

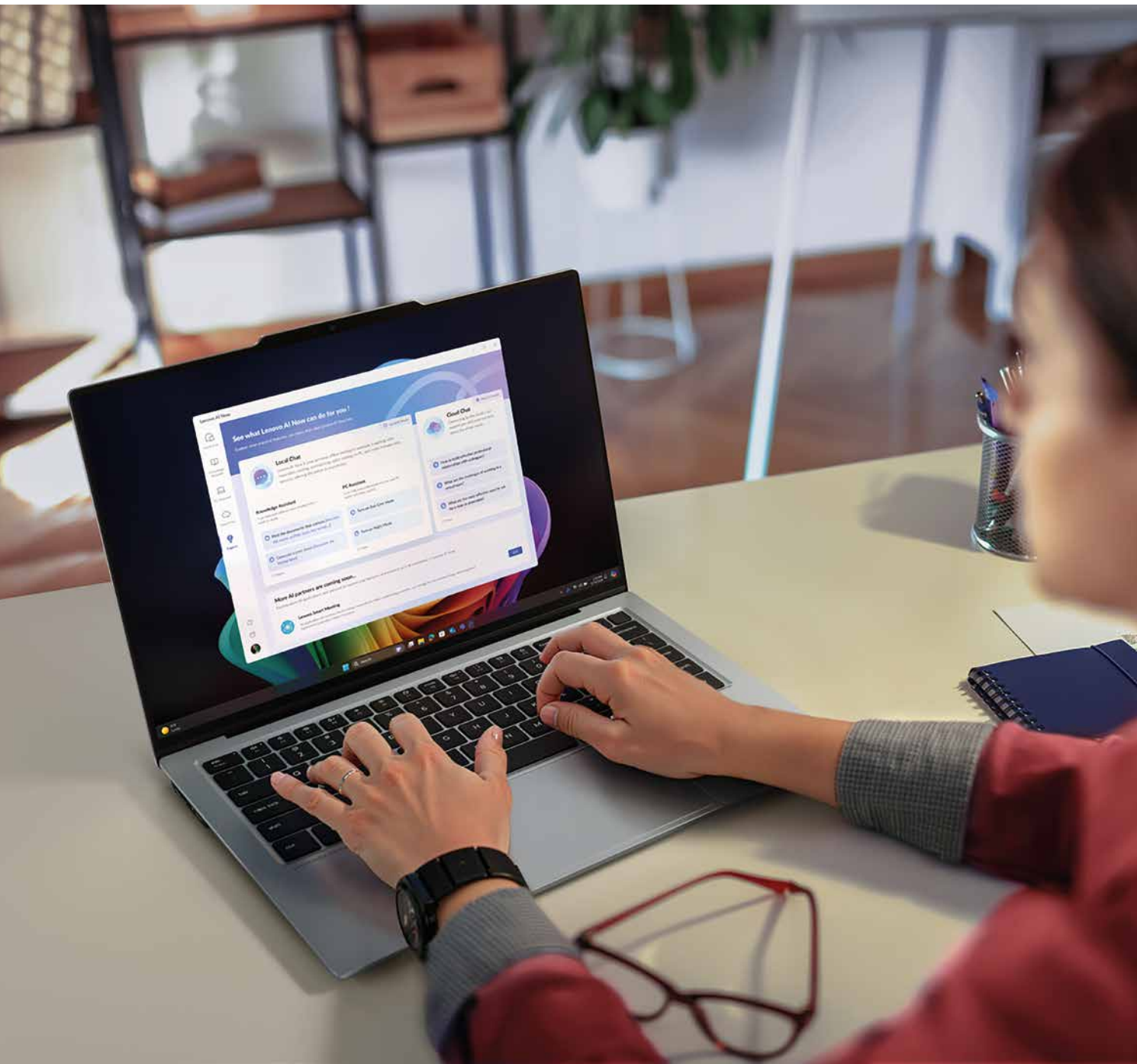


FOTO: LENOVO

Ciberseguridad en electrodomésticos y electrónica de consumo

LOS FABRICANTES SE VUELCAN EN LA SEGURIDAD

Los dispositivos que conforman el Internet de las Cosas son ya el principal objetivo para los ciberdelincuentes. Los fabricantes de electrodomésticos y electrónica de consumo son conscientes de ello y no dejan de trabajar para reforzar la seguridad de sus dispositivos.

