



**Apaseo
el Grande**
GOBIERNO MUNICIPAL 2024-2027



**Atención
Integral a la
Mujer**

GLOSARIO

**TIPOS DE VIOLENCIA
CONTRA LAS MUJERES,
NIÑAS Y ADOLESCENTES**



#YoMeSumo

Riesgos y amenazas que enfrentan
niñas, mujeres y adolescentes
en el mundo digital



Tipos de violencia de género digital



Cybermobs

Acción de grupos organizados en línea que publican contenido ofensivo o destructivo, de forma masiva, con la intención de avergonzar a alguien o lograr el retiro de su perfil de redes sociales.

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.

Cyberbullying

Este tipo de violencia consiste en el envío o la publicación de comunicaciones o contenido (mensajes orales o escritos, imágenes, videos) por medio de tecnologías para expresar la intención de cometer un daño físico o violencia sexual.

Cyberflashing

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

Deepfake o video ultra falso

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.

Discurso de odio

Es el uso de un lenguaje que denigra, insulta, amenaza o ataca a una persona a causa de su identidad y/u otras características, como su orientación sexual o discapacidad.



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.

Geolocalización

Es la capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a internet.

Grooming o ciberengaño pederasta

Son actos deliberados de un adulto para acercarse a una persona menor de edad con el objetivo de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o traficar a la menor de edad.

Outing

Revelación en línea de la identidad o preferencia sexual de una persona.



Packs

Conjunto de imágenes de mujeres de naturaleza íntima o sexual obtenidas y/o distribuidas sin su consentimiento.

Pornovenganza

Término utilizado de forma incorrecta para referirse a la distribución no consensuada de imágenes o videos íntimos.

Raiding

Publicación de mensajes provocativos, ofensivos o fuera de lugar para atacar en línea de manera coordinada, desde una gran cantidad de cuentas, a una persona usuaria específica para producir un daño.



Sexting o sexteo

Es una práctica que implica la generación e intercambio de material sexualmente explícito entre dos personas. Puede incluir la creación y envío de imágenes de forma consensuada o la creación consensuada de imágenes que se distribuyen sin consentimiento.

Sextorsión

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



Slutshaming

Es una forma de violencia que consiste en señalar públicamente a una mujer por su supuesta actividad sexual con el fin de avergonzarla, dañar su reputación y regular su sexualidad. Puede implicar el uso de fotografías y/o videos y lenguaje denigrante.

Sockpuppet o cuentas apócrifas

Cuentas falsas no automatizadas que buscan pasar como usuarios reales para desinformar o difundir contenido sesgado sobre temas específicos.

Troll o trol

Persona con identidad desconocida que publica en línea mensajes con la intención de molestar, provocar una respuesta emocional por parte de las personas usuarias o alterar las conversaciones en línea.

Troleo de género

Publicación de mensajes, imágenes o videos, así como la creación de hashtags (etiquetas), con el propósito de molestar a mujeres y niñas o incitar a la violencia contra ellas.

Upskirting

Registro sin consentimiento de fotografías tomadas por debajo de la falda de una mujer o niña.



Riesgos y amenazas que enfrentan
niñas, mujeres y adolescentes
en el mundo digital



Amenazas de ciberseguridad

Amenazas Persistentes Avanzadas (APT).

Son ataques complejos, de largo plazo, que emplean diferentes recursos y frentes para llevarse a cabo. Su objetivo es el robo de datos a personas y organizaciones:

- Utilizan múltiples técnicas de ataque (cibernéticos, físicos y engaños).
- Se extienden dentro de los sistemas y estructuras de información de las organizaciones atacadas con el propósito de extraer información, perjudicar el funcionamiento de un sistema o programa;
- Tienen la capacidad de penetrar en un los sistemas y permanecer allí el mayor tiempo posible, provocando graves consecuencias para las víctimas.

