Definición y explicación de los términos que se utilizan en el lenguaje de internet y de las Redes Sociales (RRSS)

PIENSA

Conectarse a Internet es una acción que realizamos casi a diario. Internet es en realidad un conjunto descentralizado de redes de comunicación interconectadas, que funciona como una red única de alcance mundial.

Las posibilidades que ofrece para acceder a información, para el entretenimiento, la comunicación e incluso la compra de cualquier producto son importantes, pero también encierra dificultades y desventajas. Por ello es necesario que conozcamos qué ventajas nos ofrece este sistema de comunicación, cómo utilizarlas y cómo evitar los posibles peligros.

SABÍAS QUE...

INTERNET

Si Internet fuera un país, sería el sexto más contaminante del mundo. La huella ecológica de este inmenso tráfico digital equivale a un consumo aproximado del 7% de la electricidad mundial. Se responsable con el uso que haces, no abusen por bien del planeta, y por el bien de tu salud física y mental.

Existen muchos servicios y protocolos en Internet, aparte de la web: el envío de correo electrónico, la transmisión y consulta de archivos, las conversaciones en línea, la mensajería instantánea, la comunicación multimedia o los juegos en línea.

ACCESO Y CONEXIONES:

Son varios los criterios para clasificar las conexiones a Internet, al menos tantos como tipos de redes a las que podemos conectar nuestro equipo. Dichas diferencias pueden encontrarse en el nivel físico y el tipo de tecnología de la que se sirven.

a) Línea telefónica

Se necesita un módem, el cual convierte las señales digitales del ordenador en impulsos de sonido que se trasmiten por la línea telefónica. Este sistema de conexión cayó en desuso.

b) Línea digital

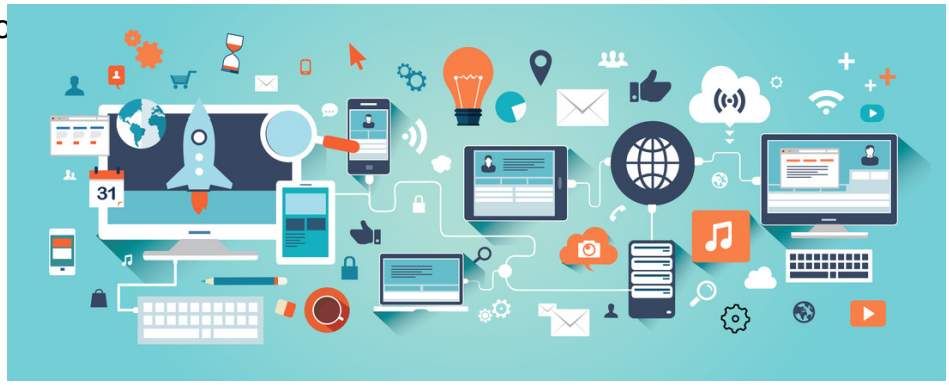
- RDSI: Se trata de una línea telefónica, pero digital (en vez de analógica).
- ADSL: La ADSL (Asymmetric Digital Subscriber Line) es una tecnología de acceso a Internet de banda. ancha y es el tipo de conexión favorito en hogares y empresas.

c) Cable

Desde el punto de vista físico, la red de fibra óptica precisa de una infraestructura nueva y costosa, lo que explica que aún hoy no esté disponible en todos los lugares.

d) Satélite

Este tipo de conexión sigue siendo utilizada en aquellos casos en los que no hay más opciones, por ejemplo en barcos, aviones o en zonas muy aisladas dónde no llega otro tipo de red o co



e) Redes inalámbricas

Las redes inalámbricas o Wireless difieren de todas las conexiones anteriores, y la más conocida y utilizada es la WI-FI.

Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Las redes Wi-Fi poseen una serie de ventajas, entre las que destaca la comodidad.

Pero, al igual que la red inalámbrica, la tecnología Wi-Fi presenta sus propios problemas intrínsecos. Algunas de estas desventajas son:

