SESIONES ACADÉMICAS NACIONALES: LEÓN

Real Academia de Ciencias Económicas y Financieras

LA CIBERSEGURIDAD COMO IMPERATIVO PARA LA ECONOMÍA DE ESPAÑA

SOLEMNE ACTO ACADÉMICO CONJUNTO ENTRE EL INSTITUTO NACIONAL DE CIBERSEGURIDAD Y LA REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

León, 17 de marzo de 2023

LA CIBERSEGURIDAD COMO IMPERATIVO PARA LA ECONOMÍA DE ESPAÑA

Solemne Acto Académico conjunto entre el Instituto Nacional de Ciberseguridad y la Real Academia de Ciencias Económicas y Financieras

La realización de esta publicación
ha sido posible gracias a

Generalitat de Catalunya
Departament de Justícia

con la colaboración de

Fundación "la Caixa"

LA CIBERSEGURIDAD COMO IMPERATIVO PARA LA ECONOMÍA DE ESPAÑA

Solemne Acto Académico conjunto entre el Instituto Nacional de Ciberseguridad y la Real Academia de Ciencias Económicas y Financieras

Publicaciones de la Real Academia de Ciencias Económicas y Financieras

Real Academia de Ciencias Económicas y Financieras
"La Ciberseguridad como imperativo para la Economía de España" / Real Academia de Ciencias Económicas y Financieras.

Bibliografía
ISBN- 978-84-09-52715-1

I. Título II. Gil Aluja, Jaime III. Colección

1. Economía 2.Ciberseguridad 3. Transformación

Editora: ©2023 Real Academia de Ciencias Económicas y Financieras, Barcelona.
www.racef.es
Fotografía portada: www.freepik.es
Académica Coordinadora: Dra. Ana Maria Gil-Lafuente

ISBN- 978-84-09-52715-1

Depósito legal: B 14214-2023

Obra producida en el ámbito de la subvención concedida a la Real Academia de Ciencias Económicas y Financieras por el Ministerio de Ciencia e Innovación.

Impreso y encuadernado en España por Ediciones Gráficas Rey, S.L.—c/Albert Einstein, 54 C/B, Nave 12-14-15
Cornellà de Llobregat—Barcelona
Impresión Julio 2023

Esta publicación ha sido impresa en papel ecológico ECF libre de cloro elemental, para mitigar el impacto medioambiental

REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

Solemne Acto Académico conjunto entre el Instituto Nacional de Ciberseguridad y la Real Academia de Ciencias Económicas y Financieras

17 DE MARZO DE 2023

"La Ciberseguridad como imperativo para la Economía de España"

ACTO ACADÉMICO

APERTURA Y PRESENTACIÓN

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"Entre recuerdos y esperanzas".

SESIÓN ACADÉMICA

Dr. Félix Antonio Barrio Juárez
Director General del INCIBE
"Ciberseguridad y riesgo tecnológico como grandes desafíos de la economía española".

Dr. Enrique López González
Académico de Número de la Real Academia de Ciencias Económicas y Financieras.
"Quo Vadis, Incibe? Desafíos emergentes y algunas propuestas de acción para facilitar resiliencia y prosperidad compartida".

CLAUSURA ACTO ACADÉMICO

Dr. Jaime Gil Aluja

Presidente de la Real Academia de Ciencias Económicas y Financieras

"A la búsqueda de una nueva axiomática de la ciberseguridad".

ÍNDICE

REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

SOLEMNE ACTO ACADÉMICO CONJUNTO ENTRE EL INSTITUTO NACIONAL DE CIBERSEGURIDAD Y LA REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

17 DE MARZO DE 2023

"LA CIBERSEGURIDAD COMO IMPERATIVO PARA LA ECONOMÍA DE ESPAÑA"

APERTURA Y PRESENTACIÓN

ENTRE RECUERDOS Y ESPERANZAS

Presentación

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras

Por segunda vez, el pleno la Real Academia, pisa tierras leonesas. Lo hicimos por vez primera hace 5 años, a raíz de nuestro encuentro científico con el Claustro de la **Universidad de León.** Firmamos un acuerdo de colaboración, cuya vigencia y eficacia no ha quedado erosionado ni por el paso del tiempo, ni por acontecimientos que hubieran podido dificultar nuestras tareas académicas, siempre al servicio de la sociedad española, a la que nos debemos.

No es ajeno a este objetivo, el Catedrático de su Universidad y Académico de Número de la Real Academia de Ciencias Económicas y Financieras del Instituto de España, el Excmo. Dr. Enrique López González, a quien desearíamos mostrar, aquí y ahora, nuestro más profundo agradecimiento.

Nuestras vivencias con León y su Universidad son mucho más antiguas de cuanto hasta ahora les he relatado.

Así, en la última década del siglo pasado tuvimos la satisfacción de realizar un conjunto de cursos de doctorado, lo que además del goce de compartir los primeros pasos epistemológicos de las disciplinas sobre el tratamiento de la incertidumbre y la complejidad, también nos permitió conocer y disfrutar de intelectuales como Juan Pérez Chencho (periodista ya fallecido), o Juan Rodriguez Garcia-Lozano, padre del Presidente Zapatero, compartiendo

conocimientos, pero también risas y mantel de la extraordinariamente rica gastronomía leonesa.

No nací en Barcelona, mi ciudad natal fue Reus, en donde viví mi infancia y juventud hasta que me trasladé a Barcelona en el año 1954 para realizar los estudios de Licenciatura y Doctorado, como alumno de la primera promoción de la recién inaugurada **Facultad de Ciencias Políticas, Económicas y Comerciales.**

Supongo que habrán adivinado el motivo que puede justificar esta referencia. No es otro que la inmensa figura del genial arquitecto Antonio Gaudí, hijo ilustre de Reus, su actividad en León y el maravilloso legado cultural que dejó en esta querida ciudad.

Resultado de estos seminarios fue una buena armonía entre las prestigiosas facultades asentadas en sus respectivas ciudades, la de León y la Rovira i Virgili, que propiciaron una serie de iniciativas de carácter investigador. Tanto es, así, que los miembros de la Universidad de León figuran en lugar destacado entre quienes forman parte de la nueva corriente del pensamiento económico que se conoce, hoy en todo el mundo como **Escuela de Economía Humanista de Barcelona**.

En una de estas idas y venidas, los amigos catalanes que participaron en una Solemne Sesión doctoral, se trajeron con ellos desde nuestra ciudad, Reus, un minúsculo arbolito mediterráneo, con la pretensión de que sobreviviera y creciera en los fríos inviernos de León.

Pues sí, sobrevivió y creció, convirtiéndose en lo que es hoy, un magnifico y **robusto almez** (celtis australis), que año tras año ofrece sus almecinas,…

Y pudimos constatar, créanme, que es **menos** difícil una actividad fructífera entre nuestras dos instituciones que la supervivencia del almez. Y, por tanto, aún hoy el almez está dando sus frutos.

Para convencer a los más lógicamente incrédulos, basta con que se den un paseo por el claustro de la Universidad y lo verán en uno de sus patios. Esto sí, se eligió el que creímos menos expuesto a los helados vientos invernales. Y allí contemplarán, fuerte y robusto, el **almez de Gaudi.**

Pero volvamos a nuestro relato central. Para quienes no la recuerden, diremos que la "escuela" define una nueva manera de concebir el tratamiento de la fenomenología social, económica y empresarial, en donde el sujeto de las relaciones entre los humanos en sociedad, ya no es el mecánico **"homo económicus"**, sino, simplemente el **humano.** Con su racionalidad, sí, pero también con sus **sueños, sus quimeras, sus necesidades, gustos y deseos.** Es decir, el humano con toda su **complejidad**: con su componente de racionalidad y su capacidad creativa. En otras palabras: con su grado o nivel de **objetividad** y su grado o nivel de **subjetividad**.

Esta nueva corriente de pensamiento dispone, ya, de sus **principios, su axiomática, sus teorías, sus métodos, modelos y algoritmos.**

Y aquí surge la primera pregunta: ¿Tiene sentido y es útil unir esfuerzos entre nuestras dos instituciones?

Hoy podemos decir, clara y rotundamente, sí, sí es posible y deseable. La **digitalización** lo ha permitido y la **cibernética** nos da las claves, con sus ventajas y horizontes casi infinitos, aún cuanto estamos advertidos de sus grandes riesgos de constreñir el **pensamiento** y la más auténtica **libertad**, que es la del **conocimiento.**

Y aquí radica, si me lo permiten, otra zona de cercanía e identidad recíproca, pues desde el actual Ministerio de Asuntos Económicos y Transformación Digital, liderado por la Vicepresidenta 1ª del Gobierno Dª **Nadia Calviño Santamaría**, hemos visto reivindicada la **perspectiva humanista de la digitalización**, que pone a las personas en una posición central, para así contribuir al bien común.

Como es sabido, la **confianza** en este nuevo entorno, dirigido por datos, **es un imperativo**, no es una opción, que ratifica el interés económico de la ciberseguridad, para la economía en general y, por ende, también para nuestra Real Corporación.

En este sentido, me permito brindar aquí y ahora el potencial investigador de nuestro equipo liderado por su Presidente, el Premio Nobel Finn Kydland, la doctora Shiqi Cheng, la doctoranda Bibiana Pacheco y la catedrática Ana Mª Gil Lafuente, su Directora, con capacidad científica y reconocido prestigio, dentro y fuera de nuestras fronteras.

Permítanme, también, poner a su disposición y al servicio de España, nuestra red de conexiones geopolíticas en cuatro continentes, incluyendo entre ellas ocho Premios Nobel y destacados científicos, algunos celebrados matemáticos en áreas consideradas de ciberriesgo. **Aquí nos tienen.**

Gracias por su atención y amabilidad por escuchar estas sencillas palabras de presentación. Con tan largo circuito hemos pretendido únicamente expresar nuestra alegría y nuestro gozo por estar aquí, en el Instituto Nacional de Ciberseguridad, el más alto exponente español en esta materia.

Porque, estar aquí y ahora, nos brinda la oportunidad de **enlazar**, en lo posible, **nuestros respectivos trabajos** mediante **un acuerdo científico** amplio y libre, y así colaborar en el alto objetivo último que nos hemos fijado: la **prosperidad compartid**a.

Muchas gracias por su atención.

SESIÓN ACADÉMICA

CIBERSEGURIDAD Y RIESGO TECNOLÓGICO COMO GRANDES DESAFÍOS DE LA ECONOMÍA ESPAÑOLA

Dr. Félix Antonio Barrio Juárez
Director General del INCIBE

León fue elegido en 2007 como sede para albergar el Centro de Alerta Temprana Antivirus. 21 años después, esta institución se conoce como Instituto Nacional de Ciberseguridad de España y ha sido la encargada de defender a los ciudadanos y empresas en el ámbito tecnológico. Esta contribución nos acerca a un objetivo claro: una sociedad y una economía más competitivas, prósperas y resilientes.

A día de hoy, la dependencia de todo ser humano de la tecnología es indiscutible; esto provoca que la ciberseguridad sea vital en nuestro día a día. Los recientes sucesos, como la pandemia, nos han empujado a los brazos de los dispositivos tecnológicos y nos han obligado a buscar soluciones especializadas a cada ámbito de nuestra vida. Sin embargo, no debemos quedarnos estancados en el hoy, sino que debemos mirar un poco más allá: ¿a qué retos nos enfrentamos? ¿Qué limitaciones tienen las tecnologías? ¿Qué obstáculos nos encontraremos en el futuro?

Es en este punto en el que entra la labor de los científicos: sus razonamientos o reflexiones nos ayudan a comprender nuestro entorno, el proceso de cambio que estamos sufriendo y cómo podemos anticiparnos a todo ello. Solamente apoyándonos en sus cimientos de conocimiento podremos prepararnos para lo que venga.

1.1. Riesgo y oportunidad tecnológica

Ante el mapa que muestra una visualización topográfica de dispositivos españoles activos, identificados a través de su IP, nos hacemos una idea de la cantidad de personas que, en un momento exacto, están en contacto con Internet. A nivel global, hablamos de más de 30.000 millones de dispositivos conectados; es decir, más de 8 dispositivos por habitante.

Figura 1: Mapa con visualización topográfica de dispositivos activos españoles en ese momento exacto (identificados a través de su IP).

Fuente: INCIBE

Un indicador nos marca el volumen de eventos de ciberseguridad que suceden en el momento exacto en España: 45%, superando levemente la media de incidentes que debería haber con una fecha y hora de tales características. Por regiones, destacan las de mayor población: Madrid, Cataluña, Comunidad Valenciana… En el momento exacto que vemos reflejado en esa imagen, hablamos de 26.000 incidentes en dispositivos de España. Este software también nos permite analizar la variante de ciberincidente que está sucediendo en cada uno de los territorios.

Si cogemos de ejemplo Barcelona, una ciudad con mucho movimiento, al realizar el desglose veremos los principales hitos: vulnerabilidades de dispositivos, bots, malwares que infectan terminales, intentos de phishing… Son solo algunos de los ejemplos de las amenazas que acechan en la red: robo de información, fraude, extorsión.

Muchos de los incidentes que citamos anteriormente podrían evitarse con el uso de un antivirus; sin embargo, la mitad de los usuarios no hace uso de esa herramienta de protección en su dispositivo móvil. Esto refleja el glan problema que existe en este campo: la falta de concienciación de los riesgos a los que nos enfrentamos y la esacasa preparación de dispositivos a nivel básico. Ni siquiera, algo tan sencillo como la actualización del sistema operativo, que también podría servir como barrera a muchas de estas amenazas, es una de las tareas que los usuarios cumplan en gran medida.

Desde INCIBE, al detectar alguna infección de un dispositivo, la primera acción a realizar es notificar de tal suceso al proveedor de telefonía e internet, los cuales disponen de 72 horas para eliminar dicha amenaza. Aún así, no es posible detectar todos los ciberincidentes que suceden día a día.

Como vemos, la tecnología conlleva un riesgo importante en términos de seguridad, pero también una oportundad de desarrollo económico y social. El impulso a la ciberseguridad es un motor de prosperidad en una economía global y digitalizada como la actual y supone, además, un sector transversal, de alto valor añadido y con un enorme potencial de crecimiento.

1.2. Aumento de uso, aumento de amenazas

Tres hechos a tener en cuenta durante la pandemia:

- La realización de pagos a través de internet ha crecido a pasos agigantados: el 58’4% de los usuarios recurre a ellos.

- Aumento de un 432’4% del uso de contenidos digitales de pago o suscripción.

- Asciende el consumo de videojuegos online y chats de comunicación.

Estos datos, si bien provienen de una situación muy particular, han venido para quedarse. Evidentemente, cuanto más uso de la tecnología hagamos y más tiempo invirtamos con dispositivos conectados a Internet, más expuestos estaremos a sus amenazas. Esto implica que:

- A día de hoy, el 65’6% ha sufrido alguna incidencia relacionada con el fraude.

- El 59’2% de los ordenadores alojan un malware en su interior.

- El 53’2% de los malware pasan desapercibidos por los usuarios.

Otros aspectos, como mezclar ámbitos en los dispositivos (familia, ocio, trabajo…) o que varios usuarios hagamos uso de diversos terminales bajo una única red y con diversos fines, nos conducen a estar más indefensos.

1.2.1. Cinco ciberamenazas globales

- *Malware*. Software específicamente diseñado para obtener acceso a un dispositivo o dañarlo sin conocimiento del propietario.
  - Minería de criptomonedas: 32%
  - Troyanos de acceso remoto 17%
  - Spyware: 13%
  - Botnets: 12%

- *Web-based attacks*. Técnicas que redirigen el tráfico desde navegadores web a sitios web maliciosos.
  - Procedencia: USA 46% | Holanda 26% | Alemania 5% | Francia 5%

- *Web application/injection attacks*. Alimentan servidores vulnerables y/o aplicaciones móviles con inputs maliciosos con el objetivo de inyectar código malicioso.
  - SQL Injection es el ataque más común: 51%.

- *Phishing*. Intento de robo/intercepción de nombres de usuario, contraseñas y credenciales mediante la combinación de emails y sitios web comprometidos.
  - Son responsables de más del 90% de las infecciones de malware y del 72% de las brechas de datos en organizaciones.
  - 88% es el crecimiento medio anual desde 2011 del número de ataques de phishing.

- *Ataques DDoS*. Denegación de denegación (distribuida) de servicio con objetivo en negocios y organizaciones volviendo indisponibles los sistemas de mailing o redes de los usuarios.
  - 59% de los ataques tienen lugar en China.
  - 55% de los ataques duran menos de 90 minutos.

Figura 2: Top 5 de ciberamenazas globales.

Fuente: ENISA

1.2.2. Otros indicadores

Algunos estudios realizados por entidades como DTEX muestran cómo, de 2020 a 2021, los incidentes de ciberamenazas aumentaron un 72%, cifra más que preocupante.

Allianz Global Corporate & Specialty, dedicada a la cobertura de seguros, informa de un crecimiento exponencial, año tras año, del número de demandas de cobertura de daños por ciberdelincuencia.

Ellos alegan que, aunque el precio medio por secuestro de información que solicitan los delicuentes sea de 5'3 millones de dólares, son su gestión las organizaciones están pagando "solamente" medio millón ($570.000).

1.3. Invirtiendo en el futuro: Programa Digital Europeo

Tabla 1: Inversión a través del Digital Europe Programme

ÁMBITO	INVERSIÓN [€]
Competencias digitales avanzadas	0'7 billion
Interoperabilidad y transformación digital	1'3 billion
Ciberseguridad	2 billion
Inteligencia artificial	2'5 billion
Computación de alto rendimiento	2'7 billion
TOTAL	**9'2 billion**

Fuente: Comisión Europea

Estos datos de los años 2019 a 2021 reflejan la gran inversión de Europa en avance tecnológico y su compromiso de afianzar las capacidades digitales en el futuro. Entre los países con más inversión, encontramos:

1. Alemania
2. Reino Unido

3. Francia
4. Italia
5. España

1.3.1. Plan Next Generation

Es gracias a esta inversión a nivel europeo como al ímpetu y la fuerza demostrados por España para mantenerse entre los países con más crecimiento (mayor que el de la media europea todos los años) de la inversión en tecnología lo que ha ocasionado que sea una gran beneficiaria del Plan de Recuperación, Transformación y Resiliencia.

En total, 564 millones de euros están destinados a INCIBE para poder cumplir todos los objetivos propuestos, siguiendo la línea europea en este sector. Un ejemplo es la digitalización básica de las PYMEs, con herramientas como el "Digital Toolkit", el bono de conectividad, el plan Protege tu empresa, el programa Acelera PYME…

En este sentido, estas inversiones sitúan al desarrollo tecnológico y la ciberseguridad como prioridades estratégicas de la Unión Europea, en el marco del impulso a la economía estratégica europea y dentro de un contexto internacional cambiante. La reconfiguración del mercado global conduce a la deslocalización del 70% de las mayores 500 empresas de ciberseguridad y la balanza global sitúa el péndulo cada vez más hacia Oriente entre los tres modelos predominantes: Estados Unidos, la Unión Europea y China.

1.4. INCIBE: Referencia en ciberseguridad para ciudadanos y sector privado en España

Desde INCIBE trabajamos en línea con un objetivo común: impulsar una economía y una sociedad más competitiva, más próspera y más resiliente. Lo hacemos desde la tecnología, el desarrollo de la confianza digital entre

ciudadanos y empresas y desde el humanismo digital: marca de identidad de nuestro Ministerio de Asuntos Económicos y Transformación Digital.

La actividad de INCIBE está alineada con el marco de seguridad nacional y basada y alineada con la agenda España Digital 2026, cuaderno de bitácora de la transformación digital española, a la que INCIBE contribuye en su eje tercero.

En este marco de referencia, y para hacer frente a los desafíos de ciberseguridad que tiene por delante la economía española, INCIBE cuenta con un **Plan Estratégico 2021-2025**, que está siendo la principal hoja de ruta con un objetivo muy claro: apoyar la transformación digital.

- El primer eje es el **fortalecimiento de las capacidades de ciberseguridad de ciudadanía y empresas**, con especial atención a menores, pymes, microempresas y profesionales, que en muchos casos no disponen de los recursos ni del conocimiento para protegerse frente a amenazas en el ciberespacio.

