CURSO VIRTUAL

Ciudadanía y Derechos Humanos en la ERA DIGITAL

Módulo 1

Violencia digital de género

¿Qué es violencia digital de género?

- La violencia de género traspasa el entorno físico y se expresa también en el entorno digital, a esto se le llama violencia digital de género.

- Es importante recordar que la violencia de género es consecuencia de la desigualdad que persiste en las relaciones entre hombres y mujeres, que está definida por los roles que socialmente se han construido sobre lo femenino y lo masculino.

¿Qué es violencia digital de género?

La Asociación de Comunicaciones para el progreso (APC) una organización internacional de sociedad civil, define a la violencia digital de género como:

- “La violencia digital de género o en línea se refiere a actos de violencia de género cometidos instigados o agravados, en parte o totalmente, por el uso de las Tecnologías de la Información y la Comunicación (TIC), plataformas de redes sociales y correo electrónico. Estas violencias causan daño psicológico y emocional, refuerzan los prejuicios, dañan la reputación, causan pérdidas económicas y plantean barreras a la participación en la vida pública y pueden conducir a formas de violencia sexual y otras formas de violencia física.”

¿Qué es violencia digital de género?

- Se tiende a pensar el mundo físico y el mundo digital como algo separado; sin embargo, no existe tal división, lo que pasa en uno afecta al otro y viceversa.

- Las violencias digitales no son un nuevo tipo de violencia, si no que representan la violencia histórica que mujeres, niñas, adolescentes, poblaciones indígenas y otras poblaciones enfrentan hasta la actualidad. Estas violencias encontraron una nueva forma y espacio para expresarse en Internet

¿Cómo enfrentan violencias digitales estas poblaciones?

- Según el Estudio Conectadas y Seguras (2021) de Plan Internacional Bolivia, 7 de cada 10 niñas en Bolivia manifestaron que sintieron acoso en línea en algún momento de su vida.

- En “Los retos de las niñas y mujeres de la tercera edad para sobrevivir a la brecha digital en tiempos de pandemia en el departamento de La Paz” menciona que las niñas y adolescentes han generado cierta desconfianza con el uso de la tecnología, las niñas y adolescentes entrevistadas para este estudio consideran que este espacio no es seguro para ellas, por experiencias de acoso que enfrentaron mientras usaban Internet.

- En un sondeo sobre violencia digital, participaron 1.123 mujeres mujeres de las cuales casi 900 recibieron mensajes molestos de forma repetitiva en medios digitales, 337 recibieron insultos en redes por su identidad sexual, y 300 mujeres dijeron que en algún momento se publicó información personal sin su consentimiento como: nombre completo, número de celular, correo electrónico, entre otros.

Violencias digitales más frecuentes y el Centro S.O.S. Digital

Violencias digitales

MÁS FRECUENTES

ACOSO

Conductas de carácter reiterado públicos y privados donde se reciben contenidos no solicitados (material sexualizado, insultos, amenazas, expresiones discriminatorias) que resultan **molestas e intimidantes.**

- Acoso sistemático con insultos:
  casos donde son desde 6 meses, 1 año y 3 años.
- Amenazas de agresión física, violación muerte o violencia a un familiar o persona cercana.
- Envío de contenido a familiares o personas cercanas:en menos cantidad pero con agravante.
- Mensajes con insultos y amenazas de perfiles falsos.
- Amenazas sistemáticas.
- En menor cantidad, realizan denuncias en la FELCV que no son aceptadas.

ABUSO DE INFORMACIÓN PERSONAL USANDO LAS TIC

Robo, obtención, pérdida, control o modificación de información personal no consentida

- Acoso sistemático
- Desprestigio, algunas usando imágenes manipuladas.
- Publicación de datos personales, nombres, contratos, usuarios de twitter con afinidad política.

ABUSO SEXUAL RELACIONADO CON LAS TIC

Ejercicio de poder sobre una persona a partir de la explotación sexual de su imagen y/o cuerpo contra su voluntad

- Acoso sistemático.
- Amenazas: de publicar contenido íntimo (fotos y videos), para obtener dinero, con difamar a la persona, con el fin de obtener más fotos íntimas.
- Captura de información sin consentimiento: a través de video llamadas o engaños.
- Crackeo: cambio de contraseñas de cuentas personales.
- Engaño: afectivo para tomar confianza de la denunciante y con ofertas laborales para cometer abuso sexual.
- Extorsión.
- Intento de captación con fines sexuales.
- Publicación de contenido íntimo, en menor cantidad pero es una agravante.
- Comercialización de contenido íntimo, en menor cantidad pero es una agravante.

