Amenazas en el mundo digital: el futuro de la ciberseguridad

Bienvenida - De la ciberseguridad a la ciberinteligencia

La jornada comenzó con la intervención de Susana Rubio, vicepresidenta de Productos y Soluciones de Mastercard en España y Portugal, y Alberto López, vicepresidente de Fraude y Crimen Financiero de Mastercard en Europa, quienes pusieron el foco en la evolución del riesgo digital y en la necesidad de pasar de la defensa reactiva a la anticipación inteligente.

Abrió el encuentro Susana Rubio destacando el propósito de la sesión: “hablar de ciberseguridad, de las amenazas que crecen en este nuevo ecosistema digital y de cómo las nuevas tecnologías las hacen cada vez más sofisticadas”. Para dimensionar el problema, recordó que “el coste asociado al cibercrimen ascenderá a 15,3 trillones de dólares en 2029”. Una cifra que, según señaló, también tiene reflejo en el ámbito nacional: España es el quinto país europeo que más amenazas recibe, con el sector financiero

entre los más afectados, según el estudio elaborado junto a Recorded Future que serviría de base para el vídeo y el debate posterior. Por su parte, Alberto López reforzó esa idea con una advertencia: “Ya no basta con protegernos, hay que anticiparse”. Recordó que el 67 % de las empresas españolas ha sufrido al menos un incidente crítico de seguridad, lo que multiplica por tres el riesgo de sufrir un ataque o un ransomware, y por doce si se incurre en negligencia. Por ello, insistió en que las organizaciones deben evolucionar desde una postura reactiva hacia una estrategia proactiva basada en ciberinteligencia. “Como en el ajedrez —explicó—, no basta con responder al movimiento del contrario: hay que prever la siguiente jugada”.

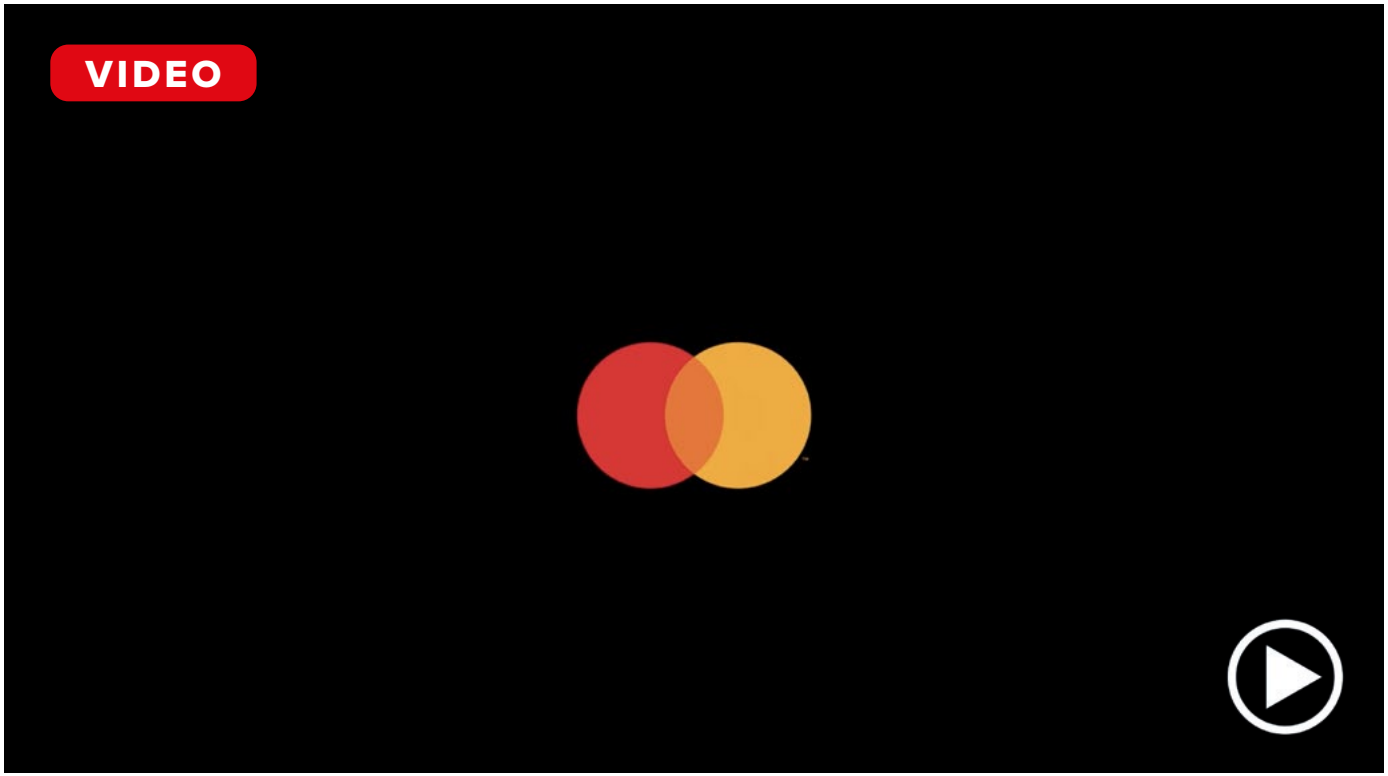
Susana Rubio completó esta visión recordando que la protección debe extenderse también a la cadena de suministro. Citó ejemplos recientes en los que ataques a proveedores afectaron a infraestructuras críticas y destacó la utilidad de RiskRecon, la solución de Mastercard que permite evaluar la fortaleza de los sistemas y la exposición derivada de las conexiones con terceros.

