



ACTIVIDADES DEL MÓDULO DEFENSA



F-74 "Asturias" v1.2 (2025). Campus Tecnológico - Deportivo

© José Manuel Redondo López. Universidad de Oviedo



Contenido

	Ejercicios de Defensa	7
	AVISO IMPORTANTE: Unas palabras antes de empezar.....	7
	Aspectos Relativos a las Personas.....	8
	Autenticación	8
	Ejercicio PROTONPASS: Probar fortaleza de contraseñas y también ProtonPass	8
	Ejercicio 2FA: Experimentar con un 2FA.....	14
	Computación "sensata"	17
	Ejercicio MALDITOBULO: Visitar "Maldito Bulo"	17
	Ejercicio ACOSO: Consulta la información contra el acoso que está publicada en Internet para ti o para tu familia	20
	Uso de Internet.....	24
	Usando el navegador de forma segura	24
	Ejercicio UBLOCK: Instalar un bloqueador de publicidad	24
	Ejercicio MALTESTWEB: Mirar si una web es o no maliciosa.....	31
	Uso de Redes Sociales	33
	Ejercicio RRSSCONF: Configura bien tus cuentas de RRSS	33
	Ejercicio RRSS_RESPORT: Reportar a alguien en una red social.....	35
	Uso de Sistemas de Mensajería.....	42
	Email.....	42
	Ejercicio CONSEJOS_ADJUNTOS: Mirar los consejos para defenderte de emails chungos.....	42
	Ejercicio PHISHREPORT: Usar las páginas que reportan phishing.....	44
	Aplicaciones de Mensajería	46
	Ejercicio WHATSCONF: Mirar algunas configuraciones típicas de WhatsApp a ver como las tienes	46
	Ejercicio PWDCHAT: Protege un chat con clave	52
	Dispositivos de Computación.....	54
	Telefonía Móvil.....	54
	Ejercicio MOVILCONF: Consultar lo que tiene el INCIBE para configurar tu móvil bien	54
	Ejercicio PLAYSTORE_OK: Mirar alguna aplicación con buena pinta en la Play Store	56
	Ordenadores.....	59
	Ejercicio WINDEF: Sácale partido al Windows Defender	59
	Ejercicio VIRUSTOTAL: Analizar algo con Virustotal	60



📡 Hardware y Redes	62
📶 Redes de Comunicaciones	62
🔗 Ejercicio NextDNS: Probar NextDNS	62
🔗 Ejercicio WAYBACK: Ver una página “en el pasado”	65
⌚ Dispositivos “Smart”	70
🔗 Ejercicio TRUSTPILOT: Probar TrustPilot	70
🔗 Ejercicio EOL: Mirar cuando te “caduca” el móvil	72
🏃 Seguridad “En el Mundo Real”	74
📍 Seguridad “Física”	74
🔗 Ejercicio FALSACAM: Buscar modelos de cámaras falsas	74
🔗 Ejercicio FARADAY: Buscar fundas de Faraday a la venta	75
💰 Seguridad Financiera	76
🔗 Ejercicio TARJETAMON: Buscar ofertas de tarjetas monedero en algún banco	76

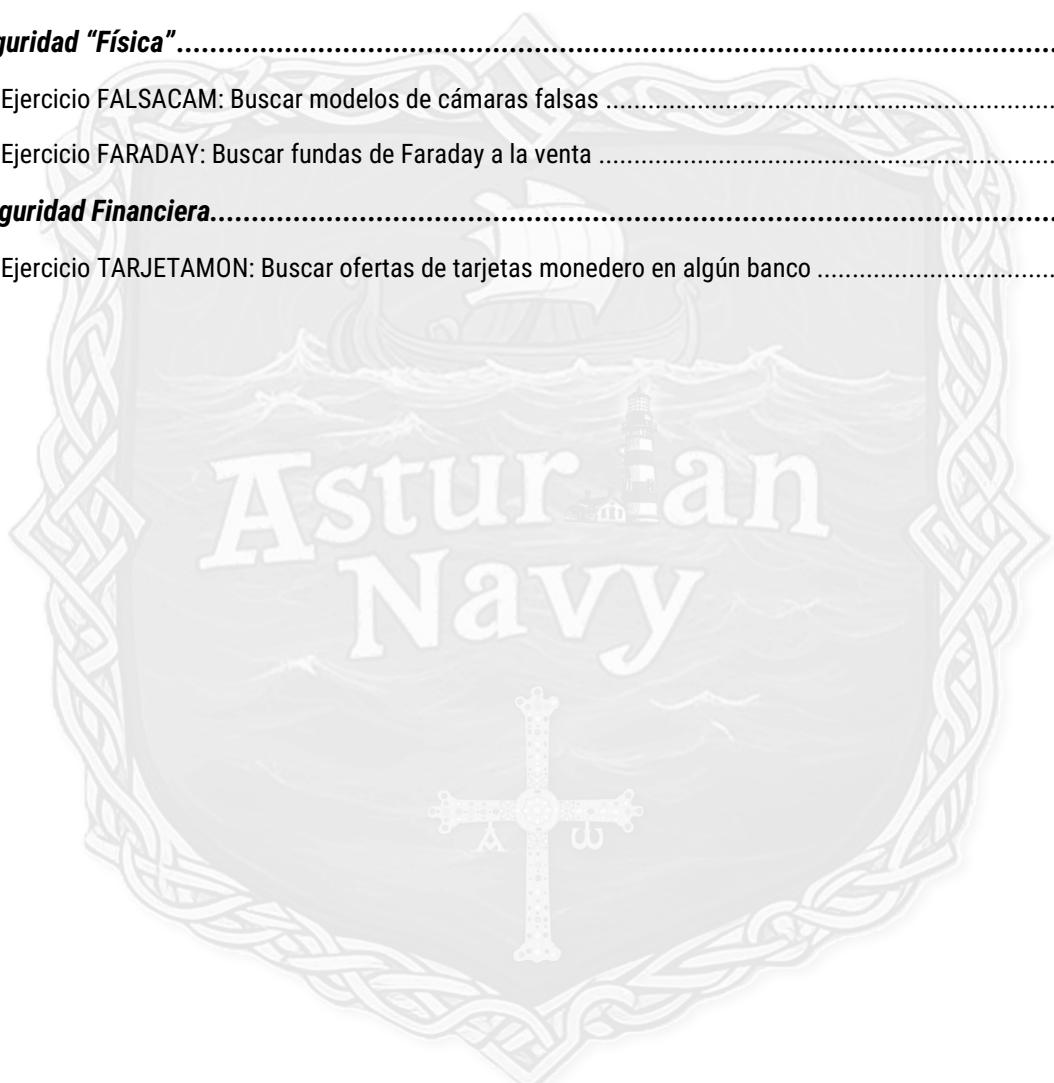




Tabla de Ilustraciones

Figura 1. Para que te voy a decir yo nada, si la web ya te lo dice todo.....	8
Figura 2. Dentro de 1245 siglos tienes que acordarte de cambiar la contraseña, eso sí. ¡No te olvides!	9
Figura 3. Entrar en este apartado hace que suba el indicador de hacker un punto	9
Figura 4. Guardar contraseñas en el navegador no es lo mejor...pero es mejor alternativa que apuntarlas en un post-it a la vista de todos, y también tiene sus perks	9
Figura 5. Esta persona tiene un PROBLEMA (mayúsculas a propósito).....	10
Figura 6. Los ataques de fuerza bruta lo van a tener fácil con este usuario	10
Figura 7. ¡Anímate a hacerlo! No es tan difícil . Fuente: https://www.incibe.es/ciudadania/formacion/infografias/crea-tu-contrasena-segura	11
Figura 8. Todo lo que te da una VPN puedes usarlo gratis. Olvídate de las que te recomiendan algunos YouTubers. ¡ProtonVPN de momento tiene una fama a prueba de balas!. Fuente: https://www.incibe.es/ciudadania/formacion/infografias/dispositivo-vpn	13
Figura 9. Quien dice contraseñas dice "cualquier información que sea importante para algún servicio", como nºs de tarjeta, PINs, etc. Es una caja fuerte, ¡no hay mucho más que entender! :)	14
Figura 10. Que tu identidad en Internet no dependa solo de que alguien se sepa una contraseña o no es uno de los mayores avances de seguridad ever. Fuente: https://twitter.com/ecrimeforense/status/952979528938336256	15
Figura 11. Estas "contraseñitas" son muchas veces 6 números que debes meter donde te lo pidan antes de que caduquen...y caducan rápida, así que atento	15
Figura 12. Ahora tu teléfono te mostrará 3 números y tú tienes que tocar el correcto para entrar. Es un 2FA muy fácil de usar	16
Figura 13. Ojo cuidao. Si te sale esta pantalla y no eres tú el que está intentando entrar, es que alguien sabe tu contraseña real. Así que pulsa en "No, no soy yo" y déjate aconsejar.....	16
Figura 14. ¡Vamos a morir! A lo mejor...y cuando pase ya estaremos todos muertos igualmente porque es dentro de muchísimos años. Pero eh, que rico el clickbait.....	18
Figura 15. Pocas páginas tienen un nombre que deja tan claro para lo que sirven, ¿no crees?	18
Figura 16. Lo de los bulos es realmente un pedazo de problema. Fuente: https://www.ucsf.edu.ar/pautas-y-recomendaciones-para-detectar-y-evitar-la-desinformacion/	19
Figura 17. El doxing es acoso. No participes de esto. Fuente: https://juventud.asturias.es/-/p%C3%ADdora-informativa-sobre-ciberseguridad-doxing-duplicar-0	23
Figura 18.Es muy sencillo: Solo con entrar en este apartado se actualiza solo	25
Figura 19. Actualizado en segundos, como si no hubiera pasado nada	25
Figura 20. ¿Sabías que Edge es Chrome con otra "cara"? Pues ahora ya lo sabes	26
Figura 21. Las extensiones de mi Firefox. Estas dos son buenas, créeme	27



Figura 22. Extensiones de mi Chrome. Algunas vienen instaladas de serie o cuando compras el PC.....	27
Figura 23. Yo la verdad ya no puedo navegar sin él. Internet es un lugar menos hostil.....	29
Figura 24. Mucho cuidado: Google quiere nerfear las extensiones que bloquean publicidad porque les quita ingresos, así que no sé con qué te encontrarás en Chrome en el futuro en este aspecto.....	29
Figura 25. Todo navegador que se precie tiene un bloqueador de publicidad. Unos integrado (como Brave) y otros instalable	30
Figura 26. Hay un poco de periódico pegado a este anuncio.....	30
Figura 27. Now we are talking	31
Figura 28. Somos buenos	32
Figura 29. Estos otros no tanto (era una tienda fraudulenta)	32
Figura 30. Clásico ejemplo de ragebait. No entres al trapo, encima les das dinero. Bloquéalo y a pastar .	33
Figura 31. Wow, seguro que ya se puede comprar un Lambo	34
Figura 32. En Twitter se llama "Proteger tus posts". En otros sitios directamente te dice "hacer tu cuenta privada"	34
Figura 33. Instagram te puede servir como ejemplo, pero todas las redes sociales tienen más o menos las mismas opciones.....	35
Figura 34. ¿Troll? ¿Pornobot? ¿Estafa financiera? ¿Se ha pasado tres pueblos? Denuncia la publicación o la cuenta. Es anónimo, palabrita	36
Figura 35. Cada red social tiene sus motivos de denuncia, pero bueno al final acaban siendo más o menos lo mismos en realidad, expresados de distintas formas	37
Figura 36. Esto te lo preguntan porque no todo tiene la misma prioridad. Es más prioritario quitar cierto tipo de posts que otros, y así los organizan para su revisión manual	37
Figura 37. Informe enviado. Si hay muchos así, se le ha caído el pelo (y la cuenta)	38
Figura 38. Si lo has denunciado lo más lógico es luego bloquearlo	38
Figura 39. Y con esto, hasta luego	39
Figura 40. Te has pasado, espera que te mando un recazo.....	39
Figura 41. La tercera opción es donde podemos precisar más.....	40
Figura 42. El nº de razones para denunciar se ha ampliado últimamente	40
Figura 43. Como ves, son esencialmente las mismas que Instagram	41
Figura 44. El INCIBE resume los problemas de ciberseguridad más comunes del día a día de forma brillante en sus infografías. Hazles caso. No es magia, son (literalmente) tus impuestos	43
Figura 45. Da igual el programa de Office que sea. Este botón no se toca NUNCA., Por lo que pueda pasar. Fuente: https://www.incibe.es/empresas/blog/evitar-incidentes-relacionados-los-archivos-adjuntos-al-correo	44
Figura 46. ¡Un tal José Manuel Redondo me está enviando spam de una asignatura! Denunciado (tranquis no lo hice , es solo para enseñaros la opción)	45



Figura 47. Todos los proveedores de correo tienen una opción de estas. Si les ayudas a "limpiar", les beneficias.....	45
Figura 48. Estas dos opciones son las importantes en este caso.....	47
Figura 49. Cuidado con la última opción (por suerte pregunta si le das por error).....	47
Figura 50. Esto es también una forma de saber si un/una colega ha cambiado de teléfono	48
Figura 51. Aquí solo hay dos opciones: Teléfono nuevo o reinstalación del WhatsApp	48
Figura 52. Muchas estafas tratan de engañarte para que les des tu contraseña y asignar tu WhatsApp a otro nº de teléfono (robártelo, vamos). Con esto ya no es tan fácil	49
Figura 53. Tu cuenta de WhatsApp y tu nº de teléfono están "casados", pero se pueden "divorciar" y buscar otra pareja . El problema es que los delincuentes lo aprovechan para estafar	49
Figura 54. Si desactivas esto, ya no te pueden acusar de "dejar en visto". Claro que entonces tu tampoco verás si los demás te lo hacen...	50
Figura 55. Si eres de los/as que cuenta tus estados de WhatsApp, igual te conviene restringirlo un poco	50
Figura 56. Básicamente compórtate de forma responsable de la misma forma que lo harías en una red social	50
Figura 57. Las copias de seguridad salvan vidas. Y facilitan cambiar de teléfono también	51
Figura 58. Entre Telegram y WhatsApp hay pocas diferencias. Pero no tienes que dar tu teléfono y tiene muchos foros de temas que te puedan interesar.....	52
Figura 59. Un problema, una ficha explicativa, para iOS y Android. ¡Así si se pueden hacer las cosas! :) ..	54
Figura 60. Aquí tienes un resumen de lo mínimo a hacer con tu teléfono y su configuración https://www.incibe.es/ciudadania/formacion/infografias/5-consejos-para-mejorar-la-seguridad-y-privacidad-en-dispositivos-moviles	55
Figura 61. Nº de valoraciones (reseñas), nº de descargas, quien es el autor (si es conocido o no)...	56
Figura 62. Cuando la puntuación baja de 4 estrellas, conviene leer las más bajas un poco a ver si hay una mención a virus o similar, o si solo es mal funcionamiento u otras críticas del servicio distintas.....	56
Figura 63. Cada permiso es una puerta a un posible problema de seguridad. ¡Mucho cuidado!. Fuente: https://www.incibe.es/ciudadania/formacion/infografias/permisos-de-apps-y-riesgos-para-tu-privacidad	57
Figura 64. Consejos del INCIBE con la instalación de aplicaciones. El INCIBE sabe, hazle caso al INCIBE. Fuente: https://www.incibe.es/ciudadania/formacion/infografias/instale-app-no-fiable	58
Figura 65. Típico estado de Windows Defender cuando lo arrancas y no has hecho nada más con el nunca	59
Figura 66. Configurar bien el Windows es difícil, pero por suerte lo mínimo es accesible gracias al INCIBE	60
Figura 67. ¿Te has descargado algo sospechoso? ¡Pregúntale al oráculo!	61
Figura 68. Está limpio. No es garantía de nada, pero ayuda	61
Figura 69. La cantidad de cosas que tiene esto es tremenda. Si no las entiendes no te preocupes, activalas, pruébalas y si no se rompe nada, tira para adelante con ellas	63
José Manuel Redondo López. Proyecto "F-74 'Asturias'"	



Figura 70. Esto evita que caigas por accidente en algún tipo de página en la que no quieras estar por accidente.....	64
Figura 71. ¿Te has enfadado con algún juego o quieres autolimitarte por algún motivo en algún servicio? No hay cosa mejor que esta	64
Figura 72. ¿Como poner esto en cualquier navegador que tengas? Te lo cuenta paso a paso	65
Figura 73. Todas las páginas que alguna vez fueron publicadas en uniovi.es. Casi na.....	67
Figura 74. ¿Qué hay dentro de estos "PDFs perdidos"? Sabe Dios	67
Figura 75. El robots.txt de uniovi.es. Uno puede sorprenderse de lo que puede encontrar si pone robots.txt al final del nombre de cualquier página de Internet (Ej.: www.uniovi.es/robots.txt)	68
Figura 76. Hay páginas que tienen un montón de capturas a lo largo de la historia y otras que menos. Todo depende de lo "popular" que sea	68
Figura 77. Y dime, ¿de qué quieres saber opiniones hoy? Fuente: https://www.trustpilot.com/categories	71
Figura 78. En el mercado actual, todo software “caduca” (se deja de mantener, actualizar...). Lo importante es sabe cuándo lo hace, y https://endoflife.date/ te lo dice.....	72
Figura 79. El tema de la caducidad de los móviles Android porque su sistema operativo deja de recibir actualizaciones es un auténtico problema que parece no tener solución. Espérate una “vida útil” de unos 4 años con los últimos cambios legales. Fuente: https://endoflife.date/android	73
Figura 80. Amazon (por poner un ejemplo) tiene un surtido de estos aparatos bien grande. Para todos los gustos, formas y colores	74
Figura 81. Será por formas y tamaños...	75
Figura 82. Un ejemplo de tarjeta monedero del Banco Santander. Fuente: Ej.: https://www.bancosantander.es/particulares/cuentas-tarjetas/tarjetas/debito/virtual-e-cash	77



Ejercicios de Defensa

⚠ AVISO IMPORTANTE: Unas palabras antes de empezar

Como parte de las actividades prácticas os doy **una máquina virtual Linux ya instalada** y lista para funcionar, especialmente preparada para hacer experimentos de ciberseguridad y por Internet en un entorno aislado. También se entrega **un manual de cómo ponerla en marcha** y lo que necesitáis para ello.

💡 *Si este manual se te queda corto, recuerda que en el R-11 "Príncipe de Asturias" se ven más cosas de máquinas virtuales 😊*

De esta manera podéis hacer experimentos en ella, probarlos, y si después de un tiempo os convence y no da problemas, pasarlo ya a vuestra máquina principal.

💡 *Por cierto, si después de seguir este taller tus padres quieren "ponerse al día" siguiendo tu ejemplo, que sepas que el INCIBE tiene formación para ellos aquí: <https://www.incibe.es/ciudadania/experiencia-senior> ¡Pásasela! 😊*





Aspectos Relativos a las Personas

Autenticación

Ejercicio PROTONPASS: Probar fortaleza de contraseñas y también ProtonPass

Descripción de la actividad

Consiste en aprender a **crear contraseñas fuertes de acuerdo con los estándares** en vigor actuales vistos en la teoría.

Resultados Esperados

Puedes crear una contraseña fuerte y sustituir cualquier contraseña que uses actualmente por una que cumpla con esos estándares se fortaleza, si no lo hace ya. Además, sabes cómo funciona un gestor de contraseñas, por ejemplo *ProtonPass*.

Otra información necesaria para su realización

Una medida básica de seguridad es **no comunicar públicamente el nombre de usuario** de ninguna de tus cuentas. Si bien esto es muchas veces imposible, puesto que muchos de ellas están públicos en redes sociales, etc., conviene no hacerlo aún más fácil.

La siguiente medida de seguridad es **tener una buena contraseña**. Para ello hay que cumplir las siguientes normas:

- **No usar la misma clave en varias de tus cuentas.** Idealmente, usar una clave **distinta** para cada cuenta.
- **No usar una clave débil**, sino una de suficiente longitud que combine letras mayúsculas, minúsculas, nºs y letras como vinos en la teoría. **NUNCA UNA PALABRA DEL DICCIONARIO.**

Como saber si una clave es buena puede ser difícil, podemos usar un servicio gratuito de un vendedor de antivirus conocido: <https://password.kaspersky.com/es/>. Debemos usar una clave que **no** dé esto:

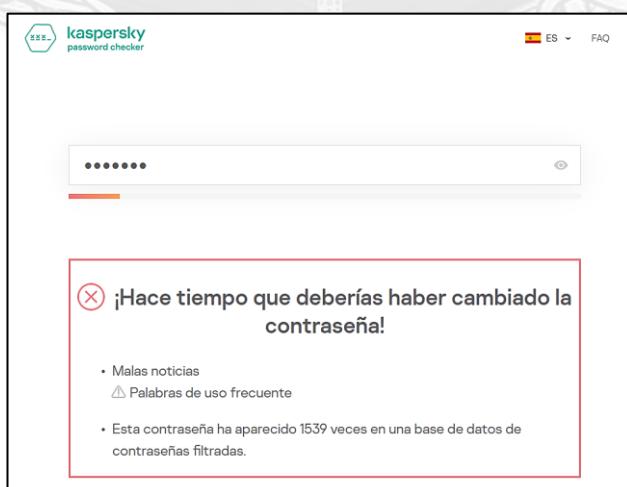


Figura 1. Para que te voy a decir yo nada, si la web ya te lo dice todo...

Sino este (la contraseña correspondiente es **E1_7_De_Setiembre**):

José Manuel Redondo López. Proyecto "F-74 'Asturias'"



The screenshot shows a password input field containing a long string of characters. Below it, a green box displays a checkmark and the message "¡Buena contraseña!" (Good password!). A bulleted list indicates the password is resistant to hacking and not found in any breached password database. At the bottom, a note states that the password can be cracked by a common computer in 1245 years.

