acceso 360

08/07/2026

Desayuno informativo_Cib-erespacio

Elite CONEXION

ÍNDICE

CLUB DIÁLOGOS PARA LA DEMOCRACIA

acceso 360

CLUB DIÁLOGOS PARA LA DEMOCRACIA

Elite CONEXION

Los organismos públicos de ciberseguridad piden más inversión, y que sea continua, ante nuevos riesgos como la IA

Miércoles, 08 de julio de 2026 12:36

Archivo - Ciberseguridad - PIXABAY - Archivo

MADRID 8 Jul. (EUROPA PRESS) -

El Mando Conjunto del Ciberespacio (MCCE), el Centro Criptológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (INCIBE) han reclamado este miércoles más inversión, y que esta sea "continuada" en el tiempo, ante nuevos retos y riesgos como la Inteligencia Artificial ofensiva.

En un desayuno informativo organizado por Club Diálogos por la Democracia, el comandante del MCCE, vicealmirante Javier Roca, ha expuesto la labor que realiza el mando y ha afirmado que, si bien tiene medios "suficientes", estos no lo son para proporcionar "seguridad digital" ni a España ni a las Fuerzas Armadas. "Rotundamente no", ha subrayado.

De su lado, el subdirector general del CCN, Javier Candau, ha pedido que la inversión sea "continua" y ha esbozado que es necesario un plan "a tres o cinco años", según lo considere el Gobierno. "Ante los nuevos riesgos, hace falta inversión, sin inversión focalizada (...) no llegaremos a tiempo, y tiene que ser continuada, no sirve destinar muchos millones un año y luego abandonarlo", ha explicado.

Candau aboga por potenciar "capacidades estratégicas", entre las que ha ubicado la "detección y neutralización de amenazas". "Esto es un punto en el que se pasa de ser defensivo a disponer de unas capacidades ofensivas que permitan neutralizar el foco de los problemas", ha añadido.

NO "DESPERDICIAR" EL DINERO

El director general del INCIBE, Félix Barrio, se ha expresado en la misma línea, lamentando que la inversión en esta materia "va a saltos" y "no tiene esa continuidad". "Es la pena", ha ahondado.

En cualquier caso, considera que "no va a haber problema de dinero" para destinarlo a este ámbito en España, y ha aludido al Fondo Europeo de Defensa, dotado con 7.900 millones de euros, y los fondos Next Generation. Y ha lanzado una advertencia: "No podemos desperdiciar ni un euro de los que podamos conseguir".

Requeridos por una cifra concreta que consideren adecuada para la inversión en ciberseguridad, Candau ha dicho que "no se atreve", mientras que el vicealmirante Roca ha señalado que 200 millones de euros son "una cifra razonable".

Javier Roca, comandante del Mando Conjunto del Ciberespacio (MCCE): “Sin soberanía no hay seguridad”

Miércoles, 8 de julio de 2026 13:41

La seguridad nacional ha dejado de dirimirse exclusivamente en las fronteras físicas. En un entorno en el que lo digital actúa como sistema nervioso de la sociedad, la soberanía tecnológica, la...

ESPAÑA ANTE EL RETO DE LA CIBERSEGURIDAD Y SOBERANÍA EUROPEA en el Club Diálogos para la Democracia, dirigido por Antonio Gavilanes.

Miércoles, 08 de julio de 2026 00:00

Nos espera la Amenaza cuántica. Todas las cifras en que está basada la ciberseguridad estarán rotas entre 2030 y 2050. Habrá un nuevo escenario cibernético y hay que estar preparados. Necesitamos resiliencia de los activos y neutralizar los focos de problemas. Las tecnologías cuánticas son el futuro.

Antonio Gavilanes, presidente del Club Diálogos para la Democracia
Ponentes de los Diálogos

Julia Sáez-Angulo

Fotos: Adriana Zapisek

9/7/26.- Madrid.- España ante el reto de la Ciberseguridad y Soberanía Europea, título de ponencia y debate en el Club Diálogos para la Democracia, dirigido por Antonio Gavilanes. El evento tuvo lugar en el Salón del Hotel Palace. Patrocinadores Accenture, IndraMind y Paz y Cooperación.

