La gestión de la ciberseguridad en el mundo digital de niñas y mujeres

33

Cuadernos de transparencia

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

ANAHIBY ANYEL BECERRIL GIL

DIRECTORIO

PLENO DEL INAI

Blanca Lilia Ibarra Cadena
Comisionada Presidenta

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Río Venegas
Comisionada

Josefina Román Vergara
Comisionada

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)
Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, C.P. 04530, Ciudad de México

Equipo Editorial
Sergio Octavio Contreras Padilla,
Kenya Soraya Martínez Ponce,
Griselda Rubalcava Hernández,
María Fernanda de León Canizalez,
María Alicia Barrera Aviña.

Diseño editorial y portada
Diego González Hernández

Primera edición, noviembre 2023
ISBN: 978-607-59844-5-2

Hecho en México / *Made in Mexico*
Ejemplar de descarga gratuita

ÍNDICE

LA AUTORA

Anahiby Anyel Becerril Gil

Abogada, Doctora en Derecho y Globalización, con más de 10 años de experiencia en temas relacionados con Derecho de las Tecnologías de la Información y Comunicación; protección de datos personales; ciberseguridad y derechos humanos. Autora de diversos artículos en la materia. Docente en diversas instituciones públicas y privadas, en temas relacionados con: ciberseguridad y derechos humanos; protección de datos personales; derecho y tecnologías; *LegalTech*, *blockchain* y *smart contracts*; comercio electrónico; entre otros.

Colaboradora con diversas organizaciones y organismos regionales en materia de ciberseguridad. Participante en diversas asociaciones, como: Academia Mexicana de Ciberseguridad y Derecho Digital (AMCID); Conectadas MX; Federación Iberoamericana de Asociaciones de Derecho Informático (FIADI). Reconocida como *Top Women in Cybersecurity Latin America 2021*. Distinción otorgada a 50 mujeres de la región por WOMCY-Latam, *Women in Cybersecurity* y WISECRA, Alianza de Mujeres en Seguridad y Resiliencia.

PRESENTACIÓN

La gestión de la ciberseguridad en el mundo digital de niñas y mujeres

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) consigue difundir, mediante este proceso de divulgación, nuevos conocimientos de interés público enfocados a la protección de datos personales aunados a la era tecnológica.

A través de la colección de los Cuadernos de Transparencia, el INAI sigue abonando a la discusión temas cada vez más actualizados como es el caso del presente número, el cual se encuentra enfocado a la gestión de la ciberseguridad en el mundo digital de niñas y mujeres.

Este ensayo, escrito por Anahiby Becerril, Doctora en Derecho y Globalización, Especialista en Derecho Digital y Ciberseguridad, Miembro de la Academia Mexicana de Ciberseguridad y Derecho Digital (AMCID), detalla de manera clara y concisa esta otra cara del mundo digital, en específico la violencia de género que existe dentro de espacios virtuales.

A lo largo del texto, la autora remarca un problema social contundente que se ha ido generando con la llegada de nuevos escenarios en el avance de las Tecnologías de la Información y la Comunicación (TIC), algunos de ellos se encuentran relacionados con la vulneración a la privacidad, la exposición de información y el robo de datos.

De esta manera, Anahiby Becerril inicia su narrativa explicando que, si bien la tecnología nos ha

traído otras oportunidades de acceder de manera eficaz a una vasta cantidad de información en cuestión de tiempo, es una realidad que al igual que el mundo físico, el ciberespacio se ha transformado en un espacio hostil para grupos vulnerables como lo son niñas, niños, adolescentes y mujeres.

Hechos respaldados y que pueden ser comprobables gracias a estudios verídicos que la autora menciona a lo largo de las consecuentes páginas. Gracias a ello y al claro manejo del lenguaje en la narrativa, podemos dar cuenta de un problema visible que se encuentra presente ya no solo en el mundo físico, sino en un entorno digital.

De esta forma, las y los lectores podrán vislumbrar entre líneas una realidad social derivada de una violencia digital de género. Razón por la cual, en su incursión por contribuir en la sociedad, en el INAI resulta imprescindible abordar y dar seguimiento al conocimiento y prevención de dichos factores para así evitar el mal uso que usuarios suelen replicar en internet, entre ellos, amenazas físicas, abuso y acoso sexual, acecho y trolling sexual.

Para los cuales, en el texto se exponen dichos comportamientos que se encuentran dirigidos a un entorno que pareciera ser que sigue fomentando estereotipos y conductas reprochables de odio en cuestiones de género hacia infantes y mujeres.

Asimismo, el artículo presente busca la difusión ante este hecho que se ha ido clarificando. Sin embargo, también indaga en concientizar a ese grupo vulnerable sobre riesgos y amenazas en el mundo digital con el objetivo de brindar herramientas de ciberseguridad en un entorno privado con el fin de minimizar los peligros y prevenir ser víctima de las conductas antes mencionadas.

Por lo que, a manera de sugerencia, la autora desglosa una serie de recomendaciones para que usuarios de plataformas digitales mantengan su derecho a la privacidad y a la protección de datos personales con el objetivo de navegar en espacios seguros, visión que deja muy en claro la importancia de tener una sociedad informada.

Destacando la notoria explicación de mantener una conciencia sobre los efectos y las consecuencias que causan el mal uso de la información, para que de esta manera podamos disfrutar plenamente de los beneficios que el avance tecnológico ha traído en la vida diaria.

La autora no pierde de vista este hecho, derivado de la desinformación que existe en el consumo de nuevas tecnologías y por ello resulta menester reconocer y dar pie a cuestiones de ciberseguridad para de esta forma defender fundamentos básicos como son el acceso a la información pública, la protección de datos personales y la libertad de expresión.

Actualmente vivimos en un entorno digital, y como navegadores de múltiples plataformas digitales, el presente libro también nos invita a reflexionar sobre el debido tratamiento de la información que deseamos compartir al público, así como las posibles consecuencias de

una violencia digital derivada de la gran cantidad de datos que se recolectan en internet sobre nuestra persona.

Así, esta nueva producción editorial del INAI afronta una nueva realidad social mediante datos y estadísticas comprobables que medirán el alcance y la importancia de la protección de datos personales en entornos físicos y digitales.

Estimadas y estimados lectores, confiamos en que este **Cuaderno de Transparencia número 33** invitará a la reflexión y, a su vez, sumará en la prevención de nuevos espacios seguros dentro del ciberespacio. Por lo que consideramos que es de gran interés y relevancia acercar este tipo de temas a una sociedad que se encuentra en constante contacto con la tecnología.

Derivado de la vasta experiencia de la autora en cuestiones de la materia para detallar entre líneas su expertise en el ámbito de la divulgación sobre coyunturas sociales como es la protección de datos personales en entornos digitales, es que ponemos a su disposición este libro, que sin duda traerá no solo reflexiones, sino cambios significativos dentro y fuera de la vida digital.

Comité Editorial del INAI

INTRODUCCIÓN

La gestión de la ciberseguridad en el mundo digital de niñas y mujeres

Definir el mundo digital puede llevarnos a encontrar múltiples perspectivas, sin embargo, algo seguro es que se trata del paradigma actual que tiene que ver con el adelanto exponencial que ha tenido la tecnología. Este avance ha representado la atomización de la vida cotidiana, es decir, determinadas actividades diarias pueden ser fragmentadas e imitadas por algún proceso tecnológico; hoy enfrentamos los embates de la inteligencia artificial. La aceleración tecnológica parece no tener fin, y eso ha puesto a todo el cono global en una constante discusión sobre sus beneficios, repercusiones, y los retos que estamos atravesando.

El mundo digital opera a través de una enorme red de conexiones que han originado plantearse nuevos escenarios, por ejemplo, estadísticas del *Special Report Digital* sugieren que en México (2021)[1] los usuarios de 16 a 64 años usan constantemente dispositivos que van desde los celulares hasta los relojes inteligentes, pasando por las tabletas, laptops, consolas de videojuegos o bien, los dispositivos inteligentes para el hogar. La interconectividad se convirtió en una realidad social, cultural y política que ha ocasionado otro tipo de brechas, pero algo es real, y es que no es una simple tendencia o época, la digitalización de la vida cotidiana llegó para quedarse.

Autores como Nicholas Negroponte (1995) sostenían hace algunos años que la transformación de átomos a bits es irrevocable e imparable, y eso refiere al nivel exponencial con el que las consecuencias tecnológicas pueden impactar la vida de una persona en tan solo 48 horas, y quizás hasta menos, por ejemplo, la bolsa de valores puede tener un cierre de periodo y tener cambios inmediatos en cuestión de segundos.

El dedo humano se ha convertido en una inversión multimillonaria, y fue cuando pasó de ser una simple extensión del

1 Consultado el 14 de septiembre en: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/

cuerpo humano a una entrada gráfica. Ahora, los cajeros automáticos, las pantallas sensibles al tacto, los celulares y ciertos mecanismos de seguridad llegan a ser un riesgo de ciberseguridad cuando el almacenamiento de huellas digitales se vuelve un mercado donde el usuario no sabe que arriesga su propia identidad.

Los procesos tecnológicos han dado una vuelta de 180° grados a la forma en que vemos la vida, muestra de ello es el anonimato con el que la violencia digital ha escalado o la capacidad de trasmitir datos e información que es falsa, inexacta o bien, que puede causar un conflicto de escala mundial. Recordemos el caso de la pandemia, donde millones de personas compartían antídotos herbolarios o hasta oraciones milagrosas para enfrentar una enfermedad multisistémica de amplio espectro y con un gran semiología, tanto clínica como bioquímica y radiológica. La violencia digital, la desinformación y los ataques cibernéticos son actualmente una preocupación en todas las escalas de gobierno tanto nacionales como internacionales.

La tecnología y el internet, como aliados de la sociedad del conocimiento e inmersos en el mundo del contenido y la creatividad, lograron una serie de modificaciones en la vida económica, social y hasta política de todas las personas. Este proceso se asocia con la omnipresencia de la red y la multiplicidad de actividades que parecieran se pueden realizar de manera simultánea, no obstante, eso nutrió exorbitantemente los focos de atención de los mercados, los cuales cambiaron su cadena de producción y las formas de comercialización, es decir, ahora toda la atención debe estar en el usuario y en su alto nivel de conectividad.

Las aplicaciones y las redes sociales están listas para recopilar a toda costa una mina de oro, y ya no es un lingote cualquiera, y muchos menos un tipo de mineral. Hoy en día, la mercancía con mayor valor es el almacenaje, estadísticas sobre las necesidades de los usuarios a un nivel tan alarmante, que incluso podrían asegurar cierto nivel de personalización, que a su vez da a las empresas las certezas sobre productos, colores, texturas y tamaños que consumidores van a comprar con mayor rapidez.