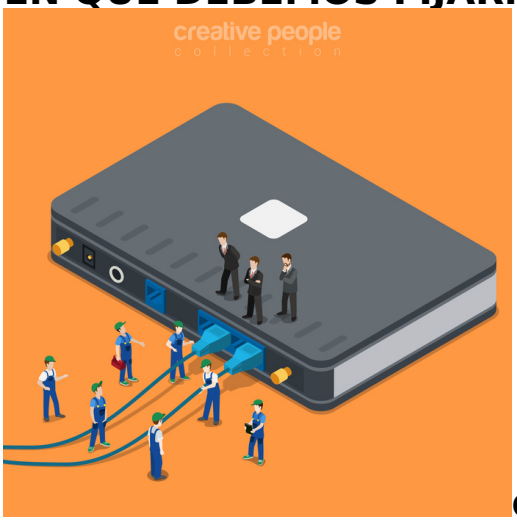
1. Falta de seguridad. Muchas de estas redes se convierten en redes abiertas, sin proteger la información que por ellas circulan.
2. Menor velocidad en comparación con una conexión por cable, debido a las interferencias.

f) Telefonía móvil

La conexión a Internet, dentro de la tecnología móvil, utiliza distintos sistemas derivados del GSM (Global System Mobile).

Para acceder a Internet tenemos que recurrir a proveedores, es decir, a compañías que crean una conexión directa y permanente y nos ofrecen la posibilidad de acceso contratando una cuenta a cambio de un pago por este servicio. Conviene, como en todos los contratos, leer atentamente las condiciones.

EN QUÉ DEBEMOS FIJARNOS AL CONTRATAR UNA CONEXIÓN A



Cobertura del lugar de la conexión

Ofertas hay muchas, pero es muy probable que, de no vivir en grandes ciudades, no podamos acceder a todas ellas.

Publicidad vinculante en las promociones

La publicidad es vinculante. Muchas veces, el precio final o la velocidad de conexión, no suele coincidir con lo anunciado.

Se puede exigir que nos cobren el precio anunciado en la publicidad.

No te fíes sólo de la publicidad y contrata sólo lo que necesites.

Que exista la posibilidad de contratar una mayor velocidad de conexión no implica tener la obligación de contratarla.

Infórmate si existe alguna cláusula de permanencia.

Servicio técnico

Es recomendable que compruebes en la medida de lo posible cómo funcionan los servicios de atención al cliente.

ASPECTOS ÉTICOS, LEGALES Y DE SEGURIDAD

Todos conocemos las ventajas de la red Internet, pero al ser una red abierta y universal, está sujeta a distintos riesgos relacionados con su propio funcionamiento y con el uso que de ella hacemos. En Internet debemos utilizar la lógica y el sentido

Al igual que ocurre en las actividades que realizamos en el mundo físico, todas las funcionalidades de Internet pueden comportar algún riesgo, entre los que podemos destacar:

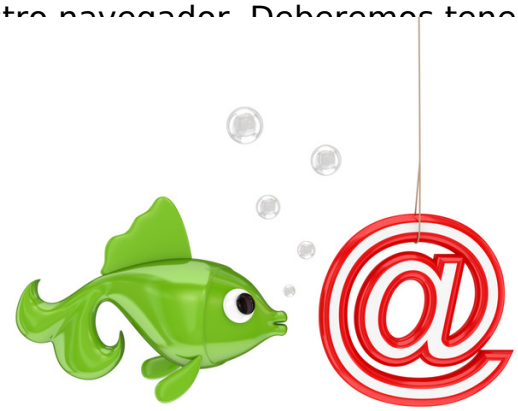
- Relacionados con su funcionamiento: Problemas con la accesibilidad, la conexión a determinadas webs o servicios de Internet, virus, spams, etc.
- Relacionados con la información: Existe mucha información poco fiable ya que cualquiera puede subir contenidos a la red.

- Acceso a información inapropiada: Información peligrosa (violencia, inmoral o ilícita) sobre todo para el colectivo menor de edad.
- Relacionados con la comunicación interpersonal: Bloqueo del correo electrónico, mensajes basura y ofensivos, pérdida de intimidad personal y de terceros, acciones ilegales como plagios, difamaciones, amenazas, etc.
- Relacionados con actividades económicas: Compras inducidas, publicidad, gasto telefónico desorbitado, estafas, robos o descargas ilegales.
- Relacionadas con la propiedad industrial e intelectual: pirateando una marca o los derechos de autor, cuando nos descargamos de manera ilícita música, un juego, un libro o una película.
- Relacionados con las adicciones: Existen riesgos relacionados con el abuso de determinadas prácticas como el juego, compras compulsivas, adicción a entornos sociales como chats, videojuegos online...

