ACTOS INTERNACIONALES EN BARCELONA

Real Academia de Ciencias Económicas y Financieras

LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONÓMICAS

II SEMINARIO INTERNACIONAL DE PRIMAVERA DE BARCELONA

Barcelona, 24 y 25 de mayo de 2023

LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONÓMICAS
(II Seminario Internacional de primavera de Barcelona)

La realización de esta publicación
ha sido posible gracias a

MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES

con la colaboración de

Fundación "la Caixa"

con el patrocinio de

Generalitat de Catalunya
Departament
de Justícia

LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONÓMICAS

(II Seminario Internacional de primavera de Barcelona)

Publicaciones de la Real Academia de Ciencias Económicas y Financieras

Real Academia de Ciencias Económicas y Financieras
"La Ciberseguridad en la Ciencia y en las Actividades Económicas" / Real Academia de Ciencias Económicas y Financieras.

Bibliografía
ISBN- 978-84-09-57484-1

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

1. Economía 2. Tecnología 3. Transformación

La Academia no se hace responsable de las opiniones científicas expuestas en sus propias publicaciones.
(Art. 41 del Reglamento)

Editora: ©2024 Real Academia de Ciencias Económicas y Financieras, Barcelona.
Fotografía portada: www.freepik.es
Académica Coordinadora: Dra. Ana Maria Gil-Lafuente

ISBN- 978-84-09-57484-1

Depósito legal: B 22391-2023

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.

Imprime: Ediciones Gráficas Rey, S.L.—c/Albert Einstein, 54 C/B, Nave 12-14-15
Cornellà de Llobregat—Barcelona
Impresión Enero 2024

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

BARCELONA ECONOMICS NETWORK

SEMINARIO INTERNACIONAL DE PRIMAVERA DE BARCELONA

II EDICIÓN

24-25 DE MAYO DE 2023

"La Ciberseguridad en la Ciencia y en las Actividades Económicas"

ACTO ACADÉMICO

APERTURA Y PRESENTACIÓN PRIMERA JORNADA

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"Ciberseguridad: mensaje de España al mundo"

PRIMERA SESIÓN ACADÉMICA

Dr. Petre Roman
Miembro de la Barcelona Economics Network
"Incertidumbres y falta de coherencia generadas por la cyberciencia (Inteligencias Artificiales) en la sociedad y en el campo económico en particular"

SEGUNDA SESIÓN ACADÉMICA

Sr. Enrique Lecumberri Matí
Académico de Número de la Real Academia de Ciencias Económicas y Financieras
"Tendencias y desafíos en la ciberseguridad actual: Una mirada desde la perspectiva empresarial"

Dra. Ana Maria Gil-Lafuente
Académica de Número de la Real Academia de Ciencias Económicas y Financieras
"Una revisión Bibliométrica de la investigación sobre Ciberseguridad y negocios, 2004-2022"

Tercera Sesión Académica

Dr. Valeriu Ioan Franc
Académico Correspondiente por Rumanía de la Real Academia de Ciencias Económicas y Financieras
"Cyber-Economy, le paradox de la Roumanie"

Dr. Korkmaz Imanov
Académico Correspondiente por Azerbaiyán de la Real Academia de Ciencias Económicas y Financieras
"Interval-Valued intuitionistic fuzzy model for simulation of Azerbaijan national cyber security index"

Segunda Jornada

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"Un momento para la memoria de Eugen Simion"

Cuarta Sesión Académica

Dr. Domenico Marino
Miembro de la Barcelona Economics Network
"Guidelines for the development of cybersecurity economics"

Quinta Sesión Académica

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"Ensayo de un algoritmo para la gestión de la Ciberseguridad"

Dr. Dobrica Milovanovic
Miembro de la Barcelona Economics Network
"Cybersecurity context in Serbia: Legislative and strategic framework"

Séptima Sesión Académica

Dr. Carlo Morabito
Miembro de la Barcelona Economics Network
"Deep learning and explainable AI approaches to automatic vulnerability detection and classification for improved cyber-resilience"

Dr. Enrique López González
Académico de Número de la Real Academia de Ciencias Económicas y Financieras
"Finanzas sostenibles en la era del argocapitalismo: el papel de la ciberresiliencia"

Octava Sesión Académica

Dr. José Daniel Barquero
Académico de Número de la Real Academia de Ciencias Económicas y Financieras
"Economía y ciberdelicuencia cuántica"

Dr. Janusz Kacprzyk
Academico Correspondiente por Polonia de la Real Academia de Ciencias Economicas y Financieras
"Cybersecurity: economic and non- economic aspects"