Figura 2. Dentro de 1245 siglos tienes que acordarte de cambiar la contraseña, eso sí. ¡No te olvides! 😊

No obstante, hay gente que prefiere no usar estos servicios para comprobar la robustez de las claves **por miedo a que las claves en sí se filtren**. Si bien no hay pruebas de ello, **es una preocupación válida**. Si no queremos usar esto, podemos usar una funcionalidad similar que tiene **Google Chrome** con las contraseñas que guardamos en este navegador. Podemos acceder a ella a través de esta opción de menú:



Figura 3. Entrar en este apartado hace que suba el indicador de hacker un punto 😊

Y en el apartado "**Seguridad y Privacidad**" vemos esto:

The screenshot shows the "Comprobación de seguridad" section with a shield icon and the text: "Chrome puede protegerte frente a quebradas de seguridad de datos, extensiones dañinas y mucho más". A blue button labeled "Comprobar ahora" is visible. Below it, the "Seguridad y privacidad" section includes a "Borrar datos de navegación" button.

Figura 4. Guardar contraseñas en el navegador no es lo mejor...pero es mejor alternativa que apuntarlas en un post-it a la vista de todos, y también tiene sus perks



Al comprobar las contraseñas que tengamos guardadas en el navegador de cualquiera de nuestras cuentas, Google Chrome consultará sus bases de datos para saber si alguna ha sido **filtrada**, se ha **reutilizado** en varios servicios o se considera **poco segura**. A veces esta revisión nos da algunas sorpresas desagradables:



Figura 5. Esta persona tiene un PROBLEMA (mayúsculas a propósito)

Recuerda siempre que si tu contraseña **es demasiado corta o contiene palabras**, lugares o nombres del diccionario, entonces puede ser fácilmente descifrada a través de la **fuerza bruta** (probando un gran nº de contraseñas distintas a lo largo del tiempo), o adivinada por alguien que haya robado el fichero donde un determinando servicio la guarda. Esto es lo que típicamente aparece en las noticias como una “**brecha de datos**” o que se “**filtre**” una contraseña: que alguien le robe el fichero de usuarios y contraseña de una tienda, proveedor, empresa, etc.

Si te preocupa **cuanto tiempo podrían tardar en robarte la contraseña** si ese fichero se filtra y quieres tener una segunda opinión, el servicio *HowSecureIsMyPassword* (<https://www.security.org/how-secure-is-my-password/>) te da una estimación de ello. Comprobarás que **a mayor fortaleza, mayor tiempo**, hasta llegar a tiempos inabordables por cualquier atacante. En la imagen desde luego, aparece un muy mal ejemplo 😊.



Figura 6. Los ataques de fuerza bruta lo van a tener fácil con este usuario



💡 Los ataques de fuerza bruta (probar millones de contraseñas generadas automáticamente o de un fichero de posibles contraseñas) son poca broma. Pero con una contraseña buena, puedes ser inmune a ellos. También te digo que un servicio decente debería meterte un ban temporal de media hora o así si metes más de 10 veces mal la contraseña (nadie en su sano juicio hace eso por error), pero confiar en que hagan eso es mucho confiar...

Crear una buena contraseña es algo que mucha gente sabe ya, pero por si acaso el INCIBE te explica como en esta infografía y aquí:

https://www.incibe.es/sites/default/files/docs/c3_pdf_rp_mejora_tus_contraseñas.pdf

Crea tu contraseña segura
PASO A PASO

PASO 1
Pensar una frase
Puede tener significado para nosotros o simplemente unir 2 o 3 palabras al azar, pero que nadie más conozca. La longitud mínima recomendada es de 10 caracteres.

Mi cuenta segura

PASO 2
Alternar mayúsculas y minúsculas
Unimos las palabras y resaltamos las iniciales con mayúsculas.

MiCuentaSegura

PASO 3
Sustituir letras por números
Un truco es intercambiar algunas letras por cifras, como "o" por 0, "í" por 1, "e" por 3 o "a" por 4.

M1Cu3nt4S3gur4

PASO 4
Añadir caracteres especiales
Solo queda incluir algún símbolo (~!@#\$%^&*+-_=|[{}]{})"; "<>,.?/).

M1Cu3nt4S3gur4!

PASO 5
Personalizar la clave para cada servicio
Podemos utilizar las dos primeras letras del servicio y una la ponemos al principio y otra al final de la clave, ambas en mayúsculas. Ejemplo: si el servicio se llama "Mailbook", usaremos la M y la A.

MM1Cu3nt4S3gur4!A

¡Y listo! Así de sencillo hemos creado nuestra contraseña robusta, segura y fácil de recordar.

Y como medida de seguridad extra, sigue estos consejos y los ciberdelincuentes no tendrán nada que hacer:

- Utiliza gestores de contraseñas para controlar todas tus claves.
- No repitas las mismas contraseñas en distintas cuentas.
- Cambia las cada cierto tiempo (3 meses).
- No las compartas con nadie, ni amigos ni familiares.
- Utiliza la verificación en dos pasos siempre que sea posible.
- Configura tu móvil para que, cuando se muestran los caracteres que pulsas.
- Recuerda que tienes a tu disposición la Línea de Ayuda en Ciberseguridad de INCIBE 017, gratuita y confidencial, para cualquier duda relacionada con la ciberseguridad.

www.incibe.es | www.osi.es

GOBiERNO DE ESPAÑA. MONTEREY. SECRETARÍA TÉCNICA DEL GOBIERNO. SEDE: MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. SECRETARÍA DE ESTADO DE INVESTIGACIONES, INVESTIGACIÓN, INTELIGENCIA ARTIFICIAL

incibe INSTITUTO NACIONAL DE CIBERSEGURIDAD

osi Oficina de Seguridad del Internauta

Figura 7. ¡Anímate a hacerlo! No es tan difícil 😊 . Fuente:
<https://www.incibe.es/ciudadania/formacion/infografias/crea-tu-contraseña-segura>



La última pregunta que surge de esto es *¿Pero si te roban el fichero de usuarios y contraseñas no pueden leerla directamente?* *¿Para qué tanto esfuerzo en averiguar una contraseña?* Y la respuesta es que, **si el servicio hace las cosas bien, NO.** Las contraseñas **nunca se deberían guardar tal cual tú las metes**, sino en una formato especial que impide averiguarlas fácilmente (solo por fuerza bruta), que se llama **hash**. No voy a explicar más sobre el tema, pero esto sirve para que te des cuenta de dos cosas:

- **Que la fortaleza de tu contraseña es algo muy útil, más de lo que crees:** A más fortaleza, más tiempo para averiguarla por fuerza bruta en un servicio que haga bien las cosas.
- **Que un servicio realmente no puede conocer tu contraseña:** Una de las ventajas que tiene guardarla en forma de hash es que el servicio solo puede comparar si lo que tú has introducido es idéntico a lo que ellos guardan, ¡pero no pueden saber cuál es exactamente tu cuenta simplemente leyendo el sitio donde las guardan!

Y ahora sobre **ProtonPass**, un gestor de contraseñas. Usar un gestor de contraseñas fuera de lo que tienen los navegadores a día de hoy es muy “pro”, pero ¿Quién dijo miedo? 😊. Si te animas a dar el paso, yo te recomiendo que uses uno de la empresa **Proton**, que forma parte de un pack de servicios chulísimos que te dan incluso una capa gratis de uso. Simplemente hazte una cuenta gratuita (<https://proton.me/mail>) y podrás acceder a:

- **ProtonMail:** Un email de toda la vida, pero que todo lo que envíes va cifrado siempre, sin que hagas nada, por lo que solo tú y el receptor podréis conocer lo que os enviáis. ¡Máxima privacidad para tus secretos! (**Créeme, el mail “normal” NO es así**).
- **ProtonDrive:** 1Gb de almacenamiento en nube. No es mucho, pero ¡it's free!. Por supuesto, cifrado también, a diferencia de otras opciones
- **ProtonVPN:** *¿Quieres conectarte como si fueras otra máquina o estuvieras en otro país para que nadie sepa que eres tú?* Para eso sirven las VPN, como te explica el INCIBE en la siguiente imagen. De forma gratuita podrás hacer creer a cualquier web que estás en Suiza, EEUU o Japón 😊. ¡No es nada difícil!: <https://peakd.com/hive-106817/@soy-laloreto/por-que-usar-un-vpn>



Figura 8. Todo lo que te da una VPN puedes usarlo gratis. Olvídate de las que te recomiendan algunos YouTubers. ¡ProtonVPN de momento tiene una fama a prueba de balas! Fuente:
<https://www.incibe.es/ciudadania/formacion/infografias/dispositivo-vpn>

- **ProtonPass:** Un gestor de contraseñas, o lo que es lo mismo, **una caja fuerte** donde tus contraseñas se guardan de manera cifrada y solo tú puedes acceder. Te las recuerda cuando las necesitas (¡olvídate del post-it!) pero te las protege de robos. Aquí tienes un tutorial para usarlo: <https://proton.me/support/use-pass-web>



The screenshot shows the Proton Pass application interface. On the left, there's a sidebar with 'Vaults' (All vaults: 21, Personal: 18, Work: 3, Trash: 3). The main area shows 'Today' with items: 'Security door PIN' (1234), 'Company card' (1234 1234), and 'Proton login' (@proton.ch). To the right, a 'Proton login' panel shows fields for 'Username' (@proton.ch), 'Password' (redacted), and 'Websites' (https://mail.proton.me/). There are also 'Edit', 'Delete', and 'More' buttons.

Figura 9. Quien dice contraseñas dice "cualquier información que sea importante para algún servicio", como nºs de tarjeta, PINs, etc. Es una caja fuerte, ¡no hay mucho más que entender! :)

Ejercicio 2FA: Experimentar con un 2FA

Descripción de la actividad

Consiste en **activar el segundo factor de autenticación** en algún servicio que uses y no lo tenga

Resultados Esperados

Puedes **proteger alguno de tus servicios con un segundo factor de autenticación** que dependa de una aplicación específica de tu teléfono móvil. Puede responder a estas preguntas

- *¿Entiendes por qué este sistema te protege, aunque alguien averigüe tu clave?*
- *¿Entiendes por qué el código que te sale en la aplicación es casi imposible de reproducir por un atacante?*
- *¿Comprendes que pasa si en el teléfono te sale un código que debes introducir, pero tú no has intentado meterte en tu cuenta en ese momento?*

Otra información necesaria para su realización

Una de las cosas que quiero dejarte clara es la importancia de activar un 2FA en todos los servicios que puedas. Lo primero que debes entender es lo que se cuenta en la imagen siguiente: Un 2FA es un dato más que aportas **tras introducir tu usuario y contraseña correctamente** en el servicio que lo tenga activo. Esto es muy importante: **correctamente**. Nadie ajeno a ti puede lanzar el proceso 2FA sin que sepa o haya averiguado de alguna forma tu contraseña en primer lugar.

Como ves en la imagen, ese segundo factor varía en función de lo que introduzcamos después y de dónde lo saquemos.



Figura 10. Que tu identidad en Internet no dependa solo de que alguien se sepa una contraseña o no es uno de los mayores avances de seguridad ever. Fuente: <https://twitter.com/ecrimeforense/status/952979528938336256>

La activación de 2FA para el acceso a servicios típicos **es una necesidad hoy en día**, y por tanto debemos identificar cuántos de nuestros servicios lo admiten y activarlo. La forma de 2FA que da un nivel de seguridad adecuado con un coste de puesta en marcha más reducido es mediante **una aplicación en el teléfono que genere códigos OTP (One-Time Password)** como *Google Authenticator* (en la imagen) o *Microsoft Authenticator*. Ambas son fácilmente instalables en teléfonos *Android*:

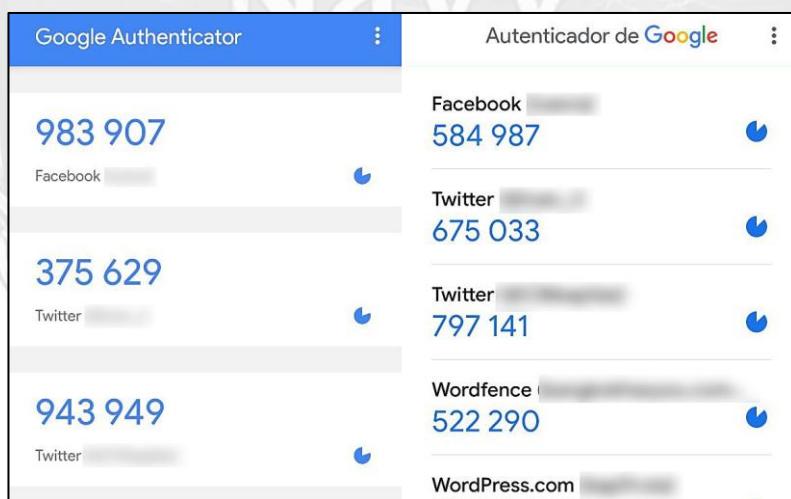


Figura 11. Estas "contraseñitas" son muchas veces 6 números que debes meter donde te lo pidan antes de que caduquen...y caducan rápida, así que atento

💡 A lo mejor ahora te estás preguntando: "Eh, eh, para el carro. ¿No me acabas de decir antes que una contraseña de 6 números es muy débil? ¿Qué pasa aquí?" Pasa que tienes razón, como contraseña es malísima. Pero pasan también dos cosas: solo valen 1 minuto (literal) porque luego cambian, y te aparecen en la pantalla de tu teléfono, que solo tú puedes ver. Así que una cosa compensa a la otra. Aquí te interesa poner esta segunda contraseña rápido mientras siga siendo válida. Si te la complico, vas a odiar el sistema. Y lo peor que puede pasarle a un sistema de seguridad es que la gente lo odie 😊



Otros servicios tendrán esta funcionalidad entre sus opciones, solo tenemos que buscarla y seguir las instrucciones. Como veremos también luego, **no siempre se nos va a pedir un código** de una aplicación, a veces se nos pedirá que introduzcamos en nuestro móvil un nº que nos aparece por pantalla o pulsar un botón. Todo depende de cómo lo haya configurado el servicio.

Figura 12. Ahora tu teléfono te mostrará 3 números y tú tienes que tocar el correcto para entrar. Es un 2FA muy fácil de usar

Figura 13. Ojo cuidao. Si te sale esta pantalla y no eres tú el que está intentando entrar, es que alguien sabe tu contraseña real. Así que pulsa en "No, no soy yo" y déjate aconsejar

En la última imagen ves la idea que te quiero hacer llegar: Aunque alguien te haya birlado tu clave y la use, no va a poder entrar porque le falta dar ese segundo paso para que el servicio sepa que tú eres tú

Si quieras saber más sobre el 2FA, el INCIBE te lo explica aquí: <https://www.incibe.es/ciudadania/blog/el-factor-de-autenticacion-doble-y-multiple>.



Computación “sensata”

Ejercicio MALDITO BULO: Visitar “Maldito Bulo”

Descripción de la actividad

Consiste en tener un sitio web de referencia para desmentir noticias falsas o bulos que puedan existir por redes sociales u otros medios en internet

Resultados Esperados

Tienes acceso a un sitio que te permite **desmentir los bulos que puedes leer**, y te has acostumbrado a hacerlo en cuanto a alguna noticia suena exagerada o rara. Puedes contestar a estas preguntas:

- *¿Tiene el sitio un método de consulta directo de algún bulo que hayas recibido o de alguna noticia que te resulte inverosímil?*
- *¿Crees que el sitio se mantiene actualizado (en el sentido de hablar de cosas que has recibido muy recientemente?)*
- *A juzgar por lo que has visto, ¿Consideras que tu entorno está sometido a muchos bulos o noticias falsas?*

Otra información necesaria para su realización

Hoy en día la propagación de noticias falsas se ha convertido en un auténtico problema por la cantidad de **personas que se dedican a extender esos bulos con fines maliciosos**. Esto se consigue de dos formas:

- **Contando directamente mentiras.** Hay grupos organizados de desinformación social afiliados a determinadas organizaciones o partidos políticos (todos ellos, aquí no estoy señalando a ninguno porque los hay de todos), encargados de propagar ciertos mensajes en momentos concretos de tiempo (elecciones, eventos importantes, “tapar” escándalos...). La **“ciber-guerra” de la información es un hecho, no algo teórico ni típico de películas.**
- **Escondiendo parte de la verdad** para que una noticia suene de forma distinta. Es muy típico de publicaciones de carácter periodístico, sobre todo para que el público entre en la noticia (el famoso “clickbait”) y de esta forma vea la publicidad embebida y generen ingresos, además de “engordar” sus estadísticas de lectores. Un ejemplo esta noticia, donde el titular omite que la posibilidad de impacto es muy pequeña y que, de ocurrir, lo haría después de varios milenarios:



20minutos.es @20m

Un asteroide "asesino de planetas" se esconde en el resplandor del Sol y amenaza la Tierra: "Sería un evento de extinción masiva"

20minutos.es

Un asteroide "asesino de planetas" se esconde en el resplandor del Sol y su ór...
Hace pocas semanas la NASA lanzó su nave DART para desviar de la trayectoria del asteroide Dimorphos. El pasado 11 de octubre pudo confirmar el impacto y...

Figura 14. ¡Vamos a morir! A lo mejor...y cuando pase ya estaremos todos muertos igualmente porque es dentro de muchísimos años. Pero eh, que rico el clickbait

Dado que esto es un verdadero problema (y que se acentúa en determinadas fechas, como por ejemplo elecciones, guerras, etc.) es necesario que tengamos algunas páginas de referencia que nos ayuden a desmentirlos o donde podamos preguntar si alguna información tiene visos de verdad o bien solo es verdad a medias. Una de las más conocidas es **Maldito Bulo** (<https://maldita.es/malditobulo/>):

Figura 15. Pocas páginas tienen un nombre que deja tan claro para lo que sirven, ¿no crees?



Como puede verse, no solo listan las noticias falsas del momento en portada sino que además ofrece un servicio vía **WhatsApp** para desmentir bulos, si por la razón que sea nos corre prisa desmentir alguno. Si no queremos depender de estos servicios, es necesario desarrollar una conciencia sobre lo que leemos, que se puede resumir en esta infografía.

FILTRAR ANTES DE PUBLICAR PREGUNTARSE ANTES DE COMPARTIR PENSAR Y CONSULTAR ANTES DE CREER

INDICIOS DE QUE PODEMOS ESTAR FRENTE A INFORMACIÓN FALSA

-  Se desconoce la **fuente**
-  Los **datos** principales son **inciertos**
(fecha, lugar, nombres de los protagonistas, etc)
-  Se presenta en **modo condicional**:
"habría", "podría", "iría", etc...
-  Apela directamente a tus **emociones**

PREGUNTAS QUE PODÉS HACERTE ANTES DE COMPARTIR INFORMACIÓN DUDOSA

-  ¿Cuál es el **origen de la información**?
Quién la dijo o publicó, ¿es **confiable**?
¿Hay alguna **fuente oficial/reconocida** que la respalde?
-  ¿El **contenido** es **espectacular e impactante**?
¿Coincide plenamente con tus **convicciones** y las alienta?
-  ¿Hay **material** gráfico o audiovisual complementario
que **confirma la información**?

Infografía: UCSF

Figura 16. Lo de los bulos es realmente un pedazo de problema. Fuente: <https://www.ucsf.edu.ar/pautas-y-recomendaciones-para-detectar-y-evitar-la-desinformacion/>



🛠 Ejercicio ACOSO: Consulta la información contra el acoso que está publicada en Internet para ti o para tu familia

💻 Descripción de la actividad

Consiste en que tengas **recursos para defenderte contra situaciones de acoso o ciberacoso** a ti o a alguien que conoces

🏆 Resultados Esperados

Puedes contestar a las siguientes preguntas:

- ¿Tienes ya claro que el INCIBE tiene recursos que te pueden ayudar en muchas cosas relativas a temas de ciberseguridad?
- ¿Te queda claro que el acoso es un delito denunciable y que tienes a quien acudir y dónde sacar recursos para poder defenderte?
- ¿Entiendes que “mirar hacia otro lado” no te va a librarte del problema porque la próxima víctima puedes ser tú y sabes cómo actuar en contra del acoso, aunque sea de forma anónima?

📋 Otra información necesaria para su realización

El acoso escolar es una **lacra** que o paramos entre todos (profesores, padres y sí, tú también) o **puede convertir la vida de algunas personas en auténticos infiernos**. Algunas personas creen que esta forma de comportarse es “normal” porque se trata de “un juego” y que no lleva a nada serio. Pues es todo lo contrario. **Aquí perdemos todos**, fíjate las consecuencias del acoso escolar:

- **Para la víctima** (que se lleva, con diferencia, la peor parte de todo esto):
 - *Emocionales*:
 - Baja autoestima e imagen de sí mismo.
 - Ansiedad, depresión e incluso ideas suicidas.
 - Miedo, irritabilidad y cambios de humor.
 - Dificultades para concentrarse y aprender.
 - Problemas para dormir y comer.
 - Sentimientos de soledad y aislamiento.
 - Dificultades para formar relaciones sociales.
 - Trastornos psicosomáticos como dolores de cabeza o estómago.
 - *Sociales*:
 - Aislamiento social y exclusión.
 - Dificultades para hacer amigos y mantener relaciones.
 - Hostilidad y agresividad hacia los demás.
 - Dificultades para confiar en las personas.
 - Miedo a ir a la escuela.
 - Abandono escolar.
 - *Físicas*:
 - Lesiones físicas por el acoso.
 - Problemas de salud como dolores de cabeza o estómago.
 - Debilitamiento del sistema inmunológico.
 - Dificultades para dormir.
 - *A largo plazo*:



- Dificultades para encontrar un trabajo.
- Problemas para mantener relaciones sanas.
- Depresión y ansiedad crónicas.
- Abuso de sustancias.
- Problemas de salud mental graves.
- **Para el acosador (sí, también para ellos/as):**
 - *Emocionales:*
 - Falta de empatía y remordimiento.
 - Baja autoestima.
 - Dificultades para controlar la ira.
 - Problemas para seguir las normas.
 - Dificultades para formar relaciones sociales sanas.
 - Sentimientos de culpa y vergüenza.
 - *Sociales:*
 - Dificultades para hacer amigos y mantener relaciones.
 - Aislamiento social.
 - Exclusión de actividades sociales.
 - Reputación negativa.
 - Problemas para encontrar un trabajo.
 - *Legales:*
 - Responsabilidad civil por los daños causados a la víctima.
 - Posibles cargos penales.
 - Para los testigos:
 - Emocionales:
 - Sentimientos de culpa y vergüenza por no haber intervenido.
 - Miedo a ser el próximo objetivo del acoso.
 - Ansiedad y estrés.
 - *Sociales:*
 - Dificultades para hacer amigos y mantener relaciones.
 - Aislamiento social.
 - Exclusión de actividades sociales.
 - Problemas para encontrar un trabajo.
- **Para la familia:**
 - *Emocionales:*
 - Angustia, estrés y ansiedad.
 - Sentimientos de impotencia y culpa.
 - Dificultades para comunicarse con el niño o la niña.
 - Problemas para dormir y comer.
 - Dificultades para concentrarse en el trabajo.
 - *Sociales:*
 - Aislamiento social.
 - Exclusión de actividades sociales.
 - Problemas para encontrar un trabajo.
- **Para la escuela:**
 - *Emocionales:*
 - Deterioro del clima escolar.
 - Disminución del rendimiento académico.