- El segundo eje es **el impulso al ecosistema de ciberseguridad** español para hacerlo más innovador y competitivo dentro y fuera de España a través 3 palancas:

  - el desarrollo de la **industria**, desde el emprendimiento en las fases más tempranas (incubación, aceleración) hasta la internacionalización;
  - el apoyo a la **I+D+i en ciberseguridad**, clave para generar las soluciones, productos y servicios necesarios en un mercado global y enormemente competitivo. Con iniciativas estratégicas como la Compra Pública Innovadora para fomentar el desarrollo de soluciones novedosas de ciberseguridad.
  - y la identificación, generación y desarrollo del **talento** necesario para consolidar las dos palancas anteriores.

- El tercer eje estratégico es el impulso de España como nodo internacional en seguridad digital. No hay que olvidar que la ciberseguridad es un **área transnacional donde la cooperación internacional es clave**.

Numerosas acciones en diversos programas y proyectos impulsados desde INCIBE contribuyen al desarrollo más seguro de los agentes en el entorno digital, contribuyendo al fortalecimiento de la economía española y su transformación digital.

QUO VADIS, INCIBE? DESAFÍOS EMERGENTES Y ALGUNAS PROPUESTAS DE ACCIÓN PARA FACILITAR RESILIENCIA Y PROSPERIDAD COMPARTIDA

Dr. Enrique López González
Académico de Número de la
Real Academia de Ciencias Económicas y Financieras

Todos los imperios del futuro serán imperios del conocimiento, y solamente los pueblos que entiendan cómo generar conocimiento y cómo protegerlo, cómo buscar jóvenes que tengan capacidad para hacerlo y asegurarse de que se queden en el país, serán países exitosos. Los otros, por más que tengan recursos materiales, materias primas diversas, litorales extensos, historias fantásticas, etc., probablemente no se queden ni con las mismas banderas, ni con las mismas fronteras, ni mucho menos con un éxito económico".

Albert Einstein

"España no alcanzará su pleno florecimiento cultural y político, mientras los docentes de todos los grados no acierten a fabricar en cantidad suficiente (hoy son centenas y sería precioso que sumasen centenares de miles), el español que nos hace falta, es decir, un tipo humano tan impersonal como abnegado, tan firme y entero de carácter, tan tolerante y abierto a todas las ideas, tan agudamente sensible a nuestros infortunios, que, reaccionando pujantemente contra las causas de nuestro atraso y de nuestros errores, consagrara lo mejor de sus energías y de sus luces a la prosperidad del país, al servicio del Estado y al enaltecimiento de la Nación. Hay que soñarla grande para que España sea grande".

Santiago Ramón y Cajal

1. Consideraciones previas: anécdota del título y descarga de responsabilidad.

En cuanto a la Anécdota del Título. En tiempos de Nerón, aquel emperador al que le gustaba aporrear el arpa y quemar ciudades, según relata el evangelio apócrifo de los "Hechos de Pedro", temeroso por lo que le podría

suceder, trata de huir de Roma por la Via Appia, pero en el camino se encuentra con Jesucristo. Hablamos del año 64, treinta y un años después de haber sido Cristo crucificado. Al verlo, Pedro le pregunta: *Quo Vadis, Domine?* (¿A dónde vas, señor?) Ojo, ¿a dónde vas? no en el sentido correctivo, de que se está equivocado. No, sino en el sentido de querer conocer. Su respuesta le hizo cambiar de opinión y regresar: "*Romam vado iterum crucifigi"* (Voy a Roma para ser crucificado de nuevo). Por tanto, al traer tal paremia al título de mi disertación, querría dejar claro el sentido y sensibilidad con el que está hecho, esto es, la total ausencia de arrogancia o, muy lejos en todo caso, de que ello pudiera suponer algún tipo de condicionamiento o, de alguna forma, que al incluir el acrónimo de INCIBE se pudiera interpretar una falta de respeto. Y solo valga la expresión como identificación de la marca como bandera de la ciberseguridad en España. Y también cabe mencionar que no tenía ningún deseo de poner la palabra ciberseguridad en el título. Confío en que comprenderán, cuando vaya avanzando el texto, la razón de esto.

Respecto al Descargo de Responsabilidad. Esta exposición no ha sido debatida en el seno de la RACEF, ni siquiera ha sido elevada como ponencia de estudio para su consideración en nuestra Real Corporación. Ya saben ustedes cómo son los debates entre académicos cuando se trata "solo de una tilde", lo que les quiero hacer suponer cuando se aborda algo que tiene impacto económico. Por tanto, eximo totalmente a la RACEF de aquellas posibles aseveraciones, recomendaciones o posibles interpretaciones versadas en la disertación cuya responsabilidad solo a mí me compete.

2. ¿De dónde venimos? El nacimiento del INCIBE.

La cita de Einstein de los años cuarenta del siglo pasado que copa el presente trabajo, además de evidenciar su avizorada visión de futuro, denota a las claras la realidad del mundo que ahora conocemos; así, al vaticinar que en la nueva «sociedad del conocimiento» el activo más importante de un país serían precisamente sus habitantes, anticipo la importancia estratégica y cada vez más que adquiriría para un país el contar con ciudadanos debidamente educa-

dos, con capacidad de convertirse en agentes de cambio económico y social en un contexto de trabajo global, altamente competitivo, basado en la tecnología, rápidamente cambiante y, sobre todo, basado en el dominio del conocimiento desde una perspectiva internacional, en coherencia a su vez con lo mencionado por Ramón y Cajal veinte años antes, con motivo del Discurso leído el día 7 de mayo de 1922 en la solemne sesión Real Academia de Ciencias Exactas, Físicas y Naturales celebrada bajo la presidencia de S. M. El Rey D. Alfonso XIII, para la entrega de la Medalla Echegaray.

Traer a colación tales citas en el frontispicio de esta disertación, se justifica por la carga motivadora de las mismas, porque bajo su inspiración es posible responder a preguntas en apariencia sencillas: ¿Queremos que la economía de la Provincia de León sea competitiva y con un crecimiento económico sostenible e inclusivo, esto es, que pueda gozar de un alto grado de prosperidad compartida? Las posibles respuestas sin duda tendrán un gran impacto en nuestros estudiantes, constituyendo a su vez la semilla prístina del nacimiento del INCIBE, esto es, el surgimiento de la institucionalidad pública a nivel nacional de la ciberseguridad.

El INCIBE es un instituto nacional que tiene su sede en León, se trata de una estrategia de descentralización después de una promesa electoral. ¿Cómo nace el INCIBE? Permítanme que me refiera a ello desde mi perspectiva personal, dada mi implicación en dicho acontecer.

Realmente el primer punto para comprender el advenimiento del INCIBE es después de la huelga general de 1991 en León, una huelga que como decía la portada del 16 de mayo de 1991 del Diario de León: “todos somos culpables” (Ver Imagen 1). Entonces se creó una Mesa de Trabajo para formular desafíos y propuestas, donde participó como representante del partido socialista leonés su secretario provincial, D. José Luis Rodríguez Zapatero, que como es conocido fue el principal dinamizador de la existencia del INCIBE.

Imagen 1

Por mi parte, tengo que mencionar que mi participación en la Mesa Técnica, como director entonces de la Oficina de Transferencia de los Resultados de Investigación de la Universidad de León, me facilitó una línea directa en la elaboración de alguna de las propuestas que de allí surgieron y, sin duda, tal actividad ha marcado indeleblemente parte de mi carrera como servidor público.

Algunos de los que conocían el León entonces recordarán que, por ejemplo, al lado de San Marcos, donde pasaba una carretera nacional, cruzando el puente romano colindante y a escasos 40 metros de su puerta principal, había una gasolinera y todo lo que existia detrás era un cascajal, constituyendo el límite de la ciudad.

No han faltado voces que cuestionaron para qué sirvió esto. Pues, al menos, cabe suponer que sirvió para ensanchar León, para abrir Onzonilla como Polígono Industrial, a la par de otros adyacentes como los de Torneros o Villadangos, y el surgimiento del actual Polígono Tecnológico, esto es, para generar una serie de temas de funcionamiento económico anquilosado y hacer la ciudad que hoy conocemos.

¿Cuál era la fotografía económica de León en la década de los noventa del siglo pasado? Una "en blanco y negro" (Pérez Chencho, *dixit*). Aquella era una foto de una economía que se basaba estrictamente en la remolacha y en la minería, algo que amarilleaba, que ya probablemente iba a desaparecer.

Para los efectos de esta exposición, también cabe mencionar que quizás uno de los hitos que marcó la dinámica de trabajo con impacto en el objeto de nuestra consideración, fue asumir la responsabilidad de organizar y desarrollar el Congreso ITHURS'96, cuya presidencia científica residió precisamente en el Prof. Dr. Jaime Gil Aluja. Se trataba de un Congreso Internacional de ciencias y tecnologías inteligentes relacionadas con los humanos. Un gran Congreso pionero en la utilización de internet. Probablemente fue el primer gran encuentro científico que hubo en León por la afluencia de más de 600 investigadores de más de 40 países. Aquel fue un Congreso que para poder llevarlo contamos con la operatividad de conexión en Internet de la EPFL de Lausanne, donde uno de los colaboradores que nosotros teníamos era profesor Teodorescu. De esta forma, pudimos desarrollar iniciativas de comunicación telemática nunca vistas antes en España y que entonces, por su ausencia en nuestra alma Mater, la conexión digital se realizó gracias a la colaboración con la plataforma Gugu de la Universidad de Salamanca. Así, Internet, la cuna de la digitalización, nos permitió llegar donde antes no había llegado ningún otro evento académico parecido por estas lindes.

Otro hito muy significativo, aunque quizás poco conocido, radica en que como motivo del centenario de la revista Tierras de León, editada por la Diputación Provincial, me solicitan participar en dicho número con un trabajo sobre la economía local titulado "Retrospectiva y perspectiva de la economía leonesa. ¿Hacia la Sociedad de la Información?"[1]. En este trabajo hacía un alegato fundamental ("Leoneses, ¡al Internet!") y establecía una acción en-

1 López González, E. (1996). Retrospectiva y perspectiva de la economía leonesa. ¿Hacia la Sociedad de la Información? Revista tierras de León, nº 100, págs. 35-50.

tonces disruptiva para el futuro de León: frente a la idea de que abundar en una economía que está en sus horas bajas, despoblándose a raudales, el "todo León" podría apostar por la creación de un "Instituto de Investigación en Tecnologías de Información y Comunicación Avanzadas (INTECO)".

En mi contribución sobrevolaba la idea de la necesidad imperiosa de disponer de un cierto tejido empresarial vinculado a "las tecnologías que vienen", para catalizar que los estudiantes de la Universidad de León no tuvieran que migrar como imperativo de futuro personal, tal como rezaban las citas de Einstein y Ramón y Cajal. Entonces, sencillamente, se planteó que, al disponer de tal hub o infraestructura tecnológica, podría ser posible que en el futuro tuviera una cierta viabilidad económica, se abriese una ventana de oportunidad que otros territorios ni siquiera avizoraban en ese momento, basada en la idea, que venía del mundo anglosajón, acerca de que eran "los clicks y no los bricks" los que definirían un futuro de prosperidad compartida, basada en el tránsito de una "economía de bits" hacia a una "economía de átomos", que tres décadas después es la condición (llámese transformación digital o argocapitalismo) de las economías competitivas y donde la ciberseguridad deja de ser una opción empresarial para convertirse en un imperativo.

Con todo, dicho desiderátum se tornó en realidad gracias al compromiso electoral que se puede ver en la portada del Diario de León del 23 de mayo de 2003 (Ver Imagen 2), en la que, haciéndose eco de la relevancia de la propuesta, el entonces ya secretario general del Partido Socialista de España, prometía crear en León, si ganaban las elecciones, el Instituto Nacional de la Comunicación. De hecho, hablaba de convertir la provincia leonesa en referencia del cambio tecnológico nacional. Esta promesa se concluyó en el consejo de ministros de 29 de abril de 2005, de forma que, posteriormente, en el consejo de ministros de 21 de diciembre de 2007, se creó la Oficina de Seguridad del Internauta. Desde entonces, su historia es pública y notoria y su actual director, el Dr. Barrio Juaréz, nos acaba de ilustrar, con detalle pedagógico, su funcionamiento como baluarte de la ciberseguridad en España.

Imagen 2


Diario de León

Zapatero: «Voy a dejarme la piel por esta provincia»

3. ¿Dónde estamos?

3.1. Sociedad 5.0 (argocapitalismo)

En el último Mobile World Congress, el mayor evento relacionado con la tecnología y la movilidad, que se celebró en Barcelona del 27 de febrero al 2 de marzo de 2023, el CEO de la Telefónica Alemana nos explayó la Imagen 3, donde decía que el campo de juego era muy asimétrico y donde el papel de Europa era bastante escaso. De hecho, recordaba que Europa no es un país competitivo en el espacio digital (Ver Imagen 4), pues el 92% de las bases de datos del mundo occidental estaba en territorio norteamericano, es decir, esto que hablamos de la nube, tal nube se encuentra en las profundidades de unas minas subterráneas de Estados Unidos.

Imagen 3

Imagen 4

¿Qué dice la Comunidad Económica Europea al respecto? Fíjense, no hace mucho, el pasado 13 de febrero (Ver Imagen 5) nos recuerda que estamos en tiempos de megatendencias disruptivas y que la tecnología está cambiando tanto la naturaleza como la velocidad de los descubrimientos científicos, lo que va a permitir transformar los sistemas de producción, gestión y gobernanza, pero, también, incluso, cómo aprendemos, cómo socializamos y cómo trabajamos. En definitiva, nos da una voz de alerta de algo que ya todos estamos viviendo intensamente.

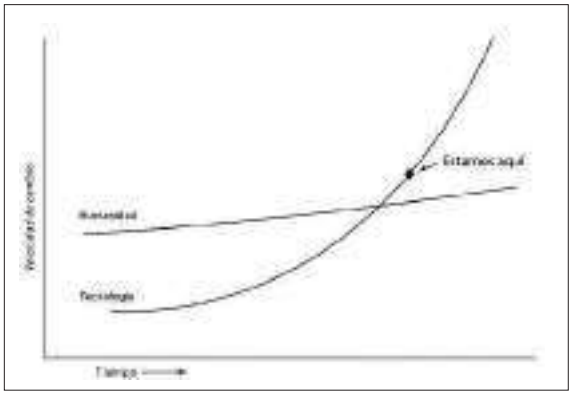
Imagen 5

Y es que la tecnología se está acelerando más rápida que nuestra capacidad, incluso, de adaptación o de comprensión. ¿Esto qué significa? Que el comportamiento humano presenta un crecimiento que se podría calificar de casi logarítmico frente a un crecimiento de tecnología de carácter exponencial.

Un ejemplo de la incapacidad para converger el movimiento tecnológico exponencial con el aprendizaje humano logarítmico se puede encontrar en un vídeo con la intervención de Thomas Friedman, periodista norteamericano merecedor de varios premios Pulitzer, el 2 de agosto de 2017 en el Resnick Aspen Action Forum, donde explicó que las bases para adaptarse al rápido cambio tecnológico están establecidas: "el futuro de la humanidad dependerá de nuestra capacidad para adaptarnos y trabajar con la tecnología y el camino hacia este objetivo es el aprendizaje permanente".

Friedman obtuvo esta idea gracias a una entrevista con Astro Teller, de Google X, mientras investigaba para su nuevo libro "*Gracias por llegar tarde: una guía optimista para prosperar en la era de la aceleración"*. Teller dibujó a Friedman un gráfico (Ver Imagen 6) que mostraba la tasa de adaptación humana frente a la tasa de cambio tecnológico a lo largo del tiempo y dónde nos encontramos "ahora", en este punto de la historia: "estamos aquí"[2].

Imagen 6 [3]



2 https://www.youtube.com/watch?v=9WmWnIdhbq4
https://news.mit.edu/2018/thomas-friedman-impact-global-accelerations-1003

3 Thomas L. Friedman (2018). "Gracias por llegar tarde. Cómo la tecnología, la globalización y el cambio climático van a transformar el mundo los próximos años". Deusto, pág. 25

Como sigue comentando Friedman: "Ese punto, explicó Teller, ilustra un hecho importante: a pesar de que los seres humanos y las sociedades se han adaptado paulatinamente a los cambios, de promedio la velocidad del cambio tecnológico está acelerándose tanto que ha subido por encima de la velocidad promedio a la que la mayoría de las personas pueden asimilar todos esos cambios. Muchos de nosotros no podemos seguir el ritmo…. Esto es un verdadero problema. Cuando la velocidad se incrementa, el hecho de tardar más en adaptarte te convierte en lento… y te desorienta. Es como si todos estuviéramos en uno de esos pasillos mecánicos del aeropuerto que va a ocho kilómetros por hora y de repente fuera a cuarenta kilómetros por hora, aunque todo lo demás a tu alrededor permaneciera más a menos igual. Para mucha gente, esto resulta sorprendente… Si para la sociedad la plataforma tecnológica puede actualmente cambiar en un plazo de entre cinco y siete años, pero tardamos entre diez y quince en adaptarnos, todos tendremos la sensación de haber perdido el control, porque no somos capaces de adaptarnos al mundo a la velocidad en la que éste está cambiando. Cuando nos hayamos acostumbrado al cambio, ese cambio ya ni siquiera será el predominante, ya estaremos inmersos en otro nuevo".

Al objeto de comprender la dinámica exponencial que caracteriza de forma consustancial a la digitalización, una parábola explicativa del vertiginoso ritmo de crecimiento es posible encontrarla en el símil de la carrera de la Reina Roja del maravilloso libro de Lewis Carroll "A través del espejo y lo que Alicia encontró allí" (1872) que en su capítulo 2, titulado "El jardín de las flores vivas" (se trata de un jardín que, en palabras de Alicia, "está trazado exactamente como un gran tablero de ajedrez" [4], esto es, el mayor tótem de los estudiosos de la función exponencial), se presenta a la protagonista cogida de la mano de la Reina Roja para poder correr las dos a través de las casillas de ajedrez. Alicia zozobra al ver que, aunque marchan muy veloces, prácticamente no se han movido de donde estaban (Ver Imagen 7).

4 Cabe destacar que dicho jardín, donde transcurre la historia, en palabras de Alicia, "está trazado exactamente como un gran tablero de ajedrez" (el mayor tótem de los estudiosos de la función exponencial).

Imagen 7 [5]

El famoso diálogo entre Alicia y la Reina Roja es como sigue:

> La Reina Roja seguía gritando: "¡Deprisa, más deprisa!", pero Alicia sentía que no podía correr más, aunque estaba sin aliento y no podía decírselo. Lo más curioso era que los árboles y las cosas que tenían a su alrededor no cambiaban de lugar: por deprisa que corrieran, no parecían dejar nada atrás. "¿Se moverán las cosas a la vez que nosotras?", pensó la pobre Alicia, perpleja. […] Alicia miró en torno suyo, muy sorprendida.
>
> "¡Vaya, para mí que todo el tiempo hemos estado bajo este árbol! ¡Todo es igual que antes!"
>
> "¡Naturalmente!" -dijo la Reina-. "Pues ¿cómo querías que fuera?"
>
> "Bueno, en mi país -dijo Alicia, jadeando todavía un poco- "habríamos llegado a algún sitio … si hubiésemos estado corriendo deprisísima tanto tiempo, como hemos corrido aquí".
>
> "¡Pues sí que es lento ese país!" -dijo la Reina-. "Aquí, como ves, necesitas correr con todas tus fuerzas para permanecer en el mismo sitio. Si quieres ir a otra parte, tienes que correr lo menos el doble de rápido".

El *"principio o hipótesis de la Reina Roja"* vio la luz por primera vez en 1973 de la mano del biólogo evolucionista Leigh Van Valen, que utilizó la alegoría de la carrera de la Reina Roja de Carroll para hacer referencia a una teoría sobre la evolución que describe la necesaria mejora continua de las especies con el único fin de mantener el *statu quo* con su entorno. En términos

5 Fuente: https://www.scylladb.com/wp-content/uploads/800x400-blog-redqueen.jpg

evolutivos, se expresa así: *"Para un sistema evolutivo, la mejora continua es necesaria sólo para mantener su ajuste a los sistemas con los que está co-evolucionando"*[6].

