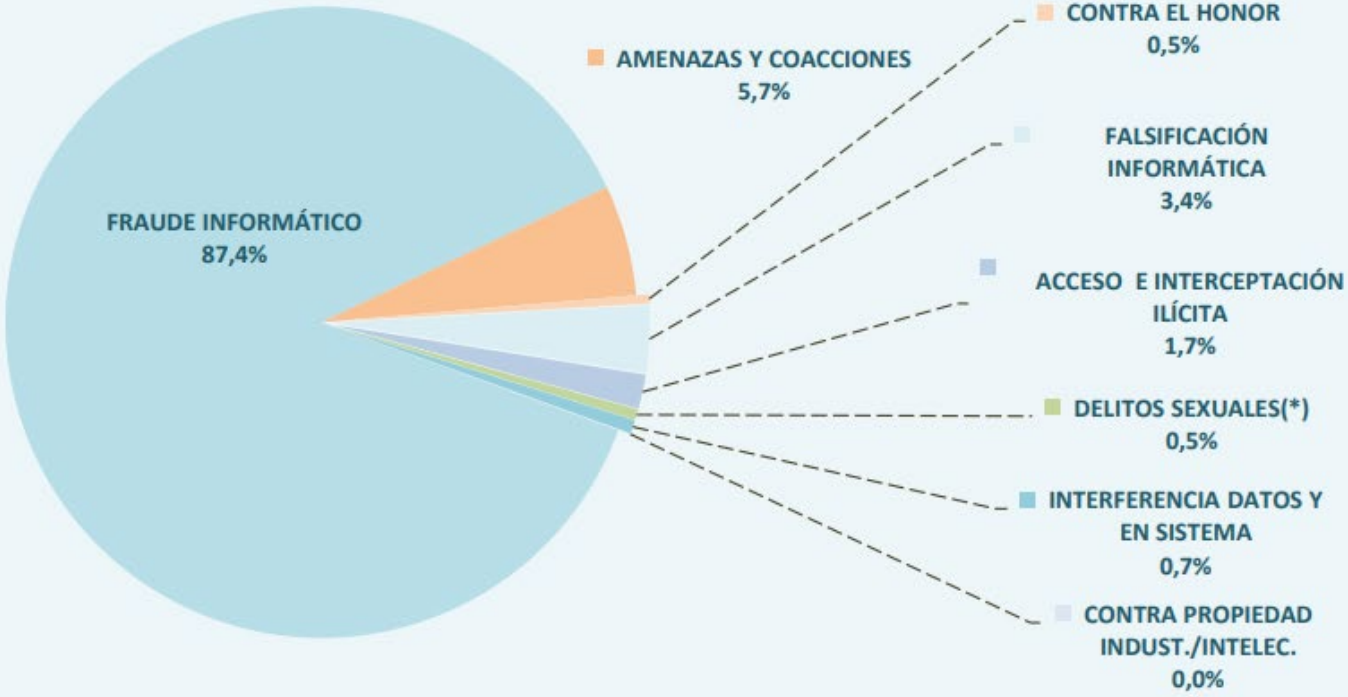
Buenas prácticas para sentirse **seguro** en el entorno digital

Leticia Barrionuevo
buffl@unileon.es
Ext. 1004

https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf

HECHOS CONOCIDOS	2017	2018	2019	2020	2021
ACCESO E INTERCEPTACIÓN ILÍCITA	3.150	3.384	4.004	4.653	5.342
AMENAZAS Y COACCIONES	11.812	12.800	12.782	14.066	17.319
CONTRA EL HONOR	1.561	1.448	1.422	1.550	1.426
CONTRA PROPIEDAD INDUST./INTELEC.	121	232	197	125	137
DELITOS SEXUALES(*)	1.392	1.581	1.774	1.783	1.628
FALSIFICACIÓN INFORMÁTICA	3.280	3.436	4.275	6.289	10.476
FRAUDE INFORMÁTICO	94.792	136.656	192.375	257.907	267.011
INTERFERENCIA DATOS Y EN SISTEMA	1.291	1.192	1.473	1.590	2.138
Total HECHOS CONOCIDOS	**117.399**	**160.729**	**218.302**	**287.963**	**305.477**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



INCIBE gestionó más de 118.000 incidentes de ciberseguridad durante 2022, un 9% más que en 2021

05/04/2023

110.000 corresponden a ciudadanos y a empresas, 546 a operadores estratégicos y 7.980 a la Red Académica.

