



en tiempos en los que en las almazaras conviven la esencia ancestral con los avances en biotecnología de alta precisión.

De nuevo sobre el terreno, Raúl Mora, CEO de la almazara Palacio de los Olivos, en Almagro (Comunidad de Castilla-La Mancha), señala cómo la vigilancia de la temperatura ya empieza en el mismo olivar: «La aceituna en el árbol tiene la temperatura que marca la meteorología del día en que se recoge: unos grados más baja por la mañana que a mediodía, por lo que aprovechamos para recoger a primera hora. En cuanto se separa la aceituna del árbol, empiezan procesos naturales de oxidación y fermentación que hacen subir su temperatura, y esa subida continúa mientras la aceituna espera a ser molidura». Por ello, la oliva se empieza a procesar unos 20 minutos después de ser recogida, sin casi tiempo para calentarse.

Mejoras en calidad

«Ya en la almazara (continúa Mora), mantenemos ese frío refrigerando el exterior de la batidora, y controlamos tiempos y temperaturas en cada fase de la elaboración para garantizar que el proceso se mantenga siempre por debajo de los 27°C. Somos conscientes de que se producen menos litros por kilo de aceituna, pero el resultado es un aceite notablemente mejor, porque renunciamos conscientemente a rendimiento graso a cambio de más aroma, más sabor y más micronutrientes naturales».

Un ciclo integral 'del árbol a la botella', en el que las mejoras en el proceso de extracción frío suponen un 'dream team' de buenas noticias para el consumidor: «en aromas, en riqueza nutricional, en sabor, en estabilidad (resiste mejor

la oxidación y mantiene sus cualidades durante más tiempo) y en los resultados de los análisis físico-químicos».

En este proceso, los avances aplicados en el 'decanter' (o centrifugadora horizontal) son esenciales, ya que es el 'corazón tecnológico' de la almazara moderna, clave en la extracción en frío del AOVE. Su función principal es separar mecánicamente la fase líquida (aceite) de la masa sólida y acuosa de la aceituna mediante fuerza centrífuga, sin necesidad de aplicar calor elevado ni productos químicos. Instituciones como la Interprofesional del Aceite de Oliva Español, que aglutina al sector (compuesto por productores, almazaras, envasadores), destacan cómo la extracción en frío se utiliza como elemento de posicionamiento de marca e internacionalización, como señal de identidad, signo de distinción. Así ha sucedido en proyectos como Innolivar (desarrollo para trabajar en frío el fruto y la extracción del aceite), liderado por la Universidad de Córdoba y realizado por las empresas Itea y Calderería Manzano.

Tecnología nacional

En el caso de Palacín, con más de cien años de experiencia en el diseño, la fabricación y el mantenimiento de maquinaria industrial especializada en el sector oleícola, ha desarrollado su trayectoria (desde Úbeda, Jaén) acompañando la evolución tecnológica de las almazaras y contribuyendo a la modernización de sus procesos de producción (fundamentales, en este caso, para el denominado 'control crítico de la temperatura'). En 2025, la compañía dio un paso estratégico con el desarrollo de su propio 'decanter' (decanador), la Serie P, diseñado y fabricado íntegramente en España.

«El principal valor diferencial de nuestro 'decanter' Serie P (señala Mariana Martínez, gerente) es su capacidad de adaptación y personalización. Cada almazara tiene sus propias particularidades, condicionadas por las variedades de aceituna que trabaja, sus objetivos de producción y las características del aceite que quiere obtener. Por eso, no consideramos que la innovación deba consistir simplemente en fabricar una máquina estandarizada, sino en desarrollar una solución que pueda ajustarse a las necesidades reales de cada cliente».

Una opción, fabricada en España, «que supone reforzar la capacidad tecnológica de la industria oleícola para poder ofrecer a las almazaras una alternativa basada en la experiencia, la flexibilidad y la proximidad». Todo un ejemplo de innovación aplicada, en este caso en una actividad tan ligada a nuestra historia como la producción de aceite de oliva.

