CIBERSEGURIDAD

Ingeniería Sin Fronteras

PRESENTACIÓN

En la actualidad las personas dependen de un dispositivo electrónico para realizar **muchas tareas cotidianas**, pero qué sucede con la seguridad para llevar a cabo a estas labores.

Seguro que has escuchado hablar de ciberseguridad como el proceso de protegerse ante ataques de *hackers* que suplantan la identidad de empresas o personas para sustraer sus datos, pues en **esta guía te presentamos algo más de lo que se puede entender como seguridad informática**.

En las siguientes paginas encontrar información acerca de la ciberseguridad clásica, centrada en los ataques o robo de datos que pueden sufrir los sistemas informáticos, también te introducirá en temas como el phishing, los bulos, la sextorsión como **prácticas frecuentes que vulneran tus derechos digitales.**

Por otro lado, se presentarán **buenas prácticas** que se puedes realizar para intentar protegerte de cualquiera de estas prácticas maliciosas.

También se analiza **el papel de los estados** en el fortalecimiento de esta seguridad o la entrega por parte de estos de los datos al oligopolio de tecnológicas que controlan los servicios de almacenamiento o herramientas de ofimática.

Por último, se aborda sobre **el impacto que tiene en la salud y el bienestar digital**, el sufrir este tipo de ataques, o la manipulación de los algoritmos que influyen en la percepción de la realidad, así que como las consecuencias que tiene el uso de la tecnología en los menores.

ÍNDICE

CIBERSEGURIDAD CLÁSICA

ATAQUES Y ROBO DE DATOS

CIBERSEGURIDAD CLÁSICA

ATAQUES Y ROBO DE DATOS

MALWARE

Usamos la palabra *malware* para designar aplicaciones que realizan **acciones ilegítimas, dañinas y normalmente ocultas.** A veces el término virus se usa indistintamente como sinónimo de *malware*.

Podemos clasificarlos según su forma de propagarse:

VIRUS: Añaden su código a archivos legítimos

GUSANOS: Se replican como archivos independientes, sin necesidad de archivo huésped

CABALLOS DE TROYA: Se hacen pasar por software legítimo para realizar una función oculta.

Y también según la acción maliciosa que llevan a cabo:

Spyware: Roban información relevante

Adware: Generan publicidad no solicitada

Ransomware: Bloquean un dispositivo y piden un rescate

Puertas traseras / rootkits: Controlan remotamente un dispositivo

BUENAS PRÁCTICAS

Instala el software solo de fuentes de confianza

Mantén el sistema operativo actualizado

En sistemas Windows, ten activo y actualizado el antivirus del sistema (Microsoft Defender)

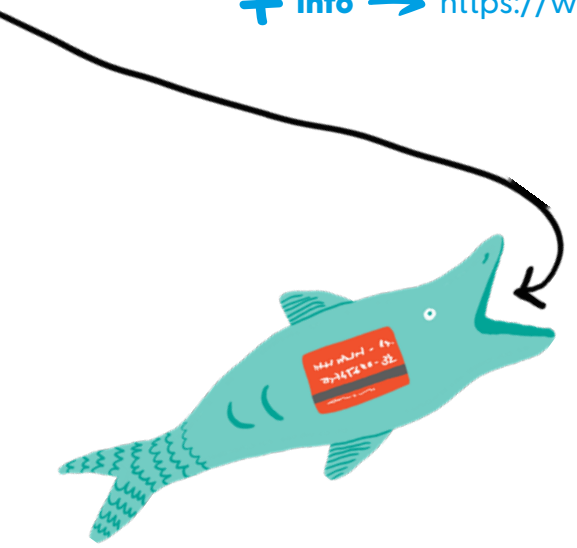
BULOS Y PHISHING

Los **bulos electrónicos**, a veces nombrados como *hoaxes* y otras veces como bulos, sin más, son **falsedades difundidas deliberadamente para crear expectación, miedo, manipular comportamientos, generar opinión o preparar el contexto para acontecimientos posteriores**, entre otras finalidades.

