reseña", https://openknowledge.worldbank.org/bitstream/handle/10986/29510/211259ovSP.pdf. Consultado el 1° de febrero de 2021.

En particular, **en el contexto de la pandemia del COVID-19 la falta de acceso a las TIC y los bajos niveles de alfabetización digital han propiciado la exclusión de las mujeres** de las acciones en materia de salud, educación[21] y trabajo que están utilizando las tecnologías digitales para enfrentar la contingencia, y limitan su acceso a la información y noticias públicas sobre medidas de aislamiento y cuarentena así como a los programas de apoyo o subsidios (CIM, 2020b; CEPAL, 2020: 5). Y sin acceso ni habilidades digitales suficientes, las mujeres tienen menos capacidad para recibir información vital, comprenderla y actuar en consecuencia oportunamente (UIT, 2020a: 14), lo cual pone en riesgo su salud y su bienestar.

Por último, es importante tener presente que, en una época de digitalización creciente como la que se vive actualmente, estas brechas digitales no sólo colocan a las mujeres en una situación de mayor vulnerabilidad, sino que impactan a toda la sociedad en su conjunto. Dado que las mujeres "desempeñan un papel desproporcionado como trabajadoras de primera línea, cuidadoras y educadoras, la brecha de género tiene costos adicionales para las familias, las comunidades y las economías" (Chair et al, 2020b: 5), quienes dependen de ellas para poder preservar su bienestar, salud y, en muchos casos, su vida.

B. La continuidad de las realidades online-offline: la discriminación de género y los impactos de la pandemia del COVID-19 en las mujeres

> *El segundo elemento a tomar en consideración al realizar un análisis sobre los impactos de género de la pandemia en el ciberespacio es el hecho de que las experiencias en línea y las ciberamenazas que enfrentan las mujeres no pueden separarse de las realidades que estas viven fuera de línea (Brown y Pytlak, 2020), las cuales están determinadas por las condiciones sistémicas de desigualdad que las afectan en todos los ámbitos de su vida y que se han agudizado durante la crisis sanitaria.*

Tal y como lo ha reconocido la ONU, las mujeres están por debajo de los hombres en todos los indicadores de desarrollo sostenible y representan el mayor porcentaje de personas en situación pobreza y sin acceso a la educación[22]. Este **contexto de desigualdad se replica también en el área de las TIC**[23], donde la participación de las mujeres apenas alcanza un porcentaje aproximado del 20% (con un 22% en el área de Inteligencia Artificial y 11% en el ámbito de la ciberseguridad)[24], estimándose que tomará al menos 100 años alcanzar la paridad de género en el sector de las tecnologías digitales[25].

---

[21] Dado que con frecuencia no tienen acceso a métodos de escolarización en línea (incluyendo la falta de dispositivos electrónicos y/o de datos para conectarse), las niñas y jóvenes también están en riesgo de sufrir una exclusión cada vez mayor ante el cierre general de las escuelas durante la crisis sanitaria. Si tomamos en cuenta que mujeres y niñas conforman el porcentaje más alto de pobres en el mundo y que los niños tienen 1.5 veces más oportunidades que las niñas de tener un celular, es previsible que gran parte de las niñas y adolescentes están viendo truncada su educación durante este período crítico ya sea porque en su casa no tienen datos o un dispositivo para conectarse o porque, de tenerlo, tradicionalmente muchas familias valoran más la educación de los niños por sobre la de las niñas, siendo probable que sean estos quienes utilicen los dispositivos disponibles en casa. Véase: Organización de las Naciones Unidas para la Educación, la ciencia y la Cultura (UNESCO), ¿Cómo estás aprendiendo durante la pandemia de COVID-19? https://es.unesco.org/covid19/educationresponse; Vodafone Foundation, MITD-Lab y Girl Effect, Executive summary. Real girls, real lives, connected. A global study of girls' access and usage of mobile, told through 3000 voices, https://static1.squarespace.com/static/5b8d51837c9327d89d936a30/t/5bbe7cbe9140b7d43f282e21/1539210748592/GE_VO_Executive+Summary+Report.pdf

[22] A nivel mundial, sólo 49.6% de las mujeres forma parte de la población económicamente activa en comparación con 76% de los hombres, y persiste una brecha de género salarial del 16% que es una causa fundamental de desigualdad en términos de ingresos a lo largo de toda la vida de las mujeres. Además, las mujeres siguen representando más de dos tercios de las personas analfabetas a escala mundial y, a pesar de los avances registrados en los últimos años, la tasa de escolaridad continúa siendo menor entre niñas que entre niños (sobre todo a nivel de educación secundaria y superior), las cuales se enfrentan a obstáculos tales como el matrimonio forzado y embarazos precoces, la violencia de género y actitudes tradicionales que hacen que la educación de los niños sea privilegiada por sobre la de las niñas. Además, la violencia también sigue siendo una condición sistémica que mantiene a las mujeres en situación de subordinación. Una de cada tres mujeres ha sido víctima de violencia física o sexual principalmente por parte de un compañero sentimental, la cual se ha calificado como una pandemia mundial extendida también al ciberespacio. Véase: ONU Mujeres (25 septiembre 2015). "Infografía: Igualdad de género- ¿Dónde nos encontramos hoy?"; Noticias ONU (14 febrero 2018). "Las mujeres están por debajo de los hombres en todos los indicadores de desarrollo sostenible", https://www.unwomen.org/es/digital-library/multimedia/2015/9/infographic-gender-equality-where-are-we-today; ONU Mujeres, "Mujeres y Pobreza". https://news.un.org/es/story/2018/02/1427081; https://beijing20.unwomen.org/es/in-focus/poverty. Consultado el 1° de febrero de 2021.

[23] PWC, "Women in Tech. time to close the gender gap". https://www.pwc.co.uk/who-we-are/women-in-technology/time-to-close-the-gender-gap.html. Consultado el 1° de febrero de 2021.

[24] World Economic Forum. "Assessing Gender Gaps in Artificial Intelligence". Global Gender Gap Index 2018, http://reports.weforum.org/global-gender-gap-report-2018/assessing-gender-gaps-in-artificial-intelligence/; The Conversation (2020). "The lack of women in cybersecurity put us all at greater risk". The Next Web. https://thenextweb.com/syndication/2020/06/28/the-lack-of-women-in-cybersecurity-puts-us-all-at-greater-risk/ Consultado el 1° de febrero de 2021.

[25] Cade Metz (21 junio 2019). "The gender gap in computer science research won't close for 1000 years". The New York Times. https://www.nytimes.com/2019/06/21/technology/gender-gap-tech-computer-science.html. Consultado el 1° de febrero de 2021.

Estas condiciones de desigualdad y vulnerabilidad se han visto magnificadas por la pandemia. Como lo ha subrayado la Comisión Interamericana de Mujeres, "la emergencia derivada del COVID-19 está provocando impactos específicos sobre las mujeres y profundizando las desigualdades de género existentes" (CIM, 2020b: 4), sobre todo para aquellas mujeres y niñas que enfrentan formas múltiples de discriminación por factores tales como su raza, origen étnico, religión o creencias, discapacidad, edad, orientación sexual, clase social y situación migratoria (European Women's Lobby, 2020).

La pandemia ha incrementado los niveles de pobreza de mujeres, y ha afectado su trabajo y las brechas de género en el empleo. Antes de la contingencia sanitaria, las mujeres ocupaban la mayor parte de los empleos en el área de servicios y de los empleos inseguros, precarios e informales[26], sectores que se han visto especialmente afectados durante los últimos meses[27].

Las mujeres constituyen también 70% del personal del sector salud y de cuidados y asistencia social, y son la mayoría del personal médico que se encuentra en la primera línea de respuesta de la crisis, asumiendo mayores costos físicos y emocionales y un mayor riesgo de infección[28]. Además, estas han sido víctimas en diversos países de crecientes actos de discriminación, xenofobia y estigmatización derivado de la ansiedad y el miedo al contagio del COVID-19 (ONU Mujeres, 2020d).

A lo anterior se suma el hecho de que muchas mujeres han visto elevarse su trabajo doméstico y de cuidados en detrimento de su trabajo productivo remunerado[29]. Antes de la pandemia, las mujeres en todo el mundo hacían casi tres veces más trabajos de cuidados y domésticos no remunerados que los hombres, cifra que se ha elevado durante la contingencia[30]. La saturación de los sistemas sanitarios, el cierre de las escuelas y las medidas de confinamiento han provocado que haya más personas en casa que necesitan alimentos, cuidados y educación, y muchas mujeres han tenido que renunciar a sus empleos, reducir sus jornadas laborales o sortear empleos de tiempo completo para asumir trabajos de cuidados y domésticos y la supervisión de los procesos de aprendizaje de sus hijas e hijos, todo ello con importantes impactos en su salud física y mental, en su independencia y en la cantidad de tiempo que tienen disponible (CIM, 2020c; CIM 2021; ONU Mujeres 2020f).

El contexto generado por la emergencia ha incrementado también la violencia contra las mujeres y las niñas, llegándose a afirmar que a la sombra de la pandemia del COVID-19 se está verificando también una pandemia de violencia de género (CIM, 2020a; ONU Mujeres, 2020c). En todos los países se han registrado tasas más elevadas de violencia doméstica derivado de las medidas de confinamiento, las cuales han aumentado las tensiones y conflictos dentro de los hogares y el aislamiento de mujeres y niñas, quienes se han visto obligadas a convivir permanentemente con agresores (CIM, 2020a). Según estimaciones de la ONU, por cada tres meses que continúe el confinamiento, habrá 15 millones casos adicionales de violencia de género en todo el mundo[31]. Esto seguramente limitará su acceso al internet y su adquisición de habilidades digitales.

---

[26] A nivel regional, antes de la pandemia 54% de las mujeres trabajaban en el sector informal como empleadas del hogar, vendedoras ambulantes, agricultoras de subsistencia y temporeras (aproximadamente 126 millones de mujeres, según la Organización Internacional del Trabajo). Véase: ONU Mujeres. "Las mujeres en la economía informal". https://www.unwomen.org/es/news/in-focus/csw61/women-in-informal-economy. Consultado el 1° de febrero de 2021.

[27] De acuerdo con la Organización Internacional del Trabajo (OIT), la reducción de la actividad económica ha afectado en primer lugar a las trabajadoras informales quienes perdieron sus ingresos intempestivamente y tendrán dificultades para hallar trabajo en la ya pronosticada recesión económica. Véase: Organización Internacional del Trabajo (OIT) (2020). Policy Brief. A Gender-responsive employment recovery: Building back fairer.

