INTERNET Y SUS RIESGOS

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: tendencia al aislamiento social, parados de larga duración...

En muy poco tiempo, las redes sociales se han instalado como uno de los hábitos más frecuentes de millones de usuarios en Internet. Es tal su popularidad que en la actualidad para la gran mayoría de internautas, una red social es el principal motivo para conectarse a Internet.

El hecho de que existan millones de usuarios en redes sociales compartiendo información al instante, puede tentar a que ciberdelincuentes desarrollen todo tipo de actividades fraudulentas en Internet. Los peligros existentes son muy variados con características particulares según el caso y no solo afectan a los usuarios desprevenidos sino que además pueden generar graves consecuencias para las empresas en las que estos trabajan, lo cual, genera la controversia sobre si se debe permitir o no el uso de redes sociales en entornos corporativos.

Entre los peligros más comunes presentes en redes sociales y que pueden afectar a las organizaciones, se destacan:

El Malware o códigos maliciosos: En vista de que hay tantos usuarios conectados al tiempo a estos servicios, la ocasión se presta para ejecutar códigos malignos que permitan propagar todo tipo de amenazas informáticas (Virus, gusanos, troyanos, spywares, adware, entre otros) ya que al lograr que un mensaje circule entre los usuarios enlazando a un archivo dañino, hará que un atacante alcance su objetivo. Un ejemplo de esto es el gusano koobface, una amenaza que se propagó masivamente durante el año 2009 y a la fecha sigue haciendo de las suyas, utilizando a Facebook como principal via de ataque, al enviar automáticamente mensajes a los contactos de los usuarios infectados con enlaces dañinos.

Privacidad y robo de identidad:

Cada vez es mayor la información que los usuarios comparten en redes sociales. No solo es el nombre, la edad o el sexo, sino que además es posible añadir datos de contacto, ubicación geográfica, fotografías, vídeos, entre otros. La exposición de la privacidad no solo es un riesgo asociado para los usuarios sino también para las empresas. Un ejemplo de ello es el de usuarios publicando situaciones laborales, problemas con compañeros o jefes, información de clientes, temáticas de reuniones, trabajos o proyectos y otros datos confidenciales de la empresa que expuestos, pueden afectar la integridad de la misma. De igual manera sucede con el robo de identidad donde el hecho de que un empleado pueda ser victima de este delito también representa un alto riesgo para la organización; por lo que evitar la exposición de información sensible es la principal medida de protección existente.

El Phishing es una de las principales amenazas en este campo, la cual consiste en el robo de información personal a través de la falsificación de un ente de confianza (en este caso la red social del usuario). La perdida de nuestro usuario y contraseña por ejemplo, puede ser el canal directo para que un delincuente acceda a nuestra información personal e incluso aquella que este configurada como privada.

Fuga de información y reputación para la empresa: Las redes sociales pueden afectar la reputación de una empresa y el habito de los usuario de publicar su acontecer laboral en estas, acrecienta los riesgos. La publicación de comentarios negativos sobre una marca o la distribución de material ilegitimo de una compañía, pueden circular por la web y representar altos costos para una empresa que no detecte a tiempo tales incidentes, afectando la imagen y reputación de la misma. Para enfrentar esta problemática las organizaciones deben contar con presencia en la web y tener

herramientas que permitan detectar este tipo de contenidos para tomar acciones cuando se considere necesario.

Las redes sociales en la empresa, ¿SI o NO?

Conforme a lo expuesto anteriormente si bien el creciente uso de las redes sociales supone que los usuarios desean ingresar a estos servicios desde los equipos de la empresa, lo cierto es que significa un riesgo potencial. Sin duda, permitir o no el uso de redes sociales en una organización es una de los grandes dilemas que acecha a gerentes y administradores de TI.

A medida que pasa el tiempo, normas conservadoras como prohibir el uso de redes sociales para el trabajo cada vez son menos aplicables, aún más si la marca necesita tener un contacto directo con sus clientes. No obstante, permitir su uso no implica tener que sufrir los peligros asociados, sino que es posible tomar medidas de seguridad para mitigarlos mientras se utilizan este tipo de recursos, como por ejemplo:

Utilizar Antivirus o herramientas de seguridad de protección contra códigos maliciosos para evitar infecciones de este tipo.

Definir políticas de seguridad en la organización, para prevenir incidentes referentes a la fuga de información o reputación de la empresa.

Desarrollar campañas de educación y concientización sobre los riesgos asociados y así evitar que los usuarios sean victimas de los diferentes ataques que se presentan en las redes sociales.