El **correo electrónico** también puede causarnos muchos problemas. Podemos vernos bombardeados por spam (publicidad no solicitada), ser engañados con falsas cadenas de solidaridad o diferentes métodos de estafa, así como recibir virus que afectan a nuestro ordenador. (Véase ficha Correo electrónico)

Elige un navegador seguro

La mayor parte de las actividades que desarrollamos por Internet se centran en nuestro navegador. Deberemos tener en cuenta también el nivel de seguridad que



Cuida la protección de tu equipo

Debemos tener instalado un antivirus en nuestro sistema operativo.

Comprueba la configuración de tus perfiles

Es importante revisar el grado de privacidad que has elegido para tu perfil en las redes sociales en las que participas. Si navegas desde un PC compartido, acuérdate de cerrar la sesión de todas tus cuentas de email o páginas en las que estés registrado cada vez que te conectas. Y, por supuesto, jamás compartas tus contraseñas ni perfiles. Si es preciso, cámbialas con frecuencia para evitar que alguien pueda utilizarlas.

Si compartes imágenes o información de otras personas a través de Internet, asegúrate de que esos datos o fotografías no vayan a perjudicar o molestar a su protagonista, ni estén invadiendo su privacidad o violando su intimidad.

No reenvíes cadenas

Nunca reenvíes a todos tus contactos las famosas cadenas, ya que con frecuencia contienen virus, incluso cuando procede de un contacto de confianza.

Recuerda que Internet «no olvida» fácilmente la información, expresiones o imágenes que tú o personas de tu entorno, empresas y páginas de todo tipo, cuelgan en la web sobre ti.

Solo amigos verdaderos

Antes de aceptar una petición de amistad o de agregar tú a alguien en cualquiera de las redes sociales, piensa si de verdad le conoces y no hay ningún inconveniente en que acceda a tus datos, a tu entorno y a tu vida íntima.

Publicar contenido personal

Este es uno de los mayores errores que se llevan a cabo, sobre todo en redes sociales. Exponer demasiado las actividades diarias y a tu familia es algo peligroso. Un ejemplo de mal uso de las redes sociales puede ser visto con mucha frecuencia en Instagram. Esta red tiene una herramienta llamada Stories. En ella, puedes publicar imágenes o vídeos de 15 segundos que muestran lo que estás haciendo en ese momento y queda a disposición de los usuarios de la red durante 24 horas.

Compartir información proveniente de otras personas

No debes divulgar imágenes, mensajes o testimonios de terceros sin que ellos lo permitan. Además, no debes compartir contenidos que puedan denigrar la imagen de alguien. El cyberbullying es una práctica considerada como acoso virtual.

Exponer la seguridad

Informaciones como datos bancarios, ubicación y compras de bienes no deben ser jamás compartidas en las redes sociales.

Hacer clic en todo lo que se ve

Sabemos que para realizar varias acciones en Internet necesitamos hacer clic en varios enlaces, y eso no es un problema. El verdadero error está en acceder a todos los enlaces que se sugieren, sin siquiera saber antes si son seguros. A pesar de que muchas personas conocidas sugieren que hagas clic en ciertos vínculos, no creas en todo lo que lees.

Protege tus datos personales

Antes de aceptar o rechazar la propuesta de utilización de tus datos personales para comunicaciones comerciales, piensa lo que supondrá para ti la avalancha de información de terceras empresas que vas a recibir.

REDES SOCIALES

Una red social es una página web o aplicación que sirve como herramienta de comunicación entre los usuarios que la utilizan. Principalmente se comparte información en formato de texto, imágenes y vídeos, aunque en los últimos años se ha visto un auge del formato en audio.

En España existen 29 millones de personas emplean de manera activa sus redes sociales según el Estudio sobre el uso de estas plataformas en España de The Social Media Family.

Las redes sociales se han convertido en una de las principales vías de comunicación e interacción de los jóvenes. En ocasiones, a causa de esto, se ven empobrecidas las relaciones sociales del día a día, digamos que como consecuencia del uso excesivo de estas redes sociales, las personas interactúan menos en el día a día. (Por ejemplo: vas a un restaurante con tu familia o amigos y comprobar que cada persona está consultando su teléfono sin hablar entre ellos).

Con el aumento del uso de las redes sociales han aparecido amenazas y riesgos debidos a la mala utilización de estas. Como personas consumidoras y usuarias de las redes sociales se deben adquirir hábitos para un uso responsable de las mismas. Hay aspectos que conviene tener muy claros: se debe respetar a todas las personas, no se debe publicar información personal de interés (localización, residencia, tu colegio o instituto, tus futuros viajes, etc).