Abrió el acto **Antonio Gavilanes** para subrayar la importancia de desarrollar la logística en Defensa en España y Europa, como fuente de empleo y desarrollo sostenible, amén de la Defensa misma. Europa no puede ser la colonia chica de Estados Unidos, señaló. En un futuro habrá una nueva invasión de Rusia en el Ártico o el Báltico. Cobra fuerza el dicho latino si vis pacem para bellum (si quieres la paz, haz la guerra). Estamos a favor de la Defensa, no de la guerra. La opinión pública se conquista en la calle.

María Jesús Paniagua, Directora del Sector Público en Accenture, señaló que hay que sacar ventaja del espacio digital, donde existen amenazas en los espacios digitales, porque aparecen de continuo, nuevas capacidades para encontrar vulnerabilidades en ese espacio. Es importante la ciber-resiliencia de las organizaciones. Hay que procurar tener soberanía estratégica plena, algo en apariencia imposible, pero nos hemos puesto en camino. El talento de la población es necesario con una buena educación en este campo. En el ciberespacio nos jugamos el futuro, por eso necesitamos inversiones en IA, ciberseguridad, talento e industria.

Antonio Martínez González, Director General de IndraMadrid, recordó que ahora tenemos fronteras digitales y un ciberataque puede acaban con entes especiales y necesario de un país. Hoy, una empresa puede tener más poder ciber-digital que un Estado. El dominio es el mismo. Hay que conectar capacidades. Las amenazas pueden cambiar en la Defensa y frente al ciberataque se necesita resiliencia cibernética, máxime en una Administración en crisis.

El debate sobre la soberanía cibernética depende en parte de la dependencia tecnológica. La ventaja no es quien tiene más información sino quien sabe traducir los datos en conocimiento y acción. La soberanía no se decreta, se construye. Hay que saber anticipar amenazas y tomar decisiones. Las soluciones no son aisladas, sino un combinatorio en tiempo real de IA y acción. Hay que proteger el agua, la electricidad, la economía y la liberta de acción militar para defendernos. Sin seguridad no hay resiliencia. La soberanía no es solo territorio, sino bienes que hay que proteger.

Rosa Olazábal, presidenta de Paz y Cooperación dijo que hablamos de que España, dentro de Europa, defiende una energía compatible, que la línea de actuación para la soberanía digital y el ciberespacio está en la capacidad de actuación en la Defensa, la industria y la tecnología. Insistió en que el talento por la buena preparación educativa de la población es clave. Hay que insistir en educación digital y cibernética.

Javier Roca, vicealmirante. Comandante del Mando Conjunto del Ciberespacio, recordó también que la soberanía ha cambiado su frontera, porque necesita seguridad digital y física, ciberseguridad apoyada en tres pilares: tecnología (software y hardware) fácil de adquirir; operacional y dominio de datos con la capacitación de una población que tenga talento en la especialidad. Puso de ejemplo a los ucranianos en la guerra, que no tienen tecnología, pero sí capacidad operacional para actuar con la que se le entrega. No existe la soberanía al cien por cien. Junto a los datos se requiere la interpretación y la acción.

Félix Barrio, Director General del Instituto Nacional de Coberseguridad, INCIBE,informó de que mantenemos un gran nivel de resiliencia en términos estadísticos; trabajamos en. Continuidad con distintos países. Hay inversiones. La ciberseguridad afecta la soberanía nacional y debe cubrir hasta el último pueblo. Ha de haber proveedores de proximidad en el mundo digital. El 45% de las empresas son PYMES y requieren ciberseguridad frente a los ataques. Somo un país que no pierde el des. Somos el segundo país del mundo en la industria de la automoción y todas las empresas dependen de la digitalización. Hay que seguir insistiendo en el I+D. La Universidad ha de ser potente en este campo y ha de funcional la transferencia del conocimiento. Ya existen

títulos de ciberseguridad en la Formación Profesional. Somos un país donde no cunde el desánimo, pese a ser hipercríticos.

Javier Candau, Subdirector General del Centro Criptológico Nacional, recordó que la Covid hizo replantearse las cosas en la Defensa y ciberseguridad. También la guerra de Ucrania y los requerimientos de la OTAN. Se necesita la IA defensiva y ofensiva ante la vulnerabilidad por agente ofensivos de la IA. Pero nos espera la Amenaza cuántica. Todas las cifras en que está basada la ciberseguridad estarán rotas entre 2030 y 2050. Habrá un nuevo escenario cibernético y hay que estar preparados. Necesitamos resiliencia de los activos y neutralizar los focos de problemas. Las tecnologías cuánticas son el futuro.