https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-115000-incidentes-ciberseguridad-durante-2022-9-mas

malware

Hacker

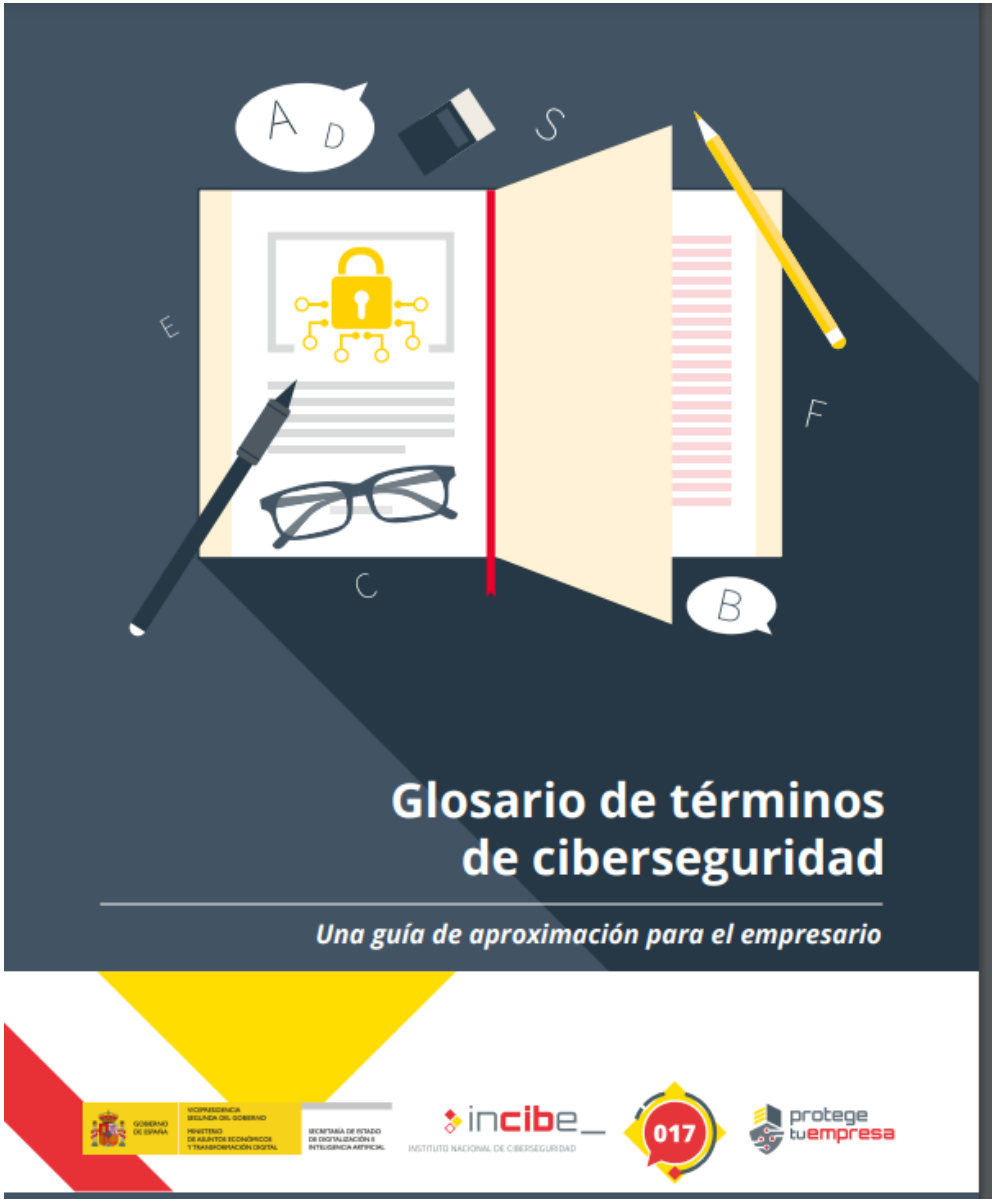
Ciberdelincuente

sniffer

adware

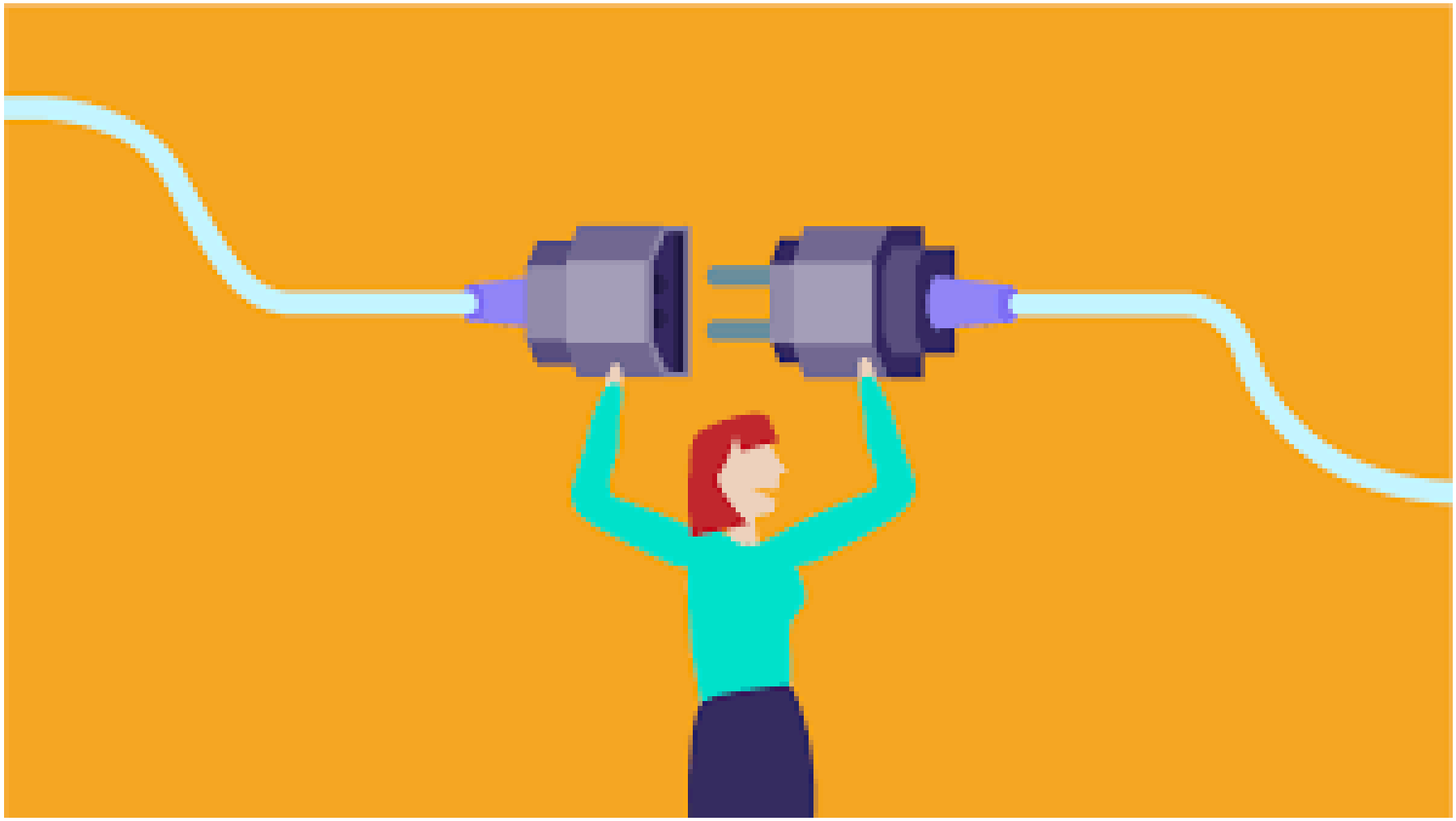
spyware

phishing



https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

BUENAS PRÁCTICAS



HIGIENE DIGITAL

1. Contraseñas

llaves de entrada a nuestra vida digital

¿Es **práctico** tener una única llave para todo?

¿Es **seguro** tener una única llave para todo?