- Dificultades para mantener la disciplina.
- Mala imagen pública.
- Sociales:
 - Dificultades para atraer y retener estudiantes y profesores.
 - Problemas para mantener relaciones con la comunidad.

 **Efectivamente, aquí perdemos todos, sin excepción. Obviamente mucho más la víctima y su entorno. El culpable siempre es el que decide acosar, porque lo hace a sabiendas (decidir hacer daño a los demás es un acto consciente y voluntario)**

Es importante recordar que **cada caso de acoso escolar es diferente** (no los hay “de verdad” y “de mentira”, “mejores” o “peores”, si te hace sentir mal es acoso, y punto) y que las consecuencias pueden variar en función de la gravedad del acoso, la duración de este y la capacidad de la víctima para afrontarlo. Si tú, o alguien que conoces, está sufriendo acoso escolar, es **importante buscar ayuda**. Hay muchos recursos disponibles para ayudar a las víctimas, a sus familias y a las escuelas a prevenir y abordar el acoso escolar. Fíjate que el problema es tan grave que el **INCIBE** y otras organizaciones han tomado cartas en el asunto para ayudar a las víctimas a combatir este problema:

- Página de información sobre el tema del gobierno de Canarias: <https://guaguasglobal.com/acoso-escolar-o-bullying/>
- Ciberacoso escolar: <https://www.incibe.es/menores/tematicas/ciberacoso>
- Cyberbullying: <https://www.incibe.es/menores/tematicas/ciberacoso>
- El 017 te puede ayudar también con eso. Llámalo

Todo este material te tiene que dejar clara una cosa: **actúa para defender a personas en necesidad** y, en último caso, para defenderte a ti mismo y a la gente que quieras: Si tienes *bullies* en tu entorno, **tu entorno nunca va a ser algo sano**, y eso tienen que entenderlo todos los que no participan en estas actividades, que deberían aliarse contra los que sí.

Una última cosa que quiero dejar clara, porque me consta que no todo el mundo lo tiene claro, es que el **doxing**, que parece algo no relacionado porque está desgraciadamente muy normalizado hoy en día, **es también una forma de acoso**, así que denúncialo pero, sobre todo, **NO LO PRACTIQUES**.

 **Todas estas cosas hacen sufrir a personas, y muchas veces de manera muy bestia. Ten empatía y piensa en el daño que están haciéndoles. No, las víctimas nunca se lo merecen. Y mañana podrías ser tú ¿Crees que un acosador necesita inventarse una excusa muy elaborada para elegirte como su próxima víctima? Las excusas son simplemente justificaciones cutres para seguir con su labor de “destrucción personal”. No hay excusa válida que justifique esto.**



DOXING
PRÁCTICA DE REVELAR INFORMACIÓN PERSONAL DE UNA PERSONA POR INTERNET SIN SU CONSENTIMIENTO

¿Qué te podría pasar si alguien practica doxing contra ti?

- 1 Perjudica tu reputación online.
- 2 Acoso o extorsión.
- 3 Suplantación de identidad.
- 4 Te expone a fraudes y otras amenazas online.
- 5 Pone en peligro tu seguridad física.

Además, te recomendamos:

- 1 Ajustar la configuración de privacidad de tus cuentas y perfiles online.
- 2 Ser más estricto con lo que compartes o publicas online.
- 3 Actualizar tus contraseñas y activar la doble verificación en tus cuentas.
- 4 Activar alertas para recibir notificaciones en tu email en caso de que se identifique que tus datos están siendo utilizados en Internet.
[\(https://www.google.es/alerts\)](https://www.google.es/alerts)
- 5 Realizar búsquedas por tus datos personales para localizar posibles contenidos publicados sobre ti.

Te animamos a que te pongas en contacto con la Línea de Ayuda en Ciberseguridad de INCIBE si necesitas más ayuda sobre este o cualquier otro tema relacionado con ciberseguridad.

¿Qué puedes hacer si te ves afectado?

GUARDA las evidencias.

BLOQUEA al usuario y solicita la eliminación del contenido.

DENUNCIA los hechos ante las Fuerzas y Cuerpos de Seguridad.

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia España | digital 2020

incibe_ Instituto Nacional de Ciberseguridad

CSI Oficina de Seguridad del Internauta

www.incibe.es/ciudadania

Figura 17. El doxing es acoso. No participes de esto. Fuente: <https://juventud.asturias.es/-/p%C3%ADdora-informativa-sobre-ciberseguridad-doxing-duplicar-0>



Uso de Internet



Usando el navegador de forma segura



Ejercicio UBLOCK: Instalar un bloqueador de publicidad



Descripción de la actividad

Consiste en comprobar que tu navegador **está actualizado y no tiene instalada ninguna extensión** que pueda ser peligrosa o que no conozcas, para luego instalar algunas que te mantengan más seguro.



Resultados Esperados

Puedes contestar a las siguientes preguntas:

- ¿Crees que tu navegador se actualiza automáticamente?
- ¿Tienes alguna extensión en el navegador de la cual no eras consciente?
- ¿Cómo crees que ha podido llegar hasta ahí?
- ¿Has podido desinstalar una extensión que ya no querías fácilmente?
- ¿Eres consciente de la cantidad de anuncios que estabas viendo casi sin darte cuenta?
- ¿Ha mejorado tu experiencia de navegación en muchas páginas web ahora?
- ¿Crees que la navegación es más rápida también?
- ¿Entiendes ahora la importancia de tener un bloqueador de publicidad integrado al navegar?



Otra información necesaria para su realización

Si bien las actualizaciones de cualquier producto que usemos son importantes, **las de un navegador de Internet son si cabe aún más**, puesto que es el que “da la cara” ante las páginas por las que navegamos. Existen páginas creadas con el único objetivo de **dañar** de alguna forma a todos aquellos que las visitan (especialmente las que son el destino de algún mensaje de *phishing* o similar), y para ello muchas veces se aprovechan de **vulnerabilidades conocidas** en algunos navegadores.



Esas vulnerabilidades se arreglan con actualizaciones, de ahí que su instalación sea super importante

No obstante, por suerte para nosotros, los fabricantes de los navegadores principales han hecho desde hace mucho tiempo **que se actualicen solos** cada vez que los abramos en el caso de que haya alguna versión mayor nueva. En caso de que el navegador nos avise de que debe reiniciarse a consecuencia de una actualización, debemos hacerlo inmediatamente para estar a salvo de posibles problemas.

No obstante, otros navegadores permiten desactivar las actualizaciones automáticas (que insisto, **no conviene hacerlo**), no contemplan hacer esto en cada arranque o no lo hacen automáticamente si se trata de una actualización menor. Por otro lado, es posible que salga una actualización para arreglar un problema muy nuevo y grave, y si somos de los que tienen el ordenador encendido muchas horas seguidas sin reiniciarlo quizás tarde en instalarse más de lo debido.

En todos estos casos podemos **forzar la actualización de un navegador** entrando en su configuración y simplemente consultando la opción de esta correspondiente. Esto es lo que ocurre por ejemplo en *Google Chrome*:



The screenshot shows the 'About' section of the Google Chrome settings. It displays the following information:

- Google Chrome logo
- Actualizando Chrome (100%)
- Versión 99.0.4844.82 (Build oficial) (64 bits)
- Links: Obtener ayuda de Chrome and Notificar un problema

Below this, there is a 'Configuración avanzada' dropdown menu.

Figura 18.Es muy sencillo: Solo con entrar en este apartado se actualiza solo

Y, como vemos, al terminar nos pide reiniciar el navegador, algo que, como decía, **debemos hacer inmediatamente para que la actualización sea efectiva**.

💡 No te preocupes, este proceso hace ya tiempo que no pierde lo que estabas haciendo y el navegador al reiniciarse volverá a tener todas tus pestañas y webs abiertas, como si no hubiera ocurrido nada 😊

The screenshot shows the 'About' section of the Google Chrome settings after the update has completed. It displays the following information:

- Google Chrome logo
- La actualización ya casi ha terminado. Reinicia Chrome para completar la actualización.
- Versión 99.0.4844.82 (Build oficial) (64 bits)
- Links: Reiniciar, Obtener ayuda de Chrome, and Notificar un problema

Figura 19. Actualizado en segundos, como si no hubiera pasado nada



Microsoft Edge y Firefox tienen opciones similares en el mismo sitio de su configuración:

The screenshot shows the Microsoft Edge configuration interface. On the left, a sidebar lists various settings like Profiles, Privacy, Appearance, and Languages. The 'About Microsoft Edge' option is selected. The main panel displays the 'About' information for Microsoft Edge version 99.0.1150.52 (Official Build) (64-bit), stating it is up-to-date. It also includes a section for downloading updates via usage-based connections, which is currently disabled. Below this, there's a note about the browser being built on open-source Chromium and links to Microsoft's terms of use, privacy statement, and service contract. The 'Microsoft Edge Insider' section is also visible, encouraging users to try early versions and participate in the developer community.

Figura 20. ¿Sabías que Edge es Chrome con otra “cara”? Pues ahora ya lo sabes 😊

Cabe destacar que **no conviene suscribirse** a programas que nos ofrezcan probar las últimas novedades de un navegador antes de que se lancen al público, porque básicamente estaremos ofreciéndonos a hacer de **probadores de funcionalidades** que no esté del todo pulidas de manera gratuita, aumentando la probabilidad de que haya inestabilidades o problemas (incluso de seguridad).

💡 **¿Te mola hacer de beta-tester? Pues mejor con un juego popular y no con un navegador. Al menos lo primero es divertido (si el juego es bueno, claro 😊)**

Y ahora llega el asunto de las **extensiones de un navegador**. Un navegador hace muchas cosas, pero no puede hacerlas todas ni adaptarse a lo que cada persona necesita. Para eso nacieron las extensiones: programitas que se les instalan, se acoplan al navegador y **les dan funcionalidades extra**. Pero son programas creados muchas veces por desconocidos, que tu adquieres en una tienda del navegador...que te da la misma seguridad que la de Android en cuenta a *malware*: **NINGUNA**. Así que mucho ojo con lo que instalas, no vaya a ser que te robe hasta las comas de tu contraseña...

En lo relativo a extensiones podemos consultar las que nuestro navegador tiene instaladas en las siguientes opciones:



Firefox:

The screenshot shows the Firefox Add-ons page. On the left, there's a sidebar with icons for General, Inicio, Buscar, Privacidad & Seguridad, Sincronización, and Más de Mozilla. Below this is a section for 'Extensiones y temas'. A red arrow points from this section towards the main content area. The main area has a header 'Administre sus extensiones' and a sub-header 'Habilitado'. It lists two extensions: 'NoScript' and 'uBlock Origin', both with toggle switches set to 'on'. To the right of each extension is a small description and a context menu with options like 'Eliminar', 'Preferencias', 'Informe', and 'Administrador'. At the bottom, it says 'Extensiones recomendadas'.

Figura 21. Las extensiones de mi Firefox. Estas dos son buenas, créeme 😊

Chrome:

The screenshot shows the Chrome Configuration page. On the left, there's a sidebar with various settings: Configuración, Tú y Google, Autocompletar y contraseñas, Privacidad y seguridad, Rendimiento, Aspecto, Buscador, Navegador predeterminado, Al iniciar, Idiomas, Descargas, Accesibilidad, Sistema, Restablecer configuración, Extensiones (which has a checked checkbox), and Información de Chrome. A red arrow points from the 'Extensiones' section towards the main content area. The main area has a header 'Extensiones' and shows two extensions: 'Documentos de Google sin conexión' and 'McAfee® WebAdvisor', each with a 'Detalles' button and a 'Quitar' button.

Figura 22. Extensiones de mi Chrome. Algunas vienen instaladas de serie o cuando compras el PC



En este caso cabe destacar que la extensión “Documentos de Google sin conexión” viene siempre instalada por defecto y no debemos borrarla si abrimos documentos de **Google Docs**.

Dentro de dichas opciones podemos encontrar la forma bastante sencilla de quitarlas si no vamos a usarlas más, o si no sabemos por qué están ahí. Pero ahora hablemos del tipo de extensión más interesante de todos: los bloqueadores de publicidad.

NOTA PREVIA MUY IMPORTANTE: Dado que las extensiones son software de terceros que podrían potencialmente ser vulneradas o tener problemas de seguridad, se recomienda que se instalen en un navegador aparte que solo usemos “para navegar” sin más, y que usemos otro distinto para leer el correo, compras, gestionar nuestras cuentas, etc. (es decir, operaciones que manejen datos económicos o privados) sin extensiones instaladas.

Esta advertencia se hace porque estas extensiones necesitan para funcionar legítimamente un acceso muy completo a las webs por las que navegamos y por tanto podrían leer información privada. Separarlas es la única forma de estar razonablemente seguro de que no habrá problemas en el futuro, y es aplicable tanto para esta extensión como para cualquiera que instalemos (incluidas las dos siguientes que veremos). También es compatible con las recomendaciones que damos en este curso.

Hecha esta aclaración, dejar claro que una cosa es limitar la información que puedan tener sobre nosotros las webs, para que no sepan nuestros hábitos y servirnos publicidad “personalizada”, y otra distinta el ver publicidad (personalizada o no, si una página tiene 8 anuncios veremos 8 anuncios, se adapten a nuestros supuestos gustos o no). Por suerte, también hay formas de eliminar todos o la mayoría de los anuncios que vemos en una página web, lo cual tiene una serie de ventajas más allá de las obvias:

- Nos concentraremos en los contenidos de la página y eliminamos elementos distractores
- No caeremos en hacer clic por error en anuncios potencialmente maliciosos
- La navegación será bastante más rápida (mostrar anuncios hace a tu PC trabajar más de lo que crees)

Una de las formas más populares de bloquear anuncios es instalar un complemento o extensión a nuestro navegador habitual. Todos los navegadores tienen extensiones pero, como decíamos, al igual que con las aplicaciones de los móviles, y de acuerdo con lo dicho antes en lo relativo a minimizar lo que instalamos, **NO es bueno instalar cualquiera**. ¡Algunas pueden tener/ser malware! Lo mejor es instalar aquellas que:

- Estén **recomendadas**/verificadas por el fabricante
- Tengan **muchos** (millones) de **usuarios**
- Tengan **muy buenas valoraciones**
- **No pidan demasiados permisos** (de nuevo, como con las aplicaciones del móvil)

Una extensión para bloquear publicidad que cumple con todas estas características es **uBlock Origin**, de Raymond Hill. Para instalarla (al igual que cualquier extensión) podemos ir a “**Complementos y Temas**” de la configuración de **Firefox** o navegar a esta dirección: <https://addons.mozilla.org/es/firefox/search/> y buscarla e instalarla desde allí



The screenshot shows the 'Details' tab of the uBlock Origin extension page. The extension icon is a shield with a white 'u' and 'b'. The title is 'uBlock Origin' with a 'verified' badge. Below it says 'Finally, an efficient blocker. Easy on CPU and memory.' A toggle switch is on the right. The 'Details' tab is selected, showing the following text:

uBlock Origin is not an "ad blocker", it's a wide-spectrum content blocker with CPU and memory efficiency as a primary feature.

Out of the box, these lists of filters are loaded and enforced:

- EasyList (ads)
- Peter Lowe's Ad server list (ads and tracking)
- EasyPrivacy (tracking)
- Malware domains

More lists are available for you to select if you wish:

- Fanboy's Enhanced Tracking List
- Dan Pollock's hosts file
- MVPS HOSTS
- Spam404
- And many others

Additionally, you can point-and-click to block JavaScript locally or globally, create your own global or local rules to override entries from filter lists, and many more advanced features.

Free.
Open source with public license (GPLv3)
For users by users.

Figura 23. Yo la verdad ya no puedo navegar sin él. Internet es un lugar menos hostil

O bien, si en lugar de Firefox usamos **Google Chrome**, ir a <https://chrome.google.com/webstore/category/extensions?hl=es> y buscarla allí:

The screenshot shows the 'uBlock Origin' extension page on the Google Chrome Web Store. The top navigation bar shows 'Inicio > Extensiones > uBlock Origin'. The extension icon is a shield with a white 'u' and 'b'. The title is 'uBlock Origin' and it says 'Ofrecido por: Raymond Hill (gorhill)'. It has a rating of ★★★★☆ 25,409 and categories 'Productividad' and '10.000.000+ usuarios'. A blue button on the right says 'Añadir a Chrome'. Below the header, there are tabs: 'Descripción general' (selected), 'Prácticas de privacidad', 'Reseñas', 'Ayuda', and 'Relacionados'. A large preview window shows a screenshot of a web browser with the uBlock Origin extension active, displaying a stats overlay with 'Blocked this page 72 or 14%', 'Demos completed 5 out of 22', 'Blocked since install 12,301 or 16%', and a note about not making age correlations. Below the tabs, there are two news cards: one about Ford F-150 vs Tesla Cybertruck and another about Mark Zuckerberg's fortune.

Figura 24. Mucho cuidado: Google quiere nerfeart las extensiones que bloquean publicidad porque les quita ingresos, así que no sé con qué te encontrarás en Chrome en el futuro en este aspecto...

O, en el caso de **Edge**, a <https://microsoftedge.Microsoft.com/addons/Microsoft-Edge-Extensions-Home> y buscarla allí también.



The screenshot shows the Microsoft Edge Add-ons page for the "uBlock Origin" extension. The extension is rated 4.5 stars (1347 reviews) and has over 5 million users. It is categorized under "Productividad". A large "Obtener" (Get) button is visible. The description section highlights its efficiency in blocking ads compared to other blockers like ABP. The details sidebar shows the version is 1.41.8, updated on February 28, 2022, and available in 58 languages.

Figura 25. Todo navegador que se precie tiene un bloqueador de publicidad. Unos integrado (como Brave) y otros instalable

La instalación es bastante simple en los tres casos, puesto que simplemente hay que darle al botón correspondiente. Los efectos son visibles de forma inmediata, por ejemplo, en la web del periódico *El País*:

The screenshot shows a news article from *El País* titled "Torra destituye a tres consejeros para satisfacer a la dura del independentismo". The article discusses the resignation of three ministers to satisfy the hard-line of the independence movement. Below the article is a video thumbnail showing a medical professional in protective gear performing a COVID-19 test on a person wearing a mask. The *EL PAÍS* logo is visible in the bottom right corner.

Figura 26. Hay un poco de periódico pegado a este anuncio

Después de la instalación del complemento, nos aparecerá así:



La crisis del coronavirus

Datos actualizados Casos en España y resto del mundo Situación global Expansión del virus en cada país App de rastreo Descárgate Radar-Covid Nueva Normalidad Buscador Avance del virus Evolución por provincias

Última hora · Podcast · Ver especial

Torra destituye a tres consejeros para satisfacer al ala dura del independentismo

PERE RÍOS | Barcelona 13

Los consejeros que ya han salido del Govern son los de Interior, Miquel Buch; la de Cultura, Mariàngela Vilallonga, y la de Empresa, Àngels Chacón

Tres nuevos consejeros a medida de Puigdemont



Personal sanitario hace el seguimiento de enfermo por coronavirus en Barcelona. A.G. (EFE)

Un estudio de 64.000 enfermos de covid en España

Figura 27. Now we are talking

NOTA: Esta extensión también elimina los anuncios de YouTube si lo ves desde el navegador donde la has instalado, si bien de vez en cuando YouTube la detecta y bloquea la visualización de videos o hace alguna movida del estilo. Está disponible en Firefox para móvil también.

Ejercicio MALTESTWEB: Mirar si una web es o no maliciosa

Descripción de la actividad

Necesitas saber si una web está **identificada como maliciosa** por Google

Resultados Esperados

Esta actividad se completará cuando puedas obtener un informe de Google Safe Browsing de cualquier URL que elijas.

Otra información necesaria para su realización

Google Safe Browsing escanea miles de millones de URL para localizar sitios web inseguros. Descubre miles de nuevos sitios inseguros diariamente, muchos de los cuales son sitios web legítimos que han sido pirateados. Cuando detecta sitios web inseguros, muestra advertencias en la Búsqueda de Google y en los navegadores web que utilizan esta tecnología. Además, puedes buscar manualmente una URL para ver si es peligroso visitar su sitio web aquí: <https://transparencyreport.google.com/safe-browsing/search>



Comprobar el estado de un sitio web

Estado actual

🟢 No se ha detectado contenido no seguro

Figura 28. Somos buenos 😊

Comprobar el estado de un sitio web

Estado actual

⚠ Este sitio web no es seguro

El sitio web https://irivoclub.000webhostapp.com incluye contenido dañino, como páginas que pueden:

- Intentar engañar a los visitantes para que compartan información personal o descarguen software

Recomendaciones

- **No te preocupes.**

Chrome y otros productos de Google tienen funciones de seguridad integradas para protegerte mientras navegas. [Más información](#)

- **Protégete**

Para obtener información sobre cómo protegerte de sitios web dañinos, visita el [Centro de seguridad de Google](#).