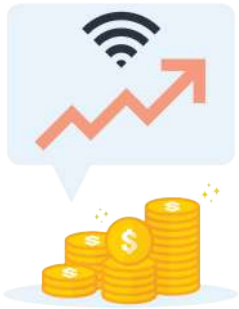
[28] Investigaciones han revelado que en países como Alemania, Italia, España y Estados Unidos la tasa de contagio de trabajadoras de la salud es entre dos y tres veces más alta que aquella de los trabajadores hombres del sector. Véase: Global Health 5050. The COVID-19 Sex-Disaggregated Data Tracker. https://globalhealth5050.org/the-sex-gender-and-covid-19-project/. Consultado el 21 de febrero de 2021.

[29] Se estima que el tiempo dedicado a la educación de las y los hijos ha aumentado 36%, mientras que el tiempo dedicado a realizar compras para la familia ha incrementado 24%. Ver: ONU Mujeres (20 octubre 2020). "El avance de las mujeres hacia la igualdad se estanca" https://news.un.org/es/story/2020/10/1482722; Matt Krentz et al (21 mayo 2020). "Easing the COVID-10 burden on working parents". BGG; https://www.bcg.com/publications/2020/helping-working-parents-ease-the-burden-of-covid-19; Richard Blundell et al (11 junio 2020). "COVID-19: the impacts of the pandemic on inequality". Institute for Fiscal Studies. https://www.ifs.org.uk/publications/14879. Consultado el 1° de febrero de 2021.

[30] En Estados Unidos y Europa, las mujeres han asumido una carga extra de trabajo doméstico y de cuidados no remunerado de 15 horas semanales. Esta situación se vuelve aún más crítica en el caso de las mujeres a cargo de hogares uniparentales, que representan el 75% a nivel mundial. Asimismo, evidencias señalan que durante la pandemia las madres han tenido mayores probabilidades que los padres de perder sus empleos temporal o permanentemente, alcanzando pérdidas de hasta 60% en sus ingresos. Véase: Matt Krentz et al (21 mayo 2020). "Easing the COVID-19 burden on working parents". BGG. https://www.bcg.com/publications/2020/helping-working-parents-ease-the-burden-of-covid-19

[31] Naciones Unidas (28 abril 2020). "Millones de mujeres sufrirán embarazos no deseados durante la pandemia de coronavirus". Noticias ONU. https://news.un.org/es/story/2020/04/1473572. Consultado el 1° de febrero de 2021.

Antes de la pandemia del COVID-19, mujeres no conectadas en países del Sur Global ya señalaban los altos costos como una de las principales razones para no acceder a internet (World Wide Web Foundation, 2015)[32], situación que es previsible se verá exacerbada ante su importante pérdida de ingresos y empleos durante esta etapa.



También pueden esperarse impactos negativos a mediano y largo plazo en el desarrollo de habilidades digitales por parte de niñas y jóvenes ante las repercusiones que la pandemia está teniendo en su educación. En anteriores brotes epidémicos se ha comprobado que el cierre de escuelas afecta desproporcionadamente a las niñas, muchas de las cuales nunca retoman su educación al verse obligadas a trabajar para compensar la pérdida de ingresos familiares, o al ser víctimas de matrimonios infantiles, violencia y/o explotación sexual (ONU Mujeres, 2020e: 14-15). Así, es muy probable que las alteraciones educativas durante la pandemia del COVID-19 significarán un obstáculo para el acceso y uso significativo del internet por parte de niñas y jóvenes, al estar comprobado que la educación es uno de los impulsores más importantes de la brecha de género en el acceso a las TIC, con estudios que indican que las mujeres con educación básica tienen seis veces menos probabilidades de estar en internet que quienes han completado la educación media (World Wide Web Foundation, 2015).

A lo anterior se suman las múltiples formas de ciberabuso y violencia en línea que se han incrementado durante la crisis del COVID-19 casi a la par del aumento de la violencia doméstica (APC, 2020; ONU Mujeres, 2020a; Brudvig et al, 2020). De acuerdo a lo reportado por diversas fuentes, ha habido un incremento del abuso de género en línea de hasta el 38% (Glitch UK, 2020), siendo común la distribución no consensuada de imágenes íntimas y de actos de sextorsión, ciberhostigamiento y ciberacoso, violencia sexual en línea, sí como actos de *grooming* y explotación sexual facilitada por las TIC en contra de mujeres y niñas (ONU Mujeres, 2020a; CIM, 2020a; Derechos Digitales, 2020)[33].

La violencia en línea, que es una de las manifestaciones más claras de la desigualdad de género en el ciberespacio, incrementa también la brecha digital que mujeres y niñas enfrentan al tener por consecuencia que estas se autocensuren o decidan mantener un perfil bajo en internet por temor a que su privacidad o seguridad se vean vulneradas. Además, afecta su capacidad para moverse libremente y sin miedo en los espacios online, negándoles la oportunidad de interactuar con las tecnologías para la construcción autónoma de sus identidades digitales (REVM-ONU, 2018: par. 29)[34].

Como se expone en el apartado IV, estas condiciones de desigualdad y discriminación por motivos de género que afectan a las mujeres se reflejan en el ciberespacio y son la base de muchas de las amenazas cibernéticas que estas enfrentan puesto que determinan los patrones de uso del internet y sus posibles vulnerabilidades en línea.

[32] De acuerdo con la investigación Derechos Digitales de las Mujeres de la Fundación World Wide Web realizada en 10 países en vías de desarrollo, el costo en esos países de datos prepagados de 1GB (equivalente a 13 minutos de internet al día sin considerar costos de video) era equivalente al 10% del ingreso per cápita promedio, lo cual es 10 veces más alto en relación con los ingresos per cápita en los países del OCDE y el doble de lo que una persona gasta en salud en los países en desarrollo. Véase: World Wide Web Foundation (2015). Women's Rights Online. Translating Access into Empowerment. http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf. Consultado el 1° de febrero de 2021.

[33] De acuerdo con un estudio realizado por Glitch UK y la Coalición End Violence Against Women, 46% de las personas encuestadas señalaron haber sido víctimas de abuso en línea. De las personas que sufrían abuso en línea un año antes de la pandemia, 29% señaló que el abuso se había vuelto más grave, cifra que aumenta a 38% en el caso de mujeres negras o personas no binarias.

[34] De acuerdo con investigaciones referidas por la Relatora Especial sobre la violencia contra la mujer de la ONU, 28% de las mujeres víctimas de violencia de género en línea han reducido deliberadamente su presencia en línea. Véase: Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias (2018). Informe acerca de la violencia en línea contra las mujeres y niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. Organización de las Naciones Unidas.

C. ¿Qué sabemos acerca de los usos que las mujeres le están dando al internet durante la pandemia del COVID-19?

> *Finalmente, como un tercer elemento de análisis es importante tomar en consideración que* ***los usos que se le dan al internet se ven condicionados cuantitativa y cualitativamente por el género de las personas,*** *encontrándose variaciones importantes entre la forma en que hombres y mujeres navegan en el ciberespacio y los objetivos que persiguen al conectarse (Brown y Pytlak, 2020).*

Antes de la pandemia, estudios en la materia registraban que los propósitos de uso del internet de las mujeres estaban más relacionados con el bienestar social, con entablar comunicación con familiares y amistades (recibir o hacer llamadas y chatear) y buscar información sobre salud (Agüero, Bustelo y Viollaz, 2020; Sainz, 2020; Brown y Pytlak, 2020). Los hombres, por su parte, tendían a utilizar el internet para enviar correos electrónicos, buscar información sobre noticias, clima y transporte, acceder a servicios de banca electrónica y para realizar actividades de entretenimiento como videojuegos, escuchar música o ver videos. Además, estos solían utilizar de forma más intensiva y variada los dispositivos electrónicos y daban un uso mayor del internet para desarrollar actividades económicas, de trabajo y administración (por ejemplo, trámites en línea) (Agüero, Bustelo y Viollaz, 2020; Sainz, 2020).

Se ha documentado también que las mujeres dependen más que los hombres del internet para ejercer ciertos derechos. Por ejemplo, el internet puede facilitarles acceder a la educación si sus responsabilidades en el hogar les impiden trasladarse hasta un centro educativo, expresarse si viven en comunidades particularmente opresivas, acceder a información sobre derechos sexuales y reproductivos cuando no está disponible *offline*, o proteger su seguridad personal en casos de violencia doméstica (Brown y Pytlak, 2020).

Si bien la digitalización acelerada durante la pandemia del COVID-19 ha propiciado una modificación radical para todas y todos en los hábitos de uso de dispositivos electrónicos y del internet, **dados los roles y normas de género que persisten dentro y fuera del ciberespacio, es muy probable que durante la crisis y con posterioridad a ella se hayan mantenido algunas de estas tendencias de uso.** Como se señaló previamente, faltan aún estudios en la materia que nos permitan conocer con certeza cómo las mujeres están utilizando el internet durante este periodo. Sin embargo, **pueden proyectarse algunos posibles escenarios a partir de tendencias previas de navegación y de los impactos que la pandemia** está teniendo actualmente en sus vidas.

Así, dado que durante esta etapa las mujeres han asumido en mayor medida que los hombres la carga de trabajo doméstico y de cuidados no remunerado, es de esperarse que estas estén usando preponderantemente el **internet como un medio para mantenerse en contacto con sus familiares y amistades,** a fin de estar al tanto de su estado de salud, así como para realizar compras de alimentos y medicinas en línea, obtener noticias sobre la evolución de la enfermedad, y para facilitar la educación a distancia de sus hijas e hijos. Asimismo, dado que estas constituyen la mayor parte del personal del sector salud, es factible que estén valiéndose de la tecnología para brindar **teleconsultas y coordinar sus labores de cuidados y asistencia** social en las comunidades.

Otros impactos de la pandemia en la vida de las mujeres pueden darnos claves adicionales sobre sus usos, necesidades y prioridades durante esta época cuando acceden a internet. Por ejemplo, dado el alto porcentaje de mujeres que laboraban en el autoempleo o en el sector informal, es previsible que una parte de ellas esté buscando mantener sus negocios **incursionando en plataformas de *e-commerce*, o que estén accediendo por primera vez a sitios de ofertas de trabajo** ante el gran aumento en la tasa de desocupación femenina. Siguiendo esta misma lógica y dado el número de niñas inscritas en la educación primaria, es previsible también que estas (y sus familias) hayan tenido que vencer rápidamente estereotipos de género que las mantenían alejadas de las tecnologías a fin de incorporarse a clases en formatos digitales.

Algunas otras tendencias de uso ya han sido confirmadas conforme avanza la crisis sanitaria. Por ejemplo, siguiendo una tendencia previa, se tiene conocimiento que las mujeres y jóvenes están utilizando el internet durante esta época **para obtener información sobre su salud sexual y reproductiva,** cuyos servicios han sido suspendidos en muchas partes del mundo ante la reducción de presupuestos y las medidas preventivas de distanciamiento físico[35].