En **primer lugar**, cuando una persona decide entrar a formar parte de una red

diversas situaciones conflictivas:

a) Para poder acceder a la red, es necesario aceptar las condiciones de uso de la página y la política de privacidad de la misma. Esta información no siempre es directamente visible y resulta necesario descargársela para poder acceder a ella. Sin embargo, es posible aceptarla señalando la opción de «acepto» sin necesidad de leerla. Esto es algo muy frecuente y puede suponer un riesgo ya que, al aceptar esas condiciones, estamos dando nuestro consentimiento al administrador de la página para que disponga de nuestros datos y nuestras imágenes.

b) En muchos formularios de registro se solicitan excesivos datos de carácter personal, como, por ejemplo, las creencias religiosas, la ideología política, la orientación sexual, etc. Habitualmente estos datos no se solicitan como «imprescindibles», y NO debemos facilitarlos.

c) La persona usuaria decide quién puede acceder a su perfil y ver sus datos personales. Es necesario, por seguridad, que solo aceptes en tus redes sociales a personas que conozcas y sean de tu entorno cercano. Debemos utilizar SIEMPRE un perfil privado para relacionarnos en una red social que solo permita a tus amigos/seguidores/subscriptores ver la información y publicaciones que haces.

Después de entrar a formar parte de la red, nos podemos encontrar con **nuevas situacione**s:

a) Muchos motores de búsqueda indagan en los contenidos.

b) Un gran número de páginas requieren la instalación de cookies para poder funcionar. Estos dispositivos, instalados en el disco duro del usuario, recogen información sobre los sitios web que se visitan y pueden obtener información sobre los gustos y preferencias del usuario para personalizar el contenido de su página y mostrarlo acorde a estos, con fines publicitarios cada vez que se accede a ella.

c) Si, por ejemplo, decidimos subir una foto personal a nuestro perfil en una red social, es posible que esa foto deje de pertenecernos solo a nosotros y a partir de ese momento los derechos sean compartidos con la entidad que la aloja, que puede emplearla para diversos fines.

Después de haber participado en una red social, cuando la persona usuaria se plantea dejar de pertenecer a ella, puede surgir una nueva dificultad. El riesgo principal en ese momento es la imposibilidad de llevar a cabo una baja efectiva. Aunque el perfil esté cerrado y no se pueda acceder a él, los datos de registro siguen estando a disposición de los responsables de la red social. La persona interesada debe saber que tiene derecho a obtener, sin dilación por parte del responsable del tratamiento, la supresión de los datos personales que le conciernan.

Una de las mayores preocupaciones que también surgen respecto al uso que los menores hacen de las redes sociales, es la posibilidad de que sean víctimas de algún tipo de acoso. Actualmente, cuando hablamos de acoso a través de la red, en función de los protagonistas de la situación, podemos diferenciar dos tipos de acoso: cyberbullying y grooming.

El **cyberbullying**, o acoso escolar a través de Internet, es un problema que se produce entre iguales o, en ocasiones, de alumnos hacia profesores.

Los grupos de WhatsApp se emplean en muchas ocasiones, como medio para insultar y desvalorizar a uno de los miembros. Siempre existió el bullying en los centros escolares, pero no tener que dar la cara para desvalorizar y hacer sufrir a una persona e

El **grooming**, o acoso sexual a través de Internet, viene dado por parte de un adulto, que actúa contra una persona menor con un fin sexual. La facilidad e inmediatez con la que, a día de hoy se comparten imágenes de nuestro día a día, puede ser un punto muy importante a tener en cuenta en este tema.

Ambos problemas no son nuevos y no surgen con las redes sociales, pero el anonimato, la rapidez y la sensación de inmunidad que proporcionan las comunicaciones a través de las redes sociales, han contribuido al agravamiento de este tipo de problemas.

TIPOS DE REDES SOCIALES

Hay redes sociales que reúnen a los usuarios sin tener en cuenta una temática concreta, redes sociales generalistas y otras que están especializadas en un interés o tema en común, redes sociales especializadas:

Redes sociales generalistas más conocidas y utilizadas son: WhatsApp, Facebook, Twitter, Instagram, TikTok, Snapchat, VKontakte.

Redes sociales especializadas: LinkedIn, InfoJobs, 21Buttons, Spotify, Pinterest, Flickr.

Abono de una contraprestación para los datos personales

Se trata de un contrato como el resto, pero en este caso en lugar de dinero como contraprestación, se paga con datos. La Directiva 2019/770 ha sido la primera norma en reconocer la posibilidad de que exista un contrato en el que el consumidor

pueda explotar sus datos personales y utilizarlos como moneda de cambio en el mercado digital [1].

