Universidad Camilo José Cela



Unidad Didáctica

Bienestar digital: Protección, seguridad y privacidad en la red. De la reputación online a las prácticas de riesgo.

COLABORA: Campuseducacion formación on-line

Facultad de Educación de la Universidad Camilo José Cela
© Reservados Todos los Derechos

ASPECTOS DIDÁCTICOS

OBJETIVOS ESPECÍFICOS

- Analizar la importancia de mantener un equilibrio entre el uso de tecnologías y el bienestar personal, promoviendo hábitos saludables en el entorno digital.
- Reconocer las amenazas y vulnerabilidades asociadas al uso de los dispositivos digitales y aprender a aplicar medidas de seguridad básicas para protegerlos.
- Conocer los fundamentos de la privacidad online, aprender a gestionar la identidad digital y desarrollar estrategias para proteger la reputación online en diferentes plataformas.
- Desarrollar habilidades críticas para identificar y evaluar la veracidad de la información difundida en la red, distinguiendo entre fuentes confiables y noticias falsas.
- Conocer los conceptos básicos sobre virus y programas malignos, así como las técnicas y herramientas de prevención que ayudan a proteger la información y los dispositivos.
- Examinar las características de los contenidos virales, desafíos y retos que pueden representar riesgos, comprendiendo sus posibles consecuencias en la salud y la seguridad digital.
- Saber identificar señales de acoso online, tanto en sus formas tradicionales como en el ciberacoso.
- Desarrollar una actitud crítica y ética en el manejo de la identidad digital, considerando el impacto de las acciones en línea sobre la imagen personal y la reputación a largo plazo.

MAPA CONCEPTUAL

Bienestar digital

La seguridad de los dispositivos móviles

Privacidad, identidad digital y reputación online

Bulos, *hoax* y *fake* news

Contenidos virales, retos y desafíos

Ciberseguridad: virus y programas malignos

Prácticas de riesgo

Acoso y ciberacoso



BIENESTAR DIGITAL: PROTECCIÓN, SEGURIDAD Y PRIVACIDAD EN LA RED. DE LA REPUTACIÓN ONLINE A LAS PRÁCTICAS DE RIESGO

GLOSARIO DE TÉRMINOS

- **Bienestar digital**: Equilibrio personal entre el uso de la tecnología y el bienestar físico y mental. Este bienestar digital implica aprovechar las herramientas digitales de manera consciente, evitando que su uso excesivo o inadecuado afecte a la salud, las relaciones o la calidad de vida. De igual forma, se trata de integrar la tecnología de forma saludable en la rutina diaria, asegurando que contribuya al desarrollo personal en lugar de generar estrés, distracciones o dependencia.
- **Ciberacoso**: Introduce el acoso al entorno de las Tecnologías de la Información y Comunicación. Generalmente, este término es utilizado para denominar cualquier tipo de acoso que se produce en un entorno digital, como puede ser redes sociales, correo electrónico, sistemas de mensajería instantánea, etc. El ciberacoso se sirve de intencionalidad y de un abuso de poder mal empleado y mal entendido, además de cobijado, en muchas ocasiones, en el anonimato.
- **Ciberbullying**: Se refiere al acoso virtual que se produce entre menores o adolescentes que comparten entorno educativo y escolar, por lo que existe entre víctimas y agresores una relación de convivencia.
- **Ciberseguridad**: Se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciberamenazas.
- **Fake news**: Noticias falsas o bulos que se propagan por Internet con el objetivo de desinformar, engañar y manipular a los usuarios. También puede ser usadas para desprestigiar o enaltecer a determinadas personas o instituciones con el fin de obtener un beneficio económico.
- **Grooming**: Se refiere al acercamiento de un adulto a un menor con fines sexuales mediante la construcción gradual de una relación de confianza, es otro riesgo importante asociado al sexting.
- **Hoax**: Un hoax es un tipo de desinformación o engaño que se difunde principalmente a través de Internet y redes sociales, además de mensajería instantánea. A diferencia de las fake news, que suelen estar diseñadas para parecer noticias verídicas, los hoax generalmente se presentan como alertas, advertencias o mensajes preocupantes, a menudo relacionados con riesgos, amenazas o actividades ilícitas que, en realidad, son falsas.
- **Identidad digital**: Conjunto de características que nos identifican dentro de la red y que se va configurando con el rastro que, consciente o inconscientemente, deja nuestro paso por internet.
- **Pornovenganza**: Constituye otra amenaza grave, ya que implica la difusión ilícita de contenido erótico o sexual con el objetivo de vengarse o causar daño, afectando mayoritariamente a mujeres y siendo considerada una forma de ciberviolencia de género.
- **Reputación online**: Es el prestigio que tiene una persona, marca u organización y se fragua a partir de la opinión o consideración que los internautas vierten a la red sobre las acciones on y off-line de dicha entidad.
- **Sexting**: Surge de la combinación de las palabras en inglés sex (sexo) y texting (enviar mensajes de texto), y se define como la producción, difusión, recepción e intercambio de contenidos de carácter sexual (ya sean textos, imágenes, vídeos o audios) a través de medios tecnológicos.
- **Sextorsión**: Se produce cuando una persona utiliza contenidos sexuales para chantajear a otra, exigiendo la producción de más material o incluso concesiones sexuales físicas. Este riesgo afecta tanto a menores como a adultos y puede evolucionar hacia situaciones de abuso.
- **Sharenting**: Término derivado de la combinación de las palabras en inglés share (compartir) y parenting (paternidad). Se utiliza para describir la práctica mediante la cual los padres comparten en redes sociales grandes cantidades de información, a menudo acompañada de imágenes o vídeos, sobre sus hijos. Esta conducta, impulsada por el deseo de documentar y compartir momentos familiares, ha generado un intenso debate sobre las implicaciones que puede tener en la privacidad de los menores y en la huella digital que dejan desde una edad temprana.

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN 3

2. BIENESTAR DIGITAL 4

3. LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES 8

3.1. SEGURIDAD ANTE PÉRDIDAS O ROBOS 8

Guardar la factura de compra 8

Proteger el teléfono con un código de acceso o patrón de desbloqueo, así como un PIN en la tarjeta SIM 9

Tener apuntado y guardado en un lugar seguro el número IMEI 9

Tener instalada una aplicación antirrobo para localizar y bloquear el dispositivo 9

Realizar copias de seguridad periódicas 9

Limpiar regularmente el contenido almacenado en el dispositivo 9

3.2. SEGURIDAD DEL SOFTWARE 9

Mantener el sistema operativo y las aplicaciones actualizadas 10

Tener un antivirus actualizado 10

Descargar aplicaciones solo desde fuentes confiables 10

Respetar las restricciones del fabricante 10

Verificar la autenticidad de las aplicaciones antes de descargarlas 10

3.3. SEGURIDAD PARA LA PRIVACIDAD 11

Leer detenidamente las cláusulas y condiciones de uso de las aplicaciones 11

Verificar los permisos solicitados por cada aplicación 11

Eliminar aplicaciones innecesarias 11

3.4. SEGURIDAD EN LAS CONEXIONES 12

Seguridad en redes inalámbricas 12

Seguridad en servicios de almacenamiento en la nube 13

Seguridad en el uso de ordenadores públicos 13

4. IDENTIDAD DIGITAL, REPUTACIÓN ONLINE Y PRIVACIDAD 15

4.1. IDENTIDAD DIGITAL 16

4.2. REPUTACIÓN ONLINE 18
4.3. PRIVACIDAD 20
5. BULOS, HOAX Y FAKE NEWS 23
6. CIBERSEGURIDAD: VIRUS Y PROGRAMAS MALIGNOS 26
Correo electrónico 29
Dispositivos de almacenamiento externo 29
Descarga de archivos y aplicaciones 30
Navegación web 30
Redes sociales 30
Vulnerabilidades del sistema 30
7. CONTENIDOS VIRALES, RETOS Y DESAFÍOS 32
Mannequin Challenge 33
Bird Box Challenge 33
Momo Challenge 33
Ballena Azul 34
Tide Pod Challenge 34
Ice Bucket Challenge 34
8. PRÁCTICAS DE RIESGO 36
9. ACOSO Y CIBERACOSO 39
10. CONCLUSIONES 44
11. REFERENCIAS BIBLIOGRÁFICAS 46

1. INTRODUCCIÓN

Es increíble todo lo que dos palabras pueden abarcar y eludir. “Bienestar digital” se erige hoy como un concepto amplísimo, cada vez más vasto, donde tienen cabida múltiples campos y consideraciones de toda índole: aspectos legales, morales, cívicos, éticos, de seguridad…

Sobre todo, el bienestar digital es sumamente importante en terreno educativo ya que los menores de edad pasan cada vez más tiempo en la red. Pero no solo se vincula a los aspectos en torno a la identidad digital de estos menores o los posibles problemas de acoso y ciberacoso que puedan surgir, sino que, también, el bienestar digital es un campo vinculado a los bulos y las fake news, a los virus y programas malignos, a los fraudes en la red e incluso a la seguridad de nuestros propios dispositivos móviles.

Podemos entender el bienestar digital como el **equilibrio óptimo y saludable entre el uso de la tecnología y la calidad de vida, de modo que el uso de dispositivos digitales no intervenga negativamente en la salud mental, emocional ni física de los usuarios**. Y es que el uso excesivo o inadecuado de la tecnología puede generar efectos negativos, como el estrés digital, la fatiga informativa, la disminución de la concentración e incluso el deterioro de las relaciones interpersonales.

En relación a los problemas de cariz más personal o incluso psicológicos, el bienestar digital incluye establecer límites en el tiempo de uso de las pantallas, sobre todo en niños y menores de edad, fomentar el establecimiento de pausas en el uso de los dispositivos, proteger la privacidad y la seguridad en línea y, muy en concreto, promover un uso responsable de las redes sociales, tan en boga en la actualidad.

Dado el carácter amplio y complejo del bienestar digital, en esta unidad abordaremos una visión general de sus múltiples dimensiones, conscientes de que muchos temas de gran relevancia quedarán fuera de nuestro análisis. No obstante, nuestro objetivo es proporcionar herramientas y reflexiones que permitan comprender la importancia de este concepto y fomentar un uso más consciente, seguro y saludable de la tecnología en la vida cotidiana.

