GUÍA DE PREVENCIÓN DE CIBERDELITOS Y RIESGOS DIGITALES

Protección y educación digital para la comunidad

Buenos Aires Ciudad
Ministerio de Seguridad
División Innovación y Capacitación
Subsecretaría de Relaciones con la Comunidad y Asuntos Interjurisdiccionales e Internacionales en Seguridad
POLICIA
SUBSECRETARÍA DE INVESTIGACIONES

INTRODUCCIÓN

Puntos claves: Protección y educación digital para la comunidad

En la actualidad, la tecnología forma parte esencial de nuestra vida cotidiana. Nos comunicamos, trabajamos, estudiamos y nos entretenemos a través de dispositivos digitales. Sin embargo, este entorno también presenta riesgos que pueden afectar nuestra seguridad, privacidad y bienestar emocional. Las estafas en línea, el robo de datos, el acoso digital, el grooming, el uso inadecuado de redes sociales y las apuestas online son algunas de las amenazas más frecuentes.

Esta guía tiene como objetivo brindar información clara y sencilla para que cada persona, familia y comunidad pueda identificar riesgos, prevenir delitos y actuar de manera segura frente a diversas situaciones que puedan llegar a comprometer la integridad digital.

1. Identidad Digital y Vulnerabilidad Emocional

Puntos claves: Comprender los ciberdelitos más comunes

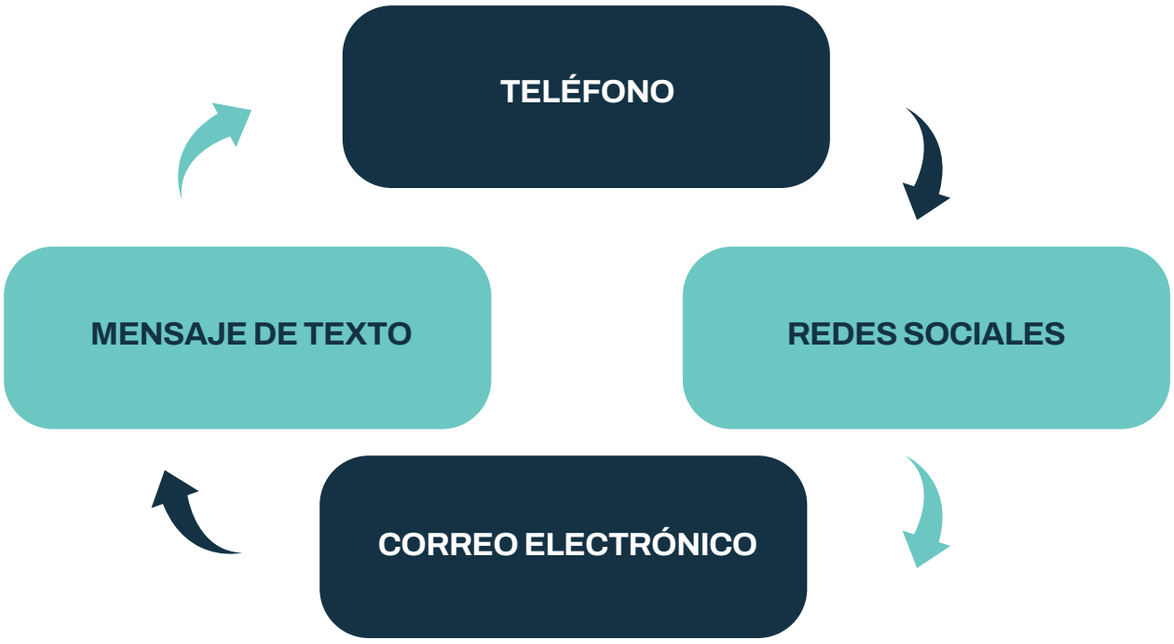
Las estafas en línea suelen aprovechar la vulnerabilidad emocional, como el miedo o la urgencia, para engañar y manipular a la víctima. Los ataques pueden llegar a través de mensajes de texto, llamadas telefónicas, correos electrónicos o redes sociales. Además, nuevas tecnologías como la inteligencia artificial permiten crear imágenes o videos falsos muy realistas, complicando la detección de fraude.
Cada usuario construye una identidad digital a través de sus perfiles, publicaciones, comentarios y actividades en línea. Esa huella digital puede ser aprovechada por ciberdelincuentes para obtener información personal, manipular emociones o cometer fraudes.

