

Seguridad en internet

**Twitter**

**Índice**

[Seguridad en Internet 2](#_Toc36129297)

[¿Qué es Internet? 2](#_Toc36129298)

[¿Qué es la seguridad en Internet? 2](#_Toc36129299)

[¿Para qué sirve la seguridad en Internet? 3](#_Toc36129300)

[Tipos de seguridad en Internet 3](#_Toc36129301)

[Leyes en España de seguridad en Internet 4](#_Toc36129302)

[Twitter 5](#_Toc36129303)

[Estadísticas de Twitter 6](#_Toc36129304)

[Problemas de seguridad en Twitter 7](#_Toc36129305)

[Mejoras de seguridad en Twitter 8](#_Toc36129306)

[Conclusión 9](#_Toc36129307)

[Bibliografía 10](#_Toc36129308)

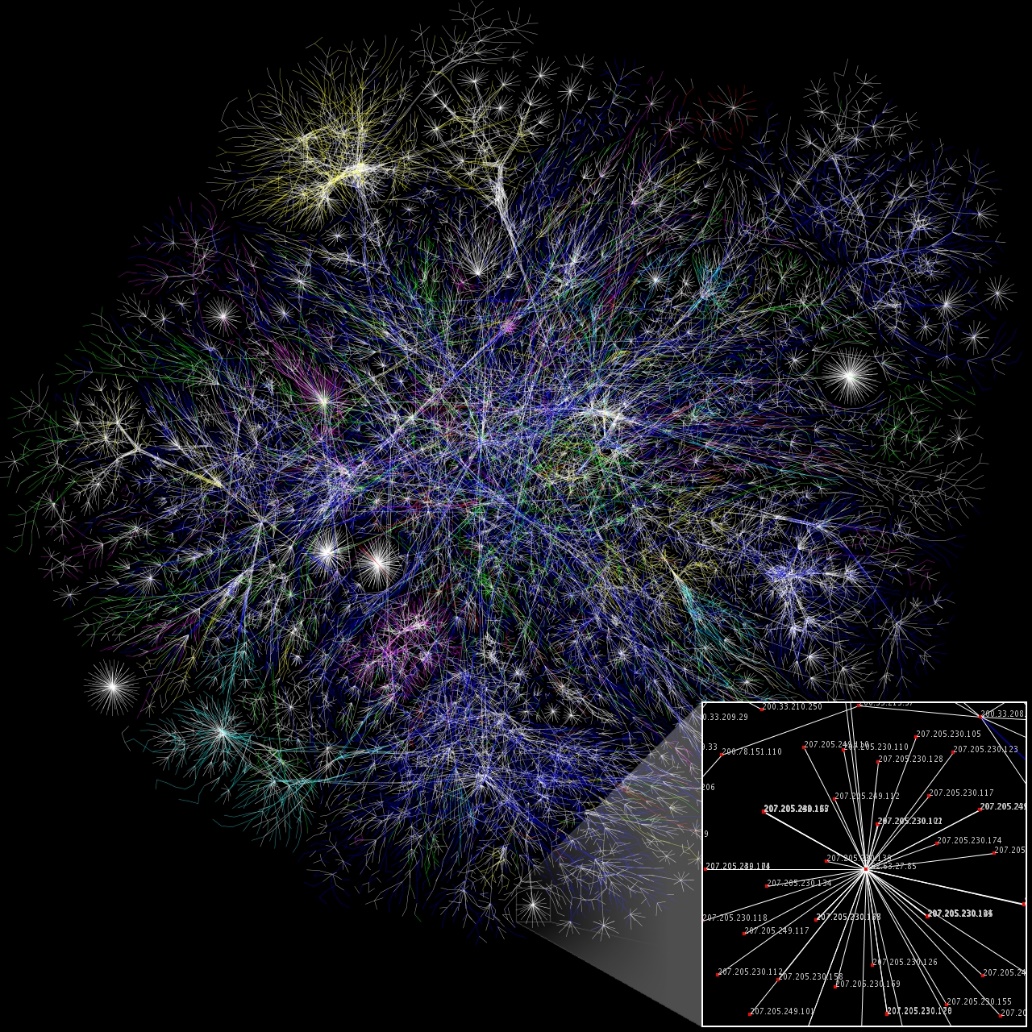
# 

# **Seguridad en Internet**

**El primer paso para poder hablar sobre seguridad en Internet es saber a qué nos referimos al hablar de Internet, de esta manera podremos conocer el fin de la seguridad en Internet y cómo se lleva a cabo.**

## **¿Qué es Internet?**

Internet **se define como una red mundial de equipos informáticos la cual, debido a su complejidad, no tiene una estructura bien definida; formando así una red con topología irregular que sirve como red troncal para la interconexión de redes de todo el mundo. Esta red proporciona numerosos servicios como el envío de correo electrónico, transmisión de archivos o páginas web entre otros muchos que, en definitiva, permiten a los usuarios transmitir información.**



Mapa lógico (direcciones IP) de Internet en 2005

## **¿Qué es la seguridad en Internet?**

**Si antes hemos hablado de Internet como un medio de transmisión de información entre dos puntos, la seguridad en Internet es la encargada de proteger todos los elementos, es decir, no solo la información sino también los equipos que forman parte de la red.**

**La seguridad en Internet o seguridad informática es la encargada de crear protocolos y herramientas que permitan detectar y eliminar las vulnerabilidades en los equipos informáticos o en el envío de información. Se pueden distinguir tres fases acerca de la seguridad informática:**

* **Protección / prevención: Tratar de configurar los equipos de la forma más correcta posible.**
* **Detección: Capacidad de identificar cuando la configuración cambia u ocurre un problema.**
* **Reacción: Responder ante el problema y volver a un estado seguro lo más rápido posible.**

## **¿Para qué sirve la seguridad en Internet?**

Mediante la seguridad informática podemos lograr proteger y mantener los cuatro pilares que la hacen tan importante:

* Confidencialidad: La información solo está disponible para los usuarios autorizados.
