INTER MUN 2024

ONU MUJERES

ANTECEDENTES

“DESARROLLO DE UN MARCO NORMATIVO INTERNACIONAL PARA GARANTIZAR LA SEGURIDAD CIBERNÉTICA DE LA MUJER”

TABLA DE CONTENIDOS

BIENVENIDA

Estimados Delegados y Delegadas,

Sean ustedes bienvenidos al comité de ONU Mujeres del Modelo de las Naciones Unidas del Sistema de Colegios Jesuitas 2024 (INTERMUN) presentado por el Instituto Cultural Tampico.

Este comité ha sido creado con el propósito de acrecentar su competencia de debate, argumentación y resolución de conflictos desde un punto de vista objetivo y diplomático, siempre buscando el empoderamiento femenino y la lucha contra los esquemas sociopolíticos que con gran esmero agrava la sociedad en la que vivimos y lamina la vida y oportunidades de miles de millones de mujeres.

La mesa directiva de este comité siempre se encontrará a su entera disposición, con la satisfacción y dicha de tener la oportunidad de trabajar con delegados tan capaces, con un entusiasmo sin igual y una imaginación sin límites para hacer de este planeta un mundo más igualitario y justo.

El tema con el que tenemos la dicha de desenvolvernos en esta edición de InterMUN es el del Desarrollo de Un Marco Normativo Internacional Para Garantizar la Seguridad Cibernética en el Mundo.

El tema de la seguridad cibernética es una problemática seria, así se ha vuelto con el desarrollo tecnológico que hemos presenciado los últimos años. Este desarrollo ha formado una nueva aldea global, en la que nos desenvolvemos diariamente sin que sea nuevo ya. Estos cambios constantes presentan una problemática persistente para asegurar la paz.

Gracias por seleccionar el comité de ONU Mujeres, esperamos que disfruten esta experiencia y se convierta en un gran recuerdo para ustedes. Les deseamos mucho éxito a todos.

Atentamente,

- Mesa del Comité de la Organización de las Naciones Unidas Mujeres.

Presidente: Ricardo Javier Hernández Ortiz
Secretaria: Graciela Emilia Acuña Oviedo
Moderador: Ángel Santiago Treviño Hernández

HISTORIA DEL COMITÉ

ONU Mujeres es la organización de las Naciones Unidas dedicada a promover la igualdad de género y el empoderamiento de las mujeres. Como defensora mundial de mujeres y niñas, ONU Mujeres fue establecida para acelerar el progreso que conlleva a mejorar las condiciones de vida de las mujeres y para responder a las necesidades que enfrentan en el mundo.

ONU Mujeres apoya a los Estados Miembros de las Naciones Unidas en el establecimiento de normas internacionales para lograr la igualdad de género y trabaja con los gobiernos y la sociedad civil en la creación de leyes, políticas, programas y servicios necesarios para garantizar que se implementen los estándares con eficacia y que redunden en verdadero beneficio de las mujeres y las niñas en todo el mundo. Trabaja mundialmente para que los Objetivos de Desarrollo Sostenible sean una realidad para las mujeres y las niñas, y promueve la participación de las mujeres en igualdad de condiciones en todos los ámbitos de la vida.

La igualdad de género no es solamente un derecho humano básico, sino que su logro tiene muchísimas consecuencias socioeconómicas. El empoderamiento de las mujeres impulsa economías prósperas y estimula la productividad y el crecimiento. Aun así, las desigualdades de género siguen estando fuertemente arraigadas en la sociedad. Las mujeres encuentran obstáculos para conseguir trabajos dignos y enfrentan discriminación laboral y brechas salariales de género. A menudo, no pueden acceder a la educación básica y a la atención médica. Las mujeres sufren violencia y discriminación en todas partes del mundo. Están subrepresentadas en los procesos de toma de decisiones políticas y económicas.

Durante muchas décadas, las Naciones Unidas logró importantes avances a favor de la igualdad de género, entre ellos, acuerdos históricos como la Declaración y la Plataforma de Acción de Beijing, y la Convención sobre la Eliminación de Todas las Formas de Violencia contra la Mujer (CEDAW).

Durante muchos años, las Naciones Unidas enfrentó profundos desafíos en su lucha por la promoción de la igualdad de género en todo el mundo. Entre estos desafíos se incluían un financiamiento inadecuado y la falta de algún factor de impulso reconocido que dirigiera las actividades de las Naciones Unidas en las cuestiones relativas a la igualdad de género. En julio de 2010, la Asamblea General de las Naciones Unidas creó ONU Mujeres, la Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres, para que abordara dichos desafíos. Con este acto, los Estados Miembros de las Naciones Unidas dieron un paso histórico acelerando los objetivos de la Organización relativos a la igualdad de género y el empoderamiento de las mujeres. La creación de ONU Mujeres surgió como parte del programa de reforma de las Naciones Unidas, que reunió recursos y mandatos que generarán un mayor impacto.

INTRODUCCIÓN

La violencia en línea contra las mujeres no es un fenómeno aislado, sino que se localiza en un contexto social más amplio de desigualdad y discriminación de género contra las mujeres y las niñas. Por ello, para entender la violencia digital, es crucial que nos detengamos primero a analizar qué es la violencia de género, puesto que las agresiones y los ataques que viven las mujeres en sus interacciones en línea no son más que una extensión de la violencia que por muchos años las ha afectado en todas las esferas de su vida.

En una época en la que los datos y la información se comercializan como si fueran mercancías, es esencial protegerlos. Una forma de hacerlo es aplicar una gestión de la seguridad de la información basada en la serie de normas de seguridad de la información ISO/IEC 2700 x. Se trata de una familia internacional de normas para la seguridad informática y de la información en organizaciones privadas, públicas o sin ánimo de lucro. Sobre la base de la norma ISO 27001, se puede implantar un sistema de gestión de la seguridad de la información (SGSI) que las organizaciones y las autoridades públicas pueden establecer, aplicar y certificar para su propia protección.