¿Cuál es el patrón común de las estafas?

Los ataques más comunes apelan a nuestras emociones:

- **Alegría** (“Ganaste un premio”)
- **Preocupación** (“Tu cuenta será bloqueada”)
- **Urgencia** (“Tenés que actuar ya”).

Estos mensajes buscan que la persona responda sin pensar. Recordá: cuanto más urgente parezca la situación, más tiempo debes tomarte para verificarla. Aprovechan nuestra vulnerabilidad emocional para manipularnos y conseguir datos o dinero. La prevención comienza con la calma, el sentido común y la verificación de la fuente.



2. ¿Qué son los ciberdelitos?

Puntos claves: ¿Cuáles son los delitos más comunes?

Los ciberdelitos son actividades ilegales que se realizan a través de dispositivos electrónicos y redes informáticas, como internet, con el objetivo de causar daños, robo de datos, fraudes o acoso. Incluyen acciones como el robo de identidad, el fraude en línea, el acoso (ciberbullying, sexting y grooming), el uso de malware para dañar sistemas y el sabotaje informático.

Principales tipos:

Estafas por urgencia: Mensajes o llamadas que generan una falsa sensación de urgencia para engañar a la víctima. Por ejemplo, pueden decir que has ganado un premio que debes reclamar de inmediato, o que tu cuenta bancaria está en riesgo y debes "verificar" tus datos urgentemente para evitar la pérdida de tu dinero.

Phishing: Se trata de correos electrónicos, mensajes de texto o sitios web falsos que imitan a empresas legítimas (como bancos, redes sociales o tiendas). El objetivo es hacer que el usuario revele información confidencial como nombres de usuario, contraseñas, números de tarjeta de crédito o datos bancarios.

Ciberbullying: Es el acoso o la intimidación a través de plataformas digitales como redes sociales, mensajería instantánea o juegos en línea. Puede manifestarse de varias maneras: Difundiendo mentiras o rumores, publicando fotos o videos vergonzosos de alguien sin su permiso, enviando mensajes, imágenes o videos hirientes, abusivos o amenazantes, creando perfiles falsos para hacerse pasar por otra persona y causar daño.

Grooming: Es una forma de abuso infantil en la que un adulto contacta a un menor, usualmente a través de chats o redes sociales, para ganarse su confianza y eventualmente tener una relación de carácter sexual o explotarlo.

Sexting: es el envío de mensajes, fotos o videos de contenido sexualmente explícito a través de dispositivos electrónicos. El riesgo surge cuando este material es compartido sin consentimiento o usado para extorsionar a la persona que lo envió.

Juegos y apuestas online: Pueden generar adicción, pérdidas económicas y problemas legales dependiendo que plataforma se utilice y pueden ser usados para realizar estafas o chantajes.

Además, nuevas tecnologías de inteligencia artificial permiten crear imágenes y videos falsos, complicando distinguir lo real de la manipulación.

3. Las tres reglas básicas de la prevención digital

No actuar bajo presión. Si el mensaje genera miedo, enojo o apuro, detente. Las emociones nublan el pensamiento.

Verificar la identidad. Confirma siempre quién te contacta. ¿Te llamaron llamaste? ¿De dónde sacaron tus datos?

Tomarte tu tiempo. Las urgencias de los demás no deben ser las tuyas. Revisar y comprobar antes de actuar evita ser víctima de estafas.

4. Prevención en correos, mensajes y redes

- **Puntos clave:** Los correos electrónicos falsos **(phishing)** y los mensajes engañosos **son métodos frecuentes de estafa.**
- **Revisa siempre el remitente.** Las direcciones falsas imitan a las reales cambiando una letra o agregando símbolos.
- **Presta atención a la redacción.** Si el texto parece traducido o usa un tono poco habitual, probablemente sea fraudulento.
- **Nunca hagas clic en enlaces** ni abras archivos adjuntos sin verificar su origen.
- **Ante la duda, ingresa directamente a la página oficial** del organismo o empresa.
- **No compartas códigos de verificación ni contraseñas**, aunque te los pidan desde supuestas cuentas “oficiales”.

