Módulo 3. Protección de amenazas en línea

Módulo 3. Protección de amenazas en línea

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

En el módulo **'Protección de amenazas en línea'**, avanzamos un paso más en nuestro compromiso de crear un entorno digital seguro. Tras haber explorado cómo navegar resguardando nuestra privacidad, nos transformaremos en defensores activos de nuestro espacio digital. Te convertirás en un **'Detective digital'**, desenmascarando estafas y fraudes; un **'Navegador intrépido'**, evadiendo sitios webs fraudulentos y otras trampas cibernéticas; y fortalecerás tus comunicaciones con **'Correos fortificados'**.

Este módulo te equipará con las herramientas necesarias para identificar y repeler las amenazas más comunes en el ciberespacio.

Módulo 3. Protección de amenazas en línea

3.1 Detectives digitales

En el bloque **'Detectives digitales'**, nos adentramos en el mundo del cibercrimen para identificar y analizar las trampas más comunes. Nos enfocaremos endetectar **señales de alerta**, como ofertas que parecen demasiado buenas para ser verdad y mensajes que presionan para actuar de manera urgente, tácticas comunes para engañar a los desprevenidos.

Además, exploraremos la **cronología del engaño**, desde correos sospechosos hasta cibertrucos avanzados, equipándonos con herramientas prácticas y conocimientos para actuar de manera segura frente a cualquier estafa.

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Este módulo no solo aumentará nuestra vigilancia ante las estafas en línea, sino que también fortalecerá nuestras **competencias digitales**, enseñándonos a proteger nuestra información y la de nuestro alumnado en el contexto educativo.

Fraudes digitales

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Como docente, es importante estar al tanto de los **diferentes tipos de estafas** que nos pueden afectar tanto a nosotros como a nuestros estudiantes en el día a día. En este apartado, te presentamos algunas de las estafas más comunes, incluyendo **phishing**, **fraudes financieros** y **scams románticos**, entre otros.

Aprender a reconocer estas amenazas es el primer paso para defenderse de los ciberdelincuentes y proteger nuestra información.

Objetivos:

- Identificar los diferentes tipos de estafas cibernéticas más comunes.
- Comprender las tácticas utilizadas por los ciberdelincuentes para diseñar estas estafas, preparando a los docentes para anticipar y mitigar riesgos.

Lecturas recomendadas:

- Ingeniería social y fraudes online <https://www.incibe.es/ciudadania/tematicas/ingenieria-social-fraudes-online> (INCIBE). Un artículo detallado sobre cómo los ciberdelincuentes utilizan técnicas de ingeniería social para cometer fraudes en línea.
- Cuáles son algunos de los tipos de estafas más comunes <https://www.consumerfinance.gov/es/obtener-respuestas/cuales-son-algunos-de-los-tipos-de-estafas-mas-comunes-es-2092/> (CFPB). Esta

guía ofrece ejemplos de estafas comunes y consejos para protegerse de los estafadores.

Vamos a echar un vistazo a los tipos de estafas más comunes:

- **Phishing:** El phishing es una técnica en la que los estafadores envían correos electrónicos, mensajes de texto o llamadas telefónicas haciéndose pasar por instituciones o personas de confianza, con el objetivo de obtener información personal, como contraseñas o datos bancarios. Estos mensajes a menudo incluyen enlaces o archivos adjuntos maliciosos.
- **Fraudes Financieros:** Los fraudes financieros implican intentos de robar dinero o información financiera. Pueden tomar la forma de falsos esquemas de inversión, facturas falsas o solicitudes de pago fraudulentas.
- **Estafas Románticas:** Las estafas románticas ocurren cuando los estafadores se hacen pasar por personas interesadas en una relación amorosa con el objetivo de obtener dinero o información personal. Pueden comenzar en sitios de citas o redes sociales y luego solicitar ayuda financiera o envío de fotos o vídeos íntimos.
- **Estafas de Soporte Técnico:** En estas estafas, los delincuentes se hacen pasar por representantes de empresas de tecnología y contactan a las víctimas, afirmando que hay problemas con sus dispositivos o software. Luego intentan engañarlos para que les den acceso remoto a sus dispositivos o que realicen pagos.
- **Ransomware:** El ransomware es un tipo de malware que cifra los archivos de una víctima y exige un rescate a cambio de la clave de descifrado.

Entre las principales señales de alerta:

- **Promesas o amenazas exageradas:** Los estafadores suelen jugar con la codicia o el miedo, haciendo promesas demasiado buenas para ser verdad o amenazando con consecuencias graves si no se sigue sus instrucciones.
- **Urgencia y plazos ajustados:** Cuando un mensaje indica que hay un plazo muy corto para reclamar un premio o realizar una compra, es probable que se trate de una estafa para presionar a la víctima.
- **Diseño amateur y errores:** Mensajes con faltas de ortografía, mala redacción o un diseño poco profesional son señales de alerta de una posible estafa.
- **Solicitud de información personal o financiera:** Si se pide compartir datos confidenciales como contraseñas, números de tarjeta de crédito o acceso a cuentas, es muy probable que sea una estafa.
- **Llamadas o mensajes no solicitados:** Correos electrónicos, SMS o llamadas inesperadas que buscan generar urgencia o presionar a la víctima, son comunes en las estafas.
- **Algo "no está bien":** Si el mensaje, oferta o situación genera desconfianza, es mejor detenerse y verificar la legitimidad antes de proceder.

Si bien existen numerosos tipos de estafas online, los delincuentes suelen utilizar canales de comunicación similares para llevarlas a cabo. Algunas de las principales formas en que los estafadores contactan a las víctimas son:

- **Correos electrónicos:** Los estafadores envían mensajes de phishing haciéndose pasar por instituciones o personas de confianza, con el objetivo de obtener información personal o financiera.
- **Mensajes de texto:** A través de SMS, WhatsApp u otras aplicaciones de mensajería, los delincuentes también intentan engañar a las víctimas solicitando datos o dinero.
- **Llamadas telefónicas:** Las estafas telefónicas, donde los impostores se hacen pasar por representantes de empresas o agencias gubernamentales, son otro método común para presionar a las víctimas a realizar pagos o compartir información.
- **Redes sociales:** Las estafas románticas y de suplantación de identidad a través de perfiles falsos en plataformas de citas y redes sociales son cada vez más frecuentes.
- **Anuncios online:** Los delincuentes también utilizan anuncios engañosos en sitios web, aplicaciones y marketplaces digitales para atraer a posibles víctimas con ofertas demasiado buenas para ser verdad.

Estar alerta ante cualquier solicitud de información o dinero a través de estos canales, y verificar siempre la legitimidad de la fuente, es fundamental para evitar caer en las trampas de los ciberdelincuentes.

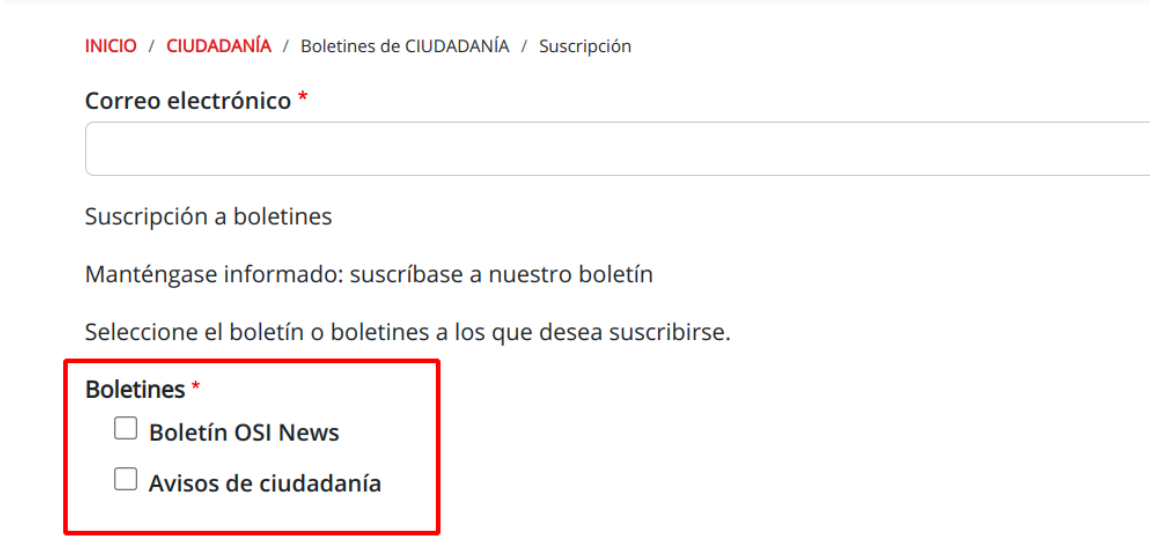
La primera **clave** para protegerse de las estafas en línea es **estar al día** con las **últimas tácticas** y alertas de seguridad. Para ello, puede ser de gran utilidad suscribirse a los **boletines de INCIBE <https://www.incibe.es/ciudadania/simplenews/subscriptions/landing>** .

Recibirás por correo electrónico los avisos de seguridad que mayor impacto están teniendo en cada momento, junto con una descripción y pautas sobre cómo actuar ante cada uno de ellos.

Tienen disponibles los siguientes boletines:

- **Boletín OSI News**. Recibe los últimos artículos publicados tanto en el blog como en la sección de historias reales para elevar tu cultura de ciberseguridad y poder así desenvolverte con confianza y seguridad en la era digital.
- **Avisos de ciudadanía**. Infórmate de manera temprana de los últimos avisos de seguridad publicados para prevenir las distintas amenazas que circulan por internet.

Al suscribirte, puedes elegir el boletín que más te interese o incluso optar por ambos:



INCIBE (Dominio público)

Actividad (opcional): Reflexión personal sobre estafas en línea

Descripción: Reflexiona sobre experiencias personales o conocidas de estafas en línea. Analiza las razones detrás de la estafa, cómo podría haberse evitado y si has cambiado tus hábitos en línea después del caso.

Pasos:

- Piensa en alguien que haya sido víctima de una estafa en línea, ya sea personalmente o conocido a través de Internet.
- Analiza las circunstancias que llevaron a la estafa. ¿Qué fue lo que permitió que ocurriera?
- Reflexiona sobre cómo podría haberse evitado la estafa. ¿Qué medidas de seguridad podrían haberse implementado?
- Considera si has cambiado tus hábitos en línea como resultado de este caso. ¿Has tomado precauciones adicionales?

Recursos necesarios:

- Acceso a información sobre casos de estafas en línea para la reflexión.

Nunca, never, jamais, hacer clic en enlaces no solicitados

La prevención es la clave en la protección contra las estafas en línea, y una regla fundamental es **evitar hacer clic en enlaces no solicitados**. Esta medida es crucial por diversas razones.

En primer lugar, los estafadores suelenutilizar **enlaces maliciosos** en correos electrónicos o mensajes para dirigir a **sitios web falsos** o descargar **malware**. Esto compromete la seguridad del dispositivo y puede exponer información

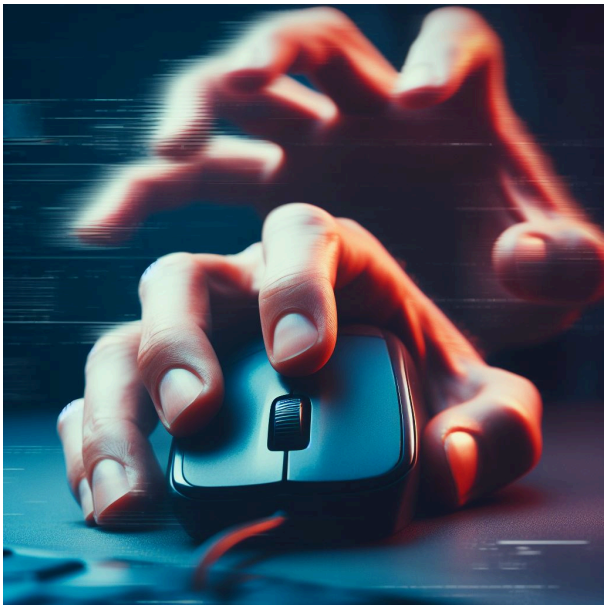


Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

personal. Además, los enlaces pueden llevar a páginas web falsas que imitan a empresas legítimas, lo que dificulta discernir su autenticidad.