El derecho a la privacidad es fundamental para el goce y el ejercicio de los derechos humanos en línea y fuera de línea. Constituye uno de los pilares de una sociedad democrática y desempeña un papel fundamental en la realización de una amplia gama de derechos humanos, incluso en la esfera digital, que van desde la libertad de expresión, la libertad de asociación y de reunión, hasta el acceso y el disfrute de los derechos económicos y sociales. La injerencia en el derecho a la privacidad también puede tener repercusiones desproporcionadas en determinadas personas o grupos, agravando así la desigualdad y la discriminación.

A medida que el poder de transformación de la computación en la nube entra en el punto de mira, hay una creciente preocupación por el aumento del ciberespacio como campo de batalla para conflictos cibernéticos y un conducto para los ataques lanzados por los gobiernos y sus representantes. Como resultado, existe una creciente urgencia de desarrollar e implementar normas de seguridad cibernética que proporcionan claras expectativas internacionales para la prevención y gestión de conflictos en el ciberespacio.

El establecimiento de normas de seguridad cibernética internacional es un paso esencial en la protección de la seguridad internacional y nacional, el mantenimiento de la confianza en la tecnología, y la protección de la estabilidad de la economía global conectada.

Hasta hace poco, la mayoría del trabajo para desarrollar normas de seguridad cibernética se ha centrado en las discusiones conceptuales sobre los derechos y responsabilidades de las naciones. Ahora el movimiento es hacia propuestas más concretas de las normas de seguridad cibernética.

Esto es especialmente evidente a medida que los legisladores, los defensores de los sectores público y privado, el mundo académico y la sociedad civil proponen una amplia gama de ideas más específicas sobre cómo hacer frente a los retos planteados por la explotación de la tecnología para el conflicto.

Muchas de estas propuestas reconocen que las naciones no deben permitir que la actividad cibernética maliciosa se lance desde dentro de sus fronteras, y que la infraestructura crítica no debe ser considerada un objetivo válido en tiempos de paz. Hasta ahora, solo ha habido un progreso limitado. Además, no se ha prestado suficiente atención a la necesidad crítica de que las Normas de seguridad cibernética los sectores público y privado trabajen juntos para proteger los sistemas de tecnología y la infraestructura contra los ataques.

La implementación de medidas eficaces de ciberseguridad no es algo sencillo ya que, debido a la gran cantidad de equipos y tecnologías utilizadas, los ciberdelincuentes siempre encuentran nuevas opciones de llevar a cabo sus ataques. Sin embargo, existe una forma de implementar medidas de protección de datos e información que hace que el procedimiento de implantación de dichas medidas de seguridad informática sea algo más pautado y natural.

Se trata de los estándares y normas ISO relacionadas con la ciberseguridad y seguridad de la información. Las normas ISO son estándares desarrollados y publicados por la Organización Internacional de Normalización (ISO). Tanto ISO como IEC (la Comisión Electrotécnica Internacional) son la referencia especializada para la normalización a nivel mundial. A través de comités técnicos formados por los organismos miembros tanto de ISO como de IEC, se elaboran normas internacionales redactadas con el objetivo de regularizar procesos específicos sobre ámbitos tales como la seguridad de la información.

Estas normas constituyen, hoy en día, un elemento indispensable en el sistema de cumplimiento de las organizaciones, otorgando prestigio y reconocimiento internacional a las mismas. El valor diferencial que aportan las implantaciones de las normas ISO a las organizaciones frente a sus competidores se debe a que dichos estándares certificados son revisados y auditados periódicamente para garantizar su cumplimiento, haciendo que la apreciación por parte de partes interesadas tales como clientes o accionistas mejore considerablemente.

Las normas ISO se numeran de forma incremental en función de su propósito y se dividen en familias para agrupar aquellas que traten aspectos de la misma índole. El objetivo de estos estándares y normas es identificar técnicas, políticas, guías, capacitación, etc. en referencia a su propósito (seguridad, continuidad, calidad, entre otros).

IMPACTO

La violencia de género facilitada por las nuevas tecnologías es un fenómeno que de forma creciente afecta la privacidad y seguridad de las mujeres dentro y fuera del ciberespacio. Investigaciones sobre el tema indican que las mujeres son víctimas de ciertos tipos de ciberviolencia de manera desproporcionada en comparación con los hombres (REVM-ONU, 2018; EIGE, 2017). De acuerdo con un estudio publicado en 2015 por la Comisión de la Banda Ancha para el Desarrollo Sostenible, de las Naciones Unidas, 73% de las mujeres habían vivido alguna forma de violencia de género en línea, mientras que 61% de los atacantes eran hombres (UNBC, 2015). Otras fuentes señalan que 23% de las mujeres han experimentado acoso en línea al menos una vez en su vida, y se estima que una de cada diez mujeres ya había sufrido alguna forma de ciberviolencia desde los 15 años de edad (REVM-ONU, 2018, párr. 16; EIGE, 2017: 3; AI, 2017).

Este fenómeno se observa en un escenario con múltiples retos. La información sobre la ciber violencia contra las mujeres es aún escasa. Es muy poco lo que se sabe sobre el porcentaje real de víctimas y la prevalencia de los daños que provoca (EIGE, 2017). Además, hasta la fecha no hay una definición acordada a escala regional o internacional de la violencia de género en línea ni una terminología precisa. Hay una gran disparidad entre las respuestas de los Estados y los organismos internacionales y, en general, una falta de marcos jurídicos adecuados para proteger a las víctimas.

Tomando en consideración este contexto, el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE), en alianza con la Comisión Interamericana de Mujeres (CIM), ha elaborado esta guía de conceptos básicos dirigida a instituciones públicas, profesionales y partes interesadas en el sector de la ciberseguridad. En ella se abordan las características y el impacto de la violencia de género en línea (primera parte), los tipos de ataques que pueden ser considerados como manifestaciones de violencia de género digital (segunda parte), y se presenta una breve reseña de los últimos desarrollos en la materia en la región latinoamericana y de las medidas que pueden adoptar las autoridades para prevenir y combatir esta forma de violencia de género (tercera parte).