Recordá que los bancos, organismos públicos y plataformas legítimas nunca piden datos personales por mensaje o correo electrónico.

5. Inteligencia Artificial y manipulación de imágenes

Puntos claves: El avance de la inteligencia artificial (IA) Usos y Abusos

El avance de la inteligencia artificial (IA) permite crear imágenes, videos o audios falsos con gran realismo. Esta tecnología tiene usos positivos, educativos, creativos o artísticos, pero también puede emplearse para difundir engaños, manipular información o suplantar identidades.

Riesgos principales:

Creación de noticias o videos falsos (deepfakes), imágenes o audios que han sido manipulados, normalmente con el objetivo de suplantar la identidad de alguien, utilizando inteligencia artificial (IA).

Difusión no consentida de imágenes íntimas **creadas o manipuladas** utilizando inteligencia Artificial (IA).

Estafas basadas en suplantación de voz o rostro. Se trata de un tipo de fraude en el que los delincuentes utilizan inteligencia artificial (IA) para imitar la voz o la apariencia de una persona y engañar a las víctimas.

Recomendaciones:

- **Verifica siempre la fuente del contenido.** Ante cualquier información, llamada, video o mensaje que recibas, especialmente si te solicita algo urgente o inusual, debes confirmar quién es la persona o entidad que se está comunicando. No confíes solo en lo que ves o escuchas.

- **No compartas material sensible:** Evita publicar en redes sociales o en cualquier otro medio digital contenido personal que pueda ser usado en tu contra.

- **Promové el pensamiento crítico:** no todo lo que ves o escuchas en internet es real. No te dejes llevar por las emociones. Cuestiona la autenticidad de lo que te llega, aunque parezca convincente

6. Riesgos para niños, niñas y adolescentes

Puntos claves: Grooming, sexting y otros riesgos para niños, niñas y adolescentes

Las personas menores de edad son especialmente vulnerables en entornos digitales. Existen diversas formas de violencia y abuso que deben ser conocidas y prevenidas.

Grooming: Es un delito en el que un adulto contacta a un niño, niña o adolescente a través de medios digitales para ganarse su confianza y obtener material sexual o concretar un abuso. En Argentina, el Artículo 131 del Código Penal establece penas de 6 meses a 4 años de prisión para quien contacte a menores con fines sexuales.

Sexting: Consiste en el envío voluntario de imágenes o videos íntimos. Aunque parezca una práctica privada, su difusión no consentida puede tener consecuencias graves: exposición pública, extorsión, acoso o daño emocional.

Prevención:

- **Mantener el diálogo abierto** y de confianza con niñas, niños y adolescentes.
- **Evitar prohibiciones extremas:** enseñar es más efectivo que prohibir.
- **Supervisar el uso de dispositivos** en espacios comunes del hogar.
- **Configurar la privacidad en redes sociales** y evitar compartir fotos personales o datos sensible

7. Juegos y apuestas online
Puntos claves: Los juegos y plataformas de apuestas Usos y Abusos

Los juegos y plataformas de apuestas en línea están diseñados para generar interacción constante y sensación de recompensa. Su uso desmedido puede provocar adicción, pérdidas económicas y aislamiento social.

Etapas del uso problemático:

Uso recreativo: En esta etapa, el juego es una actividad de ocio más, una forma de entretenimiento que se practica de manera ocasional y con límites claros. La persona puede disfrutar de la experiencia, ya sea ganando o perdiendo, sin que ello afecte negativamente otras áreas de su vida.

Juego problemático: aumento del tiempo y gasto de dinero. Es una fase de transición en la que el juego empieza a dejar de ser una simple diversión y ocupa un lugar más prominente en la vida de la persona. Se incrementa la frecuencia, el tiempo y la cantidad de dinero que se gasta en el juego, generando las primeras consecuencias negativas.