No son más que una versión electrónica de los bulos tradicionales, pero han cobrado gran protagonismo con el auge de las redes sociales y la mensajería instantánea.

Los bulos con formato pseudoperiodístico que tratan de pasar por noticias reales son conocidos como **noticias falsas o fake news**.

+ info → https://www.incibe.es/aprendeciberseguridad/hoax-bulo



Por otro lado, el **phishing** es un caso particular de bulo electrónico con la finalidad de robar credenciales para obtener acceso fraudulento a un servicio. Es un término derivado de la palabra inglesa *fishing* (pesca). Y como la pesca, consiste en **utilizar un cebo o señuelo para conseguir una presa**, que normalmente son credenciales de acceso a algún servicio por internet.

- Un ejemplo típico de phishing es suplantar la página de un banco (este sería el cebo) para conseguir una contraseña de acceso (la presa). Esto se puede extender a cualquier práctica orientada a robar credenciales de acceso usando una suplantación.

El phishing se puede realizar **a través de una página web, de un correo electrónico, de una red social, de mensajería instantánea (Whatsapp o Telegram),** etc. En realidad, por cualquier medio, y normalmente se realiza con una combinación de éstos.

- El caso más común es recibir un correo electrónico que suplanta a tu banco, tu proveedor de correo, etc., con un enlace a una página web que imita la página donde introduces tus credenciales.
- También podría denominarse phishing la **suplantación de dispositivos físicos**, como por ejemplo las alteraciones en cajeros automáticos colocando lectores de tarjeta y teclados superpuestos para captar la información de usuarias y usuarios.
- Un ejemplo muy popularizado de combinación ataques son los correos cadena (bulo), que buscan reenvíos sucesivos encadenados, para ir recolectando en el cuerpo del mensaje direcciones de correo electrónico. Estas direcciones luego se usan para enviar spam o realizar ciberataques de phishing. (INCIBE)

La popularización de la Inteligencia Artificial (IA) ha traído nuevas formas de atacar y suplantar, como el phishing con chatbots maliciosos para extraer información, o los llamados *deepfakes*. **Bulos realizados con IA generativa** (IAg) que **suplantan la imagen real o la voz de personas conocidas** con fines manipulativos.

BUENAS PRÁCTICAS

Comprueba en la barra de direcciones que la dirección a la que accedes es la correcta.

Ante la duda, accede directamente a la web que necesitas usar, no desde un enlace recibido.

SEXTORSIÓN

La **sextorsión** es una forma de extorsión a través de medios electrónicos, en la que se **amenaza con difundir contenido sexual** de la víctima. El contenido ha podido ser obtenido mediante *malware* o manipulación de la cámara web en páginas pornográficas, que actúan como señuelo, o bien a través de conversaciones ilegítimas por mensajería instantánea.

Normalmente, cuando es un ataque organizado, **persigue fines lucrativos** (pago de rescate bajo amenaza de difundir contenido sexual) y se puede acompañar de phishing para **robo de credenciales de redes sociales** y **acceso a contactos cercanos** a quienes difundir.

En otros casos se realiza de forma individual y representa una forma de **violencia, acoso y manipulación sexual**, pues se persigue extorsionar a la víctima para que siga enviando contenido o acceda a tener contacto o comportamiento sexual o íntimo. (INCIBE)

BUENAS PRÁCTICAS

No compartas contenido sexual o íntimo digitalmente.

Si usan este tipo de ataque, antes de tomar ninguna decisión contacta con el INCIBE (017)

No pagues el rescate ni respondas a las amenazas: el pago no detiene la extorsión, la alimenta.

Guarda las pruebas (capturas, perfiles, mensajes, cuentas de pago) antes de bloquear a la otra persona.

CIBERSEGURIDAD CRÍTICA

¿QUIÉN NOS PROTEGE DE GOBIERNOS Y MULTINACIONALES?

CIBERSEGURIDAD CRÍTICA
¿QUIÉN NOS PROTEGE DE GOBIERNOS Y MULTINACIONALES?