Dr. Mario Aguer
Académico de Número de la Real Academia de Ciencias Económicas y Financieras
"El humanismo como marco de la actividad empresarial"

Clausura del II Acto Internacional de Primavera de Barcelona

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"El tratamiento de la subjetividad, un nuevo horizonte para la ciberseguridad"

ÍNDICE

REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

BARCELONA ECONOMICS NETWORK

SEMINARIO INTERNACIONAL DE PRIMAVERA DE BARCELONA II EDICIÓN

24 - 25 de mayo de 2023

“LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONOMICAS”

Apertura y Presentación

Sesión Académica

Clausura del II Acto Internacional de Primavera de Barcelona

GUIDELINES FOR THE DEVELOPMENT OF CYBERSECURITY ECONOMICSN

Domenico Marino
Miembro de la Barcelona Economics Network de la Real Academia de Ciencias Económicas y Financieras

Pietro Stilo
Mediterranea University of Reggio Calabria

Davide Maniscalco
Mediterranea University of Reggio Calabria

Cybersecurity and Economics

The digital revolution that we have been going through for at least two decades now has entailed and is entailing a whole series of changes leading up to the digital transition, which during the pandemic phase of Covid-19, but also after it, has experienced and is experiencing a strong acceleration. All these changes have entailed a transfer from the real world to the virtual world of a whole series of data and information that make their way around the world on a daily basis via the network. These data and information now constitute the vast majority (not to say almost all) of those used and disseminated worldwide. It is tautological that this mass of data and information must be protected and safeguarded, hence other sectors have developed, such as cybersecurity, and within it various facets have been identified, going so far as to activate insurance policies on cyber risks, something that was unthinkable a few years ago. Among them in recent times, there has been increasing talk of an aspect that is perhaps little known to the general public, but of extreme importance for the years to come, namely cybersecurity economics, or the economics of information security. This is a field of study that focuses on the application of economic principles to cybersecurity, as it has been realized that cybersecurity generates costs but also value, as it protects the most important commodity of our time, or at least one of the most pivotal, namely information and data.

Considering that cyber security has become a key concern for organizations in every sector, economic analysis can provide a useful framework for making informed decisions on risk management and resource allocation.

When we speak of economics applied to the domains of information security, we are therefore referring to a vast field of research that moves from a socio-technical and technological perspective to investigate the following economic aspects of information security

- budget
- information asymmetry
- governance
- types of goods and services

This investigation is, in turn, aimed at a very specific purpose, namely, to identify new sustainable policies, regulatory options and best practices that can improve the cybersecurity posture of players in the digital ecosystem.

In this regard, it should be pointed out from the outset that the economics of cyber security should be understood as an interdisciplinary field of study made functional to cyber security and economics.

Authoritative doctrine (1) has attributed to the economics of cybersecurity the connotation of transdisciplinary (i.e., a synthetic creation that incorporates works from different disciplines), which treats cybersecurity and economics as two different, relatively independent systems of thought that interact in a complex socio-technical system.

And it is precisely the characteristic interaction between the two disciplines that allows one to appreciate the level of contamination of one over the other.

The study of the economics of cyber security enables decision makers to make informed and informed decisions that improve guidance in the assessment and management of complex scenarios, ensuring the sustainability of their governance actions in the digital ecosystem.

Drawing on these insights, cybersecurity practitioners have been able to respond to many complex problems that have emerged in the cybersecurity environment over the past two decades.

The academic field of cybersecurity economics is highly interdisciplinary as it combines key findings and tools from disciplines such as sociology, psychology, law, political science and computer science.

Within the cybersecurity discipline, information security is a term often used interchangeably with information security.

However, it must be said that computer security goes far beyond information security to include the protection of information resources and other assets, including human and cyber-physical systems.

According to this view (2), also supported by the international standard ISO/IEC 27032:2012, in information security, a reference to the human factor usually refers to the human role(s) in the security process.

In information security, however, this factor has an additional dimension, namely humans as potential targets of cyber-attacks or even humans unknowingly participating in a cyber-attack due to lack of awareness.

The European Information Security Agency (ENISA) has clarified that there is no need for a definition of cyber security (3) because it encompasses all practices and standards involving people, processes and technologies within an organization, group or autonomous environments where computers and cyber-physical systems with valuable data are connected to cyberspace.

According to ISO/IEC 27002, an asset is anything of value to an organization

Assets can be classified into different sub-types according to their convertibility (current and non-current assets), physical existence (tangible or intangible assets) and use (operational or non-operational assets).

With the rapid development of information technology, digital assets have been recognized as critical parts of organizations.

