ASOCIACIÓN NACIONAL DE UNIVERSIDADES
E INSTITUCIONES DE EDUCACIÓN SUPERIOR

Dirección General de Administración
Dirección de Tecnologías de la Información y Comunicación

Seguridad de Internet

Contenido

Internet

Internet ha revolucionado muchos ámbitos y especialmente el de las comunicaciones de una manera radical hasta el punto de llegar a convertirse en un medio global de comunicación hoy día cotidiano en nuestras vidas. Lo utilizamos para casi todo, desde compartir un momento con un amigo enviando una foto a través de mensajería instantánea hasta pedir una pizza o comprar un televisor. Antes, si queríamos leer un periódico debíamos comprar una edición local en papel cuando abría el quiosco de prensa con las noticias del día anterior. Hoy, con un solo clic no solo podemos leer nuestro periódico local, sino también el periódico de cualquier parte del mundo, con una actualización permanente de contenidos.

Internet ha evolucionado muchísimo desde su creación, que es, sin embargo, muy reciente desde la perspectiva de la historia, y poco ha quedado de esa primera red estática concebida para transportar unos cuantos *bytes* o para enviar un pequeño mensaje entre dos terminales. Hoy cantidades infinitas de información son cargadas y descargadas en este gigante electrónico. Hasta hace no mucho tiempo internet era un simple repositorio de información donde solo aquellas personas capaces de entender y manipular código eran las encargadas de publicar y mantener contenidos; ahora todos somos partícipes fundamentales, teniendo la posibilidad de generar contenidos y comentar contenidos existentes.

¿Qué es Internet?

Internet es una gran red de ordenadores a nivel mundial, que pueden intercambiar información entre ellos. Se pueden comunicar porque están unidos a través de conexiones telefónicas, cable, ondas u otro tipo de tecnología y gracias a que utilizan un lenguaje o protocolo común el TCP/IP, que son unas normas que nos dicen como tienen que viajar los datos por la red.

¿Cómo funciona internet?

Todos los ordenadores conectados en internet tienen que utilizar el mismo protocolo o normas para comunicarse entre ellos, en caso contrario no podrían comunicarse e intercambiar información. Ahora veamos cómo se conectan y las normas "protocolos" que utilizan.

Imagina que ahora tenemos un ordenador y queremos conectarnos a esa gran red llamada Internet. Para conectarnos se hace por medio de un ISP (proveedor de acceso a internet), por ejemplo, Telmex, Izzi, TotalPlay, etc, es decir, empresas que nos facilitan la conexión. Tendremos que ponernos en contacto con uno de ellos y contratar el servicio para que nos conecten a internet.

El ISP o proveedor lo primero que hace es asignarnos un número único a nuestro ordenador dentro de la red para que cuando nuestro ordenador se conecta a la red este identificado. Este número será único en toda la red y se llama el **IP** de nuestro ordenador. No puede haber otro ordenador dentro de la red con el mismo IP. El IP es como el nombre, apellidos y dirección de nuestro ordenador dentro de la red. Estos número IP se llaman "**direcciones IP**".