Por otro lado, los estafadores también pueden utilizar **enlaces acortados** para ocultar su verdadero destino, lo que dificulta identificar si se trata de un sitio seguro o no. Esta práctica añade una capa adicional de complejidad para los usuarios, haciendo que sea aún más difícil discernir si un enlace es legítimo o no.

Objetivos:

- Concienciarnos sobre la peligrosidad de los enlaces.
- Aprender a identificar enlaces maliciosos.

Lecturas recomendadas:

- Nunca hagas clic en estos enlaces que te llegan por WhatsAp <https://www.redeszone.net/noticias/seguridad/enlaces-falsos-whatsapp-evitar/> (RedesZone). Este artículo ofrece consejos prácticos para identificar y evitar enlaces falsos en WhatsApp, una táctica comúnmente utilizada por los estafadores.
- ¿Qué son los enlaces maliciosos y cómo protegerse ante esta amenaza? <https://www.bbva.com/es/innovacion/que-son-los-enlaces-maliciosos-y-como-protegerse-ante-esta-amenaza/> (BBVA). Este recurso proporciona información detallada sobre los enlaces maliciosos, incluyendo cómo funcionan, cómo identificarlos y consejos para protegerse contra ellos.

Existen herramientas muy útiles para **comprobar la seguridad de una URL**, como por ejemplo:

- **Analizadores de URL:** Sitios web como VirusTotal <https://www.virustotal.com/> , URLScan <https://urlscan.io/> o Google Safe Browsing <https://transparencyreport.google.com/safe-browsing/search> permiten escanear una dirección web y detectar si está asociada a actividades maliciosas.
- **Extensiones de navegador:** Complementos para el navegador como Web of Trust <https://www.mywot.com/> , pueden avisarte sobre sitios web peligrosos mientras navegas.
- **Servicios de verificación de enlaces:** Plataformas como LongURL <https://longurl.in/> o CheckShortURL <https://checkshorturl.com/> permiten analizar enlaces acortados y determinar su destino real.

Como vemos, si bien los ciberdelincuentes utilizan enlaces maliciosos para engañar a las víctimas, existen diversas formas de verificar la seguridad de una URL antes de acceder a ella.

Actividad (opcional): Análisis de URL en acción

Descripción: Prueba algunas de las herramientas de análisis de URL proporcionadas, usa diferentes enlaces para testear su eficacia y comparte tus descubrimientos en el foro del curso.

Pasos:

1. Revisa el listado de herramientas de análisis de URL proporcionadas en los materiales del curso.
2. Elige una herramienta que creas que mejor se adapte a tus necesidades de análisis.

3. Analiza con ella varios enlaces, asegurándote de incluir URLs seguras y sospechosas.
4. Discute en el foro del curso tu experiencia con la herramienta seleccionada, explicando por qué la elegiste y cómo evaluas su rendimiento.

Recursos necesarios:

- Listado de herramientas de análisis de URL disponibles en los materiales del curso.
- Conexión a internet.

Actuando ante una estafa

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Si detectas o caes en una estafa, es fundamental **actuar de manera rápida y efectiva** para minimizar el impacto y evitar futuros incidentes. Este apartado explora las **medidas que debemos tomar** ante estas situaciones, desde el momento en que identificamos la estafa hasta las acciones de recuperación y prevención a largo plazo.

Además, te proporcionaremos información sobre **cómo reportar estafas** a través de canales oficiales, proteger tu identidad y tu información financiera, y cómo compartir información sobre la estafa para educar y proteger a otros.

Objetivos:

- Conocer los medios para reportar una estafa que detectemos, aprendiendo a utilizar los canales oficiales.
- Aprender a responder y aplicar las medidas necesarias si se ha sido víctima de una estafa, incluyendo la protección de la identidad y la recuperación financiera.

Lecturas Recomendadas:

- **Cómo actuar en caso de phishing <https://andaluciavuela.es/cambiar-todas-las-contrasenas-como-actuar-en-caso-de-phishing/>** (Andaluciavuela). Este artículo ofrece consejos específicos sobre cómo actuar si has sido víctima de phishing.
- **Cómo actuar ante una estafa en internet <https://www.redeszone.net/noticias/seguridad/como-actuar-estafa-internet/>** (Redeszone). Este artículo proporciona pautas y recomendaciones sobre cómo responder si te encuentras con una estafa en Internet.

Estas son las principales medidas que se deben tomar si hemos detectado una estafa en línea:

1. No responder ni interactuar:

Al detectar una posible estafa, es fundamental no responder ni interactuar con los estafadores. Mantener la calma y evitar proporcionar información personal o financiera es clave para evitar ser víctima de un fraude.

2. Mantener registros y pruebas:

Es aconsejable mantener registros y pruebas de la estafa detectada, como capturas de pantalla, correos electrónicos o mensajes recibidos. Estos documentos pueden ser útiles para respaldar la denuncia y facilitar la investigación.

3. Reportar a las autoridades competentes:

Es importante reportar la estafa a las autoridades correspondientes. Para reportar una estafa, es recomendable utilizar los canales oficiales, esto garantiza que la denuncia sea recibida y gestionada de manera adecuada. Los canales oficiales incluyen:

- **Brigada Central de Investigación Tecnológica de la Policía Nacional <https://www.policia.es/_es/denuncias.php>**
- **Grupo de Delitos Telemáticos de la Guardia Civil <https://www.guardiacivil.es/es/servicios/denuncias/index.html>**
- **Línea telefónica gratuita del INCIBE <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>**

4. Protege tus cuentas:

Si has proporcionado información personal o financiera, cambia las contraseñas de todas tus cuentas afectadas y notifica a tu banco o entidad financiera.

5. Compartir la información sobre la estafa:

Comparte la información sobre la estafa con las personas de tu entorno y en redes sociales para alertar a otras personas y evitar que caigan en la trampa. Cuanta más difusión tenga, mejor será la prevención.

Estas son las principales medidas que se deben tomar si se ha sido víctima de una estafa en línea:

1. Desconectarse de internet de inmediato:

Al detectar que has sido víctima de una estafa en línea, es importante desconectarse de la red de internet de inmediato para evitar que los estafadores accedan a más información sensible.

2. Cambiar las contraseñas de las cuentas comprometidas:

Para proteger tus cuentas, cambia las contraseñas de todas las cuentas que puedan haber sido comprometidas durante la estafa. Utiliza contraseñas seguras y únicas para cada cuenta.

3. Escanear el dispositivo en busca de posible malware:

Realiza un escaneo completo del dispositivo en busca de posible malware o software malicioso que pueda haber sido instalado durante la estafa. Utiliza un antivirus fiable y actualizado.

4. Contactar de forma urgente con los bancos y entidades financieras:

Es crucial contactar de forma urgente con los bancos y entidades financieras afectadas para bloquear tarjetas y evitar transacciones fraudulentas.

5. Mantener registros y pruebas:

Es aconsejable mantener registros y pruebas, como capturas de pantalla, correos electrónicos o mensajes recibidos. Estos documentos pueden ser útiles para respaldar la denuncia y facilitar la investigación.

6. Analizar y anotar las acciones previas al fraude:

Analiza y anota las acciones previas al fraude, como sitios web visitados y correos electrónicos recibidos, para facilitar la investigación y recuperación. Esta información puede ser útil para las autoridades.

7. Reportar a las autoridades competentes:

Es importante reportar la estafa a las autoridades correspondientes. Para reportar una estafa, es recomendable utilizar los canales oficiales, esto

garantiza que la denuncia sea recibida y gestionada de manera adecuada. Los canales oficiales incluyen:

- **Brigada Central de Investigación Tecnológica de la Policía Nacional <https://www.policia.es/_es/denuncias.php>**
- **Grupo de Delitos Telemáticos de la Guardia Civil <https://www.guardiacivil.es/es/servicios/denuncias/index.html>**
- **Línea telefónica gratuita del INCIBE <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>**

8. Realiza una revisión completa de tus medidas de seguridad:

Tras detectar una estafa, es recomendable actualizar las medidas de seguridad en línea, como cambiar contraseñas, revisar la configuración de privacidad y mantener el software actualizado para prevenir futuros ataques.

9. Compartir la información sobre la estafa:

Comparte la información sobre la estafa con las personas de tu entorno y en redes sociales para alertar a otras personas y evitar que caigan en la misma trampa. Cuanta más difusión tenga, mejor será la prevención.

Actividad de reflexión (opcional): "Cuanta más difusión tenga, mejor será la prevención"

Descripción: Reflexiona sobre la importancia de compartir experiencias de estafas en línea y cómo esto puede ayudar a prevenir futuros fraudes.

Recursos educativos

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Explora estos **recursos** para enseñar ciberseguridad: actividades, lecturas y más, diseñados para promover la **prevención de estafas y fraudes en línea** entre nuestros estudiantes.

- **Guía para aprender a identificar fraudes online:** Guía completa que proporciona información detallada sobre cómo identificar fraudes en línea. Ver guía <https://www.incibe.es/ciudadania/formacion/guias/guia-para-aprender-identificar-fraudes-online> .
- **Cómo comprobar si un enlace es malicioso:** Documento PDF que explica cómo verificar si un enlace es malicioso y qué acciones tomar. Descargar PDF <https://www.incibe.es/sites/default/files/docs/como-comprobar-enlace-malicioso.pdf> .
- **Refranero de las compras seguras online:** Recopilación de refranes relacionados con las compras seguras en línea y consejos prácticos. Descargar PDF <https://www.incibe.es/sites/default/files/docs/refraneo_compras_seguras_online.pdf> .
- **Juego de mesa - Detecta el Fraude:** Juego de mesa interactivo para aprender a detectar fraudes en línea. Acceder al juego <https://www.incibe.es/ciudadania/juegos/juegos-mesa/detecta-el-fraude> .

- **Prueba de detección de ingeniería social:** Actividad interactiva para poner a prueba tus habilidades de detección de ingeniería social. Acceder a la actividad <https://www.incibe.es/ciudadania/formacion/actividades/prueba-deteccion-ingenieria-social> .
- **Cómics para identificar fraudes online:** Colección de cómics educativos para identificar y prevenir fraudes en línea. Ver cómics <https://www.incibe.es/ciudadania/formacion/recursosdescargables/comics-para-identificar-fraudes-online> .

Módulo 3. Protección de amenazas en línea

3.2 Navegadores intrépidos

En el bloque '**Navegadores intrépidos**', nos sumergimos nuevamente en las aguas turbulentas de internet, pero esta vez con un enfoque diferente: la seguridad. Si en el módulo anterior exploramos el arte de navegar desapercibido, ahora nos adentramos en el **desafío de navegar, identificando y eludiendo las trampas cibernéticas** que acechan en cada esquina con determinación y conocimiento.

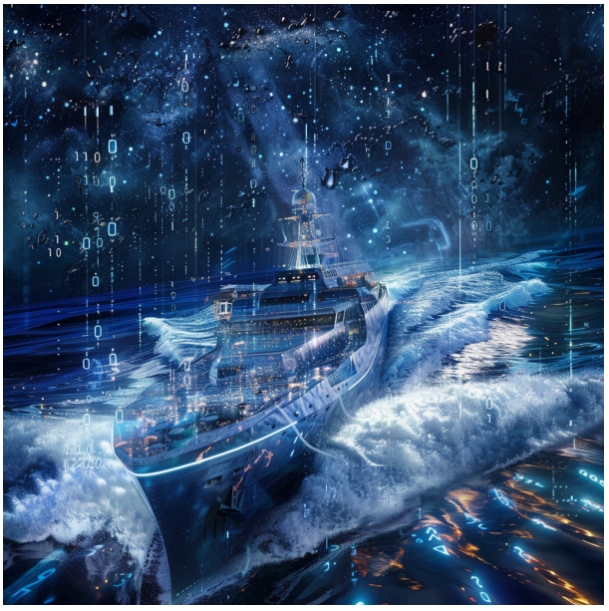


Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Convertirte en un navegador intrépido implica no solo comprender los riesgos, sino también estar preparado para enfrentarlos con resolución. Desde los astutos **ataques homográficos** hasta las sutiles amenazas que se ocultan en descargas aparentemente inofensivas, aprenderás a detectar y evadir las trampas que acechan en cada clic.