El enfoque hegemónico de la ciberseguridad se basa en **protegernos de ataques delictivos.** Si bien esta visión es parcialmente cierta, peca de simplista y reduccionista, y responde a una retórica de **"buena y mala gente"**, de **"policías y ladrones".**

La realidad, desde una mirada más amplia, está sujeta a **factores mucho más complejos:**

- La industria digital opera como un oligopolio, que a veces es referido como **Big Five, o GAFAM (Google, Amazon, Facebook, Apple y Microsoft)**
- Lejos de actuar únicamente como protectores, estas multinacionales perpetran sistemáticamente **ataques a nuestra privacidad** y seguridad, además de a nuestra salud y bienestar digital.
- Frecuentemente existe **connivencia entre gobiernos y multinacionales,** cuando no coacciones directas. Se legisla en favor del oligopolio y las leyes proteccionistas se ven reducidas en numerosas ocasiones a medidas meramente cosméticas.
- Este enfoque simplista de la ciberseguridad desvía la atención de la verdadera realidad, hasta el punto de que, en ocasiones, estas acciones monopolísticas y de control son **justificadas y disfrazadas como medidas de seguridad** ante ataques.

La ciberseguridad no es sólo problema técnico de cortafuegos y antivirus que nos protegen de hackers prodigiosos encerrados en su habitación o de redes mafiosas. Es también un **desafío sociopolítico** en el que las personas, además de víctimas, somos un activo central, consciente y crítico, a la vez que garantes de nuestra propia privacidad, seguridad, salud y bienestar digital.

MALAS PRAXIS

Pasamos ahora detallar un poco más aquellas **prácticas llevadas a cabo por multinacionales o gobiernos que representan ataques digitales contra las personas.** Todas ellas son comunes en internet, y se dan en servicios que usamos de manera cotidiana.

SILOS DE DATOS

Se usa para provocar que las personas **perdamos la noción y el control de los datos que compartimos.** La idea es que nuestros datos se almacenen, aparentemente, como el grano en un silo: en un espacio enorme, y sin mecanismos eficientes para encontrar algo ya almacenado. Esto se lleva a cabo al diseñar el servicio: una interfaz muy simple y fácil de manejar pero que no representa una metáfora fiel o intuitiva de la información que tenemos almacenada.

Sin embargo, del lado del proveedor, la información se analiza e indexa de forma muy exhaustiva para crear categorías con interés comercial, ideológico, etc., **para ofrecerlas a terceras partes (gobiernos u otras empresas).**

BUENAS PRÁCTICAS

Utiliza servicios con espacio limitado. Es más ecológico, y el tener que hacer limpieza te ayudará a tener la noción de los datos que tienes almacenados.

No almacenes tus datos solamente en un servicio que siga estas prácticas. Archiva tus fotos, noticias, etc. en servicios libres y de fácil acceso a tu información.

EL PRODUCTO ERES TÚ

Cuando nos ofrecen **servicios como gratuitos** nos están ofreciendo una **visión distorsionada de la transacción,** en la que las personas ocupamos el lugar de prestatarias del servicio. Es decir, recibimos un servicio de un proveedor a coste cero.

Esta visión pone de manifiesto una sospecha: **¿qué gana el proveedor?**

La realidad es que hay dos transacciones:

1. El proveedor, al prestarnos el servicio, recopila nuestros datos. Recibimos el servicio, pero no de manera gratuita: **pagamos con nuestros datos.**
2. **El proveedor vende nuestros datos** a otras empresas, o los usa con otros fines lucrativos, para prestar otro servicio. En esta segunda transacción, ocupamos el lugar de producto.

Los datos también pueden ser **cedidos a gobiernos** para control poblacional, a cambio de dinero o de la obtención de legislación favorable.