La violencia de género contra las mujeres tiene su origen en estereotipos y prejuicios acerca de los atributos y las características que poseen hombres y mujeres y en expectativas de las funciones sociales que ambos supuestamente deben desempeñar (por ejemplo, que las mujeres son las únicas encargadas de las labores domésticas, que no tienen suficiente autoridad para ocupar cargos directivos o que son débiles por naturaleza). Estos patrones socioculturales colocan a las mujeres en una posición inferior o subordinada respecto de los hombres y propician su discriminación, elementos que son los principales impulsores de la violencia dirigida hacia ellas (MESECVI, 2017, párr. 37).

Es importante subrayar que la violencia opera en sinergia con la desigualdad de género y no solo como una consecuencia de ésta última, sino como mecanismo social que busca mantener a las mujeres en una situación de desventaja.

Esto significa que la violencia se usa en muchos casos para “castigar” o “corregir” a mujeres cuyas actitudes o actividades supuestamente van en contra de lo que la sociedad espera de ellas (MESECVI, 2017, párr. 36).

Las Naciones Unidas han señalado que la violencia contra las mujeres es un problema omnipresente en todos los países del mundo y una violación sistemática y generalizada de los derechos humanos, con alto grado de impunidad.

Las mujeres y las niñas experimentan violencia de género a lo largo de los años en todos los espacios offline y online donde concurren y participan, ya sea en el hogar, la escuela, el trabajo, la vía pública, la política, los medios de comunicación, el deporte, las instituciones públicas o al navegar en redes sociales (Comité CEDAW, Recomendación General 35).

Esta violencia no tiene fronteras, está dirigida contra todas las mujeres por el simple hecho de que son mujeres e incide más en ciertos grupos de mujeres debido a que sufren formas de discriminación interseccional, como es el caso de las mujeres indígenas, migrantes, con discapacidad, lesbianas, bisexuales y transgénero, entre otras (MESECVI, 2017).

Uno de los logros más importantes para las mujeres ha sido el reconocimiento de que la violencia cometida en su contra no es un problema privado, sino que constituye un asunto de interés público y una violación de los derechos humanos reconocida en instrumentos internacionales y legislaciones nacionales que prescriben la obligación de los Estados de prevenirla, atenderla, investigarla, repararla y sancionarla (Edwards, 2010).

En el caso del sistema interamericano, el derecho de las mujeres a vivir una vida libre de violencia está reconocido en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belém do Pará), el primer tratado en la materia que elevó el combate de la violencia de género contra las mujeres al rubro de problema de interés regional.

Admonición Política para Alcanzar la Seguridad Cibernética

El proceso de desarrollar e implementar normas internacionales de seguridad cibernética continúa evolucionando a medida que avanza la tecnología, cambian las partes responsables, se exploran las implicaciones de las políticas potenciales y surgen nuevos foros de discusión.

Fundamentalmente, sin embargo, el éxito de las normas de seguridad cibernética vendrá determinado por la forma en que se aplican y cuándo y cómo los infractores deben rendir cuentas.

Esto significa que es fundamental que los gobiernos sean proactivos y colaboradores a la hora de contribuir y evaluar las normas de seguridad cibernética, y determinar cómo hacer que sean efectivas y aplicables.

Los gobiernos pueden conseguir estos objetivos de forma más efectivas si tienen en cuenta las siguientes recomendaciones:

- Aumentar los esfuerzos para conseguir un acuerdo sobre las normas de seguridad cibernética globalmente aceptadas. Si bien hay signos de alineación en torno a un pequeño número de normas de seguridad cibernética, la urgencia de avanzar permanece. Las naciones deben entender los posibles resultados de sus acciones en el ciberespacio y seguir trabajando para acordar las normas para la mejora de las defensas y la limitación de los conflictos y las operaciones ofensivas. Si queremos evitar los efectos potencialmente catastróficos de la guerra cibernética, el compromiso continuo es esencial.
- Proporcionar los medios para la entrada y la participación del sector privado. Las aportaciones de la industria mundial de las TIC es fundamental para garantizar que el lenguaje de las normas de seguridad cibernética refleja con exactitud la realidad de la defensa de los usuarios de la tecnología a escala mundial. Es importante establecer foros apropiados y procesos claros para que el sector privado contribuya. Además, la industria está en la mejor posición para utilizar la información acerca de las tácticas, técnicas, procedimientos e indicadores de consenso para fortalecer las defensas para los usuarios de la tecnología en todo el mundo.
- Explorar las oportunidades y los retos asociados con el uso de un órgano independiente para ayudar con la atribución y verificación. El éxito del desarrollo de las normas de seguridad cibernética requerirá nuevas formas de cooperación y nuevos mecanismos para hacer frente a las alegaciones políticamente sensibles tales como la atribución. Los gobiernos y el sector privado necesitan un foro en el que puedan proporcionar evidencia para apoyar la atribución técnica y obtener la validación a través de una rigurosa revisión por pares. Un modelo que ha funcionado es la competencia en los conflictos nucleares y de guerra química. Esto proporciona un modelo para la verificación de las normas cibernéticas futuras.

Normas Para la Seguridad de la Información: La Familia de Normas ISO 2700X

Las normas individuales para la seguridad de la información de la serie ISO 2700x tratan diversos temas en el ámbito de la seguridad de la información. Por ejemplo, la norma internacional especifica ISO 27001 Un sistema de gestión de la seguridad de la información (SGSI), ISO 27701 un sistema de gestión de la protección de datos, la norma ISO 27017 ofrece orientación sobre las medidas de seguridad de la información para la computación en la nube, y la norma ISO 27005 proporciona directrices para la gestión de los riesgos de seguridad de la información.

Las empresas de todos los sectores pueden beneficiarse del enfoque sistemáticamente estructurado de estas normas para la seguridad de la información. Permite proteger los datos confidenciales contra la pérdida y el uso indebido, y ayuda a identificar y reducir de forma fiable las amenazas (potenciales). El enfoque ayuda a garantizar la disponibilidad de los sistemas informáticos de la empresa, contribuyendo así a la optimización de los procesos empresariales, los costes de las TI y los procesos, y la minimización de los riesgos empresariales y de responsabilidad.

Familia ISO 27000

Entre las ya mencionadas normas ISO, destaca la familia ISO 27000. Ésta es una serie compuesta por varias normas de seguridad de la información que detallan las pautas y requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de gestionar la seguridad de la información de las organizaciones.