2. BIENESTAR DIGITAL

Como ya hemos dicho en la introducción, el bienestar digital alude a múltiples conceptos y desde esa perspectiva polisémica es como vamos a analizarlo a lo largo de esta última unidad, pero, ¿qué quiere decir exactamente el bienestar digital? ¿Cuál es, o ha sido, la principal definición que se le ha dado, la cual ha hecho que podamos delimitar concretamente a este concepto?

Desde aquí entendemos el bienestar digital como el **equilibrio personal entre el uso de la tecnología y el bienestar físico y mental**. Este bienestar digital **implica aprovechar las herramientas digitales de manera consciente**, evitando que su uso excesivo o inadecuado afecte a la salud, las relaciones o la calidad de vida. De igual forma, **se trata de integrar la tecnología de forma saludable en la rutina** diaria, asegurando que contribuya al desarrollo personal **en lugar de generar estrés, distracciones o dependencia**.

Desgraciadamente, este bienestar digital, tal y como lo acabamos de describir, no abunda entre los usuarios de las nuevas tecnologías, especialmente entre los jóvenes. Aunque no debemos culpar exclusivamente a las nuevas generaciones o a los usuarios de menor edad, pues los adultos se ven en la misma situación: pegados a la pantalla de su teléfono móvil constantemente, ansiosos por recibir comentarios en sus redes sociales y consultando de manera compulsiva su dispositivo. Sin embargo, es evidente que el foco máximo de atención apunte hacia los más jóvenes, pues familias, docentes y sociedad en general deberían velar por que su población más joven creciera sin el impacto negativo de las nuevas tecnologías.



Según un informe de Digital Information World (2023), las personas tienen un promedio de 6 horas y 58 minutos de tiempo de pantalla por día, habiendo aumentado la exposición diaria a las pantallas en 50 minutos por día, con respecto al anterior análisis de 2013.

Además, este informe reveló que, a nivel mundial, el usuario promedio pasa 2 horas y 51 minutos mirando la pantalla de sus ordenadores, y unas 3 horas y 46 minutos mirando sus teléfonos móviles. En el caso de los niños de 0 a 2 años, casi la mitad (un 49%) pasan varias horas diarias interactuando con smartphones.

Pero, ¿qué opinan los expertos? La Asociación Española de Pediatría (AEP) recomienda **cero pantallas hasta los 6 años y solo una hora al día entre los 6 y los 12 años**. De hecho, la AEP ha actualizado sus recomendaciones sobre el uso de pantallas en la infancia y la adolescencia en base a la nueva evidencia científica e incorpora las siguientes novedades (2025):

- *Aumenta el rango de edad por debajo del que se considera que no debe exponerse a los niños a pantallas, que pasa de los 2 a los 6 años.*
- *Se demuestra una fuerte asociación entre el tiempo que los padres pasan frente a las pantallas y el de sus hijos, sobre todo durante las comidas y en el dormitorio.*
- *Se corrobora que el uso excesivo de pantallas perjudica áreas como el sueño, el riesgo cardiovascular, el volumen cerebral o la alimentación, entre otros.*
- *La Asociación Española de Pediatría urge medidas tanto a los gobiernos como al sistema educativo, para evitar los potenciales efectos nocivos en la salud y el desarrollo de niños y adolescentes.*

Según Salmerón (2025), coordinadora del grupo de trabajo de Salud Digital de la Asociación Española de Pediatría, en la actualidad ya nadie puede dudar de que los medios digitales afectan a la salud a todos los niveles, y a cualquier edad. En 2016, la Academia Americana de Pediatría alertó por primera vez del impacto del mundo digital sobre la salud, y en estos últimos años han ido aumentando progresivamente los ensayos clínicos que corroboran este vínculo.

Consulta aquí el Plan Digital Familiar de AEP.

Siguiendo a la propia AEP (2025), el impacto del uso excesivo de pantallas en la infancia y adolescencia es multifactorial afectando a diversas áreas relacionadas con la salud y el bienestar, que reducen la calidad de vida e impactan profundamente sobre la salud:

- **Problemas de descanso y sueño**

Un mayor tiempo de uso de las redes sociales y videojuegos se asocia con permanecer un menor número de horas en la cama, acostarse más tarde y mayor latencia del inicio del sueño. Además, el uso de pantallas antes de acostarse produce un aumento de la somnolencia diurna, una disminución de la somnolencia nocturna, una reducción de la secreción de melatonina, un retraso del reloj circadiano, y una disminución y retraso del sueño REM. Todo ello favorece el estado de ánimo depresivo, las alteraciones de la conducta, la disminución de la autoestima, y la alteración del desarrollo cerebral.

- **Trastornos en la alimentación y nutrición**

Algunos estudios asocian el tiempo frente a pantallas (móviles, tabletas, ordenadores, televisores) con una dieta menos saludable, favoreciendo el consumo de alimentos hipercalóricos y, por consiguiente, aumentando el riesgo de sobrepeso y obesidad.

- **Deterioro de la actividad física**

Se ha demostrado que los adolescentes que ya tienden al sedentarismo pasan más tiempo usando pantallas. Por el contrario, la limitación de su uso favorece la práctica de actividad física. Se recomienda la realización de actividad física moderada o vigorosa durante un mínimo de 60 minutos diarios en niños y adolescentes.

- **Riesgo cardiovascular**

La falta de ejercicio físico por dedicar demasiado tiempo a las pantallas aumenta el riesgo de desarrollar síndrome metabólico. Por el contrario, se ha vinculado la reducción del tiempo de pantallas con una reducción de la presión arterial y un aumento del colesterol “bueno” (HDL).

- **Fatiga visual**

El ojo seco, la picazón ocular, el lagrimeo, la sensación de tener un cuerpo extraño en el ojo o la visión borrosa son algunos de los síntomas causados por el exceso de pantallas, así como el dolor cérvico-lumbar, la fatiga general y la cefalea. Además, en la infancia y adolescencia favorece especialmente la miopía progresiva y el estrabismo agudo.

- **Disminución del volumen cerebral**

La evidencia científica apunta a una disminución del espesor de la corteza cerebral en varias regiones, debido al uso excesivo de pantallas.

En la adolescencia finaliza tanto la maduración del sistema límbico como la maduración de la corteza cerebral. Los medios digitales interfieren a esta edad de dos formas distintas: aumentando la activación de la región límbica, al estar expuestos a sistemas de gratificación inmediata, y disminuyendo la actividad frontal por efecto desplazamiento de los estímulos adecuados para la edad. Además, la multitarea relacionada con las pantallas se asocia con peores resultados cognitivos, una disminución de la capacidad de filtrar las distracciones y un aumento de la impulsividad y disminución de la memoria de trabajo. De este modo, los adolescentes que pasan demasiado tiempo frente a una pantalla tienen más probabilidades de presentar dificultades cognitivas graves.



Teniendo en cuenta los resultados de la investigación de los últimos años, las evidencias científicas y los estudios de caso analizados directamente por profesionales, la Asociación Española de Pediatría, en su última recomendación, propone la siguiente temporalización en la incorporación progresiva de las pantallas

- **De 0 a 6 años:**
  - Cero pantallas, no existe un tiempo seguro.
  - Como excepción y bajo supervisión del adulto se puede usar para el contacto social con un objetivo concreto. Por ejemplo, que la persona que está al otro lado de la pantalla le cuente un cuento o le cante una canción.
- **De 7 a 12 años:**
  - Menos de una hora (incluyendo el tiempo escolar y los deberes).
  - Limitar el uso de los dispositivos con acceso a Internet.
  - Priorizar los factores protectores: actividades deportivas, relaciones con iguales cara a cara, contacto con la naturaleza, sueño, alimentación saludable, etc.
  - Si se decide que utilicen un dispositivo es recomendable: que sea bajo la supervisión de un adulto, con dispositivos fijos y evitar el baño y dormitorio.
  - Pactar límites claros previamente tanto en tiempo como en contenidos adaptados a la edad.
- **De 13 a 16 años:**
  - Menos de dos horas (incluyendo el tiempo escolar y los deberes).
  - Si se permite el acceso a dispositivos -sin ser la única medida que se tome instalar herramientas de control parental.
  - Priorizar el uso de teléfonos sin acceso a internet.
  - Retrasar la edad del primer móvil inteligente (con conexión a internet).

Aunque el concepto de bienestar digital se centra principalmente en lograr un equilibrio saludable en el uso de dispositivos y tecnologías, como estamos viendo, su alcance va mucho más allá, ya que está intrínsecamente vinculado a una variedad de problemáticas derivadas del entorno digital. Así pues, lo podemos relacionar sin dificultad con el ciberbullying, la suplantación de identidad, los riesgos de privacidad o incluso la exposición a contenidos dañinos. Todo ello afecta tanto a la experiencia de los usuarios (en nuestro ámbito académico, a los menores) como a la salud mental, emocional y social. Por eso comenzamos diciendo que el bienestar digital no puede abordarse de manera aislada, sino como un campo multidimensional que exige una visión integral, donde la educación, la concienciación y la regulación juegan un papel clave para garantizar una interacción segura y saludable con la tecnología.

Consulta aquí la guía de mediación parental sobre el uso seguro de Internet (INCIBE).

Por otra parte, no podemos desdeñar que el bienestar digital se relacione, también, con la construcción de un entorno digital más seguro y equitativo para todos. La presencia de amenazas como la desinformación, el fraude en línea y la manipulación algorítmica afecta la capacidad de los usuarios para tomar decisiones informadas y ejercer su autonomía

digital. En este sentido, promover el bienestar digital implicará, además, el fomento de hábitos saludables en el uso de la tecnología, dotar a las personas de herramientas críticas para identificar riesgos, proteger su privacidad y navegar de manera consciente en lo que se está llamando “ecosistema digital”.