- **Obtén ayuda**

Descubre cómo limpiar tu sitio web y protegerlo de ataques futuros en los [artículos de ayuda sobre Navegación Segura para webmasters](#).

Información sobre el sitio web

Esta información se actualizó por última vez el 16 feb. 2019.

La seguridad del sitio web puede cambiar con el tiempo. Vuelve a consultar esta página para estar al día.

Figura 29. Estos otros no tanto 😞 (era una tienda fraudulenta)

Y recuerda que para saber el “pedigree” de una web (o su IP) tienes muchos más sitios en los que preguntar por ella (es como pedir referencias, vamos 😊):

- **Virustotal:** <https://www.virustotal.com/gui/home/url>
- **IP Reputation Check:** <https://www.abuseipdb.com/>
- **CyberGordon:** <https://cybergordon.com/>
- **URLScan:** <https://urlscan.io>



Uso de Redes Sociales

Ejercicio RRSSCONF: Configura bien tus cuentas de RRSS

Descripción de la actividad

Consiste en que examines las opciones de tu red social y para ver si permite hacer tu **cuenta privada**.

Resultados Esperados

Eres capaz de contestar a las siguientes preguntas:

- Ahora que tienes una cuenta privada ¿puedes controlar quién te añade?
- ¿Entiendes que ahora solo las personas que están añadidas a tu cuenta como amigos pueden ver lo que escribes, y por tanto te puedes sentir más libre?
- ¿Entiendes que siendo la cuenta privada no tienes restricción para leer otras cuentas públicas?

Otra información necesaria para su realización

Existen personas que **no están preparadas para el "clima" que hay en algunas redes sociales**, donde decir cosas, que en principio no se hacen con mala fe, pueden causarle un acoso y hostigamiento online que les puede provocar daño psicológico. En las redes sociales cada vez hay más usuarios que se dedican a tergiversar las cosas que otras personas escriben a propósito y a generar polémica, bien porque les conviene por alguna razón, o bien porque simplemente disfrutan con ello. A esos usuarios se les suele denominar coloquialmente **trolls**.

Un ejemplo muy reciente de ello son **los usuarios verificados** de Twitter (los del "check azul"), ya que esta gente recibe una compensación económica cuantas más interacciones consiga en la red. ¿Cómo va a hacerlo entonces? generando polémica para que mucha gente escriba. Este tweet por ejemplo ataque a la comunidad de los ingenieros del software a propósito para ello

RED FLAGS IN SOFTWARE ENGINEERS

- uses macOS
- uses ChatGPT
- drinks pour over coffee
- can't reverse a linked list
- uses more than 1 monitor
- tries new languages for "fun"
- doesn't push to prod on friday (live a little?)
- works on side projects outside of work
- actually does the mega backdoor Roth IRA
- builds mechanical keyboards (zero personality)
- makes less than 500k (borderline homeless)
- owns a mouse (use vim?)
- needs code reviews before merging (have some confidence)
- hobbies include "rock climbing" (grow up)
- uses languages with garbage collection (pick up after yourself?)
- actually reads documentation (i just threw up in my mouth a little)

Figura 30. Clásico ejemplo de ragebait. No entres al trapo, encima les das dinero. Bloquéalo y a pastar



En realidad el contenido de los mensajes no les importa, solo quieren interacciones que a cambio les dan dinero...

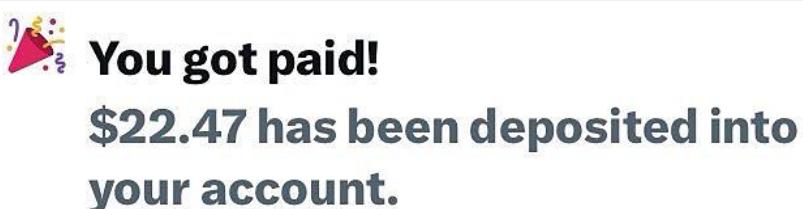


Figura 31. Wow, seguro que ya se puede comprar un Lambo

Uno siempre puede **bloquear un usuario en una red social** que le hace daño pero, cuando se juntan muchos a por ti (estas cosas pasan, y no pocas veces es un conocido/a el que "agita" por detrás), muchas veces la única solución **es hacer privada tu cuenta** y evitar que te lean o te puedan añadir sin tu consentimiento. Por eso es importante que aprendas a hacerlo, y que quizás si es las primeras veces que te inicias en una red social empieces ya directamente con tu cuenta privada hasta que vayas cogiendo confianza.



← Audience, media and tagging

Manage what information you allow other people on X to see.

Protect your posts



When selected, your posts and other account information are only visible to people who follow you. [Learn more](#)

Photo tagging



Anyone can tag you

Figura 32. En Twitter se llama "Proteger tus posts". En otros sitios directamente te dice "hacer tu cuenta privada"

Para hacer tu cuenta privada (o lo más privada posible) en las siguientes redes sociales sigue estas instrucciones:

- **Twitter:** <https://help.twitter.com/es/safety-and-security/how-to-make-twitter-private-and-public>
- **Instagram:** <https://www.xataka.com/basicos/como-hacer-privada-tu-cuenta-de-instagram>
- **Facebook:** <https://jessicaquero.com/facebook-privado/>
- **LinkedIn:** <https://triunfaconlinkedin.com/blog-linkedin/modo-privado-linkedin/>
- **TikTok:** <https://support.tiktok.com/es/account-and-privacy/account-privacy-settings/making-your-account-public-or-private>

El INCIBE te ofrece guías de cómo configurar bien tus redes sociales. Esto por ejemplo es lo que dice acerca de Instagram:



Figura 33. Instagram te puede servir como ejemplo, pero todas las redes sociales tienen más o menos las mismas opciones

Ejercicio RRSS_RESPORT: Reportar a alguien en una red social

clave Descripción de la actividad

Consiste en que identifiques los mecanismos existentes para **reportar cuentas en la red social que quieras**, porque estén escribiendo contenidos inadecuados, hagan amenazas o cualquier otro tipo de cosa que pueda consistir en un delito, rompa las normas de la propia red o sea un perjuicio para los demás.

clave Resultados Esperados

Tienes localizados y **sabes usar los mecanismos de denuncia de mensajes** que consideres inapropiados de cualquier red social en la que participes.

clave Otra información necesaria para su realización

Una cosa es cierta, el número de participantes en una red social en la actualidad es tan alto que, si no **colaboramos en moderar** los contenidos denunciando aquellas cosas que nos resulten dañinas o inapropiadas, la propia red **no va a poder reaccionar con agilidad** cuando existan este tipo de contenidos, ya que son demasiados.



Por tanto, aunque muchas redes tienen su propio equipo de moderación, confían en que los usuarios sean capaces de regular este tipo de contenidos mediante la denuncia de aquellas cosas que les parezcan inapropiadas.

 **Vamos a ser sinceros: también les sale más barato que seas tú el que lo reporte que no buscarlo ellos. Pero bueno, es lo que hay...**

En los siguientes enlaces tienes indicaciones acerca de cómo denunciar contenidos en cada una de las redes sociales más conocidas del mundo

- **Twitter:** <https://help.twitter.com/es/safety-and-security/report-abusive-behavior>
- **Facebook:** <https://es-es.facebook.com/help/263149623790594>
- **Instagram:** <https://es-es.facebook.com/help/instagram/370054663112398>
- **LinkedIn:** <https://www.linkedin.com/help/linkedin/answer/a549405/denunciar-una-pagina-de-linkedin?lang=es>
- **Tik Tok:** <https://support.tiktok.com/es/safety-hc/report-a-problem/report-a-user>

Las siguientes imágenes ilustran en proceso en **Instagram**. El primer paso es ir a las acciones sobre la publicación que queramos denunciar, entre las que se encuentra la de **Denunciar**:



Figura 34. ¿Troll? ¿Pornobot? ¿Estafa financiera? ¿Se ha pasado tres pueblos? Denuncia la publicación o la cuenta. Es anónimo, palabrita

Hecho esto, la red social nos preguntará por el **motivo de la denuncia**. Como se ve, hay una gran cantidad de motivos que cubren muchos posibles casos de contenido malicioso o destructivo. Según el motivo escogido, **se nos desplegarán más opciones** o no:

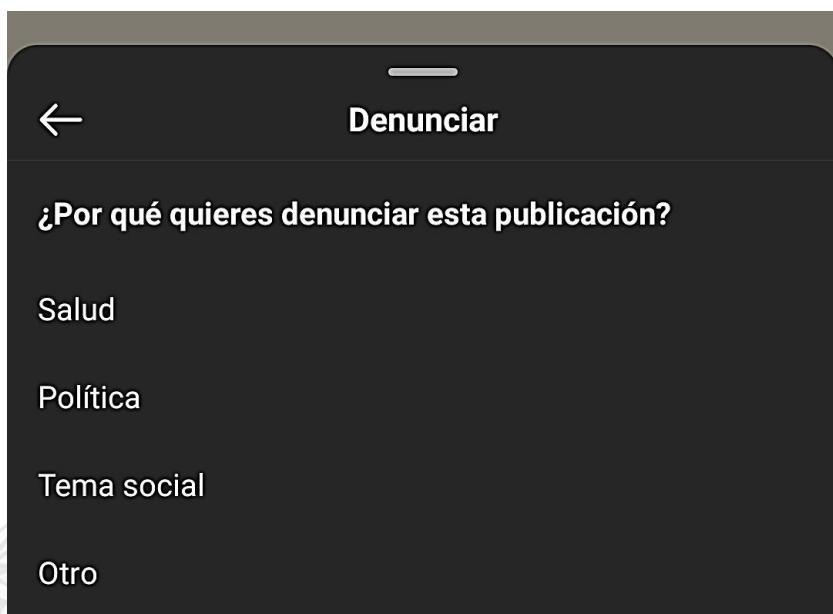


Figura 35. Cada red social tiene sus motivos de denuncia, pero bueno al final acaban siendo más o menos lo mismos en realidad, expresados de distintas formas

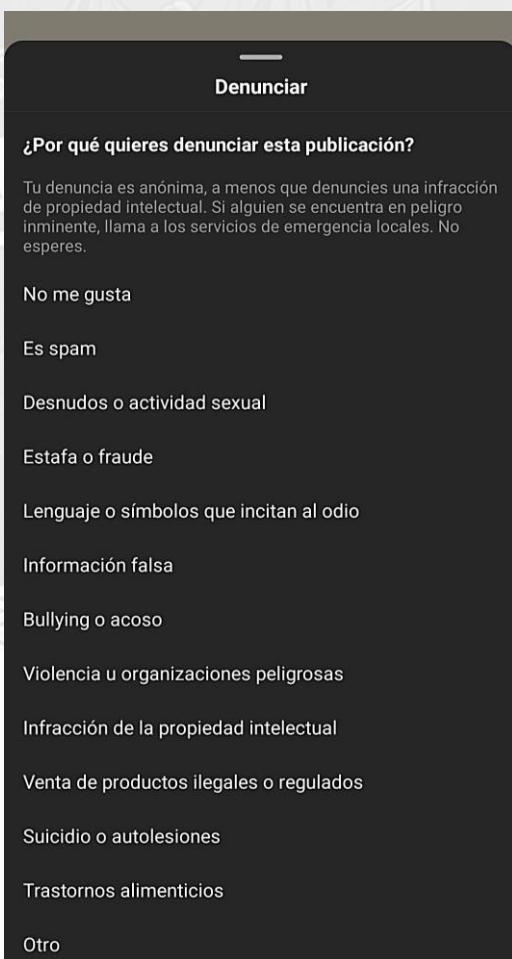


Figura 36. Esto te lo preguntan porque no todo tiene la misma prioridad. Es más prioritario quitar cierto tipo de posts que otros, y así los organizan para su revisión manual

Elegido el motivo, la denuncia estará hecha y la red social pasará a examinar si es pertinente o no:

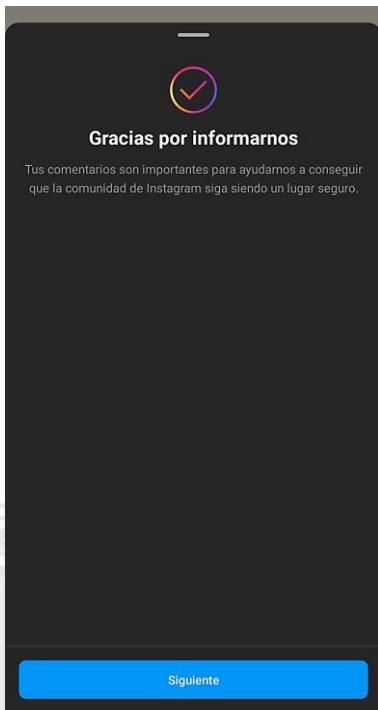


Figura 37. Informe enviado. Si hay muchos así, se le ha caído el pelo (y la cuenta)

Tras hacerlo, también nos dará la opción de **bloquear o restringir (silenciar) la cuenta denunciada**:

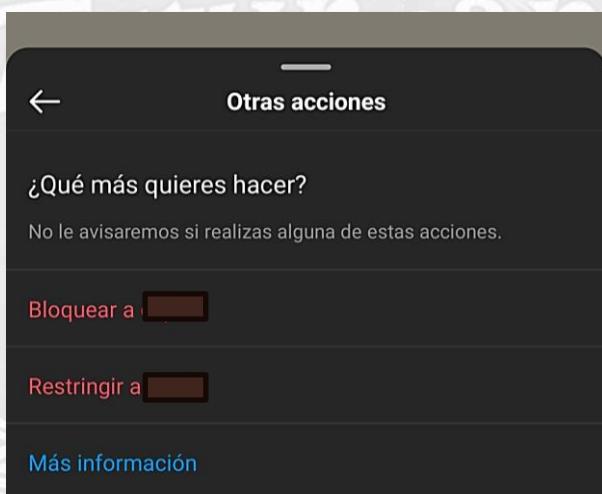


Figura 38. Si lo has denunciado lo más lógico es luego bloquearlo

Si elegimos bloquearla, se nos mostrará las acciones que esto lleva a cabo. La cuenta denunciada **no recibirá notificación de que la hemos bloqueado ni tampoco sabrá que la hemos denunciado**.

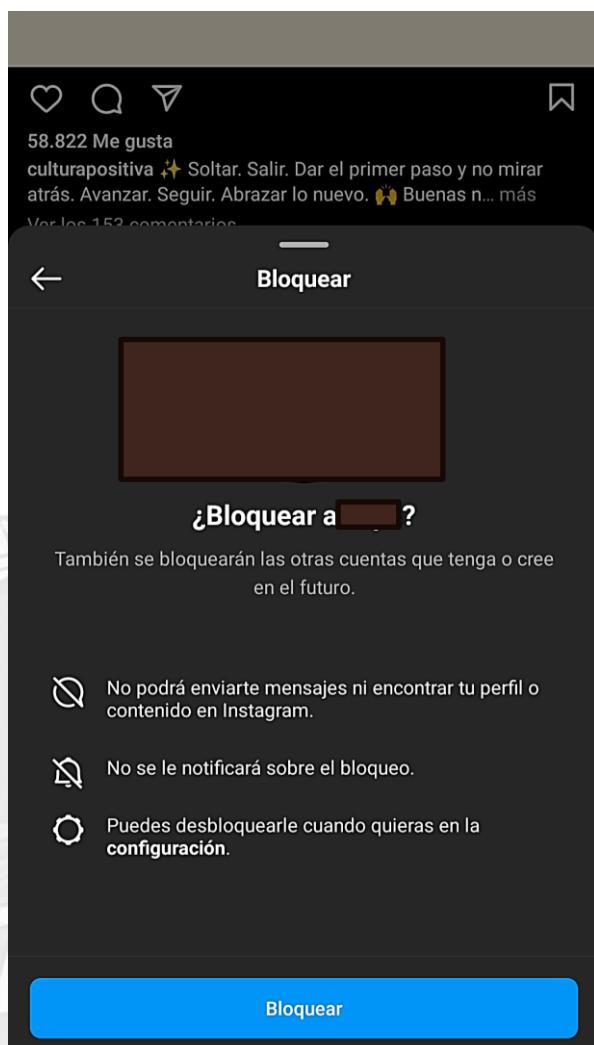


Figura 39. Y con esto, hasta luego

En el caso de **Twitter**, el proceso es similar. Al denunciar un mensaje haciendo clic en los ... que hay encima del mismo y usar la opción de menú adecuada:

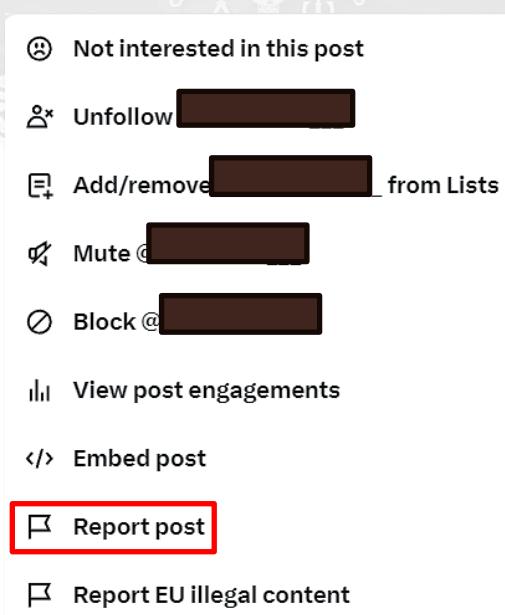


Figura 40. Te has pasado, espera que te mando un recaco



Se nos pedirá a continuación **la razón de la denuncia**, que en esta red puede ser cualquiera de las de esta imagen:

X Denunciar

¿Por qué lo denuncias?

No notificaremos al miembro sobre tu denuncia a menos que se trate de una infracción de propiedad intelectual.

Creo que es molesto o no me interesa →

He visto el mismo anuncio muchas veces →

Creo que es otra cosa diferente. →

Figura 41. La tercera opción es donde podemos precisar más

💡 Por cierto, últimamente si intentas reportar un anuncio Twitter te dice que noes y que pagues para no verlos 😞

Si decimos que es una cosa diferente, nos pedirá que especifiquemos exactamente qué es:

← Denunciar

Selecciona una razón para la denuncia:

Sospechoso, spam o falso →

Acoso o incitación al odio →

Violencia o agresión física →

Contenido para adultos →

Difamación o infracción de la propiedad intelectual →

Figura 42. El nº de razones para denunciar se ha ampliado últimamente

Cada razón seleccionada nos llevará a distintas razones más concretas, pero en el caso de que digamos que es **sospechoso, spam o falso**, tendremos estas opciones:



← Denunciar

¿Por qué es sospechoso, falso o spam?

Información errónea
Difunde información falsa o engañosa como si fuera real

Fraude o estafa
Engaña a otros para obtener dinero o acceder a información privada

Nuestras políticas prohíben:

- actividades ilegales o promoción o venta de productos ilegales
- virus, gusanos u otro software que puede destruir o interrumpir el funcionamiento de ordenadores o datos

[Más información](#)

No deseado (spam)
Comparte contenido irrelevante o repetido para generar visibilidad o ganancias económicas

Cuenta falsa
Representación imprecisa o engañosa

[Enviar](#)

Figura 43. Como ves, son esencialmente las mismas que Instagram

Con esto finalmente terminamos la denuncia y ahora Twitter podría ofrecernos bloquear la cuenta. También, **si la denuncia ha prosperado** porque otros usuarios han hecho lo mismo, **es posible que nos informe** en una notificación.

 **NOTA: No abuses de esta funcionalidad para reportar a todo el que te caiga mal sin dar un motivo aparente. Reportar a lo loco sin motivo aparente puede acabar con el reportador reportado por la propia red social. No obstante, si te planteas si algo puede ser o no una estafa, hay un canal de YouTube, @Coffeozilla, que habla de este tipo de cosas, y algunas son espeluznantes (un auténtico programa de "True Crime"): <https://www.youtube.com/@Coffeozilla/playlists>**



Uso de Sistemas de Mensajería

Email

Ejercicio CONSEJOS_ADJUNTOS: Mirar los consejos para defenderte de emails chungos

Descripción de la actividad

Consiste en que entiendas que **debes evitar a toda costa descargar ficheros adjuntos a tu máquina** y que, si tienes que verlos, mejor hazlo de manera online

Resultados Esperados

Puedes contestar a estas preguntas:

- ¿Entiendes que si abres un adjunto “con bicho” puedes estar en un problema grave?
- ¿Entiendes también que el problema ocurre si te lo descargas y lo abres en tu máquina fundamentalmente y que eso es lo que debes intentar evitar a toda costa?
- ¿Entiendes que antes de abrir nada en tu máquina te queda verlo de forma online?
- ¿Comprendes que esto es algo que debes divulgar y nunca quedarte para ti?

Otra información necesaria para su realización

Ante la proliferación de estafas de distintos tipos, la cantidad tan enorme de formas de engaño que existen, y todo lo que ello conlleva, para defenderse de la mayoría de ellas no queda más remedio que ser muy tajante con lo que hacemos: **NO se descarga nada a la máquina**. Punto. Ni siquiera hago distinción entre si te lo envía un conocido o no, porque no sabes si tu conocido tiene “bicho” y no lo sabe, y está propagando una infección sin saberlo, o alguien le ha robado la cuenta y está intentando estafarte

Eso de que un conocido lo suplanten para atacar a sus contactos es más común de lo que crees... 😱

Mira primero lo que el INCIBE tiene que contarte sobre el tema:

- <https://www.incibe.es/empresas/blog/riesgos-abrir-los-archivos-adjuntos-origen-desconocido-el-correo-electronico>
- <https://www.incibe.es/empresas/blog/evitar-incidentes-relacionados-los-archivos-adjuntos-al-correo>

Fíjate también en este cartel de concienciación:



ADJUNTOS MALICIOSOS

CÓMO IDENTIFICAR CORREOS ELECTRÓNICOS MALICIOSOS

1 El remitente

¿Lo conoces?