Dentro de este conjunto de normas, la principal es la ISO 27001, la referencia certificable de toda la serie. Esta norma proporciona requisitos para el establecimiento, implantación, mantenimiento y mejora continua de un SGSI. El proceso de mejora continua se basa en el conocido Ciclo Deming o PDCA (de las siglas de las palabras en inglés Plan-Do-Check-Act) que consta de las 4 fases de Planificar, Hacer, Verificar y Actuar.

Las demás normas de la familia sirven de guía y ayuda para la implantación del SGSI. Otra norma bastante reseñable es, por ejemplo, la ISO 27002. Se trata de una guía de buenas prácticas que describe los objetivos de control y controles exigibles en lo referente a la seguridad de la información.

De la misma familia y con un propósito más específico es la ISO 27031. Este es un estándar no certificable que sirve de guía y proporciona un conjunto de métodos y procedimientos para establecer aspectos que conlleven una mejora en la preparación de las TIC de una organización para garantizar y consolidar la continuidad de negocio. Es decir, el objetivo principal de este estándar es proporcionar la continuidad de los servicios y asegurar que la organización podrá recuperarse ante una situación de desastre restableciendo un estado de funcionamiento acordado anteriormente.

Similar al caso anterior, podemos hablar de la norma ISO 27701, también de la familia ISO 27000. En ella se establecen requisitos para administrar, gestionar y proteger la privacidad de los datos personales de la compañía en función de reglamentos y leyes tales como el RGPD (Reglamento General de Protección de Datos). Basada en los requisitos, controles y objetivos de la norma ISO 27001 de seguridad, incluye indicaciones para proteger la privacidad y confidencialidad de los datos de carácter personal tratados en una compañía. Cabe destacar que la certificación de esta nueva norma es alcanzable solamente de forma conjunta a la certificación de la ISO 27001.

Marco Jurídico Internacional

El artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos establecen que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

Asimismo, establecen que “toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. Si bien el derecho a la privacidad en las normas internacionales de derechos humanos no es absoluto, cada caso de injerencia debe

estar previsto por la ley y su necesidad y proporcionalidad deben ser objeto de un examen minucioso y crítico.

Elementos Básicos de la Violencia En Línea en Contra de las Mujeres

- No es algo nuevo. Forma parte de un contexto de discriminación de género y violencia sistémica contra las mujeres que se da en todos los ámbitos de su vida.
- No está desconectada de la violencia “fuera de internet”: es parte de la serie de formas múltiples, interrelacionadas y recurrentes de violencia contra las mujeres y las niñas que ahora fluye por el mundo online-offline y lo atraviesa.
- Conlleva diversas violaciones de los derechos humanos de las mujeres y las niñas.
- Es una expresión dinámica que abarca prácticas muy diversas de violencia facilitadas o reconfiguradas por las tecnologías de la información y las comunicaciones (TIC).
- Causa en las víctimas daños y sufrimientos psicológicos, físicos, sexuales y/o económicos, y tiene efectos familiares, sociales y colectivos.

¿Qué es la Violencia de Género En Línea Contra las Mujeres?

Si bien varias organizaciones de la sociedad civil, el sector académico y organismos internacionales han realizado esfuerzos importantes para precisar qué es la violencia de género en línea en contra de las mujeres, como se señaló al inicio, hasta la fecha no se ha alcanzado un consenso en torno a su definición ni existe una terminología consolidada (Van Der Wilk, 2018).

En 2015, la Asociación para el Progreso de las Comunicaciones (APC), que ha trabajado en este asunto por más de diez años, definió la violencia en línea contra las mujeres como los actos de violencia por razones de género que son cometidos, instigados o agravados, en parte o en su totalidad, por el uso de tecnologías de la información y las comunicaciones (TIC), como teléfonos móviles, internet, plataformas de redes sociales y correo electrónico (APC, 2017: 3).

Además, el Proyecto de Debida Diligencia (Due Diligence Project) destacó que estos actos tienen o pueden tener como resultado un daño o sufrimiento físico, sexual, psicológico o económico (Abdul, 2017).

El Centro Internacional de Investigaciones sobre la Mujer, por su parte, define la violencia de género facilitada por las tecnologías como actos de una o más personas que dañan a otras por razón de su identidad sexual o de género o al imponer normas dañinas de género.

Estos actos, para los cuales se usan la internet o la tecnología móvil, consisten en hostigamiento, intimidación, acoso sexual, difamación, discurso de odio y explotación (Hinson et al., 2018: 1).

Finalmente, en el ámbito de la Organización de las Naciones Unidas (ONU), la Relatora Especial sobre la Violencia contra las Mujeres definió en 2018 la violencia en línea contra las mujeres como “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 o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada" (REVM-ONU, 2018, párr. 23).

La ciberviolencia de género es un concepto en constante cambio. Como lo reconoció la Relatora Especial sobre Violencia contra las Mujeres de las Naciones Unidas, las rápidas transformaciones tecnológicas influyen en la violencia en línea, y surgen nuevas y diferentes manifestaciones de violencia a medida que los espacios digitales se transforman y trastocan la vida fuera de internet (REVM-ONU, 2018, párr. 24).

La Estrecha Relación Entre la Violencia de Pareja y las Nuevas Tecnologías

Desde hace varios años, las TIC están desempeñando un papel muy importante en el surgimiento de nuevas estrategias de abuso y control por los perpetradores de actos de violencia doméstica y de pareja (Dragiewicz, 2019). Varios estudios han revelado que 77% de las víctimas de ciberacoso han sufrido también alguna forma de violencia física o sexual a manos de una pareja íntima (FRA, 2014) y que conocían por lo menos a la mitad de los agresores en línea (APC, 2015).

A medida que las nuevas tecnologías se han ido incorporando en prácticamente todas las actividades diarias de las personas, los agresores se han aprovechado, extendiendo e intensificando comportamientos abusivos, posesivos y controladores que antes no eran posibles (Woodlock, 2017). En consecuencia, las mujeres ahora experimentan esta violencia sin límites de espacio y tiempo y con la sensación de que el agresor es omnipresente (Harris, 2018), lo cual tiene efectos graves en su salud mental.