Asimismo, el impacto de la tecnología en el ámbito laboral y educativo refuerza la necesidad de abordar el bienestar digital desde una perspectiva amplia. La hiperconectividad y la exigencia de disponibilidad constante pueden generar estrés, ansiedad y dificultades para desconectar del trabajo o los estudios, lo que afecta la calidad de vida. Por ello, el bienestar digital no debe entenderse únicamente como una cuestión de uso moderado de pantallas, sino como una estrategia integral que abarque desde la regulación del tiempo en línea hasta la promoción de espacios de descanso y desconexión.

Bienestar Digital – Yo tampoco lo sabía (ING)

https://www.youtube.com/watch?v=1SOVn6XjSuo

3. LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES

Comenzaremos el camino del bienestar digital por una de las cosas más sencillas y obvias: la seguridad de los dispositivos móviles.

En un mundo donde los smartphones parece que se han convertido en una extensión de la propia vida personal y profesional, protegerlos adecuadamente se convierte en un paso fundamental para garantizar nuestro bienestar digital. No obstante, a pesar de la importancia de este tema, la gran mayoría de personas pasan por alto las recomendaciones más básicas de seguridad y cometen ciertas torpezas o temeridades que están poniendo en peligro tanto sus datos personales como sus propios dispositivos.

Vamos a analizar la seguridad de los dispositivos en torno a tres dimensiones esenciales: las precauciones ante posibles pérdidas o robos, la seguridad del propio software, las precauciones en torno a la privacidad y los peligros de las conexiones o redes públicas, todo ello en base a INTEF (2023); INCIBE (2025); y PantallasAmigas (2021).

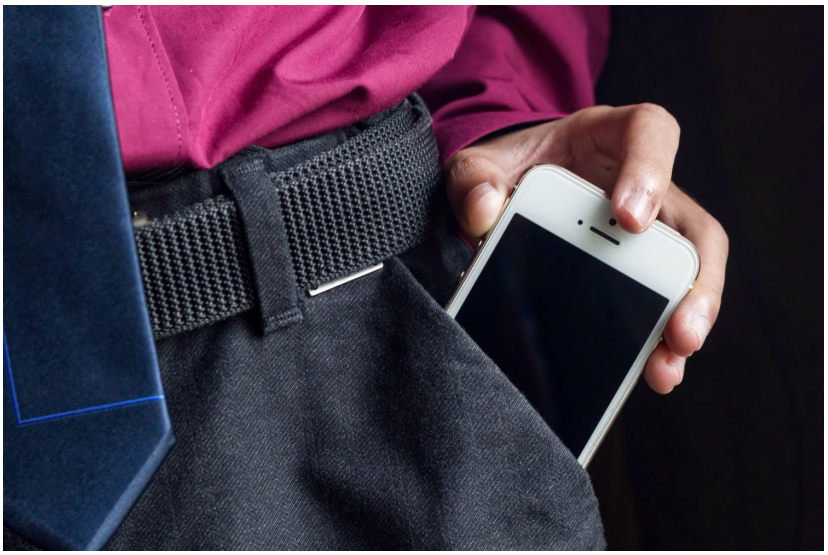
Proteger y usar de manera segura los dispositivos móviles - INCIBE

https://www.youtube.com/watch?v=HuwOrqqXz6U

3.1. SEGURIDAD ANTE PÉRDIDAS O ROBOS

El teléfono móvil es un aparato que fácilmente puede extraviarse e, igualmente, es un tipo de dispositivo que se presta a ser sustraído, especialmente si es de alta gama.

Puesto que no se pueden evitar todos los posibles accidentes, sí se pueden poner ciertas medidas que actúen a modo de barrera de seguridad de nuestros datos personales y de todo el contenido que tengamos asociado en el dispositivo si lo perdemos o nos lo roban. Conocer estas medidas nos ayudan a proteger nuestra información personal y nos facilitan la solución de problemas al brindarnos la tranquilidad que supone saber que, incluso ante una situación adversa, tenemos herramientas para minimizar los riesgos asociados con pérdidas o robos.



Implementar prácticas de seguridad adecuadas es fundamental para mantener el control sobre nuestra privacidad y garantizar que, en caso de incidente, podamos actuar de manera rápida y efectiva.

Guardar la factura de compra

La factura de compra no solo sirve como prueba de adquisición, sino que también puede ser clave en situaciones de

pérdida o robo. En caso de que sea necesario denunciar el robo a las autoridades, la factura puede ser requerida como parte del proceso. Además, la factura será un documento necesario para validar la propiedad del dispositivo si se pidiese su desactivación o recuperación a través de la operadora de telefonía.

Proteger el teléfono con un código de acceso o patrón de desbloqueo, así como un PIN en la tarjeta SIM

Establecer una contraseña de acceso al teléfono es un mecanismo muy sencillo y, a la vez, muy eficaz para proteger el dispositivo. Dependiendo del modelo y la marca del teléfono se puede escoger entre una combinación numérica, un patrón de desbloqueo o un reconocimiento biométrico, bien sea con la huella dactilar o a través del reconocimiento facial. Tener esta primera barreara impedirá el acceso no autorizado a los datos personales que contenga el aparato. Además, es recomendable que la tarjeta SIM esté debidamente protegida con un código PIN lo que agrega una capa extra de seguridad, evitando que alguien pueda extraer la tarjeta del teléfono y usarla en otro dispositivo para acceder a contactos y otro tipo de datos vinculados.

Tener apuntado y guardado en un lugar seguro el número IMEI

El IMEI (International Mobile Equipment Identity) es un número de identificación único para cada dispositivo móvil, que puede ser esencial para rastrear el dispositivo en caso de pérdida o robo. Este número se puede encontrar generalmente en la parte posterior de la batería, en la caja original o en la factura de compra. También, es posible obtenerlo marcando *#06# en la pantalla del dispositivo. Es fundamental anotar este número y almacenarlo en un lugar seguro, distinto al teléfono, ya que en caso de que tu sea robado se podrá proporcionar a las autoridades o a la operadora para bloquearlo y evitar que sea utilizado.

Tener instalada una aplicación antirrobo para localizar y bloquear el dispositivo

En caso de pérdida o robo existen muchas aplicaciones antirrobo que llevan bastante tiempo funcionando como herramientas indispensables y de gran ayuda para la protección de nuestra información. Estas aplicaciones permiten localizar el teléfono de forma remota, bloquearlo y, si es necesario, borrar sus datos. Dependiendo del sistema operativo existen distintas apps: para Apple contamos con Buscar mi iPhone, mientras que los usuarios de Android pueden contar con Encontrar mi dispositivo. Ambas aplicaciones ofrecen una excelente protección, pero, además de ellas, existen otras más que cuentan con opciones adicionales como la eliminación remota de archivos o la posibilidad de hacer sonar el teléfono, incluso cuando está en modo silencioso. Desde el Instituto Nacional de Ciberseguridad (INCIBE) se pueden acceder a múltiples herramientas para proteger nuestros dispositivos.

Realizar copias de seguridad periódicas

Una de las mayores preocupaciones tras la pérdida de un dispositivo es la posible pérdida de datos importantes, como contactos, fotos, videos, aplicaciones y otros archivos. Para evitar este riesgo, es recomendable realizar copias de seguridad de forma regular, ya sea en la nube o en un dispositivo externo.

Limpiar regularmente el contenido almacenado en el dispositivo

Además de las medidas de seguridad más técnicas, también es importante practicar buenos hábitos de almacenamiento. Evita guardar información sensible e innecesaria en tu dispositivo, como contraseñas o documentos confidenciales, que podrían comprometer tu seguridad en caso de pérdida o robo. Realizar limpiezas periódicas de los contenidos almacenados optimizará el rendimiento del dispositivo y reducirá el riesgo de exposición de información personal en situaciones adversas.

3.2. SEGURIDAD DEL SOFTWARE

Los teléfonos móviles se han convertido en la principal vía de acceso a Internet para la mayoría de los usuarios, en detrimento del convencional ordenador de sobremesa, que ocupó el puesto principal hasta que surgieron los dispositivos inalámbricos y las conexiones sin necesidad de cable.

Sin embargo, los dispositivos móviles son los más vulnerables a los riesgos digitales. Esto se debe, en gran parte, a que, como usuarios, no hemos interiorizado completamente la necesidad de protegerlos con el mismo nivel de cuidado que aplicamos a nuestros ordenadores de sobremesa y no suele ser habitual que la gente lleve descargado un programa de

seguridad o antivirus en su teléfono móvil.

Cosulta aquí las Apps de seguridad para dispositivos móviles (INCIBE).

A continuación, se presentan una serie de medidas esenciales para proteger el móvil frente a softwares maliciosos y otros posibles ataques cibernéticos.

Mantener el sistema operativo y las aplicaciones actualizadas

Una de las primeras medidas de seguridad es mantener siempre el sistema operativo del dispositivo móvil y las aplicaciones frecuentes constantemente actualizadas. Los desarrolladores de software trabajan de forma constante en mejoras de seguridad, corrección de vulnerabilidades y resolución de errores, de modo que las actualizaciones suelen incluir parches de seguridad que protegen el dispositivo contra amenazas nuevas. Si no se actualiza regularmente, el dispositivo se expone a riesgos que ya han sido resueltos en versiones posteriores. Lo mismo pasa con el propio sistema operativo del aparato que, aproximadamente cada mes, notifica al usuario de una nueva actualización con mejoras para la seguridad y la experiencia de uso.

Tener un antivirus actualizado

Los teléfonos inteligentes son uno de los principales objetivos del malware, ya que almacenan una gran cantidad de datos personales, credenciales bancarias y archivos sensibles, de modo que es imprescindible contar con un antivirus actualizado para detectar y bloquear amenazas como virus, troyanos, spyware y ransomware, que pueden infiltrarse a través de aplicaciones maliciosas, enlaces fraudulentos o archivos adjuntos en correos electrónicos sospechosos. Además, muchas soluciones antivirus incluyen funciones avanzadas como protección en tiempo real, análisis de redes Wi-Fi sospechosas, bloqueo de aplicaciones no seguras y rastreo de actividad sospechosa en el sistema.

Es importante elegir un antivirus de confianza, preferiblemente de desarrolladores con buena reputación en ciberseguridad, y mantenerlo siempre actualizado para que pueda responder eficazmente a las nuevas amenazas que surgen constantemente. También se recomienda configurar análisis automáticos y evitar descargar software de fuentes no verificadas, ya que el mejor antivirus es, en última instancia, el uso responsable del dispositivo.