Con estas medidas, es posible hacer uso de estos servicios y disfrutar de sus beneficios, además de minimizar los riesgos de sufrir consecuencias negativas a partir del uso de las redes sociales en el ámbito corporativo.

En el caso de los niños, la falta de una adecuada atención por parte de los padres (que muchas veces están trabajando fuera de casa todo el día) les deja aún más vía libre para acceder sin control a la TV e Internet, si está disponible en el hogar, cuando vuelven de la escuela. Si el ordenador familiar no dispone de filtros que limiten el acceso a las páginas inadecuadas, de forma accidental o buscando nuevos amigos y estímulos se irán encontrando allí con toda clase de contenidos, servicios y personas, no siempre fiables ni convenientes para todas las edades. Y lo que empieza por curiosidad puede acabar en una adicción ya que los niños y los adolescentes son fácilmente seducibles. Por desgracia hay muchos padres que no son conscientes de estos peligros, que ya se daban en parte con la televisión y los videojuegos y que ahora se multiplican en Internet, cada vez más omnipresente y accesible a todos en las casas, escuelas, cibercafés...

Todas las funcionalidades de Internet (navegación por las páginas web, publicación de weblogs y webs, correo electrónico, mensajería instantánea, foros, chats, gestiones y comercio electrónico, entornos para el ocio...) pueden comportar algún riesgo, al igual como ocurre en las actividades que realizamos en el "mundo físico". destacamos los siguientes riesgos:

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 rapida, 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, weblogs...), 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 interaccción 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 informaicón, insultar, difamar o amenazar a través de los canales comunicativos

de Internet... puede acarrear responsabilidades judiciales (como también ocurre en el "mundo físico").

- Malas compañías. Especialmente en los chats, se puede entrar en contacto con personas que utilizan identidades falsas con oscuras intenciones, en ocasiones psicópatas que buscan víctimas para actos violentos o delictivos a las que prometen estímulos, experiencias y amistad.

Para paliar estos riesgos es conveniente informar 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. Nuevamente esta sensibilización resulta especialmente necesaria en el caso de los menores, que resultan mucho más vulnerables ante las personas que quieran aporvecharse de ellos..

- Riesgos relacionados con actividades con repercusión económica

(compras y gestiones, envío y recepción de archivos...). 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 dificil 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 mas 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...

- Gastos telefónicos desorbitados.

Si no se dispone de una conexión adecuada con tarifa plana que fije el coste mensual por uso de Internet, o el internauta entra de manera inconsciente en páginas (generalmente de contenido sexual) en las que al solicitar un servicio aparentemente gratuito le conectan a líneas telefónicas de alta tarifación, las facturas telefónicas pueden proporcionar serios disgustos.

Ante la gravedad de estos riesgos y la relativa novedad que supone Internet en nuestra sociedad para la mayor parte de los ciudadanos, entendemos que deberían hacerse campañas informativas a nivel nacional a través de todos los medios de comunicación, con una especial incidencia en los centros docentes. Al mismo tiempo deben seguir desarrollándose la legislación que regule el uso de Internet y las medidas policiales dirigidas a la captura de los delincuantes del ciberespacio.

- 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 dedida 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 amacenados. 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

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 dificil 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 si, 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...

Consejos. Diversas iniciativas institucionales, como "Internet Segura", han elaborado estudios y programas de sensibilización para promover el uso seguro de Internet contribuyendo a generar una cultura de responsabilidad que permita a los niños y adolescentes beneficiarse cada vez más de este nuevo medio al tiempo que se minimizan sus riesgos. Se considera que más allá de los filtros que puedan proporcionar ciertos programas de protección, se debe incidir sobre todo en la información y la educación de los menores, A partir de sus indicaciones a continuación se presentan unos consejos:

- Consejos prácticos a tener en cuenta por los padres y educadores (es necesario formar a los padres, que muchas veces no saben como funciona Internet ni sus riesgos, y deben asumir su deber de educar y negociar reglas sobre el uso de Internet en casa con sus hijos menores) :

- Conviene que los padres hablen con los centros educativos para asesorarse y conocer cómo se trata el tema en la escuela.

- En casa, colocar el ordenador a la vista de todo el mundo, en una dependencia familiar (salón, biblioteca) distinta del dormitorio de los niños.

- Hacer de Internet una actividad abierta y familiar, navegar juntos (sobre todo con los más pequeños) , saber con quienes se comunican y el tiempo que dedican . Muchas veces los hijos pueden enseñar mucho a sus padres.

- Hablar abiertamente con los menores sobre el uso de Internet, su utilidad y sus riesgos.