Este bloque te proporcionará las herramientas y estrategias necesarias para navegar por internet con seguridad y confianza. A lo largo de este viaje, exploraremos estrategias clave para **navegar de manera segura** y mantener a raya a los ciberdelincuentes.

Navegando entre sitios webs fraudulentos

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Los ciberdelincuentes crean **sitios web fraudulentos** que buscan **robar información confidencial**, como contraseñas, detalles de pago o información personal que pueden usar para robar tu identidad. Algunos sitios web falsos pueden incluso **infectar tu dispositivo con malware** o engañarte para que compres productos inexistentes o falsificados.

No te dejes engañar por un diseño aparentemente profesional. Los ciberdelincuentes han perfeccionado sus técnicas y pueden crear sitios web que parezcan legítimos. Investiga la reputación y la procedencia del sitio antes de confiar en él.

Mantén una **actitud escéptica** y **crítica al navegar.** Si algo te parece demasiado bueno para ser verdad, probablemente lo sea. En este bloque de contenido, vamos a estudiar cómo proteger tu seguridad digital y **aprender a identificar los sitios web fraudulentos** que acechan en la red.

Objetivos:

- Desarrollar la habilidad para identificar señales de alerta en sitios web que sugieran prácticas fraudulentas.
- Entender y aplicar métodos efectivos para verificar la autenticidad de un sitio web antes de compartir información personal o financiera.

Lecturas recomendadas:

- **Análisis de una web de venta falsa <https://www.incibe.es/ciudadania/blog/detectando-fraudes-analisis-de-una-web-de-venta-falsa>** (INCIBE). El artículo analiza una tienda online fraudulenta que vende productos de ropa, calzado y complementos.
- **Consejos de BBB sobre cómo identificar un sitio web falso <https://www.bbb.org/all/spot-a-scam/how-to-identify-a-fake-website>** (Better Business Bureau). Consejos prácticos para detectar sitios web falsos que pueden parecer legítimos pero están diseñados para estafar.

Estas son algunas de las formas más comunes en las que los estafadores utilizan sitios web falsos:

- **Tiendas online falsas con ofertas demasiado buenas para ser verdad.** Los estafadores crean tiendas online falsas que ofrecen ofertas increíbles y luego publican anuncios en las redes sociales. Estos sitios roban tu información de pago o te engañan para que compres productos fraudulentos.
- **Páginas de inicio de sesión con contraseñas falsas.** Los estafadores crean sitios que parecen páginas de inicio de sesión (tu banco, Netflix, etc.) y luego incluyen enlaces a ellos en mensajes de phishing.
- **Ventanas emergentes maliciosas que descargan malware.** Los delincuentes informáticos crean ventanas emergentes en sitios web legítimos que descargan malware en tu dispositivo.
- **Sitios web falsos de atención al cliente.** Los estafadores se hacen pasar por empresas de soporte técnico e intentan que les demos acceso remoto a nuestro ordenador.
- **Sitios web fraudulentos de seguridad social o seguros médicos.** Los delincuentes también pueden atacar tu información médica creando

sitios web falsos que te piden que “verifiques” tu número de seguridad social.

- **Sitios web falsos de entrega de paquetes.** Con el aumento de las compras en línea, los estafadores crean sitios web falsos que figen ser agencias de transporte como, UPS, Seur, Correos.
- **Sitios web falsos de reserva de vuelos.** Recientemente, han comenzado a crear sitios web falsos de reserva de billetes de avión que roban tu información personal o te venden billetes falsos.

Los sitios web falsos están por todas partes y cada vez son más difíciles de detectar. A continuación, te mostramos cómo puedes asegurarte de no estar tratando con un sitio web fraudulento:

1. Verifica detenidamente el nombre de dominio: La forma más sencilla de saber que estás en un sitio web falso es cuando el nombre de dominio no coincide con el sitio web oficial de la empresa. Por ejemplo, los estafadores suelen utilizar nombres de dominio similares (o incluso que contienen) la URL oficial dentro del nombre de dominio falso.

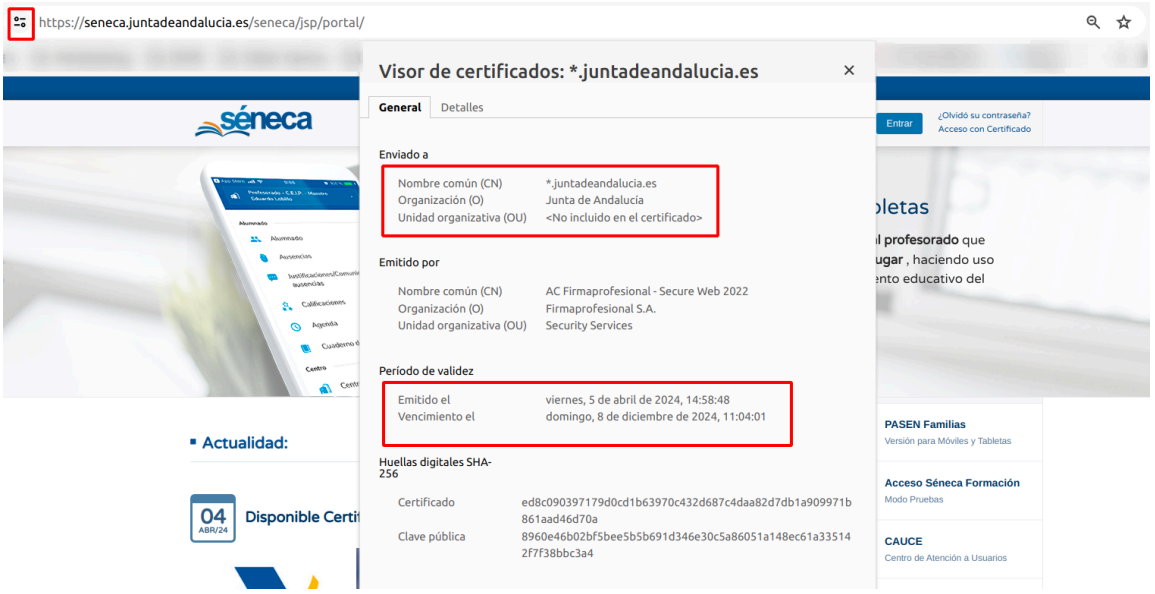
A continuación se muestran algunos ejemplos de cómo los estafadores falsifican dominios de sitios web:

- bancosanttander.es/particulares (agregando una “t” adicional)
- Paypal.com.secure-site.com (en este caso, el nombre de dominio es en realidad “secure-site.com”, no “paypal.com”)
- seneca.juntadeandaIucia.es/ (usando una “i” mayúscula en lugar de una “l” minúscula)
- Netflix-support.net (combinando un dominio falsificado con una extensión de dominio diferente)

2. Busca el símbolo de un candado (pero no confíes en él como único medio de verificación): Todos los navegadores web (como Safari, Firefox y Google Chrome) muestran si un sitio tiene lo que se llama un "certificado de seguridad". Este certificado, también conocido como certificado SSL, verifica que cualquier información que envíes al sitio no pueda ser interceptada por delicuentes informáticos.

Licencia: Dominio público

Desafortunadamente, los estafadores ya usan certificados SSL para engañarnos y hacernos creer que sus sitios falsos son genuinos. Si no estás seguro acerca de un sitio, haz clic en el candado y verifica cualquier información adicional sobre el certificado de seguridad.



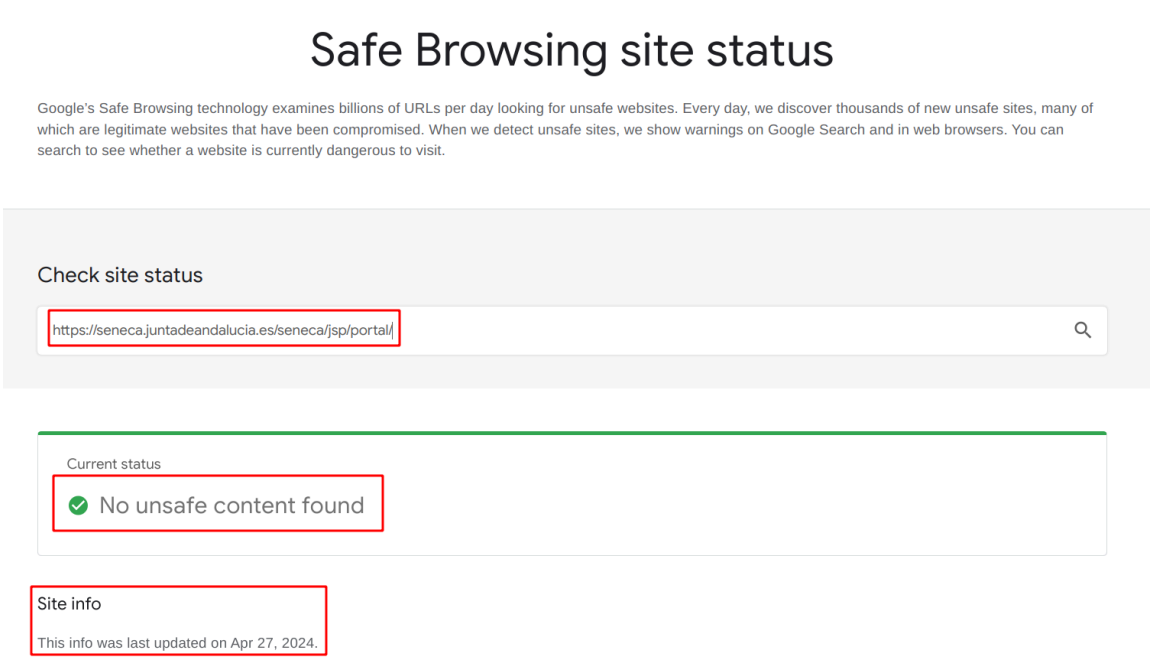
Licencia: Dominio público

Busca detalles como el nombre de la empresa registrada, el país de origen, la provincia o estado y la localidad, validez del certificado. Todas estas son señales de que el sitio web utiliza un nivel más alto de seguridad, conocido como “certificado de validación de organización (OV)”, que es más difícil de falsificar para los estafadores.

3. Utiliza un verificador de sitios web o herramientas de navegación segura: Un verificador de sitios web te ayuda a verificar si es seguro visitar un sitio web. Por ejemplo, te indica si el sitio utiliza cifrado para proteger tus datos, junto con el nivel de certificado de verificación del sitio.