Bot

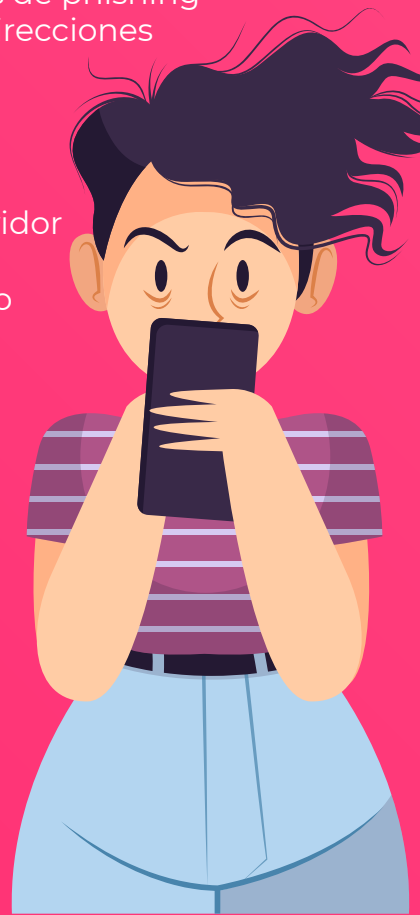
Es un programa o software que realiza tareas repetitivas, predefinidas y automatizadas. Algunos bots cumplen funciones útiles, como buscar y catalogar páginas web o ayudar a los clientes de una empresa.

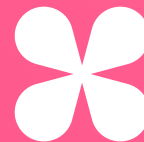
Bot malicioso

Existen otro tipo de bots que son enteramente maliciosos. Estos programas suelen imitar ciertos comportamientos de los usuarios legítimos, estos programas maliciosos pueden ser utilizados para:

- Robar archivos
- Cometer robos de identidad
- Hackear cuentas de usuario
- Enviar correos en forma masiva y realizar campañas de phishing
- Registrar información privada como contraseñas, direcciones y detalles bancarios
- Atacar sistemas, espiar a las personas u ocasionar interrupciones o vulnerar sitios web

Algunos bots maliciosos pueden incluso conectarse a un servidor central que cumple las funciones de “centro de control” para comandar una red de dispositivos comprometidos. A este tipo de red se le llama Botnet.





Cifrado de información

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

Denegación de servicio

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

Gusanos

Software malicioso que tiene la capacidad de replicarse y expandirse rápidamente en los archivos y programas de una computadora, generando a su paso diferentes tipos de daño. La existencia y expansión de los gusanos depende de la conectividad en red de varias computadoras. Los gusanos, a diferencia de los virus, no suelen infectar los archivos de la computadora, sino que infectan otros equipos conectados a la red. Los gusanos, a través de su carga útil, pueden infectar a los dispositivos con cualquier tipo de malware y con ello, permitir a terceros tomar el control del sistema, recopilar datos personales confidenciales, instalar ransomware o convertir los dispositivos en «zombis» para usarlos en ataques de redes de bots (botnet).



Hackeo

Uso de técnicas y procedimientos por un hacker para introducirse sin autorización en sistemas informáticos ajenos con el fin de manipularlos o de obtener información o por diversión. El cracking es una práctica relacionada con el hackeo, pero implica entrar en sistemas ajenos con fines delictivos para violar la intimidad de la persona afectada o la confidencialidad de la información o dañar la información o los soportes físicos.

Hacker

Persona que obtiene acceso no autorizado a un sistema informático.²



Keylogger o registrador de teclas

Es un software malicioso que se coloca entre el teclado y el sistema operativo para interceptar y registrar información de cada tecla pulsada en el dispositivo sin que la persona usuaria lo sepa.

² El término Hacker ha tenido connotaciones negativas. No obstante, este término en realidad se refiere a los especialistas informáticos, que a través de sus conocimientos pueden detectar amenazas y riesgos de ciberseguridad y a su vez, apoyar a personas y organizaciones para protegerse y resguardarse de ciberdelincuentes, a este tipo de especialistas se les conoce como hackers éticos o hackers de cuello blanco

Malware o programa malicioso

El término nace de la unión de las palabras en inglés maliciosa software y hace referencia a un tipo de software que tiene como objetivo infiltrarse y/o dañar un sistema de información sin el consentimiento de la persona usuaria.

Phishing o ataques con técnicas de ingeniería social

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

Ransomware de cifrado

Código, programa o software malicioso que, al introducirse a los dispositivos, tiene la capacidad de “secuestrar” la información de los usuarios (del inglés ransom), impidiendo el acceso a la misma por medio de técnicas de cifrado, es decir, por medio del uso de una contraseña que impide al usuario legítimo acceder a su información.