Aunque la investigación en la materia es aún incipiente, varios estudios iniciales indican que algunas tecnologías se usan más que otras para cometer abusos y ejercer cibercontrol en contextos de violencia doméstica o de pareja. Ese es el caso de los mensajes de texto, redes sociales o software para monitorear la ubicación de las víctimas por medio de sus celulares (Dragiewicz, 2019).

Se ha observado también en parejas jóvenes nuevos comportamientos que se han normalizado en el actual contexto online-offline, disfrazados con ideas y mitos del amor romántico, pero que en el fondo buscan el cibercontrol y la limitación de la vida digital de las mujeres

La Violencia En Línea Contra las Mujeres Produce Daños Reales

Como consecuencia de la violencia en línea, las mujeres y las niñas sufren graves daños psicológicos, físicos, sexuales, emocionales, económicos, laborales, familiares y sociales (REVM-ONU, 2018).

Las manifestaciones y las repercusiones de esta violencia pueden ser muy variadas dependiendo de la forma que tome; por ejemplo, sentimientos de depresión, ansiedad, estrés, miedo o ataques de pánico en casos de ciberhostigamiento, intentos de suicidio por parte de mujeres afectadas por la distribución no consensuada de imágenes sexuales, daños físicos contra las víctimas de doxxing5 o perjuicios económicos ante la pérdida del empleo como consecuencia de actos en línea que desprestigian (Pew Research Center, 2017; Kwon et al., 2019; AI, 2017).

Se ha observado además que las características de ciertas tecnologías hacen que la magnitud del daño de algunos actos de violencia se incremente exponencialmente y se extienda más allá del acto original (como su rápida propagación, alcance, anonimidad y permanencia) (APC, 2017), dado que las mujeres son juzgadas con mayor severidad que los hombres por sus actitudes en línea. Tal es el caso de incidentes de distribución no consentida de imágenes sexuales, en los que se ha visto que mujeres y niñas son estigmatizadas por el ejercicio de su sexualidad y, después de ver sus imágenes distribuidas, tienen que vivir en un contexto de humillación y vergüenza permanente en su entorno social, lo cual en muchos casos las ha empujado al suicidio.

Las mujeres afectadas a menudo se responsabilizan a sí mismas por acciones que pudieran haber causado la violencia y se retiran de los espacios digitales, se autocensuran o se aíslan socialmente (Citron, 2014). Además, es muy común que sean revictimizadas por familiares, autoridades y medios de comunicación, que con frecuencia les atribuyen la responsabilidad de protegerse, en vez de recalcar la conducta ilícita de los agresores, y de esta forma normalizan y minimizan esta violencia (REVM-ONU, 2018, párr. 25).

Aunado a los efectos individuales, la violencia en línea conlleva daños colectivos e intergeneracionales y tiene costos directos e indirectos para las sociedades y las economías, dado que las víctimas y sobrevivientes no solo requieren atención médica y servicios judiciales y sociales, sino que también pueden ver disminuida su productividad y sus interacciones en la comunidad (UNBC, 2015). Asimismo, esta violencia tiene un efecto silenciador, puesto que es una amenaza directa a la libertad de expresión de las mujeres (AI, 2017) y afecta su acceso y participación en línea como ciudadanas digitales activas, lo cual crea un déficit democrático al impedir que las voces de las mujeres se escuchen libremente en los debates digitales (REVM-ONU, 2018, párr. 29).

Los Agresores

Se ha observado que los agresores y los responsables de la violencia de género en línea contra las mujeres tienen por lo general una identidad masculina (Van Der Wilk, 2018, 34-37). Estos agresores pueden ser una persona que la víctima no conoce (como un acosador sexual en línea que dirige sus ataques sistemáticamente hacia diversas mujeres o sujetos que practican el grooming o ciber engaño pederasta) o un integrante del círculo familiar, profesional o una amistad. Algunos estudios indican, por ejemplo, que entre 40% y 50% de las víctimas conocían a sus agresores en línea (una ex pareja sentimental, un miembro de la familia, un amigo o un colega) y que, en un tercio de los casos, los agresores tenían o habían tenido

una relación íntima con la persona atacada (Pew Research Center, 2017; APC, 2015).

Pueden identificarse dos tipos de responsables de la violencia en línea contra las mujeres (Abdul, 2017):

- El perpetrador original: La persona que comete el acto inicial de violencia o abuso digital o que crea, manipula o publica por primera vez información dañina, datos personales o imágenes íntimas sin el consentimiento de la víctima.
- El perpetrador o los perpetradores secundarios: Persona o grupo de personas que participan en la continuación y propagación de un acto de violencia en línea al reenviar, descargar, volver a publicar o compartir información dañina, datos personales o imágenes íntimas obtenidas sin el consentimiento de la víctima.

Distintas Iniciativas Nacionales para la Ciberseguridad

El Plan es una de las estrategias más importantes de Paraguay para afrontar riesgos y desafíos que conllevan el uso de nuevas tecnologías. El documento, aprobado a través del Decreto 7052/2017, contiene dos partes que son relevantes para este análisis: el diagnóstico de la situación del país y los objetivos del plan. Todo el documento del plan plasma una visión clásica de la seguridad, donde el Estado es el único proveedor de seguridad y el objeto que necesita ser asegurado (Campbell, 1998).

Aunque se hacen reiteradas menciones a la necesidad de cuidar a las personas en el entorno digital, en particular niños, niñas y adolescentes, y también se reconoce que las ISPs pueden promover la seguridad de los usuarios, predomina una visión estatal de lo que constituyen peligros y por tanto, lo que se entiende por seguridad. Esta visión se concentra en delitos informáticos como un ejemplo de los peligros que acarrean las TICs, como la clonación de tarjetas de crédito o alteración de datos en sistemas informáticos. También se desconoce la diversidad de experiencias de las personas y que los peligros que ellas sufren son particulares.

La violencia que viven las mujeres en Internet es marcadamente distinta a la que sufren los hombres. El cyber-acoso, el doxing y la sextorsión son algunos ejemplos. Distinta también es la violencia y la discriminación que sufre la comunidad LGBTQ.