Descargar aplicaciones solo desde fuentes confiables

El riesgo de descargar aplicaciones maliciosas aumenta considerablemente cuando se recurren a fuentes no oficiales. Para obtener aplicaciones, es esencial hacerlo desde las tiendas oficiales, como Google Play Store o App Store. Además, en Android, se puede desactivar la opción "Permitir orígenes desconocidos" en la configuración de seguridad, para evitar la instalación de aplicaciones de tiendas no verificadas, siendo una medida muy sencilla pero que a la vez reduce considerablemente el riesgo de introducir softwares perjudiciales en el dispositivo.

Respetar las restricciones del fabricante

Aunque pueda parecer tentador desbloquear un dispositivo para acceder a funciones adicionales o instalar aplicaciones no disponibles en las tiendas oficiales, realizar un jailbreak (en iOS) o rootear (en Android) el teléfono compromete gravemente su seguridad. Estos procedimientos, al permitir un acceso total al sistema operativo, abren vulnerabilidades en la protección del dispositivo, lo que facilita la instalación de software malicioso y puede anular las garantías del fabricante. Así pues, es fundamental evitar estas prácticas, ya que alteran la arquitectura de seguridad del teléfono.

Verificar la autenticidad de las aplicaciones antes de descargarlas

Antes de proceder a la descarga de una aplicación, es importante asegurarse de que realmente proviene de una fuente confiable y de que su reputación es sólida. Para saberlo, se pueden consultar las valoraciones y opiniones de otros usuarios, y atender a si es una aplicación con tiene pocos comentarios o puntuaciones bajas. Los expertos suelen comentar que se debe desconfiar de aquellas aplicaciones que tienen muchos comentarios positivos, más de lo que sería normal, a la par que reseñas que no aportan información significativa ni detalles específicos, ya que esto puede ser un indicio de que se trata de una aplicación falsa o maliciosa, alimentada a base de comentarios generados por bots. Otra cosa fundamental es comprobar que las aplicaciones que se descargan no exijan acceso a información innecesaria.

3.3. SEGURIDAD PARA LA PRIVACIDAD

La privacidad en Internet se refiere a la capacidad de un usuario para controlar el acceso y uso de sus datos personales mientras navega, interactúa y comparte información en la red.



Proteger la privacidad resulta fundamental, ya que no solo están en juego datos básicos como el nombre, la dirección o el correo electrónico, sino también información más sensible, como intereses, hábitos de consumo, creencias o incluso la ubicación en tiempo real. Por ello, es necesario gestionar adecuadamente la privacidad, implementando medidas que permitan resguardar la información y mantener un equilibrio entre seguridad y privacidad en el entorno digital.

Evidentemente, los dispositivos móviles contienen una gran cantidad de información personal valiosa, como datos de ubicación, comunicaciones, intereses y hábitos, todo un compendio de información que, aunque puede ser conveniente, también es susceptible de ser explotada si no se toman precauciones adecuadas. A continuación, se presentan algunas medidas clave para proteger nuestra privacidad en el entorno digital.

Leer detenidamente las cláusulas y condiciones de uso de las aplicaciones

Antes de instalar una aplicación se deberían revisar sus términos y condiciones de uso, pero, nadie suele hacerlo. Aunque parezca algo tedioso, en estos documentos aparece información esencial para que los usuarios sepan qué tipo de datos va a recopilar la aplicación, cómo los utilizará y si los va a compartir con terceros. Muchas aplicaciones solicitan permisos que exceden su función principal, lo que puede suponer un riesgo para la privacidad, y es habitual ver que, antes de la instalación, el propio programa pide acceso a carpetas como Fotos, acceso a la cámara o al micrófono e incluso a los contactos y correos electrónicos. Comprender el alcance de estos permisos permite tomar decisiones informadas sobre qué aplicaciones instalar, permitiendo cuestionarnos si realmente necesitamos dichas aplicaciones o si nos merece la pena conceder acceso a determinada información de nuestro teléfono.

Verificar los permisos solicitados por cada aplicación

Las aplicaciones móviles suelen requerir acceso a diferentes funcionalidades del dispositivo, pero no siempre de forma justificada. Antes de proceder a la instalación, es recomendable analizar qué permisos solicita la aplicación y cuestionarse si realmente son necesarios. Por ejemplo, una aplicación de edición de imágenes no debería requerir acceso a los contactos o al micrófono. Para mejorar la seguridad, los sistemas operativos actuales permiten gestionar estos permisos desde la configuración del dispositivo, ofreciendo la opción de restringirlos o revocarlos en cualquier momento.

Eliminar aplicaciones innecesarias

Las aplicaciones que no se utilizan no solo ocupan espacio de almacenamiento, sino que pueden continuar ejecutándose en segundo plano, recopilando datos y representando un riesgo potencial de seguridad. Si nos encargamos de desinstalar periódicamente aquellas aplicaciones que ya no nos son necesarias optimizaremos el rendimiento del dispositivo y

reduciremos la exposición a posibles filtraciones de información personal. Como medida adicional, se recomienda revisar periódicamente las aplicaciones instaladas y evaluar si siguen siendo útiles o si es preferible eliminarlas.

3.4. SEGURIDAD EN LAS CONEXIONES

Para finalizar, nos detendremos en la seguridad de las conexiones pues el acceso a redes Wi-Fi es cada vez más amplio y muchos usuarios desconocen que conectarse a redes públicas puede suponer un riesgo para su privacidad y su propio dispositivo.

Aunque la conectividad es una parte esencial de la vida digital, ya que permite acceder a información, comunicarse y gestionar numerosos servicios en línea, las conexiones inalámbricas no siempre son seguras, y los ciberdelincuentes pueden aprovechar vulnerabilidades para interceptar datos, robar credenciales o infectar dispositivos con software malicioso. Por ello, es fundamental adoptar medidas de protección al utilizar redes públicas, servicios de almacenamiento en la nube y ordenadores compartidos.

Cómo proteger tu red Wi-Fi (INCIBE)

https://www.youtube.com/watch?v=nV9zOtHDmcA

Seguridad en redes inalámbricas

Las conexiones inalámbricas facilitan la movilidad y el acceso a internet, pero también pueden ser vulnerables a ataques cibernéticos si no se gestionan correctamente. Para reducir los riesgos, se recomienda:

- **Evitar redes Wi-Fi públicas abiertas**

Estas redes pueden ser utilizadas por ciberdelincuentes para interceptar datos sensibles. Si es imprescindible usarlas, se deben evitar transacciones bancarias y el acceso a información personal.

- **Desactivar la conexión automática a redes Wi-Fi**

Mantener esta opción activada puede hacer que el dispositivo se conecte sin el consentimiento del usuario a redes potencialmente peligrosas.

- **Borrar redes Wi-Fi guardadas que ya no se utilicen**

Esto impide que el dispositivo se conecte automáticamente a redes que podrían haber sido comprometidas con el tiempo.

- **Verificar la autenticidad de la red antes de conectarse**

En lugares públicos, es recomendable confirmar el nombre exacto de la red con el establecimiento antes de conectarse.

- **Usar una VPN (Red Privada Virtual)**

Este servicio cifra la conexión y protege la información transmitida incluso en redes inseguras.

- **Activar la autenticación en dos pasos en servicios sensibles**

Esto añade una capa extra de seguridad en caso de que la información de inicio de sesión sea interceptada.



Seguridad en servicios de almacenamiento en la nube

El almacenamiento en la nube facilita la gestión y acceso a archivos desde múltiples dispositivos. Sin embargo, implica riesgos que deben mitigarse con medidas de seguridad adecuadas:

- **Elegir una contraseña robusta y cambiarla periódicamente**

Esto dificulta el acceso no autorizado a la cuenta.

- **Activar la verificación en dos pasos**

Esta función ofrece una capa adicional de protección contra accesos no autorizados.

- **Cifrar archivos sensibles antes de almacenarlos en la nube**

En caso de una brecha de seguridad, los datos estarán protegidos.

- **Revisar los permisos de acceso de aplicaciones y dispositivos conectados**

Es importante eliminar aquellos que ya no sean necesarios.

- **Leer y comprender las condiciones del servicio**

Esto permite conocer cómo se gestionan los datos almacenados.

- **Evitar compartir enlaces de acceso abiertos**

Siempre que sea posible, utilizar opciones que requieran autenticación para acceder a los archivos.

- **Realizar copias de seguridad en dispositivos locales**

Esto evita la pérdida de información en caso de que la cuenta sea comprometida o el servicio tenga fallos.

Seguridad en el uso de ordenadores públicos

Los ordenadores de acceso público, como los de bibliotecas, cibercafés, hoteles o aeropuertos, pueden representar un riesgo para la seguridad de la información personal debido a la posibilidad de estar infectados con malware o keyloggers.

Para minimizar los riesgos al usarlos, se recomienda:

- **Evitar el uso de credenciales personales en estos equipos**

No iniciar sesión en cuentas bancarias, redes sociales o correos electrónicos importantes.

- **Cerrar siempre las sesiones después de utilizarlas**

Para evitar accesos no autorizados posteriores.

- **Utilizar la navegación privada o modo incógnito**

Esto evita que el navegador almacene información sobre las actividades realizadas.

- **No conectar dispositivos de almacenamiento externo**

Podrían infectarse con malware y comprometer la seguridad de los datos.

- **Si es necesario consultar correos electrónicos...**

...utilizar una cuenta alternativa, la cual debe tener una contraseña diferente a la de uso habitual.

- **Si es imprescindible iniciar sesión en un servicio importante...**

...activar la verificación en dos pasos desde otro dispositivo confiable.

- **Usar un teclado virtual para ingresar contraseñas sensibles**

Esto puede ayudar a evitar que sean capturadas por keyloggers.



4. IDENTIDAD DIGITAL, REPUTACIÓN ONLINE Y PRIVACIDAD

En el mundo en que vivimos parece que la gente tiene ya más presencia en Internet que en el plano físico. El avance de la tecnología y la proliferación de las redes sociales han transformado la manera en que la gente se muestra ante los demás, difuminando la frontera entre la vida privada y la pública, además de tergiversando la realidad y transfigurando, en beneficio del ego, cualquier atisbo de normalidad.