* Integridad: La información podrá ser modificada sólo por los usuarios autorizados.
* Disponibilidad: La información debe estar disponible para los usuarios en cualquier momento.
* Autenticación: La información viaja realmente al usuario con el que te quieres comunicar.

## **Tipos de seguridad en Internet**

**Para llevar a cabo esta protección existe una amplia variedad de métodos que permiten, de una forma u otra, garantizar la seguridad informática de los equipos y la información. Algunos de los ejemplos más conocidos son:**

* **Control de acceso: permite que solo los usuarios verificados sean capaces de acceder al dispositivo o información que están autorizados. En muchas ocasiones este supone la primera línea de defensa por lo que cada vez se demanda una mayor sofisticación de las técnicas empleadas en el control de acceso.**
* **Cortafuegos (firewall): este es probablemente el primer concepto que se nos viene a la mente al escuchar seguridad en Internet. Este es uno de los primeros métodos de seguridad informática que surgieron y nos permite regular el tráfico que entra o sale en nuestra red, es decir, bloquea la información no permitida y deja pasar la información entre comunicaciones autorizadas.**
* **Antivirus: quizá sea la técnica de seguridad más utilizada a día de hoy, prácticamente cualquier equipo tiene un antivirus y gracias a ellos podemos escanear nuestro equipo en busca de software malicioso (malware), eliminarlo y reparar el daño que haya podido causar.**
* **Criptografía: técnica que permite codificar una información con el fin de hacerlos incomprensibles para todo el mundo a excepción del usuario receptor autorizado. Cada vez las técnicas de encriptación son más complejas y juegan un papel crucial en la seguridad en Internet.**
* **Cuidado con la ingeniería social: esta consiste en engañar a los usuarios para obtener su información personal como datos bancarios o contraseñas o infectar sus equipos con (malware). Esta práctica habitual en las redes sociales por lo que entraremos más en profundidad y de cómo luchar contra ella en los próximos puntos.**

# **Leyes en España de seguridad en Internet**

Debido al contexto histórico sufrido en España durante el siglo XX, las nuevas tecnologías tardaron mucho tiempo en llegar y, por consiguiente, las leyes que la regulan. No fue hasta 1985 donde la Ley del Patrimonio Español hacía referencia a un documento como una expresión de lenguaje o gráfica recogida en un soporte material o informático.