El modelo de cambio de comportamiento y los procesos de investigación se encuentran asociados a nivel tecnológico y a los procesos de redes que interactúan en el ciberespacio. Desde Gordon Bell y hasta James Grey, varios autores describían el ciberespacio y su anatomía como un momento histórico en el que el internet iba a revolucionar cada partícula del mundo. Así está ocurriendo, la tecnología ha vuelto a la sociedad aún más compleja, porque provocó una nueva brecha social, una donde los más conectados tienen una ventaja abismal frente a los desconectados.

Ahora bien, la interconectividad y la desigualdad en el mundo digital previamente encarado tiene una nueva arista, la gobernabilidad, que a su vez comparte preocupacio-

nes en materia de protección de datos personales. La información en cantidades exponenciales se ha vuelto de vital interés para las corporaciones que convierten cualquier dato en una mina de oro.

Datos que van desde el nombre, domicilio, tipo de sangre, CURP, y que en realidad puede ser cualquiera que permita identificar a una persona. Razón por la cual, el nuevo paradigma de la protección de datos, a través de un tratamiento responsable y urgente, se ha convertido en uno de los principales desafíos de los gobiernos actuales en el mundo, no obstante, el proceso de explicar y concretar el resguardo de información ha representado una nueva crisis pedagógica entre los que usan excesivamente las nuevas tecnologías, y también entre aquellos que no las aprovechan.

Cualquier proceso relacionado con el internet deja de rastro datos personales, historial, cookies, y el problema se encuentra en cómo un tercero los usa para sus propios fines. De esta encrucijada surge la búsqueda constante por entender y priorizar la privacidad digital a la hora de navegar. Pensemos, por ejemplo, en el uso constante y desmedido del teléfono móvil, el cual solicita nuestro acceso o la aceptación de ciertas cláusulas y avisos de privacidad, los cuales, es casi un hecho que pocos leen o saben su utilidad.

El desarrollo tecnológico y sus efectos pusieron en tela de juicio la labor de cada país en materia de frenar los posibles efectos negativos de tecnología. Hay que considerar también que en nuestro país el acceso a la información pública se encuentra consagrado como un derecho fundamental, al igual que el derecho a la protección de datos.

Sin embargo, considerarlos en nuestra carta magna no es suficiente, porque además requiere de una visión garantizada por parte del Estado, que a grandes rasgos significa favorecer todos los procesos, mecanismos y herramientas para permitir que esos derechos fundamentales tengan cabida en cada sector de la población.

El recorrido histórico nos lleva con certeza a pensar que las normas en el contexto nacional han contribuido a la construcción del derecho de protección de datos personales, que a su vez ha trabajado en dos sectores, tanto en el privado como en el público, sin olvidar las obligaciones de transparencia, rendición de cuentas y de gobierno abierto que ya no puede ser considerado un mero acuerdo de buena voluntad, sino un ejercicio necesario para compartir información con la ciudadanía ante el escrutinio público de toda la población.

Actualmente, contamos con una serie de instrumentos que han proporcionado una definición de datos personales, entre los cuales destacan el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, y establece que es *"toda la información sobre una persona física identificada o identificable"*[2].

2 Gómez Robledo, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal,* México, Universidad Nacional Autónoma de México, pp. 16

No obstante, no ha sido nada sencillo gestionar todos los flancos en donde han surgido conflictos en materia de ciberseguridad, o bien, en aquellas circunstancias donde la información, como las bases de datos, han quedado expuestas a filtraciones que atentan contra la seguridad nacional de un país. Tal es el caso de las alertas emitidas por el Centro de Respuestas a Incidentes de México (CERT-MX) de la Guardia Nacional (GN), que difundió una alerta para las instituciones del sistema financiero con el fin de salvaguardar la seguridad de la información de sus clientes y empleados. Estas situaciones ponen en jaque a cualquier país, por ello, merecen una seria reflexión sobre sus efectos, costos y mejoras en sus sistemas operativos, que a su vez vuelve a poner en la mesa la necesidad de insistir en la innovación tecnológica.

Después de varias referencias sobre el desarrollo tecnológico, los datos personales y el impacto de las herramientas digitales en nuestra vida cotidiana se vuelven imprescindibles para hacer frente a otra nueva arista, la violencia digital que viven las niñas, niños, adolescentes y mujeres de manera asimétrica en un contexto de vulnerabilidad hacia ciertos sectores de la población. Las estadísticas se encuentran en focos rojos. Un ejemplo, la Unidad de Prevención e Investigación Cibernética informó que del total (4,739 reportes) de incidentes atendidos durante el primer semestre de 2023, relacionados con violencia digital, 61% de este total (2,556 reportes) fueron por acoso cibernético.

El libro que a continuación está por leer incorpora a sus reflexiones una serie de escenarios donde la violencia de género pone el dedo en el renglón -ya no como entrada gráfica- en la violencia digital que viven los niños, niñas, adolescentes y mujeres en redes sociales, correo electrónico o aplicaciones tecnológicas, lo que irremediablemente pone en riesgo su dignidad, desarrollo, libertad de expresión y hasta su propia vida.

Invito a cada lector a leer esta investigación realizada por la autora Ahahiby Becerril, quien ha puesto todo su esfuerzo en este libro, el cual busca instigar, reflexionar y encauzar los esfuerzos para tomar acción sobre el debido tratamiento de la información que deseamos compartir al público. Además, puntualizar que compartir datos personales no debería ser un hecho que coarte la libertad de expresión o bien, ponga en riesgo la vida de cualquier usuario. Sin olvidar, la responsabilidad que tienen las empresas como Amazon, Facebook y Google en la recolección masiva de datos.

RESUMEN

Al igual que sucede en el mundo físico, vivimos en un mundo digital inseguro. En los últimos años y debido a múltiples factores, la violencia se ha abierto espacio en nuestro mundo digital.

Sin embargo, hay un tipo específico de violencia dirigido a niñas, adolescentes y mujeres que se lleva a cabo particularmente: la violencia digital de género. Las mujeres somos foco de atención para diversos actores maliciosos con múltiples finalidades. Si bien la ciberseguridad es un proceso personal resultado de nuestra interacción con la tecnología, existen un número general de recomendaciones que tomar para prevenir ser víctimas de la violencia digital de género.

Este trabajo busca ser un aporte para concientizar a las adolescentes y mujeres sobre los riesgos y amenazas que se encuentran en el espacio digital, algunos especialmente dirigidos contra nosotras; también queremos brindar elementos básicos de ciberseguridad que nos permitan prevenir ser víctima de estas conductas.

LA REALIDAD DIGITAL DE NIÑAS, ADOLESCENTES Y MUJERES

De conformidad con el informe *Digital 2022 April Global Statshot de DataReportal*[1], más de 5 mil millones de personas nos encontramos usando Internet, lo que representa un aproximado de 63% de la población mundial. Es decir, más de la mitad del mundo usamos Internet, llevando a cabo actividades en línea. Mientras que la otra parte, muy probablemente, desconozca o no esté consciente de que gran parte de los servicios, programas e interacciones que pueden tener.

Las Tecnologías de la Información y la Comunicación (en adelante TIC), en específico Internet, han creado oportunidades para grupos históricamente desfavorecidos, abriendo la puerta a más voces en la conversación pública digital. La arquitectura participativa de la web 2.0 fomentó el intercambio no solo de conocimiento entre sus participantes, sino de ideas y brindó voz a quienes no la tenían o eran excluidos. Los blogs, Facebook, Twitter, TikTok, YouTube -entre otros-, ahora sirven como esferas públicas digitales, brindando un espacio e incluyendo la práctica de la discusión abierta sobre asuntos de interés común.[2]

Sin duda, el ciberespacio nos ha empoderado, no solo brindándonos la oportunidad de acceder a información, de compartir nuestras ideas, experiencias y conocimiento, de hacer redes de apoyo, sino también de ser partícipes en economías colaborativas, trabajo remoto, educación y salud digitales, así como foros públicos de discusión.

1 DataReportal (2022). *Digital 2022 Digital 2022 April Global Statshot*, disponible en: https://datareportal.com/reports/digital-2022-global-overview-report
2 Habermas, Jürgen (1991). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society,* Cambridge, The MIT Press.

Sin embargo, de la misma forma en que el ciberespacio nos presenta grandes bondades, también puede transformarse en un medio hostil, enfocado en grupos como las niñas, adolescentes y mujeres. Las TIC se han convertido en nuevos escenarios a través de los cuales se recrean y permanecen las desigualdades de género. Es una realidad que cuando las mujeres acceden a Internet enfrentan más violencia que los hombres.[3]

Comprender y hacer frente a la violencia que diariamente acontece contra niñas y mujeres es un requisito para poder lograr la igualdad de género y el desarrollo sostenible. Las vulneraciones a la privacidad, la exposición de nuestra información, el robo de datos personales o perfiles de grupos específicos, dirigido a las niñas, adolescentes y mujeres, nos expone a situaciones que afectan nuestros derechos humanos y libre desarrollo de la personalidad. La tecnología se ha empleado para facilitar el abuso y violencia contra nosotras.

De conformidad con el informe "Combatir la violencia en línea contra las mujeres y las niñas: Una llamada de atención al mundo", de ONU MUJERES[4], 73% de las mujeres en el mundo han estado expuestas o experimentado algún tipo de violencia en línea. Otros datos señalan que, en la distribución digital no autorizada de imágenes íntimas, 90% de las víctimas son mujeres. Mientras que 28% de las mujeres que fueron objeto de violencia basadas en TIC han reducido deliberadamente su presencia en línea.[5]

Las niñas y mujeres tienen 27 veces más posibilidades de ser acosadas en línea que los hombres. El Instituto Europeo para la Igualdad de Género (*European Institute for Gender Equality, EIGE*) estima que una de cada 10 mujeres ya ha experimentado una forma de violencia cibernética desde los 15 años.[6] Las cuestiones relacionadas con la seguridad, inclusive, pueden ser motivo para la oposición de las familias al uso de Internet o a poseer un smartphone. Por ejemplo, en la República Popular China y México, el acoso es una de las principales barreras para poseer o utilizar estos dispositivos.[7]

En nuestro país, de conformidad con el MOCIBA[8], las mujeres en el rango de edad de 18 a 24 años tienen una alta probabilidad de sufrir acoso sexual, además de amenazas físicas en línea. El ciberacoso nos afecta a 9.4 millones de mujeres; conductas como las insinuaciones sexuales (40.3%) y el envío de contenido sexual no solicitado (32.8%) están entre las primeras amenazas de este tipo.