BUENAS PRÁCTICAS

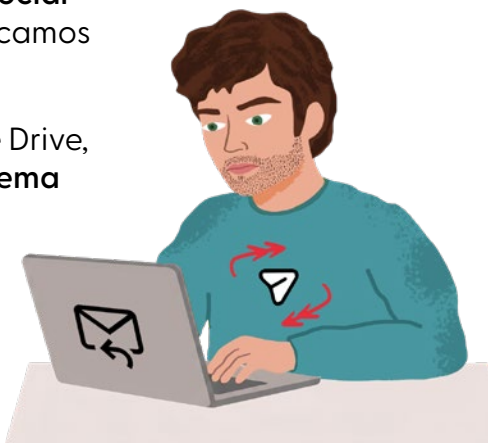
Usa servicios libres, o al menos servicios que no moneticen tus datos.

Cuando un servicio sea imprescindible, revisa qué permisos y qué datos le estás concediendo.

EL COMERCIAL ERES TÚ

Se usa en servicios aislados, y consiste en **utilizar la ingeniería social** para que, al usar el servicio, hagamos de comerciales y lo ofrezcamos a otras personas.

- Por ejemplo, al tratar de compartir un archivo desde Google Drive, nos pide una dirección de correo. **Se nos hace ver que el sistema no es aislado,** generándonos la sensación de que podemos compartir fuera de Gmail.



Sin embargo, el sistema es aislado. Lo que hace con las direcciones externas a Gmail es enviarles un correo ofreciéndoles crear una cuenta de Gmail para verlo. Lo cual es una recopilación de datos encubierta e ilegítima.

BUENAS PRÁCTICAS

Comparte siempre por enlace, para no obligar a la persona destinataria de tu contenido a usar el mismo servicio que tú.

EFECTO CASINO

Consiste en la incorporación de principios de los juegos de azar en el diseño de las aplicaciones digitales, con el objetivo de **aumentar el tiempo en el dispositivo**. Esto se consigue generando un estado de trance en el que se produce una disociación de las señales naturales que nos indicarían cuando detenernos.

Esto se consigue, sobre todo, a través del **refuerzo intermitente:** Consiste en generar una acción repetitiva (como la palanca de las tragaperras) y asociar a ésta recompensas de manera inconstante y esporádica, generando una **esperanza indefinida en la próxima recompensa.**

Algunos ejemplos:

Servicio digital	Acción repetitiva	Refuerzo
Videos cortos	Desplazar hacia arriba	Contenido interesante
Aplicaciones de citas	Desplazar hacia izquierda o derecha	Match
Chatbots de IA	Preguntar	Respuesta relevante que resuelve el problema
Juegos de simulación social	Generar una rutina diaria (recolección, conversión económica, reinversión)	Objetos que se compran para el avatar, que mejoran la infraestructura, etc.
Mensajería instantánea	Volver a mirar el móvil	Alguien me ha hablado
Redes sociales	Volver a consultarlas	He recibido likes.

Otra forma de retención en pantalla es **fomentar el comportamiento multitarea,** con cambios constantes de contexto, lo que retrasa la saturación de realizar una misma acción durante mucho tiempo.

BUENAS PRÁCTICAS

Desactiva las notificaciones innecesarias.

Prioriza la comunicación presencial a la digital.

Establece horarios o tiempo máximo de uso de servicios digitales.

AGENDA SETTING 2.0

El “establecimiento deliberado de agenda”, es una práctica sutil de los medios de masas que consiste en favorecer o visibilizar unos temas, en detrimento de otros que son oscurecidos o censurados para **determinar qué es actualidad y qué no.**

Aplicado a los servicios digitales, y sobre todo a las redes sociales, supone una forma de **vulnerar la neutralidad de la red**, que además es mucho más potente y automatizada que en la prensa. **Los algoritmos definen qué es tendencia,** qué se ve y qué no. Esto coloca a las multinacionales con un **poder descontrolado**, para arruinar reputaciones, popularizar productos o hacer caer gobiernos.

La “agenda setting” también se lleva a cabo “a domicilio”, aplicando los algoritmos **de manera individual**, para decidir qué ve cada persona, y, por tanto, inducir a cierta acción y no otra: compras, opciones políticas, opinión, etc.