El 13 de diciembre de 1999 entró en vigor la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD). En ella se clasifican los datos personales según su grado de importancia de tal modo, los requisitos legales y la seguridad informática que protejan estos datos deberán ser más estrictas en función de la importancia de los mismos. Esta Ley obliga a informar a los usuarios de la existencia de un fichero con sus datos. Pese a esto sigue siendo posible tratar la información personal sin haberla obtenido directamente de la persona en cuestión, aunque deberá ser informada dentro de los tres meses siguientes del tratamiento de dicha información. En caso de haber obtenido los datos de una fuente pública no será necesaria la comunicación, es decir, los datos obtenidos mediante la publicación de un usuario en una red social pueden ser tratados sin que el usuario sea comunicado.

El organismo público encargo de hacer cumplir la LOPD es la Agencia Española de Protección de Datos (AEPD). Esta fue fundada en 1994 y tiene el deber velar por la privacidad y protección de datos de los ciudadanos, así como garantiza el cumplimento de la LOPD.

Esta Ley estuvo en Vigor hasta el año 2018, cuando fue remplazada por la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD). Esta va acorde con la Ley de Protección de Datos Europea aprobada en mayo de 2018.

En ella aparecen multitud de novedades con respecto a su predecesora. Entre estas novedades podemos destacar el principio de transparencia por el cual los usuarios están en su derecho de ser informados de forma clara de la manera en la que sus datos van a ser tratados.

Además, aparece la figura del Delegado de Protección de datos, el cual se encarga de comprobar que el tratamiento de datos se haga de forma adecuada y siempre acorde a la Ley. Así mismo, las empresas que traten con información estarán obligadas a contar con esta figura.

Otra de las novedades trata sobre el reconocimiento expreso de los derechos digitales el cual otorga a los trabajadores el derecho a la desconexión digital, lo que significa que, una vez termina su jornada laboral, un trabajador no estará obligado a utilizar dispositivos electrónicos con motivos profesionales.

Por último, esta Ley también protege a los menores, haciendo así que solo los mayores de trece años puedan dar su consentimiento para el tratado de información personal.

# **Twitter**

Twitter es, a día de hoy, una de las redes sociales más populares del mundo con más de 100 millones de usuarios activos cada día y más de 500 millones de tweets enviados diariamente.

Es una herramienta útil para seguir noticias, famosos o simplemente compartir tu estado o multimedia con amigos.

Twitter surgió de la mano de Jack Dorsey y Evan Williams en 2006 con la idea de crear una plataforma basada en SMS en la cual amigos pudieran estar al tanto entre ellos mediante sus estados. Estos estados sólo podían contener 140 caracteres debido a las limitaciones de los móviles, aunque esto se mantuvo ya que una de las principales razones de la expansión tan rápida que sufrió Twitter en 2007 fue su simpleza (a finales de 2017 este límite se expandió hasta los 280 caracteres).

Aunque en un primer momento Twitter solo permitía publicar texto plano, hoy en día, los usuarios pueden compartir mensajes, fotos, videos, gifs, música, etc.… a través de un Tweet.

Un Tweet es una pequeña publicación que permite a los usuarios comunicarse con sus seguidores. De esta manera un usuario puede seguir a tanta gente como desee y de este modo en su muro aparecerán todos los Tweets de las personas a las que está siguiendo. Además, existe la opción de *retwittear* que republicará el Tweet de otra persona para que tus seguidores lo puedan ver.