3 UN Women. (2020) *COVID-19 Response: Online and ICT facilitated violence against women and girls during COVID-19 New York, NY: United Nations Entity for Gender Equality and the Empowerment of Women (UN Women),* disponible en: https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/brief-online-and-ict-facilitated-violence-against-women-and-girls- during-covid-19-en.pdf?la5en&vs52519.
4 UN Broadband Commission for Digital Development Working Group on Broadband and Gender (UN-BC-DDWGBG). (2015). *Cyber violence against women and girls: A worldwide wake up call* (pp. 1–70). Disponible en: https://www.unwomen.org/ ~/media/headquarters/attachments/sections/library/publications/2015/cyber_vio- lence_gender%20report.pdf?v=1&d=20150924T154259
5 Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias de la Organización de las Naciones Unidas (REVM-ONU). *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos*, A/HRC/38/4, 2018.
6 Instituto Europeo de la Igualdad de Género (EIGE). (2017). *La ciberviolencia contra mujeres y niñas*, disponible en: http://eige.europa. eu/rdc/eige-publications/cyber-violence-against-women-and-girls
7 GSMA (2015). *Connected Women 2015: Bridging the Gender Gap: Mobile Access and Usage in Low- and Middle-income Countries*, disponible en: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/02/Connected-Women-Gender-Gap.pdf
8 INEGI (2020). *Módulo sobre ciberacoso*, disponible en: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/MOCIBA-2020.pdf

Los datos anteriores brindan un panorama digital complicado para que las mujeres estemos seguras al navegar o emplear Internet, lo que va en detrimento de nuestros derechos humanos. Esta violencia digital de género a que estamos expuestas ha llevado que muchas se alejen y desconecten del mundo en línea, incrementando la desigualdad y brecha digital de género. La autocensura, aislamiento social, desactivación o suspensión de cuentas en línea o incluso desaliento en la profesión, son algunas de las consecuencias que trae consigo este tipo de violencia.

Nuestras identidades y género se utilizan como armas en contra nuestra. Los espacios digitales se encuentran plagados de resistencia masculina a las mujeres que en ellos participan. En lugar de cuestionar nuestras ideas, los abusos se dirigen a nuestras identidades, atacando nuestra apariencia, comportamiento sexual, fomentando estereotipos misóginos, e incluso de raza. En algunos casos estos atropellos surgen en respuesta al activismo o profesión que desempeñan las mujeres; en otros casos es el "precio a pagar", al compartir pensamientos, actividades, triunfos o experiencias a través de los medios digitales.

Una encuesta de Amnistía Internacional IPSOS MORI de 20179 informaba que más de tres cuartas partes (76%) de las mujeres que dijeron haber experimentado abuso o acoso en una plataforma de redes sociales hicieron cambios en la forma en que usaban las plataformas. Esto incluyó restringir lo que publican: 32% de las mujeres dijeron que habían dejado de publicar contenido que expresaba su opinión sobre ciertos temas. El 61% de las participantes señalaron haber sufrido abuso o acoso en línea, como resultado, habían sentido una baja autoestima o pérdida de confianza en sí mismas. Más de la mitad (55%) dijo que había padecido estrés, ansiedad o ataques de pánico después de haber sufrido abuso o acoso en línea.El 73% señaló que no había podido dormir bien como resultado de estas conductas. Más de la mitad (56%) indicó que el abuso o el acoso en línea significaba que no había podido concentrarse durante largos períodos. Alrededor de una cuarta parte (24%) de las que admitieron haber sufrido abuso señalaron que les había hecho temer por la seguridad de su familia.

La violencia digital de género tiene afectaciones que van más allá del entorno online, trasladando sus efectos al mundo físico, en ocasiones puede dejar un trauma permanente en su víctima, en casos extremos las perjudicadas pueden lesionarse a sí mismas y en otros más desafortunados les ha ocasionado la muerte.

La violencia y discriminación que sufrimos niñas, adolescentes y mujeres son problemas sociales globales, donde el abuso se inflige de manera sistemática, implacable y, a menudo, se tolera, si no se aprueba explícitamente. La violencia que se ejerce con el uso de las TIC

9 Amnistía Internacional, *Amnesty reveals alarming impact of online abuse against women*, noviembre, 2017, disponible en: https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

trasciende fronteras, culturas, razas y grupos sociales. Para poder hacerle frente debemos entender que la tecnología y el género no son entidades separadas, sino más bien coproducidas; la tecnología es una fuente y una consecuencia de las relaciones de género.[10]

Como mujeres, estamos acostumbradas a realizar gestiones de riesgos y elaborar estrategias para sortear diversos espacios públicos que resulten incómodos y nos generen miedo al pasar, nos preguntamos: ¿A dónde es seguro ir? ¿Es seguro caminar por esa calle? ¿Cómo debo comportarme o vestirme para minimizar la posibilidad de acoso? ¿Cómo reaccionaré si algo sucede? En el mundo físico, gran parte de las mujeres operamos con la conciencia de la posibilidad inminente de atención no deseada al transitar por los espacios públicos; parece que el entorno digital ha reflejado estas prácticas. Muchas mujeres disfrutamos el entorno online, adoptando tácticas del mundo real para navegar en espacios de línea de alto riesgo.

La Agenda 2030 para el Desarrollo Sostenible de Naciones Unidas considera que la tecnología es un medio para combatir la violencia que se desarrolla contra las niñas, adolescentes y mujeres. De la misma forma que la tecnología puede promover y perpetuar nuevas formas de violencia; el desconocimiento en el uso de las tecnologías nos hace menos consientes de los riesgos que corremos al usarlas. Para quienes no se conectan o lo hacen sin conocimiento, se agudiza la brecha en detrimento de sus derechos, a medida que más niñas y mujeres se suman al mundo en línea, para ellas surgen nuevos riesgos. La falta de una alfabetización digital y desarrollo de habilidades en la materia puede limitar la adopción de las TIC. Para sacar provecho a las tecnologías y minimizar los riesgos en el uso de estas, resulta necesario que las niñas y mujeres tengamos una alfabetización digital[11] adecuada, que nos permita conocer la importancia de aplicar la ciberseguridad en nuestro entorno privado.

10 Wajcman, Judy (2010). *Feminist theories of technology*. Cambridge Journal of Economics, 34(1), pp. 143–152.
11 Entendemos a la alfabetización digital como el desarrollo de habilidades técnicas que se requieren, como la capacidad de interactuar con los contenidos en línea de manera crítica.

Ante esto hay que preguntarnos,

¿CUÁL ES EL ROL DE LA CIBERSEGURIDAD EN MI VIDA?

- Ejercer y garantizar nuestros derechos humanos en el mundo *online* y *offline*
- Empoderarnos y reapropiarnos de nuestro espacio en línea
- Proteger nuestra identidad digital
- Gestión de riesgos en nuestra vida digital
- Ciberseguridad es un proceso personal en donde hay diversas realidades y necesidades

Imagen 1: ¿Cuál es el rol de la ciberseguridad en mi vida?

Para poder empoderarnos en el espacio público, y obtener el máximo aprovechamiento de las bondades que brinda la tecnología, debemos eliminar los tabúes relativos a que la ciberseguridad es un tema meramente técnico y que solo corresponde a personas con conocimientos especializados; al emplear dispositivos como smartphones, tabletas o computadoras, nos adentramos en el mundo digital y somos parte de esa corresponsabilidad de mantenerlo seguro. Entonces, la ciberseguridad:

- Nos ayuda a ejercer nuestros derechos humanos tanto en el mundo online, como en el offline;
- Permite empoderarnos y reapropiarnos de nuestro espacio digital;
- Nos ayuda a proteger nuestra privacidad, datos personales e identidad en línea;
- Habilita nuestro aprovechamiento de las TIC y el respectivo desarrollo.

Es por lo que este trabajo busca ser un aporte para concientizar a las personas, en especial a las adolescentes y mujeres, sobre los riesgos y amenazas que se encuentran en el espacio digital, algunos especialmente dirigidos contra nosotras, y brindar elementos básicos de ciberseguridad, que nos permita prevenir ser víctima de alguno de estos.

LA VIOLENCIA DIGITAL DE GÉNERO

En su informe, la Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer refiere que la violencia digital de género[12] constituye:

> "todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales como comercio electrónico, dirigida contra una mujer porque es mujer o que la afecta de forma desproporcionada".[13]

La Asociación para el Progreso de las Comunicaciones (2015) señala que la violencia contra las mujeres relacionada con el empleo de las tecnologías se refiere a los "actos de violencia de género cometidos, instigados o agravados, en parte o totalmente, por el uso de las TIC" [14], incluyendo a las plataformas de redes sociales y al correo electrónico, mismos que causan daño psicológico y emocional. Estos actos refuerzan perjuicios, causan pérdidas económicas y constituyen barreras en la participación de la vida pública de las mujeres.

Por su parte, en el Informe del Relator Especial sobre el Derecho a la Privacidad, del año 2019, cuyo tema central versó sobre las recomendaciones para la protección contra las vulneraciones de la privacidad por motivos de género, reconoció que:

12 De conformidad con lo dispuesto por la Resolución 73/148 de la Asamblea General de Naciones Unidas, en la actualidad no existe una terminología o definición consensuada de la violencia contra las mujeres y las niñas en medios digitales, y términos como "violencia en línea" y "violencia contra las mujeres relacionada con la tecnología de la información y las comunicaciones", "ciberviolencia contra las mujeres y las niñas", "violencia contra las mujeres y las niñas facilitadas por la tecnología" y "violencia de género en línea", se utilizan indistintamente; Crf. Naciones Unidas, *Intensificación de los esfuerzos para eliminar todas las formas de violencia contra mujeres y las niñas. Informe del Secretario General*, A/77/302, 18 de agosto de 2022.

13 Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias de la Organización de las Naciones Unidas (REVM-ONU). *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos*, A/HRC/38/4, 2018.

14 Association for Progressive Communications (2015). *Technology-related violence against women, A briefing paper*, disponible en: https://www.apc.org/sites/default/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf

"Las vulneraciones a la privacidad por motivos de género son una forma sistémica de denegación de los derechos humanos, son discriminatorias por naturaleza y a menudo perpetúan la desigualdad de las estructuras sociales, económicas, culturales y políticas;" (párr.19).[15]

Señalando que la privacidad, la protección de datos personales y el género, se han considerado aspectos de "segundo orden", pero su complejo impacto en la sociedad reviste importancia crítica (párr. 17)[16]. Estas vulneraciones y sus daños no solo afectan a las mujeres, sino a la sociedad en su conjunto, además de socavar la democracia.