Supone un importante avance para la protección de los consumidores, ya que se extienden los mecanismos de protección legalmente previstos a aquellos supuestos en los que el consumidor no ha de pagar un precio, pero ha de ceder sus datos personales.

Por ello, al existir una relación de consumo, el consumidor tiene la obligación de reclamar sus derechos.

[1] https://indret.com/wp-content/uploads/2021/10/1672.pdf

EN INTERNET, NO TE CREAS TODO LO QUE VES

Un uso responsable de Internet en un entorno escolar, familiar y social implica tener presentes las siguientes cuestiones:

Publicidad encubierta

Youtubers o influencers publicitan en sus medios digitales y redes sociales, a cambio de una contraprestación económica o en forma de productos (estrategia llamada product placement) dichos artículos o servicios. Por eso, conviene tener presentes que muchos de sus mensajes son simplemente reclamos publicitarios para sus seguidores.

Publicidad engañosa en Internet

Ver ficha compras seguras en internet.

Correos electrónicos fraudulentos

Con ellos intentan vendernos productos. Ver Ficha compras seguras en internet.

Con ellos intentan acceder a nuestros datos personales. Ver Ficha compras seguras en internet.

Smishing y Vishing

Dos de las nuevas estafas que se han detectado en los últimos tiempos, además de las señaladas en la ficha compras seguras en internet, son smishing y vishing.

Smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. -con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto[2].

Vishing es un tipo de fraude basado en la ingeniería social y en la suplantación de identidad. Se realiza a través de llamadas telefónicas, donde el atacante suplanta la identidad de una empresa, organización o incluso de una persona de confianza, con el fin de obtener información personal de sus víctimas. Primero, el atacante debe haber obtenido información confidencial sobre su víctima, como su nombre y apellidos, el correo, domicilio, parte de los datos de su tarjeta de crédito, etc. Esto lo obtiene gracias a otros ataques realizados sobre sus víctimas, como el phishing (Ver ficha compras seguras en internet). Una vez obtenida esta información, es el momento de realizar una llamada telefónica al cliente, haciéndose pasar por su banco, una empresa de mensajería o un servicio técnico para utilizar la información anterior y que su víctima confíe en él. Tras esto, tratará de obtener más información, conseguir que el usuario instale algún malware (software hostil e intrusivo, como un virus,etc.) en su equipo o realice algún tipo de pago.

[2] INCIBE

PARA SABER MÁS...

- INCIBE (Instituto Nacional de Ciberseguridad)
- OSI (Oficina de Seguridad del Internauta)
- AEPD (Agencia Española de Protección de Datos)
- Brigada de Investigación Tecnológica de la Policía
- Grupo de Delitos Telemáticos de la Guardia Civil
- Educlic: Riesgos en Internet
- Instituto Nacional de Tecnologías Educativas y Formación del Profesorado
- MSCBS

Materiales didácticos:

- Guía de uso seguro y responsable de Internet para profesionales de servicios de protección a la infancia

- Guía para la comunidad educativa de prevención y apoyo a las víctimas de ciberacoso en el contexto escolar
- SEDE EDUCACIÓN
- EDUCACIÓN Y FP
- Guía S.O.S. contra el Ciberbullying
- EDUCA TOLERANCIA
- INCIBE

Guía de actuación contra el ciberacoso:

- INJUVE. Guía de actuación contra el ciberacoso
- Internet segura
- AEPD
- Compra segura en INTERNET GUÍA PRÁCTICA
- Juguetes conectados
- Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado

Guías para un buen uso del móvil y las redes sociales

- Guía de actuación para prevenir y solucionar el abuso de los móviles
- Aprender a convivir con el móvil
- Guía para padres y educadores sobre el uso seguro de Internet, móviles y videojuegos
- Guía para jóvenes y adolescentes sobre buen uso de las tecnologías
- Guía de seguridad en redes sociales
- Servicio de atención a adicciones tecnológicas (Madrid) Agencia Española de Protección de datos
- Grupo de Delitos Telemáticos de la Guardia Civil
- Brigada Central de Investigación Tecnológica de la Policía
- Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF)
- Instituto Nacional de Ciberseguridad de España
- Cómo evitar la publicidad no deseada
- Ejerce tus derechos
- Guía de privacidad y seguridad en internet
- Tú decides en internet
- Observatorio de la infancia
- Guía para jóvenes y adolescentes sobre buen uso de las tecnologías