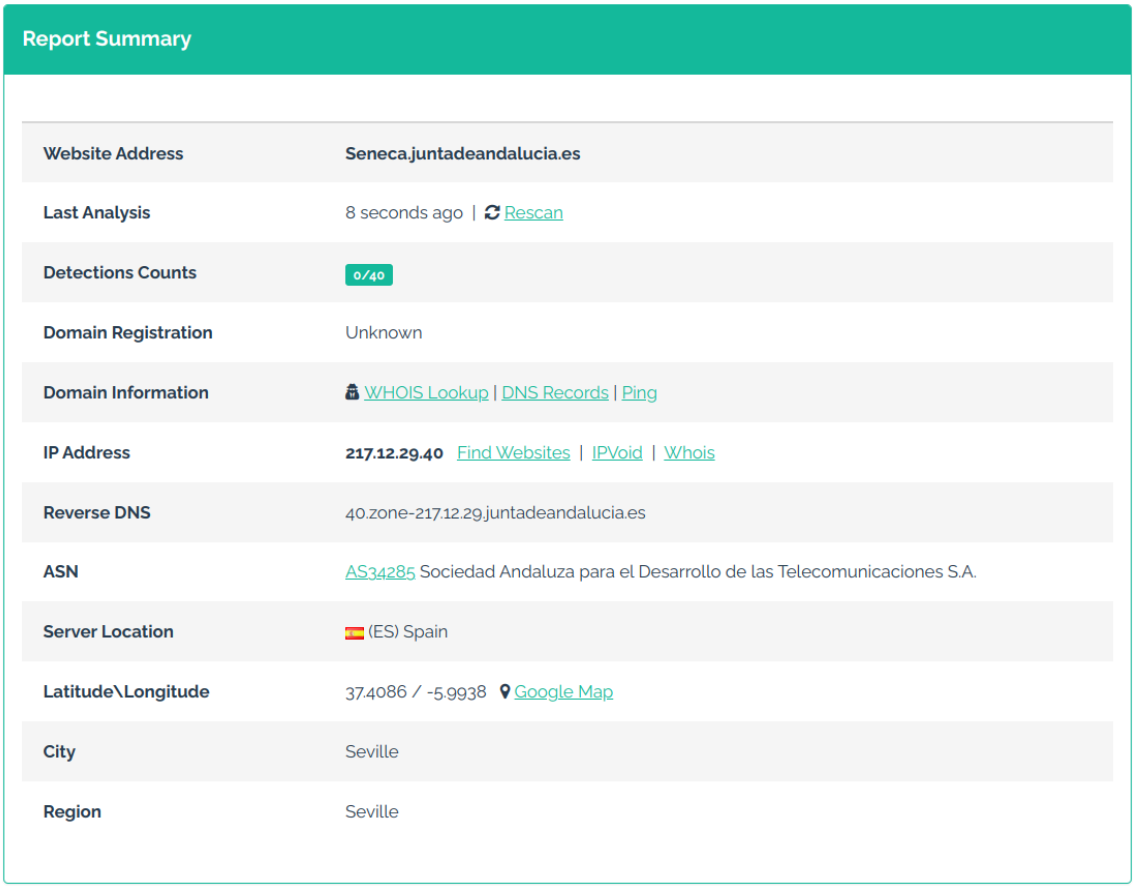
Existen algunos buenos recursos gratuitos que puedes utilizar para comprobar si un sitio web es seguro. En el bloque anterior ya vimos algunos de ellos, pero veamos algún otro recurso más que puede resultar interesante:

- El **Informe de transparencia de Google <https://transparencyreport.google.com/safe-browsing/search?hl=en>** es un recurso gratuito que examina miles de millones de URL diariamente para encontrar sitios web inseguros o comprometidos.



Licencia: Dominio público

- URLVoid <https://www.urlvoid.com/> es otra herramienta que escanea las URL en busca de contenido peligroso y las compara con bases de datos de sitios web fraudulentos conocidos.

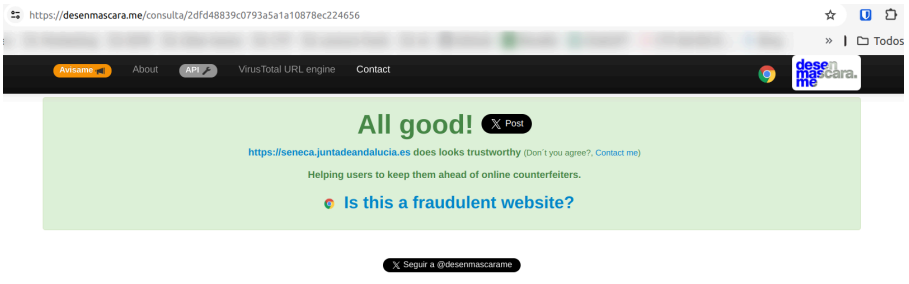


Report Summary

Website Address	Seneca.juntadeandalucia.es
Last Analysis	8 seconds ago | Rescan
Detections Counts	0/40
Domain Registration	Unknown
Domain Information	WHOIS Lookup | DNS Records | Ping
IP Address	217.12.29.40 Find Websites | IPVoid | Whois
Reverse DNS	40.zone-217.12.29.juntadeandalucia.es
ASN	AS34285 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
Server Location	(ES) Spain
Latitude\Longitude	37.4086 / -5.9938 Google Map
City	Seville
Region	Seville

Licencia: Dominio público

- La plataforma desenmascara.me <https://desenmascara.me/> analiza sitios web para determinar si son fraudulentos o no.



Licencia: Dominio público

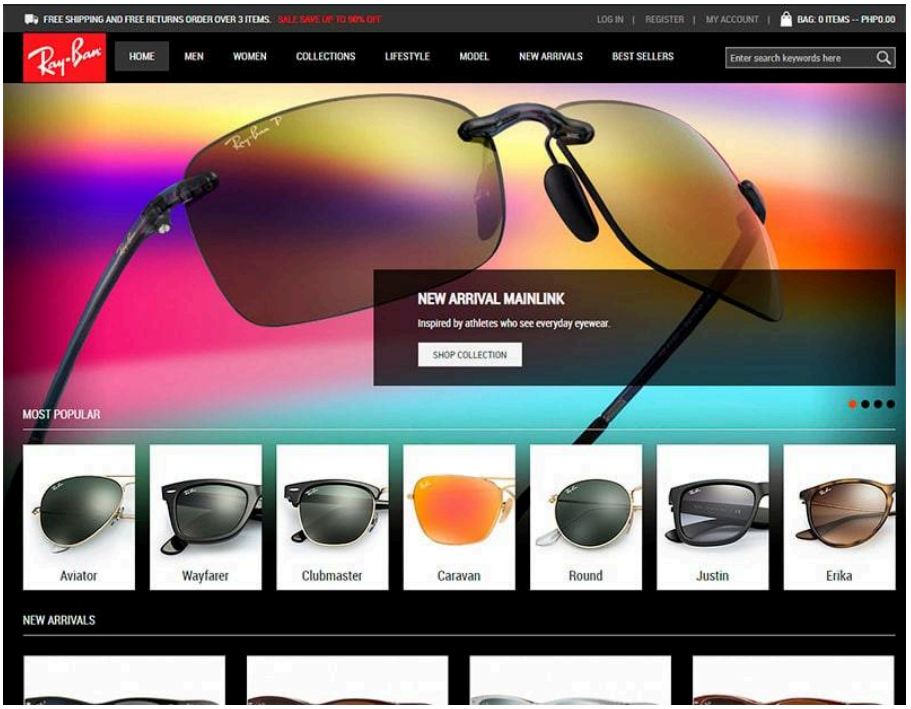
Además tienen un plugin para Google Chrome <https://chromewebstore.google.com/detail/desenmascarame-fake-web-v/egimhkfghkdkffalnjbkeoidpildondf> que nos puede ayudar a detectar webs fraudulentas a la vez que navegamos, sin necesidad de ir a la web de la herramienta.

4. Busca mala ortografía, problemas de diseño y otras señales de alerta: Los estafadores se mueven rápidamente y, a menudo, no quieren tardar demasiado en crear sitios web falsos (ya que podrían identificarse como fraudulentos y ser eliminados rapidamente). Al igual que los correos electrónicos y mensajes de texto fraudulentos, los sitios web de phishing a menudo incluyen fallos y errores básicos que las empresas legítimas no pasarían por alto.

5. Verifica la antigüedad del dominio (cuánto tiempo ha estado activo el sitio): Los sitios web falsos rara vez permanecen en línea por mucho tiempo. Una forma de saber si un sitio web es real o falso es comprobar cuánto tiempo ha estado activo mediante el rastreador de dominios Whois Lookup <https://whois.domaintools.com/> .

Licencia: Dominio público

6. Ten cuidado con las ofertas que parecen demasiado buenas para ser verdad: Los estafadores saben que estás dispuesto a dejar de lado tus sospechas a cambio de un buen trato.



Licencia: Dominio público

7. Busca reseñas de usuarios y compruebe si hay informes de estafas: En un esfuerzo por parecer más legítimos, los estafadores suelen publicar reseñas falsas en sus sitios web. Pero al mismo tiempo, los clientes reales (que podrían haber sido estafados) también pueden escribir reseñas advirtiéndote sobre sus experiencias. A continuación, se indican algunos consejos para detectar reseñas falsas:

- Hay muchas reseñas que suenan similares.
- Las reseñas carecen de detalles que incluiría un comprador real.
- Ten cuidado si te encuentras con reseñas genéricas que son inusualmente positivas y carecen de descripciones precisas de la experiencia del producto.

8. Lee la política de envíos y devoluciones: Las páginas oficiales tienen un apartado que detalla su política de envío y devolución. Si el sitio web en el que te encuentras no explica cómo devolver un artículo, es una estafa.

9. Cuidado con las opciones de pago no tradicionales: A veces, los sitios web falsos intentan obligarte a pagar productos utilizando métodos de pago no reversibles o no rastreables, como tarjetas de regalo, transferencias bancarias, criptomonedas o aplicaciones de pago como Zelle, Cash App y Venmo.

10. No te dejes engañar por “señales de confianza” (premios, logotipos de seguridad, etc.): Los estafadores saben que a los clientes les supone mucho trabajo investigar una marca para asegurarse de que sea legítima. También saben que es más probable que los consumidores compren en un sitio que muestre pruebas sociales de su credibilidad, como premios de la industria, certificaciones o logotipos de seguridad.

Denunciar a través de los Navegadores:

- **Google:** Puedes denunciarlo directamente a través de su departamento Safebrowsing en Reporte de Navegación Segura <https://safebrowsing.google.com/safebrowsing/report_phish/> .
- **Mozilla Firefox:** Abre Firefox, navega al sitio web fraudulento, haz clic en el icono del candado en la barra de direcciones, selecciona "Informar de este sitio web" y sigue las instrucciones para reportarlo.
- **Microsoft Edge:** Abre Edge, navega al sitio web fraudulento, haz clic en los tres puntos verticales en la esquina superior derecha, selecciona "Ayuda y comentarios", luego "Enviar comentarios" y elige la opción "Sitio web no seguro".

Denunciar ante Organismos Oficiales:

- En España, puedes interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado, como la Policía Nacional, la Guardia Civil, la Ertzaintza o los Mossos d'Esquadra. Puedes realizar la denuncia presencialmente en una comisaría o a través de los portales web de estos organismos.

Denunciar ante el INCIBE:

- El Instituto Nacional de Ciberseguridad (INCIBE) ofrece varios canales para reportar casos de fraude: Línea gratuita de Ayuda en Ciberseguridad 017, formularios de contacto <https://www.incibe.es/incibe-cert/incidentes/notificaciones> para ciudadanos, empresas y menores, y buzón de su Centro de Respuesta a Incidentes de Seguridad en incidencias@incibe-cert.es.

Actividad (opcional): Que no te den 'gato por liebre'

Descripción: Pon a prueba tus habilidades de detección de fraudes online con un test diseñado por el INCIBE. Accede al siguiente enlace y realiza el test de autoevaluación: Ponte a prueba VIII: ¿Cuánto sabes sobre ciberseguridad? <https://www.incibe.es/ciudadania/formacion/autoevaluacion/ponte-prueba-viii-cuanto-sabes-sobre-ciberseguridad> . Este test te ayudará a evaluar tu capacidad para identificar estafas y prácticas de seguridad cuestionables en internet.

Di NO al software pirata

El **software** se ha vuelto indispensable en nuestras vidas cotidianas. Ya sea para trabajar, estudiar o simplemente entretenernos, dependemos cada vez más de aplicaciones y programas informáticos. La posibilidad de obtener este software de manera gratuita a través de descargas piratas puede ser muy tentadora. Pero,

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

¿realmente vale la pena correr los riesgos?

El **software pirata** conlleva una serie de peligros que no deberían ignorarse. Uno de los principales problemas es la presencia de **malware y virus**. Estos programas maliciosos pueden dañar gravemente tu dispositivo, **robar tus datos personales** e incluso secuestrar tu sistema para pedir un rescate.

Pero los problemas no se limitan solo a la seguridad. Descargar y utilizar software pirata también puede acarrear consecuencias legales.

Objetivos:

- Concienciar sobre los riesgos y las consecuencias legales y de seguridad asociadas con la descarga y uso de software pirata.
- Identificar fuentes seguras de software y fomentar la adopción de prácticas responsables en la instalación y mantenimiento de software legítimo.