Enseñarles a navegar con seguridad: explicarles normas básicas de uso y aspectos legales a tener en cuenta (no dar datos personales...), que distingan contenidos no recomendables...

Que cumplan las normas de netiquete.

Fomentar una actitud crítica: no todo lo que se ve es cierto.

- Establecer reglas básicas de uso en casa y en el centro educativo: momento del día en el que se puede usar Internet y el móvil (no el clase ni en el cine...), tiempo, considerar los costes de determinados servicios... Tener en cuenta las posibilidades de acceso a Internet en la casa de amigos, cibercafés..

- Tener un cortafuegos (firewall) y un antivirus actualizado que proteja el ordenador de los virus y de los programas espía.

- Utilizar navegadores infantiles (que solo acceden a páginas adecuadas) o instalar programas protectores que filtren la información facilitando el acceso a sitios web seguros y controlando el tiempo de conexión.

- Si se detecta algún peligro, contactar con las autoridades o con instituciones como "Protegeles"

- Consejos para los niños y cibernautas en general (sobre Internet y teléfono móvil):

- Disponer en el ordenador de un antivirus y cortafuegos actualizado. Asegurarse de que el antivirus está activado.

- Pasar el antiviris a los nuevos disquetes o pendrive que se introduzcan en el ordenador (aunque sean de nuestors amigos)

- No divulgar información privada personal (contraseñas, teléfono, dirección del domicilio familiar, datos bancarios...) o de de personas conocidas por Internet.

- No enviar fotografías sin el permiso de los padres, podrían utilizarlas otras personas para violar nuestra intimidad.

- No comprar sin la supervisión de un adulto. Y ante instrucciones poco claras, NO seguir el proceso de compra.

- No contestar e-mails que tengan contenido ofensivo o resulten incómodos y cuidar de no molestar o ofender a otros en los mensajes por e-mail, SMS o chat. No fotografiar ni grabar a nadie sin su permiso... y menos aún distribuir luego su imagen sin autorización.

- No abrir mensajes cadena.

- Ante cualquier correo que nos infunda sospechas, lo mejor es borrarlo inmediatamente.

- No concertar encuentros con personas conocidas on-line o por el móvil, las personas que se conocen on-line pueden ser muy distintas a lo que parecen (en Internet a veces las personas ocultan su verdadera personalidad)

- Si se recibe o se en cuentra una información que resulte incómoda, comunicarlo a los padres.

- No abrir mensajes de desconocidos ni mensajes de los que se desconoce el contenido.

- desconfiar de correos que hagan grandes promesas.

- No bajar programas de procedencia desconocida; podrían tener virus e infectar el ordenador.

- No bajar ni ejecutar archivos adjuntos sin comprobar que el remitente es de confianza.

- Tras conectarse desde un lugar público (cibercafé, escuela...) siempre cerrar la conexión para evitar que otra persona pueda usurpar su personalidad.

- No perder de vista el móvil y el ordenador portátil, si se pierde, comunicarlo enseguida.

- Evitar delinquir distribuyendo a través de Internet materiales (música, imágenes, películas...) de los que no tengan permiso para ello.

- No usar el móvil en clase ni en el cine, tampoco cuando hacemos una actividad que requiere mucha atención: ir en bicicleta, cruzar calles con poca visibilidad...

- Atención a los costes del uso excesivo del móvil o Internet. Conocer el coste de los servicios que se utilicen.

- Sistemas de seguridad e instrumentos de control.

Informaicón sobre los virus actuales:

Antivirus, que debe estar siempre activo y actualizado (hoy en día suelen ser autoactualizables a través de Internet).

Conviene que revise el correo de entrada y salida, analice disquetes y pendrives.

Vigilar acciones sopechosas 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 colicitados 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 restingidos.

Ajustar los filtros de contenidos del navegador, restringiendo el acceso a contenidos como:< violencia, sexo...

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..

ALGUNAS HABILIDADES NECESARIAS PARA UTILIZAR INTERNET

Para poder aprovechar las posibilidades educativas de Internet, son necesarias unas habilidades básicas, algunas de las cuales requieren un largo período de aprendizaje que conviene empezar en la escuela a edad temprana. Además de una buena predisposición y capacidad para el autoaprendizaje, y de los imprescindibles conocimientos instrumentales sobre el sistema operativo (windows o mac) y los editores de textos, destacamos las siguientes habilidades y conocimientos:

- Saber utilizar (y configurar) las principales herramientas de Internet:: navegadores, correo electrónico , FTP, listas de distribución y grupos de noticias, charlas, videoconferencias, programas de navegación off-line...