La lista de contraseñas más usadas en España demuestra que a mucha gente le preocupa muy poco su seguridad

3 comentarios

https://www.xatakamovil.com/seguridad/lista-contrasenas-usadas-espana-demuestra-que-a-mucha-gente-le-preocupa-muy-poco-su-seguridad

Contraseñas

- Construyelas **robustas**
- No las compartas
- No las enseñes
- Cámbialas
- Créalas s*encillas* pero *robustas* en aplicaciones y herramientas que utilices de forma puntual; otra *especiales de costosa robustez* para proteger servicios o cuentas de vital importancia

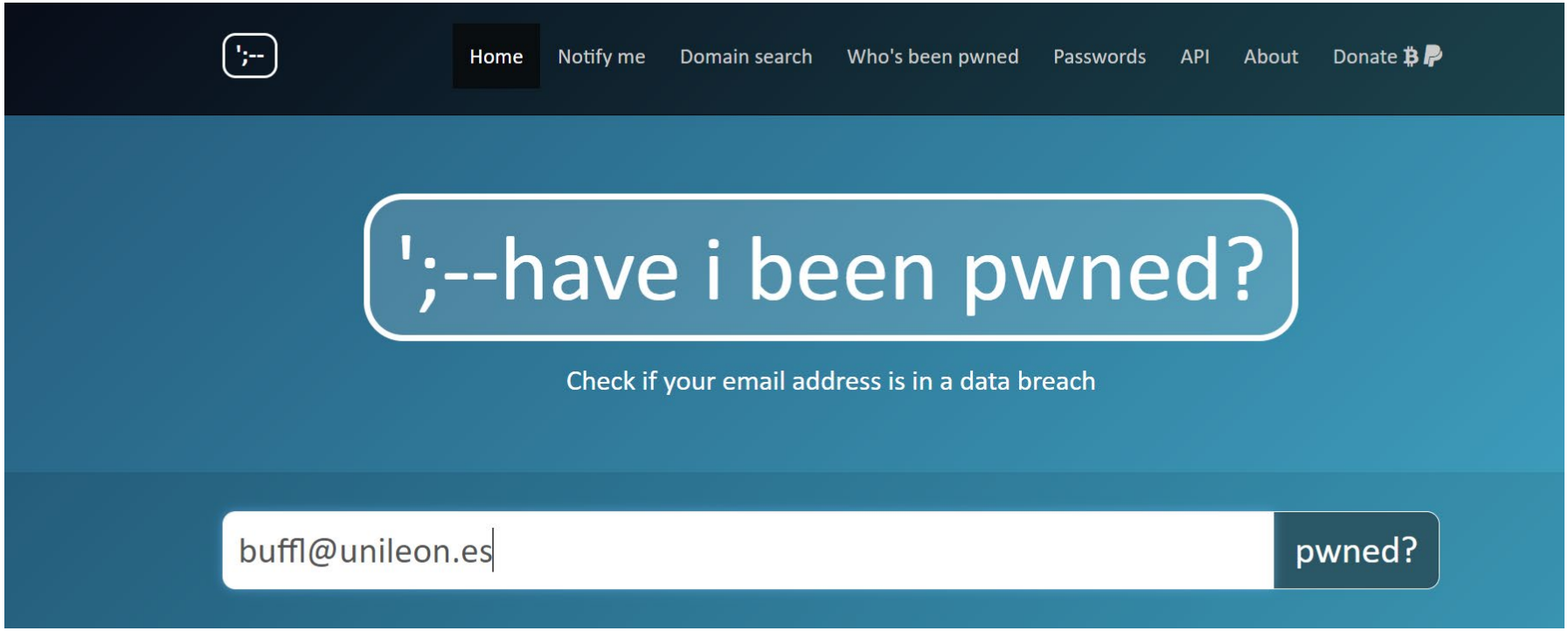
¿Qué significa construir una contraseña robusta?