However, information security is not limited to digital assets. Over the past decade, the increasing number of cyber-attacks against physical assets and critical infrastructure (i.e. ex plurimus Stuxnet) has indicated that cyber security can be labelled as a serious cyber and physical challenge for organizations and governments.

For these reasons, an accurate assessment of resources and assets is crucial to make efficient investments in their protection, capital budgets and strategic planning.

Much of the published research on the economics of cybersecurity has focused on the economic evaluation of assets and finding the optimal level of security investment in organizations to protect those assets.

However, the economics of cybersecurity is not only concerned with whether an organization is spending enough to protect its resources and whether the security budget is being spent on the right security measures and controls, but is also concerned with how a digital ecosystem and its operational agents function and behave.

The economics of cyber security covers regulatory changes and competitive pressures (e.g. how cyber security can be aligned with broader business processes).

It studies how the allocation of resources by governments and businesses meets the requirements of creating a resilient cyber environment for themselves and other agents.

Furthermore, the economics of cyber security focuses on the efficiency surrounding decisions made as a result of incentives and policies designed to maximize profit and trust within the environment.

The cyber ecosystem

Among the various topics that cybersecurity economics has triggered almost as an appendix to it, but instead as a pivotal part, is that of the cyber ecosystem, within which all stakeholders in this aspect fall, including the industries in the cyber risk value chain, the risk owners, e.g. companies, but not only them, also individuals and the public sector, companies dealing with cybersecurity, and the insurance sector . But let us go in order.

In general, the cyber risk holders are private companies, individuals and the public sector. According to some scholars, companies also generate value through the use of information and communication technologies (ICT) for their business activities, but in the course of these activities, they may be subject to cyber-attacks. This is why they must be protected and safeguarded.

Both the specialized literature on cyber risk quantification and the cyber risk value chain focus almost exclusively on the public and corporate sectors, leaving out private individuals, whose data and information are important in some cases even beyond the individual (for whom they are always of primary importance). Private individuals are therefore increasingly targeted by cyber-attacks, as they are easier ‘prey’ to attack in many cases, either due to a lack of knowledge of the problem or due to the use of simple forms of cyber protection. Individuals are the target of: identity theft, sensitive information such as credit card numbers and social security .

According to data provided by the International Data Corporation (2019), global ICT investments amount to approximately USD 4.9 trillion in 2020, with an estimated annual growth rate of around 5% until 2023. Increasing digitisation has added value to companies and service and product providers in the area of communication and information technology. This is why many companies have taken out IT insurance to cover against IT risks. In this context, providers of IT protection services can also insure themselves against these risks through an Errors and Omissions (E&O) policy. In this context, the most common errors are in software or temporary interruptions in their cloud protection provision, which obviously represent an IT risk for their customers and a source of liability or fines against them.

The cyber insurance market has gained a lot of momentum since the mid-2010s and has grown by 30 per cent annually, to reach around USD 6 billion in gross premiums in 2020. For up-to-date data, please visit our Market Statistics.

In the field of private insurance, cyber is a very popular and fast-growing area. It is an area that by its very nature is very risky and often difficult to explore by definition. One of the most widespread fears is that of a far-reaching systemic event, just as the same insurers that provide such products are concerned about little-known events, perhaps single ones, but which repeatedly pose a widespread risk. A veritable market for insurance companies and their services has been built around this business, with very strong competition between insurance companies.

The capital market is directly exposed to cyber risks through shares and bonds. While a cyber incident could cause the shares of a single company to plummet, as in the case of Marriot in 2018, where the share value fell by 7% when the breach was announced (see Hermeneut (2018)), a cyber catastrophe could bring down an entire industry sector and even the entire world economy. An analysis of such catastrophic scenarios can be found under 1.2.2 in the cyber-economics.com library. The ILS market as of 2020 (year of the covid-19 pandemic) has become very large (USD 45 billion)(4).

Fundamentals of Cybersecurity Economics

As with any new field of research, the basic starting point is to identify fundamental principles from which an articulated body of knowledge can be built.

The fundamental principles of cybersecurity economics include:

I. Risk management: the main objective of cybersecurity economics is risk management. Organizations need to make decisions on how to invest in cybersecurity by assessing the costs and benefits associated with different risk mitigation strategies. Economic analysis can help identify the most relevant threats and assess the potential financial or reputational losses resulting from security breaches.

II. Resource allocation: Resource allocation is a crucial aspect in cybersecurity economics. Since resources are limited, it is necessary to decide how to allocate them effectively to maximize security. Economic analysis can help determine the optimal mix of investments in security technologies, personnel training, implementation of policies and procedures, and incident response management.