Además, Twitter permite tener conversaciones privadas con otros usuarios que, a diferencia de los Tweets, nadie puede ver.

Uno de los motivos que hace a Twitter una de las redes social más popular es la barra de tendencia, cuando una multitud de usuarios *tweetean* sobre el mismo tema este aparece en tendencias por lo que los demás usuarios pueden estar informados en todo momento sobre la actualidad.

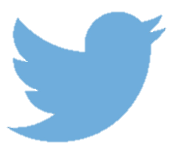
Las cuentas en Twitter pueden ser públicas (todo el mundo puede ver tus publicaciones) o privadas (solo las personas que te siguen pueden ver tus publicaciones, habiendo sido aceptadas previamente por el usuario).

Para iniciar sesión en una cuenta es necesario un nombre de usuario o teléfono móvil y la contraseña asociada a dicha cuenta. Es necesario introducir una dirección de correo electrónico para registrase lo que permite recuperar la cuenta en caso de robo u olvido de la contraseña.



Ejemplo de Tweet básico

## **Estadísticas de Twitter**



# **Problemas de seguridad en Twitter**

Como cualquier otro fenómeno global Twitter es susceptible a todo tipo de ataques y ciberdelincuencia mediante las técnicas de ingeniería social comentadas en el punto “Seguridad en Internet”.

Existen multitud de *cuentas bot* que se dedican a publicar numerosos tweets por cualquier tipo de tendencia global en busca de la mayor visibilidad posible (spam). Muchos de estos son inofensivos, pero otros pueden contener enlaces que llevan sitios web maliciosos y poner en riesgo la seguridad de tu equipo. Es muy importante que el usuario sea consciente en todo momento a qué sitio web se dirige cuando pulsa en un enlace y los riesgos que esto conlleva

Además, muchos cibercriminales utilizan la plataforma para engañar a un usuario con una premisa falsa con el fin de obtener los datos personales o contraseñas de la víctima, está práctica es conocidas como “phishing” y si bien es cierto que Twitter la prohíbe completamente es muy difícil de detectar y aún más de sancionar por lo que supone un riesgo para los usuarios de Twitter que sean vulnerables a estas técnicas.

Durante su historia Twitter ha recibido numerosos ataques que han puesto en compromiso las cuentas de los usuarios y sus datos personales en varias ocasiones. Algunos de los ejemplos más significativos son:

* Ataque durante el 3-4 de febrero de 2013: a raíz de una brecha de seguridad en navegadores que utilizan Java, más de 250 000 usuarios vieron comprometidas sus cuentas. Una vez detectado y solucionado el problema Twitter reinicio las contraseñas de los usuarios y les solicito un cambio de estas.
* En mayo de 2018 Twitter encontró un problema por el cual, la contraseña de todos sus usuarios por aquel entonces (más de 330 millones) fueron almacenadas estaban erróneamente almacenadas como texto plano en lugar de texto enmascarado. Pese a que no se detectó ninguna brecha o robo se notificó a todos los usuarios que deberían cambiar su contraseña para evitar problemas con la seguridad de sus datos.
* Uno de los ataques más recientes sufridos en Twitter fue el último 23 de diciembre cuando se descubrió un problema de seguridad que permitía a un atacante, mediante la inserción de código malicioso en la aplicación de Twitter para Android, a varias cuentas ajenas y acceder a la información personal y estas, pudiendo incluso publicar Tweets desde estas cuentas. No se confirmó ningún casó en el que esto llegara a ocurrir, pero Twitter afirmo que “no pueden estar completamente seguros” de que nada hubiera pasado antes de lanzar una actualización que corregiría dicho problema

# **Mejoras de seguridad en Twitter**

Twitter, al estar en continua amenaza ante ataques de todo tipo, está en constante actualización. Cada vez que aparece una nueva brecha de seguridad o intento de ataque, los desarrolladores de Twitter responden con una nueva actualización de seguridad al poco tiempo que corrige estos errores como hemos visto en el punto anterior.