Asimismo, ante el incremento durante esta etapa de la violencia de género fuera y dentro del internet en contra de las mujeres, las mujeres están utilizando los dispositivos digitales como una línea vital de defensa **para solicitar ayuda y mantener contacto con su red de apoyo** por medio de servicios de mensajería instantánea con función de geolocalización, llamadas gratuitas a líneas de ayuda contra el abuso doméstico, o aplicaciones que brindan apoyo e información a sobrevivientes en caso de ser vigiladas por sus abusadores. También están acudiendo en mayores números al internet **para reportar y hacer públicos los actos de violencia de género** en línea que están cometiéndose en su contra y para crear redes de apoyo a víctimas.

Sin duda, queda mucho por explorar en cuanto a las experiencias de uso del internet de las mujeres y niñas durante esta etapa y se requerirán mayores estudios con una perspectiva de género sobre los impactos de la pandemia en el nuevo ecosistema digital. Sin embargo, como se señaló previamente, una lectura conjunta de las dinámicas de acceso y uso del internet por parte de las mujeres, así como de los impactos que la propia pandemia está teniendo en sus vidas *offline*, puede darnos una primera guía para conocer sus experiencias digitales y, a partir de ello, sus necesidades, intereses y vulnerabilidades cuando acceden a internet.

[35] Ximena Casas (12 Mayo 2020). "Protecting Women's Reproductive Health During the Pandemic". Human Rights Watch. https://www.hrw.org/news/2020/05/12/protecting-womens-reproductive-health-during-pandemic. Consultado el 1° de febrero de 2021.

04 Las ciberamenazas y riesgos específicos que enfrentan las mujeres en el nuevo ecosistema digital: Una reflexión en curso

> *Ante la falta de estudios y datos desagregados por sexo sobre la prevalencia del cibercrimen durante la pandemia, en este apartado* ***se realiza una proyección sobre cuáles son las posibles amenazas que estarían enfrentando las mujeres en el ciberespacio durante la pandemia del COVID-19.***

Como se apreciará a continuación, tomar en cuenta las experiencias de las mujeres en el ciberespacio revela que los peligros y amenazas que enfrentan en línea tienen características específicas y les afectan de forma diferenciada en función de los roles de género y la discriminación y desigualdad que viven dentro y fuera de línea (Brown y Pytlak, 2020).

Se destaca que esta identificación de ciberamenazas es enunciativa y no limitativa, pues ante los constantes cambios observados en el ciberespacio y en las interacciones *online-offline*, es de esperarse que el tipo de amenazas y peligros cibernéticos que enfrentan las mujeres se modifiquen conforme evolucione la pandemia del COVID-19.

A. Un factor de riesgo común: la falta de habilidades en materia de seguridad digital

En este escenario de identificación de riesgos, debe de hacerse una mención especial al nivel de habilidades de seguridad digital que tienen las mujeres. Este es un factor que determina en gran medida el tipo de ciberataques que enfrentan y las consecuencias que tienen en su vida esos ciberataques.

Como se señaló previamente, la pandemia del COVID-19 ha expuesto la carencia generalizada de conocimientos básicos para prevenir riesgos y amenazas en línea y el alto grado de exposición a riesgos cibernéticos. Sin embargo, ante la brecha que enfrentan las mujeres en cuanto a la adquisición de habilidades digitales en general y de ciberseguridad en particular, estas se encuentran en una situación particularmente vulnerable frente a ataques cibernéticos.

A esto se suma el hecho de que persisten aún estereotipos de género que las previenen para fortalecer su seguridad digital. Muchas de ellas perciben al ciberespacio como un lugar irremediablemente inseguro para mujeres y niñas, lo cual tiene sus orígenes en prejuicios e ideas preconcebidas sobre su supuesta incapacidad natural para entender y controlar las tecnologías. A esto se le suman también los efectos de la violencia de género sistémica que ha permeado el ciberespacio y normalizado las agresiones en línea en su contra.

Esto implica que un importante número de mujeres tiene a su alcance muy pocos o nulos recursos para afrontar comportamientos ilícitos y abusivos en línea, lo cual las coloca en una situación de mayor riesgo que a los hombres frente a ciertos ciberataques, muchos de los cuales buscan dirigirse contra quienes pueden significar un blanco fácil (UNODC, 2020).

Lo anterior sin dejar de mencionar que esta falta de habilidades en materia de ciberseguridad tiene efectos en cadena al permear en todas las interacciones digitales que las mujeres mantienen en línea y trascender más allá del ciberespacio dada la continuidad entre su vida dentro y fuera del internet. La seguridad digital es también una cuestión de derechos humanos, y el hecho de que las mujeres se sientan inseguras en línea no solo afecta su acceso al internet sino a todas las oportunidades que éste brinda para ejercer sus derechos *online y offline*.

Asimismo, esta falta de habilidades tiene impactos en sus familias y comunidades. Son las mujeres quienes durante esta época de crisis sanitaria han asumido la mayor parte del trabajo de cuidado no remunerado y la supervisión de los procesos de aprendizaje de sus hijas e hijos ante el cierre de las escuelas, por lo que su desconocimiento sobre las amenazas cibernéticas que pueden enfrentar niñas, niños y adolescentes (NNA) o adultos mayores en la nueva normalidad digital coloca también a las personas bajo su cuidado en una situación de riesgo[36].

B. Explorando algunos riesgos que enfrentan las mujeres en la nueva normalidad digital

Si bien resta aún mucho por conocer acerca de la dimensión de género de los incidentes de seguridad y las amenazas específicas que las mujeres están enfrentando en el ciberespacio durante la pandemia del COVID-19, al realizar un análisis de los ciberataques más comunes reportados a nivel mundial durante la pandemia del COVID-19, en conjunto con las experiencias de las mujeres dentro y fuera del ciberespacio, podemos identificar cierto tipo de amenazas en línea que les estarían afectando especialmente:

Cierto tipo de fraudes y estafas a través de campañas de *phishing* o difusión de *malware*.

Ante el rol preponderante que las mujeres tienen durante la crisis sanitaria en el trabajo doméstico y de cuidados no remunerados de familias y comunidades, puede estimarse que el tipo de ataques de phishing que significarían un mayor riesgo para ellas estarían relacionados con compras de alimentos y medicamentos o información de salud.

[36] En el caso del cuidado de los NNA, por ejemplo, una falta de conocimiento de los procesos de educación virtual y las medidas básicas de protección digital puede colocarles en un mayor riesgo de grooming, violencia sexual, sextorsión o acceso a información falsa.

Fraudes y estafas dirigidos en contra de mujeres que están incursionando en el comercio en línea, el uso del dinero móvil o en la recepción de transferencias de efectivo de programas sociales.

Dado que hasta antes de la pandemia las mujeres representaban más de la mitad de las personas financieramente excluidas de la economía digital, es previsible que los ciberataques se dirijan específicamente en contra de nuevas usuarias dada su falta de familiaridad con las herramientas financieras digitales y de conocimientos de ciberseguridad para proteger sus transacciones en línea. Es previsible también que estos ataques tengan mayores impactos en la economía de las mujeres que en el caso de ciberataques dirigidos a hombres dadas las tasas elevadas de desigualdad de género en el empleo y el ingreso.

Fraudes vía *phishing* dirigidos en contra de mujeres de edad avanzada.

Existen reportes que indican un aumento de ataques a personas de edad avanzada durante esta etapa en forma de correos fraudulentos, llamadas telefónicas o servicios de mensajería instantánea, mediante los cuales los cibercriminales se hacen pasar por alguien de confianza para la víctima (como el banco o personal médico) a fin de obtener datos personales. En el contexto actual de mayor uso del internet, las mujeres mayores son especialmente vulnerables ante ciberataques dada su carencia de habilidades informáticas en general y de seguridad digital en particular, la cual es mayor que en el caso de los hombres de su mismo grupo de edad[37].

Campañas de desinformación.

La infodemia y distribución de información falsa es un riesgo en línea que afecta particularmente a las mujeres dado el uso preponderante que estas le dan al internet para obtener noticias relacionadas con la salud. Estudios han demostrado que existe una fuerte dimensión de género en las actividades de desinformación dado que la identidad de género y la orientación sexual pueden convertirse en la base para que alguien reciba información al hacerse suposiciones sobre los intereses de la persona y su capacidad de ser influenciada (Brown y Pytlak, 2020).

[37] Las mujeres están sobrerrepresentadas entre las personas adultas mayores (conforman 57% de las personas mayores de 70 años y 62% de las que tienen más de 80 años) y son tres veces más propensas que los hombres a vivir solas. Estudios en Europa indican que tan solo 48% de las personas mayores de 65 años cuentan con habilidades digitales, y que las mujeres mayores tienen menos habilidades que los hombres mayores con una diferencia de 10 puntos. Se ha registrado que sólo la mitad de las personas entre 65 y 74 años que usaron internet en el último año contaba con algún tipo de *software* o herramienta de seguridad informática en sus dispositivos, mientras que 13% señaló no conocerlas. Asimismo, un gran número de personas mayores no utiliza contraseña en sus dispositivos por temor a no recordarlas o utiliza contraseñas débiles que son fácilmente identificables por *hackers*. La empresa de seguridad informática McAfee reportó que 50% de las personas usuarias de redes sociales mayores de 60 años comparten voluntariamente información personal con individuos que no han visto nunca en persona y sin seguridad alguna. Véase: Abby Ellin (12 septiembre 2019). "Scammers Look for Vulnerability, and find it in Older People". The New York Times. https://www.nytimes.com/2019/09/12/business/retirement/scams-elderly-retirement.html;
ONU Mujeres (mayo 2020). "Informe de políticas: Los efectos de la COVID-19 en las personas de edad". https://www.un.org/sites/un2.un.org/files/old_persons_spanish.pdf; Enrique Arieas Fernandez et al. (2018). "Acceso y uso de las TIC de las mujeres mayores de la Europa comunitaria". Prisma Social. Revista de Ciencias Sociales. No. 21. https://revistaprismasocial.es/article/view/2458. Consultado el 1° de febrero de 2021.

Ataques vía *software*, redes y/o las herramientas de trabajo remoto.

Es común que los ciberatacantes se aprovechen del uso distraído de herramientas de trabajo remoto para ingresar a los sistemas corporativos, lo cual es un riesgo latente cuando la persona trabajadora está afectada por el cansancio o fuentes de distracción constantes, como es el caso de las mujeres que durante esta etapa están teniendo que empatar su trabajo productivo remunerado con el incremento de sus labores domésticas y de cuidados no remunerados, soportando una doble o hasta triple jornada laboral (CIM, 2020c; ONU Mujeres, 2020f).

Ataques de ransomware a hospitales a través de los dispositivos electrónicos de las mujeres que integran el personal médico.