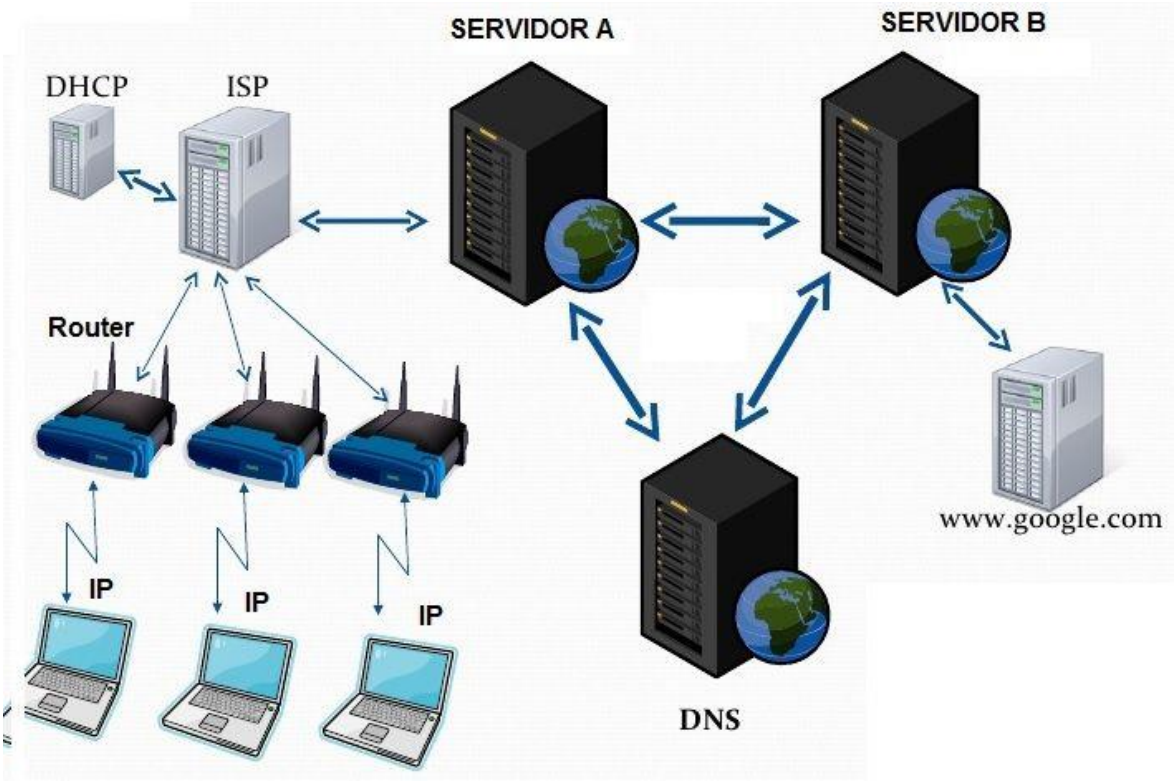
Si alguien quiere enviarte una carta a tu casa pondrá tu nombre y apellidos, el número de tu portal, el del piso en el que vives, el código postal, la ciudad, el país, etc. Es decir esos datos no puede tener los mismos nadie en el mundo, se podrá llamar igual, pero no tendrá el mismo código postal o no será de la misma ciudad. Cuando el cartero quiera llevarte la carta a tu casa no podrá confundirse porque no hay dos iguales. Tu dirección postal es única. Pues la IP de tu ordenador dentro de la red también debe ser única para que cuando quieras recibir o enviar información por la red no existan confusiones.

Gracias a ese **IP** único que tiene cada ordenador conectado a la red de internet se pueden identificar y comunicar los ordenadores unos con otros sin confusiones ni errores. Un ejemplo podría ser el siguiente número IP:

150.214.90.20

Además los datos que queremos enviar por la red, antes de enviarlos debemos codificarlos (convertirlos) de forma que sean datos que puedan viajar por los cables o por las ondas. Tenemos que convertir las señales digitales del ordenador en analógicas al enviarlos y viceversa al recibirlos. De esta forma puedan ser transmitidas por la red de forma inteligible. Esto lo hacía antiguamente un aparato que se llama modem (modulador/demodulador). Hoy en día se utilizan los **routers** que son más inteligentes, ya que además de hacer las funciones del modem, también es capaz de gestionar los datos que enviamos o recibimos (decide por donde irán, qué enviar y a donde).

Enrutamiento es el proceso de transmisión de paquetes de información de una red a otra. Un router es un dispositivo que codifica y descodifica los datos al entrar y salir de nuestro ordenador, une las redes y decide las rutas de tráfico de los datos entre ellas. Ahora veamos como hace todo esto.



Servicios que ofrece Internet

Internet nos ofrece infinidad de servicios y cada poco aparece uno nuevo. Veamos algunos de los principales servicios que ofrece.