El número de dispositivos del Internet de las Cosas (IoT, por sus siglas en inglés) está creciendo aceleradamente. Cuando arrancó la presente década, se calcula que había unos 9.760 millones de dispositivos IoT desplegados en todo el mundo, según los datos recabados por Statista. 10 años después, en 2030, se estima que la cifra se habrá duplicado sobradamente, sumando 32.100 millones de dispositivos. Y apenas tres años más tarde, aquella cifra se cuadruplicará, alcanzado unos 39.600 millones de dispositivos IoT en 2033.

Estos datos, que dan auténtico vértigo, son una clara muestra del auge del IoT, a medida que los usuarios van descubriendo las ventajas a las que pueden acceder gracias a la conectividad de infinidad de aparatos con los que conviven en su hogar, como electrodomésticos, altavoces, robots aspiradores, cámaras de vigilancia, termostatos, enchufes, bombillas, smartphones...

Sin embargo, esta hiperconectividad en la que vivimos también conlleva un aumento del perímetro de seguridad que se debe controlar para evitar ciberataques o brechas de datos.

Los ciberdelincuentes son conscientes de ello y tratan de explotar las vulnerabilidades de estos dispositivos. Por ejemplo, algunos expertos aseguran que los ordenadores han dejado de ser

FOTO: REALME



FOTO: HP

la principal puerta de entrada de los hackers a las empresas, accediendo a través de dispositivos como impresoras multifunción, máquinas de café o vending contactadas, teclados y ratones inalámbricos, televisores inteligentes, sensores, cámaras de videovigilancia e incluso ascensores.

Muchos de estos dispositivos también los tenemos en casa, con los riesgos que ello conlleva si los fabricantes y los propios usuarios no toman las precauciones oportunas.

En el caso de los usuarios, conviene cambiar las contraseñas predeterminadas, mantener al día las actualizaciones de seguridad o utilizar redes específicas para conectar estos aparatos, entre otras medidas.

Y los fabricantes deben incorporar la seguridad desde el diseño de sus productos, enviar los datos bajo cifrado y dar respuesta inmediata ante posibles brechas de seguridad, publicando los parches necesarios.

Así pues, como consecuencia de este auge del universo de dispositivos conectados, tanto en el ámbito empresarial como doméstico, el gasto en ciberseguridad del IoT se disparará en los próximos años. Según los datos de la consultora Juniper Research, los ingresos generados por el mercado

global de ciberseguridad del IoT en todo el mundo alcanzarán los 60.000 millones de dólares en 2029, lo que supone un crecimiento del 124% en el próximo lustro.

Respuesta de los fabricantes

Los fabricantes no descuidan la ciberseguridad de sus dispositivos y trabajan incesantemente para tratar de evitar que los hackers se salgan con la suya y pongan en riesgo a sus usuarios. Así se plantean la ciberseguridad las compañías del sector de los electrodomésticos y la electrónica de consumo.

Asus

“En Asus abordamos la ciberseguridad con un enfoque integral, desde el diseño hasta las actualizaciones periódicas. Nuestros dispositivos integran de base varias medidas de seguridad, como antivirus y tapas Shield para webcams que garantizan una mayor seguridad en el hogar y en el trabajo. Además, con la llegada del WiFi 7, se están incorporando nuevos protocolos de seguridad que refuerzan la protección contra posibles ciberataques. También mantenemos una actualización constante mediante MyASUS y Windows Update, lo que permite parchear de manera rápida cualquier vulnerabilidad que surja”,



FOTO: PANDO (INOXPAN)

detalla Antonio Torregrosa, Technical PR & Phone de Asus Spain.