Lo que antes era una vida normal y corriente ahora es un escaparate abierto al mundo entero, donde cada publicación, cada comentario, cada "me gusta", cada vídeo… contribuye a construir una suerte de identidad digital de cada usuario que, en la mayor de las ocasiones, dista mucho de la verdad pero que, sin embargo, se engalana con la apariencia y con lo que los demás puedan llegar a pensar. Sin lugar a dudas, esta exposición constante trae consigo importantes riesgos y desafíos que no solo afectan a los jóvenes, como se suele creer, sino a toda la sociedad.



Cada vez es más común encontrar personas de todas las edades compartiendo su día a día en redes sociales, subiendo fotografías de sus comidas, publicando sus estados de ánimo, describiendo el lugar donde se encuentran de vacaciones o relatando cada aspecto de sus vidas como si se tratara de una serie documental. Este fenómeno, además de alimentar el deseo constante de "estar conectado", muy relacionado con la adicción digital, responde a una búsqueda incesante de validación que denota fuerte problemas de autoestima y confianza. La cantidad de "likes" y comentarios positivos se ha convertido en un parámetro para medir la aceptación social, generando una dependencia emocional que en muchos casos diluye la autenticidad de las personas.

El problema se agrava cuando el deseo de compartirlo todo nos hace olvidar el valor de la privacidad. Exponer demasiada información personal en internet puede traer consecuencias muy graves, desde la suplantación de identidad hasta el robo de datos o el ciberacoso, aspectos en los que nos detendremos más adelante. Además, muchas personas no son conscientes de que lo que publican en internet puede permanecer allí indefinidamente, afectando su reputación digital en el futuro. Un comentario impulsivo, una imagen comprometida o una publicación desafortunada pueden convertirse en obstáculos a la hora de buscar empleo, establecer relaciones profesionales o incluso mantener una imagen pública adecuada.

Las redes sociales han dado lugar a una paradoja interesante: mientras nos ofrecen herramientas para expresarnos libremente, también han fomentado una homogeneización del pensamiento y de la imagen personal. Se ha instaurado una suerte de "molde digital" al que muchas personas intentan ajustarse para encajar en los estándares que dictan las tendencias del momento. Esto se traduce en perfiles prácticamente idénticos, con fotografías similares, discursos calcados y una constante necesidad de demostrar que se lleva una vida ideal. La autenticidad ha quedado relegada a un segundo plano en favor de una versión editada de la realidad, cuidadosamente filtrada para satisfacer las expectativas de los demás.

Desde el plano académico no podemos sino reflexionar sobre el impacto que esta exposición digital tiene en nuestra

identidad real y, en concreto, sobre el normal desarrollo psicológico de nuestros jóvenes. *¿La gente se muestra en internet tal y como es, o simplemente proyecta lo que creen que los demás quieren ver?* O, más bien, *¿se muestran de la forma, artificial y postizamente, que quisieran ser pero que, en verdad, no son en absoluto?* Recuperar la autenticidad en un mundo digital saturado de artificio implica aprender a valorar el silencio, la discreción y la capacidad de reservar ciertos aspectos de nuestra vida solo para nosotros mismos y nuestro círculo más cercano.



Para abordar este problema, es esencial fomentar la educación digital en todas las edades. No se trata de demonizar las redes sociales ni de rechazar su uso, sino de aprender a gestionarlas de manera responsable y consciente, promoviendo la idea de que la privacidad es un derecho, no una opción, y que preservar cierta información en el ámbito privado no significa desconectarse del mundo, sino proteger nuestra identidad y bienestar.

4.1. IDENTIDAD DIGITAL

Podemos definir la identidad digital como el **conjunto de características que nos identifican dentro de la red y que se va configurando con el rastro que, consciente o inconscientemente, deja nuestro paso por internet** (INTEF, 2025). La forma en que se maneja toda esa información personal que generamos y publicamos se conoce como gestión de la privacidad. Se trata de un concepto personal y subjetivo, y es vital encontrar un equilibrio entre las ventajas que nos ofrece la exposición de información personal y los riesgos asociados en Internet (INCIBE, 2025).

Según INCIBE (2025) al publicar o facilitar información a través de los distintos servicios online sobre quiénes somos, vivimos, trabajamos, hobbies, gustos, intereses, fotos, vídeos, etc., ponemos en riesgo nuestra privacidad e incrementamos las opciones de ser víctimas de algún tipo de fraude o sufrir las consecuencias negativas de esa exposición, ya sea por daños reputacionales u otros.



Figura 1. ¿Cómo cuido mi reputación online? (extraído de /incibe.es)

Los principales riesgos son:

- **Robo y suplantación de identidad**

Los delincuentes pueden utilizar la información publicada en Internet para robar y suplantar la identidad de una persona y hacer compras fraudulentas, abrir cuentas bancarias, obtener un crédito u otras acciones maliciosas en su nombre.

- **Vigilancia**

Las empresas, los ciberdelincuentes y resto de usuarios pueden utilizar la información disponible en Internet para usarla en su beneficio.

- **Extorsión**

Usuarios con malas intenciones pueden usar la información personal de las personas disponible en la Red para hostigarlas, amenazarlas y difamarlas en las redes sociales u otros canales web.

- **Discriminación**

Cualquier persona con acceso a la información publicada puede aprovecharla para discriminar a las personas en función de su género, raza, orientación sexual, ideología, condición física, estatus económico, etc.

- **Sexting**

La distribución de fotos y vídeos producidos por uno mismo con connotación sexual puede suponer una práctica de riesgo ya que la persona que lo recibe podría comprometer la privacidad si lo redifunde sin consentimiento, o no toma las medidas de seguridad adecuadas para salvaguardarla.

- **Doxing**

Publicación de información sobre uno mismo en Internet sin nuestro consentimiento.

- **Fraudes y amenazas**

Los ciberdelincuentes pueden enviar mensajes manipulados y personalizados a sus víctimas, teniendo en consideración la información recopilada sobre ellas en Internet, resultando mucho más creíbles, de tal forma que las probabilidades de caer

en el engaño sean más altas.

¿Quiénes somos en la red? – Oficina de Seguridad del Internauta

https://www.youtube.com/watch?v=rNmXiYY9iHA

Omatos y Cuevas (s.f.) sostienen que la identidad digital se compone de distintos tipos de datosque se generan a partir de nuestra actividad en la red:

- **Datos formales**

Son aquellos que proporcionamos de manera consciente y deliberada. Un ejemplo claro es el currículum que subimos a LinkedIn, donde detallamos nuestra formación, experiencia laboral y competencias profesionales con un propósito específico.

- **Datos informales**

Se trata de la información que compartimos de manera involuntaria o inconsciente al interactuar en el entorno digital. Estos datos suelen estar implícitos en el contenido que publicamos intencionadamente. Tal como indican los autores citados, las fotografías son una fuente significativa de datos informales. Por ejemplo, una imagen tomada en una reunión de amigos en casa puede revelar detalles como los libros de nuestra biblioteca, el tamaño y estilo de nuestro salón, la marca de nuestros dispositivos electrónicos o incluso la ubicación de nuestra vivienda si a través de la ventana se distingue un punto de referencia reconocible. Además, los metadatos de la imagen pueden proporcionar información adicional, como el modelo del dispositivo con el que se tomó la foto, la fecha y hora exacta de la captura, la geolocalización e incluso los filtros utilizados.

- **Datos reales**

Son aquellos que reflejan hechos objetivos y verificables. Por ejemplo, si una persona publica una entrada en su blog personal cada dos semanas y colabora mensualmente con otra plataforma digital, esta actividad constituye un dato real de su identidad digital.

- **Datos inferidos o imaginarios**

Son conclusiones que otras personas pueden extraer a partir de la información disponible, pero que no necesariamente reflejan la realidad. Por ejemplo, si en la fotografía de la reunión mencionada anteriormente aparecen cuatro botellas de vino vacías sobre la mesa y solo cuatro personas en la imagen, un observador podría inferir erróneamente que cada uno ha consumido una botella completa. Sin embargo, la realidad puede ser muy distinta: tal vez hubo más invitados que no aparecen en la foto porque ya se habían marchado, o quizá las botellas estaban vacías desde una ocasión anterior. Incluso si efectivamente se consumió esa cantidad de vino, podría tratarse de una situación excepcional y no de un hábito regular. Esta interpretación errónea ilustra cómo la información digital puede generar percepciones sesgadas que distorsionan la imagen que los demás construyen sobre una persona, especialmente si no cuentan con suficiente contexto adicional.

Accede aquí a la serie de vídeos sobre Identidad digital de Antonio Omato y Víctor Cuevas.

4.2. REPUTACIÓN ONLINE

Por otra parte, la reputación online es el prestigio que tiene una persona, marca u organización y se fragua a partir de la opinión o consideración que los internautas vierten a la red sobre las acciones on y off-line de dicha entidad (INTEF, 2025).

Se construye a partir de la información disponible en internet, incluyendo publicaciones en redes sociales, reseñas, noticias, comentarios y cualquier otro contenido generado por los usuarios. Dado que esta reputación es una construcción social, depende en parte de nuestras acciones, pero también de las interacciones y opiniones de terceros.

Del Fresno (2012) indica que esta reputación online es la construcción social alrededor de la credibilidad, fiabilidad,

moralidad y coherencia que se tiene de una persona, ente, organismo, institución, empresa, etc. Esto es, la reputación sólo es parcialmente controlable ya que se crea y recrea a partir de las percepciones que conforman un estado de opinión, consideración y valoración de otros, a partir de las decisiones y comportamientos ético-morales y/o profesionales. Asimismo, se puede sostener que la reputación es una construcción social, un producto creado y acumulado de forma colectiva y que de manera inevitable tiene efectos positivos o negativos sobre el despliegue social, económico, etc. al tener una evidente connotación pública.