El ciberdelito llama siempre dos veces a la puerta del hogar conectado

Las contraseñas débiles, los dispositivos sin actualizar y la falta de protección de las redes domésticas convierten la domótica en un agujero para la privacidad y la seguridad

Charo Barroso

El debate sobre los hogares conectados suele girar en torno a si los dispositivos IoT (internet de las cosas) se han convertido en una alfombra roja para las ciberamenazas. «Más que una alfombra roja -dice Raúl Aguilera, vocal de Aeinse (Asociación Española de Ingenieros de Seguridad) y responsable de liderar el grupo de trabajo de ciberseguridad en sistemas de seguridad física de esta organización-, yo hablaría de una puerta adicional en una casa que antes tenía una sola. Una cámara, un panel de alarma, una cerradura inteligente o un detector de humo conectado están accesibles desde fuera de la vivienda. Es lo que los hace cómodos, porque permiten ver la casa desde el móvil o recibir un aviso estando de viaje, y también lo que los hace vulnerables, porque esa misma conexión permanece abierta de forma permanente y sin vigilancia».

El cibermalo no tiene objetivos concretos: rastrea internet de forma automatizada en busca de dispositivos mal configurados. «La inmensa mayoría de los incidentes domésticos no son ataques sofisticados, sino oportunidades aprovechadas», aclara Aguilera.

Los riesgos reales del hogar, advierte, son «menos espectaculares de lo que sugiere el cine, y en general más prosaicos y más frecuentes». El primero son las credenciales débiles, las que resultan fáciles de deducir. «Entran en esta categoría las que vienen de fábrica, pero también

las previsibles: secuencias como '123456', el apellido de la familia, la fecha de nacimiento, el nombre de la calle o la propia marca del dispositivo», detalla. A estos riesgos se añaden el software sin actualizar, la pérdida de privacidad, la inutilización del sistema, el uso del dispositivo como trampolín hacia otros equipos de la red doméstica y el compromiso de la cuenta en la nube.

Poner en el foco

¿Pero dónde hay que poner el foco de la defensa? Estima el experto que no todos los hogares necesitan lo mismo: «Quien vive en un piso con un sistema sencillo, por ejemplo una alarma, una cámara y algún detector conectado, no necesita una estrategia compleja». Bastaría con sustituir las contraseñas de fábrica por otras largas que no se puedan deducir y que sean distintas para cada dispositivo y cuenta, activar la verificación en dos pasos en las cuentas asociadas, mantener activadas las actualizaciones automáticas y no exponer los dispositivos directamente a internet con configuraciones improvisadas, y usar los servicios que ofrece el fabricante para el acceso remoto. La situación cambia en una vivienda con varios sistemas integrados. Propone entonces por «separar en la red los equipos de seguridad del resto de dispositivos del hogar».

Eso de que lo barato sale caro tiene especial relevancia en este ámbito. La duda, para el usuario, es si un dispositivo doméstico económico puede tener un blindaje digital solvente. Aguilera apunta que «el precio es un mal indicador de la seguridad de un dispositivo». «Lo que de verdad la determina es quién está detrás del producto y durante cuánto tiempo está dispuesto a responder por él. Hay equipos baratos de fabricantes serios que publican actualizaciones, obligan a cambiar la contraseña en el primer uso y mantienen su soporte durante años. También hay equipos caros, con una estética impe-



Los incidentes domésticos no son ataques sofisticados, sino oportunidades aprovechadas

▶ cable, que se abandonan al poco de salir al mercado», añade.

Como consejos prácticos, plantea que conviene fijarse en tres aspectos que pueden comprobarse en la tienda o en la web del fabricante: «Que la marca sea identificable y tenga presencia estable en el mercado, que indique por escrito durante cuántos años garantiza actualizaciones y que el producto obligue a establecer una contraseña propia al instalarlo».

Cambio normativo

La Unión Europea (UE) ha endurecido las obligaciones de los fabricantes a través del Reglamento de Ciberresiliencia (Cyber Resilience Act). Está previsto que el 11 de diciembre de 2027 empiecen a exigirse mayores responsabilidades en la gestión de vulnerabilidades, el suministro de actualizaciones y la información suministrada a los compradores.