Como cierre, Alberto López trazó un recorrido por la evolución natural de Mastercard hacia la ciberresiliencia, impulsada por la inversión de 11.000 millones de dólares en ciberseguridad, incluyendo la adquisición de empresas de seguridad en los últimos cinco años, que sitúan a la compañía como la segunda del mundo que más invierte en ciberseguridad, solo por detrás de Cisco.

“Hoy somos mucho más que una red de pagos”, concluyó. “Todo lo que aplicamos para proteger nuestra propia red queremos hacerlo extensivo a nuestros clientes. Nuestra ambición es combinar ciberseguridad, ciberinteligencia y ciberresiliencia para garantizar la continuidad del negocio y la confianza en el ecosistema digital”, aseguró el directivo.

Radiografía del cibercrimen en España

Tras la bienvenida, los asistentes pudieron ver el vídeo "España en la diana: radiografía del cibercrimen 2024–2025", donde se recogen los principales datos de un informe elaborado por Mastercard y Recorded Future que analiza la evolución del cibercrimen en España y las tendencias que están marcando el futuro inmediato de la ciberseguridad.



Antes de iniciarse un diálogo con Alberto López y Recorded Future, se dejó claro que el vídeo refleja los desafíos que hoy nos ocupan: cómo transformar el riesgo en inteligencia y la información en resiliencia.

Tres pilares: inversión, inteligencia y colaboración

Alberto López calificó los datos como "escalofriantes, pero reales" y explicó que el auge del tráfico automatizado en Internet —donde "un tercio de los bots son maliciosos"— obliga a replantear las estrategias de defensa. Según detalló, Mastercard articula su respuesta en tres ejes fundamentales:

1. Inversión continua en innovación y adquisición de talento tecnológico.
2. Ciberinteligencia proactiva, capaz de anticipar riesgos, detectar la presencia de la marca en la dark web y prever posibles campañas dirigidas.

3. Colaboración e intercambio de información, dentro y fuera de la compañía, para fortalecer el ecosistema de seguridad.

“Tenemos que usar la IA para defendernos”, subrayó el directivo, añadiendo un mensaje final: “El aprendizaje es constante. No podemos parar de aprender”.

Recorded Future: amenazas persistentes y nuevas prioridades

Por su parte, Anna Angulo, Intelligence Consultant & Technical Lead de Recorded Future identificó las tres grandes frentes de riesgo que las organizaciones deben reforzar a partir de los datos del estudio:

- Proveedores externos y cadena de suministro, uno de los vectores más críticos y difíciles de controlar.
- Concienciación y cultura de seguridad, que debe llegar “a todos los niveles de la organización”.
- Uso responsable y defensivo de la IA, aprovechando las mismas herramientas que emplean los atacantes.

“La buena noticia es que las prácticas clásicas siguen funcionando, pero hay que potenciarlas”, afirmó, señalando que la inteligencia y el threat profiling son claves para priorizar recursos y focalizar esfuerzos ante la escasez de talento en ciberseguridad.