- **Páginas Web**: son documentos de textos enriquecidos con multitud de formatos como texto, imagen, sonido, video, etc. La principal diferencia con los demás documentos es que pueden tener enlaces, vínculos o también llamados hipervínculos, es decir enlaces a otros sitios diferentes. Las páginas web tienen extensión .html porque están escritas en este lenguaje de programación.

- **Correo Electrónico**: este servicio permite enviar y/o recibir documentos de texto y multimedia (imagen, sonido, etc.). Hay que especificar la dirección del destinatario y del remitente y estas direcciones tienen este formato **correo@gmail.com.** La primera parte es el nombre del correo particular y la segunda (después de la arroba) es el servicio que lo envía, en este caso Gmail de google.

- **Transferencia de Archivos FTP**: Es un servicio que sirve para enviar archivos desde un ordenador a otro de manera rápida, sobre todo para subir páginas web.

- **Telefonía IP**: también llamado VoIp, voz sobre Ip. Permite tener una conversación por vía telefónica a través del ordenador. El más famoso es Skype.

- **Redes P2P**: permite comunicarse dos ordenadores directamente, uno de ellos cede el archivo y el otro el que lo recibe. La red más famosa P2P es el Emule con el que mucha gente baja películas, documentos, etc.

También gracias a internet tenemos mensajería instantánea, videoconferencias, redes sociales, etc.

Riesgos en internet

Pese a las infinitas posibilidades que ofrece Internet como infraestructura económica y cultural para facilitar muchas de las actividades humanas y contribuir a una mejor satisfacción de nuestras necesidades y a nuestro desarrollo personal, el uso de Internet también conlleva riesgos, especialmente para los niños, los adolescentes y las personas que tienen determinados problemas como tendencia al aislamiento social.

Las oportunidades que nos brinda Internet para facilitar muchas de las actividades humanas y contribuir al desarrollo personal de los usuarios son indiscutibles, pero también conlleva riesgos.

Todas las funcionalidades de Internet (navegación por las páginas web, publicación de blogs y webs, correo electrónico, mensajería instantánea, foros, chats, gestiones y comercio electrónico, entornos para el ocio) pueden comportar algún riesgo, al igual que ocurre en las actividades que realizamos en el «mundo físico».

Algunos de estos riesgos son:

Riesgos relacionados con la información.

Las personas frecuentemente necesitamos información para realizar nuestras actividades, y muchas veces la podemos obtener en Internet de manera más rápida, cómoda y económica que en el "mundo físico". No obstante hemos de considerar posibles riesgos:

- Acceso a información poco fiable y falsa. Existe mucha información errónea y poco actualizada en Internet, ya que cualquiera puede poner información en la red. Su utilización puede dar lugar a múltiples problemas: desde realizar mal un trabajo académico hasta arruinar una actuación empresarial.

- Dispersión, pérdida de tiempo. A veces se pierde mucho tiempo para localizar la información que se necesita. Es fácil perderse navegando por el inmenso mar informativo de Internet lleno de atractivos "cantos de sirena". Al final el trabajo principal puede quedar sin hacer.

- Acceso de los niños a información inapropiada y nociva. Existen webs

que pese a contener información científica, pueden resultar inapropiadas y hasta nocivas (pueden afectar a su desarrollo cognitivo y afectivo) para niños y menores por el modo en el que se abordan los temas o la crudeza de las imágenes (sexo, violencia, drogas, determinados relatos históricos y obras literarias…). La multimedialidad de Internet puede hacer estos contenidos aún más explícitos e impactantes.