Beko / Grundig

“En Grundig y Beko, la ciberseguridad es una prioridad; especialmente, dado el crecimiento exponencial de la conectividad en el mercado. Por ello, adoptamos un enfoque integral para asegurarnos de que nuestros dispositivos son seguros y protegen la privacidad de los usuarios. Desde la fase de diseño hasta la integración de ac-

ciones de concienciación y educación, pasando por controles periódicos, todo está medido al milímetro con la finalidad de evitar ciberataques, incluso en las primeras etapas de desarrollo. Esto atañe al uso de protocolos exigentes y la realización de auditorías internas para detectar posibles vulnerabilidades a lo largo de todo el proceso”, explica Manuel Royo, Director de Marketing de ambas marcas.

“Para complementar todas estas medidas técnicas, confiamos y contamos

con un equipo de profesionales especializados en materia de ciberseguridad y seguimos las mejores prácticas del sector”, añade.

Cecotec

Cecotec indica que la ciberseguridad es una prioridad esencial en el diseño y desarrollo de sus productos conectados a Internet. “Desde el inicio, incorporamos medidas y protocolos avanzados para asegurar la protección de nuestros usuarios y sus datos.

Al mismo tiempo, contamos con un riguroso programa de actualizaciones periódicas para nuestros dispositivos. Estas mejoras no solo sirven para optimizar sus funcionalidades, sino que también abordan cualquier vulnerabilidad que pueda surgir frente a nuevos ataques. De este modo, garantizamos que nuestros productos estén siempre a salvo de las últimas amenazas”, recalca la empresa.

Daikin

“La seguridad es una de las bases de nuestro diseño. Como empresa japonesa, nos gusta hacer productos fiables y seguros”, declara Marcos Casas, Adjunto a la Dirección de Servicio, Control, Monitorización y Energía de la compañía.

Además, remarca que la preocupación de Daikin en torno a la ciberseguridad va más allá. “Aunque lo abordamos desde el diseño, la seguridad que tenga que ver con el entorno de internet necesita actualizaciones periódicas que se vayan adaptando a las nuevas amenazas, por lo que es requisito indispensable contar con un programa que recoja y contemple que estas actualizaciones se adaptan al contexto actual y legislación vigente. Este programa garantiza la actualización de nuestros equipos compatibles de forma automática y remota”, agrega.

Elica

Giovanni Soggiu, Marketing Manager Iberia de Elica, señala que “el tema de la ciberseguridad es muy importante” para su firma. “Todos los softwares utilizados están protegidos y respetan to-

FOTO: DAIKIN



dos los requerimientos, para evitar que pueda pasar un fallo de seguridad”, comenta.

Además, indica que su equipo informático “está pendiente de las nuevas reglas y actualiza constantemente los programas y las plataformas según las mismas”.

Eurofred

“Nuestras aplicaciones cumplen con la normativa europea para asegurar la protección de los datos de los usuarios y que puedan disfrutar del conjunto de funciones sin exponerse a un riesgo externo”, precisa la compañía.

Asimismo, reseña que “el desafío de la ciberseguridad es un camino de esfuerzo continuo”, por lo que la empresa trabaja incesantemente para mejorar y adaptar sus sistemas a las nuevas normativas.

Honor

Jesús Domingues, Product Manager de Honor España y Portugal, reconoce que la ciberseguridad “es un tema