BUENAS PRÁCTICAS

Diversifica tus fuentes

Consulta información de servicios que no dependan de algoritmos

Consulta información en medios que no dependan de multinacionales o poderes fácticos.

EFECTO “POR DEFECTO”

Favorecer un determinado uso o unas determinadas acciones al usar un servicio de internet colocándolas como acciones u opciones de configuración por defecto. Las opciones preseleccionadas o mostradas con más claridad **son estadísticamente más usadas.**

BUENAS PRÁCTICAS

Revisa las opciones por defecto antes de aceptarlas, y elige tus propias configuraciones.

Desconfía cuando rechazar sea mucho más difícil que aceptar: eso indica dónde está el interés del proveedor.

AISLAMIENTO DE SERVICIOS

Evitar que un servicio interactúe con otros similares para hacer valer **la hegemonía en el sector.** De este modo estamos bajo coacción a la hora de elegir servicio, ya que, si elegimos el que no es hegemónico, quedaremos en **incomunicación**.

Si la empresa de telefonía con más clientes decidiera aislarse, estaría coaccionando al resto de personas usuarias para abonarse.

Esto, que en telefonía parece descabellado, **ocurre en mensajería instantánea con WhatsApp (Meta) o Gmail (Google).**

BUENAS PRÁCTICAS

Apuesta por servicios interoperables entre sí frente a servicios cerrados.

OTRAS PRÁCTICAS ABUSIVAS

- **EXPORTACIÓN DE MONOPOLIO:** Aprovechar el monopolio **en un sector de mercado** para ganar una posición monopolística en otro asociado.

- **CONTROL DE LA APLICACIÓN CLIENTE:** No permitir que aplicaciones de terceros se conecten a un servicio, para influir y **controlar las pautas de uso mediante ingeniería social.**

- **MIERDIFICACIÓN: Deterioro deliberado de un servicio para forzar la adquisición de la opción premium,** o acelerar la sustitución por otro servicio que resulta más ventajoso al proveedor. Una parte es deteriorar deliberadamente productos de la competencia, con un buen estudio y control previo de áreas de mercado estratégicas.

CONSECUENCIAS EN LA SALUD Y EL BIENESTAR DIGITAL

Aunque todos los ciberataques tienen consecuencias sobre **nuestra salud física, mental y emocional,** los perpetrados por estamentos de poder (multinacionales y gobiernos) tienen efectos mayores, por diversos motivos:

1. Estos ataques están planificados **desde la fase de diseño** de las aplicaciones y servicios que utilizamos.

2. No solemos tomar medidas para protegernos, ya que habitualmente **no tenemos sensación de estar bajo un ataque o abuso.**

3. Al contrario que con los ciberataques clásicos, que ocurren de manera puntual, la exposición a estos ciberataques **es constante y prolongada en el tiempo.**

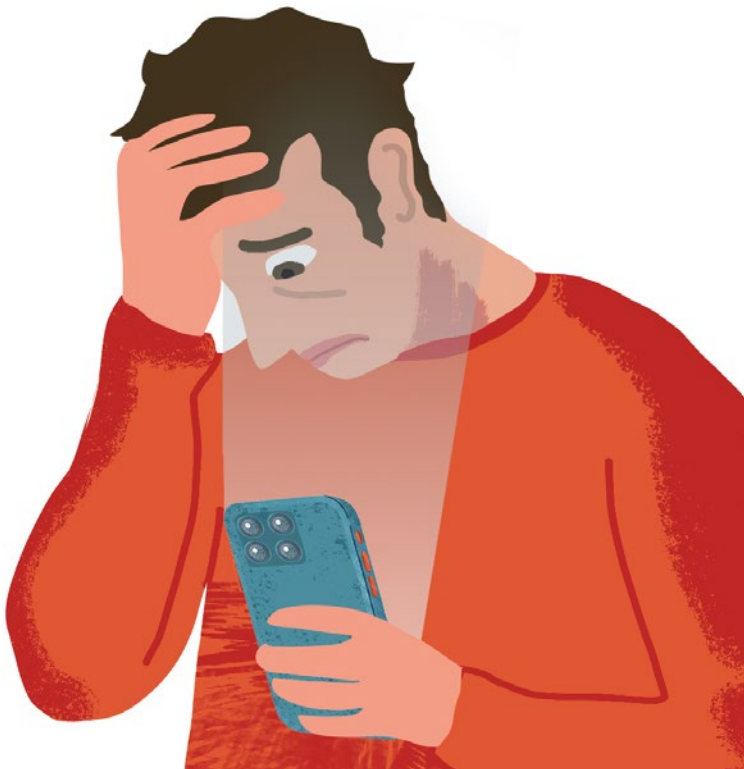
Pasamos a mencionar brevemente **algunos de estos efectos:**

