

LAS REDES SOCIALES Y SUS PELIGROS



QUE SON LAS REDES SOCIALES

Las redes sociales son plataformas digitales que conectan a personas con intereses o relaciones en común.

Funcionan como espacios virtuales donde los usuarios pueden:



Compartir información

Publicar textos, imágenes, videos, opiniones y experiencias personales con una audiencia global.



Interactuar

Comentar, compartir publicaciones, enviar mensajes privados y participar en conversaciones.



Conectar con otros

Encontrar a amigos, familiares, conocidos o personas con intereses similares de todo el mundo.



Pero... siempre hay un **"PERO..."**

Donde hay oportunidades, también existen riesgos que debemos conocer y evitar.

La protección de nuestros datos personales: <https://youtu.be/CXminNoDrTI>



PELIGROS DE LAS REDES SOCIALES



Adicción digital

El uso excesivo de las redes sociales puede ser adictivo y afectar gravemente la salud mental, física y el rendimiento académico de los jóvenes.



Violación de privacidad

Es crucial ser consciente de la información personal que compartimos y cómo las empresas utilizan nuestros datos privados.



Ciberacoso

Las redes sociales pueden convertirse en un espacio para el acoso, hostigamiento online, difamación y exclusión social digital.



Comparación social

Compararse constantemente con los demás en redes sociales puede generar sentimientos de baja autoestima, ansiedad e insatisfacción personal.



Desinformación

En las redes sociales circula abundante información falsa, engañosa o manipulada que puede influir en nuestras decisiones y creencias.



EL ADIVINO DE LAS REDES SOCIALES: <https://www.youtube.com/watch?v=j-tFoYNHi1w>

PELIGROS DE LAS REDES SOCIALES

Top 10 de los principales peligros de las redes sociales para los jóvenes

- 01 Problemas para la privacidad
- 02 Suplantación de identidad
- 03 Adicción a las RRSS
- 04 Ciberbullying
- 05 Contacto con desconocidos que pueden ser peligrosos
- 06 Grooming
- 07 Sexting
- 08 Sextorsión
- 09 Fake news y la distorsión de la realidad
- 10 Challenge o retos muy peligrosos, en ocasiones delictivos