- Saber "bajar" información de la Red: textos, imágenes, programas...

Redactar los mensajes de manera cuidada y repasarlos antes de enviarlos.

- Atención a las faltas de ortografía.

- Atención a lo que se escribe, asegurarse de que nadie pueda sentirse molesto al leerlo.

- Escribir siempre las frases en minúsculas. Las mayúsculas indican enfado, significan gritos

- Si no es necesario para la comprensión del mensaje, al responder mejor no enviar los textos de los mensajes anteriores (hacen crecer el tamaño de los envíos)

- No enviar ficheros adjuntos (si el destinatario no lo sabe o ya está de acuerdo en ello)

- Conocer las características básicas de los equipos e infraestructuras informáticas necesarias para acceder a Internet: ordenadores, módems, líneas telefónicas... También resultará útil conocer aspectos concretos del funcionamiento de las redes como las horas de menor tráfico y por lo tanto mayor velocidad en la línea telefónica o en determinados servidores, la existencia de "mirrors" (espejos locales de servidores internacionales) que sirven la información más rápidamente, etc.

- Saber aprovechar las fuentes informativas de Internet.

..... Diagnosticar cuando es necesaria una información. Definir lo que se necesita: ¿qué busco?, ¿para qué lo necesito?. Determinar la información que se precisa buscar e identificar los conceptos

clave relacionados y el área de conocimiento a la que pertenece. Acotar la búsqueda lo más posible.

..... Saber encontrar la información que se busca y recuperarla con agilidad: dónde lo busco?, ¿cómo?-

- Conocer el significado de una dirección URL: identificar el servidor..

- Conocer y saber utilizar los programas buscadores (motores de búsqueda y directorios, generales y temáticos), bibliotecas, bases de datos y webs especilizadas.

- Saber localizar listas de discusión, grupos de noticias, webs de grupos de interés relacionados con las temáticas que se estén indagando.

- Resistir la tentación a la dispersión al navegar por la red.

- Algunos trucos:

- Si salen muchos resultados: usar palabras más relevantes; usar frases en vez de palabras; usar mayúsculas cuando corresponda; usar más palabras-clave y relacionarlas con el operador

-Si salen pocos resultados: quitar palabras-clave (si había varias); comprobar la ortografía; usar sinónimos; traducir en inglés; quitar operadores desconocidos y utilizar operadores conocidos; usar solamente minúsculas

- Para ahorrar trabajo: grabar las páginas interesantes sin leerlas del todo y guardar las direcciones en "favoritos"

..... Evaluar la calidad de la información que se obtiene (fiabilidad, autenticidad, actualidad...) . Suele convenir contrastar los datos obtenidos en distintas webs. Algunos indicios de calidad son:

- El contenido, la valoración que podemos hacer a partir de nuestros conocimientos sobre el mismo (profundidad, actualidad, estructuración...)

- El autor (reputación, ver si tiene otros trabajos en Internet), si es posible contactar con él

- La institución a la que pertenece el autor.

- La entidad que acoge en su website esta web (ver también el dominio de la URL: comercial, sin ánimo de lucro...)

- Razón de ser de la página, ¿por qué fue creada? (propósito: informar, compartir, vender, persuadir...)

- Objetividad (si hay opiniones, que se diferencien de lo objetivo)

- La existencia de la fecha de creación y de última actualización

- Existencia de enlaces a otras páginas complementarias (ver su calidad, si están operativos...)

- La existencia de bibliografía, fuentes de información...

..... Evaluar la idoneidad de la información obtenida para ser utilizada en cada situación concreta, organizarla y utilizarla: ¿qué he encontrado de lo que buscaba?, ¿de qué nueva información dispongo?, ¿cómo la organizo?, ¿cómo la aplico a la resolución del problema?. No basta con encontrar información, hay que saber recopilarla, estructurarla y organizarla para luego, ya elaborada, recuperarla cuando convenga y aplicarla en la resolución de los problemas que se presentan.

- Saber aprovechar las posibilidades de comunicación que ofrece Internet (correo electrónico, listas de discusión, grupos de noticias...) en las actividades laborales, culturales y recreativas

- Evaluar la eficacia y eficiencia de la metodología empleada en la búsqueda de información y en la comunicación a través de Internet. Con esta revisión, se mejorarán progresivamente las técnicas y estrategias empleadas y cada vez se actuará con más eficacia y eficiencia.

- Organizar un entorno personal de direcciones interesantes del ciberespacio, a través de favoritos o de una página web personal.