Si bien resta realizar investigaciones en la materia, es previsible que los ataques de *ransomware* a hospitales o centros de salud tengan un componente de género, puesto que son mujeres quienes conforman la mayoría de las personas trabajando en el sector y quienes pueden ser en un blanco fácil de ciberataques ante su menor grado de conocimientos de seguridad digital en comparación con los hombres trabajando en el sector salud.

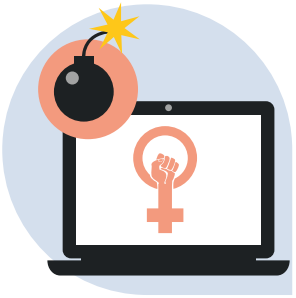
Violencia de género en línea.

Se ha comprobado que la violencia de género en línea en contra de las mujeres aumenta de forma directamente proporcional a su acceso a internet (REVM-ONU, 2018; EIGE, 2017; Van Der Wilk, 2018;). Siguiendo esta tendencia, estudios durante la crisis sanitaria han comprobado que, ante el incremento de su participación en el ciberespacio, las mujeres están siendo víctimas de forma desproporcionada de ciberacoso, ciberhostigamiento, distribución no consensuada de imágenes íntimas y sexuales, doxxing, violencia sexual a través de troleo, recepción de imágenes y videos sexuales sin consentimiento y amenazas de violencia sexual (ONU Mujeres, 2020ª; Glitch UK; APC, 2020).

Asimismo, siguiendo tendencias observadas antes de la pandemia, la violencia de género digital está afectando particularmente a mujeres activas en redes sociales como por ejemplo, periodistas reportando sobre la evolución de la enfermedad, activistas, bloggers, defensoras de derechos humanos y mujeres con un perfil público que utilizan las redes sociales para abogar por la igualdad de género, y quienes han reportado ser víctimas de campañas de desinformación y desprestigio (AI, 2018; REVM-ONU, 2018; ONU Mujeres, 2020a)[38].

[38] Véase: Julie Posetti et al (2020). Online violence against women journalists. A global snapshot of incidence and impacts. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000375136. Consultado el 1° de febrero de 2021; Maria Giovanna Sessa (4 diciembre 2020). "Misogyny and Misinformation: An analysis of Gender Disinformation Tactics during the COVID-19 Pandemic". EU Disinfo Lab. https://www.disinfo.eu/publications/misogyny-and-misinformation:-an-analysis-of-gendered-disinformation-tactics-during-the-covid-19-pandemic/. Consultado el 1° de febrero de 2021.

Ataques a organizaciones feministas o grupos de mujeres que trabajan en el ámbito de la igualdad de género y los derechos sexuales y reproductivos.



Se ha documentado también que la violencia de género en línea está dirigiéndose de forma específica a organizaciones de mujeres que están utilizando el internet durante esta etapa para mantenerse conectadas y organizarse, reivindicar sus derechos, y prestar apoyo y acompañamiento a víctimas de violencia de género. Estas organizaciones han reportado sabotajes de video llamadas y ataques vía *zoombombing*[39] mediante el envío de material sexualmente explícito, racista y sexista, ataques a sus canales de expresión mediante el hackeo de sus páginas de internet, redes sociales o cuentas de correo electrónico, y ataques de Denegación de Servicio Distribuido (DDoS), entre otros (APC, 2020).

Estrategias de sextorsión digital.

Se ha comprobado que este ataque, cuyos índices han aumentado de forma significativa durante la pandemia, tiene un importante componente de género enfocándose preponderantemente en mujeres, jóvenes y niñas[40] dado que la difusión pública de imágenes íntimas tiene mayores consecuencias para ellas ante las normas y estereotipos de género en torno al control de la sexualidad femenina[41]. El incremento en este ciberdelito ha sido consecuencia de una combinación de factores, entre los que pueden destacarse, las medidas de distanciamiento físico y la necesidad de mantener cercanía con otras personas utilizando las herramientas virtuales, prácticas inseguras de *sexting*, y estafas de sextorsión vía *phishing*.

Grooming y acoso sexual de niñas y adolescentes.

Ante el aumento del tiempo en línea se ha reportado un incremento paralelo en la vigilancia, asedio, contacto sin consentimiento y la imposición de conductas de carácter sexual indeseadas en contra de menores de edad, ciberataques que se realizan a través de espacios de interacción como juegos en línea, redes sociales y salas de chat (INTERPPOL, 2020).

[39] Véase: Lizle Loots et al. (14 abril 2020). "Online safety in a changing world- COVID-19 and cyber violence". Sexual Violence Research Initiative. http://www.svri.org/blog/online-safety-changing-world-%E2%80%93-covid-19-and-cyber-violence; Sophie Davies (18 marzo 2020). "Risks of online sex trolling as coronavirus prompts home working". https://www.reuters.com/article/us-women-rights-cyberflashing-trfnidUSKBN2153HG. Consultado el 1° de febrero de 2021.

[40] Benjamin Wittes et al (11 mayo 2016). "Sextortion: Cybersecurity, teenagers, and remote sexual assault". Brookings. https://www.lawfareblog.com/new-data-sextortion-124-additional-public-cases; Katherine Kelley (19 marzo 2019). "New Data on Sextortion: 124 additional public cases". Lawfare. https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/. Véase también: Claudia Long (3 junio 2020). "Coronavirus shutdown prompts spike in reports of sextortion toe Safety Commissioner", ABC News. https://www.abc.net.au/news/2020-06-03/spike-reports-esafety-commissioner-coronavirus-shutdown/12314442 Consultado el 1° de febrero de 2021.

[41] Christina Elia (11 agosto 2020). "My sextortion birthday: Digital violence during COVID-19". Genderit.org. https://genderit.org/feminist-talk/my-sextortion-birthday-digital-violence-during-covid-19. Consultado el 1° de febrero de 2021.

Si bien aún falta por recopilar datos desagregados por sexo sobre la prevalencia de estos cibercrímenes, se puede estimar que el *grooming* y acoso sexual son un peligro cibernético que afecta particularmente a mujeres y niñas. Investigaciones realizadas antes de la pandemia han confirmado que éstas tienen el doble de probabilidades de ser acosadas sexualmente en internet[42] y que los tipos de comentarios violentos que reciben en línea son cualitativamente diferentes de los que reciben los niños y jóvenes, basándose a menudo en su apariencia física e incluyendo amenazas de violencia sexual[43].

Explotación sexual y trata de mujeres y niñas facilitada por las nuevas tecnologías.

Tomando en consideración tendencias observadas antes de la pandemia, puede estimarse que mujeres y niñas se encuentran en un mayor riesgo de ser víctimas de la red internacional de trata de personas como consecuencia del incremento en sus niveles de pobreza. Estudios en la materia han documentado que el 80% de las víctimas de trata de personas son mujeres, número que asciende a 95% en casos de explotación sexual[44].

[42] Angus Reid (2016). Trolls and Tribulations: One-in-Four Canadians Say They're Being Harassed on Social Media. http://angusreid.org/wp-content/uploads/2016/10/2016.10.04-Social-Media.pdf

[43] De acuerdo con un estudio de Plan Internacional, casi 60% de las niñas y jóvenes de todo el mundo han sido víctimas de diferentes formas de ciberacoso en línea, quienes se enfrentan a esta forma de violencia tan temprano como los 8 años. Véase: Plan Internacional (2020). Inseguras Online. Experiencias de niñas, adolescentes y jóvenes en torno al acoso online. https://plan-international.es/inseguras-online. Consultado el 1° de febrero de 2021.

[44] European Parliament (2016). Briefing. The gender dimension of human trafficking 2016. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI(2016)577950_EN.pdf; Sylvia Walby et. al. (2016). Study on the gender dimension of trafficking in human beings. Final Report. European Commission. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._final_report.pdf

05 La seguridad digital de las mujeres en el nuevo ecosistema digital: Un núcleo duro de medidas de autocuidado

> *La identificación de los posibles riesgos que están enfrentando las mujeres en la nueva normalidad digital es solo el primer paso en la construcción de una cultura de ciberseguridad atenta al género. Dado que no se cuenta con información de calidad sobre las características de estos nuevos escenarios, se vuelve necesario ir develando y precisando estos riesgos digitales para generar un esquema de autocuidado para las mujeres.*

Esta identificación de riesgos debe acompañarse de esfuerzos específicos de todos los sectores involucrados para visibilizar aquellas herramientas que les permitan a las mujeres protegerse y navegar seguras y con confianza, bajo el entendido de que existe en el ciberespacio un contexto de riesgo y discriminación que las afecta por el sólo hecho de ser mujeres, y que es un reflejo del mismo contexto de violencia por razones de género presente en la vida fuera de línea.

Como se mencionó en líneas previas, la falta de prácticas personales de seguridad digital por parte de las mujeres es un problema generalizado como consecuencia de la poca información de calidad que reciben. Esta falta de adopción de medidas de seguridad digital no es un problema atribuible a las mujeres sino que, por el contrario, son necesarios mayores esfuerzos por parte de los actores implicados para cerrar la brecha de género en la alfabetización digital y para disminuir los impactos negativos de los estereotipos de género que las alejan del control de las tecnologías.

Ante ello, uno de los principales mensajes a destacar en el marco de una estrategia de ciberseguridad con perspectiva de género es que, a pesar de que el ciberespacio es un entorno que conlleva riesgos, las mujeres no están irremediablemente condenadas a ser víctimas, sino que se les debe hacer llegar la información necesaria para protegerse y para prevenir ciberataques y actos de violencia en línea mediante la implementación de medidas básicas de autocuidado.

Asimismo, es de suma importancia tener presente que la identificación de estas prácticas de seguridad digital no debe entenderse en el sentido de colocar la responsabilidad en las mujeres y niñas por la violencia en línea y los ciberataques cometidos en su contra, responsabilidad que recae invariablemente en los atacantes y cibercriminales responsables del daño, quienes deben ser sancionados por estas conductas.

En atención a los riesgos que enfrentan, en este apartado se ha condensado un núcleo duro de medidas básicas de protección para mujeres durante la actual crisis sanitaria. Es crucial promover su adopción en paralelo al desarrollo de políticas de ciberseguridad enfocadas en la identificación de las condiciones que facilitan estos ciberataques y en la persecución y sanción de los responsables.

A. Kit básico de medidas de seguridad digital para la nueva normalidad

Adoptar una política personal de ciberseguridad en respuesta a la pandemia

- **Darse cuenta que se es un blanco. La concientización es la primera línea de defensa** contra las nuevas y cambiantes amenazas cibernéticas surgidas durante la pandemia.

