Guía de Ciberseguridad y Bienestar Digital

CONTENIDO

“Protegernos también es cuidarnos”

INTRODUCCIÓN: VIVIMOS CONECTADOS

Hoy usamos internet para casi todo: hablar con la familia, hacer gestiones, leer noticias o mirar vídeos. Pero igual que cerramos la puerta de casa por seguridad, debemos **cerrar bien la puerta digital**.

“La ciberseguridad no es desconfianza, es sentido común.”

Estar conectados es maravilloso, pero también implica responsabilidad. Aprender a proteger nuestros datos y nuestra identidad digital es esencial para disfrutar de internet sin sustos.

1. ¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad es el conjunto de medidas y hábitos para proteger nuestros dispositivos (móviles, ordenadores, tablets) y nuestra información personal en Internet. Es como tener una alarma en casa, pero en versión digital. No evita todos los problemas, pero reduce mucho los peligros.

Hoy en día, casi todo lo que hacemos pasa por la red: hablar con familiares, hacer la compra, consultar el banco o guardar fotos. Por eso debemos protegernos, especialmente las personas mayores y adolescentes, ya que son el objetivo más frecuente de los estafadores.

“Tu información vale más que el oro. Cuídala.”

2. DELITOS INFORMÁTICOS

Nuestro Código Penal recoge distintos delitos cometidos a través de Internet.

Los delitos informáticos están regulados en el **Código Penal (Ley Orgánica 10/1995, de 23 de noviembre)**:

- **Art. 197:** Acceso a datos o cuentas sin permiso.
- **Art. 248:** Estafas informáticas.
- **Art. 264:** Daños informáticos.
- **Art. 270:** Protección de derechos de autor.

A continuación, se muestra una tabla con diferentes delitos y las leyes que los tipifican:

Delito	Descripción sencilla	Artículos (leyes)
Estafas online	Engañar para que pagues o des datos	Art. 248–251 (Código Penal, Ley Orgánica 10/1995)
Acceso ilegal a cuentas	Robar contraseñas	Art. 197 (Código Penal)
Suplantación de identidad	Hacerse pasar por ti	Art. 401 (Código Penal)
Daño a dispositivos	Virus o bloqueos	Art. 264 (Código Penal)

También nos encontramos protegidos por la **Ley Orgánica 3/2018** y el **Reglamento General de Protección de Datos (RGPD)**.

📍 **Dónde denunciar:**

- Policía Nacional (Brigada de Investigación Tecnológica)
- Guardia Civil (Grupo de Delitos Telemáticos)
- Oficina de Seguridad del Internauta → https://www.osi.es
- INCIBE → https://www.incibe.es

"La denuncia no solo te protege a ti, también protege a los demás."

3. ESTAFAS Y AMENAZAS MÁS COMUNES

📨 **PHISHING:**

Mensajes o correos falsos que parecen venir de bancos o empresas.

Ejemplo: *"Su cuenta ha sido bloqueada. Pulse aquí para verificar sus datos."*
Al hacer clic, los estafadores pueden robar tus contraseñas.

- **Prevención:**
  - No pulses en enlaces sospechosos.
  - Comprueba siempre el remitente.
  - Si tienes dudas, entra tú mismo en la web oficial.

🦠 **VIRUS Y MALWARE**

Programas que se instalan sin permiso y dañan el equipo o roban datos.

Ejemplo real: un jubilado descargó un "limpiador gratuito" y perdió todas sus fotos.

- **Prevención:**
  - Instala un antivirus confiable.
  - Descarga solo de sitios oficiales.
  - Haz copias de seguridad.

"Haz una copia de tus recuerdos antes de que otro los borre."

📱 ESTAFAS POR TELÉFONO O WHATSAPP

A veces los estafadores se hacen pasar por familiares o bancos.

Ejemplo real: Una mujer recibió un mensaje que decía: *"Mamá, soy tu hijo. Cambié de número. Necesito una transferencia urgente."*

No era su hijo. Era un estafador.

- **Prevención:**
  - No transfieras dinero sin confirmar por llamada.
  - No des información personal por WhatsApp.
  - Desconfía de mensajes con prisas o miedo.

🦹 SUPLANTACIÓN DE IDENTIDAD

Usan tu nombre o tus fotos para engañar a otros.

- **Prevención:**
  - Revisa tu configuración de privacidad.
  - No compartas datos personales públicamente.
  - Denuncia las cuentas falsas.

📰 NOTICIAS FALSAS / FAKE NEWS

A veces se comparten noticias inventadas que buscan engañar.

- **Prevención:**
  - Verifica la fuente antes de reenviar.
  - Desconfía de titulares que asustan o enfadan.
  - No difundas si no estás seguro.

"No todo lo que se comparte, merece ser compartido."

También podemos encontrar otro tipo de estafas más concretas como:

Estafa del falso banco: Te llaman diciendo ser del banco y piden claves. Nunca digas datos por teléfono. Denunciar en Policía Nacional.

"Paquete pendiente" / Correos: Un SMS con enlace fraudulento. No pulses enlaces inesperados.

Amor estafa (Romance scams): Personas que enamoran para pedir dinero. Si pide dinero → bloquear.

