Domus automaticus,

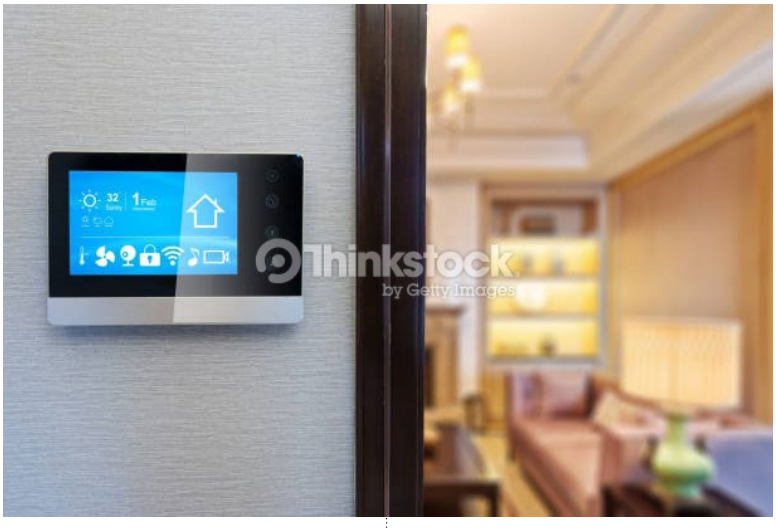
la casa del futuro ya es presente

En 1989, la segunda entrega de la mítica saga cinematográfica *Regreso al futuro* nos presentaba un modelo de casa en el que las puertas se abrían con botones, las ventanas se reemplazaban por proyecciones de paisajes, la comida se cocinaba en un "hidratador" y las llamadas se atendían desde las gafas o el televisor. Con bastantes matices, los escenarios que imaginábamos entonces a través de las aventuras de Marty McFly y Doc Emmett cada vez se parecen más a lo que vemos hoy en los hogares del siglo XXI, estructuras que han ido adoptando paulatinamente la automatización a su funcionamiento en un viaje sin retorno. Se abre por delante un universo de oportunidades pero también de riesgos a los que el sector asegurador debe dar respuesta.

TEXTO **JAVIER ORTEGA** | FOTOS **THINKSTOCK**

El concepto de domótica, formado por la unión de *domus* (casa en latín) y *tica*, del griego *automática* (que funciona por sí sola), se acuñó a comienzos de la década de los 70 cuando, a modo de proyecto piloto, aparecieron los primeros dispositivos *inteligentes* integrados en edificios. Casi 50 años después, los hogares digitales son una realidad y crece el número de viviendas conectadas en las que es factible mecanizar y optimizar tareas que tradicionalmente han dependido de la acción directa del hombre.

Las posibilidades parecen casi infinitas y, entre las opciones que ofrece la tecnología, las más valoradas son las relacionadas con el *internet de las cosas* (IoT, por sus siglas en inglés) y los sistemas de gestión que comunican todos los aparatos electrónicos del hogar. En la práctica, esto se traduce en un nuevo uso a través de *la red de redes* de objetos como cámaras o sensores que antes se conectaban solo mediante circuitos cerrados. Aunque de momento el IoT tiene más éxito en sectores como el de la salud o el control de infraestructuras urbanas, la irrupción de la etiqueta "inteligente" en los hogares está llegando con fuerza de la mano de una industria que ya la rentabilizó hace tiempo, la de los *smartphones*.



Inteligente, ecológico, y eficiente

Hace apenas unos años podría parecer ciencia ficción pero actualmente, gracias a diversas apps, desde un teléfono se puede vigilar con cámaras a nuestros bebés o el interior de una vivienda; controlar la temperatura del termómetro del horno en la cocina; encender y apagar bombillas, televisores o el aire acondicionado; o calcular si a las plantas les falta agua o abono y si la humedad, temperatura y luz son las adecuadas.

Frigoríficos que avisan cuando se van acabando los alimentos, robots de limpieza que se ponen manos a la obra en el momento en el que la casa está vacía, purificadores de aire que se activan si el ambiente se ha cargado con partículas nocivas... Aunque sigamos usándolos para hablar, los móviles van camino de convertirse en el mando a distancia universal y el catálogo de dispositivos que se pueden controlar desde ellos aumenta sin parar.