Con el fin de dificultar el espionaje a la privacidad de los usuarios, Twitter mejoro las técnicas de encriptación de la información en 2013. Hasta aquel entonces utilizaban el protocolo HTTPS para encriptar las sesiones de los usuarios, pero este protocolo puede generar problemas a la hora de almacenar sesiones que se almacenan por lo que, a raíz de esto, implementaron las técnicas de encriptación *Forward Secrecy* por lo que en cada sesión se genera una clave aleatoria. Si un ciberdelincuente obtuviera esta clave seguiría sin poder acceder a la información de todo el tráfico almacenado

Pero las mejoras de seguridad no solo se basan en nuevas técnicas de encriptación. De hecho, la mayoría de actualizaciones de seguridad se basan en luchar contra la ingeniería social, no contra los ciberataques.

Twitter pone a disposición de los usuarios un gran número de herramientas para que puedan hacer frente ante cualquier tipo de contenido indeseado o malicioso.

Una de las mejores funciones que nos ofrece Twitter a la hora de proteger nuestra cuenta ante posibles intrusos que estén intentando acceder a ella es la verificación en dos fases. Gracias a esta función podemos pedir a Twitter un segundo método de autentificación además de la contraseña cuando quieras iniciar sesión en Twitter como pueda ser una app de autentificación, un SMS o una llave de seguridad.

Para evitar que personas no deseadas puedan ver la información que el usuario publica es posible bloquear cuentas o proteger tus Tweets para qué solo las personas que te siguen (habiendo sido aceptadas previamente por el usuario) pueden ver tus publicaciones.

Así mismo es posible configurar la cuenta del usuario mediante las herramientas de filtrado, búsqueda segura o deshabilitar los mensajes directos para que un usuario no pueda recibir contenido indeseado, ya sea en forma de Tweet o mensaje directo con intenciones maliciosas.

Con el paso de los años Twitter ha mejorado enormemente su seguridad mediante el uso de todas estas herramientas, pero aun así muchos de los usuarios de la plataforma no son conocedores de todas estas funciones y que son de gran utilidad de cara a una experiencia más saludable de la plataforma. Es por ello que es muy importante dedicar todos los recursos posibles en enseñar a los usuarios el uso de estas herramientas y como pueden manejarlas para su beneficio. Este es sin duda el paso más importante de cara a una red social más segura en la que la información de los usuarios no se vea amenazada por ciberdelincuentes.

# **Conclusión**

Si la información es poder, entonces las redes sociales son las armas más poderosas que tiene la humanidad y no nos debe sorprender que tanta gente ansié conocer toda esta información, desde ciberdelincuentes hasta multinacionales pasando por partidos políticos o gobiernos.

Esta información supone un valor incalculable que, en malas manos puede suponer un gran daño para la sociedad, por ello la seguridad informática supone un papel crucial a la hora de defender los derechos fundamentales de los usuarios a su intimidad y datos personales. Esta no es una tarea para nada fácil que trae de cabeza a los mejores informáticos con el fin de crear aplicaciones más seguras y protegidas ante los ataques de ciberdelincuentes.

Las redes sociales juegan un papel importantísimo en la seguridad en Internet puesto que es aquí donde nos podemos encontrar al eslabón más débil que forma toda esta cadena de seguridad: el usuario. Si bien es cierto que se hace todo lo posible para que el usuario tenga todas las herramientas necesarias para hacer un buen uso de las aplicaciones, este no siempre es el caso y debido a esto, hacer peligrar nuestra seguridad ante las técnicas de ingeniera social que, cada vez son más frecuentes y más efectivas.