- **Cuánto más larga mejor**: mínimo de 10-12 caracteres, combinación de letras mayúsculas, minúsculas, números y caracteres especiales
- **No recicles**
- **Evitar incluir elementos fáciles de adivinar**: evitar información personal
- **No incluir letras o números en serie**
- **Evitar cualquier palabra sin alterar** que se encuentre en algún diccionario

Gestores de contraseñas

Te ayudan a crear y almacenar contraseñas

Brecha de seguridad



https://haveibeenpwned.com/

2. Verificación en 2 pasos

Sistema de autenticación reforzada. Se precisa algo más que el usuario y contraseña para acceder

- **Algo que sé**: contraseñas, preguntas de seguridad, código pin etc.
- **Algo que tengo**: dispositivo móvil, tarjeta física de acceso personal, código QR, etc.
- **Algo que eres**: escaneo de datos biométricos como huellas dactilar, iris, retina, reconocimiento de voz, etc.

2FA: Two-Factor-Authentication: generalmente se combinan dos métodos para configurar la capa extra de seguridad

Sistema de autenticación reforzada

Servicios de email, redes sociales, plataformas de videojuegos, sistemas de mensajería, servicios de almacenamiento en la nube, etc. permiten activar este sistema reforzado

Configuración de la cuenta – Seguridad – Verificación en dos pasos

Sistema de autenticación reforzada

Código ICC: código único que identifica la SIM
Código IMEI: matrícula del teléfono móvil

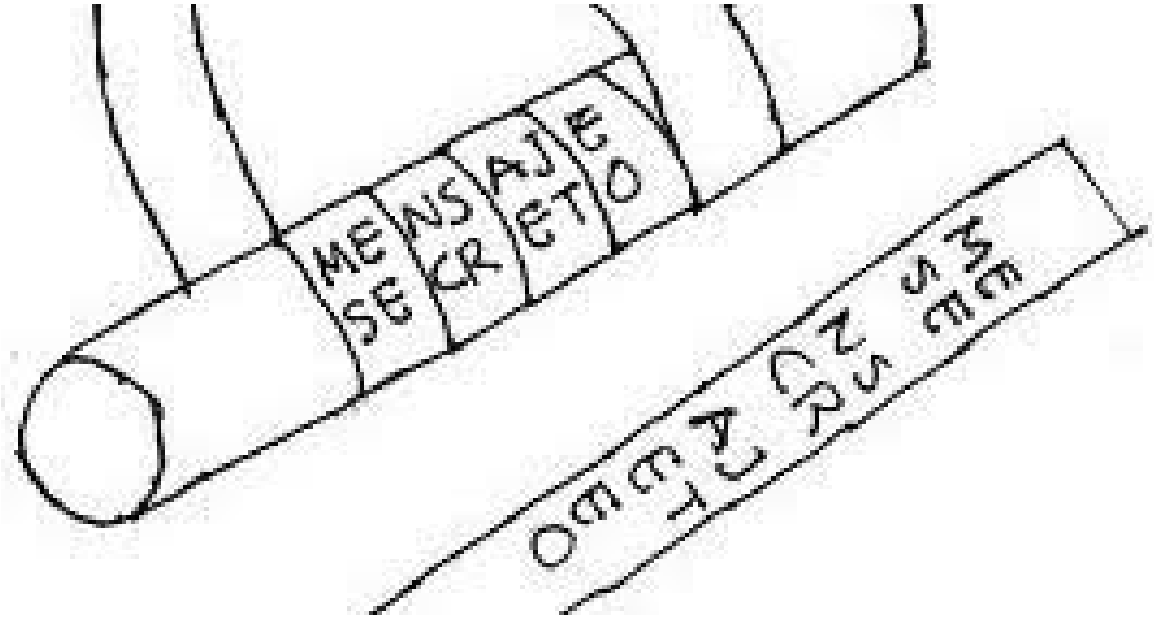
3. Copias de seguridad

Realizar copias de seguridad de documentos en los formatos que sean (texto, vídeos, fotografías, páginas web, bases de datos, etc.) en lugares diferentes al original. Si hay más de una copia, ¡mejor!

Copias de seguridad

¿Trastero?