CASI 50 AÑOS DESPUÉS, LOS HOGARES DIGITALES SON UNA REALIDAD

En China, el país del mundo donde más electrodomésticos se producen, las principales marcas han apostado desde hace tiempo por productos y aplicaciones que se ajusten al trinomio inteligente, ecológico y eficiente. El siguiente paso es crecer en la interconexión entre los propios aparatos. Hablamos de un escenario que a algunos puede producir vértigo en el que, por ejemplo, la nevera envíe un mensaje al móvil de su propietario con los alimentos que este debe comprar para cumplir una dieta establecida a su vez por algún *gadget* que controle el estado físico en función de su colesterol. La interconectividad total, aunque tentadora, no será tan fácil de conseguir, porque para ello la mayoría de los fabricantes deberán llegar a acuerdos, compartir información y negociar estándares universales. En cualquier caso, este proceso será algo más lento, pero será.

Más oportunidades... y más riesgos

Según un estudio de la consultora estadounidense Gartner, en 2020 más de 20.000 millones de objetos estarán interconectados por todo el mundo. ¿Qué ocurriría si se *crackea* uno de estos sistemas y se accede a él con fines ilícitos?

Los piratas informáticos pusieron primero el ojo en los ordenadores personales; después los virus llegaron a la telefonía móvil y, de un tiempo a esta parte, se ha notado un incremento en los ataques a sistemas de control de vehículos. Las casas inteligentes están también en su punto de mira y ya hay muestras de ello. Por ejemplo, en Israel, un grupo de hackers denominados White Hat demostró la vulnerabilidad de las bombillas de última generación atacando el sistema de iluminación de edificios

públicos y viviendas. Fue tan sencillo como pasar con un coche (también podría hacerse con un dron) a menos de 70 metros de una de las bombillas que estaban entre sus objetivos. Eso les sirvió para infectar un primer dispositivo y "contagiar" en cadena al resto, tomando el control de la instalación lumínica y encendido y apagando las luces según su capricho.

En España, el año pasado el Instituto Nacional de Ciberseguridad contabilizó 115.000 ciberataques a empresas y particulares, un 130% más que los 50.000 registrados en 2015. Cualquier dispositivo conectado a internet puede ser víctima, por ejemplo, de un *ransomware,* el programa dañino que provocó un ciberataque global en mayo y que en junio volvió a afectar a empresas de todo el mundo. En viviendas, ya se han dado casos de televisores inteligentes infectados con este tipo de virus.

El papel del seguro

Evidentemente, las probabilidades de ataques crecen con la implementación de la tecnología en más y más parcelas de nuestra vida, pero eso no debe paralizarnos. Solo es cuestión de estar más atentos y protegernos mejor con las opciones que tenemos a nuestro alcance. Y en esto, el sector asegurador tiene mucho que decir.

5 ÁMBITOS PRINCIPALES DE APLICACIÓN DE LA DOMÓTICA

- Programación y ahorro energético
- Confort (gestión de la iluminación y de aparatos multimedia del hogar)
- Seguridad
- Comunicaciones
- Accesibilidad (aplicaciones o instalaciones de control remoto del entorno que favorecen la autonomía personal de personas con limitaciones funcionales o discapacidad)

Los seguros evolucionan también de la mano del IoT y el *big data*. MAPFRE, por ejemplo, dentro de su póliza de hogar, incluye desde hace tiempo asistencia informática para ordenadores, *smartphones* y tabletas y contempla también la instalación de sistemas de antivirus, copias de seguridad de los archivos del cliente o la restauración de datos y contenidos en caso de fallos. En esa línea es en la que se va a seguir profundizando y creciendo con el diseño de nuevos servicios a la medida de las necesidades del cliente.

Para Antonio Huertas, presidente de MAPFRE, las nuevas tecnologías están propiciando el desencadenamiento de una revolución "que puede tener un carácter transformacional para la industria aseguradora en un plazo de cinco a diez años". Lógicamente, esta transformación, como todas, entraña riesgos y oportunidades, "de la capacidad de las aseguradoras existentes en el mercado para saber minimizar los primeros y maximizar las segundas dependerá que sobrevivan o no a esta revolución y que lo hagan con éxito. Unos riesgos desaparecen, otros surgen y otros se transforman. Pero las personas nunca renunciarán a protegerse de lo inesperado".