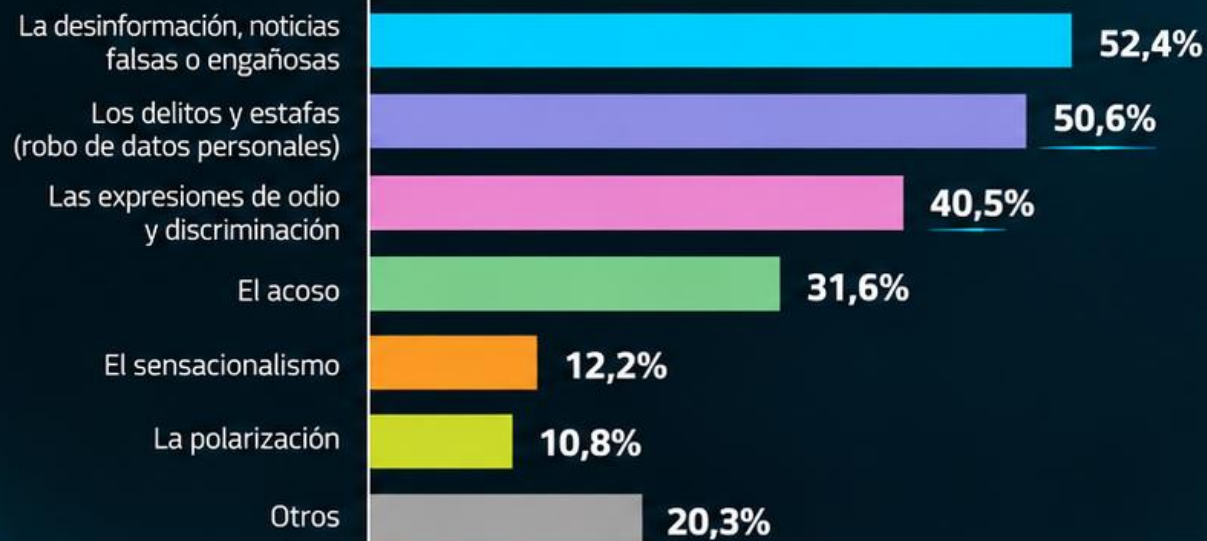


<https://farodigital.org/campanas/>

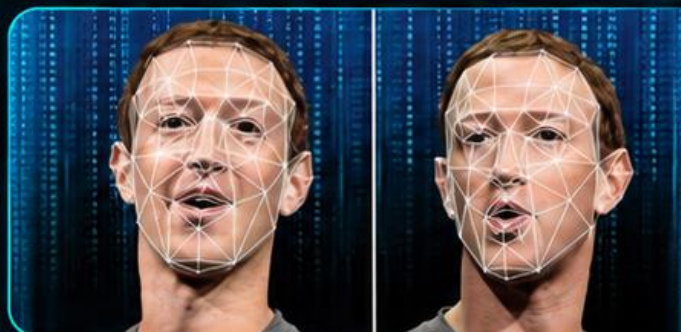


FAKES NEWS Y REDES SOCIALES

Aspectos negativos identificados



Las imágenes también pueden ser manipuladas y difundirse como reales.



Los deepfakes pueden hacer parecer reales situaciones que nunca ocurrieron.



**“Un deepfake puede destruir la reputación de una persona en segundos.
Cuidemos lo que compartimos.”**



PIENSA ANTES DE ENVIAR: <https://www.youtube.com/watch?v=cdZ4SBT4w3I>

LA LEY EMA

PROYECTO DE LUCHA CONTRA LA VIOLENCIA DIGITAL

guía EMA

Una herramienta para abordar la difusión no consentida de material íntimo en escuelas.

NoMás Mates

Encuentro

LEY OLIMPIA
ARGENTINA

LAURA CLARK
VALERIA BONOAL

defensoras
digitales

RED
FEDERAL



Ley

EMA

por una educación digital
libre de violencias

Es una serie de 6 rutas, cada una basada en un derecho de la Convención de los Derechos Digitales de niñas, niños y adolescentes, con actividades, orientaciones, carteles para usar en redes sociales y fichas para reconocer y abordar situaciones como la toma y difusión de material íntimo sin consentimiento en escuelas de todo el país.

NoMás Mates

Encuentro

LEY OLIMPIA
ARGENTINA

defensoras
digitales

RED
FEDERAL

SERIE DE
RUTAS

la virtual es real



<https://farodigital.org/portfolio/guia-ema/>



TALLERES - EL FARO DIGITAL

<https://talleres.farodigital.org/event/>

GROOMING Y CIBERACOSO

GROOMING

Estrategia utilizada por un adulto para ganar la confianza de un menor a través de Internet con fines sexuales.



- 1** Identificar a la posible víctima a través de redes sociales o chats.
- 2** Ganarse la confianza del menor acoplando gustos y comportamientos.
- 3** Seducir a la potencial víctima a través de conversaciones eróticas.
- 4** Obtención de contenido íntimo que permite ejercer presión sobre el menor.
- 5** Acoso, chantaje, amenazas y manipulación para lograr sus objetivos.

POLICÍA NACIONAL
DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INFORMÁTICA

GROOMING: CUANDO LA PEDOFILIA AMENAZA EN LAS REDES SOCIALES

Las redes más utilizadas por pedófilos son Facebook y WhatsApp.

¿CÓMO DETECTAR SI ES GROOMING?

- 1 Busca obtener información y generar confianza en la víctima.
- 2 Crea un vínculo emocional con el menor para que le envíe fotos y videos.
- 3 Acosa y extorsiona con las fotos obtenidas y puede pactar una cita.

¿CÓMO PREVENIRLO?

- ❌ NO PUBLICAR FOTOS PERSONALES NI INFORMACIÓN PRIVADA.
- ❌ USAR PERFILES PRIVADOS EN LAS REDES.
- ❌ NO ACEPTAR A DESCONOCIDOS.
- ❌ USAR CONTRASEÑAS PRIVADAS Y COMPLEJAS.

¿ESTÁS DISPUESTO/A A QUE ESA FOTO PUEDA VERLA TODO EL MUNDO Y PARA SIEMPRE?

EN SITUACIÓN DE ACOSO...

- 1 Guarda todas las pruebas que puedas.
- 2 NO CEDAS ante el chantaje. Pide ayuda.