Lecturas recomendadas:

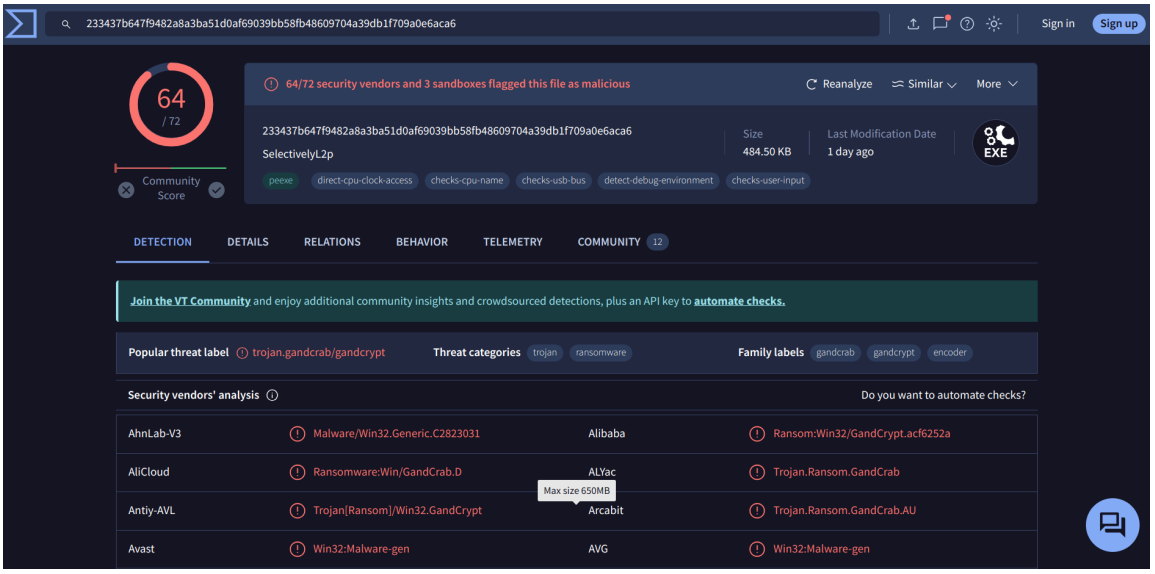
- Riesgos de descargar e instalar software pirata <https://www.infosegur.net/blog/riesgos-de-descargar-e-instalar-software-pirata> (InfoSegur). Un artículo que explora los riesgos asociados con el uso de software pirata, incluyendo la exposición a malware y las consecuencias legales.
- Peligros del software pirata <https://licendi.com/es/blog/peligros-del-software-pirata/> (Licendi). Este artículo detalla cómo el software pirata no solo pone en riesgo la seguridad informática, sino que también afecta el rendimiento del sistema y viola los derechos de autor.

Cuando descargamos archivos de internet, ya sea software, juegos, aplicaciones móviles o cualquier otro tipo de contenido, es importante tener en cuenta que, si no lo hemos descargado de fuentes oficiales, pueden contener **amenazas como virus, malware o código dañino**. Esto no solo aplica al software pirata, sino a cualquier archivo que obtengamos en línea, incluyendo adjuntos de correo electrónico.

Para asegurarnos de que un archivo es seguro antes de abrirlo o ejecutarlo, te recomendamos utilizar la **herramienta de análisis de virus de VirusTotal <https://www.virustotal.com/gui/home/upload>** . Es un servicio gratuito que permite escanear archivos y enlaces en busca de contenido malicioso utilizando más de 70 motores antivirus diferentes.

Simplemente sube el archivo que deseas analizar a VirusTotal o introduce la URL del enlace, y la herramienta te proporcionará un informe detallado sobre si el archivo contiene algún tipo de amenaza. Esto te permitirá tomar la decisión informada de si es seguro abrir o ejecutar el archivo.

A continuación vemos el informe del análisis de una aplicación descargada de una famosa web de descargas de software no legítimo:



Podemos ver que la aplicación, no solo tiene contenido malicioso, sino que es un ransomware, uno de los tipos de malwares mas dañinos.

Este problema se agrava aún más ya que, habitualmente, para instalar estas aplicaciones necesitamos **desactivar el antivirus**, **permitiendo así que cualquier 'bicho'** recién llegado a nuestro dispositivo **se mueva a sus anchas.**

Existen páginas web que proporcionan **alternativas legales y gratuitas** al software pirata, permitiéndote obtener programas de forma segura y sin infringir la ley. Algunas de estas plataformas son:

- **Alternativeto.net <https://alternativeto.net/>** : Esta página no aloja los programas en sus servidores, pero enlaza directamente a las páginas oficiales de cada aplicación, ofreciendo alternativas legales y seguras a programas populares.
- **Filepuma.com <https://www.filepuma.com/>** : Un repositorio que destaca por su simplicidad y organización, ofreciendo una amplia variedad de programas con capturas de pantalla y versiones antiguas para descargar.
- **Majorgeeks.com <https://www.majorgeeks.com/>** : Especializada en la difusión de freeware, esta web ofrece software propietario de alta calidad de forma gratuita, sin la necesidad de instalar software adicional no deseado.

Estas plataformas te brindan opciones legales y seguras para obtener software sin recurrir a la piratería, protegiendo tu dispositivo y respetando los derechos de autor de los desarrolladores. ¡Recuerda que hay alternativas éticas y legales para obtener el software que necesitas!

El ransomware es un tipo de malware que cifra los archivos de un dispositivo y exige un rescate a cambio de liberarlos. Pero tenemos buenas noticias, siguiendo las medidas de seguridad que hemos visto durante el curso, estamos protegidos.

Veamos unos **consejos clave** para protegernos de esta amenaza:

- **Evitar hacer clic en enlaces peligrosos:** Mantente alerta y evita hacer clic en enlaces sospechosos que puedan llevar a la descarga de ransomware.
- **No abrir archivos adjuntos de correos electrónicos sospechosos:** Ten precaución al abrir archivos adjuntos de correos electrónicos de remitentes desconocidos o sospechosos, ya que pueden contener ransomware.
- **Mantener tus aplicaciones actualizadas:** Instala las actualizaciones de las aplicaciones y sistema operativo tan pronto como estén disponibles. Muchos ataques de ransomware explotan vulnerabilidades en software desactualizado.
- **Utilizar software antivirus y antimalware:** Asegúrate de tener un buen programa antivirus instalado y actualizado. Realiza escaneos regulares de tu sistema para detectar y eliminar amenazas potenciales.
- **Realizar copias de seguridad periódicas:** Mantén copias de seguridad actualizadas de tus archivos importantes en un disco duro externo y desconéctalo después de crear la copia de seguridad para evitar que también se cifren en caso de un ataque de ransomware.

Siguiendo estos consejos y manteniendo una cultura de seguridad, podrás reducir significativamente el riesgo de ser víctima de ransomware y proteger tus datos de posibles ataques.

Actividad (opcional): Análisis de archivos con VirusTotal

Descripción: Aprende a utilizar VirusTotal para analizar archivos y enlaces y detectar posibles amenazas de seguridad. Esta herramienta te permitirá verificar la seguridad de los archivos antes de abrirlos, especialmente aquellos descargados de internet.

Pasos:

- Accede a VirusTotal utilizando el siguiente enlace: **VirusTotal <https://www.virustotal.com/gui/home/upload>** .
- Selecciona la opción para subir un archivo que desees analizar. Puedes elegir un archivo inofensivo de tu ordenador para comenzar.
- Analiza un segundo archivo que hayas descargado recientemente de internet y que consideres potencialmente peligroso, o simplemente uno que desees comprobar.
- Observa y compara los resultados de ambos análisis. VirusTotal te proporcionará un informe detallado indicando si se detectaron amenazas.

Recursos necesarios:

- Acceso a internet.
- Archivos para analizar.
- Enlace a la página de VirusTotal.

Recursos educativos

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Explora estos **recursos** para enseñar ciberseguridad: actividades, lecturas y más, diseñados para **promover** la **seguridad** durante la **navegación** y la **detección** de **sitios webs fraudulentos** entre nuestros estudiantes.

- **Lista de tareas para navegar de forma segura:** Guía práctica para asegurarte de que tienes todo al día en seguridad online. Ver lista <https://www.incibe.es/menores/materiales/lista-de-tareas-para-navegar-de-forma-segura-lo-tienes-todo-al-dia> .
- **Refranero de las compras seguras online:** Recopilación de refranes relacionados con las compras seguras en línea y consejos prácticos. Descargar PDF <https://www.incibe.es/sites/default/files/docs/refraneo_compras_seguras_online.pdf> .
- **Hoja de ruta para compras online seguras:** Documento PDF que ofrece una guía paso a paso para realizar compras online de manera segura. Descargar PDF <https://www.incibe.es/sites/default/files/docs/senior/osi_hoja_ruta_compras_online_seguras.pdf> .
- **Vídeo explicativo sobre fraude online:** Vídeo educativo que explica las diferentes formas de fraude online y cómo protegerse. Ver vídeo <https://www.youtube.com/watch?v=cp8uFVnJ16c> .
- **Objetivo cero fraudes online:** Infografía educativa diseñada para ayudar a prevenir fraudes en internet. Descargar PDF

<https://www.incibe.es/sites/default/files/contenidos/materiales/Campanas/Fraudesonline/is4k_objetivo_cero_fraudes_online.pdf> .

Módulo 3. Protección de amenazas en línea

3.3 Correos fortificados

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

En el bloque **'Correos fortificados'**, nos adentramos en la importancia de **proteger** nuestras **comunicaciones electrónicas** en el ciberespacio. Con el aumento de amenazas y vulnerabilidades, garantizar la seguridad de nuestros correos electrónicos se convierte en una prioridad.

Descubriremos estrategias para fortalecer la protección de nuestros correos, desde la configuración de **filtros antispam** hasta el uso de **cifrado de extremo a extremo**. Además, exploraremos la importancia de la autenticación de dos factores **y otras medidas** de seguridad para salvaguardar la confidencialidad y la integridad de nuestra correspondencia digital.

Blindando tu buzón

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Como hemos visto anteriormente, los ciberdelincuentes utilizan el **correo electrónico** como una de las principales **vías de ataque**, enviando mensajes maliciosos diseñados para robar información, instalar malware o estafar a las víctimas.

Mantener un sistema de **filtrado antispam robusto** es clave para evitar que estos correos dañinos lleguen a tu bandeja de entrada. Los filtros avanzados pueden detectar patrones sospechosos en el remitente, el asunto, el contenido y los enlaces, bloqueando automáticamente los mensajes que representen un riesgo.

Además, los filtros antispam te ayudan a mantener tu buzón organizado y libre de mensajes no deseados, mejorando tu productividad y evitando que te distraigas con correos irrelevantes.

Objetivos:

- Comprender cómo los filtros antispam pueden mejorar nuestra seguridad al identificar y bloquear correos electrónicos potencialmente peligrosos.
- Fortalecer la seguridad del buzón de correo mediante la configuración adecuada de filtros antispam para minimizar la recepción de correos maliciosos.

Lecturas recomendadas:

- El spam y el phishing en 2023 (securelist) <https://securelist.lat/spam-phishing-report-2023/98496/> . Este artículo analiza el estado del

spam y phising en durante el año 2023. Cómo dato interesante, el 45,60% de los correos electrónicos en todo el mundo eran spam.

- **Filtro antispam de Gmail <https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/filtro-antispam-de-gmail/>** (IONOS). Este artículo proporciona una visión detallada sobre cómo funciona el filtro antispam de Gmail, ofreciendo consejos para optimizar la gestión del correo no deseado.

Los filtros antispam ofrecen **importantes ventajas**, como mantener la bandeja de entrada limpia, proteger contra amenazas y mejorar la productividad. Sin embargo, también pueden tener **algunos inconvenientes**, como bloquear por error correos legítimos (falsos positivos) o requerir ajustes periódicos.

Los filtros antispam se vuelven más efectivos con el tiempo a medida que "aprenden" a identificar el spam. Es importante **marcar los correos no deseados como spam en lugar de eliminarlos** directamente. Del mismo modo, si un **correo legítimo llega a la bandeja de spam**, asegúrate de **marcarlo como "No es spam"** antes de moverlo a la bandeja de entrada para

que el filtro aprenda a reconocerlo. Esto permite que el filtro analice esos mensajes y mejore su capacidad de detección.