- Es importante realizar un **ejercicio personal de análisis de riesgo:** ¿Cuáles son las nuevas conductas de riesgo adoptadas ante el aumento del tiempo en línea y el uso de nuevas herramientas (por ejemplo, navegando por sitios que no son habituales, instalando aplicaciones desconocidas o haciendo compras en sitios poco seguros)? ¿Qué estoy haciendo para protegerme de posibles ataques?

- **Precaución ante todo.** Es crucial mantenerse vigilantes y tener mayor precaución en la forma como se interactúa en al mundo digital. Ahora que la pandemia ha forzado la adopción de nuevas tecnologías en un corto periodo de tiempo, es importante planificar, entrenar y fortalecerse en protección digital puesto que cada paso en el ecosistema digital tiene el potencial de crear riesgos.

- El éxito de los **ciberataques frecuentemente depende de errores humanos.** Cuando las personas están en un estado prolongado de estrés, tensión, cansancio o están distraídas son más propensas a cometer errores y a bajar la guardia frente a posibles riesgos cibernéticos.

- **La búsqueda de información sobre el COVID-19 es especialmente crítica.** Muchos de los ataques actuales se dirigen a quienes buscan información sobre la pandemia, por lo que se debe confiar únicamente en sitios oficiales o verificados, no solo por la calidad de la información, sino por el incremento de sitios maliciosos que explotan esa necesidad de información.

- **El cibercrimen se está aprovechando del miedo y la incertidumbre** que provoca el COVID-19 y se adapta a las noticias locales sobre el desarrollo de la pandemia. Los señuelos casi siempre replican las noticias a nivel nacional y se adaptan a la ubicación de las víctimas.

- Muchos de los **ataques no ocurren de forma aislada, sino combinada.** Por ejemplo, un acceso no autorizado a un dispositivo electrónico puede facilitar la comisión de un fraude o el *hackeo* de una cuenta de redes sociales puede servir para diseminar *spam* promoviendo compras fraudulentas de productos médicos.

- **Es fundamental estar atenta e informada** acerca de nuevos engaños y amenaza cibernéticas y las posibles respuestas.

- **Conversar con la familia,** incluyendo niñas, niños y personas adultas mayores, sobre la importancia de protegerse en línea. Se debe impulsar en familia una corresponsabilidad digital, puesto que el cuidado en entornos digitales no solamente conlleva prácticas individuales sino también el cuidado y seguridad de otras personas.

Contraseñas seguras como la primera línea de protección

Las contraseñas son el primer paso para acceder a cuentas y dispositivos y, por lo tanto, brindan una primera capa de protección ante amenazas y ciberataques. Por ello, una parte crucial de la seguridad digital sigue siendo el tener buenos hábitos personales en relación con las contraseñas en línea.

- Es importante contar con **contraseñas únicas, largas, aleatorias y difíciles de predecir** (no deben contener información personal).

- Para brindar una protección efectiva, las contraseñas tienen que incluir una mezcla de por lo menos 12 letras **mayúsculas y minúsculas, números y caracteres especiales.**

- Se debe utilizar una **contraseña distinta para cada cuenta y cambiarlas frecuentemente,** en especial las de las cuentas más confidenciales.

- Usar generadores automáticos y/o **administradores de contraseñas *online*,** los cuales crean contraseñas aleatorias y seguras para cada una de las cuentas.

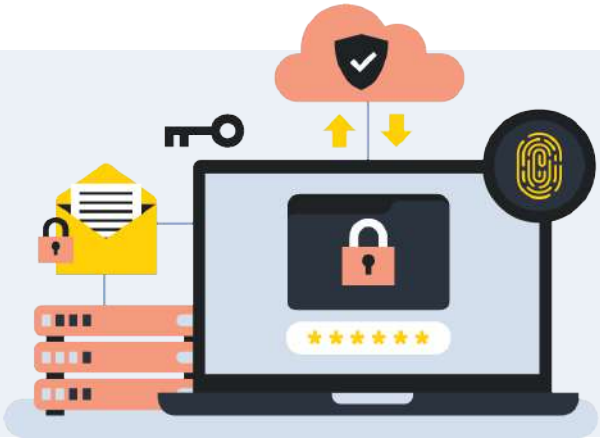
- Utilizar las **preguntas de seguridad** en los sitios que tienen disponible esta opción, pero sin responderlas con información personal.

- No guardar las contraseñas en la configuración del navegador, en la nube o en un documento poco seguro dentro de la computadora o teléfono.
- No compartir contraseñas a través de una conexión no segura, como mensajes de texto o SMS.
- Para agregar una segunda capa de protección, **activar la verificación en 2 pasos** (autentificación de factor doble o 2FA) que se encuentra disponible en el correo electrónico y redes sociales.

Navegación segura

- Conectarse únicamente en redes **Wifi privadas y confiables.**
- En las redes de hogares es importante que el router WiFi no pueda ser accedido desde el exterior y que cuente con una clave de administrador fuerte y difícil de adivinar. También debe monitorearse con regularidad cuáles son los equipos conectados a la red.
- Asegurarse de **navegar siempre en modo seguro.** Siempre verificar que la dirección web en la cual se está navegando esté reconocida por el protocolo de seguridad HTTPS, sobre todo para compras en línea, movimientos bancarios o cuando se envía información sensible y datos personales. Estas páginas también se pueden identificar por tener un candado verde en la barra del navegador, lo cual significa que la información transita cifrada punto a punto.
- Instalar complementos para bloquear publicidad, rastreadores y software malicioso en el navegador.

Otras medidas de protección básicas



- **Respaldar periódicamente** todos los datos e información personal importante, cifrarlos y almacenarlos en un disco duro externo o en la nube. Una copia de seguridad hecha de forma oportuna y regular puede evitar la pérdida de material y datos sensibles en caso del *hackeo* de dispositivos y ataques de ransomware.

- Utilizar la versión más actualizada de un **software antivirus.** Si bien los antivirus no pueden detectar todo el *malware*, sí brindarán una capa de protección adicional a los dispositivos.

- Mantener el sistema operativo, navegador y aplicaciones **en los dispositivos** electrónicos siempre actualizados, lo cual no sólo ayuda a que sean más rápidos, sino que además brinda mayor seguridad puesto que puede proteger de amenazas y reforzar las vulnerabilidades de las versiones anteriores.

- Cuidar la información personal. No compartirla en sitios web no seguros o publicarla en redes sociales.

- Revisar y familiarizarse con las opciones de **privacidad y seguridad de cuentas de redes sociales** y tomarse el tiempo para ver qué información personal está expuesta en redes.

- Desconfiar de mensajes sobre COVID-19 y enlaces o archivos adjuntos sospechosos o promociones demasiado atractivas.

- **Revisar con cuidado las aplicaciones sobre COVID-19** que se instalan en los dispositivos electrónicos, puesto que muchas de ellas imitan fuentes fidedignas como la OMS.

- Descargar aplicaciones o cualquier otro **software exclusivamente de plataformas seguras** (Google Play Store o App Store), desconfiar de aplicaciones que piden permisos innecesarios en el dispositivo y revisar las calificaciones de otras personas usuarias. Revisar las aplicaciones que ya no se utilizan y eliminarlas puesto que pueden ser una puerta de entrada para *malware*.

B. Medidas de seguridad digital ante riesgos específicos

a. Protección frente al corona-phishing y corona-smishing

Una de las formas más comunes que actualmente utilizan los atacantes para instalar *malware* en computadoras o teléfonos es a través de ataques de *phishing* o pesca de datos fraudulenta. Este ciberataque se basa en el envío fraudulento de correos, mensajes SMS o mensajería instantánea en redes sociales (Whatsapp) que parecen inocentes porque suplantan la identidad de una persona, empresa o entidad reconocida pero que en realidad disfrazan programas maliciosos o redireccionan a sitios web falsos para recabar información personal, nombres de personas usuarias, claves personales, contraseñas o datos bancarios. A través de ataques de *phishing* cibercriminales pueden también tomar control de los dispositivos y de toda la información que ahí se almacena.

Durante la pandemia, muchos de estos intentos de *phishing* han suplantado la identidad de entidades de gobierno u organizaciones de salud o filantrópicas, refiriendo información sobre el COVID-19, actualizaciones sobre el desarrollo de la enfermedad, supuestas curas, vacunas y material médico, apoyos gubernamentales, beneficios fiscales, falsas ofertas de trabajo o servicios gratuitos. Otro de los ataques más populares han sido los ataques de *smishing*, mediante los cuales se envía un SMS haciéndose pasar por una entidad de gobierno compartiendo un enlace donde se solicitan datos personales.

Recomendaciones de autoprotección:

- La mejor estrategia es **tomar conciencia sobre la recurrencia de los intentos de *phishing*.** Por regla general, desconfiar al recibir un correo electrónico o mensaje extraño o de un usuario desconocido que solicite información privada, inste a tomar acciones rápidas o de urgencia o resulte amenazante.
- **Sospechar de todos los correos electrónicos sobre COVID-19,** especialmente si no se reconoce la dirección electrónica.

- **Sospechar también de cadenas de WhatsApp.** Circulan vía WhatsApp miles de mensajes con enlaces a una gran variedad de páginas web donde supuestos expertos ofrecen recomendaciones y soluciones ante el virus. Una gran parte de esos mensajes contienen enlaces maliciosos o buscan desinformar.

- Sospechar si el correo tiene **errores gramaticales o semánticos en el texto, un diseño o calidad sospechosa** y si no está personalizado (que refiera, por ejemplo, 'estimado colega', 'estimado amigo', 'amable cliente').

- Revisar con atención el remitente o la dirección web.

- **No hacer clic en los enlaces** recibidos a través de un mensaje sobre COVID-19 (de texto, WhatsApp o mail), aunque parezcan ser de una fuente oficial como el Ministerio de Salud o la OMS. Muchos de esos enlaces redireccionan a sitios web falsos en el que se engaña para identificase o introducir datos confidenciales que los estafadores utilizan para acceder a los dispositivos y robar dinero.

- **Proteger la información personal.** Ninguna fuente oficial solicita datos por email.

- **No abrir archivos adjuntos** de correos extraños ni acceder o descargar enlaces o archivos poco confiables (sobre todo si tienen terminación .exe). Si hay dudas y el archivo adjunto parece importante, puede abrirse dentro de Google Drive para una mayor protección.

- Escanear links sospechosos utilizando herramientas como VirusTotal (si bien esta herramienta no alcanza a reconocer todos los tipos de *malware*, sí puede revelar algunos programas maliciosos comunes).

- **No contestar** en ningún caso estos correos. Si hay dudas, consultar directamente a la empresa o servicio que representa para confirmar la veracidad del correo pues es posible que hayan falseado o *hackeado* su dirección de email.

- **Contar con un cortafuegos** (firewall) instalado (las versiones más recientes de Windows y Mac OS ya tienen un cortafuegos pre-instalado, y también pueden utilizarse herramientas como Comodo Firewall, ZoneAlarm y Glasswire).