La exhortación entonces de la Reina Roja bien pudiera ser que como humanos deberíamos repensar o desaprender lo que sabemos y funcionar de forma diferente, máxime cuando gracias a la infraestructura libre de fricción que conlleva la digitalización, la distancia entre una idea y su realización digital nunca antes resultó tan corta. El problema radica en que, en general, las organizaciones, las personas que las dirigen, no están avezadas para lidiar con el cambio acelerado que es causado por las "*curvas de aprendizaje*". Y, para complicar aún más la situación, un ingrediente añadido en la sopa de la confusión, conviene tener en consideración el impacto de nuestros sesgos cognitivos, auténticas alcantarillas abiertas en las avenidas de nuestro pensamiento. Así lo acreditan las enseñanzas de los trabajos de los psicólogos Amos Tversky y Daniel Kahneman, que en 1972 desarrollaron la denominada *"teoría de la perspectiva"* (*prospect theory*) [7], según la cual los individuos toman decisiones que se apartan de los principios básicos de la probabilidad. Con el fin de tomar decisiones rápidas de utilidad para nuestro devenir, en repetidas ocasiones las personas tomamos los mismos atajos mentales, denominados *"heurísticas"*. Nuestra propia experiencia nos hace obstinados sobre el futuro. Cimentamos nuestras ideas sobre el mundo en nuestra experiencia personal, la cual ha arraigado una tasa de crecimiento de los últimos años en nuestras cabezas como "*la forma en que las cosas sucedan*". Pero, cuando nos encontramos ante situaciones que crecen exponencialmente, la simple extrapolación lineal puede no ser adecuada.

Quizás una de las causas de la confusión que plantea el crecimiento exponencial pudiera ser debida a que, en general, los humanos no estamos muy duchos para discernir los cambios disruptivos que el comportamiento exponencial conlleva. Albert Bartlett nos recuerda que ésta es una de las mayores

6 Van Valen, L. (1973). A New Evolutionary Law. Evolutionary Theory (1):1-30.

7 Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science (185):1124–1131. Doi 10.1126/science.185.4157.1124

incapacidades de los humanos[8], pues, nos olvidamos fácilmente de que el crecimiento en un tiempo necesario para doblarse es siempre mayor que todos los crecimientos anteriores juntos.

A modo de ejemplo descriptivo, imagínense que introducimos en una botella de cristal transparente, de una capacidad de un litro, una microscópica bacteria esmeralda, cuya única virtud o actividad, a nuestros efectos, radica en desdoblarse cada minuto y que, por evidencias previas, se conoce que en exactamente una hora la botella se llena totalmente hasta casi rebosar con una coloración menta. Pues bien, al cabo de media hora, ¿cómo luciría de matiz oliva la botella? ¿por la mitad, o acaso, sería casi imperceptible, un tenue deje alcachofa? ¿Cuándo acontece que la botella está medio llena, en el minuto 30 o en el 59? Resulta lógico pensar que a la media hora casi difícilmente se vislumbra más que un tono pálido lima, todavía se necesita otro tanto de tiempo para que media botella luzca jade. Si la mitad de la capacidad de la botella se alcanza a los 59 minutos. Un minuto antes, sólo habría 250 mls de helecho, en el minuto 57 tan sólo 125 mls, etc. En tal experimento hay que esperar (sin cambios perceptibles a simple vista) durante 50 minutos para avizorar una variación en la tonalidad. A mayores, en nuestro ejemplo, aunque se necesitaron 59 minutos para alcanzar la mitad de la botella, dada su "exponencialidad", si hubiera cerca otras tres botellas vacías, sólo se precisan tres minutos más para que las cuatro rebosaran de una irisación selvática radiante.

Tal comportamiento recuerda a un palo de hockey: sólo después de un largo 'letargo', zás, se eleva exponencialmente, como el interés compuesto o el maligno SARS-CoV-2. Otro ejemplo, aunque en la literatura de ficción, también se puede encontrar en la novela "Fiesta" (*The Sun Also Rises*) de Ernest Hemingway [9], su primera y muy reconocida en la pequeña ecúmene de nuestra piel de toro. En el texto, Mike, uno de los personajes protagónicos, relata que su bancarrota ocurrió de dos maneras: "*gradualmente y luego de repente*".

8 http://www.albartlett.org/presentations/arithmetic_population_energy_transcript_spanish.html

9 Hemingway, E. (2003). Fiesta. Debolsillo.

¿Cómo se puede abordar esta situación de crecimiento exponencial a nivel global? Pues, básicamente, en el mundo, es el gobierno japonés quien ha marcado cuál es, digamos, no la utopía, pero sí dónde está la frontera hacia la que deberemos aspirar, la sociedad 5.0. Sencillamente, se inspiran en el humanismo tecnológico del que hemos hablado esta semana en Salamanca, al plantear que se necesita hacer que la tecnología se enfoque en "los humanos primero".

En los últimos años, Japón ha ido desarrollando el concepto de Sociedad 5.0 para resolver sus propios problemas como el envejecimiento, la natalidad y la competitividad. En Japón ya se venden más pañales para adultos que para niños y su natalidad no compensa el incremento del envejecimiento, lo cual supone un descenso significativo de la mano de obra y el aumento de los costes médicos y de seguridad social. De esta forma, el gobierno japonés pretende aprovechar los avances tecnológicos para construir un país y un mundo mejor, donde todos puedan disfrutar de una alta calidad de vida y que nadie se quede atrás. Se trata, por tanto, de un primer experimento mundial, con objeto de que sea seguido por otros, pues el resto de países desarrollados están llegando a ese punto, si bien Japón lo está haciendo más deprisa que otros y supone para el mismo un gran desafío y al mismo tiempo una gran oportunidad.

El concepto de Sociedad 5.0 fue propuesto por primera vez en 2015, en el Quinto Plan Básico de Ciencia y Tecnología por el gobierno japonés como una sociedad futura a la que Japón debería aspirar, esto es, el próximo nivel de desarrollo tecnológico en el recorrido épico de la humanidad: Sigue a la sociedad de la caza (Sociedad 1.0), la sociedad agrícola (Sociedad 2.0), la sociedad industrial (Sociedad 3.0) y la sociedad de la información (Sociedad 4.0). Posteriormente, fue anunciado al mundo por el ministro japonés Shinzo Abe (asesinado el 8 de julio de 2022) en su discurso "Declaración de Hannover" en la conferencia CeBIT 2017 en Hannover, Alemania[10].: "…Ha llegado un importante punto de inflexión en la historia de la humanidad. En tiempos

10 http://www.japan.go.jp/letters/ebook56/book.pdf

prehistóricos, nos adentramos en el bosque para cazar. Si ese es el primer capítulo de la historia humana, entonces el segundo es cuando logramos asegurar un número estable de calorías alimentarias en forma de arroz y trigo. El telón se levantó en el capítulo tres cuando llegaron oleadas de industrialización en lo que llamamos tiempos modernos. El capítulo cuatro vio las telecomunicaciones y las computadoras fusionarse, abriendo una nueva puerta. Estamos asistiendo ahora al inicio del quinto capítulo, cuando podemos encontrar soluciones a problemas que no habíamos podido resolver. Esta era en la que todas las cosas están conectadas y todas las tecnologías se fusionan, catalizando el advenimiento de la 'Sociedad 5.0'…"

Según la literatura del gobierno japonés, la Sociedad 5.0 debería ser una que, a través del alto grado de fusión entre el ciberespacio y el espacio físico (digitalización), pueda equilibrar el avance económico con la resolución de problemas sociales, al proporcionar bienes y servicios que aborden de manera granular múltiples necesidades independientemente del lugar, la edad, el sexo o el idioma. Por tanto, la Sociedad 5.0 es una sociedad centrada en el ser humano que equilibra el avance económico y tecnológico para resolver los problemas de la sociedad con sistemas de datos superinteligentes. Representa una nueva visión para una sociedad más inteligente, donde los seres humanos, la naturaleza y la tecnología crean un equilibrio sostenible mejorado por los datos.

En Europa, bajo una clara ascendencia germánica, en lugar de hablar de Sociedad 5.0, se ha preferido utilizar la expresión "Industria 5.0". Eso sí, dejando bien claro que hay tres líneas de acción, tres fuentes, tres pilares en los que se soporta. En primer término, el humanismo tecnológico, pero también que debe de ser resiliente a la par que sostenible. Y estas son las dos palabras que probablemente encontraremos con asiduidad en nuestro vocabulario para denotar los dos desafíos principales sobre cómo vamos a enfocar el mundo en este momento de la historia, esto es, hacia la Sociedad 5.0.

Uno es la ecologización de la economía. Esto es irreversible, ya no caben ambigüedades negacionistas ni lavados verdes engañosos. Se precisa dar respuesta al capitaloceno de una manera explícita. La pregunta es si esta generación podrá ver el fin de la combustión, pues, si las tecnologías energéticas no se desfosilizan en esta generación, tendremos problemas muy serios, poniendo en peligro que podamos legar nuestro medio ambiente en un estado mejor de lo que lo encontramos. Y entonces los nietos de muchos de ustedes tendrán problemas más serios y malignos que los actuales que nos toca lidiar.

Además, existe otro desafío, el otro gran dilema es la digitalización de la economía. La transformación digital de la economía radica, por resumirlo también en una sola palabra, simplemente en dar respuesta al argocapitalismo, esto es, el sistema económico propio de la digitalización. El argocapitalismo se basa en la acumulación de datos sí o sí, esto es, la acumulación de los datos como imperativo, entendiendo los datos como una forma de capital.

A este respecto, cabe señalar la tribuna de The New York Times del pasado 27 de febrero, cuando se plantea cuál es el verdadero peligro inminente de la inteligencia artificial, Ezra Klein hace una entrevista a Ted Chiang, un conocido escritor de novelas de ciencia ficción, y le contesta que el mayor temor que hay es la ansiedad por la forma en que el capitalismo afectará de alguna forma nuestra tecnología y nuestra forma de vida (Ver Imagen 8).

Imagen 8


The New York Times

El verdadero peligro inminente de la inteligencia artificial

Como es conocido, la "digitalización"[11], entendida como la continua convergencia (fusión) de lo real y el mundo virtual, es uno de los principales motores de alteridad que ha transformado la forma en que interactuamos con nuestro entorno. La digitalización tiene el potencial de transmutar radicalmente la ciencia, la sociedad o la economía donde, cada vez más, las instituciones son sustituidas por la negociación algorítmica. En efecto, la digitalización constituye la principal fuerza impulsora de la innovación y la radical mudanza acontecida en la economía política en este inicio de Siglo XXI, lo que va mucho más allá de la observación de van Dijk, acerca de que "por primera vez en la historia tenemos una única infraestructura de comunicaciones que enlaza todas las actividades en la sociedad"[12].

La digitalización tiene el potencial de transformar radicalmente la ciencia, la sociedad, la economía y todas nuestras instituciones actuales[13]: la manera en que educamos (educación personalizada), o investigamos (análisis predictivo de datos masivos), cómo nos movemos (coche sin conductor), la forma

11 Lamentablemente nuestro Diccionario de la Real Academia de la Lengua de España (RAE) registra la palabra digitalización como «acción y efecto de digitalizar» y, a su vez, la palabra digitalizar como «expresar datos en forma digital», mientras que el Diccionario Inglés de Oxford (OED) si difiere explícitamente, dado el valor analítico fundamental que tal distinción conlleva, los términos "digitization" y "digitalization". En el OED, la "digitization" hace referencia a "la acción o el proceso de "digitizing": "la conversión de datos analógicos (ya sean imágenes, vídeo o texto) en forma digital". "Digitalization", por el contrario, se refiere a "la adopción o el aumento en el uso de la tecnología digital o el ordenador por una organización, la industria, el país, etc.". Dos letras marcan una diferencia sustancial. La digitalización va más allá de la digitización, al aprovechar la tecnología de información digital para transformar por completo los procesos de un negocio o actividad: evaluar, reingeniería y reimaginar la forma en que se genera valor. Esto es, la digitización es una conversión de datos y procesos, la digitalización es una transformación, el proceso de pasar a un negocio o actividad digital. La digitalización, además de digitizar los datos existentes, abarca la capacidad de la tecnología digital para recopilar datos, establecer tendencias y tomar mejores decisiones. Así, por ejemplo, un documento, una fotografía, se puede digitizar mientras que una fábrica se puede digitalizar.

12 Van Dijck, J. (2005). *The Network Society: Social Aspects of New Media*, Sage. Newbury Park, p. 46.

13 López González, E. (2018). *Hic Sunt Leones': el futuro del dinero. De la digitalización a la tokenización de la economía.* Real Academia de Ciencias Económicas y Financieras, Barcelona, p. 12. Accesible en https://racef.es/archivos/discursos/247_18.pdf

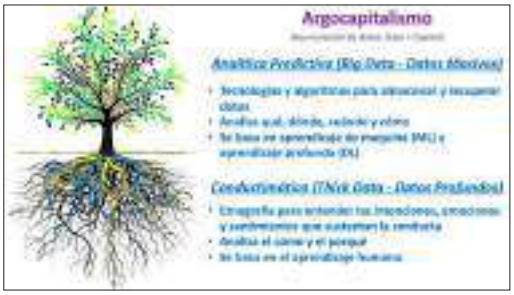
en que producimos (fabricación aditiva), cómo vamos de compras, cómo buscamos empleo o viajamos. Pero también su influencia se percibe en cómo podemos prever el clima o movimientos sísmicos (polvo inteligente), cómo nos curamos (medicina personalizada) e, incluso, en la política (participación ciudadana) y también en el conjunto de la economía. De hecho, la digitalización plantea la emergencia de un nuevo orden económico, que me he atrevido a denominar "Argocapitalismo"[14] entendido como toda la serie de cambios culturales, laborales y de tecnología profundos y coordinados que permiten nuevos modelos operativos basados en datos que transforman las operaciones, la dirección estratégica y la propuesta de valor meta-personalizada de una institución (Ver Imagen 9).

Imagen 9

A tenor de lo anterior, se hace imperativo tratar de contestar a la pregunta ¿cómo funciona la economía impulsada por datos propia del argocapitalismo? La respuesta cabe circunscribirla básicamente a la gestión de dos herramientas fundamentales; por un lado, la "analítica predictiva", basada en tecnologías de aprendizaje profundo (inteligencia artificial y datos masivos), para interesarse por saber qué, dónde, cuándo y cómo ocurren las cosas, pero también utiliza la "conductimática", basada en técnicas etnográficas con datos profundos, para saber el cómo y el por qué (Ver Imagen 10).

14 López González, E. (2020). *El argocapitalismo en la era del acercamiento digital.* Real Academia de Ciencias Económicas y Financieras, Barcelona. Accesible en https://racef.es/archivos/discursos/discurso_ingreso_dr._enrique_lopez_2020.pdf

Imagen 10



Si hay algo que diferencia particularmente a los argocapitalistas es su apuesta por conocer a sus usuarios: grabar cada acción, cada huella de la acción digital de los usuarios, junto con las metodologías de Big Data y análisis predictivos de datos, se presentan como el santo grial tecnológico que permitirá a los responsables de gestión pronosticar con precisión las demandas de los consumidores, mejorar la prestación de servicios al cliente, aumentar el valor del cliente y aumentar y liderar la cuota de participación de mercado.

No obstante, si bien ese enfoque puede proporcionar imágenes asombrosamente detalladas de algunos aspectos de sus mercados, tales retratos están lejos de ser completos, ya que es posible predecir el próximo clic o la compra de un cliente, pero difícilmente ninguna cantidad de datos cuantitativos puede decir por qué hizo ese clic o compra. Sin tal información, las empresas no pueden cerrar la brecha de complejidad. Esto es, en la prisa por reducir a los consumidores a cadenas de unos y ceros se puede perder de vista el factor humano. Los consumidores son personas, después de todo, cuyo comportamiento a menudo pudiera calificarse de irracional.

Por tanto, las empresas necesitan también datos profundos, necesitan saber cómo un producto o servicio encaja en la vida emocional de sus clientes. En esencia, todo negocio consiste en apostar por el comportamiento humano. Se trata de conocer lo que las personas hacen, pero también es oportuno estar al tanto de por qué lo hacen. ¿Qué producto es más probable que se venda,

qué empleado es más probable que tenga éxito, qué precio está dispuesto a pagar un cliente? Las empresas que despuntan en hacer este tipo de "apuestas" tienden a progresar en el mercado, mientras que la falta de conocimiento del cliente es asumida generalmente como uno de los mayores déficits en la gestión de la complejidad. No es extraño que los responsables de gestión prioricen la obtención de conocimientos del cliente muy por encima de otras tareas relacionadas con la toma de decisiones. Incluso, la "obsesión por el cliente" es comúnmente clasificada como el rasgo de liderazgo más crítico.

En resumen, resulta de fácil generalización asumir que los argocapitalistas, a través de su refinería de datos, saben, o intentan saber, cosas sobre los usuarios o consumidores que ni siquiera ellos conocen o se imaginan de sí mismos, inspirados en la "metapersonalización basada en datos", dando lugar a una nueva identidad táctica: Argocapitalismo = BaT Data (Big Data + Thick Data).

3.2. Mundo VUCA (permacrisis y resiliencia)

¿Cuál fue la palabra que escogió el diccionario británico Collins como como exponente de mayor representación del año 2022? (Ver Imagen 11)

Imagen 11

El diccionario Collins se decidió por "permacrisis", esto es, un periodo prolongado de inestabilidad e inseguridad, especialmente como resultado de una serie de eventos catastróficos. Somos legión para los que tal expresión es representativa del status quo del año 2022, si nos atenemos a la panoplia de elementos catastróficos, sindemia, calentamiento global, invasión deleznable de la guerra de Ucrania, recesiones, terrorismo, populismo, guerras comerciales, ciberseguridad, desigualdad, migración, polarización. Estos desafíos están en el orden del día, no es algo circunstancial. Es la nueva normalidad, la realidad que estamos viviendo.

Esta nueva normalidad caracteriza a este mundo denominado con el acrónimo "VUCA", por la volatilidad, la incertidumbre, la complejidad y la ambigüedad. En definitiva, se trata de un mundo que no es nada gaussiano, no es nada estable, no es nada lineal. Un mundo en el que constantemente están surgiendo nuevas oportunidades y eso significa también nuevas amenazas, día a día, con un enorme impacto en el proceso de toma de decisiones (Ver Imagen 12).

Imagen 12

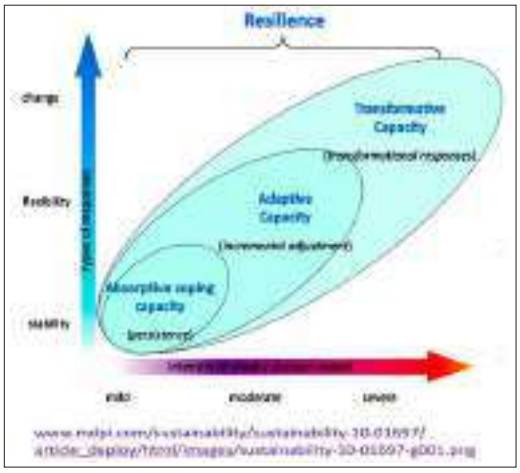
En este mundo actual, para poder sobrevivir y prosperar en esta era de permacrisis, se necesita adaptarse, transformarse, aprender, mejorar, innovar,

diferenciarse, anticiparse, responder, colaborar y cocrear, esto es, lo que ya los romanos de hace 20 siglos decían aquello de "poder rebotar, poder saltar para atrás, poder esquivar los golpes", lo que denominaban en latín *resilio* o r*esiliere*. La resiliencia es el proceso de adaptarse bien a la adversidad, a los traumas, a las tragedias, a las amenazas, a las fuentes de tensión significativas, de recuperarse de las adversidades y de salir fortalecido de ellas. No se trata simplemente de ser optimista *per se*, sino de estar bien informado.

¿Cómo desarrollar entonces la resiliencia empresarial? En este momento, la fórmula magistral de la competitividad, la salsa secreta, consiste en transformarse digitalmente. Eso sí, la digitalización tiene una exigencia directa, la ciberresiliencia (resiliencia cibernética). Sí, han escuchado ustedes bien, ciberresiliencia, no ciberseguridad.

En términos conceptuales, ¿qué podemos entender entonces por resiliencia? Pues, básicamente tres acciones en función del impacto y la gravedad que pueda haber, de que simplemente absorbamos el golpe, podamos adaptarnos a ese golpe e, incluso, pudiéramos transformarnos ante esa adversidad y renacer, por así decirlo (Ver Imagen 13)

Imagen 13



De acuerdo con Béné, Cornelius y Howland (2018) cabe entender la resiliencia como una combinación de 3 capacidades diferentes pero complementarias[15]:

- Capacidades de absorción: desarrollar y adoptar estrategias de supervivencia para moderar o amortiguar los impactos directos a corto plazo de las crisis.

- Capacidades adaptativas: los cambios y adaptaciones incrementales que se experimentan para seguir funcionando en respuesta a un shock o a un estrés creciente, sin realizar cambios cualitativos importantes en la forma en que operan normalmente.