¿Cómo responder?

- Existe desconocimiento sobre cómo proceder cuando una persona esta enfrentando violencia digital el Centro S.O.S. Digital brinda algunas estrategias:
- Es importante recordar que la persona que enfrenta violencia digital no es culpable de lo que le esta ocurriendo, la culpa siempre será de la persona agresora.
- Es importante que la persona que enfrenta violencia digital recurra a su círculo de apoyo para expresar como se siente.
- Muchas veces las personas que ejercen violencia digital solicitan el envío de fotos íntimas o envío de dinero, es importante no responder a estos mensajes.
- Sacar capturas de pantalla a los mensajes, perfiles, publicaciones y guárdalos en un lugar seguro es importante cuando una persona enfrenta violencia digital, las pruebas en Internet desaparecen rápido.
- Si la persona que enfrenta violencia digital tiene los mensajes en su celular o en sus cuentas de redes sociales, es importante no eliminarlos.

¿Cómo denunciar violencias digitales?

- Instancias promotoras de denuncia

- También se puede realizar una denuncia en: La Policia donde se presenta la denuncia de forma verbal en plataforma de la Policía Boliviana, quien toma la denuncia debe entregarte una copia. La policía, dentro de las 24 horas debe informar al fiscal para iniciar la investigación.

- En él Ministerio Público donde la denuncia de forma escrita a través de una denuncia o una querella. La o el Fiscal inicia la investigación, debiendo informar al juez de instrucción en materia penal.

Las violencias digitales de género no son un fenómeno nuevo, son violencias estructurales reflejadas en otro espacio: la tecnología.

Cultura de impunidad

- Sistema judicial: las mujeres se vean disuadidas de denunciar a las personas que comenten actos violentos.
- Escasa concientización en funcionarios y funcionarias
- No hay delitos específicos: se puede hacker el sistema legal metiendo denuncias por Pornografía, acoso sexual o violencia psicológica
- Ausencia de un sujeto punible por el anonimato
- Datos insuficientes de casos de violencia digital
- Plataformas digitales: respuesta poca proporcional a un acto violento.
- Analfabetismo digital

seguridad digital depende de la víctima

- Atención a las violencias digitales recae en la víctima/denunciante
- Depende de sus habilidades digitales para poder prevenir y resistirlas.

seguridad digital

estrategias de respuesta ante violencias digitales

resistencia tecnológica

normativa boliviana

contención psicológica

Prevención

Legal: conocer los derechos que se tienen en Internet

Psicológica: Mapear a las personas y **organizaciones que puedan brindar ayuda**

Tecnológica: Generar **hábitos digitales** (contraseñas seguras, respaldos de la información, reconocer enlaces maliciosos, activar la verificación o autenticación en 2 pasos.

Reacción

Legal: Conocer la normativa, delitos y procesos de denuncia.

Psicológica: Generar con protocolos o acciones comunitarias

Armar un grupo **autocuidado**

acompañar a la denunciante **con la escucha activa**

Tecnológica: Denunciar o reportar contenido


Informe de gestión de incidente
https://www.csirt.gob.bo/es/noticias/informe-de-gestion-de-incidentes-y
80%
CGII
Centro de Gestión de
Incidentes Informáticos
Inicio
Acerca del CGII
Noticias
Alertas de Seguridad
Publicaciones
Reportar Incidente
Estadísticas
Normativa
RFC 2350
PISI
Noticias / Informe de gestión de incidentes y vulnerabilidades informáticas - Segundo trimestre 2022
Informe de gestión de incidentes y vulnerabilidades informáticas - Segundo trimestre 2022
Fecha de publicación: Mar, 05/07/2022 - 17:16
El Centro de Gestión de Incidentes Informáticos de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación publica el informe de gestión de incidentes y vulnerabilidades correspondiente al segundo trimestre del 2022, en el marco del Decreto Supremo 2514 que establece las funciones del CGII.
Monitorear los sitios web gubernamentales y la aplicación de las políticas y lineamientos definidos por la AGETIC.
Comunicar y otorgar información a todas las entidades del sector público acerca de incidentes informáticos y vulnerabilidades de que haya tomado conocimiento.
Prestar soporte técnico a las entidades del sector público en caso de que ocurriese un incidente informático.
Otorgar soporte técnico para la prevención de incidentes informáticos a las entidades del nivel central del Estado a solicitud de las mismas.
Coordinar la gestión de incidentes informáticos gubernamentales con entidades de similar función a nivel internacional.
Durante el segundo trimestre del 2022, se gestionaron 249 incidentes y vulnerabilidades que corresponden a reportes nuevos y abiertos en meses anteriores. Del total de casos, 154 fueron resueltos a través de la correcta comunicación, seguimiento y validación con las entidades afectadas y 95 casos están siendo gestionados para su solución; los resultados serán reflejados en siguientes informes.
El informe muestra estadísticas de la atención de casos válidos de incidentes y vulnerabilidades durante el segundo trimestre del 2022, cuyos datos fueron clasificados en términos de cantidad y porcentaje. También se tiene una relación porcentual entre los casos que fueron resueltos y de aquellos que están en proceso de solución.
Acceda al informe completo desde este enlace IGIV-Segundo-Trimestre-2022.
Fuente
Centro de Gestión de Incidentes Informáticos
Search
¡Reportar Incidente!
Top 5 Muro de la Fama
REPORTANTE
PUNTOS
Joshua Provoste 857
lagear 697
UnD3sc0n0c1d0 551
r0ck3r 534
@jivan 354
Lista completa
Inicio de sesión
Username*
Contraseña*
CAPTCHA