Es importante saber que no estamos solos, tenemos una Ley estricta que nos protege e incluso una agencia que se encarga de hacer cumplir esta Ley de manera rigurosa. Es cierto que eventualmente surgen brechas de seguridad o bugs que nos ponen en peligro, pero cada vez estas son menos frecuentas, y si bien es cierto que posiblemente nunca dejarán de existir cada vez son más difíciles explotar por los ciberdelincuentes. Pero esto no debe relajarnos puesto que cada vez se desarrollan nuevas técnicas que ponen en jaque nuestra seguridad.

Las técnicas de ingeniería social como el *phishing, baiting o scavening* suponen un gran riesgo para la seguridad de los usuarios, y no son siempre fáciles de detectar. Disponemos de numerosas herramientas como puedan ser los antivirus o los cortafuegos que nos ayudan, por ello está en nuestras manos concienciar de los peligros y enseñar a todos los usuarios del uso correcto de estas técnicas de seguridad que están a nuestra disposición para disfrutar de todas las plataformas que nos brinda Internet como pueda ser Twitter.

Sin duda las redes sociales, como Twitter, son una gran herramienta que nos permite estar en contacto con nuestros amigos, conocer gente nueva o estar informados de la actualidad en el mundo entre otras muchas. Todo el mundo hace uso de ellas y por ello es muy importante conocer todos los aspectos de ellas; cómo podemos beneficiarnos de sus funciones, pero también como debemos protegernos ante sus amenazas. Los desarrolladores hacen una gran labor protegiéndonos antes ataques con técnicas de ciberseguridad muy complejas y efectivas, pero cada vez es más importante y es nuestro deber poner de nuestra parte para que, aunque pueda ser una idea utópica, podamos usar Internet de forma segura.

# **Bibliografía**

* **Libro “Seguridad en Internet” por Gonzalo Asensio →** <http://tecnologiasemergentesnegocios2012.pbworks.com/w/file/fetch/54228387/descarga_promo_SEGURIDAD%20EN%20INTERNET,%20Nowtilus.pdf>
* **Artículo de CISCO acerca de la seguridad en Internet →** <https://www.cisco.com/c/en/us/products/security/what-is-network-security.html>
* **Artículo sobre ciberseguridad →** <https://www.forcepoint.com/cyber-edu/network-security>
* **Artículo de CSO sobre la definición y tipos de seguridad informática →** <https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html>
* **Mapa lógico de Internet →** [www.opte.org](http://www.opte.org)
* **Artículo de la Universidad Internacional de Valencia sobre el uso de la seguridad informática →** <https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/>
* **Artículo sobre criptografía →** <https://searchsecurity.techtarget.com/definition/cryptography>
* **Artículo de CSO sobre el control de acceso →** <https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html>
* [**Entrada de blog acerca del fundamentos básicos de Twitter →** https://blog.hubspot.com/marketing/what-is-twitter](Entrada%20de%20blog%20acerca%20del%20fundamentos%20básicos%20de%20Twitter%20→%20https://blog.hubspot.com/marketing/what-is-twitter)
* **Noticia sobre error de seguridad en Twitter de 2016 →** <https://www.bankinfosecurity.com/33-million-twitter-credentials-may-have-been-leaked-a-9187>
* **Tweet sobre fallo de seguridad en el enmascaramiento de las contraseñas de los usuarios en 2017 →** <https://twitter.com/TwitterSupport/status/992132808192634881>
* **Ley Orgánica de Protección de datos Personales de 1999 →** <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>
* **Ley Orgánica de Protección de datos Personales y garantía de datos personales de 2018 →** <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>
* **Página web sobre leyes relacionadas con la informática →** <http://www.informatica-juridica.com/legislacion/espana/>
* [**Página web de la agencia española de protección de datos →** https://www.aepd.es/es](Página%20web%20de%20la%20agencia%20española%20de%20protección%20de%20datos%20→%20https://www.aepd.es/es)
* **Noticia sobre la mejora en la encriptación de Twitter →** <https://computerhoy.com/noticias/internet/twitter-mejora-encriptacion-proteger-tweets-7640>