Figura 2. ¿Cómo comprobar qué información hay de ti en Internet? (extraído de /incibe.es)

Existen diversas herramientas, muchas de ellas gratuitas, que pueden ayudar en la gestión de la reputación online al permitirnos rastrear menciones, analizar tendencias y responder a comentarios de manera oportuna:

- Google Search: Realizar búsquedas periódicas con nuestro nombre o el de nuestra empresa nos permite conocer qué información es visible públicamente.
- Google Alerts: Esta herramienta de Google permite recibir notificaciones en tiempo real cada vez que nuestro nombre, marca o cualquier palabra clave relevante aparezca en internet.
- Hootsuite: Ideal para la gestión de redes sociales, permite programar publicaciones y monitorear menciones en distintas plataformas en un solo lugar.
- SocialMention: Analiza en tiempo real qué se dice sobre una persona o empresa en blogs, redes sociales y otras fuentes digitales, ofreciendo métricas sobre el sentimiento de las menciones (positivo, negativo o neutral).

Igualmente, existen otras más específicas según la función que estemos buscando.

- **Herramientas de monitorización de menciones y noticias**
  - Brand24: Permite rastrear menciones en redes sociales, blogs, foros y medios de comunicación en tiempo real.
  - Mention: Similar a Google Alerts, pero con análisis más detallado sobre menciones en distintas plataformas.
  - Talkwalker: Ofrece análisis avanzado de reputación con inteligencia artificial y monitoreo en múltiples idiomas.
  - GutherUp: Ideal para la gestión de reseñas en sitios como Google, Yelp y Facebook.
- **Herramientas de análisis de redes sociales**
  - Sprout Social: Ayuda a analizar el impacto de las publicaciones y las interacciones en redes sociales.
  - Brandwatch: Proporciona análisis detallados de redes sociales y tendencias digitales.
  - BuzzSumo: Permite ver qué contenido se comparte más y quién lo difunde, útil para medir influencia y reputación.
- **Herramientas de evaluación de Rreputación en buscadores**
  - SEMRush: Analiza la visibilidad de una marca en los motores de búsqueda y su presencia en internet.

- Ahrefs: Permite rastrear menciones y enlaces que apuntan a un sitio web, evaluando su impacto en la reputación.
- Moz: Analiza la autoridad de dominio y cómo los motores de búsqueda perciben una marca.

- **Herramientas de gestión de reseñas y comentarios**
  - ReviewTrackers: Ayuda a centralizar y gestionar reseñas de distintas plataformas para mejorar la reputación.
  - Podium: Permite a empresas recopilar y responder reseñas en diferentes sitios web.
  - Trustpilot: Plataforma que facilita la recolección y gestión de opiniones de clientes.

Aprende aquí sobre el Egosurfing: ¿Qué información hay de mí en internet? (INCIBE)

4.3. PRIVACIDAD

Según diversos estudios, una proporción significativa de la información disponible en la red sobre un individuo proviene directamente de la persona en cuestión, quien la ha compartido de manera consciente, ya sea a través de redes sociales, blogs, chats o servicios de mensajería instantánea (Solove, 2008). Además, otra parte considerable de los datos proviene de personas cercanas, como familiares o amigos, quienes a menudo comparten información sensible sin ser plenamente conscientes de los riesgos que esto conlleva (Tufekci, 2015).

El hecho de que cada vez más personas expongan sus vidas de manera voluntaria en el entorno digital aumenta la vulnerabilidad a aquellos actores que buscan hacer un uso indebido de esa información. Cuanta más información personal esté disponible en línea, más sencillo se vuelve para los ciberdelincuentes o individuos malintencionados obtener detalles cruciales para actividades ilegales, como el robo de identidad, fraudes o engaños. De acuerdo con los expertos en seguridad cibernética, la información que compartimos de manera inadvertida puede tener consecuencias mucho más graves de lo que imaginamos (Peltier, 2016).



Figura 3. Tu privacidad sí importa (extraído de /incibe.es)

Es fundamental, por lo tanto, gestionar con responsabilidad y cautela qué compartimos y con quién lo compartimos. A continuación, describimos algunos de los tipos de información más sensibles que debemos cuidar para evitar poner en riesgo nuestra seguridad:

- **Datos personales**

Información como el número de identificación (DNI, pasaporte) o datos vinculados a la identidad de una persona son de particular interés para los ciberdelincuentes. Estos datos pueden ser utilizados para suplantar la identidad de una persona,

abriendo puertas a fraudes financieros y otros delitos.

- **Contraseñas**

Las contraseñas son las claves de acceso a numerosos servicios y plataformas en línea. Si alguien tiene acceso a nuestras contraseñas, puede ingresar a nuestras cuentas y hacerse pasar por nosotros. Este riesgo es más común de lo que parece, debido a la tendencia de reutilizar contraseñas en varias cuentas.

- **Correo electrónico**

La exposición pública del correo electrónico puede derivar en problemas como el incremento de spam o la posibilidad de ser víctima de intentos de phishing, en los que los estafadores intentan obtener datos personales haciéndose pasar por entidades legítimas.

- **Datos bancarios**

El acceso a los datos bancarios, como números de cuentas o tarjetas de crédito, puede resultar en una pérdida económica significativa. Para prevenir el robo de esta información, es vital evitar compartirla a través de correos electrónicos o en sitios web no seguros.

- **Ubicación geográfica**

La ubicación es otro dato que debe ser protegido. Publicar en redes sociales la ubicación exacta en tiempo real, así como la frecuencia de nuestros desplazamientos, puede facilitar que personas malintencionadas descubran cuándo estaremos ausentes de casa o, incluso, que tengan acceso a detalles de nuestra rutina diaria.

- **Fotografías y vídeos**

El contenido visual también es muy revelador. Las fotos y vídeos contienen información que, a menudo, no somos capaces de percibir. A través de una simple imagen, se pueden conocer aspectos como la ubicación, las relaciones sociales, el nivel socioeconómico, las preferencias personales e, incluso, en el caso de imágenes de alta resolución, las huellas digitales (Fuchs, 2017). Asimismo, las imágenes compartidas en un contexto social o personal pueden tener repercusiones en el ámbito profesional. Una foto inapropiada puede ser vista por empleadores potenciales, lo que afectaría negativamente nuestra imagen profesional.



Para proteger adecuadamente la privacidad, es fundamental adoptar una serie de buenas prácticas en línea. Uno de los principios básicos es **publicar con cautela**. Cada vez que compartimos información en línea, estamos perdiendo parcialmente el control sobre ella. Incluso si eliminamos un contenido de nuestras redes sociales, el mismo puede haber sido replicado o compartido por otros usuarios, perpetuando su circulación sin nuestra autorización.

Al considerar qué compartir, es importante reflexionar sobre las implicaciones que esa acción podría tener, tanto para nosotros como para las personas a quienes etiquetamos o mencionamos. De acuerdo con la teoría de la privacidad en redes sociales, debemos revisar nuestras configuraciones de privacidad y asegurarnos de que solo las personas adecuadas puedan acceder a la información que decidimos compartir (Boyd, 2014).

Asimismo, **conocer nuestros derechos** es esencial. En el marco de la legislación española y europea, la Ley Orgánica de Protección de Datos (LOPD) regula el tratamiento y protección de datos personales. Esta normativa otorga a los ciudadanos derechos fundamentales, como el acceso, rectificación, y el derecho al olvido. El derecho al olvido, por ejemplo, permite a los ciudadanos solicitar que los motores de búsqueda eliminen ciertos enlaces que contengan información obsoleta o irrelevante para su vida personal (European Court of Justice, 2014).

Además, es importante considerar la **información que nuestro navegador web recopila de manera automática** A través de las cookies y el historial de navegación, se pueden obtener detalles sobre nuestros hábitos de navegación, lo cual pone en riesgo nuestra privacidad. Se recomienda configurar los navegadores para eliminar regularmente estos datos y ajustar las configuraciones de privacidad de manera que evitemos la recopilación no deseada de nuestra información personal (EU 2016/679).

Por último, se recomienda **configurar adecuadamente las opciones de privacidad de las redes sociales**, evitando exponer información sensible. Las redes sociales ofrecen varias opciones de privacidad que permiten limitar quiénes pueden ver nuestras publicaciones, fotos y otros contenidos. Tomarse el tiempo para conocer y ajustar estas configuraciones es una medida básica para proteger nuestra privacidad.

Descarga aquí una propuesta de unidad didáctica para trabajar la privacidad, de IS4K.

Y aquí una guía de Google e INCIBE sobre privacidad.

5. BULOS, HOAX Y FAKE NEWS

La era digital, donde la información circula a una velocidad sin precedentes, es el escenario idóneo para la propagación de rumores, bulos y noticias falsas. Las fake news son relatos fabricados y distribuidos con la intención de engañar, manipular la opinión pública o generar confusión. En muchas ocasiones, estas noticias se difunden sin ser verificadas, ya sea de manera intencionada o por simple descuido. El impacto de las fake news puede ser profundo, afectando desde elecciones políticas hasta la salud pública. En este apartado, exploraremos cómo se crean, se difunden y cómo podemos identificar y contrarrestar la desinformación en el entorno digital.

Las conocidas fake news, según INCIBE (2025), son **noticias falsas o bulos que se propagan por Internet con el objetivo de desinformar, engañar y manipular a los usuarios. También puede ser usadas para desprestigiar o enaltecer a determinadas personas o instituciones con el fin de obtener un beneficio económico**. Es importante tener en cuenta que las fake news no siempre son informaciones completamente falsas, a veces pueden contener elementos reales, pero se presentan de manera engañosa o se les da un giro para manipular la percepción pública.

Estas fake news pueden promover informaciones de distinta tipología que van desde historias sensacionalistas hasta teorías de conspiración. En ocasiones se crean con algún fin como puede ser político, ideológico o económico, aunque también pueden difundirse simplemente para tratar de captar la atención y generar clics en páginas web o generar controversia sobre temas de actualidad o interés entre los usuarios.



Las noticias falsas se propagan principalmente a través de plataformas de redes sociales, aplicaciones de mensajería y páginas web no verificadas. En ocasiones, los titulares sensacionalistas o alarmistas capturan la atención de los usuarios, quienes, sin verificar la fuente, las comparten rápidamente. Las fake news suelen aprovecharse de emociones fuertes, como el miedo o la indignación, para aumentar su alcance.