Una vez que el dispositivo ha sido infectado, se muestra un mensaje, exigiendo al usuario realizar un pago (generalmente en numerario) para acceder a la información secuestrada³.

Software

Conjunto de programas, instrucciones y reglas informáticas que permiten a los dispositivos electrónicos realizar determinadas tareas.

Spyware o software espía

Un tipo de programa maligno que infecta un dispositivo y graba secretamente y sin consentimiento datos de navegación, información personal, ubicación del dispositivo, registro de llamadas o mensajes, entre otros datos personales.

³ INCIBE. “Ransomware, una guía de aproximación para el empresario” (abril, 2021). https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware.pdf



Troyanos

Archivos, programas o fragmentos de código malicioso que funcionan haciéndose pasar por archivos legítimos, con el objetivo de engañar a las víctimas para que hagan clic en ellos, los abran o los instalen. Es decir, se empaquetan y entregan dentro de software legítimo (de ahí su nombre). Cuando esto ocurre, el troyano comienza a instalar malware en los dispositivos ⁴.

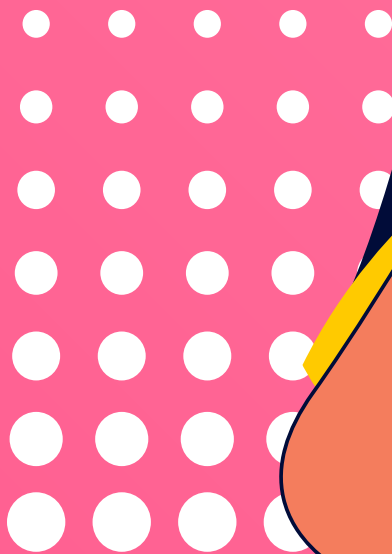
Los troyanos pueden infectar a los dispositivos móviles del mismo modo que lo hacen con las computadoras de escritorio o portátiles. Los Troyanos no puede expandirse ni infectar archivos por sí solos, requieren de un proceso de instalación por parte del usuario.

Los troyanos pueden ejecutar diversas acciones maliciosas sin el permiso de los usuarios, por ejemplo⁵:

- Eliminar datos
- Bloquear datos
- Modificar datos
- Copiar datos
- Interrumpir el funcionamiento de computadoras o redes de computadoras
- Tener acceso remoto a un sistema

Virus

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



⁴Avast Academy. "¿Qué es un malware troyano? Guía definitiva" <https://www.avast.com/es-es/c-trojan>

⁵Idem.



Conceptos básicos



Brecha de género

Se refiere a cualquier disparidad entre la condición o posición de las mujeres y hombres en la sociedad (diferencias en el acceso a recursos, derechos y oportunidades).

Estereotipos de género

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

Género

Se refiere a los roles, comportamientos, actividades, y atributos que una sociedad determinada en una época determinada considera apropiados para hombres y mujeres. El género también hace referencia a las relaciones entre mujeres y las relaciones entre hombres. Estos atributos, oportunidades y relaciones son contruidos socialmente y aprendidos a través del proceso de socialización [Fuente: ONU Mujeres, OSAGI Gender Mainstreaming - Concepts and definitions].

Igualdad de género

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

Perspectiva de género

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

Roles de género

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



Sexo (biológico)

Se refiere a las características biológicas que definen a los seres humanos como mujeres y hombres.

Violencia contra la mujer

Cualquier acción o conducta basada en su género que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado [Fuente: Artículo 1 de la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer].

Violencia de género en línea o ciberviolencia de género contra la mujer

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 Tecnologías de la Información y la Comunicación, 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 [Fuente: Relatora Especial sobre Violencia de la Organización de las Naciones Unidas].

¿Quiénes pueden ser los agresores?

Los 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 ciberengaño 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 expareja 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).



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.

¿Qué buscan los agresores con la violencia en línea contra las mujeres, niñas y adolescentes?

El objetivo de la violencia es crear un ambiente hostil en línea para las mujeres a fin de avergonzarlas, intimidarlas, denigrarlas, menospreciarlas o silenciarlas por medio de la vigilancia, el robo o la manipulación de información o el control de sus canales de comunicación (AI, 2018).



**Apaseo
el Grande**
GOBIERNO MUNICIPAL 2024-2027



**Atención
Integral a la
Mujer**