Una de las formas de violencia digital de género que gana más espacios, es la misoginia digital. Esta constituye una extensión de la que se da en el mundo físico, con la finalidad de restringir la libertad de las mujeres al usar los medios digitales públicos como iguales. Los atacantes buscan intimidar, avergonzar o desacreditar a las mujeres para excluirlas del espacio digital. Con la primera, explotan el miedo de las mujeres a la violencia digital o física; pensemos en ataques de denegación de servicio (DoS)[17] o ataques de denegación de servicio

15 A/HRC/43/52, *Informe del Relator Especial sobre el Derecho a la privacidad*, marzo 2020, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/071/69/PDF/G2007169.pdf?OpenElement
16 A/HRC/43/52, *Informe del Relator Especial sobre el Derecho a la privacidad*, marzo 2020, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/071/69/PDF/G2007169.pdf?OpenElement
17 Denominado Denial Of Service (DoS), este ataque se realiza a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones; Cfr. Instituto Nacional de Ciberseguridad de España (INCIBE), *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario*, INCIBE, 2020, p. 35

distribuido (DDoS)[18], cuyo objetivo es restringir el acceso a la web (o a un sitio en particular), o "bombardear" su correo electrónico con correo spam[19], haciendo que las víctimas se sientan vulnerables.

Otra táctica de intimidación es el *doxing*, en donde los atacantes recopilan información personal sobre una mujer (en este caso), y la publican sin su consentimiento con la intención de atraer a otros acosadores. Dependiendo la información publicada, también puede derivar en avergonzar o desacreditar a la víctima. Al avergonzar, buscan explotar su comportamiento o apariencia física. La difusión de imágenes íntimas sin consentimiento es una táctica empleada con esta finalidad. Estas imágenes ni siquiera necesitan ser reales para el logro de su objetivo, herramientas como las *deepfakes* u otras formas de tecnología permiten editar estas imágenes o videos.

18 Distributted Denial Of Service (DDoS) consituye un DoS, pero las peticiones se hacen desde diversos orígenes, de esta forma es más efectivo y más complicado detener y determinar su procedencia; Cfr. INCIBE, *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario,* INCIBE, 2020, p. 35

19 También conocido como "correo basura", es un tipo de correo electrónico caracterizado por no ser solicitado por el receptor y que se envía en grandes cantidades con fines publicitarios o como complemento de actividades maliciosas como ataques de phishing; Cfr. Instituto Nacional de Ciberseguridad de España (INCIBE), *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario*, INCIBE, 2020, p. 32.

Desacreditan a las mujeres empleando estereotipos sexistas para devaluarlas o a sus contribuciones. Los esfuerzos por desacreditar a las mujeres en medios digitales son muy comunes. Estos explotan los estereotipos de género sugiriendo que la víctima no tiene nada que aportar o que no es una fuente creíble. Los estereotipos basados en la identidad se esfuerzan por devaluar el conocimiento, las opiniones y experiencias de las víctimas.

En casos extremos de misoginia digital aparecen grupos como los "incels" o "célibes involuntarios", que constituye un movimiento en foros online de hombres cuya motivación ideológica es el odio hacia las mujeres; estos grupos protestan por su situación de inferioridad en la jerarquía masculina[20], en la cual desean ascender, expresando su frustración por no poder acceder a relaciones sexuales con mujeres, a las que consideran tienen derecho de forma natural. A través de la creación de una networked misoginy, se dedican al acoso sexual de mujeres en la "manosfera" (manosphere)[21]. Las conductas realizadas por estos grupos extremistas incrementan la probabilidad de que el acoso sexual y violencia que se ejerce en el mundo digital contra mujeres y niñas preceda incluso fuera de Internet.[22]

20 Isla-Joulain, Gabriel Luis, *Célibes involuntarios. ¿Terroristas? Análisis cualitativo del fenómeno "InCel" y discusión conceptual sobre el terrorismo*, Revista de Derecho Penal y Criminología, No. 24 (Tercera Época), 2020, pp. 193-244.

21 Este espacio digital que, al igual que muchos otros, se basa en crear la idea de un sentimiento de pertenencia, constituye un conglomerado de espacios virtuales heterogéneos que dan cabida a una multitud de movimientos masculinos basados en la propagación de discursos misóginos y antifeministas; Cfr. Ging, D. y E. Siapera (2018). *Special issue on online misogyny*, Feminist Media Studies 18(4), pp. 515-524, disponible en: https://doi.org/10.1080/14680777.2018.1447345

22 El 23 de mayo de 2014, Elliot Rodger, de 22 años, asesinó a seis personas, hirió a 13 y se suicidó durante un tiroteo en Isla Vista (California, EE.UU.), un día después de publicar en YouTube un video en el que anunciaba "su venganza contra la humanidad", tras una vida sin relaciones sexuales con mujeres. El 1 de octubre de 2015, Christopher Harper-Mercer, de 26 años, asesinó a nueve personas, hirió a siete y se suicidó en un tiroteo en el Umpqua Community College (Roseburg, Oregón, EE.UU.), tras dejar un manifiesto en el que, además de proclamas racistas y alabanzas a asesinos en masa, culpa a las mujeres de su soledad. En el año 2018, Alek Minassian, de 25 años, escribió en un post en Facebook: "La Rebelión Incel ha comenzado", minutos antes de arrollar con una furgoneta y matar a 10 personas (ocho mujeres y dos hombres), causando heridas a otras 16. En junio de 2022, Minassian fue sentenciado a cadena perpetua.

El 23 de abril de 2018, Alek Minassian, de 25 años, asesinó a 10 personas e hirió a 16 atropellándolas con una furgoneta en Toronto (Ontario, Canadá), tras escribir en un post de Facebook: "¡La Rebelión Incel ya ha comenzado! ¡Derrocaremos a todos los Chads y Stacys! [23] ¡Saluden todos al supremo caballero Elliot Rodger!".

Además, el acoso sexual en línea también puede estar relacionado con el discurso de odio por razón de género, que obedece al propósito de difundir, incitar, promover o justificar el odio por motivos de sexo.[24]

No podemos minimizar ni normalizar el abuso en línea en contra de las mujeres. ¿Acaso nuestro costo de usar el espacio público digital será vivir con la incertidumbre y preocupación constante porque es difícil saber qué opinión, trabajo o contribución desencadenará un ataque?

23 De conformidad con Jaki et al., la cultura Incel posee un vocabulario propio, por ejemplo, llaman a los hombres atractivos y exitosos "Chad", "Tyrone" o "Alphas"; a las mujeres atractivas y promiscuas "Stacy"; a las mujeres no atractivas "Becky"; y a sí mismos "célibes involuntarios", "Betas" o "no-Alphas"; Cfr., Jaki, Sylvia., De Smedt, Tom., Gwóźdź, Maja., Panchal, Rudresh., Rossa, Alexander & De Pauw, Guy. (2018). *Online hatred of women in the Incels.me forum: linguistic analysis and automatic detection. Journal of Language Aggression and Conflict,* 7(2), pp. 240-268, disponible en: https://www.jbe-platform.com/content/journals/10.1075/jlac.00026.jak

24 Naciones Unidas, *Intensificación de los esfuerzos para eliminar todas las formas de violencia contra mujeres y las niñas. Informe del Secretario General,* A/77/302, 18 de agosto de 2022, párr. 9.

LA PROTECCIÓN DE DATOS PERSONALES EN UN CIBERESPACIO INSEGURO

Toda persona, con independencia de su sexo biológico, características sexuales, orientación sexual, identidad o expresión de género, tiene derecho a disfrutar plenamente de los derechos a la privacidad y protección de sus datos personales (PDP).

En este mundo híbrido en el que nos desarrollamos, navegamos gran parte de nuestra vida a través de aplicaciones (apps) y somos prosumidoras del contenido digital que ahí se gestiona. Nos relacionamos, jugamos, compramos, aprendemos, trabajamos, nos ejercitamos y llevamos un monitoreo de nuestra salud a través de estas. Vivimos una vida impulsada por apps. Y estas, basan su modelo de negocio en el tratamiento de datos personales. Pueden monitorear desde nuestra ubicación hasta nuestros signos y ciclos vitales.

Un ejemplo de ello son las *women´s health apps,* que conforman parte del ecosistema femtech[25]. Estos servicios permiten planear o evitar embarazos, monitoreando el ciclo menstrual. Algunas, como *Natural Cycles*,[26] han digitalizado el método del "ritmo", para ayudar a concebir o prevenir un embarazo. Esta, denominada "anticonceptivo digital", es una aplicación que combina un algoritmo con lecturas diarias de la temperatura corporal basal (BBT), es decir la temperatura corporal en reposo, para predecir la fertilidad en un día determinado.

25 Constituyen productos y servicios de base tecnológica enfocados en la salud de la mujer, abarcan un amplio mercado de herramientas digitales que incluye una amplia gama de necesidades de salud de las mujeres, consejos nutricionales personalizados, entrenamiento para perder peso, extractores de leche de alta tecnología que registran cuándo y cuánto se extrae, ciclo mestrual, menopausia, entre otros, y que para 2025 podría valer jasta USD$50 mil millones; Cfr. McKinsey, *Los albores de la revolución FemTech*, 14 de febrero 2022, disponible en: https://www.mckinsey.com/featured-insights/destacados/los-albores-de-la-revolucion-femtech/es

26 Revista Wired, *The Best Women´s Health Apps*, Period, Wired, 2018, disponible en: https://www.wired.com/story/best-womens-health-apps-2018/

Sin embargo, debemos estar conscientes de que cualquier información que se recopile (que puede incluir historial de anticonceptivos, frecuencia de relaciones sexuales) puede llegar a combinarse con otros datos o inclusive considerar que en una economía de la vigilancia, una exposición de esta información podría dejar expuesta referencias que puedan ser empleadas para rastrear, arrestar e incluso perseguir a una persona que se hubiera practicado un aborto, o que a partir de su historial de búsquedas tuviera la intención de hacerlo.[27]

Es una realidad que la información que compartimos diariamente con las apps que manejan nuestra vida y las interacciones que llevamos a cabo en el mundo digital, puede exponernos a diversos tipos de conductas y, como usuarias, tal vez no somos del todo conscientes de los datos que, sobre nosotras, estamos generando.

Las violaciones a la privacidad en Internet constituyen un reflejo de transgresiones más amplias en entornos físicos. El tema central del Informe del relator Especial sobre el Derecho a la Privacidad, del año 2020 (A/HRC/43/52), fueron el estudio y recomendaciones para la protección de vulneraciones de la privacidad por motivo de género, especialmente ante los desafíos que plantean las tecnologías. En el informe se reconoció que las vulnerabilidades de la privacidad por motivos de género son una forma sistémica de denegación de derechos humanos, discriminatorias por naturaleza, que perpetúan la desigualdad de las estructuras sociales, económicas, culturales y políticas. Además, señala que factores como la etnia, las creencias, la cultura, origen social, edad, independencia económica, marcos jurídicos y políticos determinan las experiencias de privacidad.[28]

Comprender los ciberataques y amenazas como fundamentalmente entrelazados con el poder y la desigualdad nos ayuda a comprender por qué el abuso basado en la identidad se distribuye de manera desigual entre las mujeres. En su mayoría, los ataques son particularmente severos para:

> **1)** mujeres que son miembros de múltiples grupos marginados; **2)** aquellas que hablan públicamente en o sobre esferas dominadas por hombres; y **3)** mujeres que son percibidas como feministas o no cumplen con las normas tradicionales de género. Por supuesto, estas categorías no son mutuamente excluyentes.