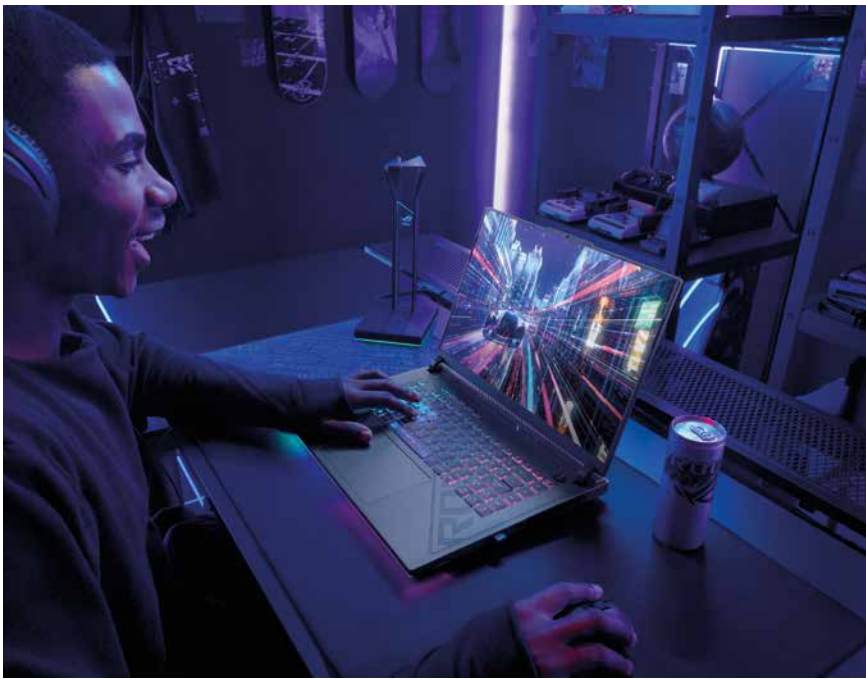


FOTO: ASUS

crucial e importante”. “Trabajamos siguiendo todas las regulaciones y normativas que son necesarias de cumplir y, adicionalmente, ofrecemos mecanismos de seguridad a través de la capa Magic OS, que permiten que la información de los usuarios siempre

se maneje de forma segura y sin poner en riesgo cualquier dato”, especifica.

HP

“HP adopta un enfoque integral de ciberseguridad para proteger a los usua-

FOTO: REALME



¿PREPARADOS PARA EL REGLAMENTO DE CIBERRESILIENCIA?

La Unión Europea aprobó el pasado mes de octubre el reglamento relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales, conocido como Reglamento de Ciberresiliencia o Cyber Resilience Act (CRA).

“El CRA es una legislación adoptada por la Unión Europea que establece un conjunto de reglas destinadas a fortalecer la ciberseguridad de productos y servicios conectados en el mercado único europeo. Es normal que, a medida que la conectividad se hace más latente, también lo haga la ciberseguridad. De aquí que estemos completamente comprometidos con la implementación de las directrices establecidas por la UE. Hemos reforzado nuestras prácticas de protección para asegurar que todos nuestros productos y servicios cumplen con los más altos estándares requisitos del reglamento”, declara Manuel Royo (Beko / Grundig).

Igualmente, Pablo Ugarte (HP) considera que “el nuevo CRA refuerza las bases de seguridad en productos digitales, por lo que representa un paso significativo hacia la creación de un entorno digital más seguro y confiable”. “Como compañía tecnológica, resaltamos la necesidad de este tipo de normativas para proteger a los consumidores y, a la vez, impulsar unos estándares de calidad y de ciberseguridad. Trabajamos para cumplir con los reglamentos establecidos y creemos que el diálogo entre sector privado, publicado y responsables de legislar fomenta crear un marco detallado que no deje de lado el impulso de la innovación”, añade.

Anaís Moreno también remarca el compromiso de LG con esta normativa. “Afecta directamente a nuestra forma de diseñar, producir y mantener nuestros productos conectados, ya que debemos asegurar que todos ellos sean más resilientes frente a los ciberataques y que contengan medidas más estrictas de protección. Para adaptarnos al CRA, además de los principios de seguridad desde el diseño y las actualizaciones, estamos fortaleciendo nuestros procesos de gestión de vulnerabilidades, alineándolos con los requisitos del CRA para garantizar una respuesta ágil ante cualquier riesgo identificado. Estamos trabajando estrechamente con las autoridades regulatorias para garantizar que nuestros productos cumplan con las normativas del CRA, realizando auditorías y obteniendo certificaciones de seguridad, como el CSMS de Nivel 3 para productos automotrices, que demuestran nuestro compromiso con la ciberseguridad”, detalla.

Asimismo, Juan José Marcilla de Teruel-Moctezuma (Lenovo) afirma que “el CRA tiene un impacto significativo en nuestra industria”, por lo que la compañía se está adaptando a sus exigencias. “Hemos revisado nuestras políticas y procedimientos de seguridad para asegurar su cumplimiento. Además, continuamos invirtiendo en tecnología avanzada y formación del personal para fortalecer aún más nuestra ciberresiliencia. Preferimos ver este tipo de reglamentos no como una obligación, sin más, sino como una oportunidad para mejorar”, comenta.