- Capacidades transformadoras: las respuestas y estrategias que apuntan a alterar de forma permanente y drástica la estructura o el funcionamiento a fin de asegurar la 'supervivencia' a largo plazo.

3.3. Impacto en la ciberseguridad

Bien, a tenor de lo comentado, ¿cómo impactan estas ideas entonces en la ciberseguridad? ¿Qué está ocurriendo en la ciberseguridad a nivel global?

Un primer referente lo podemos encontrar en el informe del *FBI* norteamericano[16] que, desde hace cinco años, termina o concluye con una idea muy clarividente: "cada año está peor".

De forma más detallada, cabe destacar el informe "Almanaque De Ciberseguridad 2023: 100 Hechos, Cifras, Predicciones y Estadísticas" de la revista

15 Béné, Ch., Cornelius, A. y Howland, F. (2018). Bridging Humanitarian Responses and Long-Term Development through Transformative Changes—Some Initial Reflections from the World Bank's Adaptive Social Protection Program in the Sahel. Sustainability 2018, 10(6), 1697; https://doi.org/10.3390/su10061697

16 Federal Bureau of Investigation (2021) Internet Crime Report 2021, accessible en www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

"*Cybercrime Magazine*" que se publicó el 24 de mayo de 2023[17] (que supone una actualización respecto de lo que se comentó en la exposición oral) donde se pormenorizan las estadísticas e información más actuales para comprender el cibercrimen y el mercado de la ciberseguridad a nivel mundial, a saber:

DAÑOS POR DELITO CIBERNÉTICO

Cybersecurity Ventures espera que los cestos globales del cibercrimen crezcan un 15 % por año durante los próximos tres años, alcanzando 8 billones de dólares a nivel mundial este año y 10,5 billones de dólares anuales para 2025, frente a 3 billones de dólares en 2015.

El delito cibernético y la inseguridad cibernética son nuevos participantes en la clasificación Top 10 de los riesgos globales más graves durante la próxima década, según el Foro Económico Mundial. Ahora, ocupando el octavo lugar, el ciberdelito se encuentra lado a lado con amenazas que incluyen el cambio climático y la migración involuntaria.

En 2018, el Departamento de Justicia de EE. UU. declaró que se denunciaron menos de uno de cada siete delitos cibernéticos. En algunos países, la tasa reportada fue aún más baja. Cybersecurity Ventures cree que las prácticas de denuncia sobre actividades cibernéticas ilegales están mejorando, pero en 2023 todavía nos enfrentamos a una situación en la que menos del 25 % de los delitos cibernéticos cometidos a nivel mundial se informan a las fuerzas del orden. Por otro lado, según IBM, el coste promedio de una violación de datos, incluida la pérdida de negocios, la detección y el escalamiento, la notificación y la respuesta posterior a la violación, fue de 4,35 millones de dólares en 2022, lo que representa un aumento del 2,6 % desde 2021 (4,24 millones de dólares). Esta cifra se alcanzó al promediar los costes basados en actividades relacionados con 550 organizaciones que sufrieron violaciones de datos en 17 países (incluidos EE. UU., Canadá, Japón y Australia) y 17 industrias, como atención médica, finanzas y energía.

17 Morgan, S. (2023) 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistic, accessible en https://cybersecurityventures.com/cybersecurity-almanac-2023/

RANSOMWARE (SECUESTRO DE DATOS)

Se predijo que el coste global del ransomware alcanzaría los 20 mil millones de dólares en 2021, frente a los 325 millones de dólares de 2015. Cybersecurity Ventures espera que los costes por daños del ransomware superen los 265 mil millones de dólares anuales para 2031 y que mientras una empresa sería víctima de un ataque de ransomware cada 11 segundos en 2021, en comparación con cada 14 segundos en 2019. La frecuencia de los ataques de ransomware contra gobiernos, empresas, consumidores y dispositivos seguirá aumentando durante los próximos cinco años y se espera que aumente a cada dos segundos para 2031.

CRIPTOCRIMEN (DELITO CIBERNÉTICO)

El criptocrimen, incluidas las estafas de salida, los tirones de alfombras y el robo, le costará al mundo 30 mil millones de dólares solo en 2025, aumentando a una tasa del 15 % anual. Esto es casi el doble de los 17.500 millones de dólares perdidos en 2021.

El Centro de Quejas de Delitos en Internet (IC3) del FBI declaró que, en 2022, las estafas de inversión fueron los esquemas criminales de mayor importe reportados. Las quejas aumentaron de 1450 millones de dólares en 2021 a 3310 millones de dólares en 2022. Entre las estafas de inversión, el fraude con criptomonedas aumentó de 907 millones de dólares en 2021 a 2570 millones de dólares en 2022, un aumento del 183 %. Los delincuentes han utilizado intercambios descentralizados (DEX), puentes entre cadenas y servicios de intercambio de monedas para ofuscar al menos 4 mil millones de dólares en ganancias criptográficas ilícitas en los últimos años.

Según el análisis de Elliptic, más de 22 millones de direcciones criptográficas se han vinculado directamente a Rusia. Muchas de estas billeteras están asociadas con actividades delictivas relacionadas con la guerra entre Ucrania y Rusia, incluidas las direcciones que se utilizan para solicitar donaciones para el ejército y los mercenarios rusos.

En 2022, los volúmenes de transacciones ilícitas de criptomonedas aumentaron por segundo año consecutivo, alcanzando un récord de 20,6 mil

millones de dólares, que Chainalysis llama una estimación límite inferior. Además, la proporción de toda la actividad de criptomonedas asociada con actividades ilícitas aumentó por primera vez desde 2019, del 0,12 % en 2021 al 0,24 % en 2022.

HACKEOS PRINCIPALES

Una de las brechas de datos más importantes registradas en lo que va de 2023 pertenece a T-Mobile. En enero, el gigante de las telecomunicaciones reveló el robo de información personal perteneciente a 37 millones de cuentas actuales de clientes de pospago y prepago, posible gracias a la explotación de API. Una segunda brecha ocurrió en mayo.

En febrero de 2023, Cloudflare detectó y mitigó el mayor ataque de denegación de servicio distribuido (DDoS) jamás registrado. El ataque DDoS de 71 millones de solicitudes por segundo (rps), denominado "hipervolumétrico", es un 54 % más alto que el ataque informado anteriormente, de 46 millones de rps de fuerza, en junio de 2022.

Yahoo sufrió una de las filtraciones de datos más grandes de la historia. Un incidente de seguridad que se remonta a 2013 afectó a los 3 mil millones de cuentas de usuario de la empresa. Solo tres meses antes de la divulgación en 2015, el gigante tecnológico reveló una brecha separada que afectó al menos a 500 millones de cuentas.

GASTO EN CIBERSEGURIDAD

Cybersecurity Ventures predice que el gasto global en productos y servicios de ciberseguridad superará los 1,75 billones de dólares acumulativos durante el período de cinco años de 2021 a 2025, con un crecimiento del 15 % año tras año. Además, se prevé que el gasto mundial en formación de concienciación sobre seguridad para los empleados (anteriormente uno de los elementos presupuestarios de ciberseguridad menos gastados) supere los 10.000 millones de dólares para 2027, frente a los 5.600 millones de dólares de 2023. Así mismo, se estima que el gasto en productos y servicios de gestión de riesgos y seguridad de la información crezca un

11,3 % para alcanzar más de 188 300 millones de dólares en 2023. Gartner dice que el trabajo remoto e híbrido, el acceso a la red de confianza cero (ZTNA) y la implementación de los modelos basados en la nube están influyendo en el aumento del gasto.

CIBERSEGURO

Cybersecurity Ventures predice que el mercado de seguros cibernéticos crecerá a 14,8 mil millones de dólares en 2025 y superará los 34 mil millones de dólares para 2031, según una tasa de crecimiento anual compuesto (CAGR) del 15 % calculada durante un período de 11 años (2020 a 2031).

Entre 2017 y 2021, el 98 % de las reclamaciones de ciberseguros supervisadas por NetDiligence fueron realizadas por pymes con ingresos anuales inferiores a los 2.000 millones de dólares. La mayoría de las reclamaciones se realizaron en relación con incidentes de ransomware y Business Email Compromise (BEC).

El informe de tendencias de compras cibernéticas de EE. UU. de Marsh indica que el coste del seguro cibernético sigue aumentando, aunque muestra signos de moderación. Los precios de los seguros cibernéticos aumentaron en promedio un 11 % en EE. UU. durante el primer trimestre de 2023, en comparación con el 28 % en el primer trimestre de 2022.

Después de desacelerarse en 2022, las reclamaciones relacionadas con ransomware aumentaron un 77 % en el primer trimestre de 2023 en EE. UU., en comparación con el cuarto trimestre de 2022.

En el informe Global Cybersecurity Outlook 2023 del Foro Económico Mundial, se descubrió que las pequeñas empresas tenían menos probabilidades de tener ciberseguros en comparación con las organizaciones más grandes. Específicamente, el 48 % de las organizaciones pequeñas informaron que no tenían seguro cibernético, mientras que solo el 16 % de las organizaciones más grandes indicaron lo mismo. Además, el 57 % de las organizaciones con más de 100 001 empleados no revelaron si habían realizado una reclamación en los últimos dos años. De las empresas

que admitieron reclamar (21 %), el 14 % tuvo éxito, mientras que el 7 % no lo tuvo.

SALA DE JUNTAS Y CONSEJO DE ADMINISTRACIÓN

En una encuesta reciente de KPMG a 1325 directores ejecutivos, el 77 % considera que la seguridad de la información es una función estratégica y una posible ventaja competitiva. La incertidumbre geopolítica está aumentando las preocupaciones sobre los ciberataques corporativos para el 73 % de los ejecutivos.

Los profesionales de gestión de riesgos y seguros calificaron los incidentes cibernéticos como el principal riesgo comercial global en el Barómetro de riesgos de Allianz de 2023, seguidos por la interrupción del negocio y los desafíos macroeconómicos, como la inflación y la deflación. La encuesta anual incorporó opiniones de expertos en 23 sectores industriales en 94 países y territorios.

Las consecuencias de los ataques cibernéticos han entrado en la sala de juntas, con Gartner prediciendo que el 75 % de los directores ejecutivos serán personalmente responsables de los ataques contra los sistemas ciberfísicos (CPS), incidentes que provocan daños físicos y ambientales, o la destrucción de la propiedad, para 2024.

CAPITAL DE RIESGO

Cybersecurity Ventures rastreó más de 15,7 mil millones en capital de riesgo dedicado a empresas de ciberseguridad en 2022. Por su parte, PitchBook informó que algunos de los inversores globales más activos involucrados en capital de riesgo de ciberseguridad desde 2017 son Evolution Equity Partners, Insight Partners, Plug and Play Tech Center, Accel y Sequoia Capital.

EMPLEOS DE CIBERSEGURIDAD

Habrá 3,5 millones de puestos de trabajo de ciberseguridad sin cubrir en todo el mundo en 2023, según Cybersecurity Ventures, que se mantendrá hasta 2025 a medida que continúa la disparidad entre la demanda y la

oferta. Por el contrario, la tasa de desempleo de seguridad cibernética para los puestos con más experiencia es del cero %, y probablemente seguirá así en los próximos años. Como nota particular, cabe añadir que se espera que solo India cree 1,5 millones de nuevos puestos de trabajo en ciberseguridad para 2025. Según NASSCOM, el mercado indio de ciberseguridad estará cerca de una valoración de 500 mil millones de dólares para 2030.

El 10 % de los líderes empresariales y el 13 % de los líderes cibernéticos creen que falta el personal y las habilidades para los roles críticos. Así, según el Global Cybersecurity Outlook 2023 del Foro Económico Mundial, el 32 % de los líderes empresariales y el 34 % de los líderes cibernéticos dijeron que existen brechas de capacitación y habilidades en algunas áreas.

Por su parte, EE. UU. tiene una fuerza laboral total de seguridad cibernética empleada que consta de más de 1,1 millones de personas, y hay más de 755.000 puestos vacantes, según CyberSeek, un proyecto respaldado por la Iniciativa Nacional para la Educación en Seguridad Cibernética (NICE), un programa del Instituto Nacional de Estándares y Tecnología (NIST) en el Departamento de Comercio de los Estados Unidos. Y la Oficina de Estadísticas Laborales de EE. UU. proyecta que el empleo de "analistas de seguridad de la información " crecerá un 35 % entre 2021 y 2031, en comparación con la tasa de crecimiento promedio del 5 % para todas las ocupaciones. El salario anual medio se registró en 102.600 en mayo de 2021.

ARGOCAPITALISTAS

Microsoft lanzó una campaña nacional con los colegios comunitarios de EE. UU. para ayudar a colocar a 250.000 personas en la fuerza laboral de ciberseguridad para 2025, lo que representa la mitad de la escasez de mano de obra del país. Microsoft también está aumentando su inversión en seguridad cibernética a 20 mil millones durante los próximos cinco años, frente a los mil millones por año que han estado gastando en ciberseguridad desde 2015.

Citando los datos de escasez de habilidades de Cybersecurity Ventures, el gigante de Redmond también anunció recientemente una nueva asociación bajo su programa *Ready4Cybersecurity* en Asia para mejorar el acceso a las habilidades y carreras de ciberseguridad para los grupos subrepresentados. El programa tiene como objetivo certificar a 100.000 mujeres jóvenes y jóvenes subrepresentados en ciberseguridad para 2025.

En 2021, Google anunció una inversión de más de 10 mil millones hasta 2025 en ciberseguridad. El esfuerzo incluirá ayudar a asegurar la cadena de suministro y fortalecer la seguridad de código abierto. Google también dice que está capacitando a 100,000 estadounidenses para trabajos vitales de seguridad y privacidad de datos.

Amazon en mayo de 2023 señaló que estaba invirtiendo más en Open Source Security Foundation (OpenSSF) al comprometer 10 millones adicionales durante los próximos tres años.

IBM se ha comprometido a brindar a 30 millones de personas oportunidades de aprendizaje para cerrar las brechas de habilidades en el sector de la tecnología, incluida la ciberseguridad, para 2030. Las asociaciones se extienden a las ONG que se enfocan en jóvenes, mujeres y veteranos militares desatendidos.

MUJERES EN CIBERSEGURIDAD

Las mujeres ocuparon el 25 % de los trabajos de seguridad cibernética a nivel mundial en 2022, frente al 20 % en 2019 y alrededor del 10 % en 2013. Cybersecurity Ventures predice que las mujeres representarán el 30% de la fuerza laboral mundial de seguridad cibernética para 2025, aumentando al 35 % para 2031.

Una encuesta de BCG de mujeres graduadas en STEM revela que el 68 % tomó un curso relacionado con la seguridad cibernética durante sus estudios. Sin embargo, el 37 % de los encuestados consideró que la ciberseguridad es un campo en el que es difícil lograr un equilibrio entre el salario, la contribución a la sociedad y el mantenimiento de un equilibrio entre la vida laboral y personal. Se supone ampliamente que la mayoría de los

ciberdelincuentes son hombres, más concretamente, un informe reciente de Trend Micro disipa este mito y encuentra que aproximadamente el 30 % de los participantes del foro de ciberdelincuentes son mujeres.

FORMACIÓN EN CIBERSEGURIDAD

Cybersecurity Ventures predice que el mercado global de capacitación en concientización sobre seguridad superará los 10 mil millones anuales para 2027, frente a alrededor de 5,6 mil millones en 2023, según un crecimiento anual del 15 %.

Según la principal certificación de seguridad cibernética del mundo CISSP (Profesional certificado en seguridad de sistemas de información) otorgada por el Consorcio internacional de certificación de seguridad de sistemas de información, también conocido como (ISC)² desde julio de 2022 hay 156.054 miembros que cuentan con la certificación CISSP en todo el mundo.

Cybercrime Magazine destaca 12 certificaciones de seguridad para trabajadores de TI en 2023 que son valiosas para los empleadores. Estas incluyen CompTIA Network+, OffSec Offensive Security Certified Professional (OSCP), CREST Registered Penetration Tester (CRT), EC-Council Certified Ethical Hacker (CEH), OffSec Certified Professional (OCSP) y TCM Security Practical Network Penetration Tester (PNPT).

RESPONSABLES DE SEGURIDAD DE LA INFORMACIÓN (CISO)

El primer CISO del mundo fue ungido en 1994, cuando el gigante de servicios financieros Citigroup (entonces Citicorp) montó una oficina especializada en ciberseguridad tras sufrir una serie de ciberataques de piratas informáticos rusos, desde entonces el 100 % de las empresas Fortune 500 emplearon un CISO o equivalente en 2022, frente al 70 % en 2018.

Según Cisco, los líderes de seguridad informan que sus tres principales áreas de responsabilidad son liderazgo en seguridad (35 %), evaluación y gestión de riesgos (44 %) y privacidad y gobernanza de datos (33 %).

En una encuesta de 125 profesionales de ciberseguridad y de respuesta a incidentes, VMWare descubrió que los equipos de seguridad están bajo presión. En total, el 65% de los encuestados dijo que los ataques cibernéticos han aumentado desde el comienzo de la guerra entre Rusia y Ucrania. Además, el 47% ha experimentado agotamiento o estrés extremo en los últimos 12 meses, y el 69% mencionó que estas condiciones les han hecho considerar dejar sus funciones. Por su parte, Gartner estima que para 2025, casi la mitad de los líderes de seguridad cibernética cambiarán de rol, y el 25% cambiará de rol por completo, debido al estrés, la presión psicológica y el agotamiento, entre otros factores.

En todo caso, cabe destacar que la brecha de género sigue siendo un abismo cuando consideramos los roles principales en ciberseguridad. Por ejemplo, las mujeres solo ocupan el 17 % de los puestos de directora de seguridad de la información (CISO) en las empresas Fortune 500.

FINANZAS

En el 60 % de los casos que una organización experimentó una brecha de seguridad, la tensión financiera resultó en aumentos de precios para los clientes. Así, según LexisNexis, el impacto anual del fraude global supera ahora el billón de dólares. Cada dólar perdido por fraude resultó en una pérdida de $ 4.23 para las empresas de servicios financieros de EE. UU. en 2022.

Según un estudio privado citado por el Servicio de Investigación del Congreso, el 25% de los ataques de malware se dirigen a empresas de servicios financieros. El coste por empresa del delito cibernético es de más de 18 millones de dólares para los servicios financieros, alrededor de un 40% más que el coste promedio de otros sectores.

Por otro lado, el 60 % de los líderes de seguridad cibernética que respondieron a las preguntas planteadas en el Índice de preparación para la seguridad cibernética de Cisco dijeron que tuvieron un incidente de seguridad cibernética en los últimos 12 meses, y el 41 % de los afectados dijeron que les costó a sus organizaciones al menos 500 000 USD.

CUIDADO DE LA SALUD

Cybersecurity Ventures predice que el mercado mundial de ciberseguridad en el cuidado de la salud crecerá un 15% año tras año durante los próximos cinco años, alcanzando los 125 mil millones de dólares para 2025. Además, IBM afirma que el coste promedio de una violación de datos en el cuidado de la salud, que comprende hospitales y clínicas, aumentó en casi 1 millón de dólares a 10,10 millones de dólares en 2022. El gobierno de los EE. UU. considera que el cuidado de la salud es una infraestructura crítica.

Los ataques de ransomware contra organizaciones de atención médica se duplicaron en los últimos cinco años, siendo la víctima más común las clínicas de salud, según un estudio del JAMA Health Forum.

USUARIOS DE INTERNET

Aproximadamente un millón de personas más se conectan a Internet todos los días. Cybersecurity Ventures estima que seis mil millones de personas estaban conectadas a Internet en 2022 y predice que habrá más de 5 mil millones de usuarios de Internet en 2030, incluido el 90% de la población humana de seis años o más.

Hay 48 mil millones de usuarios únicos de teléfonos móviles en el mundo hoy en día, según los últimos datos de GSMA Intelligence. La seguridad móvil y los riesgos asociados con una fuerza laboral híbrida son una de las principales preocupaciones de los líderes tecnológicos, junto con las vulnerabilidades del centro de datos y la nube.

SUPERFICIE DE ATAQUE

Cybersecurity Ventures predice que el almacenamiento global de datos superará los 200 zettabytes para 2025. Esto incluye datos almacenados en infraestructuras privadas, públicas y de servicios públicos, centros de datos en la nube privados y públicos, dispositivos personales y dispositivos IoT (Internet de las cosas). También estiman que el mundo necesitará asegurar 338 000 millones de líneas de código de software nuevo en 2025, frente a los 111.000 millones de líneas de código nuevo en 2017.

Dicha estimación se basa en un crecimiento interanual del 15 % en código nuevo.