CENTRO DE INVESTIGACIÓN POLICIA
Castilla-La Mancha juvenil

LOS 10 MEJORES CONSEJOS DE CIBERSEGURIDAD PARA PADRES



- 1 Estar informado, actualizado, y alerta
- 2 Conocer las herramientas, los riesgos y las reglas
- 3 Usar herramientas de protección en línea
- 4 Estimular el pensamiento crítico
- 5 Configurar tu conexión a internet para un uso seguro
- 6 Aprender acerca de las redes sociales
- 7 Entender los juegos y aplicaciones
- 8 Entender la violencia en línea
- 9 Confiar, invertir tiempo, monitorear y educar
- 10 Practicar lo que predicas



**LEY. 27499
LEY MICAELA**

#NI UN MENOS

➤ **GROOMING:** <https://www.youtube.com/watch?v=LxfcvzgKmUs>

➤ **BULLING – CIBERACOSO:** <https://www.youtube.com/watch?v=l4BEcp1Ulsg>

¿QUE NOS PROTEGE?



CONVENIO DE BUDAPEST

Convenio Budapest:

Se trata del primer tratado internacional creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional.

RGPD



Cumplimiento con Leyes y Regulaciones Locales:

Promulgada en el año 2000. Evaluar el cumplimiento de con las leyes y regulaciones argentinas relacionadas con la seguridad de datos y la privacidad, como la Ley de Protección de Datos Personales (Ley N° 25.326).

Ley 25.326

Protección de Datos Personales



Actualización Ley 25326:

En 2022, se presentaron proyectos para actualizar esta ley, buscando adaptarla más estrechamente al RGPD de la Unión Europea.



Ley de Delitos Informáticos (Ley 26.388):

Promulgada en 2008, esta ley modifica el Código Penal para incluir delitos informáticos, tales como: Acceso ilegítimo a sistemas y datos informáticos. Daños y sabotajes informáticos. Fraude electrónico. Distribución de malware.



VIDEO: Leyes en Argentina sobre ciberseguridad y delitos informáticos

¿QUE NOS PROTEGE?

Hasta Mayo 2018

LOPD (99-2007)



Naturaleza/tipos de datos Personales



Clasificación Niveles protección



Inscripción de ficheros

Información y consentimiento

Derechos: Acceso, rectificación, Cancelación etc.

Proteger transacciones y compartición de datos

Documento de Seguridad

Requisitos LOPD según niveles

Desde Mayo 2018

LOPD (2018)

=

Reglamento Europeo de Protección de datos (RGPD)

+

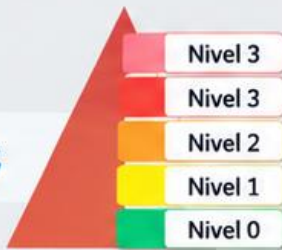
Requisitos Agencia Española



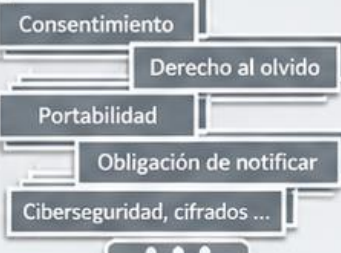
Naturaleza/tipos de datos Personales



Análisis De Riesgos



Clasificación por Nivel de Riesgo / Impacto



Nuevos Requisitos según niveles



Actualización Ley 25326 actualización 2022 basada en RGDP

DISCORD – JUEGOS EN LÍNEA

¿Qué es Discord?

Es una aplicación social que permite a los usuarios que juegan videojuegos comunicarse entre sí a través de chats y mensajes de voz.

¿Qué riesgos tiene esta aplicación?

Existen diferentes riesgos. Las personas que usan esta aplicación pueden ser víctimas de:

Ciberacoso - grooming - robo de datos personales



EL PELIGRO MAS IMPORTANTE: LA DESHUMANIZACIÓN

Detrás de todas las pantallas, algoritmos y notificaciones, existe un riesgo fundamental que a menudo pasa desapercibido: **la pérdida gradual de nuestra humanidad.**



Pérdida de empatía

La comunicación digital puede hacernos olvidar que detrás de cada perfil hay una persona real con sentimientos.



Relaciones superficiales

Las conexiones online a menudo carecen de la profundidad y autenticidad de las relaciones cara a cara.



Desconexión con la realidad

El mundo virtual puede convertirse en un escape que nos aleja de experiencias reales y significativas.

Recordemos que la tecnología debe ser una herramienta para enriquecer nuestras vidas, no para reemplazar las conexiones humanas auténticas que nos hacen verdaderamente felices.

El primer paso para protegernos es reconocer estos peligros.
El segundo, es elegir conscientemente cómo queremos relacionarnos con la tecnología y entre nosotros.

PHUBBING – ADICCION A LOS CELULARES