Una forma más avanzada de evitar que tu buzón de entrada se vea inundado con correo basura es estableciendo el filtrado activo de correo haciendo uso de reglas.

Directrices para personalizar un filtro antispam:

- **Ajustar la sensibilidad del filtro:** Aumentar la sensibilidad para bloquear más agresivamente el spam. Disminuir la sensibilidad si el filtro está bloqueando demasiados correos legítimos.
- **Crear reglas de filtrado personalizadas:** Filtrar por remitente (dominio o dirección de correo), palabras clave en el asunto o contenido del mensaje, tipo o tamaño de archivos adjuntos. Permitir correos de contactos incluidos en la libreta de direcciones.
- **Utilizar listas blancas y negras:** Agregar a la lista blanca los remitentes de confianza para asegurar que sus mensajes no se bloqueen. Incluir en la lista negra los remitentes o dominios claramente identificados como spam.
- **Monitorear y ajustar el filtro periódicamente:** Revisar los correos marcados como spam y recuperar los que hayan sido filtrados por error. Actualizar las reglas y listas según la evolución del spam recibido.

Para más información, **consulta la documentación oficial** de tu proveedor de correo:

- Outlook <https://support.office.com/es-es/article/cambiar-el-nivel-de-protecci%C3%B3n-en-el-filtro-de-correo-no-deseado-e89c12d8-9d61-4320-8c57-d982c8d52f6b>

- Gmail <https://support.google.com/mail/answer/6579?hl=es>
- Yahoo! Mail <https://es.ayuda.yahoo.com/kb/SLN26427.html?_guc_consent_skip=1537958916&guccounter=1>
- Mozilla Thunderbird <https://support.mozilla.org/es/kb/thunderbird-y-el-correo-basura>

Tanto si decides hacer uso de filtros antispam como si no, te **recomendamos**:

- **Nunca publiques tu dirección de correo en sitios web** para evitar que sea recopilada por **spammers**. Si por alguna causa tuvieras que hacerlo, publícalo de esta manera: nombredeusuario[espacio]arroba[espacio]dominio[punto]com. De esa manera los rastreadores no se harán con el.
- No reenvíes cadenas de emails con las direcciones de los destinatarios a la vista, usa **Copia Oculta (CCO)**.
- **No intentes darte de baja** del spam, ya que los ciberdelincuentes **lo utilizan para detectar cuentas activas**.
- **Utiliza un 'correo basura'** para registrarte en foros, blogs y otros sitios que no son de gran importancia. Esta dirección de correo alternativa te ayudará a mantener tu cuenta principal libre de spam y mensajes no deseados.

Actividad (opcional): Configura tu propio filtro antispam

Descripción: Aprende a configurar filtros antispam en tu cuenta de correo para mejorar tu seguridad online.

Pasos:

1. Accede a la configuración de tu servicio de correo electrónico.
2. Busca la sección de filtros o seguridad y crea un filtro antispam.
3. Ajusta los parámetros según tus necesidades y guarda los cambios.

Recursos necesarios:

- Acceso a una cuenta de correo electrónico.
- Guías de usuario del proveedor de correo (enlaces a sitios oficiales de Gmail, Outlook, etc.).

Salvaguardando tus conversaciones

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Los ciberdelincuentes están constantemente buscando formas de interceptar y acceder a la información que compartimos a través del email, lo que puede tener graves consecuencias para nuestra seguridad y la de nuestros contactos.

Afortunadamente, existen **herramientas** y **servicios** que nos permiten fortalecer la **protección** de nuestros **correos electrónicos** mediante el **cifrado** de extremo a extremo. Esta tecnología garantiza que solo el remitente y el destinatario puedan acceder al contenido de los mensajes, evitando que terceros no autorizados puedan leerlos o manipularlos.

Además, existen servicios de correo electrónico, como **ProtonMail**, que integran el cifrado de extremo a extremo de manera nativa, simplificando el proceso de proteger nuestra privacidad.

Objetivos:

- Entender la importancia del cifrado de extremo a extremo para asegurar la confidencialidad y la integridad de las comunicaciones por correo electrónico.
- Conocer herramientas de cifrado para proteger eficazmente la información personal y profesional.

Lecturas recomendadas:

- **Cifrado de extremo a extremo: ¿Qué es y cómo funciona? <https://blog.mailfence.com/es/cifrado-de-extremo-a-extremo-para-e-mail/>** (mailfence). Un artículo que explica cómo funciona el cifrado de extremo a extremo y qué protección nos ofrece.
- **Cifrado PGP en Gmail, Outlook y Mailvelope <https://www.redeszone.net/tutoriales/seguridad/cifrado-pgp-gmail-outlook-mailvelope/>** (RedesZone). Este artículo ofrece una guía práctica sobre cómo implementar el cifrado PGP en los servicios de correo más comunes como Gmail y Outlook, utilizando la extensión Mailvelope para facilitar el proceso.

El cifrado **PGP (Pretty Good Privacy)** se ha consolidado como uno de los métodos más efectivos para **proteger la privacidad y seguridad** de las comunicaciones por correo electrónico. Sin embargo, su **adopción**

generalizada se ha visto **obstaculizada** por la falta de interés y apoyo de los principales proveedores de servicios de correo.

Basado en un sistema de cifrado de clave pública, PGP permite a los usuarios enviar mensajes completamente protegidos de miradas indiscretas, incluyendo la de los propios proveedores de correo. Paradójicamente, esta característica que proporciona un alto nivel de privacidad, representa un inconveniente para estas empresas desde una perspectiva comercial.

A pesar de sus innegables beneficios en términos de seguridad y confidencialidad, el cifrado PGP se ha visto relegado a un segundo plano en el panorama actual de los servicios de correo electrónico debido a que los **intereses comerciales** de los proveedores de correo **prevalecen sobre la privacidad** de los usuarios. La mayoría de estos proveedores no solo no facilitan la implementación de PGP, sino que además complican su uso, obligando a los usuarios a gestionar el cifrado manualmente, lo que requiere un esfuerzo considerable.

Para aquellos interesados en utilizar el cifrado PGP en sus cuentas de correo, recomendamos los siguientes tutoriales:

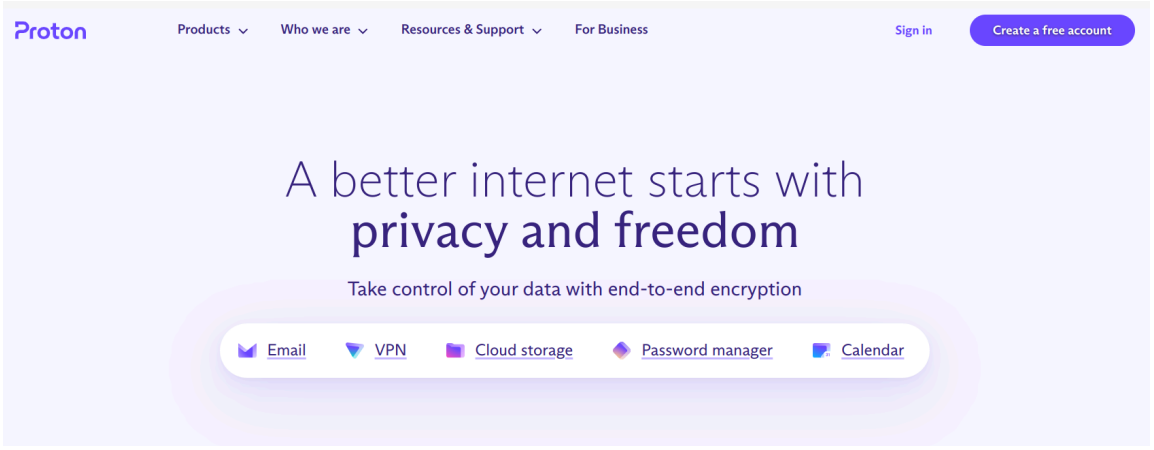
- **Configurar OpenPGP en Thunderbird para correos cifrados <https://www.redeszone.net/tutoriales/seguridad/configurar-openpgp-thunberbird-emails-cifrados/>** (RedesZone). Este artículo ofrece una guía detallada sobre cómo implementar PGP en Thunderbird, permitiendo cifrar y descifrar correos de manera efectiva.
- **Cifrado PGP en Gmail, Outlook y Mailvelope <https://www.redeszone.net/tutoriales/seguridad/cifrado-pgp-gmail-outlook-mailvelope/>** (RedesZone). Aprende a configurar PGP en Gmail y Outlook utilizando Mailvelope para una comunicación segura y privada.

Como **alternativa**, servicios como **ProtonMail** ofrecen **integración nativa de cifrado PGP**, proporcionando una solución más accesible y directa para quienes valoran la seguridad y la privacidad.

ProtonMail es un servicio de correo electrónico que se ha posicionado como una **alternativa segura y privada** a los principales proveedores de correo como Gmail, Outlook y Yahoo Mail. Impulsado por un fuerte compromiso con la privacidad y la seguridad de las comunicaciones, ofrece características que lo diferencian de la competencia.

- **Cifrado de extremo a extremo:** Los mensajes se cifran en el dispositivo del usuario antes de ser enviados y solo pueden ser descifrados por el destinatario. Es imposible que terceros, incluyendo el propio ProtonMail, puedan acceder al contenido de los mensajes cifrados.
- **Privacidad y anonimato:** ProtonMail permite a los usuarios permanecer completamente anónimos, ya que no requiere información personal para registrarse. Además, ofrece la posibilidad de utilizar alias ilimitados a través de servicios como SimpleLogin, ayudando a mantener separadas las diferentes identidades y actividades en línea.
- **Correspondencia privada:** ProtonMail incluye la verificación de la dirección para asegurar que solo el destinatario previsto pueda acceder al mensaje.
- **Servidores seguros:** ProtonMail tiene sus servidores ubicados en Suiza, un país con estrictas leyes de privacidad. Los servidores están alojados en una instalación militar subterránea con altos niveles de seguridad física y digital.
- **Planes flexibles y gratuitos:** ProtonMail ofrece una opción gratuita con 1 GB de almacenamiento y 150 correos por día.

Para probar ProtonMail y disfrutar de una comunicación segura, **regístrate y crea una cuenta <https://proton.me/>** visitando su sitio web.



Proton Mail (Dominio público)

SimpleLogin es un servicio que permite a los usuarios crear alias de correo electrónico ilimitados. Esto ayuda a mantener su identidad y dirección de correo electrónico principal separada de las diferentes actividades y registros en línea.

¿Cómo funciona? SimpleLogin actúa como un intermediario entre el usuario y los servicios en línea. Cuando es necesario proporcionar una dirección de correo electrónico, el usuario crea un alias único a través de SimpleLogin. Todos los correos enviados a ese alias son redirigidos a la dirección de correo electrónico principal del usuario.

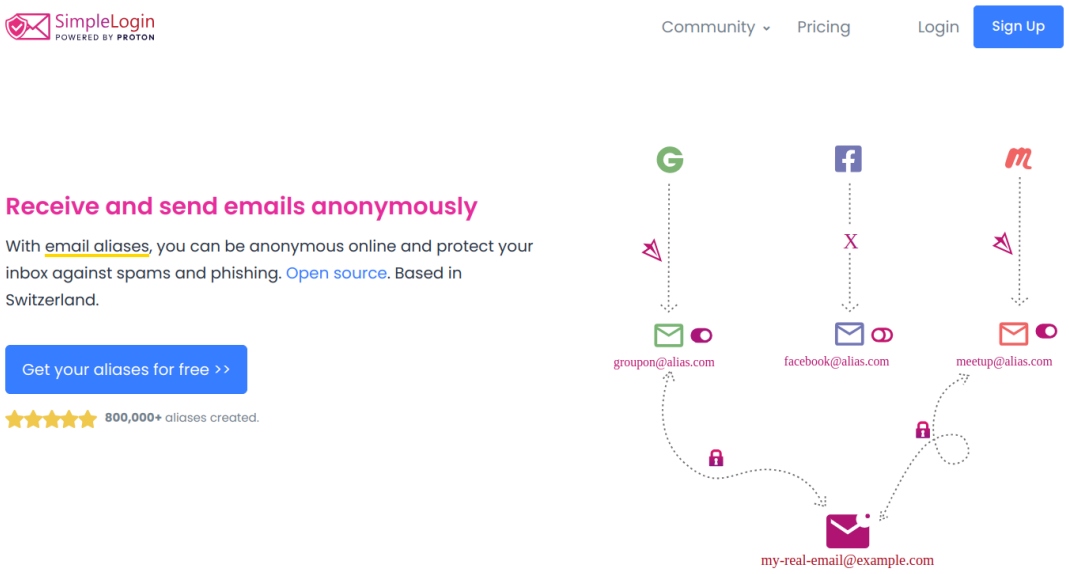
¿Para qué sirve? SimpleLogin ayuda a proteger la privacidad y la identidad de los usuarios de varias maneras:

- Evita que la dirección de correo electrónico principal se exponga en múltiples sitios web.