Por su parte, Citi predice que el mercado del metaverso podría tener un valor de entre 8 y 13 billones de dólares para 2030 a medida que se expanden las aplicaciones de metaverso. La investigación sugirió que, en 2021, las empresas de metaverso se enfrentaron con un 80 % más de ataques de bots y un 40 % más de ataques humanos que muchas otras empresas en línea.

Los dispositivos móviles continúan reemplazando a las computadoras portátiles y los sistemas de escritorio para muchas funciones, incluidas la productividad, la banca, los pagos, el entretenimiento y la socialización. A este respecto, BlackBerry estima que los dispositivos móviles generaron el 59,54 % de todo el tráfico de Internet en 2022.

Los programas de gestión continua de exposición a amenazas (CTEM) para gestionar la superficie de ataque serán cruciales. Gartner predice que, para 2026, las organizaciones que prioricen las inversiones en seguridad CTEM experimentarán dos tercios menos de infracciones.

SEGURIDAD AUTOMOTRIZ

La investigación citada por BlackBerry estima que habrá 775 millones de autos conectados en la carretera para 2023, aumentando la superficie de ataque potencial de una industria ya acosada por violaciones de datos, ransomware y ataques relacionados con hardware.

Según Upstream, en 2022, la cantidad de ataques a API automotrices aumentó en un 380 %, lo que representa el 12 % del total de incidentes. Además, el 63% de los incidentes fueron protagonizados por actores de sombrero negro, mientras que los defensores de sombrero blanco dirigieron el resto. Las estimaciones actuales sitúan la cantidad de microchips en un automóvil promedio entre 1000 y 3000, según el Centro Nacional de Ciencias de la Manufactura.

CADENAS DE SUMINISTRO

Gartner estima que para 2025, el 60 % de las organizaciones de la cadena de suministro y sus directores de la cadena de suministro considerarán el riesgo de ciberseguridad como un determinante importante en la realización de transacciones y compromisos comerciales con terceros.

La investigación del Foro Económico Mundial afirma que más de un tercio de las organizaciones se han convertido en "daños colaterales" en un incidente cibernético de terceros, de hecho, 9 de cada 10 líderes de TI están preocupados por la resiliencia cibernética de dichos terceros.

La cadena de suministro de software se ha convertido en un objetivo principal para los actores de amenazas. En los últimos tres años, se registró un aumento anual promedio de ataques del 742%, según Sonatype. En la misma línea de argumentación, una encuesta reciente de KPMG a 1325 directores ejecutivos, relató que el 76 % de los directores ejecutivos cree ahora que proteger el ecosistema de sus socios y la cadena de suministro es tan importante como construir las defensas cibernéticas de su propia organización.

AUTENTICACIÓN

Más de 300 mil millones de contraseñas fueron utilizadas por humanos y máquinas en todo el mundo en 2021, según el último recuento de Cybersecurity Ventures. Sin embargo, solo del 1 al 3% de las transacciones en los EE. UU. se envían a través de 3DS, el protocolo financiero diseñado para autenticar a los usuarios.

En 2022, Microsoft rastreó 1287 ataques de contraseña cada segundo, lo que equivale a más de 111 millones de ataques diarios.

La investigación del Ponemon Institute estima que las pérdidas comerciales promedio en todos los tipos de debilidades de autenticación oscilaron entre 39 millones de dólares y 42 millones de dólares en 2022. Además, el 66% de los encuestados del personal de seguridad de TI dicen que es difícil, o muy difícil, distinguir a los empleados y clientes de impostores ciberdelincuentes que utilizan credenciales robadas.

FBI (OFICINA FEDERAL DE INVESTIGACIONES)

La galería de delincuentes cibernéticos del FBI se ha expandido rápidamente, con 120 personas que actualmente figuran en la lista de '*Cyber's Most Wanted*' de la agencia, frente a 105 personas en 2022 y solo 63 personas en 2019. Tales delincuentes son buscados por delitos que incluyen intrusión informática, fraude electrónico, robo de identidad, lavado de dinero, extorsión a través de ransomware y más.

El Centro de Quejas de Delitos en Internet (IC3) del FBI informó que, en 2022, se recibieron 800,944 quejas relacionadas con delitos y fraudes cibernéticos, una disminución del 5% con respecto a 2021 (847,376 quejas). Sin embargo, el número de quejas que el IC3 ha recibido anualmente se ha más que duplicado desde 2018. De hecho, se han informado más de 7,3 millones de quejas desde el inicio de IC3, 3,6 millones de las cuales se han recibido en los últimos 5 años, lo que equivale a pérdidas totales de 27,6 mil millones de dólares.

Según IC3, el phishing es el delito denunciado número uno, con 300.497 denuncias en 2022 y una pérdida estimada de 52 millones de dólares. Sin embargo, los esquemas de inversión reportaron la pérdida financiera más alta para las víctimas por primera vez, con una pérdida en dólares asociada de 3.3 mil millones de dólares, aumentando un 127% año tras año.

PEQUEÑAS EMPRESAS

"Hay 30 millones de pequeñas empresas en los EE. UU. que necesitan mantenerse a salvo de ataques de phishing, espionaje de malware, ransomware, robo de identidad, infracciones importantes y piratas informáticos que comprometerían su seguridad", dice Scott Schober, autor de los libros populares "Hacked Again" y "Cybersecurity Is Everybody's Business".

El 43% de los ataques cibernéticos se dirigen a pequeñas empresas, de las cuales el 60% de las víctimas cierran dentro de los seis meses. Cuanto más pequeña es la empresa, menos recursos se dedican a la seguridad, ¿o es un mito? Un informe de Cisco que examina las prácticas de las

PYMES (250 a 500 empleados) dice que menos del 1% no tiene a ninguna persona dedicada a la seguridad; el 72 % tiene empleados dedicados a la caza de amenazas, en comparación con el 76 % de las organizaciones más grandes y el 56% tiene una rutina de parches diaria o semanal. En total, el 86% tiene métricas claras para evaluar la efectividad del proceso de seguridad, en comparación con el 90% de las contrapartes más grandes.

OTROS DATOS

Actualmente hay más de 3500 grupos de amenazas activos, incluidos más de 900 recientemente rastreados en 2022 por Mandiant.

Las organizaciones reciben notificaciones de infracciones por parte de entidades externas en más del 60% de los incidentes, dicen los investigadores, y el tiempo de permanencia promedio global para incidentes detectados internamente en 2022 es de 13 días. El tiempo medio de permanencia global fue de 18 días en 2021.

Las cinco industrias más ciberatacadas en los últimos siete años son atención médica, manufactura, servicios financieros, gobierno y transporte. Cybersecurity Ventures predice que el comercio minorista, el petróleo y el gas, la energía y los servicios públicos, los medios y el entretenimiento, el legal y la educación (K-12 y educación superior) completarán las 10 industrias principales para 2023.

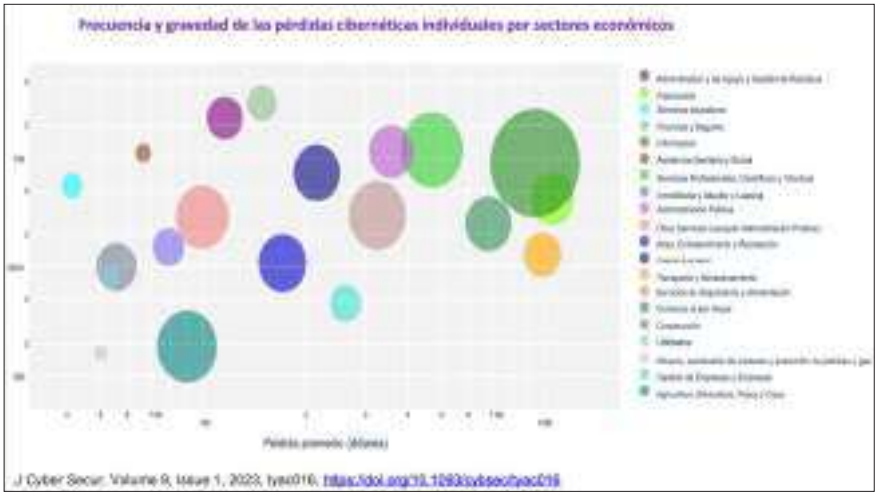
El delito cibernético se dirige cada vez más a personas de alto poder adquisitivo y oficinas familiares. Según un estudio presentado por Barclays Private Bank, más de una cuarta parte de las familias y empresas familiares de ultra alto valor neto (UHNW) con una riqueza promedio de 1.1 mil millones de dólares han sido objeto de un ataque cibernético.

Las multas por violaciones de la ley de privacidad de la Unión Europea continúan aumentando. Según una investigación del bufete de abogados DLA Piper, las autoridades de protección de datos de la UE han entregado

un total de 1,74 mil millones de dólares en multas por infracciones del Reglamento General de Protección de Datos (GDPR) del bloque desde enero de 2022, lo cual significa más de 1,25 mil millones de dólares un año antes.

En esta misma línea de estudio, pero desde una perspectiva de corte académico, cabe destacar el trabajo de Shevchenko *et al.* (2023) titulado "La naturaleza de las pérdidas por eventos cibernéticos: categorías de riesgo y sectores comerciales"[18], donde examinan la naturaleza de las pérdidas por eventos cibernéticos en diferentes categorías de riesgo y sectores comerciales y evalúan la relación entre la frecuencia y la gravedad de los eventos cibernéticos individuales y la cantidad de registros afectados, tal como se muestra en las imágenes 14 a 19.

Imagen 14



18 Shevchenko, P. et al. (2023) The nature of losses from cyber-related events: risk categories and business sectors. Journal of Cybersecurity, Volume 9, Issue 1, tyac016, https://doi.org/10.1093/cybsec/tyac016

Imagen 15

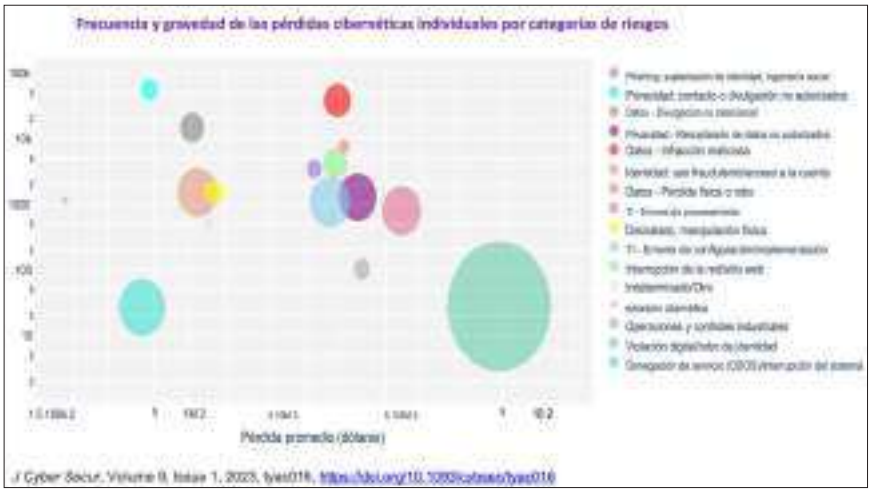


Imagen 16

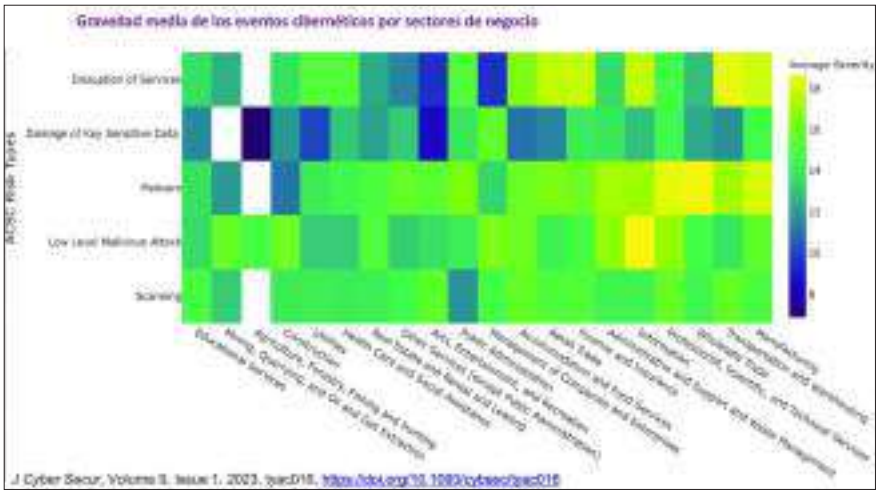


Imagen 17

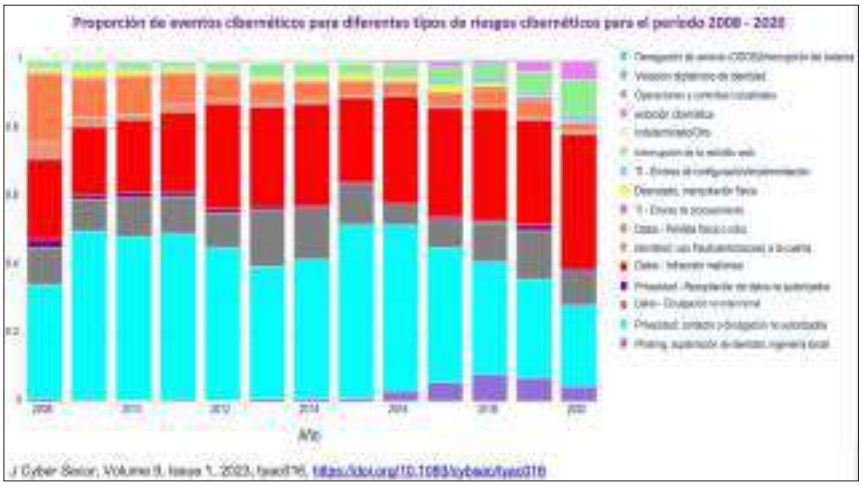


Imagen 18

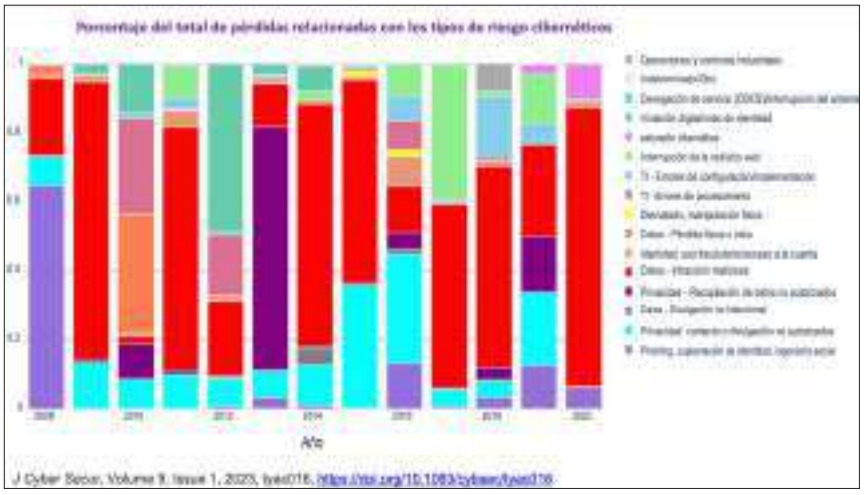
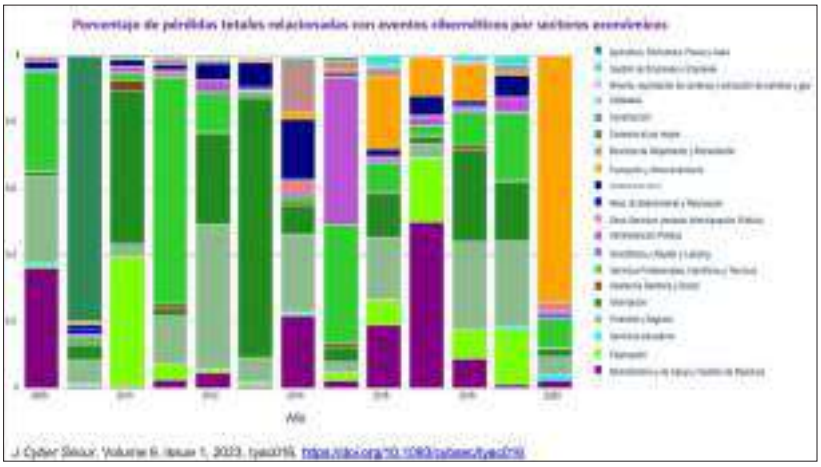


Imagen 19



La observación de las imágenes contenidas en el trabajo de Shevchenko et al. (2023) permite comprobar como la frecuencia de eventos cibernéticos informados ha aumentado sustancialmente entre 2008 y 2016. Además, la frecuencia y la gravedad de las pérdidas dependen del sector comercial y el tipo de amenaza cibernética: las categorías de eventos de pérdida cibernética más importantes, por número de eventos, estaban relacionados con violaciones de datos y la divulgación no autorizada de datos, mientras que la extorsión cibernética, el phishing, la suplantación de identidad y otras prácticas de ingeniería social mostraron tasas de crecimiento sustanciales. El análisis llevado a cabo también reveló que los riesgos cibernéticos son de cola pesada y que las pérdidas de eventos cibernéticos tienen el potencial de ser catastróficas al seguir una distribución exponencial.

Llegados a este punto, cabe suscitar la pregunta, ¿pero es posible que haya alguna cuestión que otorgue más complejidad si cabe a la ciberseguridad? Pues, afirmativamente una nueva cuestión surge a raíz de comprobar que la ciberseguridad es una decisión empresarial, esto es, la ciberseguridad

en el caso español no está en manos exclusivas del INCBE. Se trata de una decisión empresarial u organizativa, depende del apetito de riesgo que tengan las empresas o instituciones y eso es lo que define el estado real de la ciberseguridad que pueda existir. En definitiva, es un problema de demanda, no es un problema de oferta. En el INCIBE seguro que existen expertos que desarrollen sus trabajos muy bien, pero el problema está fuera, simplemente puede ser que les ayuden o no.

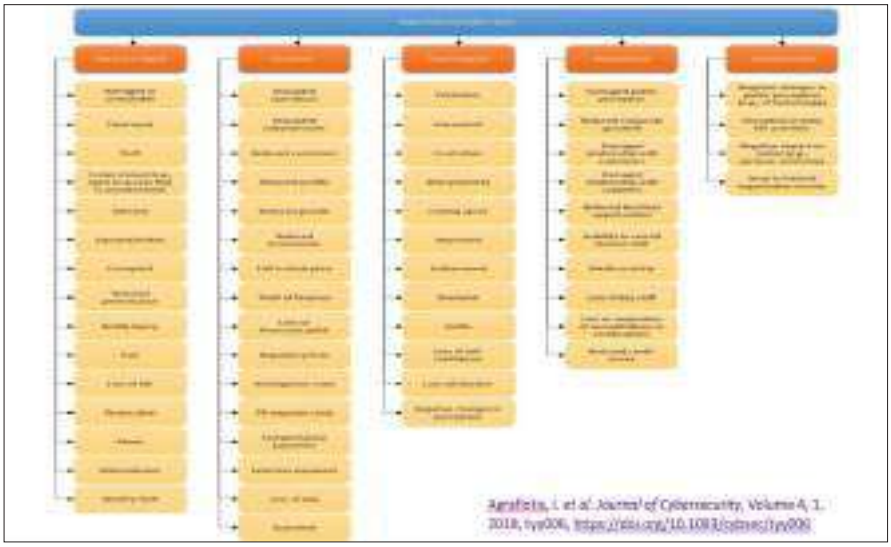
En la ciberseguridad se está hablando de un, digamos, coste de equilibrio, un umbral de rentabilidad, donde se cruza el nivel de seguridad con el coste a asumir, atendiendo a un principio fundamental de economicidad (Ver Imagen 20).

Imagen 20

Nadie va a invertir más en seguridad que lo que me costaría no tenerla. Pero tal proceder encierra un peligro enorme. Es de una gran miopía, es de una insensatez extraordinaria. ¿Por qué? En primer término, conviene tener en cuenta por una idea fundamental que radica en que además de riesgos hay daños. Y los daños cibernéticos son muy muchos y no aparecen todos al mismo tiempo, sino algunos con retrasos importantes, tal como se puede observar

de la lectura del trabajo de Agrofitis et al. (2018) [19], donde presentan toda una panoplia de estas cinco categorías de daños que puede acontecer el cibercrimen (Ver Imagen 21).