Es su dirección de correo habitual?
Comprueba la dirección detenidamente, puede que se parezca pero sea falsa.

No lo conoces

Precaución.

Cuerpo del correo

- Si es de un contacto conocido, comprueba que la firma se corresponda a la de correos anteriores.
- ¿Hay faltas de ortografía o errores gramaticales? Un correo legítimo no suele contener estos fallos.
- ¿Tiene demasiada urgencia en que hagas alguna acción? Táctica habitual de los ciberdelincuentes.

Archivos adjuntos

Comprueba la extensión del archivo.
Desconfía de aquellos que sean:

- .exe
- .vbs
- .docm
- .xlsm
- .pptm

Enlaces

El texto del enlace corresponde con el sitio al que vincula?
Los ciberdelincuentes suelen falsearlos para engañar a los usuarios.

Medidas de seguridad a tener en cuenta

Ante cualquier tipo de duda con un adjunto, **no abrirlo nunca**.
 Analizarlo con el antivirus o con herramientas en línea.
 Si se trata de un archivo Microsoft Office y lo abres, **nunca selecciones el botón habilitar edición**.
 Deshabilita las macros de Microsoft Office.
 Mantén siempre actualizado tu dispositivo.

017 TU AYUDA EN CIBERSEGURIDAD

Gobierno de España

VICEPRESIDENCIA
TECNICA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege
tuempresa

Figura 44. El INCIBE resume los problemas de ciberseguridad más comunes del día a día de forma brillante en sus infografías. Hazles caso. No es magia, son (literalmente) tus impuestos 😊



Yo voy a hacer dos puntuaciones más:

- Hay veces que no queda más remedio que abrir algo porque no tienes ningún indicio de que sea fraudulento. Vale, pero recuerda que puede ser de un conocido que tenga "bicho" en su máquina. Por eso, venga de donde venga, recuerda lo que dijimos en la teoría: "**Ver en el explorador**" siempre.
- Pongamos que es un documento de Office, has metido la pata (o cualquier otra razón), te lo descargas y lo abres. Bien, hagas lo que hagas, **NUNCA hagas clic en este botón**. Ese botón "detona" el "bicho" que lleva dentro:

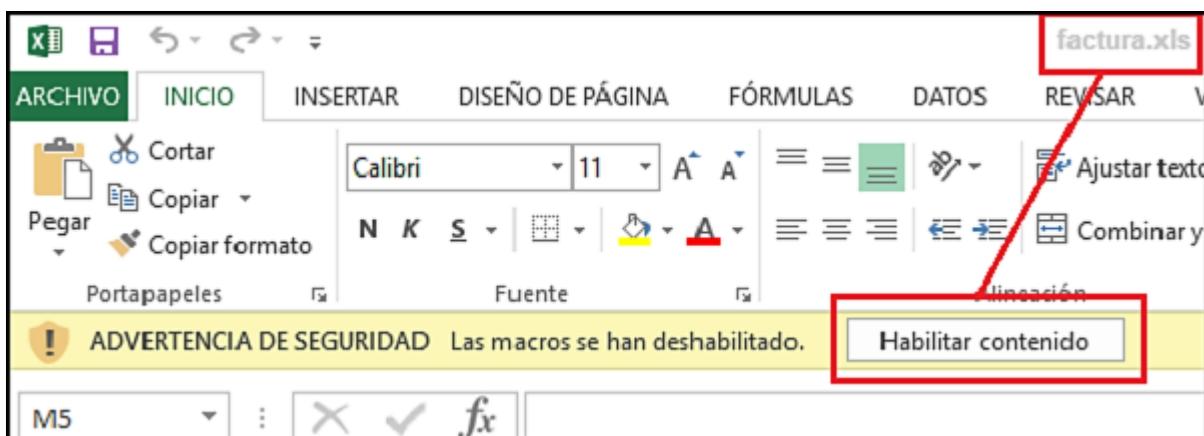


Figura 45. Da igual el programa de Office que sea. Este botón no se toca NUNCA., Por lo que pueda pasar. Fuente: <https://www.incibe.es/empresas/blog/evitar-incidentes-relacionados-los-archivos-adjuntos-al-correo>

Ejercicio PHISHREPORT: Usar las páginas que reportan phishing

Descripción de la actividad

Consiste en identificar y usar el sistema de tu cliente de correo que permite **denunciar un mensaje como spam**, para así contribuir a la limpieza mensajería general de dicho proveedor.

Resultados Esperados

Puedes **reportar un mensaje que consideras "basura"** como tal, e informar a tu proveedor de correo de que ese mensaje no es fiable.

Otra información necesaria para su realización

El sentido común es la última barrera contra los mensajes de *spam* que nos llegan a nuestra bandeja de entrada. Pero si, además de bloquear, **informas a tu proveedor de correo** de que ese mensaje es basura, entonces con suficientes informes negativos de muchos usuarios se incorporará automáticamente al algoritmo que usa tu proveedor de correo para identificar mensajes basura, de manera que con el tiempo no le volverá a llegar a nadie nunca más.

Dicho de otra forma: Este es un caso más en el cual, gracias a tu contribución, evitas que a otras personas les puede llegar algo que en caso de creérselo puede acabar en una estafa.

Los siguientes enlaces muestran cómo hacerlo:

José Manuel Redondo López. Proyecto "F-74 'Asturias'"



- **Outlook:** https://answers.microsoft.com/es-es/outlook_com/forum/all/c%C3%B3mo-reportar-el-abuso-o-spam-en-outlookcom/705f661d-d139-47b4-a9c1-ae22ead9b3f

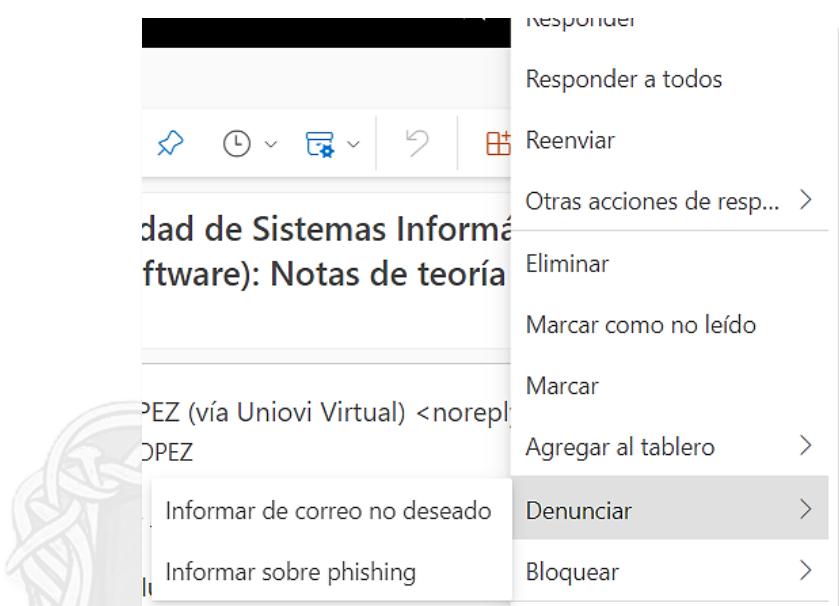


Figura 46. ¡Un tal José Manuel Redondo me está enviando spam de una asignatura! Denunciado (tranquis no lo hice 😊, es solo para enseñaros la opción)

- **Gmail:** <https://support.google.com/mail/answer/8151?hl=es&co=GENIE.Platform%3DAndroid> (opciones "Eliminar el spam de mi bandeja de entrada" y "Un correo sospechoso solicita información personal")

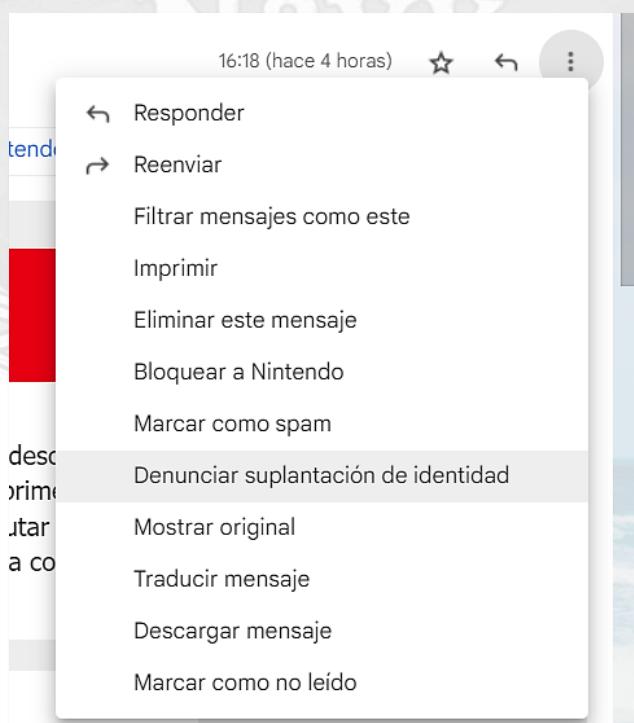


Figura 47. Todos los proveedores de correo tienen una opción de estas. Si les ayudas a "limpiar", les beneficias



Aplicaciones de Mensajería

Ejercicio WHATSCONF: Mirar algunas configuraciones típicas de WhatsApp a ver como las tienes

Descripción de la actividad

Consiste en aprender a **configurar las opciones de seguridad** de tu programa de mensajería para evitar problemas comunes.

Resultados Esperados

Puedes contestar estas preguntas:

- *¿Sabías que los programas de mensajería tenían tantas opciones de seguridad?*
- *¿Tenías tu programa de mensajería bien configurado?*
- *¿Crees que con los cambios que has hecho estás más seguro? ¿Recomendarías alguno de esos cambios a cualquiera de tus allegados?*

Otra información necesaria para su realización

Se trata de habilitar la configuración de seguridad de tu programa de mensajería, lo que incluye:

- **Verificación de contactos**
- **Notificaciones de seguridad**
- Usar **cifrado extremo a extremo**
- **Deshabilitar las funciones opcionales que no son de seguridad**: confirmación de lectura, informar de cuando es la última vez que se estaba en línea y el aviso de escritura.
- Si la aplicación admite la sincronización en la nube para el acceso a través de un **complemento de escritorio** o aplicación web (Ej.: WhatsApp Web), esto aumenta la superficie de ataque y, por lo tanto, debería deshabilitarse, salvo que sea para hacer copias de seguridad de tu información, en cuyo caso hay que pensarse mucho qué hacer.

En el caso de WhatsApp, las siguientes pantallas muestran cómo se puede acceder a esas opciones, a partir de la pantalla de **Ajustes** de este programa:



Figura 48. Estas dos opciones son las importantes en este caso

En la opción de **Cuenta**, podemos ver las siguientes opciones:

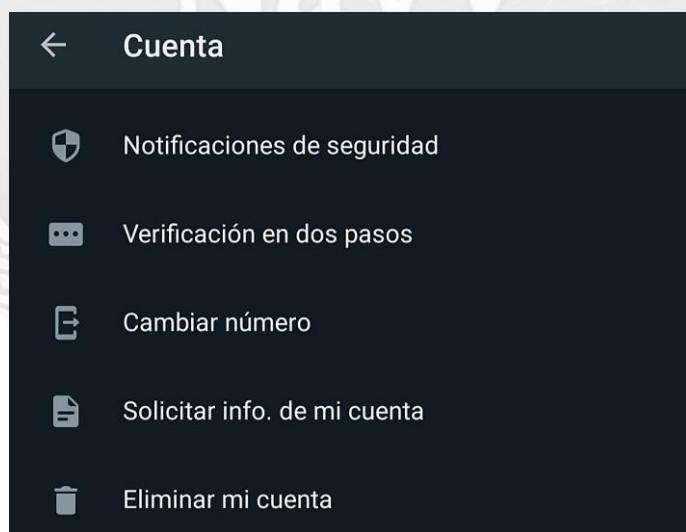


Figura 49. Cuidado con la última opción (por suerte pregunta si le das por error)

El primer apartado, de “**Notificaciones de seguridad**” podemos activar que el programa nos avise cuando alguien **cambia su dispositivo o reinstala el WhatsApp**, momento en el cual cambiará la información que se usa para mandar la información cifrada entre ambos y también se puede detectar posibles suplantaciones o robos si el interlocutor no ha hecho esas operaciones.



Figura 50. Esto es también una forma de saber si un/una colega ha cambiado de teléfono 😊

Activar esta notificación hace que cuando el interlocutor cambie de teléfono o reinstale el WhatsApp veamos esto en su pantalla de mensajes:

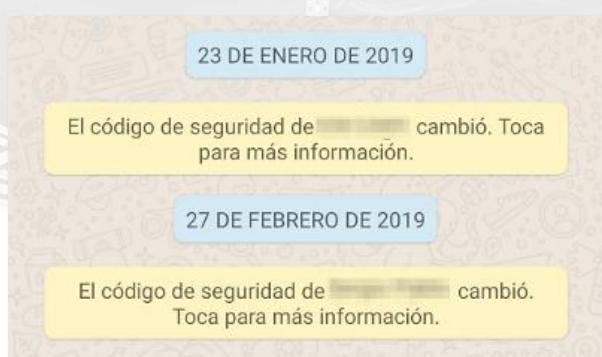


Figura 51. Aquí solo hay dos opciones: Teléfono nuevo o reinstalación del WhatsApp

La “**Verificación en dos pasos**” es un mecanismo por el cual podemos exigir introducir un código adicional que recibiremos en nuestro teléfono si alguien intenta entrar en nuestra cuenta de forma maliciosa. Puedes consultarla aquí si te interesa: <https://faq.whatsapp.com/1920866721452534/>



Figura 52. Muchas estafas tratan de engañarte para que les des tu contraseña y asignar tu WhatsApp a otro nº de teléfono (robártelo, vamos). Con esto ya no es tan fácil

Otra cosa que debes tener en cuenta dentro de la opción **Cuenta** es que para **cambiar de nº de teléfono** asociado a WhatsApp no puedes hacer de cualquier forma, sino con la opción correspondiente que aparece aquí:

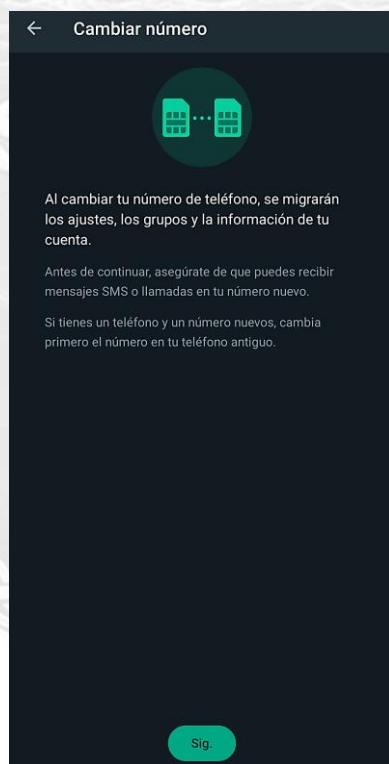


Figura 53. Tu cuenta de WhatsApp y tu nº de teléfono están "casados", pero se pueden "divorciar" y buscar otra pareja 😊. El problema es que los delincuentes lo aprovechan para estafar 😥

Pero las opciones más interesantes desde el punto de de "Privacidad" son las de la lista que mencionamos antes: elegir **quién puede ver nuestro estado conectado**, nuestra **foto de perfil**, la **información** que damos en nuestro perfil y nuestro **estado actual**. Aquí tendríamos que intentar restringir lo máximo posible quién ve estos datos.



Figura 54. Si desactivas esto, ya no te pueden acusar de "dejar en visto". Claro que entonces tu tampoco verás si los demás te lo hacen...



Figura 55. Si eres de los/as que cuenta tus estados de WhatsApp, igual te conviene restringirlo un poco 😊



Figura 56. Básicamente compórtate de forma responsable de la misma forma que lo harías en una red social



Finalmente, en la opción “**Chat**” la opción relacionada con la seguridad más relevante es gestionar las copias de seguridad de nuestros mensajes. **Normalmente se hacen sobre la cuenta de Gmail**, siempre que tengamos espacio disponible. No obstante, conviene recordar que hacerlo implica que **estaremos cediendo nuestros mensajes, fotos, etc. a Google** para sus estudios de mercado, etc.

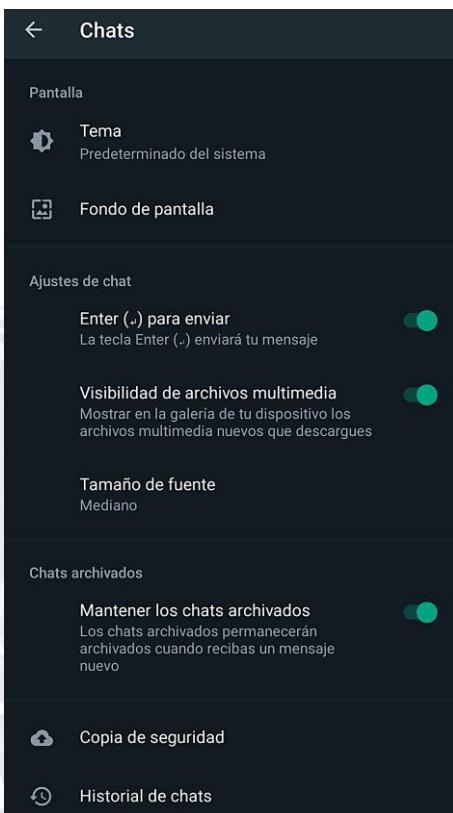


Figura 57. Las copias de seguridad salvan vidas. Y facilitan cambiar de teléfono también

En el caso de **Telegram** sería esta pantalla la que da acceso a las opciones equivalentes que hemos visto en **WhatsApp**. Podemos experimentar con ellas usando lo que ya sabemos, o seguir tutoriales como estos:

- <https://telegram.org/faq/es>
- <https://www.xataka.com/basicas/como-ocultarte-al-maximo-telegram-guia-para-maximizar-tu-privacidad>
- <https://www.xatakamovil.com/aplicaciones/nueve-consejos-para-mejorar-privacidad-seguridad-telegram>



← Privacidad y seguridad	
Privacidad	
Bloqueados	2
Número de teléfono	Nadie (+5)
Última vez y en línea	Nadie
Fotos y videos de perfil	Mis contactos
Mensajes reenviados	Nadie
Llamadas	Mis contactos
Grupos y canales	Mis contactos
Elige quién puede añadirete a grupos y canales.	
Seguridad	
Código de bloqueo	
Verificación en dos pasos	Activada
Dispositivos	
Gestiona tus sesiones en todos tus dispositivos.	
Eliminar mi cuenta	
Si estoy fuera	6 meses

Figura 58. Entre Telegram y WhatsApp hay pocas diferencias. Pero no tienes que dar tu teléfono y tiene muchos foros de temas que te puedan interesar

Ejercicio PWDCHAT: Protege un chat con clave

Descripción de la actividad

Consiste en que entiendas que puedes hacer que ciertos chats de tus aplicaciones de mensajería **sean realmente privados**, y de esta forma preservar tu intimidad.

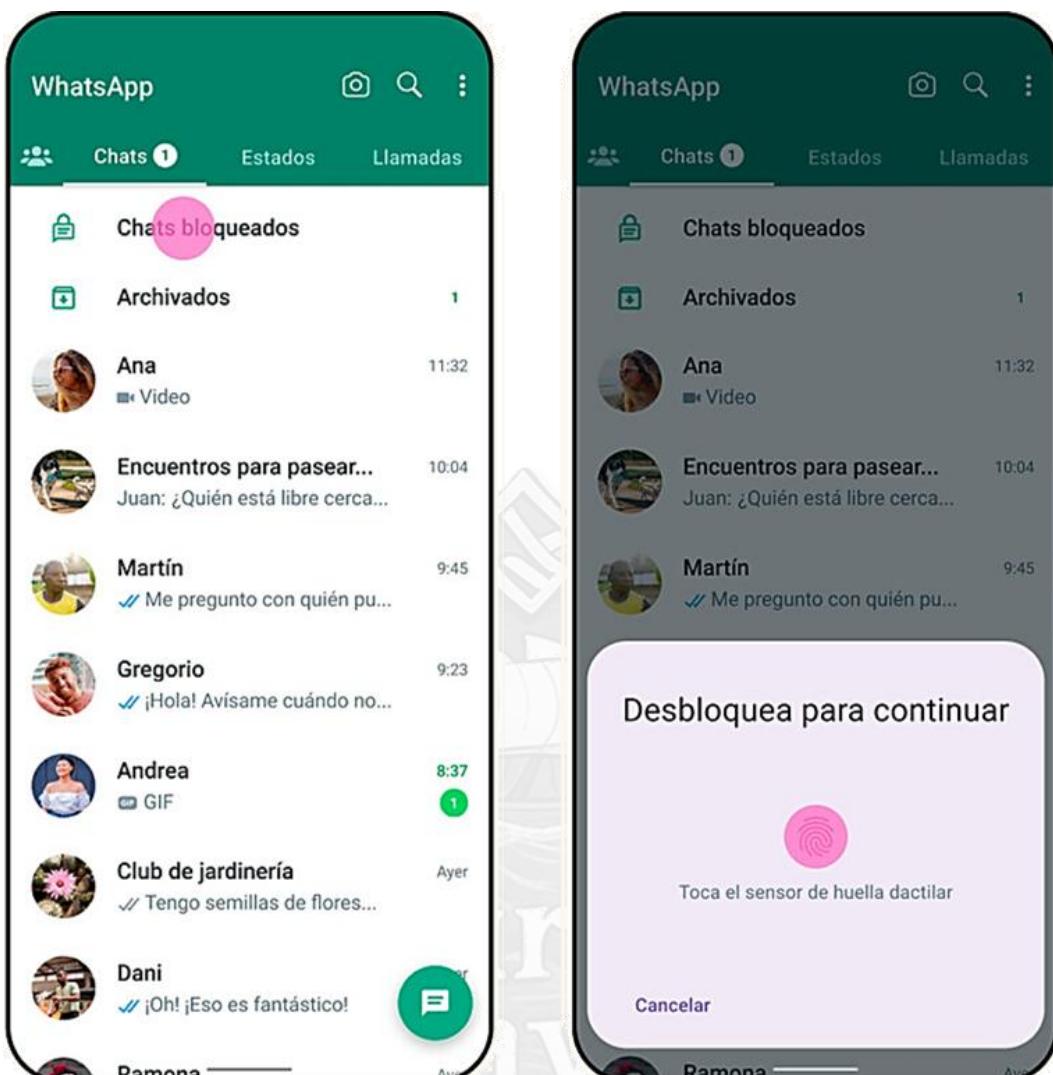
Resultados Esperados

Puedes contestar a las siguientes preguntas:

- ¿Entiendes que tienes derecho a la privacidad y la intimidad y que ahora tienes medios para preservarla realmente?
- ¿Comprendes también que no debes usar esta funcionalidad para ocultar actividades delictivas, de dudosa ética o bien peticiones de gente que se puedan categorizar así?
- ¿Comprendes que estos chats privados son también una herramienta para los *groomers* y sus víctimas y que no debes caer en esa dinámica?