La Ley Olimpia es un conjunto de reformas a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal, que buscan reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como ciberviolencia. La “Ley Olimpia” no se refiere a una ley como tal, sino a un conjunto de reformas legislativas encaminadas a reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como ciberviolencia.

OBJETIVO

La Mesa Directiva de ONU Mujeres tiene como objetivo la creación e implementación de una nueva legislación que asegure de manera internacional la seguridad cibernética, haciendo un claro y marcado énfasis en las principales víctimas de este delito; las mujeres. Para llegar a este tratado será primordial la buena comunicación entre los delegados de cada país, así como su entendimiento y empatía por las distintas culturas que conforman esta reunión.

Los delegados de ONU Mujeres deberán comprender cómo la problemática de la ciberseguridad afecta en gran parte a la integridad de la mujer. Estos tendrán que reconocer de dónde proviene este acoso y cuales son los efectos que tienen en las mujeres. La falta de seguridad cibernética ha sido ya regulada de varios modos, sin embargo es complejo frenar debido al constante avance tecnológico en el que vivimos.

Si bien, la vulnerabilidad informática se hace presente en varios ámbitos; como en la falsificación de identidad o el hurto de credenciales bancarias, el enfoque que se busca en este comité es el de su impacto en las mujeres y niñas a través del mundo.

En ONU Mujeres se encuentran a los delegados que buscan transformar a la sociedad. Este comité se caracteriza por su ímpetu por erradicar todos los estereotipos y amenazas a las que se enfrentan las mujeres en un mundo tan globalizado pero tan poco civilizado, como el que habitamos actualmente.

Clarificando el propósito de esta reunión, los invitamos ampliamente a luchar por los ideales que este comité plantea, por las metas que ONU Mujeres busca. Con una apertura cultural para recoger y analizar diferentes ideologías de género derivadas a diferentes culturas que reunimos, para así encontrar la manera de proteger a la mujer informáticamente.

Atentamente,

- La Mesa de la Organización de las Naciones Unidas Mujeres.

PAÍSES INVOLUCRADOS

Estados Unidos Mexicanos

La “Ley Olimpia” es un conjunto de reformas legislativas encaminadas a reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como ciberviolencia. Contempla sanciones de tres a seis años de prisión para quienes realicen estas acciones y multas que van de 500 a 1,000 Unidades de Medida y Actualización (UMA). En 2021 la UMA tendrá un valor de 89.62 pesos diarios, según el Inegi.

En la Ley General de los Derechos de Niñas, Niños y Adolescentes se establece que “Niñas, niños y adolescentes tienen derecho al acceso y uso seguro del Internet como medio efectivo para ejercer los derechos a la información, comunicación, educación, salud, esparcimiento, no discriminación, entre otros. Sin embargo, a lo largo del país, de acuerdo al Módulo sobre Ciberacoso (MOCIBA) 2021 de INEGI, 760 mil personas de entre 12 y 17 años recibieron insinuaciones o propuestas de tipo sexual que le molestaron a través de teléfono celular o internet entre agosto de 2020 y septiembre de 2021 (en adelante, en 2021). Lo anterior correspondía al 5.8% de las personas usuarias en el mismo rango de edad a nivel nacional.

República de Ecuador

El ciberacoso en el Ecuador es un problema social, que junto a la violencia de género se han tomado una posición latente en el país, de este modo, considerando que las tecnologías de Información y comunicación han establecido un nuevo tipo de espacio donde puede converger una delincuencia potencial y una víctima adecuada, las actividades diarias de las personas en el ciberespacio proporcionan oportunidades para ser víctimas de ciberacoso estando más propensas a estas situaciones las mujeres.

Desde enero a diciembre de 2020, según datos de la Fiscalía de Ecuador, se presentaron 230 casos de ciberacoso sexual contra niñas, niños y adolescentes. Las denuncias presentadas no representan la totalidad de los casos; sin embargo, pone en alerta a las madres, padres y cuidadores que deben velar por el buen uso de los dispositivos a los que se exponen los menores de edad y brindarles la confianza y herramientas adecuadas para saber actuar en caso de ser víctimas de acoso cibernético.

Japón

Según la enmienda al código penal del país, que entró en vigencia a fines de verano del 2022, los delincuentes condenados por insultos en línea pueden ser encarcelados por hasta un año o multados con 300.000 yenes (alrededor de US $2.200).

Es un aumento significativo de los castigos existentes de detención por menos de 30 días y una multa de hasta 10.000 yenes (US $75).

En Japón hay unas 38.000 páginas de colegios e institutos que no están supervisadas por los centros educativos, y los insultos, el contenido sexual y las expresiones violentas predominan entre ellas, según una encuesta del Ministerio de Educación.

Legisladores japoneses permanecen de pie al aprobar una ley penal enmendada en la cámara alta el viernes 16 de junio de 2023, en Tokio. El Parlamento elevó la edad de consentimiento sexual a 16 años, de los 13 en la que estaba.

República de Honduras

El 77 % de las mujeres de Honduras ha sido víctima de la ciberviolencia de género, una realidad que se canaliza principalmente por las redes sociales y se denuncia poco porque ellas consideran que no sirve de nada.

Las diversas formas de la violencia digital contra las mujeres se canalizan principalmente por las diferentes redes sociales, como WhatsApp, Instagram y Facebook, llamadas telefónicas y SMS, añade la ONG; El acoso, la extorsión y la suplantación de identidad son los delitos cibernéticos más comunes.

La violencia en internet no tiene como fin el acoso cibernético en sí, en algunos casos es la captación de personas para trata de personas, para explotación, en el caso de las mujeres suele ser sexual, y en otros es generar mecanismos de control.

La normalización de la violencia digital “dificulta” a las mujeres “los procesos de denuncia”, aunque la mayoría no lo denuncia porque considera que “no tiene sentido”, apostilló el Centro de Derechos de Mujeres.

Estados Unidos de América

En los Estados Unidos, según el informe Pew de 2017, las mujeres tienen dos veces más probabilidades que los hombres de ser atacadas como resultado de su género.
Los gobiernos del Reino Unido y de los Estados Unidos de América presentaron en el año pasado proyectos de ley sobre seguridad en línea específicamente dirigidos a la protección de mujeres y de la infancia.