- Permite a los usuarios tener un mayor control sobre la información que comparten en línea.
- Facilita la gestión de suscripciones y registros, ya que los alias pueden ser desactivados o eliminados fácilmente.
- Ayuda a detectar y bloquear el spam, ya que los correos enviados a alias específicos pueden ser identificados y filtrados.
- Ofrece una capa de seguridad adicional. Si un servicio en el que has utilizado un alias de SimpleLogin es comprometido, tu cuenta y contraseña principal permanecen seguras, ya que los datos de acceso expuestos no están vinculados a tu identidad principal.

SimpleLogin **se puede utilizar** en conjunto **con** servicios de correo electrónico como **Gmail, Yahoo, Outlook y Thunderbird**, y por supuesto, **ProtonMail**, brindando una capa adicional de privacidad y seguridad.

Para probar SimpleLogin y disfrutar de mayor control sobre tu privacidad, **regístrate y crea una cuenta <https://simplelogin.io/>** visitando su sitio web.



SimpleLogin (Dominio público)

Actividad (opcional): Uso de SimpleLogin para proteger la seguridad y privacidad.

Descripción: Aprende a gestionar múltiples identidades sin exponer tu dirección principal. Crea una cuenta en SimpleLogin para configurar alias de correo electrónico y proteger tu identidad en línea.

Pasos:

1. Crea una cuenta en SimpleLogin.
2. Configura varios alias de correo electrónico.
3. Utiliza estos alias para registrarte en diferentes servicios en línea.
4. Comparte en el foro del curso cómo estos alias pueden ayudar a proteger tu seguridad y privacidad.

Recursos:

- Acceso a Internet
- Ordenador o dispositivo móvil
- Enlace al **sitio web de SimpleLogin <https://simplelogin.io/>** .

Claves para el control de sesiones

Imagen generada con IA (Midjourney) (CC BY-NC-SA

Imagina la situación de un estudiante que, después de una clase en el aula de informática, **olvida cerrar su** sesión de **correo electrónico**. Esta vulnerabilidad puede exponer información confidencial y abrir la puerta a posibles abusos.

Siempre que abrimos nuestra cuenta de correo en algún equipo público tenemos ciertos riesgos. A fin de cuentas va a ser un ordenador al que pueden acceder muchos

<http://creativecommons.org/licenses/?lang=es>) usuarios. Existen diversas estrategias para evitar situaciones como la descrita anteriormente y reforzar la seguridad de nuestras cuentas. El **cierre de sesión remoto** y la **navegación anónima** son aliados en la protección de tus datos. Además, la **autenticación de dos factores** fortalece la seguridad frente a accesos no autorizados.

Objetivos:

- Concienciar sobre la importancia de cerrar la sesión en dispositivos compartidos para proteger la información confidencial.
- Conocer estrategias de seguridad como la navegación en modo incógnito y el cierre de sesión remoto para el control efectivo de accesos.

Lecturas recomendadas:

- **Los riesgos de abrir tu correo en un ordenador público <https://www.redeszone.net/noticias/seguridad/riesgos-abrir-correo-ordenador-publico/>** (RedesZone). Un artículo que destaca los peligros de acceder a cuentas de correo desde ordenadores compartidos y cómo protegerse.
- **Cómo evitar intrusos en tu correo y consejos de seguridad <https://www.redeszone.net/tutoriales/seguridad/intrusos-correo-consejos-seguridad/>** (RedesZone). Ofrece estrategias para mantener seguras las cuentas de correo electrónico y evitar accesos no autorizados.

Las consecuencias de un acceso no autorizado a tu correo electrónico son graves:

- **Acceso a información personal:** Pueden leer tus mensajes, acceder a archivos adjuntos con datos sensibles como facturas, contratos o información bancaria.
- **Robo de cuentas vinculadas:** Si tienes cuentas vinculadas a tu correo electrónico, como redes sociales o servicios bancarios, los intrusos pueden intentar acceder a ellas y realizar acciones maliciosas.
- **Reinicio de contraseñas:** Seguro que en alguna ocasión te has olvidado de la contraseña para entrar en alguna red social, como podría ser Facebook, o cualquier página web. Le has dado a recordar y te han enviado la clave al e-mail. Si un intruso tuviera acceso a la cuenta de correo electrónico, automáticamente podría tener el control de otras muchas cuentas.
- **Suplantación de identidad:** Pueden enviar correos electrónicos en tu nombre, engañando a tus contactos para obtener información confidencial o realizar estafas.
- **Robo de identidad digital:** Utilizando la información obtenida de tu correo electrónico, los intrusos pueden robar tu identidad en línea y cometer fraudes en tu nombre.
- **Difusión de malware:** Pueden enviar correos electrónicos con enlaces maliciosos o adjuntos infectados para propagar malware entre tus contactos.
- **Extorsión y chantaje:** Pueden utilizar información comprometedora encontrada en tu correo electrónico para extorsionarte o chantajearte.

Para proteger la cuenta de correo electrónico, es fundamental seguir una serie de medidas de seguridad que ayudarán a prevenir accesos no

autorizados y mantener la privacidad de la información. Algunas recomendaciones clave incluyen:

- **Utilizar contraseñas únicas y seguras:** Se debe crear una contraseña robusta que combine letras, números y caracteres especiales, evitando información personal fácil de adivinar.
- **No exponer la dirección de forma pública:** Hemos hablado anteriormente de uno de los problemas del correo electrónico, la entrada de Spam. Puede ser utilizado como un medio para colar malware en nuestros sistemas. ¿Cómo obtienen nuestra dirección de correo electrónico? Una de las formas más comunes es a través de bots que rastrean la red en busca de direcciones para incluir en su lista.
- **Activar la autenticación de dos factores (2FA):** La autenticación de dos factores añade una capa adicional de seguridad al requerir un segundo método de verificación, como un código enviado al teléfono móvil, para acceder a la cuenta.
- **No almacenar datos sensibles en correos:** Evitar enviar o almacenar información confidencial como contraseñas en correos electrónicos, ya que podrían ser vulnerables en caso de acceso no autorizado.
- **Mantener actualizado el software y el navegador:** Es importante mantener actualizados tanto el software de seguridad como el navegador para protegerse contra posibles vulnerabilidades.
- **No compartir contraseñas ni dejar sesiones abiertas:** Es fundamental no compartir contraseñas con terceros y cerrar las sesiones de correo electrónico en dispositivos compartidos o públicos para evitar accesos no autorizados.
- **No uses la misma cuenta para todo:** Algo que va relacionado con el punto de no exponer nuestro email, pero que no solo aplica a ello, sino que, utilizar la misma cuenta para muchos servicios, aunque no mostremos la dirección, puede ser muy peligroso, debido a las filtraciones de alguna webs, donde podrán conseguir nuestra contraseña y correo, y esto, si lo usamos en todos los lugares, dará acceso a más cuentas nuestras.
- **Sentido común:** Si hay algo imprescindible para proteger las cuentas de correo electrónico o cualquier otro servicio que usemos en nuestro día a día es el sentido común. Ser cauteloso con correos electrónicos no solicitados, enlaces desconocidos, archivos adjuntos sospechosos que podrían contener malware, iniciar sesión en plataformas no oficiales o desde links sospechosos, etc.

Recordemos que muchas de estas medidas ya han sido discutidas en diferentes partes del curso, reforzando la importancia de una buena higiene digital. Por ello, nos centraremos en aquellas no abordadas previamente, como el control de sesiones.

En la introducción de este apartado, hablábamos de una situación; Acabábamos una clase en el aula de informática, salimos del aula, y cuando nos estamos dirigiendo a la sala de profesorado, un estudiante se acerca a decirnos que se ha dejado la sesión de correo abierta. Esta es una situación que se puede dar fácilmente. Pero **no son solo los estudiantes**, todos estamos expuestos a cometer un error, **con frecuencia, se observan sesiones de correo abiertas en salas de profesores y en los ordenadores de las aulas**, lo que puede exponer datos sensibles y comprometer la privacidad.

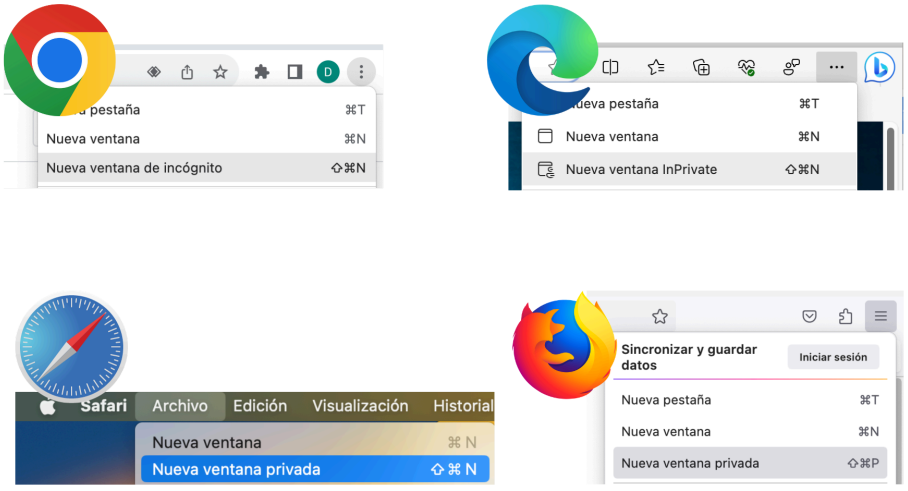
Para abordar esta preocupación, el **uso de la navegación privada** se convierte en una herramienta clave para evitar dejar sesiones de correo abiertas accidentalmente.

Beneficios de la navegación privada en entornos educativos:

- **Protección de datos sensibles:** Al utilizar la navegación privada, se evita que las credenciales de correo electrónico queden almacenadas en el historial del navegador, reduciendo el riesgo de accesos no autorizados.
- **Cierre automático de sesión:** La mayor ventaja de utilizar la navegación privada es que cuando se cierra la ventana del navegador, toda la información de la sesión, incluyendo el inicio de sesión en la cuenta de correo electrónico, desaparece por completo. Esto evita que otros usuarios puedan acceder a la cuenta después de que te hayas desconectado, ya que no queda rastro de la actividad realizada.

Pasos para activar la navegación privada:

- En Google Chrome: Abre el navegador, haz clic en los tres puntos verticales en la esquina superior derecha y selecciona "Nueva ventana de incógnito".
- En Mozilla Firefox: Accede al menú principal y elige "Nueva ventana privada".
- En Safari: Selecciona "Nueva ventana privada" desde el menú Archivo.
- En Microsoft Edge: Abre el navegador, haz clic en los tres puntos horizontales en la esquina superior derecha, y selecciona "Nueva ventana de InPrivate".



Licencia: Dominio público

Al fomentar el **uso de la navegación privada en entornos educativos**, se **promueve la protección de la privacidad y la seguridad de las cuentas de correo electrónico**, evitando posibles accesos no autorizados y garantizando la confidencialidad de la información personal y profesional.

Desde nuestra cuenta de email, podemos comprobar qué sesiones hay abiertas, cuándo se ha iniciado sesión, y los intentos de inicio de sesión fallidos o incompletos. Dependiendo del servicio de correo, esta información está en unos lugares u otros.