Imagen 21



A mayores, cuando en el mismo trabajo de Agrofitis et al. (2018) luego analiza, por ejemplo, cómo se propagan estos ciberataques en dos casos de estudio referidos a dos ciberataques muy conocidos en la literatura sobre el tópico relacionados con la empresa Sony y la empresa JP Morgan, se puede comprobar cómo, al poco de acontecer el evento, empiezan unos primeros problemas, pero con el tiempo se van desarrollando otros problemas, tanto a nivel organizativo de la propia empresa como de los trabajadores de las personas vinculadas a las mismas, de forma coincidente con la distribución exponencial aducida en el trabajo de Shevchenko et al. (2023) antes citado.

19 Agrafiotis, I. et al. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, Volume 4, Issue 1, tyy006, https://doi.org/10.1093/cybsec/tyy006

¿Qué es lo que nos está diciendo esto? Pues, simplemente, que existen efectos olvidados, en línea con lo analizado por Kaufman y Gil Aluja [20] que se han obviado, saltado, despreciado... Es la idea del huevo, la idea de que no somos conscientes de que estamos mirando al futuro con lo que sabemos de nuestro pasado. Y el futuro no está escrito de esa forma. Esta para mí una clave fundamental. Una enseñanza que no se puede soslayar del recurrente esfuerzo investigador del Dr. Gil Aluja, quien ha desarrollado multitud de algoritmos y axiomáticas precisamente para evitar este tipo de circunstancias y situaciones en la toma de decisiones.

Claro que en este trabajo estamos hablando de ciberseguridad. Pero ¿de qué ciberseguridad es la que estamos hablando? Porque la ciberseguridad tiene muchísimas aristas. No hay una sola cosa, digamos, algo que pueda definir en exclusiva, sino más bien una combinación de cosas. No es un elemento euclidiano regular, para nada (Ver Imagen 22).

No resulta extraño entonces que en este campo se hable de las cinco leyes de la ciberseguridad. Aunque se han hecho encuestas para ver si además de estas leyes o hay otras (Ver Imagen 23).

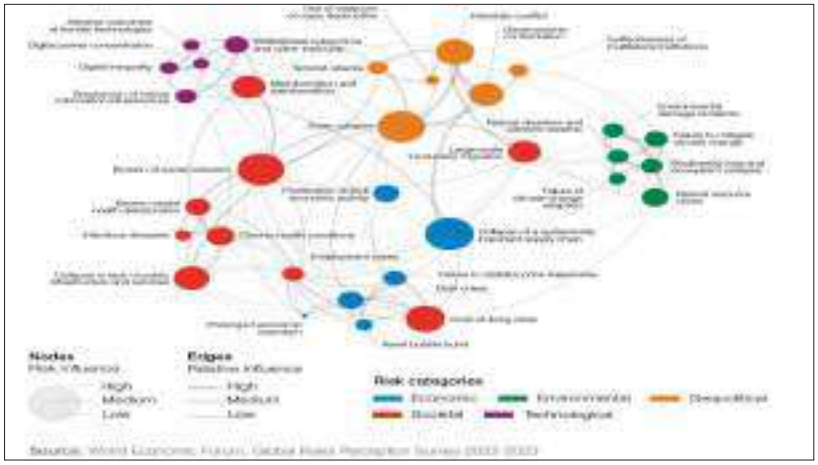
Imagen 22

20 Kaufmann, A. y Gil Aluja, J. (1988). Modelos para la investigación de efectos olvidados. Santiago de Compostela: Milladoiro.

Antes de concluir con toda esta panoplia de vicisitudes y desafíos que dan forma a la ciberseguridad, cabe tener en consideración las posibles interrelaciones dinámicas propias de todos los aspectos relacionados con la ciberseguridad. A este respecto, cabe señalar el informe "Global Risks Report 2023" del Foro Mundial Económico [21], donde nos habla de que existen muchos riesgos que se cruzan, que están interrelacionados. Así, como se puede observar en la Imagen 24, en la esquina derecha se incluyen, como no podían obviarse, los riesgos de ciberseguridad. Pero un atributo de estos riesgos, lo cual supone un problema adicional, radica en que son, digamos, muy cariñosos con sus compañeros, es decir, son muy fáciles de viralizarse y afectar pandémicamente a los demás. Hay interdependencia y esto significa, otra bandera roja importante, se trata de riesgo sistémicos. Y eso ¿qué supone, se agrava la cosa? Pues sí, la verdad y mucho. Tenemos ejemplos muy recientes, así la semana pasada salto a las noticias el tema de la empresa ferrovial, lo que significaba que simplemente tomara una decisión de traslado, cómo se movilizaba todo, porque obviamente esa empresa generaba una dinámica en otras muchas. También, en estos días, estamos asistiendo al tema de un banco del Valle de Silicio que, bueno, pues nos ha puesto a pensar si vamos a volver a repetir la crisis financiera del 2008.

21 https://www.weforum.org/reports/global-risks-report-2023

Imagen 23



Y finalmente, este apartado acerca del impacto de la transformación digital que estamos viviendo, la nueva realidad, no debería concluir sin que previamente al menos se incluyera una mínima referencia a la existencia de cuatro tecnologías disruptivas que "lo cambian todo": Multiverso (web3, blockchain, nfts,...), Inteligencia Artificial Generativa (chatgpt, bard, falcon llm,…), Computación Cuántica (criptoagilidad) y 6G (era post-latencia), Por supuesto que su impacto en la ciberseguridad es innegable, y que como se puede observar en la Imagen 24 los tres primeros ya forman parte de las portadas de la revista Time. Somos legión los que opinamos que cuando algún hallazgo tecnológico aparece en la portada Time es que ya ha superado la fase de especulación académica y "está ya en la calle", esto es, forma parte ya del mainstream o corriente/tendencia mayoritaria.

Imagen 24

3.4. Hacia la CiberResiliencia

Pues bien, con todo lo comentado sobre ciberseguridad, ¿se puede seguir hablando de ciberseguridad como un concepto exclusivo o excluyente para abordar la seguridad digital? Me permito avanzarles que desde mi perspectiva la respuesta es negativa. Les digo que no, pero vamos a ver por qué y que se propone para su superación, en concreto, la resiliencia cibernética o ciberresiliencia.

Por si fuera poca la leña que hemos situado en la hoguera de la ciberseguridad, nos asiste una noticia del The Wall Street Journal (Ver Imagen 25) donde se relata que en 2022 los precios de los seguros cibernéticos en EE. UU. aumentaron un 79 % con respecto al año anterior, según el Índice del Mercado de Seguros Globales de Marsh & McLennan Cos.

Imagen 25


THE WALL STREET JOURNAL.

Comprar un seguro cibernético se vuelve más complicado a medida que proliferan los ataques y aumentan los costos

Los precios de los seguros no dejan de aumentar y cada vez son más caros y sirven para muy poco, dando lugar, y esta es mi opinión, a que el modelo actual de la ciberseguridad se asemeje al caricaturizado en la Imagen 26, pues el modelo estandarizado de ciberseguridad está provocando que las organizaciones de todo el mundo inviertan miles de millones en protecciones de ciberseguridad. Hay que actualizar, actualizar, actualizar. Aun así, continúan ocurriendo los eventos de cibercrimen y cada vez a peor (FBI *dixit*), infracciones masivas que afectan a empresas en todo el mundo. Esto es lo único que se saca de los informes que se sabe que se hacen de ciberseguridad. Es que cada año es peor, cada día es peor que el anterior. Algo anda mal entonces. Algo anda mal cuando se gastan mil millones de dólares al año en protecciones cibernéticas y, sin embargo, se espera que las pérdidas en 2023 superen 10 veces lo gastado.

¡Los números simplemente no cuadran!

Imagen 26

Hay algo fundamentalmente roto con el modelo estándar de ciberseguridad. Las medidas típicas de ciberseguridad están tratando de resolver el problema equivocado. El defecto fundamental de la ciberseguridad es que está desactualizada: Hasta el momento, las organizaciones se han centrado en construir sistemas destinados a detectar amenazas y permitir respuestas eficientes. Esto refleja un enfoque peligroso: son los malos actores quienes marcan el ritmo de la acción, tienen "la sartén por el mango". Las soluciones de seguridad cibernética utilizadas continúan enfocándose en "mantener a las personas fuera". Tratan de ser "a prueba de balas" e impedir que los actores maliciosos rompan su perímetro e impedir que puedan "entrar dentro". Es la idea aquella que teníamos del castillo y levantar la trapa y se acabó el problema de invasión. Este es el concepto de defensa digital: Es un concepto medieval.

El modelo de ciberseguridad estándar está fundamentalmente roto, le falta un enfoque basado en la ciberresiliencia. Hay que hacer un salto de dial (Ver Imagen 27). Hay que orientarse a otro aspecto.

Imagen 27

Al objeto de conocer cuáles son las principales diferencias[22] entre ciberseguridad y ciberresiliencia, conviene detallar lo que entendemos por estos conceptos, a saber:

Definición de ciberseguridad:

- Es un componente de la ciberresiliencia
- Abarca tecnologías, procesos y medidas diseñadas para proteger sistemas, redes y datos de los delitos cibernéticos.
- Trata de reducir las posibilidades de ataques cibernéticos y trata de proteger de ataques y vulnerabilidades externos e internos.
- Las soluciones de ciberseguridad deben funcionar de forma efectiva sin comprometer la usabilidad de los sistemas.
- Cualquier estrategia de ciberseguridad también debe incluir un sólido plan de continuidad para reanudar las operaciones si un ciberataque tiene éxito.

22 www.quora.com/What-is-the-difference-between-Cyber-Resilient-and-Cyber-Security-1

Definición de ciberresiliencia:

- Abarca un alcance más amplio, que comprende la ciberseguridad, la mitigación de riesgos, la continuidad del negocio y la resiliencia organizacional, esto es, garantizando la gestión continuada (en marcha) del negocio.

- La capacidad de una organización para brindar continuamente los servicios, operaciones y resultados previstos a pesar de la ocurrencia de eventos cibernéticos adversos, propiciando que esta sea inteligente y ágil manejado ataques reales o potenciales.

- Requiere un cambio cultural a medida que la organización adopta la seguridad como un trabajo de tiempo completo e incorpora las mejores prácticas en las operaciones diarias.

- Se enfoca en instancias en que una organización se ve interrumpida (ataques maliciosos, violaciones de datos, cortes de energía, emergencias climáticas, errores humanos, ...).

Llegados a este este punto, discúlpenme, pero no puedo reprimir que aflore mi tropismo contable. De forma similar a cuando le preguntamos a un informático acerca de alguna avería en nuestro ordenador, donde lo primero que es común que dicho profesional nos solicite es saber si el aparato está enchufado, vamos, que si tiene corriente eléctrica. Porque si no está enchufado, a lo mejor es por eso por lo que no funciona. Por nuestra parte, los contables nos encomiamos en primer lugar a un principio básico: la gestión continuada. Si no hay gestión continuada, los datos de que disponemos, ¿cómo les tenemos que tratar? ¿Para qué hay una gestión continuada? La respuesta es que para qué haya un negocio en funcionamiento normal, no sorpresivo como cuando simplemente nos asisten actualizaciones o parches de software contra eventos maliciosos. En tales circunstancias, sin duda, estamos en una situación adversaria significativa y tenemos un gran problema. Y no es de los de Houston, es de todos y a todos nos concierne.

Por tanto, aunque parezca reiterativo, la capacidad de una organización para brindar continuamente los servicios, operaciones y resultados previstos, a pesar de la ocurrencia de eventos adversos propiciando que pueda reaccionar de forma inteligente y ágil, manejando los ataques, aprender de los ataques reales y potenciales, ese es de lo que va de verdad la seguridad cibernética, lo cual exhorta a un cambio cultural, que dudo forme parte del ideal estratégico a corto plazo del INCIBE.

Hay que dejar de pensar como los caballeros del Medievo. El mayor problema en el *status quo*, presente y lo que se pueda avizorar a medio plazo, de la seguridad digital es poder continuar. Hay que guardar ley, un respeto ontológico, al principio de gestión en marcha. Aquello que se dijo al principio de este epígrafe, poder rebotar y que el evento nos propicie experticia valiosa para el porvenir.

Surge entonces la cuestión de ¿cómo podríamos transitar de un lado a otro, o cuáles podrían ser los pasos o fases en la construcción de una organización ciberresiliente? A los efectos de esta presentación, cabría resumir las siguientes:

- Adoptar un enfoque holístico de ciberseguridad. Viendo todos los activos de su negocio como conectados, no solo en los equipos de seguridad.

- Mantener la higiene de seguridad básica. Custodiando los sistemas y el software a través de parches, actualizaciones y permisos de acceso regulares.

- Prepararse para el cambio. Respondiendo a las amenazas emergentes y los ataques cibernéticos con rapidez y agilidad.

- Crear redes descentralizadas. Al consolidar y analizar datos en todos sus sistemas y redes, puede definir el comportamiento básico del usua-

rio, aprovechando la automatización con AI (servicios de inteligencia de amenazas, segmentación y tokenización) para la detección en tiempo real de ataques y para responder de forma efectiva.

- Implementar la ciberseguridad basada en datos. Eclipsando las aproximaciones relacionadas con la ciberseguridad, yendo más allá de la seguridad de datos tradicional.

- Implementar la seguridad por diseño: Agendarlo como prioritario del Consejo de Administración, de hecho, a tenor de lo mencionado previamente, cabe pensar que la ciberresiliencia es el activo estratégico más importante de aquellas organizaciones, públicas o privadas, que tengan en muy alta estima su transformación digital.

Precisamente, respecto al último punto recién citado, conviene tener en cuenta que, adicionalmente, la ciberresiliencia constituye un activo estratégico para lograr ventajas competitivas, pues la estrategia de resiliencia cibernética es una arquitectura cuidadosamente diseñada que brinda la capacidad de protegerse, detectar, responder y recuperarse de los ataques cibernéticos y, como se ha mencionado, en el actual sistema argocapitalista los datos de los clientes son oro (digital), constituyen el nuevo 'perímetro de red' para proteger. Debido a que las empresas recopilan, procesan y almacenan grandes volúmenes de datos de consumidores es vital que la empresa tenga una "visión centrada en los datos" de la ciberresiliencia.

En la era de la digitalización, la ciberresiliencia es activo estratégico. No es un destino, es un viaje para el cual se alienta la aceptación proactiva de todas las partes interesadas internas y externas para arrumbar con éxito en un contexto cambiante, complejo y volátil. Es más que una función de costes, es un rasgo "cultural" que los clientes valorarán y los competidores envidiarán.

En definitiva, lo que está claro desde nuestra perspectiva es la necesidad de un cambio de narrativa, una visión diferente, a saber:

- De un enfoque reactivo a un enfoque proactivo al aceptar los ataques como incidentes de los que aprender.

- De enfocarse en mantener la continuidad operativa a corto plazo a una solución a largo plazo.

- De un mal necesario para evitar el caos inminente a una colosal oportunidad.

- De un bloqueador de negocios o Dr. No a ser un habilitador de negocios.

- De dejar de buscar al hombre del saco a buscar un competidor.

- De un "peso muerto" o un requisito engorroso exigido por las regulaciones a una fuente de ventaja competitiva a capitalizar.

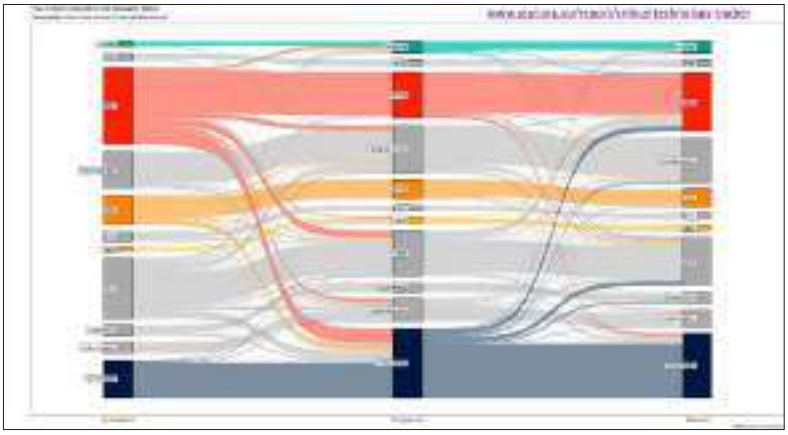
- De no contemplarse a ser una parte esencial (bajo la presión de los inversores) de ESG (Medio Ambiente, Social y Gobernanza).

4. ¿A dónde vamos?

Al objeto de responder a la cuestión suscitada en este apartado, necesariamente precario, en primer término, se propone tener en consideración la importante contribución que supone el trabajo del Instituto Australiano de Política Estratégica (ASPI) "Critical Technology Tracker de ASPI: la carrera mundial por la energía del futuro" [23], donde se plantea como problema primordial el hecho de que las democracias occidentales, también España, están perdiendo la competencia tecnológica global, sin excluir la carrera por los avances científicos y de investigación, y la capacidad de retener talento global, ingredientes cruciales que sustentan el desarrollo y control de las tecnologías más importantes del mundo, incluidas aquellas que aún no existen, lo cual se evidencia en el actual mapa del "tránsito de talentos" a nivel global (Ver Imagen 28).

23 https://techtracker.aspi.org.au/

Imagen 28



Para abordar una posible solución al respecto, en dicho estudio ASPI realiza una "Llamada de Atención" para las naciones democráticas, que deben buscar rápidamente algún avance tecnológico crítico estratégico, esto es, plantean que los gobiernos de todo el mundo deben trabajar, tanto en colaboración como individualmente, para alcanzar a China y, en términos más generales, deben prestar mayor atención al centro mundial de innovación tecnológica y competencia estratégica: el Indo-Pacífico.

¿Qué es lo que está pasando? ¿Hacia dónde podemos ir? ¿Cuál sería entonces, a tenor del trabajo de ASPI, lo que podemos hacer? La solución no es ni mucho menos simple ni sencilla, pero a los efectos de lo afrontado en este documento, desde mi perspectiva, creo que convendría tener muy presente la necesidad de hablar de un cambio cultural.

Creo que es necesario que las instituciones económicas, las empresas en general, la economía, adopte el concepto de ciberresilencia como bien común. Porque la resilencia cibernética es una función del ecosistema total. Se trata, por tanto, de promover la idea de la ciberresiliencia como otro bien común, esto es, reconocer que las empresas tienen responsabilidades básicas de ci-

berresiliencia y deberes fundamentales para operar de forma segura en una sociedad digital.

Creo que resulta perentorio lograr considerar que la ciberresiliencia sea una función del ecosistema total, como lo es la protección del medio ambiente. Si una empresa o nación no aborda las vulnerabilidades en última instancia dañará la seguridad de todos. Al mismo tiempo, elevar el nivel de ciberresiliencia para uno aumentará la protección para todos.

Creo que en este momento la resiliencia cibernética es lo más parecido a la conciencia que deberíamos tener todos con el medio ambiente. Habrá quien la tenga muy escasa, pero es un desafío muy similar. Y esto me gustaría que fuera comprendido por todos, pues aquellos países que no aborden las vulnerabilidades dañarán la seguridad de todos. Al mismo tiempo, elevar el nivel de resiliencia de uno, empresa, institución, país, aumentará la protección de todos.

Entonces, ¿cuál es el problema subsiguiente? Atención, les hablo como contable sobre lo que significa el análisis coste-beneficio, la debilidad intrínseca del análisis coste -beneficio al considerar este tema.

Ya ha sido comentado antes que se consideran muy pocos conceptos de coste. Se olvidan conceptos que van a venir luego. Pero es que también, y eso es muy grave, lo peor de todo es que se subestima el impacto que las vulnerabilidades y daños cibernéticos de una sola empresa tienen en el ecosistema digital más amplio, esto es, se omite incorporar el efecto de las externalidades negativas causadas a otras entidades económicas y a los ciudadanos.

Por tanto, no se invierte lo suficiente en ciberresiliencia en relación con el nivel de inversión socialmente óptimo. Además, las externalidades negativas también pueden crear un riesgo sistémico, que cae en cascada en componentes de su ecosistema o cadena de suministro o valor, con efectos adversos para la seguridad de todos. De ahí que, si solamente gastamos escasamente en segu-

ridad para nuestra empresa, es posible que no estemos contribuyendo al nivel de seguridad necesario para que la sociedad funcione correctamente. Tenemos que emplearnos de otra forma. El hecho de decir, esto no va conmigo, no puede tomarse como válido.