Regulación, resiliencia y geopolítica

Alberto López, al ser preguntado por el impacto de las nuevas normativas, destacó el papel positivo de NIS2 y DORA, que han logrado situar la ciberseguridad “en la mesa de dirección y no en el sótano de las organizaciones”. Apuntó también que “la regulación ha puesto el foco en la ciberresiliencia y ha convertido la seguridad en un asunto estratégico”, añadiendo que incluso las pymes se benefician al contar con pautas mínimas de cumplimiento.

En la parte final, Anna Angulo vinculó la ciberseguridad al contexto geopolítico global, donde los conflictos físicos y digitales se retroalimentan. Explicó que, tras cada episodio de guerra o tensión internacional, suelen desencadenarse campañas de ciberataques o desinformación. “Si entendemos esa secuencia, podemos anticipar la siguiente jugada y ganar tiempo de preparación”, concluyó, defendiendo la colaboración entre sectores público y privado como la única vía para mantener la prevención activa.

Mesa redonda de expertos – La ciberseguridad como reto sistémico

Moderada por Susana Rubio, la mesa de expertos reunió a voces del sector público, la consultoría, la certificación y la industria tecnológica: Rafael Vergara, director de soluciones de digitalización y tecnología de AENOR; Javier Zubieta, presidente de la Comisión de Ciberseguridad de AMETIC; Leonor Torres, presidente de ASTIC; Javier Carvajal, CEO de Icraitas; David Marco, Industrial Cybersecurity director de KPMG; y Eduvigis Ortiz, presidenta de Women4Cyber.

El objetivo: analizar las tendencias, riesgos y oportunidades que marcarán el futuro de la ciberseguridad en un contexto donde la inteligencia artificial, la regulación y la escasez de talento redefinen las prioridades del sector.

La conversación arrancó con una coincidencia general: la concienciación sigue siendo el gran desafío pendiente. Para Eduvigis Ortiz, la clave está en “desmitificar la ciberseguridad” y asumirla como una responsabilidad compartida: “cada uno de nosotros somos la primera línea

de defensa. La ciberseguridad debe dejar de verse como algo técnico para convertirse en un tema social", aseguró.

En la misma línea, David Marco (KPMG) insistió en que la educación debe empezar desde la base, que "debería ser una asignatura en los colegios" apuntando que el cambio cultural pasa por dejar de percibir la seguridad como un gasto: "no calculamos su retorno porque no medimos las pérdidas que evita".

De la reacción a la anticipación

"Somos tremendamente reactivos", aseguró Javier Carvajal (Icraitas) durante una de sus intervenciones. A su juicio, el salto cualitativo vendrá cuando las organizaciones aprendan a anticiparse. "Para prever, necesitamos herramientas y datos. La ciberseguridad debe integrarse con el negocio, porque sin ese vínculo sólo reaccionaremos", aseguró. Destacó además el papel de Mastercard y otras compañías tecnológicas en la creación de soluciones que facilitan esa transición hacia la proactividad.

> La mesa subrayó que la ciberseguridad es un reto sistémico que exige anticipación, educación y colaboración público-privada para afrontar amenazas crecientes

Desde AENOR, Rafael Vergara aportó la visión del auditor asegurando que "los controles no han cambiado tanto, lo que cambia es la forma de ataque". Reclamó estrategias ajustadas al contexto y al tamaño de cada organización, recordando que "no se puede abordar toda la ciberseguridad a la vez" y que la madurez de los comités directivos es clave para que el riesgo fluya de abajo arriba y se tomen decisiones informadas.

Inteligencia artificial: aliada y amenaza

El debate se centró después en la inteligencia artificial, con aportaciones coincidentes: su impacto será transformador, pero de doble filo.

Recordó Eduvigis Ortiz que los ciberdelincuentes "no tienen restricciones de presupuesto ni de ética" y que usarán la IA "más y mejor" que las empresas. "Tenemos que pensar cómo prevenir y cómo levantarnos rápido cuando nos ataquen", señaló, advirtiendo del auge de los "ultrafalsos", una evolución de los deepfakes.

Leonor Torres (ASTIC) destacó que la IA ya está integrada en la mayoría de las herramientas de defensa, pero que "también hay que proteger la IA misma", garantizando la seguridad de modelos y datos.