«Salvo el tratamiento de datos, el problema que había con los dispositivos IOT era la falta de normativa clara. Esto va a cambiar con la Ley de Ciberresiliencia, que obliga a cumplir distintos requisitos en función de la categoría adjudicada. La mayoría de los dispositivos de bajo consumo, es decir, de consumo extendido van a ser de la categoría primera. Estos deberán acreditar en la descripción del producto el cumplimiento de unos requisitos», explica Pedro Peris, catedrático de Ciencias de la Computación e Inteligencia Artificial de la Universidad Carlos III de Madrid (UC3M).

Esta categoría de «no clasificados», de software general y productos de consumo conectados que no figuran en las categorías «importante» o «crítico» incluye aproximadamente el 90% de los artículos, entre ellos los dispositivos de domótica básica. Requieren una autoevaluación por parte del fabricante. A partir de la fecha marcada, si no hay moratoria, toda empresa que quiera vender productos en la UE tiene que cumplir con esta normativa, sea de la UE o extracomunitaria. «La ley —comenta el docente— va a garantizar que

La UE endurecerá a partir de diciembre de 2027 las obligaciones a los fabricantes de dispositivos

85%

Más del 80% de los sistemas atacados por cibercriminales estaban relacionados con dispositivos IOT del hogar

el tráfico de datos que hay, por ejemplo, entre dos dispositivos no esté cifrado, que se va a actualizar el software y el dispositivo durante cinco años al menos».

En cuanto a dispositivos en el hogar, distingue tres tipos: «Las cerraduras inteligentes y el hub o concentrador, que son críticos, porque dan acceso físico al domicilio y son la puerta de entrada a la red; los automatismos, todo lo vinculado con luces, termostatos inteligentes, porque tienen datos sensibles, porque con ellos se pueden conocer los hábitos de vida; y por último, las cámaras y altavoces inteligentes, porque capturan imágenes y sonido, y debemos saber si son seguros y si

los datos a los que acceden no salen». Coincide también Peris en la segmentación como solución, como protección ante los posibles ciberrataques: «Debería disponerse de una red para todos los dispositivos IOT y otra para el resto de las cosas. Los proveedores de internet nos dan en nuestro router una red de wifi privada y otra que llaman de invitados. Pues sería tan sencillo como utilizar todos los dispositivos de IOT en la red de invitados».

La educación en ciberseguridad es uno de los retos que Peris considera clave: «Lo tenemos todos, los Gobiernos, las empresas... la concienciación. No le podemos cargar con toda la responsabilidad al ciudadano porque no tenga conocimientos

to del peligro».

El Balance de Ciberseguridad 2022, del Instituto Nacional de Ciberseguridad (INCIBE), informa de 122.223 incidentes de ciberseguridad a lo largo de ese año. Asusta todavía más saber que el 85% de los sistemas atacados por cibercriminales estaban relacionados con dispositivos IoT del hogar, como televisores inteligentes, decodificadores o reproductores multimedia.

Una nueva era

ADT España, compañía dedicada a la seguridad electrónica y las alarmas, cifra en más de 20 los dispositivos conectados a internet en los hogares. Sus expertos afirman que «la seguridad residencial ha entrado en una nueva era y que el blindaje del hogar moderno debe ser, a la vez, físico y digital».

Apuestan por distintas soluciones como la detección de inhibición (tecnología que identifica el bloqueo de señal generado por un inhibidor entre los dispositivos y el panel de alarma: el sistema emite automáticamente una señal de alerta que se transmite a la Central Receptora de Alarmas, CRA); la seguridad multivía (funcionalidad que garantiza la continuidad de las comunicaciones con la CRA incluso cuando el atacante intenta neutralizar uno de los canales de transmisión); la supervisión de líneas mediante una comunicación permanente entre la CRA y el sistema de alarma para detectar si ha habido sabotaje o corte; y la tecnología Crash Signal, que permite que la CRA reciba la señal de alarma aunque el panel de control haya sido destruido por el intruso.