EL MÉDICO EN CASA

► por DR. ÁNGEL LUIS LAGUNA CARRERO

Especialidad Medicina Familiar y Comunitaria
Máster Medicina de Urgencias y Emergencias
Experto universitario en Nutrición y Dietética

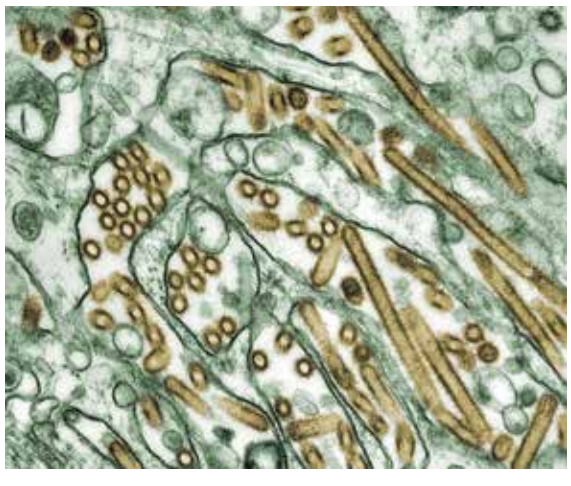
La gripe A

El virus de la gripe A, también conocido como influenza H1N1, es muy contagioso y puede propagarse durante todo el año, aunque en invierno es más común su extensión debido a las condiciones meteorológicas y porque permanecemos más tiempo en espacios cerrados, donde es más habitual relacionarnos en distancias cortas. En general, como forma de presentación es muy parecido a una gripe común, y afecta tanto a hombres como mujeres en muy parecida distribución. Estaremos más atentos a personas de edad avanzada, enfermos crónicos, diabéticos y mujeres embarazadas, porque son los grupos donde puede conllevar más riesgos y donde se recomienda tomar más precauciones para evitar el contagio.

En temporadas de invierno se hace más frecuente la presencia de todo tipo de virus. En concreto la gripe A se manifiesta por síntomas respiratorios y también en la práctica clínica se puede presentar por debilidad, malestar general, dolores articulares y síntomas digestivos como pueden ser diarrea y vómitos en algunos tipos de personas. A menudo, los síntomas pueden pasar desapercibidos, pero nos pondremos alerta al detectar que los síntomas se acompañan de fiebre, sobre todo si sube por encima de 39 ºC y si hay otros signos de gravedad como puede ser la dificultad respiratoria, pues el virus de la gripe afecta a nuestro sistema de defensas y en algunos casos una simple infección respiratoria puede llevar a desarrollar una neumonía.

Por regla general, para el tratamiento de la gripe se recomienda beber buena cantidad de líquidos para no deshidratarnos, y pueden ser necesarios medicamentos antitérmicos para bajar la temperatura (paracetamol, ibuprofeno) mientras no haya otras contraindicaciones o alergias. También puede ser adecuado tomar bebidas calientes y quedarse en casa, evitando las temperaturas más frías que resecan nuestras vías respiratorias y pueden empeorar la situación en enfermos con bronquitis. En ocasiones, cuando la temperatura no se regula bien y no cede la fiebre, es necesario consultar con el médico para una evaluación más completa y evitar que la enfermedad se desarrolle hacia complicaciones, que son más frecuentes en personas frágiles o enfermos. Tan solo en algunos de estos casos sería necesario la toma de antibióticos y es indicado que sean prescritos bajo supervisión médica, porque en caso contrario puede que éstos no sean efectivos.

Conviene tomar las medidas adecuadas para evitar el contagio y propagación de las distintas formas de gripe y COVID. Para ello se aconseja lavarse bien las manos cuando llegamos a casa o después de haber estado en contacto con otras personas, que pueden haber pasado la gripe y no haber presentado síntomas.



LA COLUMNA SANITARIA

► por TAMARA JIMÉNEZ CARO

Enfermera escolar y especialista de Pediatría
@tuenfermerainquieta

El corazón no solo es romanticismo

Febrero es conocido como "el mes del amor", pero… ¿qué pasa si esta vez le damos otro enfoque? Ocasión ideal para caer en la cuenta de que es el órgano que nos mantiene vivos.

Las enfermedades cardiovasculares son la principal causa de muerte en el mundo, según la Organización Mundial de la Salud, pero hay que saber que muchas de ellas se pueden prevenir con hábitos saludables.

¿Cómo conseguimos un corazón sano?