En Estados Unidos, la llamada “Iniciativa de Derechos”, encontró que las mujeres que son víctimas de la difusión de contenido sexual privado, es de 1.7 veces más que los hombres.

República de El Salvador

Según datos de la Fiscalía General de la República (FGR), de 2019 a 2021 se cometieron en El Salvador alrededor de 2,100 delitos de violencia sexual digital contra niñas, adolescentes, mujeres y personas con algún tipo de discapacidad.

De enero a junio de 2021, se registraron 124 casos de difusión de información ilegal y 1,874 expresiones de violencia contra la mujer a través de la tecnología, según datos del Observatorio de Violencia contra las Mujeres de la Organización de Mujeres Salvadoreñas por la Paz (Ormusa).

Según la Ley Especial Contra Delitos Informáticos y Conexos (LECDIC), las penas en El Salvador pueden ir desde los dos hasta los doce años de prisión, pero estas dependen del grado de delito informático que la persona haya cometido.

Estado de Palestina

Las mujeres en los Territorios Palestinos Ocupados afrontan altos niveles de violencia. Casi una cuarta de las mujeres casadas aseguran haber estado expuestas a abusos físicos, el 62 % a violencia psicológica y el 10 % a violencia sexual.

En Gaza, la presión del bloqueo israelí y la ocupación aumentan las tensiones en una sociedad donde las mujeres sufren severamente por culpa de tradiciones que permiten que sean discriminadas.

Es importante tomar en cuenta la falta de globalización del país, a la que pronto se verá expuesta debido al conflicto Israelí que suscita actualmente. La innovación golpeará la vida de millones de familias palestinas tan pronto como la guerra culmine. Con esta actualización tecnológica, se desatarán los riesgos de la tecnología. Si esto lo añadimos a las alarmantes cifras de acoso sexual, deducimos lo peligroso que será para las mujeres esta nueva realidad.

Reino de España

La ciber violencia de género se manifiesta de formas muy diversas. Casi dos de cada diez mujeres españolas, sido víctimas de acoso sexual y, afirman haber recibido insinuaciones sexuales humillantes, u ofensivas través de las redes sociales como Facebook, Instagram o Twitter. Y también a través de WhatsApp, correo electrónico y mensajes de texto.

Según la encuesta realizada por Save the Children en 2019 a 400 jóvenes de toda España, más de las tres cuartas partes de los encuestados han sufrido violencia online durante su infancia. El 47%, incluso más de un tipo.

Los tipos más habituales en España fueron el ciberacoso con un 40%, una práctica que sufrieron por primera vez entre los 8 y los 9 años, y que afecta en mayor medida a las niñas que a los niños. Mientras la mayoría fue por parte de un amigo o compañero del colegio, en casi el 16% de los casos se trató de una persona desconocida.

Además, el sexting sin consentimiento afectó al 3,74% de los encuestados en alguna ocasión, algunos de ellos en más de 6 ocasiones. Algo que sucedió en torno a sus 14 años, principalmente por parte del niño o niña con la que salían.

República Argentina

Las alarmantes cifras que maneja el Ministerio Público Fiscal de la Ciudad señalan que los procedimientos relacionados con la distribución de imágenes de pedofilia y el ciberacoso (grooming) crecieron dramáticamente. Durante 2020, en la Argentina aumentaron un 152% las consultas por delitos de acoso virtual contra niños y adolescentes.

Una encuesta global de Google reportó que el 49% de los padres argentinos informó que sus hijos comparten información en exceso en las redes, la cifra más alta de Latinoamérica. Otro estudio da cuenta de que el 40% de los jóvenes de entre 12 y 17 años han sido acosados online; el 30% de ellos, en más de una ocasión.

Las investigaciones llevadas a cabo por la Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (Ufedyci) condujeron a numerosos operativos para desarticular peligrosas redes tanto locales como internacionales.

República de Chile

En Chile, diversos tipos penales sobre acoso (general, sexual, laboral, escolar) contemplan medios tecnológicos para su comisión. Sin embargo, no existiría una figura penal específica de ciberacoso, como la referida en el proyecto de ley sobre violencia digital (boletín N° 13.928-07), en actual tramitación.

La PDI no cuenta con un protocolo especializado para acoger denuncias de ciberacoso de carácter sexual y extorsión, en este tipo de casos solo se aplica el procedimiento genérico. Consultados por CIPER, la institución afirmó que la Brigada de Cibercrimen Metropolitana, cuenta con un equipo especializado en la Investigación contra la Explotación Sexual de Niños, Niñas y Adolescentes y que dentro de esa unidad se investigan delitos sobre violencia de género digital. Afirman que desde marzo de 2021, la brigada mantiene un Whatsapp 24 horas, los siete días de la semana, para recibir denuncias relacionadas.

BIBLIOGRAFÍA

1. *Informar de un problema de ciberseguridad*. (s. f.). ONU Mujeres. https://www.unwomen.org/es/about-the-website/information-security/reporting-a-cyber-security-issue

2. Covarrubias, J. L. (2020, 7 septiembre). Observaciones y estudio de la iniciativa que expide la Ley General de Ciberseguridad en México | Foro Jurídico. *Foro Jurídico*. https://forojuridico.mx/observaciones-y-estudio-de-la-iniciativa-que-expide-la-ley-general-de-ciberseguridad-en-mexico/

3. *Ley Olimpia*. (s. f.). Ordenjuridico. Recuperado 25 de febrero de 2024, de http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

4. Global Open University. (2023, 2 marzo). *Ley Olimpia ¿qué es y cómo hacer uso de ella?* https://www.globalopenuniversity.mx/blog-gou/todas-las-noticias/noticias-2023/ley-olimpia-que-es-y-como-hacer-uso-de-ella.php

5. *Ciberseguridad*. (s. f.). Congresocdmx. Recuperado 25 de febrero de 2024, de https://www.congresocdmx.gob.mx/archivos/legislativas/Ciberseguridad.pdf