Abordar las externalidades negativas creadas por las debilidades de la seguridad cibernética de una empresa es una falla de mercado muy importante. Esto trae a primer plano cuestionarse sobre el papel adecuado del gobierno en la promoción del bien público de la ciberresiliencia. Se necesitan pasos audaces y coordinados para romper la tendencia anual insostenible de ataques cibernéticos cada vez más dañinos para crear un futuro digital más seguro.

En consecuencia, en aras de propiciar una mejor toma de decisiones sobre lo que debería ser la ciberresiliencia de un país, en nuestro caso España y, por tanto, con posible impacto directo en el plan de acción que pudiera llevar a cabo el INCIBE como baluarte de la seguridad que la transformación digital urge a nuestra economía, aquí y ahora podría propugnarse alguna iniciativa, que no dejaría de ser más que mera indicación de algo que se puede asumir o no asumir, por parte de quien sea. No es una llamada de atención ni al INCIBE, ni a la ministra del ramo, ni al presidente del gobierno, ni a la de Europa, ni siquiera, yo diría, al alcalde pedáneo de Aralla. A este respecto, dada la necesaria restricción que esta exposición conlleva, aquí se presentan dos políticas, una fiscal y otra educativa o de formación, con posible impacto, si fuera el caso, en dicho plan de acción, a saber:

A nivel de Política Fiscal, se trataría de ofrecer créditos fiscales para animar a las empresas y pymes a invertir en ciberseguridad. Creo que se debería de primar a las empresas y con créditos fiscales, eso sí, no a tutiplén ni a porrillo, sino segmentando claramente en función de las categorías de buenas prácticas de madurez, adaptabilidad, aceleración, cumplimiento, higiene y resiliencia de las actuaciones de seguridad que las mismas vayan llevando a cabo. Y, entonces, debería de haber una institución, podría ser el INCIBE si así se estimase, que, de alguna forma, pudiera certificar dichos niveles de

superación para que esas empresas pudieran disponer de esos créditos una vez que pasaran una especie de examen de que realmente han superando esas fases de resiliencia cibernética o cuando menos de lo que cabría denominar higiene en la seguridad.

A nivel de Política Educativa, se trataría de abordar uno de los principales problemas graves que tenemos en este campo como país, como lo es la necesidad de talento aplicado a la seguridad digital tan necesaria para alcanzar la transformación digital tan demanda de nuestras empresas, pymes e instituciones públicas. Creo que es perentorio definir, diseñar y poner en práctica un nivel de acreditación formativa de las competencias y habilidades del capital humano indispensable para obtener los niveles de ciberresiliencia antes citados, planteándose entonces una línea de actuación que bien pudiera denominarse "Academia de Ciberresiliencia".

5. Coda

Concluyo con el agradecimiento de haber contado con la generosidad de tan docta concurrencia y con el deseo de que esta disertación pudiera ser de algún interés, si cabe, al menos, como albor de una nueva agenda de investigación con innegable impacto socioeconómico o como un humilde intento de alentar la exploración de nuevas ventanas de oportunidad.

Por lo que les solicito me permitan volver a las palabras de Albert Einstein del inicio de la presente exposición: "Todos los imperios del futuro serán imperios del conocimiento, y solamente los pueblos que entiendan cómo generar conocimiento y cómo protegerlo, cómo buscar jóvenes que tengan capacidad para hacerlo y asegurarse de que se queden en el país, serán países exitosos".

Ahora más que nunca, debemos estar abiertos a aplicar estos aprendizajes y, al mismo tiempo, brindar a las personas creativas una amplia libertad para poner su toque humano en el funcionamiento de las máquinas inteligentes.

Pero también, antes de que sea demasiado tarde, todos debemos ver el espacio de posibilidades alucinantes de las próximas décadas y sopesarlos sabiamente con sus riesgos catastróficos.

De hecho, a medida que el potencial de estos avances llegue a la sociedad, las cosas a muchos nos van a parecer "mágicas" (Arthur C. Clarke, *dixit*). Ya se sabe, predecir qué dirección tomará todo lo comentado no es fácil. Los predictores usualmente sobreestiman qué tan rápido sucederán las cosas y subestiman los impactos a largo plazo. Pero, el sentido de escala, con su frenética Reina Roja azuzando "deprisa, más deprisa", sugiere que los cambios que se producirán en la mitad de este siglo serán tan inimaginables, a la par que más raudos y abruptos, que muchos de los mayores inventos acaecidos en toda la historia de la humanidad y esto no debe ni soslayarse ni exagerarse.

Si viajásemos en el tiempo, por ejemplo, a la época en que Herman Melville escribió la persecución de Moby Dick (1851) por Ahab, el capitán monomaníaco del barco ballenero Pequod, ¿qué tan sorprendidos estarían sus correligionarios de la ecúmene de Nantucket en Massachusetts, una de las primeras ciudades en el mundo en tener iluminación a base de aceite de ballena, con la multidimensionalidad de los usos actuales de la electricidad?

Eso, solo lo podemos imaginar. Pero, en otro viaje temporal a simplemente una década atrás, los expertos en el desarrollo tecnológico se sorprenderían al escuchar cuánto han disminuido los costes de la digitalización y cómo se ha exponenciado su despliegue tanto como los nuevos riesgos y vulnerabilidades que ha acarreado.

¿Qué tan sorprendidos estaremos en 2030? Eso, depende de lo que hagamos hoy.

De ahí, que me permitan insistir en las primeras consideraciones de la presente disertación, como ratificación afirmativa de lo enunciado por el ministro japonés al presentar el concepto de Sociedad 5.0, "estamos en un momento

transcendental de nuestra historia", pues, nunca como antes la humanidad ha experimentado tal peligro y oportunidad al mismo tiempo.

En consecuencia, si hubiera que sintetizar la desiderata de esta aportación en un párrafo, diría que nuestro sistema educativo debe preparar a las personas para el mundo que es y el que viene, no el que fue. Debe garantizar que las personas educadas encarnen las cualidades y competencias esenciales para la vida en una sociedad muy diferente a nuestro pasado industrial, de ahí que, en mi opinión, ya estamos tardando en reinventar la educación para producir graduados que sean exploradores multidisciplinarios, solucionadores de problemas, conectores de puntos, aprendices continuos y que no tengan miedo de desafiar el *status quo*.

Vale.

CLAUSURA DEL SOLEMNE ACTO ACADÉMICO

A LA BÚSQUEDA DE UNA NUEVA AXIOMÁTICA DE LA CIBERSEGURIDAD

Conferencia de clausura

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras

Nuestro encuentro en la Comunidad de Castilla y León toca a su fin. Y no podría hacerlo en un mejor lugar, después de la reunión universitaria salmantina, que en la leonesa sede del "Instituto Nacional de Ciberseguridad".

La colaboración de los colectivos castellano-leoneses y de los españoles miembros de la Real Academia de Ciencias Económicas y Financieras ha conseguido dejar claro algo que con tanta frecuencia se olvida: "Todo avance, sea científico o tecnológico, contiene unas incidencias positivas, **casi siempre** perceptibles mediante relaciones directas, primarias deberíamos decir, pero que a su vez provocan incidencias negativas, c**asi siempre** de segunda generación**.**

Apresurémonos a decir, de inmediato que, afortunadamente, las incidencias de segunda generación no son todas, ni mucho menos, negativas.

Hemos trabajando en este tema, durante años, junto con mi maestro el añorado Profesor Kaufmann. Fruto de esta colaboración fue la publica-

ción de una obra, **Modelos para la investigación de efectos olvidados,** a partir de la que elaboramos, después, la conocida Teoría de los Efectos Olvidados.[1]

Entre todas las incidencias de segunda generación, precisamente de talante negativo, una de ellas ha concitado la atención y preocupación de prácticamente todas las capas sociales a nivel planetario. Nos referimos a la posible pérdida de **libertad** (la máquina condiciona o dirige el pensamiento y la decisión del humano) y la **seguridad** (la programación de la máquina está sometida a interferencias externas que pueden modificar, en beneficio de terceros, los procedimientos y sobre todo los objetivos para los que fue establecida).

No escapará a la perspicacia de nuestros lectores que existe una íntima conexión, entre **libertad y seguridad,** de tal manera que el concepto de seguridad en sentido amplio, se acostumbra a contemplar, habitualmente, como concepto que incluye, también, el de libertad. No tenemos inconveniente en aceptarlo así, a los efectos de nuestro desarrollo posterior, que no es otro que un posible **diseño de cooperación** entre nuestras dos instituciones.

Para elaborar este deseado diseño es necesario encontrar, si existe, aquel o aquellos objetivos básicos, casi diría fundamentales, sobre los que existe un alto grado o nivel de **coincidencia.**

Pues bien, no dudo en afirmar, que este objetivo básico, fundamental, existe, y en ambas instituciones, destaca, entre los demás. Nos referimos al **humanismo** que inspira nuestras tareas, tanto en el Instituto Nacional de Ciberseguridad como en la Real Academia de Ciencias Económicas y Financieras del Instituto de España.

Ha bastado para convencernos de la idea inspiradora del humanismo en el Instituto, la revisión del contenido de algunas conferencias y trabajos de la

1 Kaufmann, A. y Gil Aluja, J.: Modelos para la investigación de efectos olvidados. Ed. Milladoiro, Vigo 1988 (ISBN: 84-404-3657-2).

Vicepresidenta primera y Ministra de Asuntos Económicos y Transformación Digital del Gobierno de España, Excma. Sra. Nadia Calviño.

Este viejo profesor no tiene autoridad alguno para hacer juicios de valor sobre los citados trabajos, aunque de hacerlo serían claramente positivos, pero sí creemos tener una modesta capacidad de expresar la buena impresión causada en nuestra Real Academia por el hecho de que nuestro país, España, ha sabido **adaptarse bien** a las dificultades surgidas desde el exterior de nuestra sociedad (Covid-19, invasión rusa de Ucrania, …) así como desde el interior de nuestro sistema social (burbuja financiera con la consecuente crisis económica de 2008, …). Esta ha sido la razón de lo conseguido.

Cuantas veces hemos escuchado en los años 60 y 70 del pasado Siglo XX, la potente voz de Kaufmann clamando: ¡ADAPTABILITÉ!

Otra idea maestra que desde hace dos decenios hemos repetido de manera insistente, figura, también, en el ideario de la Sra. Ministra Nadia Calviño: se trata de su percepción de la **celeridad de los cambios sociales.**

En efecto, suscribimos esta percepción de que vivimos en una sociedad tan compleja que, desde hace un tiempo, ha evolucionado unas veces de manera lenta y otras rápida, de manera profunda y en direcciones difícilmente predeterminables.

Pero desde hace algunos decenios, nos hemos vistos inmersos en un proceso de aceleración tal que, lo que antes era un **simple conjunto** de humanos con relaciones simples, se ha convertido, ya, en un **sistema** con interrelaciones que no solo provocan incidencias directas sino también de segunda, tercera y sucesivas generaciones.

El cerebro del humano, compendio de organización y eficacia para la consecución de los objetivos que justifican su existencia, actúa apelando a lo que nosotros, pobres mortales, llamamos **razón** y **emoción**. En palabras lisas

y llanas, de **manera objetiva** y de **manera subjetiva,** a un mayor o menor "grado" o "nivel" la una que la otra, según estímulos internos o externos, de distinta naturaleza.

Y, en este estadio de nuestro relato, podemos presentar una aportación que esperamos sea de utilidad si deseamos iluminar de manera, creemos, clara nuestra coincidente posición.

Para ello hemos recurrido a un concepto, de otro ámbito científico: nos referimos a la noción de **entropía,** reformulándola para darle el sentido que necesitamos en economía: "La valuación del desorden".

Hemos acuñado, así, la noción de: playa de entropía, en donde se pasean, a lo largo de su vida, los cerebros de los humanos, desde un extremo, la actividad totalmente desordenada, desestructurada, selvática (sin ánimo de menosprecio) al otro extremo, la actividad totalmente ordenada, rígida, mecánica (sin ánimo de menosprecio).

A medida que el desplazamiento tiene lugar desde el extremo del "orden" hacia el extremo del "desorden", el cerebro utiliza más el "sentimiento" que la "razón" y viceversa.

Esto por sí solo ya explica una cantidad de fenómenos cotidianos de nuestra vida en sociedad. Un ejemplo será suficiente, creemos:

La compra de víveres en un supermercado, no es habitualmente la misma si la realizamos con el estómago vacío, antes de comer, que si tiene lugar después de una buena comida, con el estomago lleno. Y sin embargo el precio de los bienes de consumo es el mismo.

Nos hemos permitido escoger este, entre los muchos ejemplos posibles, por cuanto sirvió ya en épocas pretéritas, para distinguir entre **precio** y **utilidad**: "Pretium ex re ipsa aestimatur obnibusque ídem est, emolumentum ex

conditione personae" (el precio de una cosa es igual para todo el mundo, la satisfacción es diferente de un humano a otro).

Y, antes de partir, una vez concluida nuestra tarea, desearíamos presentar nuestras credenciales con la esperanza de que sea atendido nuestro deseo de una **colaboración científica** entre nuestras respectivas instituciones.

Creemos, sinceramente, que no solo las coincidencias, algunas de ellas las hemos citado como ejemplo, que existen en nuestros respectivos idearios lo aconsejan, también lo avalan nuestra trayectoria anterior y los proyectos futuros inmediatos, ya aprobados por nuestra Junta de Gobierno, algunos de los cuales se hallan en pleno funcionamiento, como el Seminario Internacional "Ciberseguridad en el mundo" a celebrar los días 25 y 26 de mayo próximo en el que ya han comprometido su participación miembros de la red "Barcelona Economics Network" y Académicos Correspondientes extranjeros de la RACEF.

Pretendemos obtener con este Seminario información de primera mano en relación al marco jurídico de la ciberseguridad de los países participantes y, de manera prioritaria, las opiniones de tan autorizadas personalidades sobre su **evolución futura**.

Pero hay más, mucho más, sobre la potencialidad alcanzable con una posible colaboración: aprovechar, intensificando nuestros trabajos, la inercia creativa en la que nos ha colocado el resurgimiento de la **Escuela de Economía Humanista de Barcelona,** que está cambiando los cimientos de las investigaciones pioneras en economía, cambio obligado por la propia sociedad, cada vez más compleja y plagada de incertidumbres.

La sustitución del "homo economicus" por el "humano" pura y simplemente, y el "principio del tercio excluso" por el "principio de simultaneidad gradual" constituyen una plataforma simpar para sostener una **axiomática general** que, tras las pertinentes adaptaciones al nuevo objeto de estudio, po-

dría ser de gran valor para una formalización científica del gran edificio de la ciberseguridad.

Partimos, en nuestro empeño, por establecer una axiomática para el ideario humanista de la economía de los cuatro axiomas fundamentales siguientes:

1.- Axioma de la existencia: la plenitud viva del humano es de naturaleza intelectual.

2.- Axioma de extensión: el deber fundamental del humano consiste en contribuir a la promoción de los demás humanos.

3.- Axioma de regulación: la incorporación de humano a la corriente promocional es libre.

4.- Axioma de posibilidades intelectuales: mediante una pedagogía adecuada, todo humano puede promocionar en el conocimiento, sea cual fuera su edad, sea cual sea su género y sea cual sea su posición en la sociedad.

A estos axiomas nos hemos permitido añadir, para el caso que nos ocupa, un quinto. El siguiente:

5.- Axioma de no contradicción: en toda creación o innovación, sea formal o material, sea científica o técnica, cohabitan, para el objetivo buscado, incidencias positivas y negativas.

Esta es, entre otras aportaciones básicas, la que podemos ofrecer, junto con los conceptos y operadores incorporados, para iniciar la tarea común de reconvertir desde los más sólidos fundamentos, la Ciberseguridad del mañana, con métodos, modelos y algoritmos que, dentro de la Inteligencia Artificial (I.A.), permitan reducir o incluso anular, los potenciales componentes negativos que lleva aparejada la eclosión cibernética.

Nuestros brazos están abiertos y cuanto se ha logrado hasta ahora está encima de la mesa.

El deseado convenio de colaboración, libre y flexible queda a su disposición.

Gracias, muchas gracias.

Real Academia
de Ciencias Económicas y Financieras

PUBLICACIONES DE LA REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

*Las publicaciones señaladas con el simbolo
están disponibles en formato PDF en nuestra página web:
https://racef.es/es/publicaciones

***Las publicaciones señaladas con el símbolo o
están disponibles en nuestros respectivos canales de Youtube y Vimeo

PUBLICACIONES DEL OBSERVATORIO DE INVESTIGACIÓN ECONÓMICA Y FINANCIERA

M-24/11 *Nuevos mercados para la recuperación económica: Azerbaiyán.*

M-30/12 *Explorando nuevos mercados: Ucrania, 2012. (Incluye DVD con textos en ucraniano), 2012.*

M-38/15 *Desarrollo de estrategias para la cooperación económica sostenible entre España y México, 2015.*

M-41/16 *Cuba a la luz de la Nueva Ley de Inversiones Extranjeras: Retos y oportunidades para la economía catalana, (Estudio elaborado por el Observatorio de Investigación Económico- Financiera), 2016.*

MO-47/16 *Colombia: la oportunidad de la paz. Estudio sectorial para la inversión de empresas españolas en el proceso de reconciliación nacional (Estudio del Observatorio de Investigación Económico-Financiera de la RACEF).*

MO-50/17 *La gestión y toma de decisiones en el sistema empresarial cubano. Gil Lafuente, Anna Maria; García Rondón, Irene; Souto Anido, Lourdes; Blanco Campins, Blanca Emilia; Ortiz, Torre Maritza; Zamora Molina, Thais.*

MO-52/18 *Efectos de la irrupción y desarrollo de la economía colaborativa en la sociedad española. Gil Lafuente, Anna Maria; Amiguet Molina, Lluís; Boria Reverter, Sefa; Luis Bassa, Carolina; Torres Martínez, Agustín; Vizuete Luciano, Emilio.*

MO-53/19 *Índice de equidad de género de las comunidades autónomas de España: Un análisis multidimensional. Gil Lafuente, Anna Maria; Torres Martínez, Agustín; Boria Reverter, Sefa; Amiguet Molina, Lluís.*

MO-54/19 *Sistemas de innovación en Latinoamérica: Una mirada compartida desde México, Colombia y Chile. Gil-Lafuente, Anna M.; Alfaro-García, Víctor G.; Alfaro-Calderón, Gerardo G.; Zaragoza-Ibarra, Artemisa; Goméz-Monge, Rodrigo; Solís-Navarrete, José A.; Ramírez-Triana, Carlos A.; Pineda-Escobar, María A.; Rincón-Ariza, Gabri- ela; Cano-Niño, Mauricio A.; Mora-Pardo, Sergio A.; Nicolás, Carolina; Gutiérrez, Alexis; Rojas, Julio; Urrutia, Angélica; Valenzuela, Leslier; Merigó, José M.*

MO-56/19 *Kazakhstan: An Alliance or civilizations for a global challenge. Ministry of National Economy of the Republic of Kazakhstan – Institute of Economic Research; Royal Academy of Economic and Financial Sciences of Spain.*

MO-60/19 *Medición de las capacidades de innovación en tres sectores primarios en Colombia. Efectos olvidados de las capacidades de innovación de la quínoa, la guayaba y apícola en Boyacá y Santander. Blanco-Mesa, Fabio; León-Castro, Ernesto; Velázquez-Cázares, Marlenne; Cifuentes-Valenzuela, Jorge; Sánchez-Ovalle, Vivian Ginneth.*

MO-61/19 *El proceso demográfico en España: análisis, evolución y sostenibilidad. Gil-Lafuente, Anna M.; Torres-Martínez, Agustín; Guzmán-Pedraza, Tulia Carolina; Boria-Reverter, Sefa.*

MO-64/20 *Capacidades de Innovación Ligera en Iberoamérica: Impliaciones, desafíos y sinergias sectoriales hacia el desarrollo económico multilateral. Alfaro-García, VG.; Alfaro-Calderón, GG.; García-Orozco, D.; Zaragoza-Ibarra, A.; Boria-Reverter, S.; Gómez-Monge, R.*

MO-65/20 *El adulto mayor en España: Los desafíos de la sociedad ante el envejecimiento. Gil-Lafuente, Anna M.; Torres-Martínez, Agustín; Guzmán-Pedraza, Tulia Carolina; Boria-Reverter, Sefa.*

MO-68/21 *Public policy to handle aging: the seniors' residences challenge / Políticas para la gestión pública del envejecimiento: el desafío de las residencias para personas mayores. Kydland, F.; Kydland, T.; Valero Hermosilla, J. y Gil-Lafuente, Ana M.*