4. C1fr4da0



Técnica basada en complejos algoritmos matemáticos utilizado para la seguridad de los datos. Para desvelar el contenido hace falta una clave de cifrado. **IMPORTANTE**: cifrar información más relevante

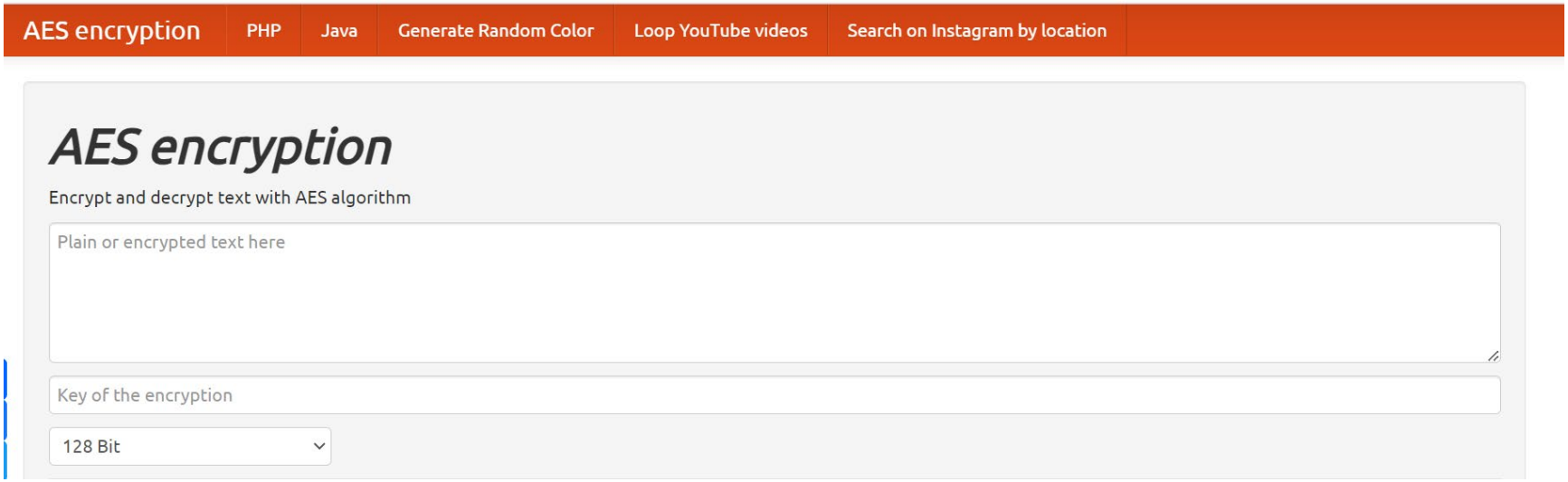
C1fr4da0

VeraCrypt

SecurStick

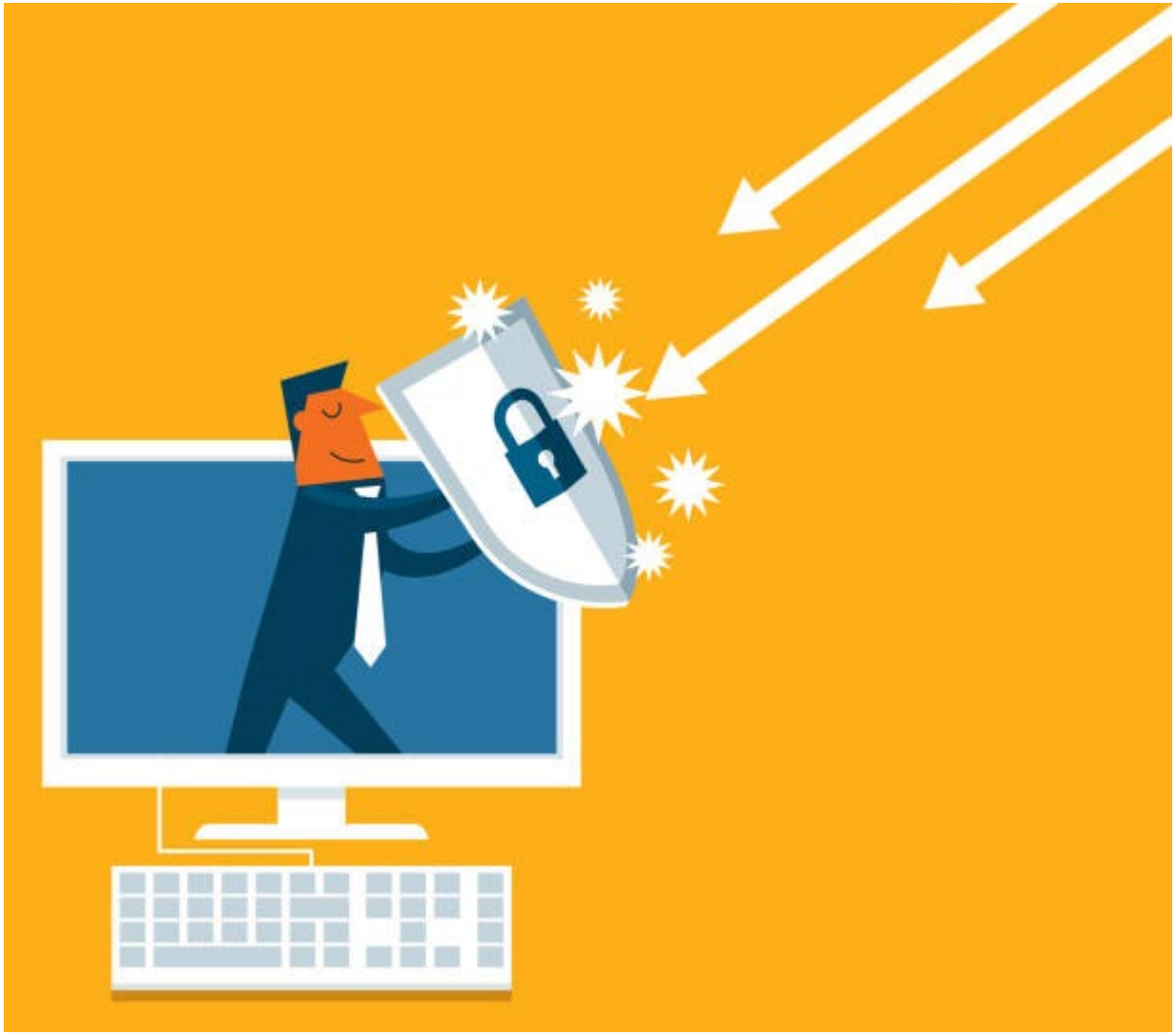
boxcryptor

C1fr4da0



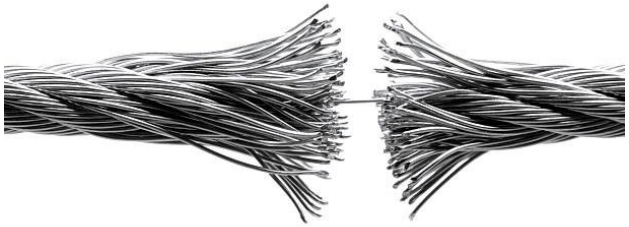
https://aesencryption.net/

5. Antivirus



Antivirus

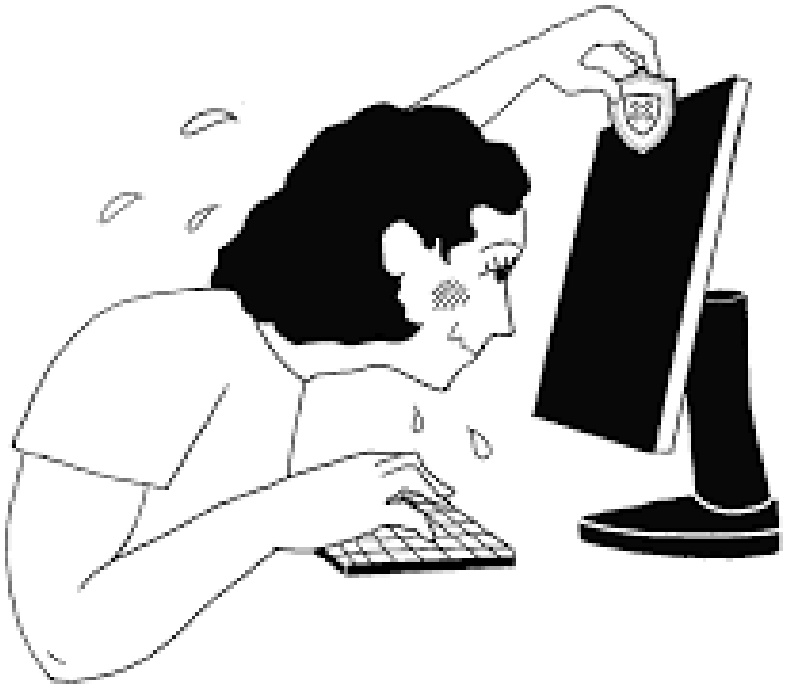
Los virus o malwares, hoy en día, no son la mayor amenaza pero **AÚN ESTÁN PRESENTES**



- Relentizan
- Interrumpen el uso de programas
- Interfieren navegación
- Falsos positivos en exceso

SE ACONSEJA SU USO en ordenadores, tabletas, teléfonos, Smart TV

6. Tapar cámaras



El *camfecting* es la práctica de tomar el control de la cámara de un dispositivo sin permiso del propietario (hoy en día más en auge por el aumento de videollamadas y teletrabajo)

7. Murallas al router

- En España, el robo de wifi es un delito penado con multa de más de 400 euros

- **IMPORTANTE**: configurar el router adoptando una serie de medidas de protección desde el panel de configuración. Por lo menos, las opciones básicas

Murallas al router

¿Qué debemos configurar?