FOTO: ELICA



FOTO: HONOR

rios en un entorno digital cada vez más conectado. Este enfoque se centra en garantizar la seguridad desde el diseño, implementando actualizaciones regulares y ofreciendo soluciones avanzadas para mitigar riesgos”, expone Pablo Ugarte, Director del Negocio de Sistemas Personales de HP.

Por ejemplo, la compañía pone a disposición de sus clientes el servicio HP Wolf Security. “Es una seguridad de clase mundial para endpoints. Disponemos de un porfolio enfocado en seguridad reforzada por hardware y servicios de seguridad centrados en los endpoints y que está diseñado para ayudar a las organizaciones a proteger los PC, las impresoras y las personas de los ciberataques”, puntualiza.

iRobot

Vilma Otero, Directora de Marketing de iRobot España, hace hincapié en que iRobot “se toma muy en serio tanto la seguridad de los productos como la privacidad de los clientes”.

“Esta preocupación se traduce en un enfoque integral de la seguridad, a través de múltiples capas de protección para nuestros robots, la nube y las aplicaciones durante todo el proceso. Además, nos aseguramos de que el desarrollo de nuestros productos siga las mejores prácticas estándar del sector en materia de seguridad. De hecho, con los robots aspiradores Roomba j7 y Roomba j7+ nos convertimos en el

primer fabricante de IoT de consumo del mundo en obtener la Certificación de Ciberseguridad (CSC) de terceros de TUV SUD, un marco aún más estricto que va más allá del estándar del sector”, relata.

Lenovo

“La seguridad es un punto clave, especialmente con la IA”, remarca Juan José Marcilla de Teruel-Moctezuma, Commercial Product Manager de Lenovo España. Explica así algunas de las medidas desplegadas por la firma y las tecnologías empleadas para garantizar dicha seguridad. “El procesamiento local con la NPU mejora la privacidad. Destacamos la importancia de un ‘entorno de seguridad’, el cifrado de datos y un marco de IA responsable con procesos de gobernanza para asegurar la privacidad y la confianza del usuario. Algunos dispositivos, por ejemplo, incluyen características como reconocimiento facial con cámara infrarroja para mejorar la seguridad del acceso”, desgrana.

LG

“Abordamos la ciberseguridad con un enfoque integral y proactivo, aseguran-

do la protección de nuestros productos conectados a Internet desde el diseño inicial hasta las actualizaciones continuas frente a nuevas amenazas, ofreciendo una experiencia segura y confiable para nuestros usuarios”, declara Anaís Moreno, Marketing Manager de LG Electronics.

“Todos nuestros dispositivos conectados, tanto los televisores como los electrodomésticos inteligentes, se diseñan con principios de seguridad desde el inicio, siguiendo las mejores prácticas de ciberseguridad en cada etapa de su desarrollo, fabricación y lanzamiento. Por ejemplo, en nuestros televisores, incorporamos LG Shield, una capa de seguridad avanzada que protege nuestros dispositivos contra ciberataques, asegurando una experiencia segura al conectarse a Internet. Además, la actualización regular de los sistemas es fundamental para mantener la seguridad de nuestros productos. Nos aseguramos de que nuestros dispositivos reciban actualizaciones de software periódicas y puntuales, tanto para mejorar sus funciones como para corregir posibles vulnerabilidades de seguridad. Esta estrategia de actualización constante ayuda a mitigar los

riesgos asociados con nuevas amenazas cibernéticas”, subraya.

Pando

“Somos plenamente conscientes de los riesgos asociados a la conectividad a Internet y la importancia de garantizar la seguridad de nuestros productos. Por ello, abordamos la ciberseguridad desde el diseño mismo de nuestros dispositivos, implementando medidas de protección robustas para salvaguardar la información de nuestros usuarios. Además, mantenemos un compromiso constante con la seguridad, realizando actualizaciones periódicas y puntuales tanto de nuestra aplicación como de los productos conectados. Estas actualizaciones incluyen mejoras de seguridad y parches para abordar vulnerabilidades, lo que nos permite minimizar los riesgos de ciberataques y proteger los datos de nuestros usuarios en todo momento”, desgrana Ivon Soto, Communication & Digital Marketing Manager de Inoxpan, fabricante de la marca Pando.