- Acceso a información peligrosa, inmoral, ilícita. Existe información poco recomendable (pornografía infantil, violencia, todo tipo de sectas…) y hasta con contenidos considerados delictivos que incitan a la violencia, el racismo, la xenofobia, el terrorismo, la pedofilia, el consumo de drogas, participar en ritos satánicos y en sectas ilegales, realizar actos delictivos… La globalidad de Internet y las diferentes culturas y legislaciones de los países hacen posible la existencia (por lo menos temporal, ya que grupos especiales de la policía dedicados a *delitos informáticos* realiza actuaciones a nivel internacional) de estas páginas web en el ciberespacio

Los primeros riesgos se pueden paliar aprendiendo buenas técnicas para buscar la información y valorarla con juicio crítico, así como adquiriendo hábitos de trabajo en Internet que limiten la tendencia a la dispersión al buscar contenidos. En cuanto a los segundos, que afectan sobre todo a los más jóvenes, exigen una adecuada respuesta por parte de padres y educadores mediante la instalación de programas de protección en los ordenadores que limiten el acceso a determinadas páginas web y alertando a los niños y jóvenes sobre estos riesgos, explicándoles de manera adecuada a su edad las razones. Entendemos que los medios de comunicación social también deberían alertar a los ciudadanos en general sobre las páginas web con contenidos ilegales y sobre la conveniencia de denunciarlas.

Riesgos relacionados con la comunicación interpersonal.

Las personas muchas veces necesitamos comunicarnos con personas lejanas o establecer nuevos contactos sociales. Internet nos ofrece infinidad de canales y oportunidades (e-mail, chats, blogs…), aunque conllevan algunos riesgos:

- Bloqueo del buzón de correo. Hay personas que ignorando las normas de ***"netiquette"*** (pautas de comportamiento que facilitan la convivencia entre los

usuarios y el buen funcionamiento de la red) adjuntan grandes archivos a los correos sin pedir previamente autorización al receptor del mensaje, con lo que acaban bloqueando temporalmente su buzón de correo.

- Recepción de "mensajes basura". Ante la carencia de una legislación adecuada, por e-mail se reciben muchos mensajes de propaganda no deseada (spam) que envían indiscriminadamente empresas de todo el mundo. En ocasiones su contenido es de naturaleza sexual o proponen oscuros negocios. Otras veces pueden contener archivos con virus.

- Recepción de mensajes personales ofensivos. Al comunicarse en los foros virtuales, como los mensajes escritos (a menudo mal redactados y siempre privados del contacto visual y la interacción inmediata con el emisor) se prestan más a malentendidos que pueden resultar ofensivos para algunos de sus receptores, a veces se generan fuertes discusiones que incluyen insultos e incluso amenazas. Por otra parte, en ocasiones hay personas que son acosadas a través del e-mail con mensajes que atentan contra su intimidad.

- Pérdida de intimidad. En ocasiones, hasta de manera inconsciente al participar en los foros, se puede proporcionar información personal, familiar o de terceras personas a gente desconocida. Y esto siempre supone un peligro. También es frecuente hacerlo a través de los formularios de algunas páginas web que proporcionan determinados servicios gratuitos (buzones de e-mail, alojamiento de páginas web, música y otros recursos digitales...)

- Acciones ilegales. Proporcionar datos de terceras personas, difundir determinadas opiniones o contenidos, plagiar información, insultar, difamar o amenazar a través de los canales comunicativos de Internet... puede acarrear responsabilidades judiciales (como también ocurre en el "mundo físico").

Para paliar estos riesgos es conveniente informar sobre las normas de "netiquette" y educar a los usuarios en el uso correcto de los canales comunicativos de Internet, alertándoles del riesgo de difundir sus datos más personales y de las repercusiones legales que pueden tener sus mensajes y los archivos que se intercambian.

Riesgos relacionados con actividades con repercusión económica

El ciberespacio que sustenta Internet es un mundo paralelo en el que se pueden realizar prácticamente todas las actividades que realizamos en el "mundo físico". Y las actividades con repercusión económica siempre suponen riesgos. En el caso de Internet destacamos los siguientes:

- *Estafas*. En las compras y demás transacciones económicas (tiendas virtuales, bancos, servicios formativos...) que se realizan por Internet, especialmente si las empresas no son de solvencia reconocida, la virtualidad muchas veces enmascara sutiles engaños y estafas a los compradores.