Ludopatía: necesidad compulsiva de jugar, pérdida de control y afectación emocional. Pierde el control sobre su comportamiento de juego, a pesar de las graves consecuencias negativas. El juego se convierte en la prioridad absoluta, por encima de la familia, el trabajo y las finanzas.

Consecuencias: bajo rendimiento escolar, endeudamiento, conflictos familiares y problemas de salud mental.

Recomendaciones:

- **Establecer horarios:** Es una medida de control para gestionar el tiempo dedicado al juego, especialmente en el caso de jóvenes. Se debe acordar un tiempo limitado y respetarlo rigurosamente. Objetivo: Evitar que el juego absorba cada vez más tiempo, lo que podría llevar al abandono de otras actividades importantes como el estudio o el ejercicio.

- **Acompañar el uso:** En el caso de los menores o personas en riesgo, es importante que los adultos supervisen activamente el uso de dispositivos y el tipo de juegos que se consumen, especialmente los juegos de azar en línea.

Objetivo: Prevenir el acceso a sitios de apuestas y detectar tempranamente cualquier señal de uso problemático.

Conversar sobre riesgos: Hablar abierta y honestamente sobre los riesgos asociados al juego. Explicar cómo funciona el azar y desmitificar la idea de que la suerte o la habilidad garantizan las ganancias. Objetivo: Desarrollar el pensamiento crítico y la toma de decisiones responsable, especialmente en los adolescentes que pueden ser más vulnerables a la publicidad engañosa.

Buscar ayuda profesional: Cuando se observan los primeros signos de una posible adicción, como el aumento de tiempo y gasto, la pérdida de control o la irritabilidad al no poder jugar, es fundamental buscar la orientación de especialistas en adicciones. Objetivo: Intervenir a tiempo para evitar que la situación escale hasta la ludopatía, que es una enfermedad grave que requiere un tratamiento especializado.

8. Qué hacer si sospechas ser víctima de un ciberdelito

No borres nada. Toda información puede servir como evidencia.

Deja de responder o interactuar. No alertes al ciberdelincuente.

Toma capturas de pantalla y guarda todos los mensajes, correos o publicaciones.

No realices pagos ni coordines encuentros personales.

Identifica el origen del mensaje o cuenta. Preserva la información: no la modifiques ni la reenvíes.

9. Dónde Denunciar

En caso de ciberdelito, podes recurrir a los siguientes canales oficiales:

Ministerio Público Fiscal: 0800-222-0151 o mpfciudad.gob.ar

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI): denunciasufeci@mpf.gov.ar – Sarmiento 663, CABA.

Línea 137: atención gratuita víctimas de violencia familiar y sexual (24 hs).

Línea 102: atención gratuita y confidencial para niñas, niños y adolescentes.

Emergencias: 911

Denunciar no solo permite sancionar a los responsables, sino también proteger a otras personas y evitar nuevas víctimas.

10. Recomendaciones para toda la familia y la comunidad

- **Educar en ciudadanía digital.** Enseñar a reconocer riesgos, respetar la privacidad y actuar responsablemente en línea.
- **Mantener actualizados** los dispositivos y antivirus.
- **Usar contraseñas seguras** y únicas para cada cuenta.
- **Fomentar el diálogo entre adultos, jóvenes y niños** sobre el uso responsable de la tecnología.
- **Desconfiar de ofertas demasiado buenas**, mensajes alarmantes o solicitudes de dinero.
- **Participar en campañas y espacios de concientización sobre ciberseguridad.**

11. Recordemos

La seguridad digital no depende solo de la tecnología, sino del uso responsable, informado y consciente que hacemos con ella. Cuidar nuestra identidad digital, enseñar a las nuevas generaciones, verificar la información y denunciar los delitos son pasos fundamentales para construir comunidades seguras en entornos digitales.

Prevenir es proteger. La información, la educación y la comunicación son las herramientas más poderosas para enfrentar los ciberdelitos y fortalecer una cultura de seguridad digital basada en el respeto, la solidaridad y la responsabilidad.

Contactos y canales de denuncia

Ministerio Público Fiscal: 0800-222-0151 |
UFECI: denunciasufeci@mpf.gov.ar |
Línea 137 | Línea 102 | Emergencias: 911

Ministerio
de Seguridad