27 Vesoulis, Abby, *How a Digital Abortion Footprint Could Lead to Criminal Charges- And What Congress Can Do About it,* may 2022, TIME Magazine, disponible en: https://time.com/6175194/digital-data-abortion-congress/
28 A/HRC/43/52, *Informe del Relator Especial sobre el Derecho a la privacidad*, marzo 2020, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/071/69/PDF/G2007169.pdf?OpenElement

Desde el ámbito digital, la violencia puede reproducirse a través de múltiples formas: correos electrónicos, mensajes instantáneos con contenidos amenazantes, de acoso o extorsión, acecho, "apagones" de Internet, desinformación e inclusive videos desarrollados con deepfakes, que atenten contra su imagen y dignidad. Este tipo de conductas pueden causar angustia, miedo, así como daños tanto emocionales y en algunos casos físicos a su víctima. Una de las grandes realidades es que la violencia en línea puede convertirse en violencia física.

Durante la epidemia de COVID-19, la violencia facilitada por las TIC se extendió. Las mujeres y las niñas se encontraron sujetas a esta violencia digital en forma de amenazas físicas, acoso sexual, acecho y trolling sexual. Los medios de comunicación y las organizaciones de derechos de las mujeres han documentado casos específicos de videos pornográficos no solicitados mostrados mientras las mujeres participaban en eventos sociales en línea[29], amenazas de violencia y contenido sexista dañino[30] y *zoombombing*[31] durante videollamadas que mostraban material con carga racial y sexualmente explícito a las mujeres.[32]

29 Glaser, A., Kesslen, B. & Solon, O., *In video chats, familiar forms of online harassment make a comeback*, march 25, 2020, disponible en: https://www.nbcnews.com/tech/security/video- chats-familiar-forms-online-harassment-make- comeback-n1168806

30 Mudgway, C. & Jones, K., *As use of digital platforms surges, we'll need stronger global efforts to protect human rights online*, April 8, 2020, disponible en: https://theconversation.com/as-use-of-digital-platforms- surges-well-need-stronger-global-efforts-to-protect- human-rights-online-135678.

31 El "**bombardeo por zoo**" describe la práctica de interrumpir una llamada de videoconferencia, o infiltrarse en ella, y mostrar a los participantes de forma inesperada material de contenido racial o sexualmente explícito; Cfr. Naciones Unidas, *Intensificación de los esfuerzos para eliminar todas las formas de violencia contra mujeres y las niñas. Informe del Secretario General*, A/77/302, 18 de agosto de 2022

32 Loots, L., Dartnall, E., Kelly, J., *Online safety in a changing world- COVID-19 and cyber violence*, April 4, 2020, disponible en: http://www.svri.org/blog/online-safety-changing-world- %E2%80%93-covid-19-and-cyber-violence

La inseguridad que las niñas, adolescentes y mujeres sentimos al navegar en Internet es un menoscabo al libre disfrute de los derechos humanos y empleo de esta tecnología para nuestro desarrollo. Ante esto, ¿las mujeres deberíamos entender a la privacidad y la PDP de forma diferente?

Para muchas personas, el Internet simplemente funciona. Sin embargo, no dimensionamos o no nos importa, con quién, cómo o cuál información estamos compartiendo con empresas e individuos. Nuestra conducta online, hábitos de consulta, preferencias de compras, listas de contactos, historial de ubicación, y muchos más son compartidos, vendidos y revendidos en una larga cadena de suministro de datos que parecería no terminar.

De la misma forma, la conciencia sobre los derechos de privacidad y de la PDP no equivale a una comprensión de cómo hacer uso de ellos. Tampoco implica un cambio de comportamiento. Si no podemos confiar en que nuestra información se está manejando correctamente, podemos limitar nuestra disposición a compartirla, por ejemplo, con el médico o en las redes sociales.

La privacidad es un concepto confuso y subjetivo. Aunque muchas usuarias se ocupan de conservarla en línea, no siempre toman precauciones para protegerla.[33] Además, estudios recientes sugieren que las mujeres generalmente están más preocupadas por la privacidad y la protección de la información, en comparación con los hombres.[34] Aun así, las mujeres pueden estar más inclinadas a divulgar información personal en las redes sociales[35] y a cambio de beneficios para el cliente.[36]

Hace tiempo que como usuarias atendemos cómo mantener segura nuestra privacidad y PDP en línea. Sin embargo, los pensamientos y las acciones no siempre son consistentes. En ocasiones, las preocupaciones por la forma en que nuestros datos personales son tratados en el ciberespacio no necesariamente llevan a proteger o tener una adecuada gestión del riesgo al compartirlos en medios digitales.

Debemos enfocarnos en prevenir las violaciones a nuestros derechos en el mundo digital y mitigar las posibles consecuencias dañinas. Es una realidad el peligro de que nuestra información pueda caer en poder de delincuentes y actores maliciosos, así como de perderlas por algún incidente. Sí sirven las medidas que van desde realizar contraseñas más robustas, cambiarlas con frecuencia y emplear el doble factor de autenticación. O no tener activa de forma constante el GPS, evitar ser etiquetadas o no etiquetar a personas, sin su autorización, en imágenes dentro de redes sociales, inclusive instalar sistemas de retransmisión de correo electrónico para evitar posibles abusos.

33 Gerber N., Gerber P. & Volkamer M. (2018). *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior*, Comp Secur (77), pp. 226–261.
34 Tifferet S. (2019). *Gender differences in privacy tendencies on social network sites: A meta-analysis*, Comp Hum Behav, (93), pp. 1–12.
35 Park N. & Kim Y. (2020). *The impact of social networks and privacy on electronic word-of-mouth in Facebook: Exploring gender differences.* Int J Comm (14), pp. 176–199.
36 Rowan. M., & Dehlinger, J., (2014). *Observed gender differences in privacy concerns and behaviors of mobile device end users,* ProcComp Sci (37), pp. 340–347.

CONOCIENDO LAS AMENAZAS CIBERNÉTICAS

Al relacionarnos con la tecnología, la ciberseguridad resulta un elemento esencial que no debe ni puede ser ignorado, así como el elemento humano en este ecosistema. Operamos en un mundo en el que 95% de los problemas de seguridad cibernética pueden atribuirse a un error humano.[37]

La ciberseguridad ha surgido como una área emocionante y emergente. Sin embargo, aún nos queda mucho por delante para concientizar a las niñas, adolescentes y mujeres sobre cuál es nuestro rol en este tema.

Es una realidad que los actores maliciosos cada vez atacan más objetivos de elección de manera más eficiente, que los de oportunidad. Al tener mayor información y dispositivos interconectados, no solo ampliamos la superficie de ataque, sino que exponemos más datos y en algunos casos más sensibles, lo que no solo incrementa el número de víctimas, sino su impacto.

37 World Economic Forum (2022). *The Global Risks Report 2022. 17th edition. Insight Report*, WEF, 2022, p. 45, disponible en: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

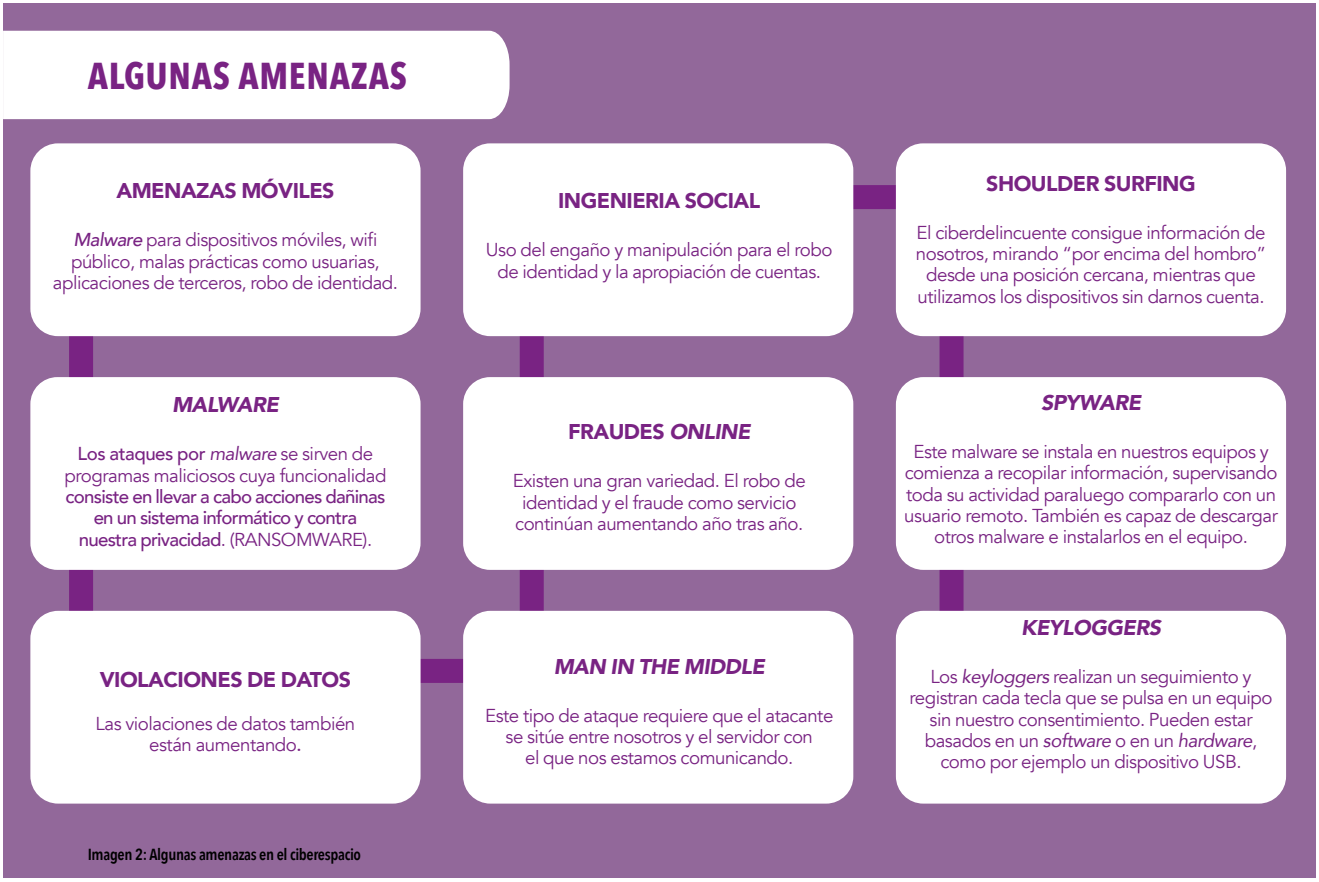


Imagen 2: Algunas amenazas en el ciberespacio

La violencia digital de género se ha visto agravada por el crecimiento en el uso malicioso de tecnologías de inteligencia artificial (IA). Un ejemplo es el empleo de videos pornográficos que se generan con esta tecnología para perjudicar a la víctima. Según el informe de la organización estadounidense *Cyber Civil Right Initiative*, titulado *"2017 National-wide online study of non-consensual porn: results"*[38], uno de cada ocho usuarios de las redes sociales ha sido objetivo de la "pornografía no consensuada" (*non-consensual pornography*, NCP). Esta incluye fenómenos como la "pornografía de venganza" y "pornografía falsa", actos de publicidad de cualquier imagen sexual inequívoca de una persona en forma de fotografías o películas sin su consentimiento previo empleando herramientas de IA.