Subrayando el exceso de regulación europea frente a la agilidad de los atacantes David Marco recordó que los ciberdelincuentes "no cumplen normativas. Nosotros debemos equilibrar innovación y cumplimiento".

Rafael Vergara introdujo una reflexión provocadora: "quizá llegará el momento en que tenga-

mos que pasar de defendernos a atacar a los malos", en alusión a la necesidad de capacidades ofensivas coordinadas por los gobiernos.

Normativa y resiliencia: entre la carga y la oportunidad

El panel coincidió en que regulaciones como NIS2 y DORA son un motor positivo, aunque su despliegue genera presión.

Vergara explicó que "DORA no inventa nada nuevo, sino que aterriza controles que ya estaban en la ISO 27001", y alertó sobre la "fatiga normativa" que puede generar sobrecostes en las empresas.

> Los expertos coincidieron en que NIS2 o DORA impulsan madurez, pero generan fatiga mientras pymes y administraciones siguen especialmente vulnerables

Eduvigis Ortiz, sin embargo, defendió su papel como catalizador: "a veces la multa es lo que consigue que se priorice la ciberseguridad", aunque criticó la dispersión de obligaciones: "Un mismo incidente puede requerir hasta 23 notificaciones distintas. Necesitamos una ventanilla única".

El sector público y las pymes, los más vulnerables

Leonor Torres puso sobre la mesa las limitaciones de la Administración: falta de profesionales,

infraestructuras antiguas y presupuestos ajustados. “Tenemos una enorme responsabilidad porque gestionamos datos de los ciudadanos y servicios críticos, pero los recursos son escasos”, lamentó.

Defendiendo iniciativas como la red de SOC públicos y la colaboración con el sector privado como vías para avanzar, Rafael Vergara coincidió en la necesidad de evitar duplicidades y crear servicios comunes que reduzcan costes y desigualdades entre administraciones.

En paralelo, Javier Carvajal apuntó que las pymes siguen siendo el eslabón más débil: “Los que tienen recursos están más preparados; los que no, quedan desprotegidos. Necesitamos soluciones escalables que adapten la ciberseguridad a su realidad”.

Talento y diversidad: motores del cambio

Eduvigis Ortiz cerraba sus intervenciones con una llamada a la acción: “necesitamos un plan de comunicación para atraer talento y visibilizar los recursos disponibles”. Recordó que España es el cuarto país del mundo con más iniciativas en ciberseguridad, y que el INCIBE es modelo para Latinoamérica. “Seamos embajadores del 017 —dijo—, porque muchas personas ni siquiera saben que existe”.

En la ronda final de conclusiones, los participantes coincidieron en tres ideas clave. Por un lado, las personas seguirán siendo el eslabón más importante, incluso por encima de la tecnología. Por otro, la colaboración público-privada será determinante para crear un ecosistema seguro y resiliente. Finalmente, la inteligencia artificial y la gobernanza del dato marcarán el nuevo equilibrio entre innovación y control.

Ciberseguridad desde dentro: resiliencia, cultura y regulación

Moderada por un representante de Mastercard, la siguiente mesa reunió a tres responsables que viven la ciberseguridad desde el terreno operativo: Fanny Pérez, CISO Global de Codere; Julio Carriscajo, jefe de ciberinteligencia y análisis de Renfe; y Rafael Hernández, responsable de proyectos estratégicos de Moeve. Cada uno compartió cómo afrontan los retos actuales de protección, cumplimiento y cultura en organizaciones con alta exposición digital y fuerte regulación sectorial.

Adaptarse a un entorno de amenazas en constante evolución

"Estamos peleando con desventaja", reconoció Fanny Pérez, aludiendo a la asimetría existente entre las empresas y los grupos criminales, "porque ellos no tienen restricciones ni éticas ni regulatorias". En el caso de Codere, su estrategia se apoya en tres pilares: ciber inteligencia, resiliencia y protección.

La compañía ha reforzado el uso de IA y la automatización para filtrar ruido y acelerar la detección de alertas, ha multiplicado por tres la frecuencia de sus simulacros de crisis —"el músculo hay que ejercitarlo"— y ha consolidado una arquitectura de Zero Trust como base de su defensa. "Resiliencia no es una palabra de moda, es una disciplina que hay que interiorizar", afirmó la CISO Global de Codere.