- Bloquear los anuncios integrados en sitios o anuncios emergentes puesto que pueden conducir a descargar archivos maliciosos (puede utilizarse complementos como uBlock Origin para evitar hacer clic en esos anuncios emergentes).

- En caso de publicaciones de ofertas de trabajo, revisar la web de la empresa, la redacción de la oferta, no revelar información privad, revisar la política de protección de datos, y utilizar portales de búsqueda de empleo fiables.

b. Teletrabajo seguro

Para muchas mujeres esta época de confinamiento ha significado incursionar en el teletrabajo y compaginar dentro de sus hogares el trabajo productivo remunerado con su trabajo doméstico y de cuidados no remunerado. En esta nueva normalidad digital, es necesario tomar precauciones especiales puesto que las redes en el hogar pueden no estar correctamente configuradas y/o controladas, lo que podría suponer la apertura de la puerta de la empresa a los ciberdelincuentes o involucrarse en una brecha de información accidental. Además, la doble carga de trabajo puede generar cansancio y distracciones que hacen a las mujeres más vulnerables que a los hombres que trabajan de forma remota y sin el mismo grado de responsabilidades en el hogar.

- **Siempre conectarse en una red Wifi segura** (no pública) y configurar de manera segura la red inalámbrica doméstica (cambiar la contraseña por defecto del enrutador y actualizarlo regularmente), lo cual brindará mayor protección frente a accesos no autorizados a la información de la organización por parte de ciberdelincuentes. De ser posible, conectarse al entorno corporativo utilizando una red privada virtual (VPN), la cual crea una conexión privada y cifrada.

- Mantener la información de trabajo en la computadora del trabajo, y evitar usar la computadora o dispositivos personales para cuestiones laborales. **Separar cuentas personales de las de trabajo,** incluyendo de correo electrónico y redes sociales.

- Hacer **un cifrado completo** de los dispositivos de trabajo.

- En caso de no contar con dispositivos corporativos para trabajar, instalar en el dispositivo personal un sistema de detección proactivo de amenazas, lo cual se logra instalando una solución integral de seguridad y manteniéndola actualizada.

- Prestar atención a la instalación de programas, puesto que la descarga de un *software* malicioso puede poner en riesgo la seguridad de toda la organización.

- Realizar respaldos periódicos de la información.

- Verificar siempre que se está en el sitio web legítimo de la empresa antes de introducir los datos de acceso o información confidencial. Además, contar con contraseñas robustas y utilizar doble factor de autenticación para acceder a cuentas críticas.

- Utilizar de forma segura las herramientas colaborativas en la nube.
- Tomar precauciones de seguridad al hacer videoconferencias.
- Si se requiere enviar información confidencial o delicada, es conveniente utilizar un servicio que encripte la información y no hacerlo por mensajería instantánea.
- Estar atenta ante intentos de phishing y correos electrónicos externos y solicitudes inusuales de las credenciales de acceso (incluyendo llamadas telefónicas inesperadas del equipo de soporte de tecnologías de la empresa solicitando las credenciales de acceso).
- Tener siempre a la mano los contactos de soporte tecnológico y, si ocurre un incidente de seguridad, denunciarlo lo antes posible.

c. Celebrar reuniones online seguras

Durante la pandemia, las aplicaciones de video llamada se han convertido en herramientas imprescindibles para continuar con las actividades cotidianas. Muchos atacantes se han aprovechado de la popularidad de herramientas de videoconferencia (Zoom, Webex, Hangout, Skype) para distribuir *malware* o para acceder y boicotear reuniones (*zoombombing*), por lo que hay que extremar la seguridad para prevenir la intrusión y garantizar la confidencialidad de las conversaciones y la información que se comparte.

Algunas medidas de protección básicas a adoptar son:

- **Controlar la privacidad de la reunión.** Requerir contraseñas para acceder a la reunión (muchas aplicaciones ya lo hacen por defecto).
- Darse tiempo para conocer la política de privacidad de la herramienta de video llamada (¿Cómo trata la información confidencial?).
- **Tener precaución con la convocatoria y añadir únicamente a contactos conocidos.** Hacer invitaciones personales, evitar el uso de canales de comunicación inseguros para lanzar la convocatoria y solicitar un pre-registro.

- Activar la sala de espera, desde donde se puede verificar la identidad de cada participante antes de admitirles a la reunión. Es importante verificar que la persona usuaria que desee entrar tenga un nombre y apellido previamente identificado.
- Si se hará una videoconferencia por primera vez con un contacto nuevo, **verificar su identidad** por otros medios.
- Una vez que las y los participantes se incorporen a la videollamada, **bloquear el acceso** a nuevas personas para asegurarse que intrusos no pueden ingresar y espiar conversaciones.
- Descargar la aplicación desde la web oficial o repositorios oficiales (Google Play o Apple Store).
- Activar las **actualizaciones automáticas del *software*** y aceptar cada vez que lo solicite, puesto que ayuda a tener las características más recientes y la versión más segura.
- **Aplicar el cifrado** de forma predeterminada y asegurarse de que sea de principio a fin.
- **Tener cuidado al compartir archivos y pantallas,** puesto que podrían revelar accidentalmente información confidencial o ser utilizados para difundir programas maliciosos.
- **Deshabilitar la compartición de escritorio y archivos y la recepción de video** por defecto.
- **Cubrir la cámara** cuando el sistema no está en uso y apagar o silenciar los micrófonos.

d. Banca por internet y compras en línea

- Utilizar una contraseña segura para las cuentas bancarias en línea y la autentificación de factor doble.
- Instalar software de seguridad en todos los dispositivos que se utilizan para compras en línea o movimientos bancarios, y mantenerlos actualizados.
- No utilizar computadoras públicas o redes de Wifi públicas para hacer movimientos bancarios, dado que esto incrementa las posibilidades de que personas extrañas puedan acceder a la información bancaria.

- Es recomendable utilizar una sola tarjeta de crédito para transacciones en línea a fin de exponer al mínimo la información bancaria.
- Revisar la cuenta bancaria frecuentemente para detectar actividad sospechosa.
- Estar prevenidas de intentos de estafa a través de correos de *phishing* en los que se solicita ingresar los datos de la cuenta bancaria o se redirecciona a sitios para ingresar esos datos. Si hay duda sobre la veracidad del correo, contactar directamente al banco para corroborar la legitimidad de ese correo.
- ¿Una cura para el COVID-19? No dejarse timar por ofertas en línea y mantenerse alertas. Si una oferta es demasiada buena para ser verdad, probablemente sea falsa.
- Crear un correo electrónico exclusivo para compras en línea.
- Convencerse de la fiabilidad de los proveedores antes de comprar en línea. Comprar siempre a vendedores establecidos, reconocidos y confiables, revisar la antigüedad de sus actividades, sus calificaciones en línea y su historial de venta.
- Hacer compras en línea con proveedores que utilizan sitios web seguros para las transacciones y pagos. Una página web segura tendrá "https://" en la dirección del sitio, y a veces un icono de candado cerrado en la barra de direcciones del navegador.
- Desconfiar si la página no tiene aviso legal con información sobre la empresa, condiciones de venta, devoluciones y reclamaciones, entre otras cosas.
- Revisar todos los detalles de los bienes y servicios que están comprándose (descripción del producto, cargos por envío, moneda y tipo de cambio, términos y condiciones, garantía, devoluciones).
- Reportar si hubo fraude.

e. Cuidados ante la infodemia y campañas de desinformación

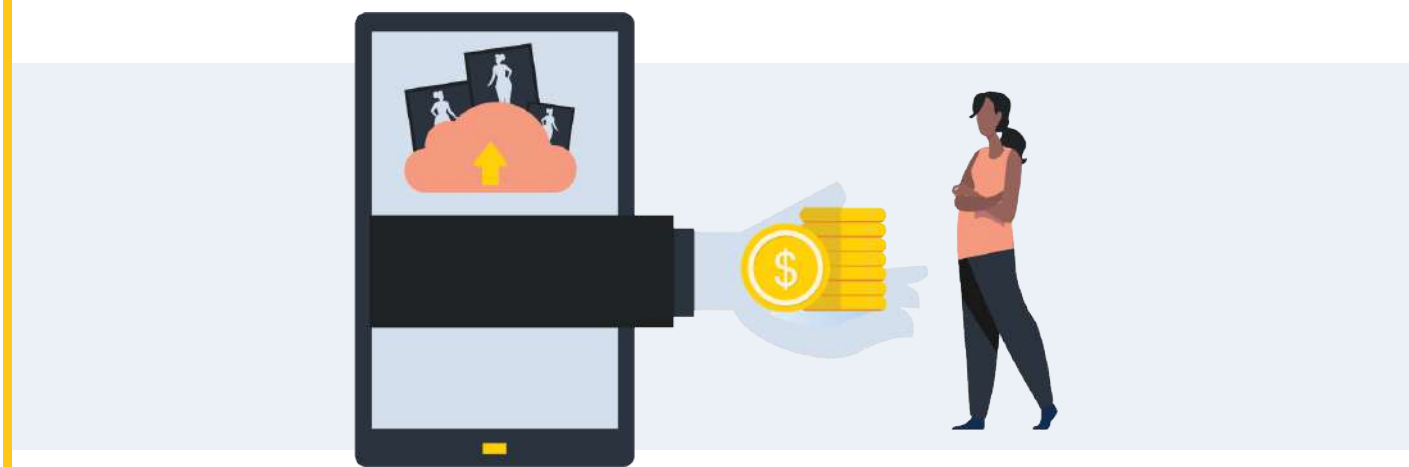
La pandemia de COVID-19 ha estado acompañada de una infodemia, la cual ha generado ansiedad y confusión ante el exceso de información que circula en tuits, mensajes de Facebook, cadenas de WhatsApp, videos y noticias. Esta saturación de información vuelve complicado discernir entre la

información que es confiable y útil con la que busca confundir, lo cual dificulta a las personas guiar sus acciones y decisiones en momentos críticos como los que se viven ahora.

La información que circula cotidianamente a través de la web está compuesta por un conjunto de noticias falsas, campañas de desinformación y manipulación, teorías conspiratorias, rumores, mitos y pseudociencia sobre los efectos del COVID-19, e información para promover supuestas curas, tratamientos y vacunas, lo cual es el escenario perfecto para fraudes y engaños. Caer víctimas de esta infodemia o sobrecarga informativa puede afectar la economía personal, elevar los niveles de ansiedad e, incluso, producir graves daños a la salud no sólo para quien consulta esta información sino para toda la familia.