- **Cambiar** el nombre de la red y la contraseña, lo que viene de serie no sirve. Suele coincidir con la compañía contratada. Sé creativo a la hora de dar nombre. Contraseña larga y robusta.
- Mantener actualizado el **firmware** del router.
- Tener activado mínimo un **cifrado** WPA2 y si lo admite WPA3
- Desactivar el sistema llamado **WPS** que es el que permite emparejar dispositivos
- Comprobar el listado de **equipos conectados** a la red inalámbrica de forma periódica. Eliminar los que nos estén autorizados.
- **Reiniciar** el router de vez en cuando.
- Crear una red **wifi de invitados** (acceso limitado a red doméstica) para que puedan acceder tus invitados

https://www.incibe.es/ciudadania/formacion/guias/guia-para-configurar-el-router-wifi

8. USB en el bolsillo

9. Borrado seguro y formateo

1. **RECUPERAR** todos los datos que queremos conservar: archivos, fotos, vídeos, agenda de contactos, descargas, etc.

2. **FORMATEAR**, más de una vez, el dispositivo, sobrescribiendo la información con datos vacíos.

3. **RESTAURAR** el dispositivo a los valores de fábrica

Borrado seguro y formateo

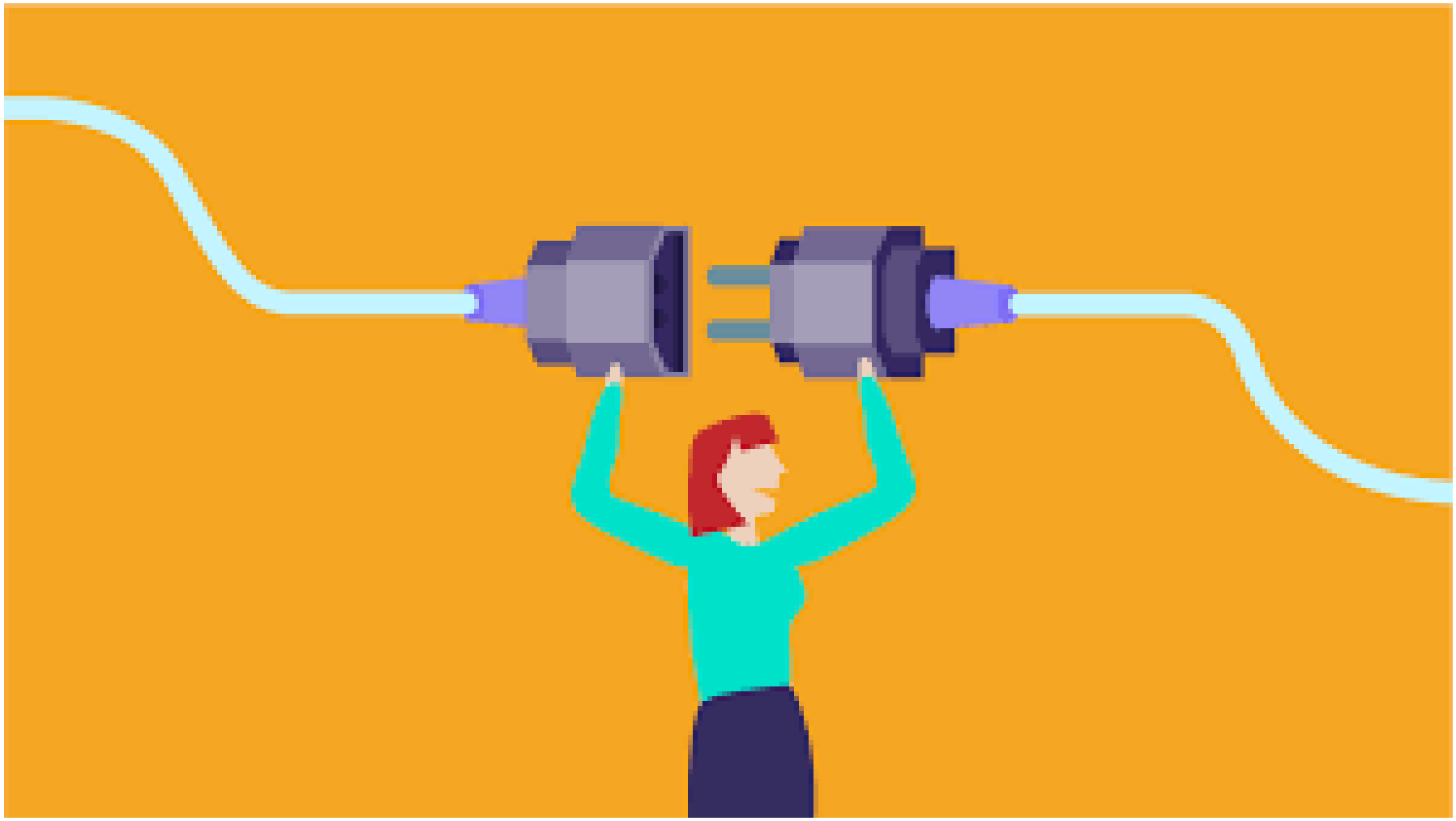
DBAN

CCLEANER

Borrado seguro y formateo

10. Documentación personal

OTROS CONSEJOS



HIGIENE DIGITAL

- **Banners publicitarios** que simulan ofertas o botones que llevan a formularios

Mantener actualizados los dispositivos, software, navegadores, antivirus, además de la llamada *incontinencia cliquera*