Desde Moove, Rafael Hernández observó que los ciberataques ya no buscan paralizar empresas, sino robar información con valor económico o estratégico. "El dinero ahora es información", señaló, destacando la necesidad de dotar a los empleados de una cultura digital sólida y de integrar la ciberseguridad en el diseño de productos y servicios, recordando que "todos los proyectos estratégicos deben incluir una componente de seguridad desde el inicio".

Por su parte, Julio Carriscajo explicó que Renfe lleva una década evolucionando hacia un modelo integrado de seguridad, con una clara separación entre funciones de supervisión y protección operativa. Subrayó el valor de implicar a las áreas de negocio desde el momento cero asegurando: "no queremos que la ciberseguridad sea una barrera, sino un habilitador", y advirtiendo que los ataques actuales se centran en los datos: "Cuando algo sale del perímetro y no va acompañado de una pieza de seguridad, perdemos el control".

> Los participantes coincidieron en que el futuro pasa por resiliencia, automatización y una cultura sólida, donde la ciberseguridad se mida en el mismo lenguaje que el negocio

Concienciación y cultura: de la formación al compromiso

Uno de los puntos más compartidos durante el debate fue la importancia de las personas como primera línea de defensa. Rafael Hernández describió el programa de Moeve, que forma tanto a empleados como a sus familias, con jornadas abiertas y materiales educativos.

En Codere, las campañas de phishing simuladas pasaron de ser semestrales a mensuales y las formaciones son ahora obligatorias, explicaba Fanny Pérez. "Cuando los empleados dudan antes de abrir un enlace, sabemos que la cultura está calando", apuntó, al tiempo que alertaba sobre la sofisticación de ataques basados en deepfakes de voz e imagen.

Renfe, por su parte, ha creado su propio campus de ciberseguridad con micro cursos interactivos, campañas adaptadas a cada perfil profesional y ejercicios internos de respuesta, explicaba su jefe de ciber inteligencia y análisis. "No queremos ser la policía, sino el 017 de nuestros empleados", resumió Carriscajo.

El cambio cultural —coincidieron— se refleja

en la implicación del negocio. “Antes el CISO estaba en el sótano; ahora recibe llamadas del área legal o de compras pidiendo colaboración”, explicó el portavoz de Renfe. Para Mastercard, , ese cambio se traduce en madurez: “Ya no se debate si invertir o no en seguridad, se asume como parte del negocio”.

Normativa y gestión del riesgo: de la obligación al valor

Otro de los asuntos en los que coincidieron los tres ponentes fue en que NIS2 y DORA son necesarias, pero su aplicación práctica requiere equilibrio.

Rafael Hernández recordó que las empresas deben “usar la regulación en beneficio propio” y que los responsables de ciberseguridad han pasado de ser “el doctor No” a habilitadores del negocio. Julio Carriscajo apuntó que la regulación puede ser “una palanca de integración”, siempre que se interprete con sentido operativo: “los marcos normativos no siempre son aplicables tal cual; hay que buscar mitigaciones realistas”, aseguró en una de sus intervenciones.

> La mesa subrayó que sin proactividad, cultura digital y automatización es imposible responder al ritmo de las amenazas y de las nuevas exigencias regulatorias

En cuanto a Fanny Pérez, advirtió sobre las diferencias interpretativas entre áreas técnicas y legales: “A veces una norma se redacta pensando en la ley, no en la práctica”, aseguró, defendiendo la necesidad de marcos unificados pero flexibles, especialmente en multinacionales.

Prioridades y desafíos: prevención, automatización y comunicación

En el cierre del debate, los tres participantes coincidieron en que el futuro pasa por la proactividad, la automatización y la colaboración.

“Es muy cierto que no se puede responder manualmente a la velocidad de las amenazas. Hay que automatizar para centrarnos en lo que de verdad importa”, destacó Fanny Pérez.

Rafael Hernández insistió en fortalecer la resiliencia y la comunicación con la alta dirección, recordando que “la ciberseguridad tiene que medirse y comunicarse en el mismo lenguaje que el negocio”.

En cuando a Julio Carriscajo, subrayó la importancia de trasladar esa información al nivel ejecutivo: “Queremos que nuestros reportes de seguridad se lean con el mismo interés que los de EBITDA”.