Otra información necesaria para su realización

Literalmente la función de la que te hablo no tiene mucho que entender. Es un hilo de conversación con alguien que mantienes privado porque **la única forma de leerlo es desbloquearlo de alguna forma que solo tu sepas**: contraseña, huella.... La imagen siguiente tiene un ejemplo, y en el artículo referenciado tienes como se hace paso a paso.



Esta opción es importante y no la conoce tanta gente como debería. Fuente:

<https://www.xataka.com/aplicaciones/whatsapp-ahora-te-permite-proteger-chats-que-quieras-contraseña-asi-funciona-opcion-bloquear>

Esta funcionalidad es ya algo común y te lo explican los periódicos generalistas incluso. Si no se usa más es porque no ha llegado a todos los posibles interesados que puede hacerse algo así 😊:

<https://www.20minutos.es/tecnologia/aplicaciones/como-proteger-chats-whatsapp-contraseña-huella-reconocimiento-facial-5174562/>



⚙️ Dispositivos de Computación

📱 Telefonía Móvil

🛠️ Ejercicio MOVILCONF: Consultar lo que tiene el INCIBE para configurar tu móvil bien

👤 Descripción de la actividad

Esta actividad quiere darte una serie de sitios con información para que **puedas configurar tu móvil de manera adecuada y segura**, algo que no es en absoluto fácil, pero que leyendo de las fuentes correctas puede ser asequible para todo el mundo con un poco de paciencia 😊 . ¡Tú puedes!

🏆 Resultados Esperados

Puedes contestar a la siguiente pregunta: ¿Entiendes que normalmente un teléfono, tal y como sale de la tienda y lo arrancas, no está precisamente en su configuración más segura, y que hay que darle una vuelta para no caer en determinados problemas?

📋 Otra información necesaria para su realización

Es muy difícil explicar en pocas palabras cómo configurar adecuadamente un teléfono móvil de manera que se entienda. Por suerte para nosotros **el INCIBE tiene disponible públicamente el material de formación que necesitamos para ello**, y que podemos consultar para saber si nuestra configuración actual es adecuada y en caso de que no saber lo que nos falta.

En la siguiente web te cuentan un poco lo más importante: <https://www.incibe.es/menores/tematicas/uso-y-configuracion-segura>. Por otro lado en este enlace tienes una serie de infografías que te enseñan a tocar los parámetros más relevantes para mejorar tu seguridad: <https://www.incibe.es/ciudadania/formacion/guias/guia-para-configurar-dispositivos-moviles>

FICHA	iOS	Android
1. Móvil nuevo en la mano, ¿y ahora qué? Elige un idioma Conéctate a una red wifi Vincula tu cuenta de Google Actualiza el software		
2. ¡Qué nadie lo use sin tu permiso! Establece contraseñas seguras Doble factor de autenticación		
3. Conexiones siempre seguras Configuraciones de redes inalámbricas		
4. Protección contra virus y fraudes Antivirus Actualización de software		
5. ¡No pierdas tu información y protégela! Copias de seguridad Cifrado		

Figura 59. Un problema, una ficha explicativa, para iOS y Android. ¡Así si se pueden hacer las cosas! :)



Si esto te parece demasiado complejo también hay una infografía que te enseña lo mínimo que por lo menos puedes usar en primera instancia para tener algo rápido que luego cuando tengas algo más de tiempo y paciencia ponerte a configurar las cosas con más detalle siguiendo el ejemplo anterior

5 consejos para mejorar la seguridad y privacidad en dispositivos móviles

1 Protege el acceso a tu dispositivo
Utiliza contraseñas robustas y mecanismos seguros de desbloqueo

En Ajustes > Seguridad y Ubicación > Bloqueo de pantalla > Contraseña / Huella digital o Smart Lock > Reconocimiento facial.

	PIN	Contraseña alfanumérica	Patrón	Huella dactilar	Reconocimiento facial
Android	✓	✓	✓	✓	✓
iOS	✓	✗	✗	✓	✓

2 Comprueba que tu dispositivo está actualizado ✓

Ajustes > Sistema > Ajustes avanzados > Actualización del sistema.

3 Haz copias de seguridad y cifra tu dispositivo
para salvaguardar tu información

COPIA DE SEGURIDAD
En Ajustes > Google > Hacer copia de seguridad > Crear una copia de seguridad.

CIFRADO
El cifrado se hace por defecto, aunque podemos cifrar una memoria externa en Ajustes > Seguridad y ubicación > Cifrar almacenamiento de tarjeta SD.

iOS

COPIA DE SEGURIDAD
En Ajustes > [nombre] > [seleccionar el dispositivo] > Copia en iCloud > Realizar copia de seguridad ahora.
Al habilitar la opción se realizarán automáticamente.

CIFRADO
El cifrado se hace por defecto.

4 Descarga e instala
Instala aplicaciones seguras desde tiendas oficiales, como Play Store o App Store.
Revisa los permisos de las apps descargadas:

Android: en Ajustes > Aplicaciones selecciona la app y haz clic en Permisos para desactivar y activar los que consideres.

iOS: en Ajustes encontrarás las aplicaciones instaladas, selecciona la que quieras y podrás desactivar los permisos.

5 Activa la verificación en dos pasos o doble factor de autenticación. Añade una capa extra de seguridad a tus cuentas

Ajustes > Google > Gestionar tu cuenta de Google > Seguridad > Verificación en dos pasos > Empezar.

Recuerda que ponemos a tu disposición la Línea de Ayuda en Ciberseguridad de INCIBE 017, gratuita y confidencial, para cualquier cuestión relacionada con la ciberseguridad.

iOS 10.3 o SUPERIOR:
Ajustes > [nombre] > Contraseña y seguridad > Activar autenticación de doble factor > Continuar.

iOS 10.2:
Ajustes > [Apple ID] > Contraseña y seguridad > Activar autenticación de doble factor > Continuar.

www.incibe.es | www.osi.es

Gobierno de España | Vicepresidencia Tercera del Gobierno | Ministerio de Asuntos Económicos y Transformación Digital | Secretaría de Estado de Digitalización e Inteligencia Artificial | INSTITUTO NACIONAL DE CIBERSEGURIDAD | Oficina de Seguridad del Internauta

Figura 60. Aquí tienes un resumen de lo mínimo a hacer con tu teléfono y su configuración

<https://www.incibe.es/ciudadania/formacion/infografias/5-consejos-para-mejorar-la-seguridad-y-privacidad-en-dispositivos-moviles>



🛠 Ejercicio PLAYSTORE_OK: Mirar alguna aplicación con buena pinta en la Play Store

💻 Descripción de la actividad

Es muy importante que sepas distinguir una aplicación fiable de una que no lo es, ahora que has entendido que **el hecho de estar en una tienda oficial no te garantiza nada**. Esta actividad quiere ayudarte a que lo hagas.

🏆 Resultados Esperados

Puedes contestar a las siguientes preguntas

- ¿Entiendes los criterios que deben seguirse a la hora de instalar o no instalar una aplicación en tu teléfono móvil
- ¿Te das cuenta de que realmente cualquiera puede subir una aplicación a una tienda oficial, porque los fabricantes de móviles viven en parte de eso, y que eso hace que las tiendas nunca vayan a ser fiables del todo?
- ¿Sabías que la tienda de *Apple* es bastante más fiable que la de *Android*, pero ni aun así puedes tener un 100% de seguridad, ya que siempre puede haber alguien que engañe a los controles que se hacen en las tiendas?

▣ Otra información necesaria para su realización

Voy a ponerte un ejemplo de una aplicación fiable en la *Play Store* de *Android* y luego, cuando leas una infografía que he puesto un poco más abajo, quiero que reflexiones y **veas por ti mismo si esta aplicación resulta fiable o no de acuerdo a esos criterios**. Olvídate de que sea una aplicación muy conocida usa esto como ejemplo de en qué casos puedes tener cierta seguridad a la hora de instalarlas o no. La aplicación es esta: <https://play.google.com/store/apps/details?id=com.netflix.mediaclient&hl=es>



Figura 61. Nº de valoraciones (reseñas), nº de descargas, quien es el autor (si es conocido o no)...

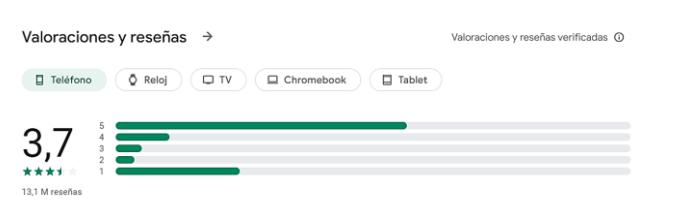


Figura 62. Cuando la puntuación baja de 4 estrellas, conviene leer las más bajas un poco a ver si hay una mención a virus o similar, o si solo es mal funcionamiento u otras críticas del servicio distintas

José Manuel Redondo López. Proyecto "F-74 'Asturias'"



No obstante, es importante que te quede claro que uno de los mayores indicios de que una aplicación no es de fiar son los permisos que te pide. El INCIBE te habla de ello aquí: <https://www.incibe.es/ciudadania/formaci%C3%B3n/actividades/acepto-no-acepto>, pero esta infografía es muy buena para saber lo que puede pasarte en función de lo que aceptas o no:



Figura 63. Cada permiso es una puerta a un posible problema de seguridad. ¡Mucho cuidado!. Fuente: <https://www.incibe.es/ciudadania/formacion/infografias/permisos-de-apps-y-riesgos-para-tu-privacidad>

¿Y qué pasa si te has equivocado y has instalado algo chungo? El INCIBE te lo explica aquí:

José Manuel Redondo López. Proyecto "F-74 'Asturias"



Instalé una app no fiable
¿Alguna vez te has descargado una aplicación móvil maliciosa o no fiable?

Estás buscando una aplicación de la que has oido hablar por Internet. De pronto, la encuentras a través de un enlace de descarga de una web, la instalas y la inicias. Sin embargo, no ocurre lo que esperabas y tu dispositivo empieza a actuar de forma extraña.

¿Qué puedes hacer?

El primer paso es desinstalarla del dispositivo. Tener en cuenta las siguientes recomendaciones para que esto no te vuelva a suceder.

Prevención y protección de tu dispositivo
Ten un antivirus instalado

Protege tu dispositivo de diversas amenazas y aplicaciones maliciosas. En la sección de herramientas gratuitas de OSI encontrarás algunas para Android e iOS.

www.osi.es

DESCARGA

En tiendas oficiales

Las plataformas Google Play o AppStore cuentan con medidas de seguridad para evitar aplicaciones fraudulentas.

Descarga Disponible Google play Descarga Disponible App Store

1. Revisa quién es el desarrollador de la app. Las empresas o desarrolladores conocidos en teoría ofrecen más garantías de seguridad. Chequea que redirigen a un sitio seguro y profesional.

2. Echa un vistazo a los comentarios. Si tiene pocos comentarios y todos positivos, o si tiene muchos y negativos... ¡Desconfíal!

3. Comprueba el número de descargas. Una app famosa con pocas descargas puede significar que nos encontramos ante una copia de la misma poco fiable.

Además de las recomendaciones anteriores, mantener nuestros móviles actualizados a la última versión de las aplicaciones y del sistema operativo nos ayudará a bloquear las posibles ventanas por las que los ciberdelincuentes puedan acceder a la información almacenada.

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD
@INCIBE
INCIBE

Mantente al día con nuestras campañas de concienciación para estar informado. ¡Es nuestra mejor defensa!

www.incibe.es | www.osi.es

osi Oficina de Seguridad del Internauta
@osiseguridad
osiseguridad

Figura 64. Consejos del INCIBE con la instalación de aplicaciones. El INCIBE sabe, hazle caso al INCIBE. Fuente: <https://www.incibe.es/ciudadania/formacion/infografias/instale-app-no-fiable>



Ordenadores

Ejercicio WINDEF: Sácale partido al Windows Defender

Descripción de la actividad

Consiste en comprobar que realmente tienes un servicio que **está vigilando si algún malware ha entrado en tu sistema**

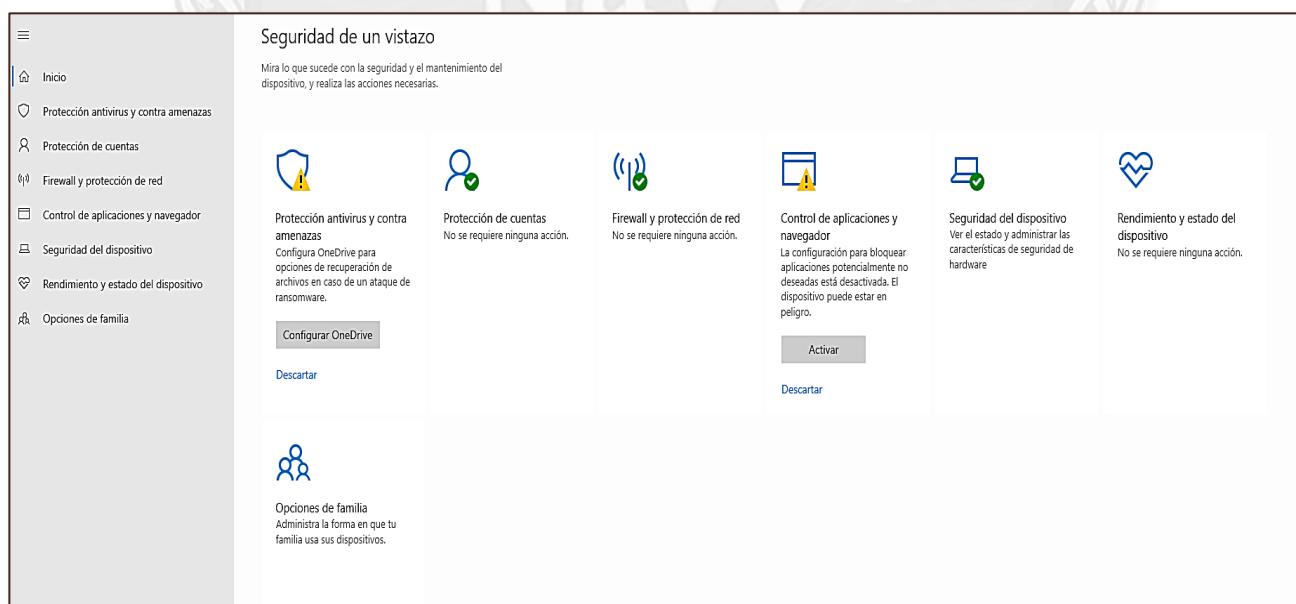
Resultados Esperados

Puedes contestar estas preguntas:

- ¿Consideras que el servicio contra *malware* de *Windows* es adecuado (en el sentido de que hace su trabajo sin ralentizar demasiado el tuyo)?
- ¿Alguna vez te has encontrado con un aviso o interferencia del sistema antimalware de *Windows*, es decir, te ha librado de una buena?

Otra información necesaria para su realización

Una de las mejores decisiones de *Microsoft* de cara a mejorar la seguridad de los sistemas *Windows* es **integrar gratuitamente una solución de seguridad muy buena, consistente en un antimalware y un firewall** bajo la marca “*Windows Defender*”. A pesar de venir incluido de serie de forma gratuita, este producto obtiene unas altas valoraciones y se trata de una solución equivalente a otras de pago existentes en el mercado. Aunque se instala de serie, sí que es posible que **no venga completamente configurado** si no revisamos su estado. Por ejemplo, es típico encontrarse con esto:



The screenshot shows the Windows Defender Security Center. On the left is a navigation pane with links like Inicio, Protección antivirus y contra amenazas, Firewall y protección de red, Control de aplicaciones y navegador, Seguridad del dispositivo, Rendimiento y estado del dispositivo, and Opciones de familia. The main area is titled "Seguridad de un vistazo" and contains five cards with status icons and descriptions:

- Protección antivirus y contra amenazas:** Configura OneDrive para opciones de recuperación de archivos en caso de un ataque de ransomware. Buttons: "Configurar OneDrive" (highlighted), "Activar", and "Descartar".
- Protección de cuentas:** No se requiere ninguna acción.
- Firewall y protección de red:** No se requiere ninguna acción.
- Control de aplicaciones y navegador:** La configuración para bloquear aplicaciones potencialmente no deseadas está desactivada. El dispositivo puede estar en peligro. Buttons: "Activar" (highlighted) and "Descartar".
- Seguridad del dispositivo:** Ver el estado y administrar las características de seguridad de hardware. Buttons: "Activar" and "Descartar".
- Rendimiento y estado del dispositivo:** No se requiere ninguna acción.

At the bottom is a section titled "Opciones de familia" with the subtext "Administra la forma en que tu familia usa sus dispositivos".

Figura 65. Típico estado de Windows Defender cuando lo arrancas y no has hecho nada más con él nunca

- **La opción de protección antivirus y contra amenazas** configura nuestra cuenta de *OneDrive* para hacer una copia de seguridad de nuestros archivos más importantes en la nube, de manera que en caso de ataque de *ransomware* o similar podamos recuperarlos en una gran parte de casos. Dado que las cuentas de *OneDrive* son gratuitas, se recomienda su activación por los beneficios que tiene.



- La opción de control de aplicaciones y navegador previene una serie de casos en donde se nos pueden instalar aplicaciones no deseadas, como por ejemplo descargadas por accidente de correos o webs no fiables. Conviene activarla también.

Finalmente, ¿Te preocupa no tener tu Windows bien configurado porque no sabes cómo hacerlo? Es un tema complicado y da respeto, porque realmente no es sencillo. Por suerte el INCIBE te cuenta lo más importante en esta infografía: <https://www.incibe.es/ciudadania/formacion/infografias/top-10-configurationes-basicas-para-windows-10>

1 Ajustar la privacidad en nuestro equipo.
Desde Configuración > Privacidad > General.

2 Controlar los datos que enviamos.
Desde Configuración > Privacidad > Comentarios y diagnósticos.

3 Controlar los permisos de las apps.
Desde Configuración > Privacidad.

4 Desactivar la reproducción automática.
Desde Configuración > Dispositivos.

5 Desinstalar software no deseado.
Desde Configuración > Aplicaciones.

6 Mantenerse actualizado.

7 Activar el antivirus y firewall.

8 Habilitar la restauración del sistema.

9 Configurar Cortana.

10 Cifrar tu sistema.

Figura 66. Configurar bien el Windows es difícil, pero por suerte lo mínimo es accesible gracias al INCIBE

Ejercicio VIRUSTOTAL: Analizar algo con Virustotal

Descripción de la actividad

Necesitas escanear URL sospechosas para ver si apuntan a una web maliciosa conocida o bien un fichero que te has descargado y no te fías de él

Resultados Esperados

Esta actividad se completará cuando puedas obtener informes de una URL o ejecutable de Virustotal.

Otra información necesaria para su realización

Virustotal es un servicio web (<https://www.virustotal.com/gui/home/upload>) que escanea cualquier archivo que se le cargue en busca de malware conocido, utilizando más de 50 motores antivirus diferentes.



También **escanea URLs** para detectar la presencia de *malware* conocido en las páginas que designan (<https://www.virustotal.com/gui/home/url>). Se puede utilizar para

- Aumentar la certeza sobre la seguridad de un archivo o documento ejecutable desconocido que estás considerando abrir.
- Probar un archivo de tu máquina para ver si está infectado (eso puede indicar que hay una infección más grande en tu sistema).
- Aumentar la certeza de que una URL que vas a visitar no oculta potencialmente malware.

Para realizar esta actividad, debes cargar y escanear con el servicio un ejecutable que elijas. Además, también debes inspeccionar la URL que quieras.

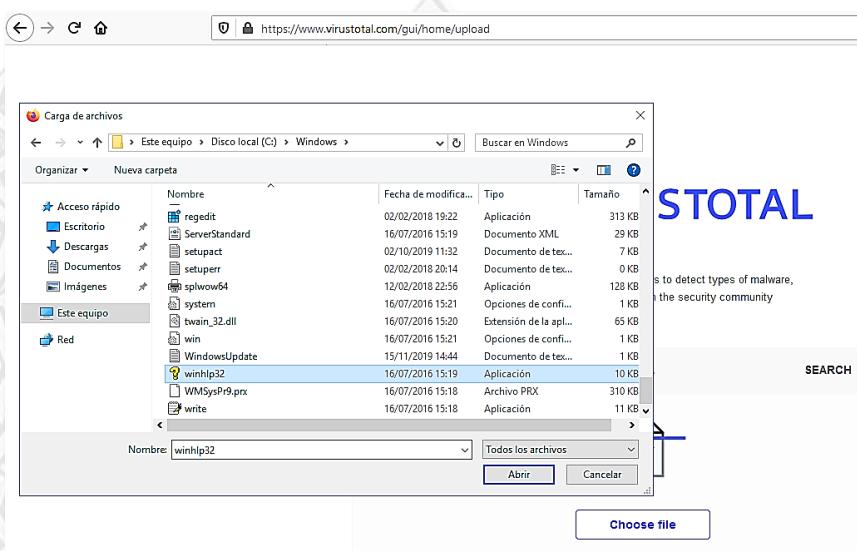


Figura 67. ¿Te has descargado algo sospechoso? ¡Pregúntale al oráculo!