- *Compras inducidas por una publicidad abusiva.* Aprovechando la escasa regulación de las actividades en Internet, las empresas utilizan sofisticados sistemas de marketing para seducir a los internautas e incitarles a la adquisición de sus productos, incluyendo publicidad subliminal. Sus anuncios de reclamo ("banners") aparecen en todo tipo de webs, y a veces resulta difícil separar los contenidos propios de la web de la publicidad. De manera que a veces se acaba haciendo compras innecesarias.

- *Compras por menores sin autorización paterna.* Niños y jóvenes pueden realizar compras sin control familiar a través de Internet, en ocasiones incluso utilizando las tarjetas de crédito de familiares o conocidos.

- *Robos.* Al facilitar información personal y los códigos secretos de las tarjetas de crédito por Internet, a veces son interceptados por ciberladrones y los utilizan para suplantar la personalidad de sus propietarios y realizar compras a su cargo. Con todo, se van desarrollando sistemas de seguridad (firmas electrónicas, certificados digitales...) que cada vez aseguran más la confidencialidad al enviar los datos personales necesarios para realizar las transacciones económicas. Hay empresas que delinquen vendiendo los datos personales de sus clientes a otras empresas y estafadores.

- *Actuaciones delictivas por violación de la propiedad intelectual*. Muchas personas, a veces incluso sin ser conscientes de ello o de la gravedad de su acción, realizan actos delictivos violando la propiedad intelectual a través de Internet: búsqueda y recepción de programas o música con copyright (piratería

musical) o software para desactivar sistemas de protección de los porductos digitales, difusión de estos materiales a personas conocidas...

- ***Realización de negocios ilegales*** a través de Internet: compra-ventas, subastas, préstamos, apuestas

Riesgos relacionados con el funcionamiento de la red Internet.

A veces por limitaciones tecnológicas, a veces por actos de sabotaje y piratería y que aún resultan incontrolables, la red Internet no siempre funciona como quisiéramos:

- ***Lentitud de accesos.*** A veces debido al tipo de conexión (modem...), otras veces debido a la saturación de algunos servidores en horas punta.
- ***Imposibilidad de conexión a una web o a un servicio de Internet***, que puede ser debida a problemas del servidor que da el servicio. Si esta circunstancia nos impide la realización de un trabajo importante, puede traernos muy malas consecuencias.
- ***Problemas de virus***, que actualmente se propagan con libertad por la red y pueden bloquear el funcionamiento del ordenador y destruir la información que almacena. Para navegar por Internet resulta imprescindible disponer de un sistema antivirus actualizado en el ordenador.
- ***Espionaje.*** A través de mecanismos como las "cookies" o de virus, se puede conocer todo lo que se hace desde un ordenador y copiar todos los archivos que tiene almacenados. Con estos sistemas algunos espías se dedican a detectar las circunstancias y preferencias de las personas con el fin de elaborar listas de posibles clientes que luego venden a las empresas comerciales.
- ***Publicidad subliminal, spam***...

En siglos anteriores las vías de comunicación entre las ciudades resultaban también lentas e inseguras (mal firme, guerras, bandidos...). Seguro que dentro de unos pocos años todos estos problemas de Internet también se habrán solucionado. De momento hay que conocerlos y tenerlos en cuenta: no podemos confiar que todo

Internet esté siempre operativo a nuestra disposición y debemos proteger nuestro ordenador con un sistema antivirus/espionaje adecuado.

Riesgos relacionados con las adicciones (IAD, Internet Addiction Disorder).

En toda adicción siempre confluyen tres elementos: una persona, unas circunstancias personales determinadas y una sustancia o situación que produzca placer (Internet puede proporcionar múltiples sensaciones placenteras).