José de la Peña, Director de la Revista de Ciberseguridad, Seguridad de la Información y Privacidad -SIC, moderó el coloquio animado, en el que el Almirante dijo que lo importante es lo que vamos y queremos hacer. Se insistió en la educación digital y en que los presupuestos deben ser constante y no a saltos, que las medidas han de ser horizontales a nivel local y se insistió en la amenaza cuántica y necesitad de tecnología cuántica del futuro. La prioridad está en las capacidades reales probadas en educación y adiestramiento operacional, con efectos relevantes para la seguridad ciberespacial. La importancia de la especialización y en las sinergias. Europa tiene retos para mantener el liderazgo.

Asistentes al desayuno informativo: periodistas, empresarios y embajadas.

ESPAÑA ANTE EL RETO DE LA CIBERSEGURIDAD Y SOBERANÍA EUROPEA en el Club Diálogos para la Democracia, dirigido por Antonio Gavilanes.

Los organismos públicos de ciberseguridad piden más inversión, y que sea "continua", ante nuevos riesgos como la IA

Miércoles, 08 de julio de 2026 00:00

08·07·26 | 13:07 | Actualizado a las 13:08

Los organismos públicos de ciberseguridad piden más inversión ante riesgos como la IA

El Mando Conjunto del Ciberespacio **(MCCE**), el Centro Criptológico Nacional (**CCN**) y el Instituto Nacional de Ciberseguridad (INCIBE) han reclamado este miércoles **más inversión, y que esta sea "continuada"** en el tiempo, **ante nuevos retos y riesgos como la Inteligencia Artificial ofensiva.**

INCIBE detectó más de 122.000 incidentes de ciberseguridad en 2025

En un desayuno informativo organizado por Club Diálogos por la Democracia, el comandante del MCCE, vicealmirante **Javier Roca**, ha expuesto la labor que realiza el mando y ha afirmado que, **si bien tiene medios "suficientes", estos no lo son para proporcionar "seguridad digital" ni al Estado español ni a las Fuerzas Armadas**. "Rotundamente no", ha subrayado.

"Capacidades estratégicas"

De su lado, el subdirector general del CCN, **Javier Candau,** ha pedido **que la inversión sea "continua"** y ha esbozado que **es necesario un plan "a tres o cinco años"**, según lo considere el Gobierno español. "Ante los nuevos riesgos, **hace falta inversión,** sin inversión focalizada (...) no llegaremos a tiempo, y **tiene que ser continuada**, no sirve destinar muchos millones un año y luego abandonarlo", ha explicado.

Candau aboga por potenciar "capacidades estratégicas", entre las que ha ubicado la "**detección y neutralización de amenazas"**. "Esto es un punto en el que se pasa de ser defensivo a **disponer de unas capacidades ofensivas que permitan neutralizar el foco de los problemas**", ha añadido.

No "desperdiciar" el dinero

El director general del INCIBE, **Félix Barrio**, se ha expresado en la misma línea, lamentando que **la inversión en esta materia "va a saltos" y "no tiene esa continuidad"**. "Es la pena", ha ahondado. En cualquier caso, considera que "no va a haber problema de dinero" para destinarlo a este ámbito en España, y **ha aludido al Fondo Europeo de Defensa, dotado con 7.900 millones de euros, y los fondos Next Generation**. Y ha lanzado una advertencia**: "No podemos desperdiciar ni un euro** de los que podamos conseguir".

Requeridos por **una cifra concreta que consideren adecuada** para la inversión en ciberseguridad, Candau ha dicho que "no se atreve", mientras que el vicealmirante **Roca ha señalado que 200 millones de euros** son "una cifra razonable".

Los organismos públicos de ciberseguridad piden más inversión, y que sea "continua", ante nuevos riesgos como la IA

Miércoles, 08 de julio de 2026 13:09

El Mando Conjunto del Ciberespacio (MCCE), el Centro Criptológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (INCIBE) han reclamado este miércoles más inversión, y que esta sea "continuada" en el tiempo, ante nuevos retos y riesgos como la Inteligencia Artificial ofensiva.

En un desayuno informativo organizado por Club Diálogos por la Democracia, el comandante del MCCE, vicealmirante Javier Roca, ha expuesto la labor que realiza el mando y ha afirmado que, si bien tiene medios "suficientes", estos no lo son para proporcionar "seguridad digital" ni a España ni a las Fuerzas Armadas. "Rotundamente no", ha subrayado.

