USO SEGURO DE INTERNET

MEDIDAS A ADOPTAR POR LOS PADRES, RESPECTO DE SUS HIJOS

- Hay que establecer unas reglas de uso y sus consecuencias.
- Adaptar sus horarios escolares y de estudio a la utilización de ordenadores.
- Controlar los tiempos de uso.
- Enseñarles a no solicitar productos sin aprobación familiar.
- Ayudarles, en la medida de lo posible, a realizar sus trabajos, estudios, búsquedas, etc.
- Motivarlo para que realice sus propias búsquedas sobre temas de interés, tanto para sus trabajos escolares como para la propia familia.
- Comentarles los efectos perjudiciales y beneficiosos que causa la intimidad al hacer uso de la red.
- Hablarles de los peligros del chat, donde se pueden confundir, al "chatear", con supuestos amigos que no resultan tales, prestando especial atención a los contenidos sexuales.
- Controlar las facturas telefónicas.
- Establecer presupuestos para gastos en línea y supervisar que se cumplen.
- Hacer comprobaciones periódicas sobre el uso que los hijos hacen del ordenador y, sobre todo, de la red.
- Educar a los hijos sobre las consecuencias de romper las leyes.
- Dedicar especial atención a los juegos que los hijos suelen recibir, intercambiar o copiar. No todos son divertidos, los hay peligrosos y violentos.
- No se deben dejar convencer sobre las supuestas ventajas económicas que suponen las compras de copias ilegales de juegos, software, peliculas, etc.
- Intercambiar conocimientos con los hijos sobre novedades informáticas.
- Animar a los adolescentes que muestran un determinado interés por la informática a compartir esos conocimientos con otros hermanos, familiares, amigos, etc.
- Revisar los contenidos que puedan ser perjudiciales para su educación y desarrollo (temas pornográficos, violentos, racistas, etc.)
- Usar proveedores solventes.
- Valorar la posibilidad de instalar filtros y programas de control para acceso a determinadas actividades.
- Consulte las páginas especializadas en medidas de seguridad.

MEDIDAS A ADOPTAR POR LOS HIJOS

- Avisar, inmediatamente, a los adultos, si aprecias contenidos que puedas considerar peligrosos o, simplemente, si los ves raros.
- No des tus datos personales, si no estás seguro del destinatario o si consideras que no son necesarios.
- No envíes tus fotos o las de tu familia ni cualquier información sobre ellos, sin autorización de tus padres.

- No entres en páginas de contenidos no aptos para tu edad.
- Si vas a tener encuentros físicos con alguien que has conocido en la red, consúltalo, antes, con tus padres o tutores.
- No contestes a mensajes extraños; incluso, a los que te adjuntan ficheros que desconocen su orígen, obviando abrirlos.
- No accedas a zonas que solicitan dinero, números de tarjetas de crédito, inversiones, etc.

PRECAUCIONES EN TRANSACCIONES ECONOMICAS

- No abandonar las copias de los resguardos de compra en las proximidades de los Terminales de Punto de Venta (T.P.V.), pues contienen información sobre las tarjetas que puede ser utilizada tanto en Internet como fuera de red.
- No utilizar la tarjeta, si el establecimiento no merece su confianza. Se conocen casos en los que ese ha utilizado el número de la tarjeta y el nombre de su titular, por personal del propio establecimiento.
- No introducir el número de la tarjeta en páginas de contenido sexual o pornográfico, en los que se solicita como pretexto, para comprobar la mayoría de edad.
- No facilitar más datos personales de los necesarios.
- Al enviar información, compruebe que, en la parte inferior del navegador Explorer, aparece un candado amarillo o un candado cerrado, en el caso de Nestcape. Esto indica que sus datos viajan encriptados.
- Compruebe que los cargos recibidos se corresponden con los realizados.

PRECAUCIONES SOBRE EL CORREO ELECTRONICO.

- No abrir mensajes de correo, de origen desconocido. Eliminarlo, directamente.
- No ejecutar ningún archivo adjunto que venga con mensajes sugerentes.
- Adopte las medidas necesaria, cuando le ofrecen "regalos" sustanciosos y, para recibirlos, tiene que llamar por teléfono a prefijos 906.
- No facilitar la dirección electrónica con "demasiada" ligereza.
- Tenga activado, constantemente, un antivirus.
- Visite páginas especializadas sobre seguridad informática.
- Para que sus datos viajen seguros, envíe sus mensajes cifrados.

MEDIDAS DE SEGURIDAD PARA USUARIOS PARTICULARES.

- No facilitar datos personales si no existe una completa seguridad sobre quién los va a recibir.
- No facilitar más datos personales que los necesarios.
- Exigir, siempre, "conexiones seguras". Asegúrese que, al transmitir datos sensibles, en la parte inferior del navegador Explorer, aparece un candado amarillo y, en el caso de Nestcape, un candado cerrado.
- Comprobar los certificados de seguridad, en páginas que requieren datos

personales.
- Comprobar los certificados de seguridad, en páginas que requieren datos personales.
- Utilizar un buen producto antivirus y actualizarlo, frecuentemente.
- Extremar la precaución en los archivos que reciben en sesiones de chat.
- Actualizar los sistemas operativos y navegadores, con los parches que publican las firmas especializadas de software.

MEDIDAS A DOPTAR POR PEQUEÑAS EMPRESAS.

- Cambiar las contraseñas, periódicamente.
- Exigir contraseñas de calidad.
- No dejar las contraseñas guardadas en el disco duro.
- Confiar la gestión de la red a un responsable.
- Diseñar un protocolo del uso de la red.
- Controlar las operaciones y transaciones, en horario no habitual por ello.
- Establecer una política adecuada de copias de seguridad.

MEDIDAS A DOPTAR POR GRANDES EMPRESAS.

- Confíe la seguridad informática a un responsable cualificado.
- Control sobre personas externas a la empresa que, en determinadas ocasiones, tiene acceso a equipos informáticos por cuestiones de reparaciones, desarrollo, mantenimiento, etc.
- Actualización constante del software.
- Consultar con empresas especializadas del sector.

MEDIDAS PARA EVITAR FRAUDES TELEFÓNICOS

- Control de las facturas, para vigilar si el gasto facturado se corresponde con las comunicaciones realizadas.
- Comprobar los números de teléfonos a los que se ha llamado, para identificarlos como conocidos. Se dan casos de facturaciones de llamadas no realizadas por el interesado. En ese caso, antes de adoptar otras medidas, consulte a los usuarios.
- Ante posibles sustracciones, tenga precaución con la correspondencia procedente de bancos y operadoras telefónicas para que, en caso de no recibir información puntual sobre consumos, ponerlo en conocimiento de la compañía, solicitando un duplicado y advirtiendo de lo sucedido.
- No facilitar los números de teléfono, tanto fijo como móvil, a personas desconocidas que los soliciten, bajo cualquier pretexto, ya que se han detectado casos en los que, sólo, intentan conocer las características de las línea para posibles desviaciones.
- Ante una llamada telefónica equivocada, cortar la comunicación, rápidamente, para evitar el posible desvío de llamadas con cargo a la factura de la persona que recibe la llamada.
- En el caso de tener contratada la modalidad de "llamada a tres", extremar las

precauciones, ya que, con un programa informático, se puede rastrear la línea y producirse una intrusión a ella, para realizar llamadas internacionales, con cargo al titular del teléfono.

- No aceptar llamadas a cobro revertido si no se está absolutamente seguro de conocer a quien lo pide. Puede tratarse de una llamada fraudulenta y pagar gastos de miles de pesetas por el engaño