Las preocupaciones comunes apuntan al mismo horizonte: consolidar una cultura de seguridad transversal, reforzar la cadena de suministro y mantener una colaboración estrecha entre empresas, administraciones y proveedores. Como mencionó Mastercard, “la cultura de la ciberseguridad ya no es un curso: es la forma en que operamos cada día”.

Conclusiones – Hacia una ciberseguridad basada en inteligencia, colaboración y resiliencia

El cierre de la jornada estuvo a cargo de Susana Rubio y Alberto López, de Mastercard, quienes sintentizaron las principales ideas del encuentro y trazaron una visión de futuro basada en tres ejes: colaboración, anticipación y formación.

Colaboración público-privada como motor de resiliencia

Recordando que las alianzas entre empresas tecnológicas, instituciones públicas y organismos reguladores son esenciales para desarrollar una resiliencia “real y sostenible”, subrayó Susana Rubio que “la ciberseguridad no puede construirse en solitario”.

Explicó que el modelo de Mastercard se basa

en cocrear soluciones, compartir inteligencia y coordinar respuestas frente a amenazas globales cada vez más rápidas y sofisticadas. Además destacó la creación del Centro Europeo de Ciber resiliencia de Mastercard, inaugurado en 2024 en Waterloo (Bélgica), donde la compañía colabora con bancos centrales, agencias regulatorias y entidades públicas y privadas en la definición conjunta de estrategias y buenas prácticas. “La cooperación es el mejor escudo ante las amenazas actuales y futuras”, concluyó la directiva.

Mastercard destacó que el futuro exige una ciberseguridad más anticipativa y colaborativa, apoyada en inteligencia, automatización y una resiliencia compartida

De la reacción a la inteligencia

Para Alberto López, el gran salto pendiente es pasar de la reacción a la anticipación. Recalcó que “la ciberseguridad debe estar en la mesa de dirección”, e insistió en que los directivos deben dejar de verla como un gasto para asumirla como una inversión en marca, continuidad y confianza.

López resumió tres prioridades urgentes para las empresas españolas: implicar al equipo di-

Mastercard e ISMS Forum: impulsando la formación en ciberseguridad

Mastercard se ha aliado con ISMS Forum, la asociación española líder en seguridad de la información, privacidad y gestión de riesgos. Esta colaboración busca fortalecer la formación práctica de los futuros líderes en ciberseguridad en España y Portugal.

Puntos clave de la alianza:

- **Enfoque educativo: la colaboración se centra en los programas de formación especializada en ciberseguridad que ISMS Forum ofrece.**
- **Acceso a tecnología: Mastercard proporcionará a los estudiantes de estos programas formativos acceso a RiskRecon, su avanzada solución impulsada por IA para la evaluación y calificación de riesgos de terceros.**
- **Beneficio para los futuros profesionales: equipar a los estudiantes con herramientas tangibles y de vanguardia para monitorear proveedores y cadenas de suministro digitales, identificando vulnerabilidades y gestionando riesgos en un entorno real.**
- **Objetivo final: preparar a la próxima generación de expertos con habilidades prácticas para enfrentar las crecientes amenazas cibernéticas y construir una resiliencia digital duradera.**

rectivo en la estrategia de seguridad; formar de manera continua a toda la organización, porque “la amenaza evoluciona cada día”; y automatizar la defensa con inteligencia artificial. “Detrás de un ataque de denegación de servicio suele haber una filtración de datos: la DDoS es la cortina de humo”, advirtió, subrayando la necesidad de contar con sistemas automáticos que detecten intrusiones en tiempo real.

Resiliencia corporativa y democratización de la seguridad

El equipo de Mastercard destacó, el avance de las empresas hacia una cultura de ciber resiliencia transversal, en la que los ejercicios ya no se limitan a los equipos técnicos, sino que involucran a toda la dirección. “Cada vez más organizaciones hacen simulacros de crisis no solo operativos, sino de comunicación y liderazgo”, señaló.

También alertaron de que la llegada de NIS2 marcará un punto de inflexión similar al del GDPR, y que “cuando caiga la primera multa, todos correrán”.

Defendieron la necesidad de pasar de la actividad a la proactividad, impulsando el uso de inteligencia de amenazas personalizada y la democratización de la ciberseguridad: que las soluciones avanzadas sean accesibles también para empresas medianas y pequeñas.

“Vamos en la dirección adecuada —concluyeron—: hacia una ciberseguridad más inteligente, colaborativa y humana”.