De su lado, el subdirector general del CCN, Javier Candau, ha pedido que la inversión sea "continua" y ha esbozado que es necesario un plan "a tres o cinco años", según lo considere el Gobierno. "Ante los nuevos riesgos, hace falta inversión, sin inversión focalizada (...) no llegaremos a tiempo, y tiene que ser continuada, no sirve destinar muchos millones un año y luego abandonarlo", ha explicado.

Candau aboga por potenciar "capacidades estratégicas", entre las que ha ubicado la "detección y neutralización de amenazas". "Esto es un punto en el que se pasa de ser defensivo a disponer de unas capacidades ofensivas que permitan neutralizar el foco de los problemas", ha añadido.

NO "DESPERDICIAR" EL DINERO

El director general del INCIBE, Félix Barrio, se ha expresado en la misma línea, lamentando que la inversión en esta materia "va a saltos" y "no tiene esa continuidad". "Es la pena", ha ahondado.

En cualquier caso, considera que "no va a haber problema de dinero" para destinarlo a este ámbito en España, y ha aludido al Fondo Europeo de Defensa, dotado con 7.900 millones de euros, y los fondos Next Generation. Y ha lanzado una advertencia: "No podemos desperdiciar ni un euro de los que podamos conseguir".

Requeridos por una cifra concreta que consideren adecuada para la inversión en ciberseguridad, Candau ha dicho que "no se atreve", mientras que el vicealmirante Roca ha señalado que 200 millones de euros son "una cifra razonable".

Los organismos públicos de ciberseguridad reclaman más inversión continua ante amenazas como la IA

Miércoles, 08 de julio de 2026 00:00

El Mando Conjunto del Ciberespacio (MCCE), el Centro Criptológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (INCIBE) han insistido este miércoles en la necesidad de reforzar la inversión en ciberseguridad, y que esta sea continuada en el tiempo, para hacer frente a nuevos desafíos y riesgos como la Inteligencia Artificial ofensiva.

Durante un desayuno informativo organizado por Club Diálogos por la Democracia, el comandante del MCCE, vicealmirante Javier Roca, ha detallado las funciones del mando y ha apuntado que, aunque actualmente dispone de medios suficientes, estos no alcanzan para garantizar la seguridad digital del país ni de las Fuerzas Armadas. Rotundamente no, ha enfatizado.

Por su parte, el subdirector general del CCN, Javier Candau, ha reclamado que la inversión sea continua y ha planteado la conveniencia de articular un plan a tres o cinco años, en función de lo que determine el Gobierno. Ante los nuevos riesgos, hace falta inversión, sin inversión focalizada (…) no llegaremos a tiempo, y tiene que ser continuada, no sirve destinar muchos millones un año y luego abandonarlo, ha indicado.

Candau ha defendido el refuerzo de las capacidades estratégicas, entre las que ha situado la detección y neutralización de amenazas. Esto es un punto en el que se pasa de ser defensivo a disponer de unas capacidades ofensivas que permitan neutralizar el foco de los problemas, ha remachado.

No desperdiciar los fondos disponibles

En la misma línea se ha pronunciado el director general del INCIBE, Félix Barrio, quien ha lamentado que la inversión en ciberseguridad va a saltos y no tiene esa continuidad. Es la pena, ha señalado.

Aun así, considera que no va a haber problema de dinero para financiar este ámbito en España, y ha mencionado el Fondo Europeo de Defensa, dotado con 7.900 millones de euros, así como los fondos Next Generation. En este contexto, ha lanzado una advertencia: No podemos desperdiciar ni un euro de los que podamos conseguir.

Preguntados por una cifra concreta que consideren adecuada para la inversión en ciberseguridad, Candau ha admitido que no se atreve a fijarla, mientras que el vicealmirante Roca ha apuntado que 200 millones de euros serían una cifra razonable.

Solo un 5% de las organizaciones españolas se siente preparada para las ciberamenazas impulsadas por la IA

Redacción Seguros Tv **Jueves, 09 de julio de 2026 07:10**

La inteligencia artificial está transformando el panorama de la ciberseguridad, pero las empresas españolas aún no se sienten preparadas para afrontar este nuevo escenario. Según datos presentados por **Accenture** durante el encuentro Ciberespacio: España ante el reto de la Soberanía y la Seguridad Europea, solo el 5% de las organizaciones españolas considera que está preparada para hacer frente a las ciberamenazas potenciadas por la IA.