CASO REAL

Una mujer de 67 años en Valencia **perdió 28.000 €** por un falso militar que decía amarle. ***¡El amor no se compra ni se pide por transferencia!***

4. CÓMO PROTEGERTE PASO A PASO

1. Usa contraseñas seguras y diferentes.
2. No compartas información personal.
3. Desconfía de los mensajes urgentes.
4. Actualiza los programas y antivirus.
5. No te conectes a Wi-Fi públicas sin protección.
6. Haz copias de seguridad.
7. Piensa antes de hacer clic.

Cómo crear contraseñas seguras

- 12 caracteres como mínimo
- Mezclar mayúsculas, números y símbolos
- Nunca datos personales

Ejemplo ✅: Perro!Sol_26NIEVE

Ejemplo ❌: 123456, Nombre+Fecha

También puedes utilizar trucos nemotécnicos como el siguiente:

"Me tomo 2 cafés cada mañana" → MeT2ccM#

"La mejor contraseña es la que nadie puede adivinar… ni tú mismo olvidar."

5. SALUD Y BIENESTAR DIGITAL

Igual de importante que la ciberseguridad es protegernos de la ciberadicción, problemas que cada vez más están apareciendo con síntomas como faltas de atención, insomnio o ansiedad, así como nuestra salud física, pues las posturas y el estar expuesto muchas horas a las pantallas también pueden acarrear problemas musculares o visuales. Así, debemos tener adquirir hábitos para generar un bienestar digital donde nuestra **salud física y mental** no se vean afectadas.

A continuación, se muestran algunos consejos para mejorar nuestro bienestar digital:

Tiempo frente a pantallas

- Descansa cada 45 minutos o una hora.
- Evita usar el móvil antes de dormir.
- No tengas varias pantallas encendidas al mismo tiempo.
- En la medida de lo posible, no utilices pantallas más de 2 horas al día si no trabajas de ello.

Postura y ergonomía

- Espalda recta, pies apoyados.
- Pantalla a la altura de los ojos.
- Luz natural si es posible.

"También hay que cuidar el cuerpo digital."

6. INTELIGENCIA ARTIFICIAL (IA) Y NUEVOS RIESGOS

La **IA** (inteligencia artificial) ya es una realidad encontrándola en infinidad de aplicaciones de nuestros móviles, redes sociales o chats automáticos. En los últimos años se ha convertido en un peligro debido a su mal uso, al crear **vídeos falsos (deepfakes)** o **voces clonadas** para engañar o hacer daño. Por otro lado, también aporta cosas buenas como: ayudar a detectar fraudes, asistentes para personas mayores o facilitar tareas del día a día.

Como todas las tecnologías, al final depende del uso ético que le de cada uno. Por ello, es necesario tomar precauciones ante los posibles delitos que se pueden cometer usando la IA, como: Imágenes falsas (deepfakes), noticias inventadas (desinformación), robots que imitan a familiares para pedir dinero.

Ejemplo real (2025): se detectaron llamadas falsas con voces de familiares pidiendo dinero.

- **Prevención:**
  - No respondas a llamadas sospechosas, aunque reconozcas la voz.
  - No subas audios personales a webs desconocidas.
  - Usa herramientas oficiales y revisa los permisos.

"La inteligencia artificial no tiene corazón, pero tú sí: usa la cabeza."

7. REDES SOCIALES: PRIVACIDAD

Las redes sociales se han convertido en una fuente de información para los delincuentes cibernéticos, pues de ellas adquieren imágenes y datos que nosotros mismos subimos y proporcionamos. Por ello, debemos prestar especial atención a lo que subimos a Internet, además de configurar nuestra privacidad en las mismas, pues si no somos creadores de contenido y queremos subir cosas para nuestros familiares y amigos, exponiéndolos también a ellos, no necesitamos tener un perfil público.

Como podemos prevenir el robo de información:

- No publiques direcciones ni viajes.
- Configura la privacidad en 'Solo amigos'.
- No aceptes a desconocidos.

"Lo que subes… se queda para siempre."

8. QUÉ HACER SI SOY VÍCTIMA DE UN DELITO

Pasos a seguir:

1. Guardar pruebas (capturas, mensajes, números.
2. Bloquear al atacante
3. Denunciar en Policía Nacional o Guardia Civil
4. Llamar a la línea de ayuda: 017 (INCIBE)

"No te sientas culpable: quien comete el delito es el estafador."

9. TEST RÁPIDO: ¿ESTOY SEGURO EN INTERNET?

Marca ✅ o ❌ en cada pregunta:

Pregunta	✅ / ❌
Uso contraseñas distintas	
No doy datos por teléfono	
No abro enlaces sospechosos	
Reviso mi privacidad	
Hago pausas cada 45 min	

10. TABLA RESUMEN DE RECOMENDACIONES

✅ Hacer	❌ No hacer
Verificar mensajes	Pagar por enlaces
Usar antivirus	Confiar en desconocidos
Actualizar equipos	Contraseñas simples
Denunciar estafas	Vergüenza de pedir ayuda

11. REFLEXIÓN FINAL

La ciberseguridad no es un tema solo técnico. Es una forma de **autocuidado digital**.
Proteger nuestros datos, nuestra salud y nuestra tranquilidad es proteger nuestra libertad.

“Tu mejor antivirus eres tú.”