Para verificar y gestionar las sesiones abiertas en plataformas populares de correo electrónico, se pueden seguir los siguientes pasos:

- **Gmail:** Para revisar las sesiones abiertas en tu cuenta de Gmail, inicia sesión en tu cuenta de Gmail. En la parte inferior derecha, haz clic en "Detalles" para ver la actividad reciente en tu cuenta. También puedes visitar la página de **Última actividad de la cuenta <https://support.google.com/mail/answer/45938?hl=es>** para ver actualizaciones de seguridad de toda tu Cuenta de Google.
- **Outlook:** Para revisar las sesiones abiertas en tu cuenta de Outlook, inicia sesión en tu cuenta de Outlook. Accede a la sección de **Actividad reciente <https://account.live.com/activity>** para ver los dispositivos y ubicaciones desde donde se ha accedido a tu cuenta.
- **Yahoo:** Para revisar las sesiones abiertas en tu cuenta de Yahoo, inicia sesión en tu cuenta de Yahoo. Navega a la sección de **Actividad reciente <https://login.yahoo.com/account/activity?.lang=es-ES&.intl=es&.src=yhelp>** para ver los detalles de las sesiones activas.
- **Thunderbird:** Al ser un cliente de correo electrónico de escritorio, no proporciona una funcionalidad integrada para revisar sesiones abiertas.

Todos podemos tener un **despiste** y dejarmos una **sesión de correo abierta en un dispositivo compartido**. Veamos cómo cerrarlas remotamente en los principales proveedores de correo electrónico.

Para cerrar sesiones de Gmail remotamente:

- Abre Gmail.
- Haz clic en tu foto (arriba a la derecha).
- Haz clic en Gestionar tu cuenta de Google.
- Haz clic en Seguridad.
- En "Tus dispositivos", haz clic en Gestionar todos los dispositivos.
- Elige un dispositivo.
- Haz clic en Cerrar sesión.

Para cerrar sesiones de Outlook remotamente:

- Inicia sesión en tu cuenta en la página web de Microsoft.
- Haz clic en "Seguridad" en la parte superior de la página.
- En la sección "Actividad reciente", haz clic en "Revisa tus actividades recientes".
- En la lista de dispositivos y ubicaciones, busca el dispositivo en el que iniciaste sesión y haz clic en "Cerrar sesión".
- Confirma que deseas cerrar la sesión en ese dispositivo.

Para cerrar sesiones de Yahoo remotamente:

- Inicia sesión en tu cuenta de Yahoo.
- Accede a la sección de "Seguridad y privacidad".
- Cierra las sesiones activas que no reconozcas.

Thunderbird: Al ser un cliente de correo de escritorio, no ofrece una funcionalidad integrada para cerrar sesiones remotamente.

Actividad (opcional): Revisión de seguridad del correo electrónico

Descripción: Realiza una revisión completa de la seguridad de tu correo electrónico para asegurarte de que estás aplicando las medidas de seguridad recomendadas, verificando las sesiones abiertas y probando el cierre de sesión en modo incógnito.

Pasos:

1. Asegúrate de que estás implementando las prácticas recomendadas.
2. Accede a la sección de seguridad de tu servicio de correo electrónico y revisa todas las sesiones activas. Cierra aquellas que no reconozcas o que sean antiguas.
3. Probar el cierre de sesión en modo incógnito: Abre tu correo electrónico en una ventana de incógnito, inicia sesión y luego cierra la ventana.
4. Verifica que la sesión se haya cerrado correctamente para asegurarte de que no se guarden datos de acceso.

Recursos:

- Acceso a tu cuenta de correo electrónico
- Enlace a la sección de seguridad de tu proveedor de correo
- Navegador web en modo incógnito

Recursos educativos

Imagen generada con IA (Midjourney) (CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

Explora estos **recursos** para enseñar ciberseguridad: actividades, lecturas y más, diseñados para **promover** un **uso seguro del correo electrónico** entre nuestros estudiantes.

- **Seguridad en el correo electrónico - 10 pasos:** Infografía que proporciona una guía práctica sobre cómo asegurar tu correo electrónico. Ver infografía <https://www.incibe.es/empresas/blog/seguridad-el-correo-electronico-si-tan-solo-10-pasos> .
- **La Oca del Phishing:** Juego de mesa interactivo que enseña sobre el phishing de manera divertida y educativa. Acceder al juego <https://www.incibe.es/ciudadania/juegos/juegos-mesa/la-oca-phishing> .
- **Actividad Interactiva - Prueba de detección de ingeniería social:** Actividad para mejorar tus habilidades de detección de técnicas de ingeniería social. Acceder a la actividad <https://www.incibe.es/ciudadania/formacion/actividades/prueba-deteccion-ingenieria-social> .
- **Cartel Phishing Consejo4Kids:** Material educativo diseñado para enseñar a los niños sobre el phishing de manera accesible. Ver cartel <https://www.incibe.es/ciudadania/formacion/recursosdescargables/comics-para-identificar-fraudes-online> .

3.4 Actividades obligatorias

Manual de Supervivencia de Ciberseguridad

Imagen generada con IA (DALL·E) (CC BY-NC-SA <http://creativecommons.org/licenses/?lang=es>)

Actividad 3.1: Manual de supervivencia de ciberseguridad III

Descripción: Esta actividad está diseñada para que continúes desarrollando tu manual personal de ciberseguridad, enfocándote ahora en el capítulo 3, que incorpora las medidas adicionales de seguridad y privacidad que hemos explorado en este módulo.

Pasos:

- **Selección de medidas de seguridad:**
  - Revisa los contenidos del Módulo 3 y elige las medidas de seguridad y privacidad, estrategias y herramientas que consideres más relevantes para tu entorno digital.
  - Justifica por qué has seleccionado cada medida y cómo se aplican a tus necesidades específicas.
  - Añade a tu manual una sección que contenga una lista de las medidas seleccionadas con una breve descripción de cada una y los recursos necesarios para su implementación. Esta sección servirá como referencia rápida de las estrategias de seguridad que has considerado importantes.
- **Implementación de una medida de seguridad:**
  - De las medidas seleccionadas, implementa al menos una en tu entorno digital actual.
  - Describe el proceso de implementación y cómo has aplicado la medida, incluyendo cualquier dificultad que hayas encontrado y cómo la superaste.
- **Estado de madurez de mi seguridad digital:**
  - Añade a tu manual una nueva sección que liste las medidas de seguridad y privacidad que ya has aplicado y las que están pendientes de implementación.
  - Reflexiona sobre tu estado actual de seguridad digital y justifica tus decisiones y planes futuros para mejorar tu seguridad.

Recursos necesarios:

- Procesador de texto (Word, Google Docs, etc.).
- Acceso a los contenidos del Módulo 3.
- Herramientas y recursos de ciberseguridad mencionados en el módulo.
- Plantilla proporcionada en el aula virtual del curso.

Formato y entrega de la actividad: La actividad debe ser entregada en formato PDF a través del enlace habilitado en el aula virtual del curso.

Nota: Cada capítulo del manual se puede trabajar de manera independiente. No es necesario haber completado los capítulos 1 y 2 para realizar esta actividad.

Rúbrica de la actividad 3.1 Aplicar

	Nivel Alto	Nivel Medio	Nivel Básico
Selección de medidas de	Se han identificado y seleccionado las	Se han identificado y seleccionado	No se ha incluido la sección. (0)

	Nivel Alto	Nivel Medio	Nivel Básico
seguridad (2,5 pts)	estrategias y herramientas de manera completa y detallada, justificando claramente su relevancia y aplicación. (2.5)	estrategias y herramientas de manera adecuada, aunque las justificaciones son poco detalladas. (1.25)	
Implementación de una medida de seguridad	Se describe detalladamente la implementación de una medida, incluyendo las dificultades encontradas y cómo se superaron, reflejando un entendimiento profundo del proceso. (2.5)	La descripción de la implementación es adecuada, pero carece de detalles sobre las dificultades encontradas o posibles soluciones. (1.25)	No se ha incluido la sección o no se ha descrito la implementación de una medida. (0)
Estado de madurez de mi seguridad digital (2,5 pts)	Se ha incluido una sección detallada que refleja un análisis completo y una comprensión de la seguridad personal, mostrando claramente las medidas aplicadas y pendientes. (2.5)	La sección incluida muestra una comprensión adecuada de la seguridad personal, pero el análisis es superficial y necesita mayor profundidad. (1.25)	No se ha incluido la sección. (0)
Elaboración del manual (2,5 pts)	El manual incluye descripciones claras y recursos necesarios bien definidos. (2.5)	El manual incluye descripciones y recursos, pero no están completamente claros o son incompletos. (1.25)	No se ha elaborado el documento. (0)

Actividad obligatoria 3.2: Reflexión colaborativa sobre medidas de seguridad

Descripción: El propósito de esta tarea es fomentar la **reflexión colaborativa** sobre las medidas de seguridad propuestas en el módulo. Para ello, debes compartir tus experiencias en la **implementación** de alguna de las **medidas de seguridad** presentadas en el módulo 3 y reflexionar sobre su efectividad en tu entorno digital. Además, se espera que comentes las contribuciones de

tus compañeras y compañeros, ofreciendo tu perspectiva y posibles alternativas de uso. Asegúrate de responder al menos a una entrada del foro para promover la interacción y el intercambio de ideas en el foro.

Considera enriquecer tus comentarios con preguntas estimulantes para promover una discusión más profunda y significativa.

Recursos necesarios:

- Acceso al foro del curso para la participación.

Formato y entrega de la actividad:

- Foro del módulo.

Rúbrica de la actividad 3.2 Aplicar

	Nivel Alto	Nivel Medio	Nivel Bajo
Participación activa en el foro (2,5 pts)	Se han compartido experiencias de manera detallada y constructiva, promoviendo la discusión. (2.5)	Se han compartido experiencias, pero de manera general o sin profundizar. (1.25)	No se han compartido experiencias en el foro. (0)
Reflexión sobre medidas implementadas (2,5 pts)	Se ha demostrado una reflexión profunda sobre las medidas implementadas, destacando su importancia. (2.5)	Se ha mostrado una reflexión básica sobre las medidas implementadas, sin detalles específicos. (1.25)	No se han compartido reflexiones sobre las medidas implementadas. (0)
Colaboración y apoyo a compañeras y compañeros (2,5 pts)	Se ha ofrecido apoyo constructivo y colaborativo a las reflexiones de las compañeras y compañeros. (2.5)	Se ha ofrecido apoyo a las compañeras y compañeros, pero de manera limitada o superficial. (1.25)	No se ha ofrecido apoyo ni colaboración a las compañeras y compañeros. (0)

	Nivel Alto	Nivel Medio	Nivel Bajo
Propuestas de alternativas a medidas de seguridad de compañeras y compañeros (2,5 pts)	Se han presentado alternativas aplicables y bien fundamentadas a las medidas de seguridad, demostrando una comprensión profunda. (2.5)	Se han planteado alternativas a las medidas de seguridad; no obstante, estas requieren de un desarrollo más amplio o ejemplos que demuestren su aplicabilidad. (1.25)	No se han propuesto alternativas aplicables, sin aportar significativamente a la discusión sobre seguridad. (0)

Módulo 3. Protección de amenazas en línea

Otros formatos y autoría

Autoría

Título	Módulo 3 del curso "La Ciberseguridad en el ámbito educativo"
Descripción	El módulo "**Protección de amenazas en línea**" equipa a los participantes con estrategias y recursos para detectar y contrarrestar estafas cibernéticas comunes, así como a fortificar sus comunicaciones electrónicas. Este módulo promueve una mentalidad de detective digital, empoderando a los usuarios para enfrentar los desafíos de la era digital con confianza y resiliencia
Autor	Manuel Jesús Rivas Sández <https://twitter.com/0xmrivas>
Licencia	Creative Commons BY-NC-SA 4.0 <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

Versión imprimible PDF

Este material está diseñado para ser leído y trabajado de manera interactiva en un ordenador, pero si quieres puedes descargártelo en este enlace <https://raw.githubusercontent.com/0xmrivas/ciberseguridad-ambito-educativo-online/main/assets/PDF/modulo3.pdf> en formato pdf.