Además, la facilidad con la que podemos compartir contenido en plataformas como Facebook, Twitter, WhatsApp o Instagram ha generado un caldo de cultivo perfecto para que la desinformación se difunda de manera viral. Si bien estas herramientas han sido diseñadas para facilitar la conexión entre usuarios, también han permitido que los bulos se diseminen rápidamente entre miles, e incluso millones, de personas sin ningún control.

Existen diferentes tipos de fake news, aunque todos comparten el objetivo de manipular a la audiencia. Entre los existentes, podemos destacar (/unesco.org; /maldita.es):

- **Fabricación de hechos**: Son historias completamente inventadas que se presentan como si fueran eventos reales. A menudo se mezclan con detalles verídicos para darles más credibilidad.
- **Manipulación de hechos**: Este tipo de fake news toma hechos reales pero los presenta fuera de contexto o los distorsiona para apoyar una narrativa determinada.
- **Clickbait (cebo de clics)**: Titulares sensacionalistas que no se corresponden con el contenido del artículo, diseñados para atraer clics y generar ingresos publicitarios.
- **Rumores y desinformación**: Este tipo de fake news se basa en información parcial o inexacta que se transmite sin verificación

Las plataformas de redes sociales tienen un papel fundamental en la propagación de las fake news. En respuesta a este fenómeno, algunas redes sociales han implementado medidas para identificar y eliminar contenido falso, como la verificación de información mediante terceros o el uso de algoritmos que detectan patrones de desinformación. Sin embargo, la efectividad de estas medidas sigue siendo objeto de debate.

Descarga aquí la guía del taller "Sin verificar, no compartas" (LevantaLaCabeza)

Y desde los siguientes enlaces puedes acceder a actividades para aprender a detectar fake news:

- Mensajes de WhatsApp
- Noticia en periódico
- Publicación en una red social
- Mensaje publicitario



Otro tipo de bulos muy extendidos (aunque, a decir verdad, su máximo apogeo se vivió en la época del estadillo de los correos electrónicos) son los hoax. Un hoax es **un tipo de desinformación o engaño que se difunde principalmente a través de Internet y redes sociales, además de mensajería instantánea**. A diferencia de las fake news, que suelen estar diseñadas para parecer noticias verídicas, los hoax **generalmente se presentan como alertas, advertencias o mensajes preocupantes, a menudo relacionados con riesgos, amenazas o actividades ilícitas que, en realidad, son falsas**. Estos engaños se propagan rápidamente debido al miedo, la curiosidad o la solidaridad de quienes los reciben, lo que facilita su viralización.

Estos hoax cumplen unos requisitos muy fácilmente identificables (/newtral.es):

- **Sensacionalismo**: Los hoax a menudo apelan a emociones como el miedo, la ira o la sorpresa, con titulares alarmistas o historias inquietantes.
- **Urgencia**: Generalmente incluyen un tono urgente o un llamado a la acción, como "reenvíalo a todos tus contactos para que estén protegidos".
- **Falta de fuentes verificables**: Los hoax suelen carecer de una fuente confiable o de referencias verificables, lo que dificulta su autenticidad.
- **Falsas advertencias o promesas**: En muchos casos, los hoax advierten sobre problemas inexistentes, como virus informáticos, fraudes o estafas, o prometen beneficios que no se materializarán.

En la siguiente imagen hemos elaborado una serie de ejemplos sobre el tipo de hoax más comunes.

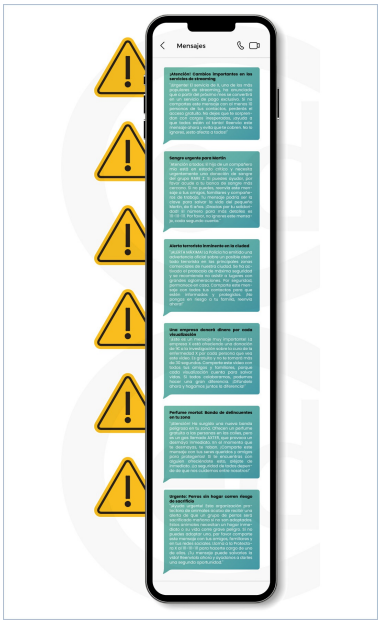


Figura 4. Tipos de hoax más comunes

Algunas de las pautas que pueden seguirse para verificar si estamos recibiendo un hoax son (INTEF, 2025):

- **Verificar las fuentes**: Antes de compartir cualquier información, especialmente si parece alarmante o sensacionalista, verifica las fuentes en sitios web de confianza.
- **Desconfiar de los mensajes que solicitan reenvíos**: Si un mensaje te insta a reenviar la información, es probable que sea un hoax. Las cadenas de mensajes no tienen fundamento y buscan aumentar su difusión.
- **Consultar sitios de verificación**: Existen plataformas dedicadas a desmentir rumores (bien sean hoax o fake news), como Snopes, PolitiFact, FactCheck.org, o Newtral que pueden ayudar a identificar si una noticia o alerta es un bulo.
- **Revisar el contenido de manera crítica**: Analiza si la información tiene sentido. Si parece demasiado alarmante o si carece de detalles verificables (como fuentes o hechos comprobables), es probable que sea falsa.

6. CIBERSEGURIDAD: VIRUS Y PROGRAMAS MALIGNOS

Como podemos imaginar, en nuestra sociedad de hoy día, la ciberseguridad se ha convertido en una preocupación global. Los programas malignos están más cerca de nosotros de lo que creemos y todos podemos ser víctimas de ellos, pues son herramientas utilizadas por ciberdelincuentes para infiltrarse, dañar o robar información de dispositivos y sistemas sin el consentimiento del usuario. Su evolución ha dado lugar a una gran variedad de amenazas que afectan a ordenadores, teléfonos móviles y redes informáticas.

Desde aquí consideramos los aspectos relacionados con la ciberseguridad como una parte sumamente importante del bienestar digital porque protege la integridad, privacidad y seguridad de los usuarios en el entorno digital. El bienestar digital se refiere al uso saludable, equilibrado y seguro de la tecnología, asegurando que ésta contribuya al desarrollo personal y social sin comprometer la seguridad, la privacidad o la estabilidad emocional del usuario.



Según el equipo técnico de Microsoft (s.f), la ciberseguridad, también conocida como seguridad digital, es la **práctica de proteger la información digital, dispositivos y activos, lo que incluye información personal, cuentas, archivos, fotos e incluso el dinero**.

Se considera que la ciberseguridad se estructura en torno a tres pilares

- **Confidencialidad**: mantener los secretos y garantizar que solo los usuarios autorizados puedan obtener acceso a sus archivos y cuentas.
- **Integridad**: garantizar que su información es la que debe ser y de que nadie ha insertado, modificado o eliminado cosas sin su permiso. Por ejemplo, cambiar de forma malintencionada un número en una hoja de cálculo.
- **Acceso**: garantizar que puede tener acceso a su información y sistemas cuando lo necesite. Un ejemplo de un problema de acceso sería una denegación de servicio, donde los atacantes desbordan el sistema con tráfico de red para hacer que el acceso sea casi imposible; o ransomware que cifra el sistema e impide que lo use.

Para IBM (2024), **la ciberseguridad se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto**. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciberamenazas.

Desde aquí puedes descargarte un completo glosario sobre términos relacionados con la ciberseguridad, elaborado por INCIBE.

Y aquí una guía sobre los ciberataques, también de INCIBE.

El término **malware** fue acuñado por Yisrael Radai en 1990 y abarca cualquier software diseñado con fines maliciosos. Aunque en el pasado se utilizaban términos como "virus informáticos", hoy en día el concepto ha evolucionado para incluir diversas amenazas. Según la Fundación del Español Urgente (FUNDEU), en español es preferible emplear las

expresiones " **programa maligno**" o " **programa malicioso**".

Igualmente, es importante distinguir entre software maligno y software defectuoso. Mientras que el primero es desarrollado con intenciones perjudiciales, el segundo contiene errores involuntarios que pueden afectar su funcionalidad.

El malware es **software intrusivo que está diseñado deliberadamente para provocar daños en equipos y sistemas informáticos** (/kaspersky.es).

Cuando hablamos de riesgos en seguridad digital solemos evocar dos conceptos, principalmente: virus y programas malignos, aunque no debemos usarlos de forma indiscriminada.

La diferencia principal entre virus y programas malignos, también conocidos como malware, es que el virus informático es solo un tipo dentro de la gran categoría de programas malignos existentes, de modo que todos los virus son malware, pero no todo el malware es un virus.

- **Virus informáticos**
  - Es un tipo específico de malware que se adhiere a un archivo o programa legítimo y se replica al ejecutarse.
  - Depende de la acción del usuario para activarse (por ejemplo, al abrir un archivo infectado).
    Puede corromper archivos, ralentizar el sistema, robar información o destruir datos.
  - A diferencia de otros tipos de malware como los gusanos, que se propagan automáticamente, el virus necesita que el usuario lo ejecute o transfiera para infectar otros sistemas.
- **Programas malignos**
  - Es el término general que engloba todas las formas de software malicioso diseñadas para dañar, infiltrarse o comprometer un sistema sin el consentimiento del usuario.
  - Existen muchos tipos de malware, entre ellos los virus, gusanos, troyanos, ransomware, spyware, adware, rootkits, keyloggers, botnets, entre otros.
  - No todos los malware se replican o infectan archivos de la misma manera que un virus.



Existen diversas categorías de malware, entre ellas (/kaspersky.es):

- **Virus informáticos**

Programas que se adhieren a archivos legítimos y se replican al ejecutarlos. Una vez dentro de la red, un virus puede robar datos confidenciales, ejecutar ataques DDoS o llevar a cabo ataques de ransomware. Un virus, que suele propagarse a través de sitios web infectados, transferencias de archivos o descargas de archivos adjuntos de correos electrónicos, permanecerá inactivo hasta que el archivo o programa infectado se active. Cuando eso sucede, el virus puede replicarse y propagarse en sus sistemas.