MO-70/21 *Ecología y tecnología para una nueva economía poscovid-19. Ana María GilLafuente, Agustín Torres-Martínez, Tulia Carolina Guzmán-Pedraza, Sefa Boria-Reverter.*

OTRAS PUBLICACIONES Y COEDICIONES DE LA REAL ACADEMIA

M-1/03 *De Computis et Scripturis (Estudios en Homenaje al Excmo. Sr. Dr. Don Mario Pifarré Riera), 2003.*

M-2/04 *Sesión Académica de la Real Academia de Ciencias Económicas y Financieras en la Académie du Royaume du Maroc (Publicación del Solemne Acto Académico en Rabat el 28 de mayo de 2004), 2004.*

M-3/05 *Una Constitución para Europa, estudios y debates (Publicación del Solemne Acto Académico del 10 de febrero de 2005, sobre el "Tratado por el que se establece una Constitución para Europa"), 2005.*

M-4/05 *Pensar Europa (Publicación del Solemne Acto Académico celebrado en Santiago de Compostela, el 27 de mayo de 2005), 2005.*

M-5/06 *El futuro de las relaciones euromediterráneas (Publicación de la Solemne Sesión Académica de la R.A.C.E.F. y la Universidad de Túnez el 18 de marzo de 2006), 2006.*

M-6/06 *Veinte años de España en la integración europea (Publicación con motivo del vigésimo aniversario de la incorporación de España en la Unión Europea), 2006.*

M-7/07 *La ciencia y la cultura en la Europa mediterránea (I Encuentro Italo-Español de la Real Academia de Ciencias Económicas y Financieras y la Accademia Nazionale dei Lincei), 2007.*

M-8/07 *La responsabilidad social de la empresa (RSE). Propuesta para una nueva economía de la empresa responsable y sostenible, 2007.*

M-9/08 *El nuevo contexto económico-financiero en la actividad cultural y científica mediterránea (Sesión Académica internacional en Santiago de Compostela), 2008.*

M-10/08 *Pluralidad y unidad en el pensamiento social, técnico y económico europeo (Sesión Académica conjunta con la Polish Academy of Sciences), 2008.*

M-11/08 *Aportación de la ciencia y la cultura mediterránea al progreso humano y social (Sesión Académica celebrada en Barcelona el 27 de noviembre de 2008), 2009.*

M-12/09 *La crisis: riesgos y oportunidades para el Espacio Atlántico (Sesión Académica en Bilbao), 2009.*

M-13/09 *El futuro del Mediterráneo (Sesión Académica conjunta entre la Montenegrin Academy of Sciences and Arts y la Real Academia de Ciencias Económicas y Financieras, celebrada en Montenegro el 18 de mayo de 2009), 2009.*

M-14/09 *Globalisation and Governance (Coloquio Internacional entre la Real Academia de Ciencias Económicas y Financieras y el Franco-Australian Centre for International Research in Management Science (FACIREM), celebrado en Barcelona los días 10-12 de noviembre de 2009), 2009.*

M-15/09 *Economics, Management and Optimization in Sports. After the Impact of the Financial Crisis (Seminario Interncional celebrado en Barcelona los días 1-3 de diciembre de 2009), 2009.*

M-16/10 *Medición y Evaluación de la Responsabilidad Social de la Empresa (RSE) en las Empresas del Ibex 35, 2010.*

M-17/10 *Desafío planetario: desarrollo sostenible y nuevas responsabilidades (Solemne Sesión Académica conjunta entre l'Académie Royale des Sciences, des Lettres et des Beaux-Arts de Bélgica y la Real Academia de Ciencias Económicas y Financieras de España, en Bruselas el día 8 de Junio de 2010), 2010.*

M-18/10 *Seminario analítico sobre la casuística actual del derecho concursal (Sesión Académica celebrada el 4 de junio de 2010), 2010.*

M-19/10 *Marketing, Finanzas y Gestión del Deporte (Sesión Académica celebrada en la Real Academia de Ciencias Económicas y Financieras en diciembre de 2009). 2010*

M-20/10 *Optimal Strategies in Sports Economics and Management (Libro publicado por la Editorial Springer y la Real Academia de Ciencias Económicas y Financieras). 2010*

M-21/10 *El encuentro de las naciones a través de la cultura y la ciencia (Solemne Sesión Académica conjunta entre la Royal Scientific Society de Jordania y la Real Academia de Ciencias Económicas y Financieras de España, en Amman el día 8 de noviembre de 2010). 2010.*

M-21B/10 *Computational Intelligence in Business and Economics (Proceedings de MS´10 International Conference celebrada en Barcelona los días 15-17 de julio de 2010). Edición de World Scientific, 2010.*

M-22/11 *Creación de valor y responsabilidad social de la empresa (RSE) en las empresas del IBEX 35. 2011.*

M-23/11 *Incidencia de las relaciones económicas en la recuperación económica del área mediterránea (VI Acto Internacional celebrado en Barcelona el 24 de febrero de 2011), (Incluye DVD con resúmenes y entrevistas de los ponentes) 2011.*

M-25/11 *El papel del mundo académico en la sociedad del futuro (Solemne Sesión Académica en Banja Luka celebrada el 16 de mayo de 2011), 2011.*

M25B/11 *Globalisation, governance and ethics: new managerial and economic insights (Edición Nova Science Publishers), 2011.*

M-26/12 *Decidir hoy para crear el futuro del Mediterráneo (VII acto internacional celebrado el 24 de noviembre de 2011), 2012.*

M-27/12 *El ciclo real vs. el ciclo financiero un analisis comparativo para el caso español. Seminario sobre política anticíclica, 2012.*

M-28/12 *Gobernando las economías europeas. La crisis financiera y sus retos. (Solemne Sesión Académica en Helsinki celebrada el 9 de febrero de 2012), 2012.*

M-29/12 *Pasado y futuro del área mediterránea: consideraciones sociales y económicas (Solemne Sesión Académica en Bejaia celebrada el 26 de abril de 2012), 2012.*

M-31/13 *Why austerity does not work: policies for equitable and sustainable growth in Spain and Europe (Conferencia del académico correspondiente para Estados Unidos, Excmo. Sr. Dr. D. Joseph E. Stiglitz, Pronunciada en Barcelona en diciembre de 2012), 2013.*

M-32/13 *Aspectos micro y macroeconómicos para sistemas sociales en transformación (Solemne Sesión Académica en Andorra celebrada el 19 de abril de 2013), 2013.*

M-33/13 *La unión europea más allá de la crisis (Solemne Sesión Académica en Suiza celebrada el 6 de junio de 2013), 2013.*

M-33B/13 *Decision Making Sytems in Business Administration (Proceedings de MS'12 International Conference celebrada en Río de Janeiro los días 10-13 de diciembre de 2012). Edición de World Scientific, 2013.*

M-34/14 *Efectos de la evolución de la inversión pública en Educación Superior. Un estudio del caso español y comparado (Trabajo presentado por la Sección Primera de la Real Academia de Ciencias Económicas y Financieras), 2014.*

M-35/14 *Mirando el futuro de la investigación científica (Solemne Acto Académico Conjunto celebrado en Bakú el 30 de mayo de 2014), 2014.*

M-36/14 *Decision Making and Knowledge Decision Support Systems (VIII International Conference de la RACEF celebrada en Barcelona e International Conference MS 2013 celebrada en Chania Creta. Noviembre de 2013). Edición a cargo de Springer, 2014.*

M-37/14 *Revolución, evolución e involución en el futuro de los sistemas sociales (IX Acto internacional celebrado el 11 de noviembre de 2014), 2014.*

M-39/15 *Nuevos horizontes científicos ante la incertidumbre de los escenarios futuros (Solemne Acto Académico Conjunto celebrado en Cuba el 5 de mayo de 2015), 2015.*

M-40/15 *Ciencia y realidades económicas: reto del mundo post-crisis a la actividad investigadora (X Acto Internacional celebrado el 18 de noviembre de 2015), 2015.*

ME-42/16 *Vivir juntos (Trabajo presentado por la Sección Tercera de la Real Academia de Ciencias Económicas y Financieras), 2016.*

MS-43/16 *¿Hacia dónde va la ciencia económica? (Solemne Acto Académico Conjunto con la Universidad Estatal de Bielorrusia, celebrado en Minsk el 16 de mayo de 2016), 2016.*

MS-44/16 *Perspectivas económicas frente al cambio social, financiero y empresarial(Solemne Acto Académico Conjunto con la Universidad de la Rioja y la Fundación San Millán de la Cogolla, celebrado en La Rioja el 14 de octubre de 2016), 2016.*

MS-45/16 *El Comportamiento de los actores económicos ante el reto del futuro (XI Acto Internacional de la Real Academia de Ciencias Económicas y Financieras, celebrado en Barcelona el 10 de noviembre de 2016), 2016.*

MS-46/17 *El agua en el mundo-El mundo del agua/ Water in the world- The World of Water (Nueva Edición Bilingüe Español-Inglés del Estudio a cargo del Prof. Dr. Jaime Lamo de Espinosa, publicada con motivo del 150 aniversario de Agbar), 2017.*

MS-48/17 *El pensamiento económico ante la variedad de espacios españoles (Solemne Acto Académico conjunto con la Universidad de Extremadura y la Junta de Extremadura celebrado los días 2-3 de marzo de 2017), 2017.*

MS-49/17 *La economía del futuro en Europa. Ciencia y realidad. Calmîc, Octavian; Aguer Hortal, Mario; Castillo, Antonio; Ramírez Sarrió, Dídac; Belostecinic, Grigore; Rodríguez Castellanos, Arturo; Bîrcă, Alic; Vaculovschi, Dorin; Metzeltin, Michael; Verejan, Oleg; Gil Aluja, Jaime.*

MS-51/17 *Las nuevas áreas del poder económico (XII Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 16 de noviembre de 2017), 2017.*

MS-53/18 *El reto de la prosperidad compartida. El papel de las tres culturas ante el siglo XXI. Solemne acto académico conjunto con la Fundación Tres Culturas del Mediterráneo (Barcelona Economics Network). Askenasy, Jean; Imanov, Gorkmaz; Granell Trias, Francesc; Metzeltin, Michael; Bernad González, Vanessa; El Bouyoussfi, Mounir; Ioan Franc, Valeriu; Gutu, Corneliu.*

MS-54/18 *Las ciencias económicas y financieras ante una sociedad en transformación. Solemne Acto Académico conjunto con la Universidad de León y la Junta de Castilla y León, celebrado el 19 y 20 de abril de 2018. Rodríguez Castellanos, Arturo; López González, Enrique; Escudero Barbero, Roberto; Pont Amenós, Antonio; Ulibarri Fernández, Adriana; Mallo Rodríguez, Carlos; Gil Aluja, Jaime.*

MV-01/18 *La ciencia y la cultura ante la incertidumbre de una sociedad en transformación (Acto Académico de la Real Academia de Ciencias Económicas y Financieras en la Universidad de Tel Aviv celebrado el 15 y 16 de mayo de 2018), 2018.*

MS-55/19 *Desafíos de la nueva sociedad sobrecompleja: Humanismo, dataísmo y otros ismos (XIII Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 15 y 16 de noviembre de 2018), 2018.*

MS-57/19 *Complejidad Financiera: Mutabilidad e Incertidumbre en Instituciones, Mercados y Productos. Solemne Acto Académico Conjunto entre la Universitat de les Illes Balears, la Real Academia de Ciencias Económicas y Financieras de España, el Cercle Financer de Balears, el Colegio de Economistas de las Islas Baleares y el Cercle d'Economia de Mallorca, celebrado los días 10-12 de abril de 2019. Rodríguez Castellanos, Arturo; López González, Enrique; Liern Carrión, Vicente; Gil Aluja, Jaime.*

ME-58/19 *Un ensayo humanista para la formalización económica. Bases y aplicaciones (Libro Sección Segunda de la Real Academia de Ciencias Económicas y Financieras), 2019.*

MS-59/19 *Complejidad Económica: Una península ibérica más unida para una Europa más fuerte. Solemne Acto Académico Conjunto entre la Universidad de Beira Interior – Portugal y la Real Academia de Ciencias Económicas y Financieras de España, celebrado el día 19 de junio de 2019. Askenasy, Jean; Gil Aluja, Jaime; Gusakov, Vladimir; Hernández Mogollón, Ricardo; Imanov, Korkmaz; Ioan-Franc, Valeriu; Laichoubi, Mohamed; López González, Enrique; Marino, Domenico; Redondo López, José Antonio; Rodríguez Rodríguez, Alfonso; Gil Lafuente, Anna Maria.*

MS-62/20 *Migraciones (XIV Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 14 y 15 de noviembre de 2019), 2019.*

MS-63/20 *Los confines de la equidad y desigualdad en la prosperidad compartida. Solemne Acto Académico Conjunto entre la Universidad de Cantabria y la Real Academia de Ciencias Económicas y Financieras, celebrado los días 7 y 8 de mayo de 2020. Ramírez Sarrió, Dídac; Gil Aluja, Jaime; Rodriguez Castellanos, Arturo; Gasòliba, Carles; Guillen, Montserrat; Casado, Fernando; Gil-Lafuente, Anna Maria, Sarabia Alegría, José María.*

MS-66/21 *La vejez: conocimiento, vivencia y experiencia (XV Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 10 y 20 de noviembre de 2020), 2020.*

MS-67/21 *Sistemas de pensiones para una longevidad creciente. Una mirada a los sistemas de pensiones en Bielorrusia, España, Finlandia, México y Suiza. Daniel i Gubert, Josep; Wanner, Jean-Marc; Gusakov, Vladimir; Kiander, Jaakko; González Santoyo, Federico; Flores Romero, Beatriz; Gil-Lafuente, Ana Maria; Guillen, Montserrat. 2021.*

MS-69/21 *Ciencia y actividad económica: propuestas y realidades (Trabajos correspondientes al I Ciclo de Conferencias Internas). Gil Aluja, Jaime; Granell Trias, Francesc; Aguer Hortal, Mario; Ramírez Sarrió, Dídac; Argandoña Rámiz, Antonio; Liern Carrión, Vicente; Gil-Lafuente, Ana María. 2021.*

MS-71/22 *Incidencias económicas de la pandemia. Problemas y oportunidades. Solemne Acto Académico Conjunto entre la Universidad de Valencia y la Real Academia de Ciencias Económicas y Financieras, celebrado los días 21 y 22 de octubre de 2021. Gil Aluja, Jaime; Aguer Hortal, Mario; Maqueda Lafuente, Francisco Javier; Ramírez Sarrió, Dídac; Liern Carrión, Vicente; Rodríguez Castellanos, Arturo; Guillén Estany, Montserrat.*

MS-72/22 *La nueva economía después del Sars-Cov-2. Realidades y revolución tecnológica. (XVI Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 18 y 19 de noviembre de 2021), 2021.*

ME-73/22 *El Banco Central Europeo y la crisis financiera (2007-2018). Sección de Ciencias Económicas de la Real Academia de Ciencias Económicas y Financieras. Argandoña Rámiz, Antonio; Castells Oliveres, Antoni. 2022.*

MS-74/22 *Ciencia y actividad económica: propuestas y realidades (Trabajos correspondientes al II Ciclo de Conferencias Internas). Gil Aluja, Jaime; Rodríguez Rodríguez, Alfonso; Guillén Estany, Montserrat; Rodríguez Castellanos, Arturo; Lago Peñas, Santiago; Barquero Cabrero, José Daniel; López González, Enrique. 2022.*

MS-75/22 *Soluciones económicas y tecnológicas a la degradación del ecosistema del planeta. (I Seminario Internacional Abierto de Barcelona de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 8 y 9 de junio de 2022) ,2022.*

ME-76/22 *Economistas Españoles Relevantes de los siglos XVIII, XIX y XX. Real Academia de Ciencias Económicas y Financieras. Aguer Hortal, Mario. 2022.*

MS-77/23 ¿Por qué no un Mundo Sostenible? La Ciencia Económica va a su encuentro. *(XVII Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 16 y 17 de noviembre de 2022) ,2022.*

MS-78/23 *Los nuevos desafíos y oportunidades de la transformación digital de la economía española. (Solemne Acto Académico conjunto entre la Universidad de Salamanca y la Real Academia de Ciencias Económicas y Financieras celebrado en Salamanca el 15 de marzo de 2023) ,2023.*

MS-79/23 La Ciberseguridad como imperativo para la Economía de España. *(Solemne Acto Académico conjunto entre el Instituto Nacional de Ciberseguridad y la Real Academia de Ciencias Económicas y Financieras celebrado en León el 17 de marzo de 2023) , 2023.) ,2023.* 

Los orígenes más remotos de la Real Academia de Ciencias Económicas y Financieras de España se remontan al siglo XVIII, cuando en 1758 se crea en Barcelona la Real Junta Particular de Comercio.

El espíritu inicial que la animaba entonces ha permanecido hasta nuestros días: el servicio a la sociedad, a partir del estudio y de la investigación., es decir, actuar desde la razón y desde el humanismo. De ahí las palabras que aparecen en su escudo y medalla: "Utraque Unum".

La forma actual de la Real Corporación tiene su gestación en la década de los años 30 del pasado siglo. Su recreación se produce el 16 de mayo de 1940. En 1958 adopta el nombre de Real Academia de Ciencias Económicas y Financieras. En el año 2017 se incorpora, con todos los honores, en la máxima representación científica española: el Instituto de España.

En estos últimos años se ha potenciado de tal manera la internacionalización de la Real Academia de Ciencias Económicas y Financieras de España que hoy es considerada la Real Academia con mayor número de convenios de Colaboración Científica de nuestro país.

Su alto prestigio se ha asentado, principalmente, en cuatro direcciones. La primera de ellas, es la incorporación de grandes personalidades del mundo académico y de la actividad económica de los estados y de las empresas, con seis Premios Nobel, cuatro ex Jefes de Estado y varios Primeros Ministros.

La segunda, es la realización anual de sesiones científicas en distintos países junto con altas instituciones académicas de otros Estados, con los que se han firmado acuerdos de colaboración.

En tercer lugar, se están elaborando trabajos de estudio y análisis sobre la situación y evolución de los sistemas económico-financieros de distintas Naciones, con gran repercusión, no sólo en los ámbitos propios de la formalización científica, sino también en la esfera de las relaciones económicas, empresariales e institucionales.

En cuarto lugar, su principal, aunque no exclusivo, ámbito de trabajo se ha focalizado en la búsqueda y hallazgo de una vía de investigación nueva en el campo económico desde sus mismas raíces, con objeto de incorporar, numéricamente, el inevitable grado o nivel de subjetividad del pensamiento y decisión de los humanos.

Por ello, la Real Academia de Ciencias Económicas y Financieras es conocida mundialmente por cuanto sus componentes forman parte y protagonizan la llamada **Escuela de Economía Humanista de Barcelona**.

La inmortalidad académica, cobra, así, su más auténtico sentido.

Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas
y Financieras de España

Real Academia de Ciencias Económicas y Financieras

SESIONES ACADÉMICAS NACIONALES

JUNTA DE GOBIERNO

MS-79/23

LA CIBERSEGURIDAD COMO IMPERATIVO PARA LA ECONOMÍA DE ESPAÑA

SOLEMNE ACTO ACADÉMICO CONJUNTO ENTRE EL INSTITUTO NACIONAL DE CIBERSEGURIDAD Y LA REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

La Real Academia de Ciencias Económicas y Financieras tiene como una de sus misiones organizar actos académicos en diferentes sedes de la geografía española. Este año 2023 como consecuencia de una de las líneas de trabajo emprendidas en nuestra Real Corporación se desarrollaron unas jornadas de investigación que tuvieron lugar en la sede del Instituto Nacional de Ciberseguridad en León quien ha acogido las sesiones académicas.

Las aportaciones científicas al encuentro que lleva por título: "La Ciberseguridad como imperativo para la Economía de España" giraron en torno a los sistemas de digitalización como motor de la nueva economía y la transformación social así como la sostenibilidad tecnológica como proceso de adaptación permanente.

La actividad científica y académica de la RACEF siempre sigue adelante adaptándose a las vicisitudes del entorno y fiel al mandato que tiene encomendado. En esta ocasión se ha asumido el reto de trabajar sobre una temática en pleno desarrollo e implementación con consecuencias económicas y sociales que están provocando una profunda reestructuración de los sistemas socioeconómicos. Analizar los retos y las oportunidades que este proceso de transformación digital comporta permitirá alcanzar niveles de bienestar sostenible sin precedentes en la historia de la humanidad.

INSTITVTO D ESPAÑA

Real Academia
de Ciencias Económicas y Financieras