La jornada, organizada por el **Club Diálogos para la Democracia** con el patrocinio de Accenture, IndraMind y Fundación Paz y Cooperación, reunió a representantes de la Administración, las Fuerzas Armadas y la industria tecnológica para analizar los desafíos de la soberanía tecnológica y la ciberseguridad europea.

La soberanía tecnológica, clave para la seguridad

El vicealmirante **Javier Roca**, comandante del Mando Conjunto del Ciberespacio, defendió que sin soberanía no hay seguridad y subrayó que la protección del ciberespacio exige desarrollar capacidades tecnológicas propias.

Durante su intervención explicó que la soberanía actual debe sustentarse sobre tres pilares: la soberanía tecnológica, la soberanía operacional y la soberanía de los datos.

En este sentido, insistió en que disponer de tecnología no es suficiente si no se acompaña de talento y capacidades operativas que permitan proteger infraestructuras críticas y responder a amenazas cada vez más sofisticadas.

La IA obliga a acelerar las inversiones

Por parte de Accenture, **María Jesús Chus Paniagua**, managing director del Sector Público en España, destacó que la inteligencia artificial está cambiando profundamente el panorama de la ciberseguridad.

Según explicó, las inversiones en defensa y seguridad deben orientarse a construir capacidades de IA soberana, multimodelo y escalable, desarrolladas conjuntamente entre administraciones e industria para reforzar la autonomía estratégica europea.

Ciberseguridad y ciberdefensa, una estrategia común

El director general de IndraMind, **Ignacio Martínez**, defendió que la ciberseguridad y la ciberdefensa ya no pueden abordarse por separado, sino como elementos de una misma estrategia nacional y europea.

Martínez aseguró que la soberanía tecnológica no implica autarquía, sino la capacidad de decidir sobre tecnologías críticas, y destacó que la inteligencia artificial será determinante para transformar los datos en conocimiento y mejorar la toma de decisiones frente a amenazas híbridas.

Educación, talento y colaboración público-privada

La presidenta de Fundación Paz y Cooperación, **Rosa Olazábal**, puso el foco en la educación como uno de los pilares para construir la soberanía tecnológica del futuro.

Los participantes coincidieron en que Europa debe reforzar las inversiones en tecnología, inteligencia artificial, formación y talento, además de impulsar una colaboración más estrecha entre administraciones públicas, Fuerzas Armadas, empresas y centros de conocimiento para reducir dependencias estratégicas y fortalecer la industria tecnológica europea.

El encuentro concluyó con un mensaje compartido: la seguridad del siglo XXI se juega también en el ciberespacio y exige convertir la innovación tecnológica en capacidades reales para proteger a ciudadanos, empresas e infraestructuras críticas.

Solo un 5% de las organizaciones españolas se siente preparada para las ciberamenazas impulsadas por la IA

Jueves, 09 de julio de 2026 07:56

La inteligencia artificial está transformando el panorama de la ciberseguridad, pero las empresas españolas aún no se sienten preparadas para afrontar este nuevo escenario. Según datos presentados por **Accenture** durante el encuentro Ciberespacio: España ante el reto de la Soberanía y la Seguridad Europea, solo el 5% de las organizaciones españolas considera que está preparada para hacer frente a las ciberamenazas potenciadas por la IA.

La jornada, organizada por el **Club Diálogos para la Democracia** con el patrocinio de Accenture, IndraMind y Fundación Paz y Cooperación, reunió a representantes de la Administración, las Fuerzas Armadas y la industria tecnológica para analizar los desafíos de la soberanía tecnológica y la ciberseguridad europea.

La soberanía tecnológica, clave para la seguridad

El vicealmirante **Javier Roca**, comandante del Mando Conjunto del Ciberespacio, defendió que sin soberanía no hay seguridad y subrayó que la protección del ciberespacio exige desarrollar capacidades tecnológicas propias.

Durante su intervención explicó que la soberanía actual debe sustentarse sobre tres pilares: la soberanía tecnológica, la soberanía operacional y la soberanía de los datos.

En este sentido, insistió en que disponer de tecnología no es suficiente si no se acompaña de talento y capacidades operativas que permitan proteger infraestructuras críticas y responder a amenazas cada vez más sofisticadas.

La IA obliga a acelerar las inversiones

Por parte de Accenture, **María Jesús Chus Paniagua**, managing director del Sector Público en España, destacó que la inteligencia artificial está cambiando profundamente el panorama de la ciberseguridad.