- **Infoxicación:** Conjunto de síntomas relacionados con la exposición continuada a **cantidades de información que exceden las que somos capaces de procesar.** Provoca estrés, ansiedad, dificultad para tomar decisiones, y pérdida de control.

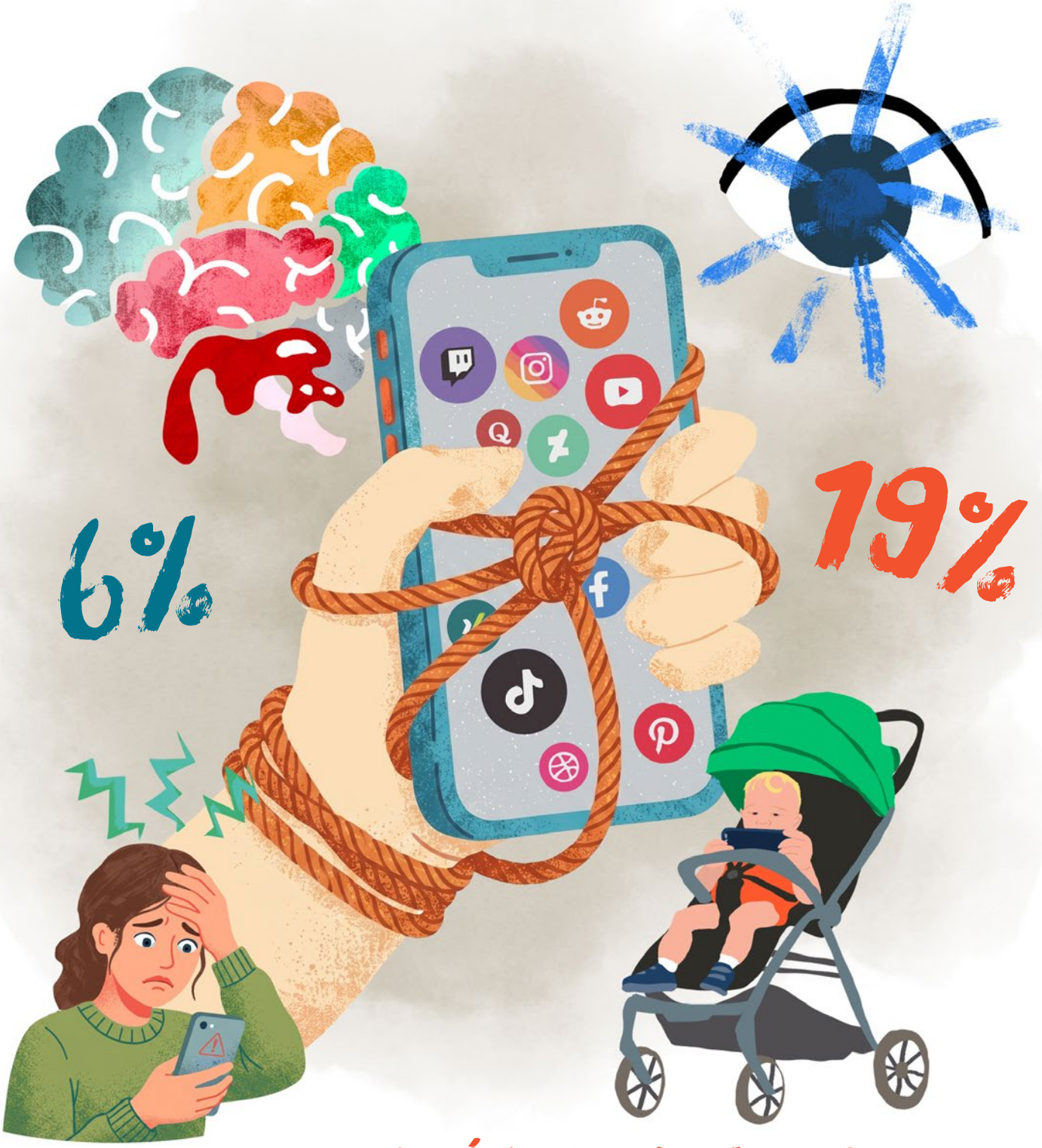
- **Adicción digital: Necesidad compulsiva de conectarse o de mantenerse en línea,** por miedo a perderse algo (FOMO) y reforzada por mecanismos de refuerzo intermitente. Altera los patrones de sueño, las relaciones personales y el rendimiento cognitivo.