Aunque la conexión compulsiva a Internet constituye un indicador significativo en los casos de IAD, no es posible establecer una correspondencia entre determinadas horas de conexión a Internet y adicción, pues el uso de Internet depende de las circunstancias personales de cada uno (algunos trabajadores y estudiantes deben estar conectados casi siempre a Internet). Incluso considerando solamente el tiempo de ocio que se emplea en Internet, resulta difícil establecer la frontera de la adicción basada en el número de horas diarias o semanales de conexión; como mundo alternativo al "mundo físico", Internet ofrece infinidad de ofertas de ocio: lecturas, música, películas, juegos, reuniones ("virtuales", esto sí, pero a veces incluso con sistemas de videochat) y cada persona puede tener sus preferencias.

Con todo, podemos considerar que una persona tiene adicción a Internet cuando de manera habitual es incapaz de controlar el tiempo que está conectado a Internet, relegando las obligaciones familiares, sociales y académicas/profesionales. Muchas veces además roban horas al sueño e incluso se reduce el tiempo de las comidas; de manera que el cansancio y la irritabilidad se irán cronificando, así como la debilidad del sistema inmunológico y muchas veces una cierta tendencia al aislamiento social.

Más que una adicción genérica a Internet, podemos considerar adicciones o usos compulsivos a determinados contenidos o servicios:

- *Adicción a buscar información* de todo tipo: noticias, webs temáticas, webs personales, servicios ofrecidos por empresas... Muchas veces incluye pornografía, imágenes o escenas que incluyen violencia... Se buscan sensaciones más que información.

- Adicción a frecuentar los entornos sociales: chats, MUDs… Los usuarios no dependientes tienen más tendencia a comunicarse con las personas conocidas. Los adictos buscan más conocer gente nueva y buscar el apoyo en los grupos de la red; a veces se crean varias personalidades virtuales.
- Juego compulsivo. Internet está lleno de webs con todo tipo de juegos, algunos de ellos tipo casino con apuestas en dinero; otros muy competitivos o violentos…, que pueden fomentar ludopatías en determinadas personas.
- Compras compulsivas: comercio electrónico, subastas…

Para superar estas adicciones que distorsionan la vida normal de los individuos, muchas veces será necesaria la ayuda de las personas próximas y hasta de médicos especialistas. En el caso de los menores, es importante que los padres estén atentos al uso que hacen sus hijos de Internet y vean de detectar estos problemas lo antes posible.

Recomendaciones para uso seguro en internet

Ante estos peligros potenciales, lo mejor es adoptar medidas preventivas para neutralizar los posibles riesgos de esta nueva y poderosa infraestructura cultural.

1. Asegúrate antes de comprar por Internet

Hoy en día, muchas de las compras que realizamos las hacemos a través de Internet. Es un método rápido y cómodo que permite conseguir buenos precios, comparar y comprar rápidamente. Sin embargo, cuando vamos a adquirir productos de manera online, debemos tener en cuenta algunas recomendaciones para navegar seguros por Internet.

Cuando compras online debes asegurarte de que estás en la página correcta y que la dirección comienza por *https*. También es importante revisar las llamadas *políticas de privacidad* de cada sitio web. Además, siempre es más conveniente utilizar cuentas en *PayPal* u otra alternativa como tarjetas prepago para proteger de esta forma los datos bancarios. Y, por supuesto, no te fíes de cualquier página o de cualquier vendedor.

2. Consigue un buen antivirus

Da igual cuál sea tu sistema operativo o el dispositivo desde el que estés accediendo. Cuando navegas por Internet es muy importante asegurarse de tener un antivirus seguro y actualizado. Con un buen antivirus evitarás que el malware entre en tus dispositivos, tanto ordenadores como móviles o *tablets*. De esta manera, podrás eludir cambios o la realización de acciones en tu nombre, así como que te roben información o comprometan tus aparatos. Recuerda que no sólo estás protegiendo tu identidad online, si no las de todas las personas de tu hogar o trabajo.

3. No confíes en las redes públicas

Como ya sabemos, cuando estamos fuera de casa utilizamos todas las redes que estén a nuestro alcance. La red *WiFi* de bares, tiendas y zonas públicas nos llama con la promesa de guardar nuestro limitado uso de tarifa de datos. Sin embargo, no solemos plantearnos la seguridad de alguna de esas redes y debemos crear mucha conciencia al respecto.