38 Civil Rights Initiative (2017). *2017 Nationwide online study of non-consensual porn: results. A Summary Report*, Civil Rights Initiative, Inc., disponible en: https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

ALGUNAS AMENAZAS ESPECÍFICAS CONTRA NIÑAS Y MUJERES

CREEPSHOT

Se refiere a una foto tomada por un hombre a una mujer o niña en público sin su consentimiento. Las fotos suelen centrarse en los glúteos, las piernas o el escote de la víctima.

CYBERFLASHING

Es el envío de fotografías obscenas a una mujer sin su consentimiento con el objetivo de molestarla, intimidarla o incomodarla.

DEEPFAKE

Técnica de inteligencia artificial que permite editar videos falsos de personas que aparentemente son reales mediante el uso de algoritmos de aprendizaje y videos o imágenes ya existentes.

DOWNBLOUSING

Registro sin consentimiento de fotografías tomadas por arriba de la blusa de una mujer.

GASLIGHTING

Es una forma de abuso psicológico realizado mediante la manipulación de la realidad de la víctima, con lo cual se busca que se cuestione su cordura, su memoria o su percepción. (Internet of Things)

Imagen 3: Algunas amenazas específicas contra niñas y mujeres

El uso de tecnología de pornografía *deepfake* puede ejercer un costo único contra las mujeres: las desalienta, las desacredita y las silencia. Estos son materiales de archivo alterado sintéticamente en el que el rostro o el cuerpo representado se ha modificado digitalmente para que parezca otra persona u otra cosa. Dichos videos, rara vez creados con el permiso de las implicadas, brindan oportunidades para el abuso y la explotación. De la misma forma que podrían generar amenazas a la seguridad nacional más amplias, ya que podrían usarse para avergonzar, socavar o explotar a agentes de inteligencia, candidatas a cargos políticos, periodistas u otros actores estatales. El 96% de todos los *deepfakes* representan a mujeres en pornografía inventada y no consentida.[39] Una investigación identificó un bot en la aplicación de mensajería Telegram que creó más de 668,000 imágenes pornográficas inventadas de mujeres sin su consentimiento.[40]

39 Aja Romano, *Deepfakes are a real political threat. For now, though, they're mainly used to degrade women*, Vox, octubre 7 de 2019, disponible en: https://www.vox.com/2019/10/7/20902215/deepfakes-usage-youtbe-2019-deeptrace-research-report

40 Jane Lytvynenko and Scott Lucas, *Thousands Of Women Have No Idea A Telegram Network Is Sharing Fake Nude Images Of Them*, BuzzFeed News, octubre 20 del año 2020, disponible en: https://www.buzzfeednews.com/article/janelytvynenko/telegram-deepfake-nude-women-images-bot

La desinformación sexualizada, dirigida por género o misógina, tiene como finalidad desacreditar a las mujeres y desalentar su participación en el espacio público. Estas publicaciones de género consisten en: "[una combinación de] viejas actitudes sexistas arraigadas con el anonimato y el alcance de las redes sociales en un esfuerzo por destruir la reputación de las mujeres y sacarlas de la vida pública"[41] . Y está basada en la difusión de información e imágenes engañosas o inexactas contra las mujeres en la política, siguiendo historias que a menudo se basan en la misoginia y la desconfianza hacia las mujeres en la política, con frecuencia refiriéndose a su sexualidad.[42]

La desinformación también es un problema de ciberseguridad. En el último informe de ENISA, se le ha identificado como una de las ocho categorías de amenazas a la ciberseguridad.[43] La gravedad del impacto de la desinformación sobre la confidencialidad, integridad y disponibilidad de la información hace necesario considerarla como una forma de ciberataque. En muchos sentidos, la desinformación es similar a un ciberataque, donde en lugar de comprometer un sistema informático, compromete nuestras capacidades cognitivas.

La desinformación (el intercambio de datos deliberadamente engañosos o sesgados) ha sido clasificada formalmente como un trastorno de la información por el Consejo de Europa.[44] Su objetivo es cambiar los pensamientos y comportamientos de un individuo, y en consecuencia influir en la opinión pública al alterar la visión de la realidad o acentuar las creencias previas de uno para interrumpir la búsqueda de la verdad. La información engañosa puede dejar a las personas confundidas acerca de hechos básicos y eventos actuales, creando una situación peligrosa que afecta la seguridad pública, la reputación de la organización o las funciones gubernamentales. Tales interrupciones se han acuñado como piratería cognitiva, donde dichas prácticas pueden resultar en una amenaza mayor.

El daño causado por la desinformación puede ser difícil de reparar, ya que las personas forman opiniones basadas en sesgos cognitivos y de confirmación. La naturaleza engañosa de esta práctica se acentúa aún más por las presiones económicas y los modelos centrados en la publicidad que la incentivan para sobrecargar los canales de información, a menudo ahogando la verdad. Así como la tecnología y la expansión de las redes sociales aumentan los riesgos de ciberseguridad, exacerban el impacto de la desinformación.

41 Nina Jankowicz, *How Disinformation Became a New Threat to Women*, Coda Story, december 11, 2017.
42 Lucina Di Meco, *#SHEPERSISTED: Women, Politics & Power in the New Media World*, The Wilson Center, Fall 2019.
43 European Union Agency for Cybersecurity (2021). *ENISA Threat Landscape 2021:* April 2020 to Mid July
44 Wardle, C.; Derakshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe: Strasbourg, Francia, disponible en: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

LA GESTIÓN DE RIESGOS EN NUESTRA VIDA CIBERNÉTICA

Para un mejor aprovechamiento del mundo digital es menester reconocernos en el centro de nuestra ciberseguridad. Nuestro empoderamiento en el ciberespacio y nuestra relación con la tecnología dependen de ello, en gran medida.

Antes de pensar en la ciberseguridad en la PDP, debemos repensar nuestra relación con la tecnología y preguntarnos:

- ¿Qué tipo de usuaria soy?
- ¿Cuál es mi relación con la tecnología?
- ¿Qué significa la tecnología para mí?
- ¿Para qué la uso?
- ¿Cuáles son los derechos que tengo en el uso de las tecnologías?
- ¿Qué significa la ciberseguridad para mí?

La interacción que como usuarias tenemos con la tecnología y nuestra información, en gran medida determinará el o los controles y riesgos que estarán involucrados en la ciberseguridad. No obstante, debemos considerar que los retos para la protección de nuestros datos personales se encuentran reflejados en los siguientes principios:

- Disponibilidad: la información se encuentra disponible para las partes o personas autorizadas cuando resulte necesario;
- Integridad: la información está protegida (durante todo su ciclo de vida) de las modificaciones no autorizadas;
- Confidencialidad: una serie de reglas limita el acceso a la información a personas que no están autorizadas (a menudo equiparada a la privacidad).

Para algunas personas la confidencialidad resultará primordial; otras preferirán acceder a la información, correos, fotos, mensajes, redes sociales en cualquier momento, por lo que privilegiarán la disponibilidad.

Al igual que el mundo físico, con el uso de las TIC nos enfrentamos a una serie de amenazas y vulnerabilidades. A la intimidación se le considera una circunstancia desfavorable que puede ocurrir, y que cuando esto sucede tiene consecuencias negativas sobre los activos de información, que pueden o no ser datos personales. Estas pueden ser accidentales o intencionadas. Aprovechan las vulnerabilidades, que a su vez constituyen fallos o debilidades que existen en los sistemas[45] y, sobre todo, en los humanos. Cuando se detecta una vulnerabilidad en un software o hardware, el desarrollador lo soluciona publicando una actualización de seguridad en el producto. De ahí la importancia de actualizar los sistemas.

La gama de posibles medidas de ciberseguridad personal es amplia, pero hay un número finito de medidas básicas que es importante considerar. Antes de elegir algún tipo de medidas o herramientas tecnológicas que nos coadyuven a resguardar nuestra información, resulta imprescindible identificar los riesgos asociados a la tecnología. Para ello debemos concientizar lo siguiente: Todas las computadoras se pueden infectar con malware; todas las computadoras pueden ser incautadas con ransomware. Todas las computadoras pueden ser arrastradas a un botnet y pueden sanitizarse de forma remota.[46]

45 En los sistemas se emplean programas llamados *"exploits"*.
46 Schneier, Bruce (2018). *Click here to kill everybody. Security and Survival in a Hyper-Connected World*, New York: Norton & Company, p. 26.

Sumemos el uso de Internet, que en estos últimos meses ha sido el sistema nervioso a través del cual sociedades, gobiernos y economías enteras han tenido continuidad. Si consideramos la tendencia de que todo dispositivo o computadora se conecten a Internet y a los sistemas entre sí para compartir información, expandimos la superficie de ataque. Como señaló el entonces presidente de ICANN[47] en el año 2011, durante la *London Conference on Cyberspace, Rod Beckstrom:*

- *Anything connected to the Internet can be hacked.*
- *Everything is being connected to the Internet.*
- *So everything is becoming vulnerable and a new dynamic of cyber crimes countered by security measures, countered by new criminal efforts, and so forth, is now unleashed.*[48]

Como usuarias, nos corresponde una parte de la responsabilidad de mantener nuestros datos personales seguros en medios digitales. Las vulneraciones de seguridad o brechas de datos son atribuibles a errores en la tecnología o de los humanos. Alguna vez has realizado lo siguiente:

- Navegar en páginas inseguras;
- Entregar datos personales sin verificar a quién se los entregas;
- Usar la misma contraseña en múltiples sitios o dispositivos;
- Abrir todos los archivos anexos que vienen en los correos electrónicos (sin verificar la fuente);
- Compartir el usuario y contraseña (solo con amigas/os).

La forma que tenemos para poder asegurar nuestros datos personales en el mundo digital en que nos desarrollamos es a través del *awareness* y entrenamiento continuo.