Realme

“Nos tomamos la ciberseguridad muy en serio”, sentencia Jason Guo, CEO

FOTO: ELICA





FOTO: EZVIZ

de Realme Europa. “En la etapa de diseño del producto, adoptamos un enfoque de ‘seguridad desde el diseño’. Nuestros equipos de I+D siguen estrictos estándares de seguridad y mejores prácticas para garantizar que se minimicen las posibles vulnerabilidades. Durante el proceso de desarrollo, llevamos a cabo auditorías exhaustivas de seguridad y pruebas de penetración. En cuanto a las actualizaciones, proporcionamos parches de seguridad regulares y oportunos para abordar cualquier amenaza recientemente descubierta”, especifica.

“También contamos con un equipo dedicado a la seguridad que monitorea continuamente el panorama de la ciberseguridad y colabora con socios de la industria para mantenerse al día con las últimas tecnologías y tendencias de seguridad. Esto nos permite responder rápidamente a problemas de seguridad emergentes y proteger los datos y la privacidad de los usuarios”, añade.

Samsung

“La seguridad es uno de los aspectos diferenciales en cómo abordamos

la integración de la IA en Samsung”, destaca la compañía. “Gracias a la plataforma Samsung Knox Matrix, incluida en cada división de producto, podemos garantizar que los datos personales de los usuarios están protegidos de forma segura de extremo a extremo y en tiempo real ante posibles casos de piratería informática o ataques al hardware.

Esta seguridad y protección de la información privada o sensible también se extiende a Galaxy AI, SmartThings y todas las funciones basadas en IA en las que los usuarios confían para hacer más sencillo su día a día. De hecho, la próxima actualización de Samsung One UI 7 incorpora potentes actualizaciones a Knox Matrix para establecer las bases de la próxima generación de seguridad móvil”, indica la empresa.

“Knox Matrix utiliza una cadena de bloques privada llamada Trust Chain para supervisar dispositivos conectados de forma segura. Así, los usuarios pueden verificar fácilmente el estado de seguridad de sus dispositivos Samsung. Knox Matrix Credential Sync también gestiona y protege identidades y credenciales en forma de claves de acceso o passkeys, con el fin de minimizar las brechas de seguridad durante la autenticación de los dispositivos y hacer

FOTO: LG



que el proceso de inicio de sesión sea más cómodo”, expone.

Además, reseña que “dado que una gran mayoría de servicios requieren que los datos se procesen en servidores en la nube, Samsung Knox también incorpora un nuevo método de recuperación que añade facilidad y comodidad al proceso de proteger y recuperar los datos almacenados en Samsung Cloud”. “De esta manera, si se pierde el acceso a un dispositivo de confianza, los usuarios disponen de una copia de seguridad para evitar la pérdida y de la seguridad necesaria para transferir sus datos privados a un nuevo dispositivo simplemente verificando la contraseña de pantalla de bloqueo del dispositivo anterior”, aclara.

TCL

La compañía indica que todos sus productos “cumplen con la normativa vigente, en conformidad con la regulación europea”, garantizado así que



FOTO: SAMSUNG

“estén diseñados y operen bajo los estándares de seguridad”.

Además, explica que periódicamente se realizan actualizaciones online de software a lo largo de la vida útil de sus productos, con los parches de seguridad proporcionados por Google, “lo que permite garantizar que todos nuestros dispositivos se mantengan al día en cuanto a la protección frente a ciberataques”.

Asimismo, la compañía recalca que se asegura de que todos sus dispositivos cuenten con las últimas mejoras para combatir vulnerabilidades, no solo en cuanto al software sino también en cuanto al hardware. Igualmente, señala que se compromete a “garantizar un marco de ciberseguridad que se alinee con el Reglamento General de Protección de Datos (RGPD).

¡Escribir a mano los valores de la presión es cosa del pasado!

1 Descarga la aplicación «beurer HealthManager Pro».

2 Abre la función «Scan & Save» en la aplicación y escanea los valores medidos.

3 Los valores medidos se guardan automáticamente en la aplicación «beurer HealthManager Pro».