- **Seleccionar una o dos fuentes de información** confiables para consultar noticias, y evitar revisar reportes falsos o no científicos.
- Generar **capacidad crítica** para distinguir las señales de una noticia falsa y desconfiar de artículos sensacionalistas sobre resultados positivos de tratamientos experimentales a pequeña escala.
- Confiar solo en sitios oficiales o verificados no solo por la calidad de la información, sino por el incremento de sitios maliciosos que explotan esta situación.
- **Verificar la información:** hacer una búsqueda del o la autora u organización, comprobar si la información proviene de un sitio se buena reputación, revisar la URL (¿inicia con HTTPS?) o utilizar sitios de verificación de hechos (Fullfact, Snopes).
- Problemas de redacción, en las imágenes o problemas en las fechas.
- **Contribuir a la lucha contra la desinformación.** No compartir información no verificada que proceda de fuentes dudosas.
- **Para los niños, niñas y jóvenes puede resultar más difícil** discernir entre la realidad y noticias falsas por lo que es importante tener conversaciones sobre el tema para desarrollar su pensamiento crítico y ayudarles a identificar información falsa o mitos peligrosos.

f. Sextorsión



La sextorsión se manifiesta mediante un chantaje basado en la posesión (o supuesta posesión) por parte del agresor de imágenes íntimas, quien amenaza con distribuirlas en caso de no recibir dinero, imágenes adicionales o mantener una relación. El agresor puede ser una pareja íntima, una persona que se conoció en la web o un atacante desconocido.

Durante la pandemia una estafa común ha consistido en el envío de un mensaje o un correo electrónico de alguien desconocido que afirma haber *hackeado* el dispositivo o cuenta amenazando con publicar imágenes privadas sino se realiza el pago de una determinada cantidad. En la mayoría de los emails se busca asustar a la víctima indicándole que se ha infectado el dispositivo con un *malware*, que se ha monitoreado la actividad del ordenador y grabando prácticas sexuales, haciendo referencia a alguna contraseña utilizada por la destinataria en una de sus cuentas. Ante ello, se recomienda:

- ☑ No abrir nunca un correo electrónico no solicitado o de una persona desconocida.
- ☑ Desconfiar de cualquier correo que parezca provenir de la propia cuenta. Muchas veces para hacer el fraude más creíble, el ciberdelincuente falsea la dirección del remitente mediante una técnica conocida como email *spoofing*.
- ☑ No responder a estos correos ni ceder ante las amenazas o pagar el rescate. Lo más probable es que sea un intento de estafa y el atacante no tenga en su posesión imágenes íntimas ni que haya infectado el equipo, incluso si refiere una contraseña personal.
- ☑ Incluso si el atacante tiene en su posesión imágenes íntimas, es recomendable no contestar, detener todo contacto inmediatamente, no pagar y denunciarlo cuanto antes. Realizar el pago alentará a que pida más dinero y, en muchos casos, el material es publicado a pesar de haberse hecho un pago.
- ☑ Tomar capturas de pantalla de las amenazas y de las cuentas involucradas para guardarlas como evidencia en caso de que se desee hacer un reporte ante la policía.
- ☑ Reportar en redes sociales y bloquear la cuenta para evitar contacto.
- ☑ Revisar las configuraciones de seguridad de todas las cuentas y redes sociales.
- ☑ Platicar con el círculo cercano y las personas que pueden verse afectadas. Los extorsionadores se refugian en el silencio de la víctima.
- ☑ Denunciar ante las autoridades.

g. Ciberseguridad en familia

Los principales tipos de violencia en línea sufridos por niños, niñas y adolescentes (NNA) son la exposición a contenidos de carácter sexual y/o violento sin consentimiento, el ciberacoso y el *grooming*. De acuerdo con un estudio realizado por Save the Children, 52% de las y los menores de edad no tenían restricciones por parte de sus padres y madres para acceder a internet, y entre quienes sí tenían, las limitaciones se basaban únicamente en el número de horas.

- Es imposible estar todo el tiempo con los NNA mientras están en línea, por lo que es importante mantener un diálogo abierto y ayudarles a desarrollar un pensamiento crítico sobre los riesgos que pueden enfrentar en línea y las herramientas de seguridad a su alcance para protegerse.
- Explicar a menores la importancia de la privacidad y ciberseguridad, incluyendo la protección de su identidad digital.
- Prestar atención a sus experiencias *online* y conocer sus hábitos de navegación. Supervisar el acceso de niños y niñas a internet para prevenir que publiquen información personal y privada (dirección, teléfono, nombre del colegio), así como el tipo de canales de entretenimiento que visitan con frecuencia.
- Establecer algunos límites en torno a cuándo y dónde pueden utilizar los dispositivos electrónicos (se recomienda que esto sea en áreas comunes).
- Instalar un programa de control parental para cuidar la actividad *online* de niñas y niños (estos programas están disponibles en casi todos los dispositivos electrónicos, televisiones y consolas de videojuegos). Se pueden también descargar controles de seguridad de familia, y establecer buscadores de internet para niñez a fin de evitar que ingresen a sitios inapropiados.
- Revisar los controles de privacidad de videojuegos, aplicaciones y juguetes inteligentes, puesto que pueden revelar los detalles personales y ubicación de los NNA.
- Recordar que los juegos en línea son una red social más que debe tomase en cuenta a la hora de revisar qué información se comparte (permiten también establecer llamadas y contactos con terceras personas).
- Mantenerse al día sobre los sitios, aplicaciones, redes sociales, videojuegos y servicios de chat que están utilizando los NNA, y explorarlos juntas y juntos, incluyendo cómo proteger la información y cómo reportar contenido o conductas inapropiadas dentro de esas plataformas.

- ☑ En ocasiones se comparten los dispositivos móviles en familia, en los cuales suele guardase información sensible como contraseñas, números de tarjeta de crédito o información laboral. Es importante revisar que no puedan acceder a esas cuentas y proteger esos dispositivos con sistemas de protección.

Para prevenir el *grooming*:

- ☑ Asegurarse que las cuentas de redes sociales y funciones de chat en videojuegos sean privadas, revisar las configuraciones de seguridad y establecer reglas acerca del tipo de contenido que deben compartir en línea. Exhortarles a borrar contactos que no conocen en persona.
- ☑ Reportar y bloquear a cualquier persona sospechosa.
- ☑ Hacerles saber que pueden hablar siempre que reciban un contacto inapropiado o si les hace sentir incómoda/o.
- ☑ Exhortarles a eliminar amistades o solicitudes de seguidores de personas que no conocen (revisar si la persona que hace solicitud tiene amistades en común).
- ☑ Prestar atención sobre las personas con quienes socializan *online y offline.*
- ☑ Estar atenta a señales de angustia.

Glosario

Análisis de género. Forma sistemática de observar el impacto diferenciado de desarrollos, políticas, programas y legislaciones sobre los hombres y las mujeres. *4, 9, 10, 13*

Brecha de género. Se refiere a cualquier disparidad entre la condición o posición de las mujeres y hombres en la sociedad (diferencias en el acceso a recursos, derechos y oportunidades). *11, 12, 13, 14, 15, 18, 24*

Cifrado de información. Es un proceso para convertir datos digitales en códigos, los cuales hacen la información ilegible excepto para la persona que posee la clave para descifrarlos. *33*

Control parental. Conjunto de herramientas para bloquear, restringir o filtrar el acceso de menores de edad a determinados contenidos o programas a fin de evitar que se expongan a riesgos a través de internet. *37*

Cortafuegos *(Firewall).* Sistema físico o digital que tiene el objetivo de permitir o prohibir el acceso desde o hacia una red a fin de asegurar que todas las comunicaciones entre la red e internet se realicen conforme a las políticas de seguridad de una organización o corporación. *30*

***Dark Web* o internet obscuro.** Es una parte del internet intencionalmente oculta a los motores de búsqueda en la que existen páginas que no están indexadas y que cuentan con IP enmascaradas accesibles sólo con navegadores web especiales. Estas páginas están dedicadas a toda clase de actividades delictivas e incluyen contenido ilegal. *7*

Denegación de servicio. Ciberataque que tiene por objeto saturar con peticiones de servicio a un servidor a fin de impedir que personas usuarias legítimas puedan utilizarlo. Un método más sofisticado es el ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas de forma coordinada entre varios equipos. *22*

Discriminación por razón de género. Toda distinción basada en el sexo que tenga por objeto o por resultado menoscabar o anular el reconocimiento, goce o ejercicio por la mujer, independientemente de su estado civil, sobre la base de la igualdad del hombre y la mujer, de los derechos humanos y las libertades fundamentales en las esferas política, económica, social, cultural y civil o en cualquier otra esfera [Fuente: Artículo 1 de la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer]. *13, 15, 24*

Estereotipos de género. Es una opinión o un prejuicio generalizado acerca de atributos o características que hombres y mujeres poseen o deberían poseer o de las funciones sociales que ambos desempeñan o deberían desempeñar [Fuente: OHCHR, *Estereotipos de género y su utilización*]. *6, 17, 18, 22, 24*

Género. Se refiere a los roles, comportamientos, actividades, y atributos que una sociedad determinada en una época determinada considera apropiados para hombres y mujeres. El género también hace referencia a las relaciones entre mujeres y las relaciones entre hombres. Estos atributos, oportunidades y relaciones son construidos socialmente y aprendidos a través del proceso de socialización [Fuente: ONU Mujeres, OSAGI *Gender Mainstreaming - Concepts and definitions*]. *4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24*

***Grooming* o ciberengaño pederasta.** Son actos deliberados de un adulto para acercarse a una persona menor de edad (posiblemente cultivando una conexión sentimental) con el objetivo de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o traficar a la o al menor de edad. *15, 19, 22, 23, 37, 38*

HTTPS. Corresponde a las siglas en ingles de *Hypertext Transfer Protocol Secur* y consiste en un protocolo de red destinado a la transferencia segura de datos cifrados. *27, 34, 35*

Igualdad de género. Se refiere a la igualdad de derechos, responsabilidades y oportunidades de las mujeres y los hombres y de las niñas y los niños [Fuente: ONU Mujeres, OSAGI *Gender Mainstreaming - Concepts and definitions*]. *21, 22*

Incorporación de una perspectiva de género. Es una estrategia para lograr que las preocupaciones y experiencias de las mujeres, al igual que las de los hombres, sean parte integrante en la elaboración, puesta en marcha, monitoreo y evaluación de políticas y programas en todas las esferas políticas, económicas y sociales, de manera que las mujeres y los hombres puedan beneficiarse de ellos igualmente y no se perpetúe la desigualdad [Fuente: UNICEF, UNFPA, PNUD, ONU Mujeres. *Gender Equality, UN Coherence and you*]. *8*

Ingeniería social. Son técnicas para engañar a potenciales víctimas a fin de que compartan su información personal (por ejemplo, contraseñas, detalles de cuentas bancarias o datos sensibles) de forma casi voluntaria. Estos métodos suelen valerse de la buena voluntad y la falta de precaución de la víctima. *7*