47 Acrónimo en inglés para: *Internet Corporation for Assigned Names and Numbers*

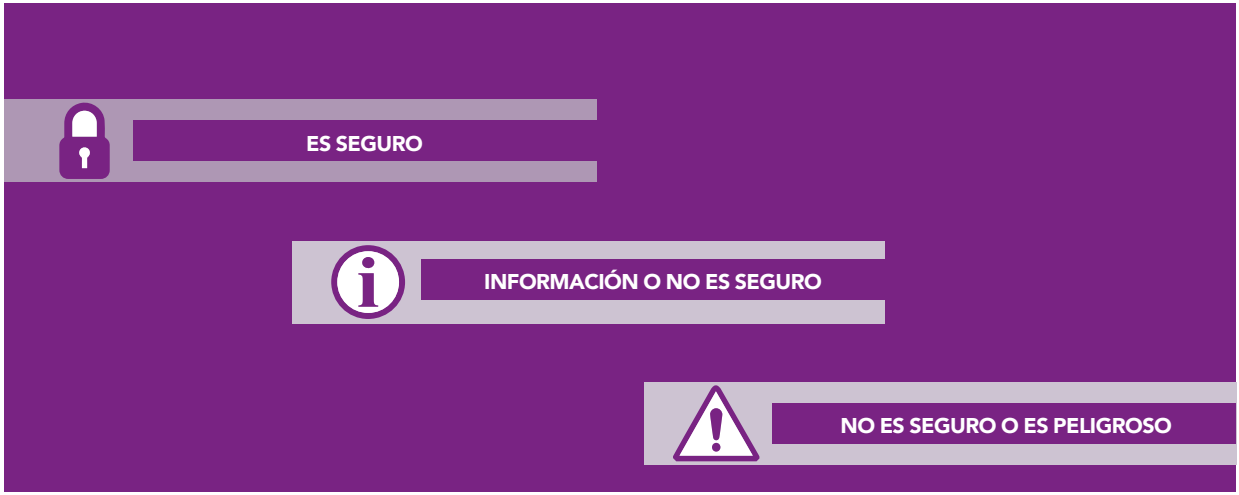
48 "1) Todo lo que esté conectado al Internet puede ser pirateado; 2) Todo está conectado a Internet; 3) Entonces todo se vuelve vulnerable y ahora se desata una nueva dinámica de ciberdelitos contrarrestados por medidas de seguridad, contrarrestadas por nuevos esfuerzos delictivos, etc." (traducción de la autora); Beckstrom, Rod (November 2011). The London Conference on Cyberspace. Obtenido de *Internet Corporation for Assigned Names and Numbers (ICANN),* disponible en: https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf

BUENAS PRÁCTICAS	MALAS PRÁCTICAS
Utiliza contraseñas con una frase o PIN para bloquear tus dispositivos.	Utilizar tu fecha de nacimiento o bloqueos con patrones sencillos.
Considera el uso de tu huella digital.	
Realiza copias de seguridad de tus archivos de forma periódica.	
Cifra tu dispositivo portátil y mantén tus dispositivos contigo en todo momento.	Conectar un cable USB a tu dispositivo, podría contener malware.
Asegura el bloqueo automático de pantalla en tus dispositivos, después de un breve período de inactividad.	Dejar tu dispositivo accesible sin algún control de seguridad.
Asegúrate de haber realizado un borrado seguro de toda tu información antes de vender o deshacerte de tus dispositivos.	No eliminar la información personal antes de deshacerte o regalar tus dispositivos.

Las copias de seguridad se pueden realizar en dispositivos externos o en la nube. Esta práctica constituye una medida de precaución para que nuestra información pueda recuperarse en caso de pérdida, robo o daño. Idealmente las copias de seguridad de información importante deben mantenerse en, al menos, otro dispositivo.

Navega en sitios seguros. No descargues contenidos de páginas o e-mails desconocidos. Evita dar clic en links que te remitan por correos electrónicos, sin que conozcas al remitente. Antes de hacerlo, posiciona el cursor encima del link para observar la página final, sin abrirlo o dar clic.

Al navegar, gestiona la seguridad y privacidad de tu navegador. Puedes navegar en modo privado o incógnito, de esta forma se iniciará una sesión sin utilizar los datos ya almacenados en el navegador y al terminar se borrarán las cookies, el historial de navegación y otros datos que hayas creado. Recuerda siempre cerrar la sesión de los lugares en los que navegues y verificar que los sitios en los que navegues son fiables. Al acceder a un sitio web que utiliza HTTPS (conexión segura), el servidor utiliza un certificado para demostrar la identidad de la página web a los navegadores. Para comprobar la seguridad del sitio, debemos fijarnos en el icono del estado de seguridad situado a la izquierda de la dirección web:



Además, al navegar, recuerda lo siguiente:

BUENAS PRÁCTICAS	MALAS PRÁCTICAS
Revisa los avisos de privacidad y cuida tu información (con quién y cómo la compartes).	Nunca des tus datos personales a cualquiera.
Gestiona tu identidad en línea: una profesional y otra personal.	No expongas toda tu información en redes sociales.
Utiliza las preguntas de seguridad de forma inteligente.	No reveles información personal como tus miedos, gustos personales, pasatiempos, etc.

PROTEGE TU NAVEGACIÓN EN LOS DISPOSITIVOS

No abras mensajes que parezcan sospechosos.
Confirma con la persona remitente.

No te conectes en wifi públicas. Si tienes necesidad de hacerlo, cuida la información que compartes (no contraseñas, ni datos bancarios u otros datos personales sensibles).

Al navegar verifica que el sitio sea seguro.

Si utilizas dispositivos ajenos,
navega en incógnito o forma privada.

No almacenes tus contraseñas en dispositivos ajenos.

Descarga apps solo de sitios oficiales y seguros.

Usa contraseñas de bloqueo en tus dispositivos.

Asegúrate de siempre cerrar tus sesiones.

Borra el historial de búsqueda de tu navegador.

Imagen 4: Protege tu navegación en los dispositivos

Otras medidas permanentes que deben ser parte de nuestra vida digital diaria son:

a) Actualizaciones. Las vulnerabilidades son consustanciales al software. Muchos delincuentes acceden de forma exitosa a los dispositivos y a la información a través de las vulnerabilidades en una red de computadoras o un dispositivo conectado a Internet.

Si bien las empresas y desarrolladores invierten en encontrar vulnerabilidades en los softwares, en algunas ocasiones estas pueden ser desconocidas para el productor de hardware y software, dándole al delincuente o actor malicioso bastante tiempo para explotarlas a su favor.

Hay otros resquicios, que se dan a conocer, que hacen más "sencillo" a los delincuentes explotar vulnerabilidades detectadas y hechas públicas y que no han sido actualizadas por los usuarios.

b) Respaldo de información. ¿Cuándo fue la última vez que realizaste un respaldo de la información que guardas en tu smartphone, computadora o tablet?

Desde hace unos años, el ramsomware se ha posicionado como uno de los principales riesgos cibernéticos existentes. El malware es un archivo o un programa que tiene como objetivo dañar el sistema informático; los ejemplos incluyen gusanos informáticos, virus, caballos de Troya y *spyware*. El *ransomware* también es un ejemplo de *malware* en el que el atacante bloquea los archivos del sistema informático de la víctima y exige un pago para desbloquear el dispositivo o entregar la información.

c) Contraseñas, ¿por qué son importantes? Mantener nuestras contraseñas confidenciales y seguras parece ser un gran reto en este mundo digital. Actualmente estas son tan importantes como la información que se protege. Tal vez esa sea una razón por la cual hemos cedido parte de nosotros, en la búsqueda de mantener la información segura, convirtiendo a los datos biométricos en contraseñas más efectivas, o tal vez así lo percibimos. “Me pueden robar mi combinación 1234567890, pero no mi cara o voz o huella”.

La contraseña, por sí misma, resulta ser un factor de autenticación. En el mundo digital, este procedimiento constituye una acción mediante la cual demostramos a un sistema o persona que somos quienes realmente decimos ser, para ello se puede emplear un documento, rasgo biológico, entre otras. Las contraseñas se consideran datos personales, ya que están asociadas a la persona y permiten identificarla.

Si empleamos una contraseña única para todos los sitios, y esta llega a estar expuesta, el impacto en nuestra información será muy grande. En una vida que se desarrolla a través de apps y diversos servicios digitales, esto podría parecer imposible, pero existen administradores de claves que pueden ayudarnos en esta tarea.

Actualmente, y para facilitarnos la tarea de no recordar tantas contraseñas, los navegadores de Internet cuentan con mecanismos que te permiten almacenarlas. Antes de utilizarlos, considera los riesgos involucrados al adoptar estas funcionalidades: ¿vas a albergar tus contraseñas en dispositivos que otras personas utilizan? ¿Vas a guardar todas tus contraseñas en un mismo lugar?

Si bien las contraseñas resultan ser las formas más comunes de autenticación en línea y se emplean diariamente por millones de personas en el mundo digital, la autenticación multifactor permite elevar nuestro nivel ciberseguridad.

Una autenticación “básica” funciona cuando ingresamos nuestro usuario y clave al solicitar el acceso en una página web.

Otros factores que podemos emplear de forma única o conjunta son:

- Qué sabemos: contraseñas
- Qué tenemos: una llave móvil que pueda estar en un dispositivo diferente o un token
- Qué somos: autenticación biométrica como la voz o reconocimiento de huella
- Cómo lo hacemos:

CONTRASEÑAS: SEGURAS Y ROBUSTAS

Emplea **contraseñas únicas:** no usar la misma contraseña o contraseñas muy similares (no las recicles o varies por un carácter).

Cambiarlas con cada estación del año, al inicio de cada cuatrimestre o por lo menos cada tres meses.

Crea contraseñas complejas, largas, únicas, aleatorias y difíciles de predecir e incluir una combinación de por lo menos 12 letras mayúsculas y minúsculas, números y símbolos.

Activa la **verificación en dos pasos** (autentificación de dos factores).

Utiliza las preguntas de seguridad de forma inteligente.

¡No compartas tus contraseñas! Si por una excepción lo debes hacer, hazlo a través de una conexión segura.

No guardes las contraseñas en la configuración del navegador (especialmente si NO es tu equipo personal o lo compartes), ni en la nube.

Imagen 5: Contraseñas: seguras y robustas

La conjugación de estos factores nos ayuda a elevar el nivel de seguridad de nuestra información.

Aun así, debemos estar conscientes de que nuestras contraseñas pueden ser vulneradas, por lo que resulta importante tener un plan de respuesta.

d) ***Phishing.*** El email es la forma en que nos hemos comunicado y trabajado desde hace décadas, por ello es el vector más utilizado para varios ataques, como es el caso del *phishing*. Muchas hemos escuchado del *phishing*, no es un nuevo modo de ciberataque, sin embargo, sigue estando vigente y es empleado diariamente. ¿Por qué es tan exitoso? En junio de 2021 se reportaron 222,127[49] ataques de este tipo.