Según explicó, las inversiones en defensa y seguridad deben orientarse a construir capacidades de IA soberana, multimodelo y escalable, desarrolladas conjuntamente entre administraciones e industria para reforzar la autonomía estratégica europea.

Ciberseguridad y ciberdefensa, una estrategia común

El director general de IndraMind, **Ignacio Martínez**, defendió que la ciberseguridad y la ciberdefensa ya no pueden abordarse por separado, sino como elementos de una misma estrategia nacional y europea.

Martínez aseguró que la soberanía tecnológica no implica autarquía, sino la capacidad de decidir sobre tecnologías críticas, y destacó que la inteligencia artificial será determinante para transformar los datos en conocimiento y mejorar la toma de decisiones frente a amenazas híbridas.

Educación, talento y colaboración público-privada

La presidenta de Fundación Paz y Cooperación, **Rosa Olazábal**, puso el foco en la educación como uno de los pilares para construir la soberanía tecnológica del futuro.

Los participantes coincidieron en que Europa debe reforzar las inversiones en tecnología, inteligencia artificial, formación y talento, además de impulsar una colaboración más estrecha entre administraciones públicas, Fuerzas Armadas, empresas y centros de conocimiento para reducir dependencias estratégicas y fortalecer la industria tecnológica europea.

El encuentro concluyó con un mensaje compartido: la seguridad del siglo XXI se juega también en el ciberespacio y exige convertir la innovación tecnológica en capacidades reales para proteger a ciudadanos, empresas e infraestructuras críticas.

El Mando del Ciberespacio advierte de que faltan medios para garantizar la ciberseguridad

Miércoles, 08 de julio de 2026 13:19

El Mando del Ciberespacio advierte de que faltan medios para garantizar la ciberseguridad

Madrid, 8 jul (EFE).- El comandante del Mando Conjunto del Ciberespacio, vicealmirante Javier Roca, ha considerado que esta unidad cuenta con los medios económicos suficientes pero, a la vez, ha a...

Madrid, 8 jul (EFE).- El comandante del Mando Conjunto del Ciberespacio, vicealmirante Javier Roca, ha considerado que esta unidad cuenta con los medios económicos suficientes pero, a la vez, ha advertido de que "no es suficiente para proporcionar ciberseguridad al país y a las Fuerzas Armadas".

Así lo ha señalado Roca durante su intervención en un encuentro informativo del Club Diálogos para la Democracia, en el que ha participado junto al director general del Instituto Nacional de Ciberseguridad (INCIBE), Félix Barrio; y el subdirector general del Centro Criptológico Nacional (CCN), Javier Candau, los tres centros de referencia responsables de la ciberseguridad en España.

"El Mando Conjunto del Ciberespacio y las Fuerzas Armadas tenemos medios suficientes, pero ¿es suficiente para proporcionar seguridad digital, ciberseguridad, al país y a las Fuerzas Armadas?. Rotundamente no", ha afirmado el vicealmirante.

El comandante del Mando Conjunto ha señalado que "cada vez los aumentamos (los medios económicos) un poquito más, el doble, pero las amenazas son 10 veces más".

En la misma línea, el subdirector del CCN, organismo adscrito al Centro Nacional de Inteligencia (CNI), ha reclamado una inversión continuada en el tiempo a través de un plan a 3 o 5 años, según decida el Gobierno, enfocado principalmente a la obtención de capacidades de Inteligencia Artificial (IA) ofensiva apoyada en tecnología cuántica.

Candau ha asegurado que la amenaza cuántica "se está acelerando" y ha advertido de que "o rediseñamos todas las cifras en las que se basa nuestra ciberseguridad o tendremos un problema crítico", a la vez que ha incidido en la importancia de considerar la ciberseguridad como un asunto de seguridad nacional.

"Ante los nuevos riesgos hace falta inversión, si no, no llegaremos a tiempo, y se requiere que sea continuada. No nos pueden llegar muchos millones un año y nada el otro", ha dicho.

Por su parte, el responsable del INCIBE ha considerado que "no va a haber problema de dinero", aunque ha lamentado que "se va a saltos, tirando de otros fondos" que tradicionalmente no se destinaban a ciberseguridad.

"La preocupación no es la inversión, sino si estamos preparados para presentar proyectos retadores y competitivos", ha señalado. EFE