1. **Alimentación equilibrada:** la dieta mediterránea es una de las más recomendadas por sus beneficios para el corazón. Se basa en frutas, verduras, cereales integrales, legumbres, frutos secos, aceite de oliva y pescado azul. Además, es importante reducir el consumo de ultraprocesados, ricos en grasas trans, sal y azúcares añadidos.
2. **Ejercicio físico regular:** la actividad física fortalece el corazón y mejora la circulación. La OMS recomienda al menos 150 minutos de ejercicio aeróbico moderado a la semana. Caminar, nadar, bailar o practicar yoga son excelentes opciones.
3. **Manejo del estrés:** éste puede afectar la presión arterial y aumentar el riesgo de enfermedades cardíacas. Practicar técnicas de relajación como la meditación, el *mindfulness* o simplemente dedicar tiempo a actividades que te gusten puede marcar una gran diferencia.
4. **Evitar el tabaquismo:** fumar es uno de los factores de riesgo más importantes para las enfermedades cardiovasculares. Dejar de fumar mejora la salud del corazón, además de aportar beneficios inmediatos, como una mejor respiración y más energía.
5. **Dormir bien:** dormir menos de seis horas al día se ha asociado con un mayor riesgo de problemas cardíacos. Asegúrate de mantener una rutina de sueño saludable, evitando la exposición a pantallas al menos una hora antes de dormir.

Señales de alerta

— Dolor o presión en el pecho.
— Dificultad para respirar.
— Mareos, fatiga extrema o desmayos.
— Hinchazón en pies, tobillos o piernas.
— Latidos irregulares o palpitaciones.

Ante cualquiera de estos síntomas, debes acudir al médico de inmediato.

Un corazón sano, una vida plena

Este febrero, recuerda que cuidar el corazón va más allá de lo romántico: se trata de mantener hábitos que te permitan disfrutar plenamente de cada momento.

Tu corazón trabaja incansablemente por ti, ¿qué estás dispuesto a hacer por él?

LA VIDA EN DIGITAL

► por CARLOS GÓMEZ CACHO

Tecnólogo
www.gestoriatecnologica.es

Diez puntos clave para una vida digital segura

No me cansaré de recordar la necesidad de estar bien informados y formados acerca de la protección de nuestra vida digital. Puede haber mucho en juego, y a veces observando unas mínimas pautas podemos evitar males mayores. Vamos a ver diez aspectos que creo son los más importantes.

1. Seguridad en contraseñas y cuentas. Usar contraseñas fuertes: largas, únicas y combinadas. Habilitar la autenticación de dos factores: añadir una capa extra de seguridad en todas las cuentas, como una segunda llave. Evitar usar la misma contraseña para múltiples cuentas. Actualizar contraseñas regularmente y cambiarlas si existe sospecha de robo.

2. Protección de dispositivos. Mantener el *software* actualizado: instalar actualizaciones de sistemas operativos, navegadores y aplicaciones para corregir vulnerabilidades. Instalar antivirus y cortafuegos confiables: proteger tus dispositivos frente a virus, *malware* y *spyware*. Configurar cortafuegos en redes y dispositivos como los *routers* de nuestra wifi. Evitar conectar dispositivos USB desconocidos, ya que pueden contener *malware*.

3. Precauciones en correos electrónicos y mensajes. No abrir correos de remitentes desconocidos o sospechosos. No hacer clic en enlaces desconocidos o descargar archivos adjuntos sin verificar su autenticidad. Verificar la URL de sitios web antes de ingresar información personal o financiera. Ignorar mensajes urgentes o alarmantes que soliciten datos personales, incluso si parecen de empresas legítimas.

4. Gestión de datos personales. Evitar compartir información sensible por correo electrónico o mensajes. Configurar la privacidad de redes sociales para limitar la información visible al público. Minimizar la publicación de datos personales en línea, especialmente en redes sociales.

5. Transacciones financieras. Comprar solo en sitios web confiables y verificados: buscar el candado y el prefijo "https" en la barra de direcciones. Usar métodos de pago seguros: evitar transferencias directas y optar por plataformas de pago protegidas. Supervisar regularmente las cuentas bancarias para identificar transacciones sospechosas.

6. Precaución en redes públicas y conexiones. Evitar conectarse a redes wifi públicas para realizar transacciones o acceder a información sensible. Desactivar la opción de conexión automática a wifi en dispositivos móviles.

7. Concienciación. Desconfiar de ofertas demasiado buenas para ser verdad. Recomendar a familiares y compañeros sobre las prácticas básicas de ciberseguridad.

8. Respuesta ante incidentes. Reportar cualquier actividad sospechosa a las autoridades o a las plataformas correspondientes. Bloquear cuentas comprometidas inmediatamente. Cambiar contraseñas de todas las cuentas vinculadas en caso de *hackeo*. Realizar copias de seguridad periódicas de tus datos en dispositivos externos o en la nube.

9. Herramientas útiles. Gestores de contraseñas para almacenar contraseñas de manera segura. Extensiones de navegador que bloqueen sitios maliciosos y rastreadores.

10. Educación. Mantenerse informado sobre nuevas ciberamenazas y tácticas de estafadores. Asiste a talleres, seminarios web, cursos… siempre que sea posible. Utiliza recursos como el INCIBE.es o la OSI.es, así como medios de verificación de datos.