Detection	Details	Relations	Community
Acronis	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
SecureAge APEX	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Bkav	Undetected	CAT-QuickHeal	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	CrowdStrike Falcon	Undetected
Cylance	Undetected	Cyren	Undetected
DrWeb	Undetected	Emsisoft	Undetected

Figura 68. Está limpio. No es garantía de nada, pero ayuda 😊



Hardware y Redes

Redes de Comunicaciones

Ejercicio NextDNS: Probar NextDNS

Descripción de la actividad

Puedes usar el servicio *NextDNS* de forma gratuita, incluso sin crear una cuenta, para poder **navegar de manera mucho más segura** de manera transparente, para entender la enorme importancia del servicio DNS en tu navegación.

Resultados Esperados

El objetivo de este ejercicio es que te des cuenta de que **sin un servidor DNS** que resuelva tus peticiones a IPs realmente **no podrías navegar**. Por ello, si ese servicio de resolución **tiene “inteligencia” que impide navegar a webs que se sepan que son perjudiciales**, podríamos lograr una web más segura (aun con un riesgo de censura). *NextDNS* es esto, pero que además te permite controlar esa “inteligencia”. Una vez lo pruebas, la idea es que puedas contestar estas preguntas:

- *¿Entiendes que al usar NextDNS estás poniendo en marcha una gran cantidad de medidas de seguridad de forma transparente (sin que seas consciente de ello)?*
- *¿Qué servicios de los que proporcionan NextDNS crees que te pueden resultar más útiles?*
- *¿Has notado alguna diferencia a la hora de navegar (errores, velocidad...) o algún problema con alguna página web?*
- *A la vista de tu experiencia con el servicio, ¿Lo instalarías en tu casa? ¿Lo harías en una máquina virtual que tengas para “navegación segura” junto con otras medidas de seguridad?*

Otra información necesaria para su realización

El servicio *NextDNS* (<https://nextdns.io/>) realmente es una forma de librarnos de muchos problemas de una manera transparente, y que se puede usar para tener una navegación mucho menos propensa a problemas. Una vez se configure en los navegadores o máquinas, el servicio se encargará automáticamente de **bloquear cualquier tipo de acceso bien directo o indirecto** (porque otra página lo cargue) a dominios que se consideren amenazas, o que pertenezcan a empresas anunciantes, que no estén aprobadas por este servicio centralizado de DNS.

 **La ventaja de este servicio es que ni siquiera te tienes que hacer una cuenta para usarlo, y si te la haces es para guardar tu configuración particular. Tampoco hace falta instalar nada si no quieres. Si bien el servicio gratuito está limitado a 300000 peticiones al mes, después de las cuales seguirá sirviéndote páginas web pero no tendrás protección, ese volumen de peticiones es suficiente para una navegación normal de cualquier usuario de conocimientos básicos.**

Para usar este servicio tenemos que ir a su web y usar la opción “*Try it now*” de su página principal, tras lo cual iremos a una URL que tiene este aspecto: <https://my.nextdns.io/< código de letras y números aleatorio>/setup>. En esa URL podremos configurar las opciones de seguridad del servicio y ver las opciones de instalación en nuestra máquina si finalmente queremos usarlas.



Como se ve, en la primera pestaña de **Seguridad** tenemos activas una serie de medidas por defecto, y se recomienda activarlas todas inicialmente a ver cómo se comporta con nuestra navegación habitual:

The screenshot shows the NextDNS web interface with the 'Seguridad' tab selected. It displays several sections with descriptive text and toggle switches:

- Fuentes de inteligencia sobre amenazas**: Describes blocking known domains for malware, phishing, and command and control. Includes a note about COVID-19 protection and a toggle switch for 'Utilizar las fuentes de inteligencia sobre amenazas'.
- Detección de amenazas basada en la IA**: Describes blocking millions of threats detected by AI. Includes a note about the technology being patented from scratch for DNS and a toggle switch for 'Activar la detección de amenazas basada en la IA'.
- Navegación Segura de Google**: Describes blocking malicious software and identity spoofing. Includes a note about the technology examining millions of URLs daily and a toggle switch for 'Habilitar la Navegación Segura de Google'.
- Protección contra el criptojacking**: Describes preventing unauthorized use of devices to mine cryptocurrencies. Includes a note about avoiding mining and a toggle switch for 'Habilitar la protección contra el criptojacking'.

Figura 69. La cantidad de cosas que tiene esto es tremenda. Si no las entiendes no te preocunes, actívalas, pruébalas y si no se rompe nada, tira para adelante con ellas 😊

Hay un gran nº de medidas que podemos activar, por lo que se recomienda recorrer toda la sección y activar todas inicialmente. Ten en cuenta que cada medida tiene una explicación de lo que es exactamente. Aunque no la entendamos, se recomienda su activación, y sólo desactivarlas si hay algún problema en nuestro uso habitual. El ejercicio consiste en **recorrer todas las opciones** que nos da *NextDNS* y activar todas las que creamos útiles para nuestro caso de uso particular:

- La opción de **bloquear TLDs** sirve para bloquear el acceso a páginas cuyo dominio acabe en un prefijo concreto (.es, .com, etc.). Puedes encontrar una lista completa aquí: https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains.
- En el apartado de **privacidad** podemos encontrar una característica muy útil: **las listas de bloqueo**. Son básicamente listas de dominios que el servicio no resolverá por pertenecer a anuncios, páginas maliciosas o servicios intrusivos o sin interés que se han considerado perjudiciales de alguna forma. Aunque el servicio viene con una ya cargada, podemos mejorarlo usando listas que están disponibles por Internet creadas para *NextDNS*. En este enlace puedes encontrar algunas: <https://github.com/hagezi/dns-blocklists>.
- *NextDNS* tiene también un apartado de **control parental** donde puedes limitar la búsqueda y el uso de Internet a las horas y dominios clasificados que quieras. Si vas a usar esta opción, ten en cuenta que implica que las páginas web a las que navegues **deben estar clasificadas por *NextDNS* dentro de la categoría a la que pertenezcan**, o especificarla (y no todas lo hacen). La **lista de categorías de sitios** usada por *NextDNS* es muy elocuente:



Añadir una categoría

Pornografía	Bloquea contenido pornográfico y para adultos. Incluye sitios de acompañantes, pornhub.com y dominios similares.	AÑADIR
Apuestas	Bloquea el contenido de apuestas.	AÑADIR
Citas	Bloquea todos los sitios web y aplicaciones de citas.	AÑADIR
Piratería	Bloquea los sitios web P2P, los protocolos, los sitios web de transmisión por secuencias que infringen los derechos de autor y los sitios web de alojamiento de videos genéricos que se utilizan principalmente para distribuir ilegalmente contenido protegido por derechos de autor.	AÑADIR
Redes sociales	Bloquea todos los sitios y aplicaciones de redes sociales (Facebook, Instagram, TikTok, Reddit, etc.). No bloquea las aplicaciones de mensajería.	AÑADIR
Juegos online	Bloquea sitios web, aplicaciones y redes, de juegos en línea (Xbox Live, PlayStation Network, etc.).	AÑADIR
Vídeo bajo demanda	Bloquea los servicios de vídeo bajo demanda (YouTube, Netflix, Disney+, páginas web ilegales de contenido bajo demanda, páginas web pornográficas, etc.) y redes sociales basadas en contenido de	AÑADIR

Figura 70. Esto evita que caigas por accidente en algún tipo de página en la que no quieras estar por accidente

- **El límite de acceso a aplicaciones y juegos** consiste en seleccionar algunos de una lista que el servicio tiene y que queramos prohibir.

Añadir un sitio web, una aplicación o un juego

TikTok	AÑADIR
Tinder	AÑADIR
Snapchat	AÑADIR
Facebook	AÑADIR
Instagram	AÑADIR
VK	AÑADIR
9GAG	AÑADIR
Tumblr	AÑADIR
Fortnite	AÑADIR
Twitter	AÑADIR
Roblox	AÑADIR
Messenger	AÑADIR

Figura 71. ¿Te has enfadado con algún juego o quieres autolimitarte por algún motivo en algún servicio? No hay cosa mejor que esta

- **El resto del servicio** son listas de bloqueo de sitios concretos que queramos, listas para permitir sitios sin importar que encajen en alguna restricción que hayamos puesto, y estadísticas de bloqueo y uso del servicio para que lo tengamos controlado.



- En el apartado de **instalación** tenemos instrucciones para poner en marcha el servicio en cualquier sistema operativo (de PC o de móvil), navegadores concretos (si no queremos hacerlo para todo el sistema operativo) o incluso en **routers**, pero solo modelos concretos que permitan la ejecución de los comandos que nos indican.

Ten en cuenta que **se genera una nueva configuración** (distinto bloque de nºs y letras en la URL) cada vez que entras en el servicio con el botón para probarlo que hemos visto. **Apunta cuál es tu identificador** para poder seguir configurando el servicio más tarde, y ten en cuenta que la configuración en los navegadores o SO usan ese identificador para distinguir tu configuración de la de los demás.

Si quieras empezar por algo sencillo para probar qué tal funciona, lo mejor es **configurar uno de tus navegadores** solamente con la configuración que has puesto y ver qué tal va.

The screenshot shows a web page with a navigation bar at the top. The 'Navegadores' tab is selected. Below it, there are two sections: one for Google Chrome and one for Firefox.

Google Chrome

1. Ve a Ajustes.
2. En la sección Privacidad y seguridad, haz clic en Seguridad.
3. En la sección Avanzado, habilita Usar DNS seguro.
4. Selecciona Con: Personalizado, luego introduce `https://dns.nextdns.[REDACTED]`.

Firefox

Solo Windows, macOS y Linux

1. Abre Preferencias.
2. Desplázate hacia abajo hasta la sección Configuración de red y haz clic en Configuración.
3. Desplázate hacia abajo y marca Habilitar DNS sobre HTTPS.
4. Selecciona Personalizado, introduce `https://dns.nextdns.[REDACTED]` y haz clic en Aceptar.
5. Introduce "about:config" en la barra de direcciones (y haz clic en ¡Acepto el riesgo! si te lo solicita).
6. Establece network.trr.mode a 3.

Figura 72. ¿Como poner esto en cualquier navegador que tengas? Te lo cuenta paso a paso

Si quieras que te lo cuente de otra forma, tengo un video sobre esto en aquí: <https://youtu.be/7eHusmdqFXq>

🛠 Ejercicio WAYBACK: Ver una página “en el pasado”

💻 Descripción de la actividad

Puedes usar el motor de búsqueda *Internet Archive* (aka “Wayback Machine”) para averiguar información acerca de sitios web **publicados en el pasado** en muchos dominios de Internet

🌟 Resultados Esperados

Esta actividad se completará cuando puedas usar la Wayback Machine para



- **Localizar la lista de URL históricas de cualquier sitio web que elijas**, cualquier archivo interesante que prefieras y las diferentes versiones históricas de cualquier documento o página web que estuviera en el sitio. Una vez que puedas hacer eso, también debes pensar en lo que esto podría significar desde el punto de vista de la seguridad (las preguntas al final del laboratorio pueden ayudarte a analizarlo).

 **PISTA:** *Imaginad que alguien ha puesto un documento indebido en alguna web, o dicho algo en una red social hace tiempo. Aunque lo borre, si ha tardado unos días en hacerlo es posible que esté en este museo de Internet, porque muchas veces no se dan cuenta de darlo de baja aquí también. ¡Internet te vigila y lo sabe todo!* 😊

- **Localizar post antiguos de una cuenta pública de la red social** que quieras de un personaje público. Tú eliges la fecha. *¿Crees que la Wayback Machine puede localizar post que se hayan borrado tiempo después de haberse publicado?*

Otra información necesaria para su realización

(**NOTA:** La Wayback Machine es masiva, y por tanto es bastante lenta muchas veces. No es tu conexión o tu ISP, es que es así, y no puedes hacer nada para evitarlo, lo sentimos 😊)

 **La mayoría de las personas (¡incluyendo bastantes administradores web!) están acostumbradas a buscar contenido comprometedor en las páginas web para eliminarlo, pero no incluyen el contenido comprometedor que ESTABA allí, pero ya no, o eliminan el contenido sin tener en cuenta que puede quedar archivado en la Wayback Machine. Este contenido puede resultar muy útil para los atacantes, y esta sección de laboratorio le enseñará cómo lidiar con él.**

Hay una página web de referencia para conocer la "historia" de cualquier sitio web en Internet y su nombre es "**The Wayback Machine**" (también conocido como *The Internet Archive*): <https://archive.org/web/>. Este sitio web es un archivo masivo de contenidos pasados ordenados por fecha que fueron mostrados por cualquier sitio web público que estuvo activo en Internet, pero también tiene usos "hacker".

Por ejemplo, puedes inspeccionar **TODAS las URL** que se han extraído de un dominio en particular utilizando una consulta como esta: http://web.archive.org/web/*<URL>/* (por ejemplo. http://web.archive.org/web/*http://www.uniovi.es/*). Ten en cuenta que la carga de URLs es asíncrona, por lo que puede tardar un tiempo. No te preocupes si inicialmente te encuentras una tabla vacía (para Uniovi, generalmente tarda 30s en cargarse).



100,000 URLs have been captured for this domain.

URL	MIME TYPE	FROM	TO	CAPTURES	DUPES	UNIQUES
http://uniovi.es/a	text/html	Jun 28, 2012	Jan 20, 2013	3	2	1
http://uniovi.es:80/1178308/3398279.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/1195304/8067200.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/1916933/4257141.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/1965168/716940.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/2336633/5843121.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/2351755/1549924.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/2727909/5884174.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/2770729/2498463.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/3079272/6607367.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/3435450/6065991.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/3441102/1716470.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/3653934/7687321.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/3833368/6063343.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/3901107/926287.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/4055244/1502844.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/4072572/1352137.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/411199/6023685.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/4280528/6237217.html	text/html	Sep 8, 2010	Sep 8, 2010	1	0	1
http://uniovi.es:80/4280528/6237217.html	text/html	Sep 8, 2010	Sep 8, 2010	-	-	-

Figura 73. Todas las páginas que alguna vez fueron publicadas en uniovi.es. Casi na

Una vez que tenemos la lista histórica de URL de un sitio, podemos utilizar esta información para obtener información muy interesante sobre el mismo. Puedes encontrar más detalles aquí: <https://www.elladodelmal.com/2013/04/hacking-con-archivecom-wayback-machine.html>

- La tabla de URL se puede procesar con código para extraer todas las URL, o las **URL de un determinado tipo** que pueden ser interesantes para un determinado propósito. Por ejemplo, puedes extraer imágenes o documentos para inspeccionar su contenido (¡o metadatos! 😊 😊). Esto también se puede hacer en la página web de *Wayback Machine*, ya que tiene un cuadro de texto de filtrado.

100,000 URLs have been captured for this domain.

URL	MIME TYPE	FROM	TO	CAPTURES	DUPES	UNIQUES
http://www.uniovi.es/-/defecto.pdf	text/html	Jun 16, 2013	Jul 15, 2013	2	0	2
http://www.uniovi.es/-/file.pdf	text/html	Jun 16, 2013	Jul 15, 2013	2	0	2
http://www.uniovi.es/-/preistabelle.pdf	text/html	Jun 16, 2013	Jul 15, 2013	2	0	2
http://www.uniovi.es/-/presitabelle.pdf	text/html	Jun 16, 2013	Jul 15, 2013	2	0	2
http://www.uniovi.es/aal/archivos_pdf/neutro_materia.pdf	text/html	Jun 6, 2011	Dec 15, 2018	7	6	1
http://www.uniovi.es/accesoyayudas/estudios/373/Oficio+de+Adjunto+Plantilla+Solicitud.pdf/5412a9a3-9730-40a4-8	text/plain	Sep 4, 2014	Sep 4, 2014	1	0	1
http://www.uniovi.es/accesoyayudas/tramites/-/asset_publisher/v9UAwM9qJpFc/content/www.uniovi.es/documents/31582/243104/INSTANCIA+VICERRECTOR+ESTUDIANTES_131028.pdf/d7cdc975-d56c-404f-b5a0-e150be637791	text/html	Sep 8, 2014	Sep 8, 2014	1	0	1
http://www.uniovi.es/Alfonso_Garcia_Legal/1993478.pdf	text/html	Jan 19, 2012	Apr 12, 2012	2	1	1
http://www.uniovi.es/Areas/MecanicaFluidos/becasempleado/investigacionaerodinamica_paniaguaSMALL.pdf	unk	Nov 11, 2014	Nov 11, 2014	1	0	1
http://www.uniovi.es/Areas/MecanicaFluidos/docencia/_asignaturas/maquinas_de_fluidos/Lecc6_r1.pdf	unk	Apr 12, 2017	Apr 12, 2017	1	0	1
http://www.uniovi.es/Areas/MecanicaFluidos/docencia/_asignaturas/maquinas_de_fluidos/Presenta_Leccion3.pdf	unk	Apr 12, 2017	Apr 12, 2017	1	0	1
http://www.uniovi.es/Areas/MecanicaFluidos/docencia/_asignaturas/mecanicas_de_fluidos/05_06/8%20FLUJO_CONDUCTOS.pdf	unk	Jul 29, 2015	Jul 29, 2015	1	0	1

Figura 74. ¿Qué hay dentro de estos "PDFs perdidos"? Sabe Dios 😊

- También puedes obtener el contenido de **archivos interesantes** de una página web. Por ejemplo, el archivo **robots.txt**



INTERNET ARCHIVE

WayBackMachine <http://www.uniovi.es/>

100,000 URLs have been captured for this domain.

URL	MIME TYPE	FROM	TO	CAPTURES	DUPLICATES	UNIQUES
http://www.uniovi.es/cecodet/formacion/UIM/index.html/robots.txt	unk	Jan 12, 2016	Sep 21, 2017	7	6	1

Showing 1 to 1 of 1 entries (filtered from 100,000 total entries)

Filter results (i.e. '.txt'):

Go Wayback!

Figura 75. El robots.txt de uniovi.es. Uno puede sorprenderse de lo que puede encontrar si pone robots.txt al final del nombre de cualquier página de Internet (Ej.: www.uniovi.es/robots.txt)

Este archivo es especial y mola. Aunque te lo cuento en otro curso asociado a este, en él puedes encontrar a veces información "secreta" (si está ahí es porque quien lo creó no tiene ni idea de para lo que sirve! 😊)

- **Historial de cualquier archivo del sitio web:** La columna de la tabla “URL” muestra el número de copias diferentes que cualquier archivo ha tenido a lo largo del tiempo. Esto significa que podemos localizar cualquier versión de cualquier archivo que haya sido indexado. Puedes iterar a través de ellos en la vista de calendario una vez que hagas clic en el archivo

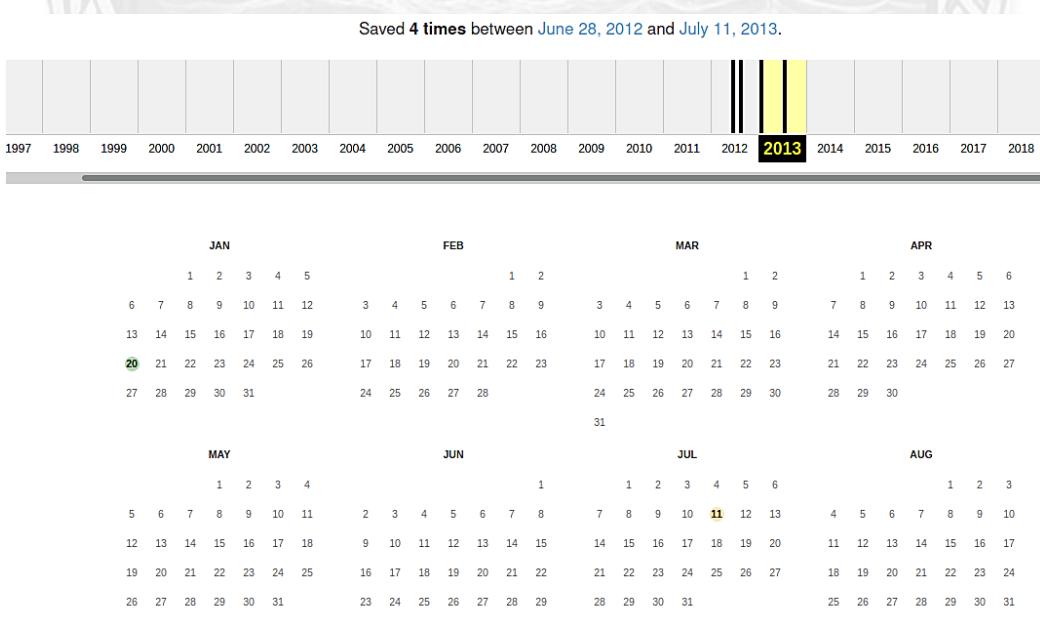


Figura 76. Hay páginas que tienen un montón de capturas a lo largo de la historia y otras que menos. Todo depende de lo "popular" que sea

Antes mencioné la palabra metadato. ¿Qué es un metadato? Es como una colección de “etiquetas” que acompañan a un archivo digital, pero no son parte de su contenido. Es información adicional sobre el archivo en sí. Los metadatos pueden incluir:

- **Nombre del archivo**
- **Fecha de creación**
- **Fecha de modificación:** La fecha y hora en que se modificó el archivo por última vez. Puede usarse para pillar a gente en alguna mentira...
- **Tamaño del archivo**



- **Tipo de archivo:** .jpg, .pdf o .docx, etc.