6. *Estándares y normas ISO para mejorar la ciberseguridad*. (s. f.). Global Suite. Recuperado 25 de febrero de 2024, de https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/

7. *Normas internacionales en materia de ciberseguridad*. (s. f.). News.Microsoft. Recuperado 25 de febrero de 2024, de https://news.microsoft.com/cloudforgood/_media/downloads/es/international-cybersecurity-norms-es.pdf

8. Dqs. (s. f.). *Normas para la seguridad de la información: una visión general*. https://www.dqsglobal.com/es-mx/aprenda/blog/normas-para-la-seguridad-de-la-informacion-una-vision-general

9. *Normas internacionales relativas a la privacidad digital*. (2024). OHCHR. Recuperado 25 de febrero de 2024, de https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy

10. *Convenio sobre la ciberdelincuencia*. (2001, 23 noviembre). OAS. Recuperado 25 de febrero de 2024, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

11. *Ciberseguridad*. (s. f.-b). IFT. Recuperado 25 de febrero de 2024, de https://ciberseguridad.ift.org.mx/seccion/mujeres

12. *La violencia de género en línea contra las mujeres y niñas*. (s. f.). OAS. Recuperado 25 de febrero de 2024, de https://www.oas.org/es/sms/cicte/docs/Guia-conceptos-basicos-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

13. Acuña, J. (2022, 11 noviembre). Buscando a las mujeres en el Plan Nacional de Ciberseguridad. *TEDIC*. https://www.tedic.org/buscando-a-las-mujeres-en-el-plan-nacional-de-ciberseguridad/

14. Del Consumidor, P. F. (s. f.). *La "Ley Olimpia" y el combate a la violencia digital*. gob.mx. https://www.gob.mx/profeco/es/articulos/la-ley-olimpia-y-el-combate-a-la-violencia-digital?idiom=es

15. *Manual de contenidos: Laboratorio de Análisis Multidiciplinario sobre la Ley Olimpia*. (s. f.). Semujeres. Recuperado 25 de febrero de 2024, de https://semujeres.cdmx.gob.mx/storage/app/media/ViolenciaDigital/Manual_Contenidos_Lab_Ley_Olimpia.pdf

16. Rivera, S. F. (2024, 6 febrero). *Ley de Ciberseguridad en México: Conoce la Nueva Ley*. https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico

17. *Acoso cibernético (ciberacoso)*. (2022, abril). Obtienearchivo. Recuperado 25 de febrero de 2024, de https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33111/2/BCN_ciberacoso_2022_CW.pdf

18. Olate, C. (2022, 2 diciembre). *Peligro en las redes: hombre acosó y extorsionó a más de 30 mujeres luego de acceder a sus fotos íntimas*. CIPER Chile.

https://www.ciperchile.cl/2022/12/01/peligro-en-las-redes-hombre-acoso-y-extorsiono-a-mas-de-30-mujeres-luego-de-acceder-a-sus-fotos-intimas/

19. *Delitos sexuales en internet y ciber violencia | Top Doctors*. (1970, 1 enero). Top Doctors. https://www.topdoctors.es/articulos-medicos/855-mujeres-fueron-victimas-de-delitos-sexuales-en-internet#

20. *Ciberacoso o ciberbullying*. (s. f.). Save The Children. https://www.savethechildren.es/donde/espana/violencia-contra-la-infancia/ciberacoso-ciberbullying

21. Nacion, L. (2021, 9 agosto). Acoso sexual en internet. *LA NACIÓN*. https://www.lanacion.com.ar/editoriales/acoso-sexual-en-internet-nid09082021/

22. Verdugo, C. V. (2023). El ciberacoso sexual, otro tipo de violencia de género en las universidades ecuatorianas en el poscovid 2020-2023: una prioridad pendiente. *Revista Educación Superior y Sociedad*, *35*(2), 237-261. https://doi.org/10.54674/ess.v35i2.841

23. *Niñas, niños y sus familias aprenden a reconocer el ciberacoso*. (2021, 5 mayo). World Vision. Recuperado 25 de febrero de 2024, de https://worldvisionamericalatina.org/ec/sala-de-prensa/niñas-niños-adolescentes-y-sus-familias-aprenden-a-reconocer-el-ciberacoso

24. *Tipificación del ciberacoso como violencia de género en la Legislación Penal Ecuatoriana*. (2018). Dspace. Recuperado 25 de febrero de 2024, de https://www.dspace.uce.edu.ec/server/api/core/bitstreams/c12c2a55-213d-447d-913e-feefa67a036d/content

25. Olivertapia. (2022, 14 junio). *Japón castigará los «insultos en línea» con un año de prisión a raíz de la muerte de una estrella de telerrealidad*. CNN. https://cnnespanol.cnn.com/2022/06/14/japon-castigara-insultos-en-linea-acosos-internet-ciberacoso-trax/

26. *El ciberacoso escolar es común en Japón, según un estudio*. (2008, 16 abril). Returners. Recuperado 25 de febrero de 2024, de https://www.reuters.com/article/oesen-internet-japon-bullying-idESCAR64299020080416/

27. Efe. (2024, 31 enero). El 77 % de mujeres ha sido víctima de ciberviolencia en Honduras, donde se denuncia poco. *SWI swissinfo.ch*. https://www.swissinfo.ch/spa/el-77-de-mujeres-ha-sido-v%C3%ADctima-de-ciberviolencia-en-honduras-donde-se-denuncia-poco/48502536

28. *Violencia contra mujeres y niñas en el espacio digital lo que es virtual también es real*. (s. f.). UNwomen. Recuperado 25 de febrero de 2024, de https://mexico.unwomen.org/sites/default/files/Field%20Office%20Mexico/Documentos/Publicaciones/2020/Diciembre%202020/FactSheet%20Violencia%20digital.pdf

29. *«Para las mujeres y las niñas, ningún lugar es completamente seguro»: a pesar de algunos avances, se necesitan medidas urgentes y más contundentes contra la violencia digital*. (s. f.). Fondo de Población de las Naciones Unidas. https://www.unfpa.org/es/news/para-las-mujeres-y-las-ninas-ningun-lugar-es-completamente-seguro-pesar-de-algunos-avances-se