El *phishing* es una técnica consistente en el envío de correos electrónicos maliciosos que pretenden ser de fuentes confiables (sitios o personas). Ocurre cuando un atacante intenta obtener de manera fraudulenta información confidencial de un usuario haciéndose pasar por una entidad confiable. Sus objetivos se pueden enmarcar de la siguiente manera:

Existe una técnica más personalizada: spear *phishing*, la cual se centra en una persona específica. A través de este método, los delincuentes personalizan emails o mensajes de

49 IBM Security, *X-Force Threat Intelligence Index 2022,* IBM, p. 20, disponible en: https://www.ibm.com/downloads/cas/ADLMYLAZ

phishing y/o se hacen pasar por contactos cercanos, reclutadores, etc. Por ejemplo: un delincuente que suplanta la información de un banco y pide a la persona usuaria información clave para "desbloquear su cuenta". Para este tipo de ataque se requiere recabar información previa de la víctima.

Me llegó un mensaje de alguien que manifiesta tener control sobre mi dispositivo y haber obtenido fotografías mías o mi *pack*. Antes de dar clic, recordemos:

- ¿El correo está redactado con errores ortográficos?
- Revisar el origen del correo, es decir, la dirección de dónde este proviene.
- No descargar ningún archivo adjunto, si se trata de alguien conocido podemos preguntarle si realizó el envío.
- No responder el mensaje y eliminarlo.

e) Ingeniería social. Básicamente se fundamenta en el engaño y la manipulación. La ingeniería social es una amenaza que se centra en la interacción humana, en la que un ingeniero social manipula a la víctima para que proporcione información confidencial. Algunos de estos ataques son:

- **Pretexting:** A través de un pretexto o historia cautivadora, los delincuentes atraen la atención de la persona y la involucran para que haga alguna acción (tal como donar a una campaña falsa) o brindar información personal sensible. Un ejemplo son los correos electrónicos en donde se promete dinero de una supuesta herencia buscando obtener detalles de una cuenta bancaria.
- **Spam de contactos:** Esta forma de ataque consiste en el envío masivo de correos electrónicos a una lista de contactos desde una cuenta que ha sido comprometida. Estos emails salen de un buzón de correo conocido para no levantar sospechas, pero el contenido le aparecerá a las personas destinatarias con links acortados y/o asuntos informales como "Mira esto". Si la persona hace clic, se instalará un software malicioso que continuará con esa cadena de spam y puede acarrear consecuencias negativas para sus datos personales.

Tanto la ingeniería *social/phishing,* al igual que la desinformación, apuntan directamente a engañar a los usuarios. En estos tipos de ataques, se aprovechan de las vulnerabilidades inherentes a la naturaleza humana, que históricamente han sido el blanco de los atacantes. La investigación ha revelado que un pensamiento intuitivo y una predisposición a compartir información personal están estrechamente relacionados con un mayor riesgo de caer en el *phishing*. Este hallazgo guarda similitud con la conclusión de Pennycook y sus colegas, quienes descubrieron que la desinformación se nutre de la tendencia de las víctimas a caer en la trampa de la pereza cognitiva. Aunque los ataques de ingeniería social y *phishing* generalmente persiguen ganancias económicas, la desinformación suele tener como motivación principal el fomento del radicalismo, la interferencia en procesos electorales o la guerra cibernética.

Las distintas motivaciones detrás de estos ataques conllevan a objetivos diferentes: en tanto que la ingeniería social y el *phishing* buscan obtener información confidencial y generar

ingresos mediante el ataque, la desinformación se emplea con el propósito de moldear la percepción pública. Los métodos utilizados para llevar a cabo la ingeniería social suelen involucrar comunicaciones a través de correo electrónico o mensajes telefónicos, mientras que en el caso de la desinformación, los vectores de ataque pueden variar y abarcar diversos enfoques, como anuncios, búsquedas en la web y redes sociales.

Para contrarrestar adecuadamente la desinformación, debemos tratarla como un problema de ciberseguridad.

En el año 2021, la Organización de Estados Americanos (OEA) presentó el "Kit básico de medidas de seguridad digital para la nueva normalidad"[50], en donde realiza las siguientes sugerencias:

- Concientización en primera línea de defensa y darse cuenta de que se es un blanco.
- Ejercicio personal de análisis de riesgo: ¿qué estoy haciendo para protegerme de los posibles ataques?
- Precaución, mantenerse vigilante y tener mayor atención al interactuar en el mundo digital.
- Los ciberataques exitosos frecuentemente dependen de errores humanos, no bajemos la guardia ante los riesgos cibernéticos.
- Estar atentas e informadas a través de fuentes certeras y fidedignas, sitios oficiales o verificados de información, sobre todo, cuando es relativa a nuestra salud.
- Conversar con la familia, incluir a nuestro entorno familiar para fomentar la corresponsabilidad digital.

Tomando en cuenta lo antes mencionado:

a) Utilizar contraseñas seguras como primera línea de protección:

- Optar por contraseñas únicas, largas, aleatorias y difíciles de predecir, que no contengan información personal.
- Asegurarse de que tenga al menos 12 letras, incluyendo mayúsculas y minúsculas, números y caracteres especiales.
- Emplear contraseñas diferentes para cada cuenta y dispositivo, y cambiarlas frecuentemente.
- Utilizar administradores de contraseñas en línea, los cuales pueden generar contraseñas aleatorias y seguras.
- En la medida de lo posible, recurrir a preguntas de seguridad sin proporcionar información personal.
- Reforzar la seguridad mediante la activación de la verificación en dos pasos, disponible en servicios como el correo electrónico y las redes sociales.

b) Navegación segura:

- Conectarse únicamente a redes wifi privadas y confiables.
- En las redes de casa es importante que el router wifi cuente con una clave robusta y difícil de adivinar. Además de realizar un monitoreo regular de los equipos conectados a la red.
- Verificar siempre que la dirección web en la cual se está navegando posea certificados seguros.

50 Organización de Estados Americanos (OEA) (2021). *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, pp. 25-26, disponible en: https://www.oas.org/es/sms/cicte/docs/Ciberseguridad-de-las-mujeres-durante-COVID-19.pdf

EMPODERARNOS EN EL ESPACIO DIGITAL

El ejercicio de nuestros derechos humanos y la forma en que la ciberseguridad se vuelve un habilitador para este debe ser una preocupación. A menudo, la inseguridad en línea es una razón fundamental por la cual las personas, en particular las mujeres, limitamos el uso de Internet o evitamos participar en el mundo en línea. Por lo tanto, es fundamental desarrollar medidas para prevenir y protegernos contra la violencia de género en línea. Esto debe ir acompañado de una adecuada educación digital y una gestión de riesgos en línea específica para las mujeres. Estas medidas preventivas son esenciales para defendernos de las amenazas y peligros que se encuentran en el entorno en línea.

La tecnología está incrustada en las relaciones sociales, es una relación co-construida. Por lo que no debería sorprendernos que la tecnología, la vigilancia y el procesamiento de datos reproduzcan, afiancen y profundicen diversas formas de discriminación, marginación y violencia ya presentes en nuestra sociedad.

Las tecnologías digitales pueden tanto proteger como socavar los derechos y la igualdad de género. La corresponsabilidad *multistakeholder* tiene un gran impacto, en si la tecnología beneficia o perjudica a las niñas y mujeres.

Los ataques pueden variar en intensidad y naturaleza, y continuarán haciéndolo mientras no tengamos políticas públicas y se emplee un enfoque multistakeholder no solo para combatir la violencia digital de género, sino la que diariamente ocurre en medios físicos. La responsabilidad no recae únicamente en las plataformas, la comunidad en línea o las autoridades. Como usuarias, podemos abordar la prevención de la violencia digital en línea y las conductas asociadas desde diversos enfoques, como mejorar nuestra ciberseguridad, conocer, identificar los espacios digitales más "riesgosos" y desarrollar nuestra ciber resiliencia, entre otros.

Para prevenir y combatir estos actos, es fundamental llevar a cabo una gestión de riesgos en nuestro entorno personal en línea. La ciberseguridad personal a menudo es un tema de debate lleno de consejos contradictorios y malentendidos, debido a la relativa novedad de la ciberseguridad en comparación con nuestra experiencia evolutiva en seguridad física.[51]

Actualmente es difícil separar el mundo físico del digital, ya que lo que sucede en uno afecta al otro y viceversa. Como usuarias de múltiples tecnologías y plataformas, nos preocupamos por la transparencia en el tratamiento de nuestra información (uso, compartición, almacenamiento, borrado), no obstante, aún no somos conscientes de la ingente cantidad de datos que se recolectan de nosotros a cada segundo.

El *phishing*, la ingeniería social, los ataques a aplicaciones web, la denegación de servicio (DoS), el *malware* y el *ransomware* han sido cada vez más frecuentes en los últimos años. Además, los abusadores utilizan tácticas creativas, como lenguaje codificado, memes visuales y textuales iterativos basados en el contexto y otras tácticas para evitar la detección, lo que agrava el problema y dificulta la respuesta.

La desinformación en línea es un problema de derechos humanos que afecta los derechos de las niñas en su participación, educación y libertad de expresión. La confianza en las fuentes de información, ya sean gubernamentales, académicas, periodísticas o comunitarias, se ve socavada a medida que luchan por discernir la verdad de la ficción. Todos debemos ser conscientes de esto para comprender los efectos específicos de la información errónea y la desinformación en línea en las niñas y mujeres jóvenes para que podamos diseñar soluciones que satisfagan sus necesidades.[52]

A medida que avanzamos hacia un mundo cada vez más digitalizado y la idea del metaverso, debemos reconocer que gran parte de nuestras vidas se desarrollará en mundos virtuales. Esto nos convierte en actores clave en esta nueva economía digital.

51 Schneier, Bruce (2018). *Click here to kill everybody. Security and Survival in a Hyper-Connected World*, New York: Norton & Company.
52 Plan International, *The State of the World's girls 2021. How misinformation and disinformation online affect the lives, learning and leadership of girls and young women*, 2021, disponible en: https://plan-international.org/uploads/2022/02/sotwgr2021-commsreport-en.pdf

Es una desafortunada realidad que los ciberataques y violencia digital contra las mujeres a menudo no se toman en serio. Esto debe cambiar, ya que la violencia digital debe abordarse como lo que es: un ataque que causa daños a sus víctimas y a la sociedad en general, o de lo contrario, los derechos de las mujeres estarán amenazados.

Si no abordamos, prevenimos y sancionamos la violencia contra niñas, adolescentes y mujeres, tanto en el mundo en línea como en el mundo real, no podremos resolver la violencia en general. Debemos afrontar este tipo de ataques empleando los marcos nacionales e internacionales de los derechos humanos existentes, esto nos permitirá trabajar para lograr un ciberespacio abierto, seguro, gratuito y resiliente como el que queremos.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Primera edición digital, noviembre 2023
Hecho en México / *Made in Mexico*