- **Otros efectos relevantes:** Existen otros efectos menos centrales pero que también afectan al bienestar digital:

  - **Necesidad de aprobación digital**
  - **Ansiedad por reemplazo**
  - **Comportamiento multitarea**
  - **Reducción del tiempo de atención**
  - **Deterioro de la memoria**
  - **Dependencia cognitiva**
  - **Sedentarismo**
  - **Cambio de los ciclos circadianos**
  - **Fatiga visual**



INFANCIA Y ADOLESCENCIA



ADICCIÓN DIGITAL TEMPRANA

ADICCIÓN DIGITAL TEMPRANA

Según un **informe de UNICEF de 2025**, **uno de cada diez menores dice sentirse adicto al móvil,** y determinadas conductas problemáticas se dan en porcentajes que van desde el 6% al 19% de las y los menores.

Los **efectos cognitivos**, llevados a la infancia, pueden provocar retrasos en el lenguaje o disminuir la tolerancia a la frustración, entre otras consecuencias. En estado de adicción digital, la tecnología se convierte en la única herramienta de regulación emocional. Además, a mayor uso, mayor vulnerabilidad al ciberacoso, al sexting (envío de mensajes con contenido sexual) o al contacto con depredadores sexuales.

En cuanto a los **efectos físicos**, por citar un ejemplo, el cristalino no puede filtrar la luz azul (hasta los 14 años de edad).

En la adolescencia, una etapa marcada por la búsqueda de identidad y la impulsividad, la **necesidad de aprobación digital** puede ser aún más intensa, y desembocar en ansiedad, depresión, dificultad en la toma de decisiones o deterioro de la autoimagen. Por otro lado, el acceso y el aprendizaje del sexo y la intimidad puede quedar por el acceso ilimitado a la pornografía, modificando de por vida la conducta sexual.

Las consecuencias son mucho más variadas y diversas, y exceden del alcance de esta guía. No obstante, podemos tomar como regla general que cualquier efecto sobre la población adulta **se ve intensificado cuando lo aplicamos a infancia y adolescencia,** al ser estas etapas críticas dentro del proceso madurativo humano.

[+] MÁS INFORMACIÓN

- Antes y después de los smartphones
- Cómo el consumo intensivo de videos cortos y redes sociales afecta la memoria y el autocontrol en niños
- El impacto de las redes sociales
- Cómo la Generación Z está plantando cara al deterioro mental digital (inglés)
- La multitarea digital afecta a la memoria
- Mecanismos neurocognitivos de la atención digital en entornos hiperconectados (inglés)
- Phishing
- Podredumbre mental
- Sobrecarga informativa
- Síndrome FOMO
- Sextorsión

Ingeniería Sin Fronteras

Zaragoza
AYUNTAMIENTO