Ten cuidado con contraseñas o datos bancarios cuando estés conectado a redes públicas. Aunque muchas de ellas tienen seguridad propia, en otras los paquetes de información que contienen son presa fácil para hackers o ciberdelincuentes. Evita entrar en ese tipo de aplicaciones cuando estés conectado una red no segura.

4. Precaución con los email recibidos y los enlaces sospechosos

Es muy común que en nuestra bandeja de entrada encontremos emails de remitentes desconocidos. Muchos de ellos tienen asuntos que llaman la atención. Otros incluso se adaptan a nuestros gustos y preferencias. Sea como sea, no hay que fiarse de ellos. Nunca hay que pinchar en los enlaces o documentos adjuntos de mensajes desconocidos. Tampoco es recomendable responder a estos correos, ya que estaríamos facilitando datos personales, como nuestra dirección de correo, por ejemplo.

Por otro lado, cada vez está más entendida una práctica en al que algunas páginas, sobre todo para visualizar contenido audiovisual o descargar algún tipo de archivo, te confunden para que pinches en ciertos enlaces o te redireccionan

directamente a este mismo. Nos lo podemos encontrar navegando, en el email o incluso en redes sociales.

Debemos tener mucho cuidado con estas prácticas puesto que se puede tratar de virus informáticos que pretenden apropiarse de tus cuentas de redes, conseguir tus datos personales o apoderarse de tus sistemas informáticos. Lo más correcto en este caso es abandonar ciertos sitios webs que nos impongan estas acciones e ignorar los enlaces que tengan dudosa procedencia.

5. Vigila el conocido "internet de las cosas"

Aunque no nos damos cuenta, cada vez hay más cosas digitales e informáticas en nuestra vida. Esto se conoce como el internet de las cosas, un concepto que habla de la interconexión de los objetos cotidianos con el ser humano a través de la red. Robots de cocina que te informan de recetas, relojes que analizan tus sueños y actividad física o prendas de ropa que monitorizan tu calor corporal. Estos son algunos ejemplos de las aportaciones que pueden tener estos instrumentos en nuestra vida.

Sin embargo, es recomendable tener actualizados todos estos objetos, no sólo para que tengan una existencia más longeva, sino también por tu seguridad. El hecho de que estas herramientas diarias puedan transmitir información personal en tiempo real puede ser objetivo de ataques informáticos. Cambiar nombres de usuarios y modificar las contraseñas con frecuencia también puede ayudar a evitar robos de información.

6. Prevé ataques informáticos

Los ataques basados en el navegador se producen en su gran mayoría haciendo uso de *JavaScript*. Los desarrolladores utilizan este código para hacer más dinámicos los sitios web, pero en alguna ocasión puede generar problemas. Para prevenir del todo esto, lo más útil es desactivar *JavaScript*, lo cual es posible a través de *pluggins* o extensiones de los navegadores, y activarlo únicamente cuando estemos 100% seguros de que el sitio es de confianza.

7. Aumenta la seguridad de tus contraseñas

Al cabo del día accedemos a decenas de plataformas, redes y lugares que requieren del uso de contraseñas. Es de vital importancia que éstas sean fuertes y seguras para evitar el robo de datos personales y cuentas. Debemos alejarnos de la utilización de datos de fácil acceso, como la fecha de cumpleaños o números en serie. Es recomendable el uso de mayúsculas intercaladas, números o símbolos. Además, debemos cambiarlas con frecuencia.

Para asegurarse de ello es conveniente gestionarlas desde un solo sitio. Actualmente existen gestores de contraseñas que te ayudan a realizar dicha tarea. De este modo, con una única clave memorizada, podrás tener acceso a todas tus credenciales, cosa muy útil sobre todo para empresas, las cuales hacen uso de muchos más sitios donde se requiere un registro.