Y cosas que delatan a quien creo o procesó el archivo, como

- **Autor:** El nombre del autor del archivo. Si querías que fuera anónimo, a lo mejor lo estás “cantando” aquí.
- **Descripción:** Una breve descripción del contenido del archivo. A veces cuenta demasiadas cosas...
- **Palabras clave:** Palabras clave que se pueden utilizar para buscar el archivo.
- **Derechos de autor:** La información sobre los derechos de autor del archivo. Si quieres que la gente lo use sin problema, este es tu sitio.
- **Ubicación:** La ubicación del archivo en el ordenador o en la red (carpeta). A veces también aparece la geolocalización (latitud y longitud) de dónde se creó, especialmente si son fotos. Entenderás que esto es muy peligroso 😊
- **Software usado:** El software que se usó para crear o modificar el archivo. Esto puede delatar que estás usando software pirata...

Por tanto, si quieres saber algo más de un archivo y su contenido no te lo dice, a lo mejor quieres **hacer clic derecho – propiedades** en el mismo y ver qué te dice el archivo de sí mismo. O subirlo a webs como esta y ver qué te cuenta: <https://www.metadata2go.com/>. Al final, es un sitio más donde buscar información de un archivo.

🔎 Ahora júntalo con disponer de cualquier archivo que históricamente tuvo una página web. La cosa se pone interesante para “cotillear”, no crees? 😊



⌚ Dispositivos “Smart”

🛠 Ejercicio TRUSTPILOT: Probar TrustPilot

💻 Descripción de la actividad

Consiste en que entiendas que antes de comprar o contratar nada tienes que **mirarlo con lupa**, y que TrustPilot es una de las mejores páginas para ello.

🏆 Resultados Esperados

Puedes contestar a estas preguntas:

- ¿Entiendes por qué las opiniones en una tienda de un producto están bien, pero tampoco puedes fiarte al 100% de ellas?
- ¿Ves ahora la importancia de contar con páginas de revisiones de productos independientes de las tiendas?
- ¿Comprendes la importancia de tener un sitio centralizado donde mirar opiniones de lo que sea, y que tenga buena reputación?

📋 Otra información necesaria para su realización

Hay una cosa que mucha gente no sabe y es que existe una **industria de la opinión**, donde los dueños de productos pagan para que decenas, cientos o miles de *bots* (depende de lo que paguen) **les hagan una revisión positiva falsa de su producto** (físico o software). Esto hace que las opiniones puedan estar viciadas, por lo que hay que cogerlas con pinzas

 **Oh, créeme, hay empresas MUY profesionales que te inyectan opiniones con patrones que hacen que sea muy difícil distinguirlas de las reales.**

Otra de las cosas que debes tener en cuenta es que hay páginas de reviews independientes muy buenas, pero que también **pueden recibir “incentivos” por hacer revisiones de algo más positivas de lo que merecen**, por lo que es mejor siempre mirar varias de ellas si un producto te interesa.

Y como tercera “pata” a la hora de tener un criterio para comprar algo o no, te quedan webs como **Trustpilot** (<https://www.trustpilot.com/>). Trustpilot es una plataforma de reseñas online donde consumidores y empresas pueden interactuar y compartir sus experiencias. Como consumidor, tienes las siguientes ventajas:

- **Encontrar información fiable:** Puedes leer reseñas sobre empresas y productos de otros usuarios para tomar decisiones informadas antes de comprar.
- **Compartir sus experiencias:** Puedes escribir tus propias reseñas sobre las empresas y productos que has usado. Con ello puedes ayudar tanto a otros consumidores como a las empresas que hayan dado buenos servicios.
- **Influir en la reputación de las empresas:** Las reseñas de Trustpilot se tienen en cuenta en los rankings de búsqueda, por lo que tus reseñas pueden ayudar a que otras personas encuentren las mejores empresas.



Para las empresas:

- **Recopilar comentarios de los clientes:** Trustpilot puede ayudar a recopilar comentarios de los clientes para mejorar los servicios o detectar fallos en los mismos.
- **Construir confianza y credibilidad:** Ante clientes potenciales.
- **Mejorar su posicionamiento en los motores de búsqueda:** Por la razón que vimos antes.

 **No es raro que una empresa tenga personal dedicado a mirar sus propias reseñas en Trustpilot y responder directamente a ellas (incluso antes que otros canales similares)**

Trustpilot ofrece **servicios gratuitos y de pago** para empresas. Y, en general, es útil para ambos perfiles.

Explore companies by category

Animals & Pets <ul style="list-style-type: none">Animal HealthAnimal Parks & ZooCats & DogsHorses & RidingPet ServicesPet Stores	Events & Entertainment <ul style="list-style-type: none">Adult EntertainmentChildren's EntertainmentClubbing & NightlifeEvents & VenuesGamblingGamingMuseums & ExhibitsMusic & MoviesTheater & OperaWedding & Party	Home & Garden <ul style="list-style-type: none">Bathroom & KitchenCultural GoodsDecoration & InteriorEnergy & HeatingFabric & StationeryFurniture StoresGarden & PondHome & Garden ServicesHome Goods StoresHome Improvements	Restaurants & Bars <ul style="list-style-type: none">African & Pacific CuisineBars & CafesChinese & Korean CuisineEuropean CuisineGeneral RestaurantsJapanese CuisineMediterranean CuisineMiddle Eastern CuisineNorth & South American CuisineSoutheast Asian CuisineTakeawayVegetarian & Diet
Beauty & Well-being <ul style="list-style-type: none">Cosmetics & MakeupHair Care & StylingPersonal CareSalons & ClinicsTattoos & PiercingsWellness & SpaYoga & Meditation	Food, Beverages & Tobacco <ul style="list-style-type: none">Agriculture & ProduceAsian Grocery StoresBakery & PastryBeer & WineBeverages & LiquorCandy & ChocolateCoffee & TeaFood ProductionFruits & VegetablesGrocery Stores & Markets	Home Services <ul style="list-style-type: none">Cleaning Service ProvidersCraftsmanHouse ServicesHouse Sitting & SecurityMoving & StoragePlumbing & SanitationRepair Service Providers	Shopping & Fashion <ul style="list-style-type: none">AccessoriesClothing & UnderwearClothing Rental & RepairCostume & WeddingJewelry & WatchesMalls & Marketplaces
Business Services <ul style="list-style-type: none">Administration & ServicesAssociations & CentersHR & RecruitingImport & Export		Legal Services & Government	

Figura 77. Y dime, ¿de qué quieres saber opiniones hoy? Fuente: <https://www.trustpilot.com/categories>



🛠 Ejercicio EOL: Mirar cuando te “caduca” el móvil

💻 Descripción de la actividad

Esta actividad quiere que entiendas **una forma de obsolescencia programada moderna común** que no todo el mundo ve: Un servicio que no se corta abruptamente, sino que deja de mantenerse y degradándose con el tiempo hasta que el cliente está forzado a cambiar al cabo de un tiempo, al tener pocas (o ninguna) alternativa a su alcance.

🏆 Resultados Esperados

Puedes contestar a estas preguntas:

- ¿Entiendes que en cuanto un sistema operativo o cualquier programa deja de mantenerse no se actualiza más?
- ¿Entiendes por tanto que cualquier nuevo error o vulnerabilidad que se le encuentra no se va a arreglar? ¿Y que eso te hace más vulnerable conforme pasa el tiempo?
- Con esto que te he dicho, ¿Ahora ves por qué la única solución que se te da a veces a un problema es “compra la versión nueva del producto”?

📋 Otra información necesaria para su realización

Este “truco” de marketing es más lento, pero normalmente hace que la gente compre un producto nuevo tirando el viejo (que a lo mejor aún funciona) **forzada por las circunstancias** que el fabricante ha puesto en el mercado, que no dejan más opción. Lo peor es que los clientes se suelen quejar menos cuando se hace así que cuando es un corte abrupto del servicio, y por eso probablemente es una táctica muy socorrida. Páginas como la mencionada al menos te dejan saber cuándo va a ocurrir

endoflife.date currently tracks 311 products. Here are some of our most popular pages:

Programming	Python	Ruby	Java	PHP
Devices	iPhone	Android	Google Pixel	Nokia
Databases	MongoDB	PostgreSQL	Redis	MySQL
Operating Systems	Windows	Windows Server	MacOS	FortiOS
Frameworks	Angular	Django	Ruby on Rails	.NET
Desktop Applications	Firefox	Internet Explorer	Godot	Unity
Server Applications	Nginx	Kubernetes	Tomcat	HAProxy
Cloud Services	Amazon Elastic Kubernetes Service	Google Kubernetes Engine	Azure Kubernetes Service	
Standards	PCI-DSS			

Figura 78. En el mercado actual, todo software “caduca” (se deja de mantener, actualizar...). Lo importante es saber cuándo lo hace, y <https://endoflife.date/> te lo dice



Un caso verdaderamente llamativo es lo que ocurre con las versiones de *Android*:

Release	Released	Security Support
14 'Upside Down Cake'	8 months ago (04 Oct 2023)	Yes
13 'Tiramisu'	1 year and 10 months ago (15 Aug 2022)	Yes
12.1 'Snow Cone v2' (aka 12L)	2 years and 3 months ago (07 Mar 2022)	Yes
12 'Snow Cone'	2 years and 8 months ago (04 Oct 2021)	Yes
11 'Red Velvet Cake'	3 years and 9 months ago (08 Sep 2020)	Ended 4 months and 2 weeks ago (05 Feb 2024)
10 'Queen Cake'	4 years and 9 months ago (03 Sep 2019)	Ended 1 year and 3 months ago (06 Mar 2023)
9 'Pie'	5 years and 10 months ago (06 Aug 2018)	Ended 2 years and 5 months ago (01 Jan 2022)
8.1 'Oreo'	6 years ago (05 Dec 2017)	Ended 3 years and 5 months ago (10 Jan 2021)
8.0 'Oreo'	6 years and 10 months ago (21 Aug 2017)	Ended 3 years and 5 months ago (01 Jan 2021)
7 'Nougat'	7 years and 10 months ago (22 Aug 2016)	Ended 4 years and 8 months ago (01 Oct 2019)
6 'Marshmallow'	8 years ago (05 Oct 2015)	Ended 5 years and 10 months ago (01 Aug 2018)

Figura 79. El tema de la caducidad de los móviles *Android* porque su sistema operativo deja de recibir actualizaciones es un auténtico problema que parece no tener solución. Espera una "vida útil" de unos 4 años con los últimos cambios legales. Fuente: <https://endoflife.date/android>



🏃 Seguridad “En el Mundo Real”

👀 Seguridad “Física”

🛠 Ejercicio FALSACAM: Buscar modelos de cámaras falsas

👤 Descripción de la actividad

Esta actividad simplemente consiste en que **busques y compares modelos de falsas cámaras** en cualquier tienda de Internet

⌚ Resultados Esperados

Has encontrado modelos de falsas cámaras e, idealmente, una cámara real que sea idéntica en aspecto, para encontrar el combo que vimos en la teoría.

📱 Otra información necesaria para su realización

Por increíble que te parezca, estos productos son más comunes de lo que parece. Mira lo que nos devuelve una simple búsqueda de “cámara falsa” mismamente en Amazon:

Resultados
Más información sobre estos resultados. Consulta la página del producto para ver otras opciones de compra.

The screenshot shows a grid of 10 surveillance camera products from Amazon. Each product card includes an image, the brand name, a brief description, customer reviews (with star rating and count), price, delivery information, and a 'Add to cart' button. The products vary in design, including dome and bullet styles, with different numbers of LED lights and mounting options.

Imagen	Nombre del Producto	Descripción	Valoración	Precio	Opciones
	Kwmobile Cámara de vigilancia Falsa - Cámara simulada de Seguridad con luz LED Parpadeante - Cámara disuasoria para Exterior e Interior -...	Patrocinado	★★★★★ 2.093	12,99 €	Ahorra 5 % al comprar 4 de esta selección Envío GRATIS mañana, 21 de jun
	Cámaras de vigilancia CCTV Falsa con LED Intermitente, en Cáscara Resistente a la Intemperie, para Uso en Interiores y Exteriores	Patrocinado	★★★★★ 82	15,00 €	Envío GRATIS mañana, 21 de jun
	2 cámaras falsas O&W Security con objetivo y LED intermitente como cámara falsa, videovigilancia en Interiores y exteriores	Patrocinado	★★★★★ 84	17,90 € (0,89€/unidad)	Envío GRATIS mañana, 21 de jun
	DODUOS 2 Piezas Cámara Falsa Vigilancia Exterior, Cámaras Falsas de Seguridad con luz, Cámara Falsa Vigilancia, Cámara Vigilancia Falsa...	Patrocinado	★★★★★ 73	17,99 € (9,00€/unidad)	Envío GRATIS mañana, 21 de jun
	Tuttoinunclick falso-Cámara de vigilancia exterior	Opción Amazon	★★★★★ 55	5,00 €	Envío GRATIS el dom, 23 de jun
	Otio - Cámara de vigilancia interior con LED, 1080p, alerta de movimiento.		★★★★★ 205	6,90 €	Ahorra 5 % al comprar 4 de esta selección Envío GRATIS mañana, 21 de jun
	JZK 2x Cámaras Domo de Vigilancia Falsas CCTV simuladas con LED Intermitente Imitación Real para Seguridad de Oficina en el hogar		★★★★★ 1.324	14,99 € (7,15€/unidad)	Ahorra 5 % al comprar 4 de esta selección Envío GRATIS mañana, 21 de jun
	Retoo Cámara fícticia giratoria para Exterior e Interior, cámara CCD inalámbrica con LED Parpadeante, cámara de Seguridad Resistente a L...		★★★★★ 78	8,99 €	Ahorra 5 % al comprar 4 de esta selección Envío GRATIS mañana, 21 de jun
	kwmobile Cámara de vigilancia Falsa - Cámara simulada de Seguridad con luz LED Parpadeante - Cámara disuasoria para Exterior e Interior -...		★★★★★ 2.093	12,99 €	Ahorra 5 % al comprar 4 de esta selección Envío GRATIS mañana, 21 de jun
	2 x cámara simulada Cámara Exterior simulada para Uso Interior o Exterior con Forma de Bola LED Intermitente		★★★★★ 1.159	17,99 € (9,00€/unidad)	Ahorra 5 % con un cupón Envío GRATIS mañana, 21 de jun

Figura 80. Amazon (por poner un ejemplo) tiene un surtido de estos aparatos bien grande. Para todos los gustos, formas y colores 😊



🛠 Ejercicio FARADAY: Buscar fundas de Faraday a la venta

👤 Descripción de la actividad

Consiste en que te des cuenta de que las **fundas de Faraday no son ya algo exótico**, sino algo común y con muchas formas, tamaños y posibles usos

🏆 Resultados Esperados

Puedes contestar a estas preguntas:

- ¿Entiendes para que sirve una funda de Faraday con una tarjeta *contactless* y cómo te protege?
- ¿Y con un teléfono móvil?

📘 Otra información necesaria para su realización

Como en el caso de las cámaras, estos productos ya son hoy día mucho más comunes de lo que parece. Fíjate lo que pasa si buscamos "Fundas Faraday" en Amazon, por ejemplo:

The screenshot shows a grid of 12 product listings from an Amazon search for "Fundas Faraday". Each listing includes a small image of the product, its name, a brief description, a star rating, the number of reviews, and a price. Most items are marked with a "prime" logo, indicating they are eligible for free two-day delivery. The products vary in size and design, some being small pouches for car keys or mobile phones, while others are larger cases for laptops or tablets.

Imagen	Título del producto	Descripción	Valoración	Nº de reseñas	Precio
	Funda Faraday Móvil para Teléfono y Llave Coche 2 Piezas Bolsa Faraday Movil Jaula Faraday Portatil Bloqueador Senal RFID/NFC Blindaje...	Patrocinado	★★★★★	588 comprados el mes pasado	10,99 € Ahorra 15% con un cupón
	Lenpard 2PCS Mini Bolsa Faraday para Llaves de Coche, Funda Bloqueo de Señal de Seguridad Anti RFID/WIFI/gsm/LTE/NFC Protecció...	Patrocinado	★★★★★	7.300 comprados el mes pasado	14,25 € Ahorra 5 % al comprar 4 de esta selección
	Samfolk Funda Faraday Movil, Bolsa Faraday Movil, Jaula Faraday Portatil Bloqueador Senal RFID/NFC, Bolsa Inhibidora de Seguridad - Fibra de...	Patrocinado	★★★★★	2.434 comprados el mes pasado	9,99 € Ahorra 5 % al comprar 4 de esta selección
	TOCA Bolsa Faraday Portátil - Bloqueador RFID/Anti-Rastreo, Protección Privacidad para Móvil, Laptop y Llaves Coche, Resistente a...	Patrocinado	★★★★★	287 comprados el mes pasado	34,90 € Ahorra 5 % al comprar 4 de esta selección
	Funda Faraday Móvil para Teléfono y Llave Coche 2 Piezas Bolsa Faraday Movil Jaula Faraday Portatil Bloqueador Senal RFID/NFC Blindaje...	Opción Amazon	★★★★★	588 comprados el mes pasado	10,99 € Ahorra 15% con un cupón
	Samfolk Funda Faraday Movil, Bolsa Faraday Movil, Jaula Faraday Portatil Bloqueador Senal RFID/NFC, Bolsa Inhibidora de Seguridad - Fibra de...	Opción Amazon	★★★★★	50+ comprados el mes pasado	9,99 € Ahorra 5 % al comprar 4 de esta selección
	Lenpard 2PCS Mini Bolsa Faraday para Llaves de Coche, Funda Bloqueo de Señal de Seguridad Anti RFID/WIFI/gsm/LTE/NFC Protecció...	Opción Amazon	★★★★★	7.300 comprados el mes pasado	14,25 € Ahorra 5 % al comprar 4 de esta selección
	ONEVER Bolsa De Bloqueo De Señal, GPS RFID Faraday Bolsa De Protección De Jaula, Funda para Teléfono Móvil Protección De La...	Opción Amazon	★★★★★	3.168 comprados el mes pasado	8,99 € Compra 3 y obtén un 5% de descuento
	Hodufy Paquete de 3 Bolsas Faraday	Opción Amazon	★★★★★	120 comprados el mes pasado	43,55 € Ahorra 5 % al comprar 4 de esta selección
	Sanguro – 2 PCS Bolsa Faraday para Llaves de Coche, Funda Faraday Bloqueo de Señal de Seguridad Anti RFID. Llavero antirrobo coche.	Opción Amazon	★★★★★	40 comprados el mes pasado	11,99 € (6,00€/Producto) PVP: 44,99€
	Sanguro – 2 PCS Bolsa Faraday para Llaves de Coche, Funda Faraday Bloqueo de Señal de Seguridad Anti RFID. Llavero antirrobo coche.	Opción Amazon	★★★★★	4 comprados el mes pasado	11,99 € (6,00€/Producto) PVP: 44,99€

Figura 81. Será por formas y tamaños... 😊



Seguridad Financiera

Ejercicio TARJETAMON: Buscar ofertas de tarjetas monedero en algún banco

Descripción de la actividad

Consiste en que investigues las opciones para hacer **tarjetas virtuales** en tu banco, y el coste que tiene hacerlo, para ver si te conviene hacerte una (o a tus padres 😊) si compras mucho por *Internet*.

Resultados Esperados

Eres capaz de saber cómo puedes **crearte una tarjeta monedero a tu nombre** a partir de las opciones para ello que te da el banco, y explicar a un familiar por qué debe hacerlo.

Otra información necesaria para su realización

A la hora de crearte una tarjeta monedero virtual es mejor seguir una serie de principios:

- Que sea **una tarjeta monedero real**, es decir, que sea imposible gastar más que el saldo que tiene cargado en un momento dado. Si alguien gasta más de eso la diferencia no debe revertir en tu cuenta o en otra tarjeta, sino que la operación debe anularse.
- Que, en lugar de ser simplemente un número, **sea una tarjeta física** que puedas usar para pagar en comercios como una tarjeta "normal". Ten en cuenta que para que esto se permita quizás tengas que activar esa opción primero
- Que **no te cobren comisiones abusivas** por el hecho de tener esa segunda tarjeta
- Que se pueda **consultar de una manera independiente** a tu tarjeta primaria, y tratarla como una tarjeta más sin vinculación ni con tus cuentas ni con otros productos.
- Que **su cancelación sea lo más rápida posible**, idealmente a través de la interfaz de la cuenta bancaria vía web, por si fueses objeto o de un fraude, algo que en este caso es más sencillo, dado que lo vas a usar para comprar por internet.
- **Que se pueda anular temporalmente**: mucha gente prefiere desactivar la tarjeta la mayor parte del tiempo y solo activarla cuando va a hacer la compra en un establecimiento con ella. Luego, una vez la compra esté reflejada, podría desactivarse de nuevo. No obstante, pregunta en tu banco cuál es la mejor política al respecto, por si la desactivación prematura anulase la compra.

 **No es difícil localizar el servicio que te permite crearlas, puesto hoy en día prácticamente todos los bancos la ofrecen (y seguro que el tuyo también! 😊).**



Santander Cuentas Bancarias Tarjetas Bancarias HAZTE C...

← Tarjetas de Débito | Tarjeta Prepago Mini Tarjeta Virtual Ventajas de tus tarjetas de débito Tarjeta Prepago Santander

TARJETAS

Tarjeta Virtual eCash

Una tarjeta virtual prepago perfecta para pagar por internet cargándola con el dinero que necesites.

Compra online de forma segura.
Recarga el importe que necesites para tus compras.
Gratis durante el primer año.

CONTRATAR

Figura 82. Un ejemplo de tarjeta monedero del Banco Santander. Fuente: Ej.: <https://www.bancosantander.es/particulares/cuentas-tarjetas/tarjetas/debito/virtual-e-cash>