- **Fraudes con tarjetas de crédito o débito**

Utilizar tarjetas prepago, cibertarjetas o pagos seguros como PayPal

- **Timo en llamadas telefónicas y SMS**

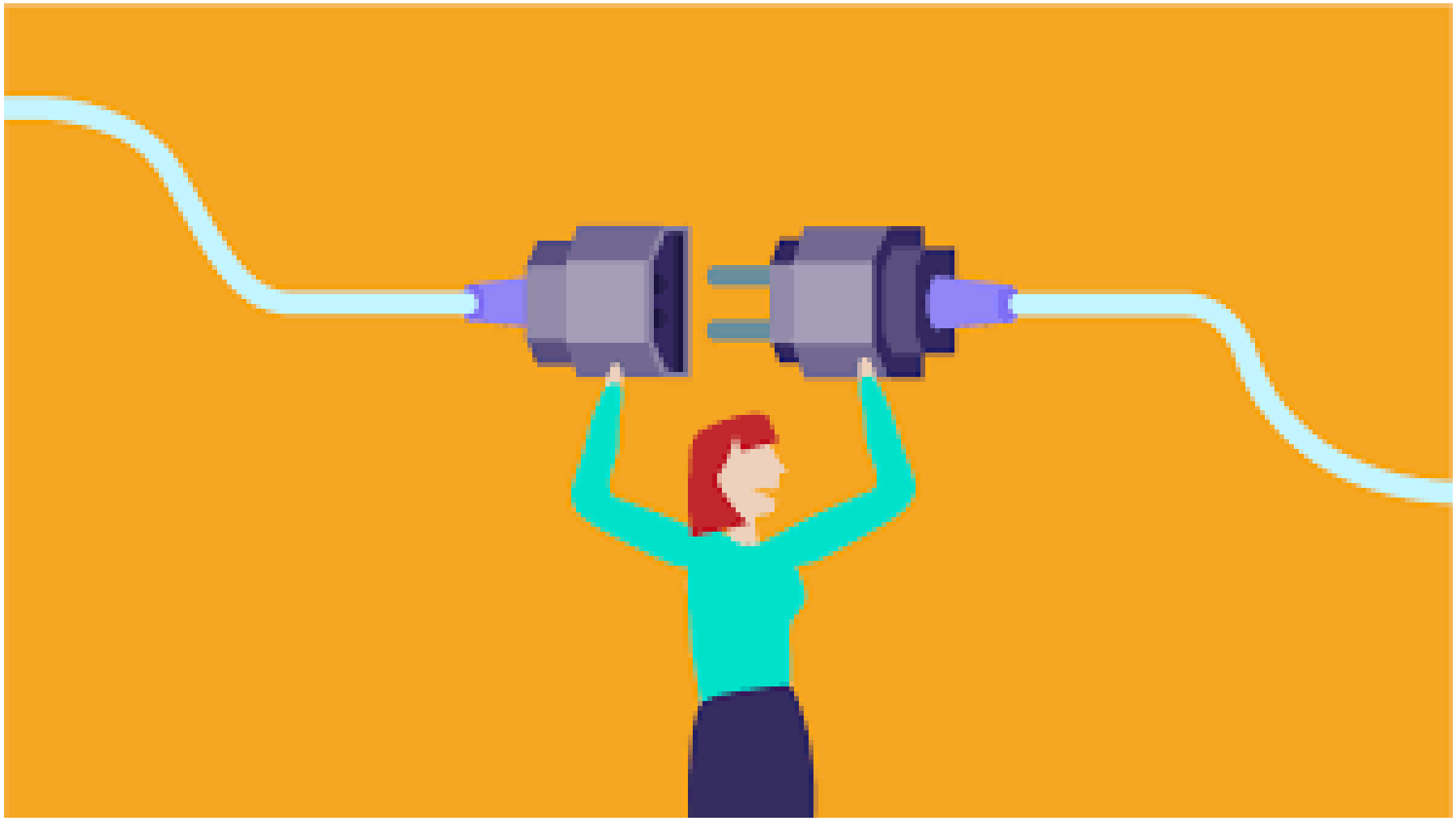
No hacer caso, bloquear

- **Phishing** o suplantación de identidad

Ver si hay algo extraño en el correo del remitente, en el asunto, archivos, enlaces

https://phishingquiz.withgoogle.com/?hl=es

10 CONSEJOS básicos



identidad DIGITAL

1. Cuida el perfil de redes sociales, aportan más información de la que piensas y conforman tu identidad digital.
2. Controla el contenido que publicas
3. Publicar demasiada información en redes tuya o de terceros supone un riesgo, sobre todo si se exponen a menores de edad
4. Se prevenido ante lo desconocido
5. Proteger el acceso a cuentas a través de la configuración adecuada de cada red
6. Ver si está activada la geolocalización de los perfiles. No es adecuado dar información sobre la ubicación a tiempo real.
7. Comprobar los ajustes de seguridad y privacidad
8. El respeto SIEMPRE
9. Cuida y protege las relaciones en internet como en la vida analógica
10. Recordar que en Internet nosotros mismos somos la primera línea de defensa para protegernos

Leticia Barrionuevo
buffl@unileon.es
Ext. 1004

Las fotos utilizadas han sido extraídas de Google Imágenes