- **Gusanos (worms)**

Malware que se propaga de forma autónoma a través de redes mediante la explotación de vulnerabilidades del sistema operativo. Un gusano es un programa independiente que se replica para infectar otros equipos sin requerir la acción de nadie. Dado que se pueden propagar rápido, los gusanos suelen utilizarse para ejecutar una carga (un fragmento de código creado para dañar un sistema). Las cargas pueden eliminar archivos en un sistema host, cifrar datos para un ataque de ransomware, robar información, eliminar archivos y crear botnets.

- **Troyanos**

Se presentan como programas legítimos, pero al ejecutarse permiten el acceso remoto al sistema. Como parece legítimo, los usuarios lo descargan y, sin darse cuenta, permiten que el malware entre en su dispositivo. Los troyanos son una puerta de entrada. A diferencia de un gusano, necesitan un host para funcionar. Una vez que un troyano se instala en un dispositivo, los hackers pueden usarlo para eliminar, modificar o capturar datos, recolectar tu dispositivo como parte de un botnet u obtener acceso a tu red.

- **Spyware**

Diseñado para recopilar información del usuario sin su consentimiento. Es una forma de malware que se oculta en el dispositivo, controla tu actividad y roba información confidencial como datos financieros, información de cuentas, contraseñas y mucho más. El spyware puede propagarse al explotar vulnerabilidades de software o puede incluirse con programas legítimos o en troyanos.

- **Adware**

Muestra publicidad invasiva y en algunos casos recopila datos del usuario. La palabra es una contracción de “advertising-supported software” (software con publicidad), muestra anuncios no deseados y a veces maliciosos en la pantalla del ordenador o dispositivo móvil, redirige los resultados de las búsquedas a sitios web de publicidad y recopila los datos de los usuarios para venderlos a anunciantes sin su consentimiento. No todo el adware es malware, ya que algunos son programas legítimos y se pueden usar de manera segura.

- **Botnets**

Un bot es un equipo infectado con malware que un hacker puede controlar de manera remota. El bot, a veces llamado "equipo zombie", se puede utilizar para ejecutar más ataques o formar parte de una colección de bots llamada botnet. Los botnets pueden incluir millones de dispositivos que se propagan de forma desapercibida. Los botnets ayudan a los hackers con numerosas actividades maliciosas, incluidos los ataques DDoS, el envío de mensajes de spam y phishing, y la propagación de otros tipos de malware.

- **Ransomware**

Cifra archivos o bloquea dispositivos exigiendo un rescate para restaurar el acceso. diseñado para bloquear el acceso de los usuarios a su sistema o denegar el acceso a los datos hasta que se pague un rescate. El malware de cifrado es un tipo de ransomware que cifra los archivos del usuario y reclama un pago antes de una fecha específica; a menudo, este debe hacerse a través de una criptomoneda, como el Bitcoin. El ransomware lleva muchos años siendo una amenaza persistente para las organizaciones de muchos sectores. Ya que cada vez más empresas adoptan la transformación digital, la probabilidad de ser objetivo de un ataque de ransomware crece considerablemente.

- **Rootkits**

Se ocultan en el sistema para permitir el control remoto del dispositivo.

- **Keyloggers**

Registran las pulsaciones del teclado para robar credenciales. Cuando se instalan con fines maliciosos, los keyloggers pueden usarse para robar datos de contraseñas, información bancaria y otra información confidencial. Los keyloggers pueden entrar en un sistema a través de phishing, ingeniería social o descargas maliciosas.

- **Malware sin archivos**

El malware sin archivos es un tipo de software malicioso que utiliza programas legítimos para infectar un equipo. No necesita ningún archivo y no deja rastro, lo que dificulta su detección y eliminación.

Puedes acceder aquí al servicio AntiBotnet de INCIBE.



Estos programas malignos pueden infiltrarse en dispositivos a través de múltiples métodos (/avast.com; González, 2022; Caballero, 2021):

Correo electrónico

El correo electrónico es una de las vías más comunes de infección por malware debido a su accesibilidad y alcance masivo. Los ciberdelincuentes envían correos fraudulentos que pueden incluir archivos adjuntos o enlaces maliciosos diseñados para instalar software dañino en los dispositivos de los usuarios.

Uno de los métodos más utilizados en estos ataques es el phishing, una técnica de suplantación de identidad en la que los atacantes se hacen pasar por entidades legítimas como bancos, empresas tecnológicas o instituciones gubernamentales. A través de correos aparentemente auténticos, persuaden a los usuarios para que ingresen credenciales de acceso, información bancaria o datos personales en páginas falsas.

Otra variante es el spear phishing, donde el ataque es personalizado y dirigido a una víctima en particular, utilizando información obtenida previamente para hacer el engaño más creíble. También existen correos con archivos adjuntos infectados, como documentos de Word, Excel o PDF que contienen macros maliciosas capaces de ejecutar código peligroso en el sistema.

Incluso si el remitente es un contacto conocido el correo puede ser malicioso ya que los atacantes pueden haber comprometido la cuenta de esa persona o haber falsificado su dirección de envío (email spoofing).

Accede aquí al documento del INCIBE "Cómo detectar un enlace malicioso".

Dispositivos de almacenamiento externo

Los dispositivos de almacenamiento externo como pendrives, discos duros externos y tarjetas de memoria pueden ser vehículos de transmisión de malware. Una de las amenazas más peligrosas en este ámbito son los virus que se ejecutan automáticamente al conectar el dispositivo a un ordenador, como los gusanos que explotan la función de autoejecución (autorun.inf).

Estos dispositivos pueden infectarse cuando se conectan a un sistema ya comprometido y, posteriormente, propagar el

malware al insertarse en otros equipos.

Para minimizar riesgos, se recomienda desactivar la ejecución automática en el sistema operativo, analizar los dispositivos con un antivirus antes de abrir su contenido y evitar conectar unidades de almacenamiento desconocidas o encontradas en espacios públicos.

Descarga de archivos y aplicaciones

Las descargas de software y archivos desde fuentes no confiables son una de las formas más frecuentes de infección. Existen numerosas amenazas relacionadas con este método, como los troyanos, que parecen programas legítimos, pero, incluyen funciones ocultas para robar datos o dañar el sistema.

Las aplicaciones móviles obtenidas fuera de las tiendas oficiales también suelen ser un vector de ataque frecuente. Los ciberdelincuentes modifican aplicaciones populares para incluir malware y las distribuyen en sitios web de dudosa procedencia para, una vez instaladas, robar información personal y credenciales, realizar suscripciones a servicios premium sin consentimiento e instalar otros programas maliciosos sin el conocimiento del usuario.

En el caso de archivos de escritorio, los formatos más utilizados para ocultar malware incluyen archivos comprimidos (.zip, .rar), documentos con macros habilitadas (.docm, .xlsm) y archivos ejecutables (.exe, .dmg).

Para reducir riesgos, es fundamental descargar software solo desde sitios oficiales, leer los permisos solicitados por las aplicaciones antes de instalarlas y contar con un antivirus actualizado que analice los archivos descargados.

Navegación web

La navegación web es otro medio de infección, ya que existen páginas diseñadas específicamente para propagar malware. Algunas de las técnicas más utilizadas son:

- **Drive-by-download**: el usuario visita un sitio web comprometido y el malware se descarga automáticamente sin necesidad de que haga clic en nada.
- **BlackHat SEO**: manipulación de los resultados de búsqueda para posicionar páginas maliciosas en los primeros lugares.
- **Pharming**: modificación de los registros DNS para redirigir a los usuarios a sitios fraudulentos sin que se den cuenta.

Algunos sitios web maliciosos están diseñados para explotar vulnerabilidades del navegador o de plugins como Adobe Flash, Java o extensiones de terceros. Por ello, es recomendable mantener el software actualizado, usar bloqueadores de anuncios y extensiones de seguridad que analicen enlaces peligrosos.

Redes sociales

Las redes sociales son un entorno ideal para la propagación de malware debido a la confianza entre usuarios y la viralización de contenidos y los ciberdelincuentes aprovechan la actitud de la gente en estas plataformas para distribuir enlaces maliciosos que suelen disfrazar de noticias falsas con títulos sensacionalistas, ofertas y promociones que solicitan datos personales y aplicaciones que requieren permisos excesivos para operar.

Otro riesgo común son las cuentas hackeadas, desde las cuales los atacantes envían mensajes privados con enlaces peligrosos a los contactos del usuario afectado.

Para evitar estos ataques, se recomienda no acceder a enlaces sospechosos, revisar los permisos de las aplicaciones instaladas y activar la autenticación en dos pasos para proteger las cuentas.

Vulnerabilidades del sistema

Los sistemas operativos y programas pueden tener fallos de seguridad que los ciberdelincuentes aprovechan para infectar dispositivos sin necesidad de interacción del usuario. Estos errores, conocidos como vulnerabilidades de software, pueden ser explotados mediante técnicas como:

- **Exploits**, que aprovechan errores de seguridad en programas desactualizados.
- **Zero-day attacks**, ataques que explotan vulnerabilidades desconocidas antes de que los fabricantes las solucionen.
- **Ataques de escalada de privilegios**, que permiten obtener acceso de administrador sin autorización.

Para minimizar estos riesgos podemos mantener el sistema operativo y los programas siempre actualizados, configurar las actualizaciones automáticas cuando sea posible y usar software de seguridad que detecte y prevenga exploits.



Las consecuencias y el impacto de estos malwares puede ser devastador, desde pérdida y destrucción de información, pasando por la ralentización del sistema y el control remoto del dispositivo, hasta llegar al robo de información personal y bancaria e incluso la suplantación de identidad.

Para minimizar el riesgo de infección se suele recomendar, ante todo, sentido común. No obstante, es importante tener presente lo que ya hemos argumentado en varios momentos: la importancia de la **actualización del software y sistemas operativos** regularmente, así como **evitar descargar archivos y programas de fuentes desconocidas**. **No hacer clic en enlaces sospechosos** en correos electrónicos o redes sociales, **usar contraseñas seguras** y **autenticación en dos pasos**, instalar **antivirus** y firewall confiables y **realizar copias de seguridad** periódicas de la información importante son las actuaciones más elementales que tener en cuenta para no ser víctima de estos ataques (INTEF, 2025).