seguridad digital feminista

CSIRT (Computer Security Incident Response Team) -> **Equipo de respuesta a incidentes de seguridad informática.**

- Impacto en los sistemas (celulares, computadoras, servidores, redes internas, Internet etc.) y mejorar los niveles de seguridad

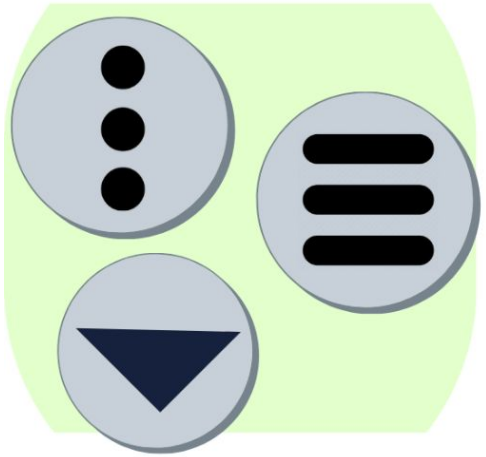
La seguridad digital con perspectiva de género

- la mejora de seguridad informática
- procesos de **alfabetización digital**
- Cuidado colectivo
- - Impactos de las violencias
- - El rol de las empresas de tecnología, academia, Estado y organizaciones que definen estándares y políticas de tecnología e Internet
- Evitar procesos de culpabilización y revictimización

SÍMBOLOS DE LA SEGURIDAD DIGITAL

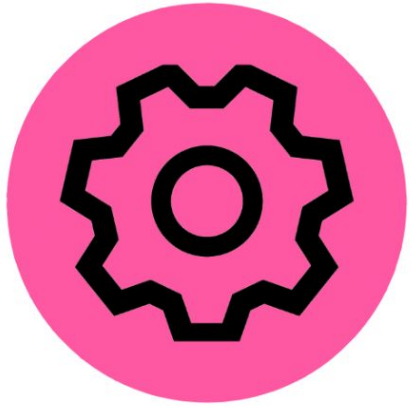
Existen símbolos que las plataformas digitales usan de manera frecuente para señalar el camino hacia la seguridad digital. Se recomienda seguir los siguientes pasos para navegar en las configuraciones con el fin de personalizar la seguridad y privacidad en cada plataforma.

1. IDENTIFICA EL **MENÚ**



El Menú puede ser visto como **3 puntos, 3 rayas** o **1 triángulo**. Normalmente los encuentras al abrir la aplicación en la parte **derecha superior.**

2. BUSCA **AJUSTES**



La sección de **Ajustes** o **Configuración** suele ser representada por un **engranaje**.

3. BUSCA **SEGURIDAD**

Encuentra **Seguridad** buscando el ícono de un **escudo**.

4. BUSCA **PRIVACIDAD**

La opción de **Privacidad** suele ser representado por un **candado**.

Práctica

- En base a las instrucciones de la Simbología de Seguridad Digital, ingresa a WhatsApp y activa la Autenticación de 2 pasos.
- Abre tu navegador e ingresa a estos enlace para instalar Extensiones que protegan tu privacidad:
  - https://www.eff.org/https-everywhere
  - https://privacybadger.org/
  - https://adnauseam.io/