Livestream. Es una plataforma de video en vivo que permite a las personas usuarias ver y difundir contenido de video utilizando una cámara y una computadora a través de internet. *6*

Malware. El término nace de la unión de las palabras en inglés *malicious software* (*software* malintencionado) y hace referencia a un tipo de *software* que tiene como objetivo infiltrarse y/o dañar un sistema de información sin el consentimiento de la persona usuaria. *7, 19, 28, 29, 30, 32, 36*

Phishing. Es una estafa cometida a través de una comunicación electrónica engañosa y aparentemente oficial (correo electrónico, mensaje de texto o telefónicamente) mediante la cual el estafador o *phisher* suplanta la personalidad de una persona o empresa de confianza para que la persona receptora facilite información confidencial (contraseñas, datos bancarios, etc.). Se denomina *smishing* cuando la estafa se realiza vía SMS y *vishing* cuando se realiza recreando una voz automatizada. *7, 19, 20, 22, 29, 32, 34*

Perspectiva de género. Mecanismo de análisis que consiste en observar el impacto del género en las oportunidades, roles e interacciones sociales de las personas [Fuente: ONU Mujeres, OSAGI *Gender Mainstreaming - Concepts and definitions*]. *4, 8, 9, 10, 17, 24*

Roles de género. Normas sociales y de conducta que, dentro de una cultura específica, son ampliamente aceptadas como socialmente apropiadas para las personas de un sexo específico. Suelen determinar las responsabilidades y tareas tradicionalmente asignadas a hombres, mujeres, niños y niñas [*Fuente:* UNICEF, UNFPA, PNUD, ONU Mujeres. *Gender Equality, UN Coherence and you*]. *4, 16, 18*

Ransomware. Es un programa de *software* malicioso mediante el cual se toma el control del equipo infectado y se 'secuestra' la información de la persona usuaria (cifrándola) con el objetivo de extorsionarla solicitando un rescate económico. *21, 28*

Red Privada Virtual. También referida como VPN por sus siglas en inglés (*Virtual Private Network*), es una tecnología de red de ordenadores que establece una extensión segura de una red de área local (LAN) sobre una red pública o no controlada, permitiendo que el ordenador en la red envíe y reciba datos sobre redes públicas como si fuera una red privada (consiguiendo que esta conexión sea segura gracias al cifrado de la información). *31*

Sexo (biológico). Se refiere a las características biológicas que definen a los seres humanos como mujeres y hombres. *18, 23*

Sextorsión. Consiste en amenazar a una persona con difundir imágenes o videos íntimos con la finalidad de obtener más material sobre actos sexuales explícitos, mantener relaciones sexuales u obtener dinero. *7, 15, 22, 35, 36*

Spoofing. Consiste en una serie de técnicas de suplantación de identidad de entidades o personas en la red llevadas a cabo mediante un proceso de investigación o con el uso de *malware* y con el objetivo de obtener información privada o para conseguir acceder a páginas con una credencial falsa. Según la fuente del ataque el *spoofing* puede clasificarse en IP *spoofing* (suplantación de dirección IP), mail *spoofing* (suplantación de correo electrónico), web *spoofing* (mediante una falsa página web), DNS *spoofing* (suplantación de identidad por fuente de dominio), ARP *spoofing* (suplantación de tabla ARP, que es un protocolo de nivel de red que relaciona una dirección MAC con la dirección IP del ordenador). *36*

Trabajo de cuidados no remunerado. Se refiere a todas las actividades diarias para mantener la vida y salud humana, tales como las tareas del hogar (preparación de alimentos, limpieza, lavado de ropa) y cuidados personales. Lo más común es que estas actividades sean desarrolladas por las mujeres en el hogar de forma gratuita [Fuentes: Orozco, Amaia. *Cadenas globales de cuidados. ¿Qué derechos para un régimen global de cuidados justo?*]. *12, 14, 16, 19, 21, 31*

URL. Por las siglas en inglés *Uniform Resource Locator*, se refiere a la dirección específica que se asigna a cada uno de los recursos disponibles en la red (páginas, sitios, documentos) con la finalidad de que puedan ser localizados o identificados. *35*

Violencia contra la mujer. Cualquier acción o conducta basada en su género que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado [Artículo 1 de la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer). *9, 14, 15, 17, 18, 21, 22, 24*

Virus. Es un programa informático auto propagado que tiene por objeto alterar el funcionamiento normal de un dispositivo electrónico. Los virus se diferencian de otros tipos de *malware* en que se replican automáticamente, es decir, son capaces de copiarse de un archivo o un ordenador a otro sin el consentimiento de la persona usuaria. *5, 11, 30*

Wifi. Es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a Internet a través de un punto de acceso inalámbrico. *27, 31, 33*

Zoombombing. Hace referencia a la intrusión sin consentimiento de una videoconferencia a través de contenido obsceno, pornográfico, sexista, racista, homofóbico, etc., usualmente resultando en la finalización de la videoconferencia. El término se acuñó en un inicio para referirse a incidentes ocurridos durante la pandemia de COVID-19 en la plataforma de Zoom, si bien ahora se aplica a intrusiones en otras plataformas de videoconferencias. *32*

Referencias

- Agudelo, Mauricio, Eduardo Chomali, Jesús Suniaga, et al (2020). Las oportunidades de la digitalización en América Latina frente al COVID-19. CEPAL, ELAC, Corporación Andina de fomento, DPL Consulting y Telecom Advisory Services.
- Agüero, Aileen, Monoserrat Bustelo y Mariana Viollaz (2020). ¿Desigualdades en el Mundo Digital? Brechas de género en el Uso de las TIC. Nota técnica No. IDB-TN-01879. Banco Interamericano de Desarrollo.
- Association for Progressive Communications (APC) (2020). COVID-19 and the increase of domestic violence against women: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on Violence against Women, its causes and Consequences.
- Brown, Deborah y Allison Pytlak (2020). Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom y Association for Progressive Communications (APC).
- Brudvig, Ingrid, Chenai Chair y Adriane van den Wilk (2020). COVID-19 and increasing domestic violence against women: The pandemic of online gender based violence. World Wide Web Foundation.
- Chair, Chenai, Ingrid Brudivg, Calum Cameron et al (2020a). Women's rights online. Closing the digital gender gap for a more equal world. World Wide Web Foundation.
- (2020b). Derechos de la mujer en línea. Cerrar la brecha digital de género para lograr un mundo más igualitario. Resumen ejecutivo.
- Comisión Económica para América Latine y el Caribe de la Organización de las Naciones Unidas (CEPAL) (2020). Informe Especial COVID-19 No. 7. Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19.
- Comisión Interamericana de Mujeres (2020a). La violencia contra las mujeres frente a las medidas dirigidas a disminuir el contagio del COVID-19.
- (2020b). COVID-19 en la vida de las mujeres. Razones para reconocer los impactos diferenciados.
- (2020c). COVID-19 en la vida de las mujeres: Emergencia global de los cuidados.
- (2021). COVID-19 en la vida de las mujeres: Los cuidados como inversión
- Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias (REVM-ONU) (2018). Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. Consejo de Derechos Humanos. Organización de las Naciones Unidas. Consultado el 9 de septiembre de 2020.
- Derechos Digitales América Latina (2020). COVID-19 and the increase of domestic violence against women in Latin America: A digital rights perspective.
- European Union Agency for Law Enforcement Cooperation (EUROPOL) (2020a). Internet Organised Crime Threat Assessment.
- (2020b). Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic.
- (2020c). Catching the virus. Cybercrime, disinformation and the COVID-19 pandemic.
- European Women's Lobby (2020). Policy Brief Women must not pay the price for COVID-19. Putting equality between women and men at the heart of the response to COVID-10 across Europe.
- Glitch UK y End Violence against Women Coalition (2020). The Ripple Effect: COVID-19 and the Epidemic of Online Abuse.

- Instituto Europeo de la Igualdad de Género (EIGE) (2017). La ciberviolencia contra mujeres y niñas
- Millar, Katherine, James Shires y Tatiana Tropina (2021). Gender Approaches to Cybersecurity. United Nations Institute for Disarmament Research (UNIDIR)
- Oficina de Naciones Unidas para la Droga y el Delito (UNODC) (2020). Cybercrime and COVID-19: Risks and Responses.
- ONU Mujeres (2020a). Online and ICT facilitated violence against women and girls during COVID-19.
- (2020b). From Insights to Action. Gender Equality in the Wake of COVID-19.
- (2020c). COVID-19 and Ending Violence against Women and Girls.
- (2020d). COVID-19 en América Latina y el Caribe: Cómo incorporar a las mujeres y la igualdad de género en la gestión de la respuesta de la crisis.
- (2020e). Spotlight on Gender, COVID-19 and the SDGS. Will the Pandemic Derail Hard-Won Progress on Gender Equality?"
- (2020f). COVID-19 y la Economía de los Cuidados: Acciones inmediatas y transformación estructural para una recuperación con perspectiva de género. Documento de Políticas No. 16.
- Organización Mundial de la Salud (OMS) (2020). El género y la COVID-19.
- Sainz, Milagros, Lidia Arroyo y Cecilia Castaño (2020). Mujeres y digitalización. De las brechas a los algoritmos. Instituto de la Mujer para la Igualdad de Oportunidades. Ministerio de Igualdad del Gobierno de España.
- Slupska, Julia (2019). "Safe at Home: Towards a Feminist Critic of Cybersecurity". St Antony's International Review, 15, no. 1: 83-100.
- The Interantional Criminal Police Organization (INTERPOL) (2020). Cybercrime COVID-19 Impact.
- Unión Internacional de Telecomunicaciones (ITU) (2020a). Measuring digital development. Facts and Figures 2020.
- (2020b). "Las mujeres, las TIC y las telecomunicaciones de emergencia: Oportunidades y limitaciones".
- World Wide Web Foundation (2015). Women's Rights Online. Translating Access into Empowerment.

OAS Cataloging-in-Publication Data

La ciberseguridad de las mujeres durante la pandemia del COVID-19 : experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital / [Preparado por la Secretaría General de la Organización de los Estados Americanos].
v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.D/XXV.16)
ISBN 978-0-8270-7184-1
1. Women's rights. 2. COVID-19 (Disease). 3. Computer security. I. Title. II. Inter-American Commission of Women. III. Inter-American Committee against Terrorism. IV. OAS/CICTE Cyber Security Program. V. Organization of American States. Secretariat for Multidimensional Security. VI. Serie Libro Blanco. VII. Series.
OEA/Ser.D/XXV.16

Secretariat for Multidimensional Security (SMS)

Libro blanco

La ciberseguridad de las mujeres durante la pandemia del COVID-19:

Experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital

OEA | Más derechos para más gente