8. No des información de tu geolocalización

La geolocalización permite obtener la situación física de un objeto en un determinado momento. Los smartphones, conectados permanentemente a internet, permiten geolocalizarnos siempre que demos el permiso. Esto general un peligro importante, puesto que publicar nuestra posición en redes sociales o en internet puede ser un regalo para un delincuente cibernético. ¿Por qué? Porque puede saber exactamente dónde te encuentras tú o tus seres queridos en cada momento del día.

Debemos vigilar la geolocalización de nuestro teléfono inteligente, de la misma manera que la publicación de imágenes. Aceptemos o no la publicación de nuestra ubicación, si tenemos activada la geolocalización en el dispositivo que realiza la fotografía, se queda un rastro digital que difícilmente está oculto y que marca dónde y cuándo ha sido realizada. Es decir, si los piratas informáticos quieren averiguar tu

posición, lo harán. Es mejor prevenir y evitar la publicación de situación a través de fotografías, y más cuando se trata de viajes otros países o ciudades.

9. Cuidado con los ordenadores de uso público

Un error muy común es olvidarnos de cerrar sesión en nuestras cuentas cuando accedemos en ordenadores de uso público. Por ello, es muy recomendable activar la doble verificación en las plataformas que lo permitan. Ésta añade una capa adicional de verificación de personalidad que aumenta la seguridad de tus cuentas.

Por otro lado, debemos cuidar la conexión a algunas aplicaciones y servidores cuando estamos en ordenadores públicos: correo electrónico o servidores Google Drive, dónde no solo se transfiere información si no también imágenes, posicionamiento, historial, etc. Hay que tener en cuenta que toda esta información puede quedar almacenada en el ordenador, permitiendo el acceso a ella de cualquier persona que se conecte después.

Por todo ello, es muy recomendable utilizar el navegador de incógnito cuando accedemos a ordenadores o dispositivos de uso público.

10. Ten cabeza cuando uses redes sociales

Algo básico a la hora de navegar con seguridad por internet es tener cabeza a la hora de utilizar redes sociales. Ten mucho cuidado cuando publiques datos sobre dónde estás, con quién o durante cuánto tiempo. Y, por supuesto, nunca facilites información personal, ni siquiera en forma de fotos, sobre cuentas bancarias, contraseñas o datos comprometedores (como el colegio de tus hijos, por ejemplo).

Sistemas de seguridad e instrumentos de control.

- ***Cortafuegos*** (firewall). regula el tráfico de entrada y salida del ordenador con Internet. Admite filtros.
- ***Antivirus***. debe estar siempre activo y actualizado. Conviene que revise el correo de entrada y salida, analice disquetes y pendrives. Vigilar acciones

sospechosas de que sean originadas por virus. Hacer copias de seguridad de los programas y los archivos importantes.

- Utilizar ***programas legales***, Evitar descargas de archivos no solicitados o de sitios no seguros.
- Definir ***cuentas de usuario personalizadas*** para cada usuario del ordenador (panel de control-configuración)
- Poner como ***página de inicio*** un portal "seguro"
- Ajustar el ***nivel de seguridad del navegador***, indicando los sitios que queremos que sean sitios restringidos.
- Ajustar los ***filtros de contenidos del navegador***, restringiendo el acceso a contenidos no deseados.
- ***Uso de programas de protección.***
- ***Revisar de manera periódica el "historial"*** y los "archivos temporales" del navegador, para conocer las páginas que los menores han visitado

Referencias

Invitado, A. (2019, 4 febrero). 10 consejos para navegar seguro por internet. Recuperado 12 de junio de 2020, de https://www.blaucomunicacion.es/el-blog-de-blau/marketing-digital/navegar-seguro-por-internet/

Riesgos en Internet. (2017, 2 marzo). Recuperado 12 de junio de 2020, de http://www.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/riesgos/

areatecnologia.com. (s. f.). Como Funciona Internet y Explicado de Forma Clara. Recuperado 12 de junio de 2020, de https://www.areatecnologia.com/informatica/como-funciona-internet.html