III. Assessment of costs and benefits: cost-benefit analysis is a central element of cybersecurity economics. This involves assessing the costs associated with the implementation of security countermeasures, such as the purchase and maintenance of security solutions, staff training and incident management. At the same time, it is important to estimate the expected benefits of reducing risks, such as preventing financial or reputational losses, maintaining customer confidence and adherence to regulations.

IV. Incentives and disincentives: cybersecurity economics also deals with the incentives and disincentives that influence the cybersecurity behavior of organizations and individuals. For example, the costs of violations may include fines, legal penalties, loss of customers and reputational damage. The proper design of incentives can promote responsible behavior, such as compliance with security policies and the adoption of preventive measures.

In terms of methods, cybersecurity economics uses several tools and techniques, including:

a. Decision models: the use of mathematical models and optimization algorithms can help evaluate cybersecurity investment decisions. These models can consider factors such as the probability of breaches, the associated costs and the potential benefits of different risk mitigation strategies.

b. Cost-benefit analysis: economic analysis is applied to assess the costs and benefits of cybersecurity decisions. This includes estimating the direct and indirect costs associated with security measures, as well as assessing the expected benefits, such as reduced financial losses, reputation protection and regulatory compliance.

c. Risk assessment: risk assessment is a fundamental method in cybersecurity economics. It consists of identifying and evaluating potential cybersecurity risks, assessing the probability of occurrence of damaging events and the associated financial consequences. These assessments help determine the prioritization of investments and direct resources to the areas of greatest risk.

d. Total Cost of Ownership (TCO) analysis: TCO is a method used to assess the total costs of an IT security infrastructure or solution over its entire lifecycle. This includes not only the initial purchase costs, but also the costs of maintenance, upgrades, staff training and replacement over time. A TCO analysis allows one to assess the efficiency of security solutions and make informed decisions on their implementation.

e. Incentive models: the use of incentive models is one method to promote safe behavior. For example, financial incentives or rewards may be offered for achieving security goals, while disincentives may be introduced for non-compliant behavior or security breaches. These models seek to align the interests of organizations and individuals with cybersecurity goals.

Importantly, cybersecurity economics is an evolving field in which new principles and methods are being developed and applied to address emerging cybersecurity challenges. The ultimate goal is to develop strategies and policies that enable organizations to effectively address cybersecurity threats while protecting their data, reputation and financial interests.

In cybersecurity economics, fuzzy logic can be applied in several areas, including:

1. Risk assessment: risk assessment in cybersecurity often involves a number of factors that are difficult to quantify accurately, such as the probability of a breach or the financial impact. Fuzzy logic can be used to represent and manage the uncertainty associated with these factors, enabling a more flexible and robust risk assessment.
2. Investment decisions: fuzzy logic can be applied to evaluate investment decisions in cyber security, considering trade-offs between costs, benefits and associated uncertainties. For example, it can be used to assess return on investment (ROI) in the presence of partial or uncertain information.
3. Modelling user behavior: fuzzy logic can be used to model user behavior in relation to cyber security. This can provide a better understanding of user preferences and actions and allow security policies to be adapted more effectively.
4. Incident response management: incident response management requires quick and dynamic decisions based on limited and uncertain information. Fuzzy logic can be used to represent and manage uncer-

tainty during incident management, allowing a more flexible evaluation of response options.

The application of fuzzy logic to cybersecurity economics enables the management of uncertainty and imprecision that are inherently present in cybersecurity. This can help to make more realistic decisions by considering a wider range of factors and adapting security strategies in a more flexible and adherent way.

The delineation of a fuzzy logic model

Let X, Y and Z be the linguistic variables representing 'system vulnerability', 'probability of attack' and 'financial impact' respectively. Each of these variables can take linguistic values such as 'low', 'medium' and 'high'.

Definition of linguistic variables:

X = {low, medium, high} Y = {low, medium, high} Z = {low, medium, high}

Definition of membership functions:

For each linguistic variable, we need to define membership functions that assign a degree of membership to each linguistic value. For example, we can use triangular functions to simplify the example:

X_low(x) = triangular(x, 0, 10, 20) X_medium(x) = triangular(x, 15, 25, 35) X_high(x) = triangular(x, 30, 40, 50)

Y_low(y) = triangular(y, 0, 0.2, 0.4) Y_medium(y) = triangular(y, 0.3, 0.5, 0.7) Y_high(y) = triangular(y, 0.6, 0.8, 1)

Z_low(z) = triangular(z, 0, 100, 200) Z_medium(z) = triangular(z, 150, 250, 350) Z_high(z) = triangular(z, 300, 400, 500)

Definition of fuzzy rules:

Fuzzy rules determine how to combine linguistic variables to obtain the desired output. For example:

- If X is high AND Y is high, then Z is high.
- If X is medium AND Y is medium, then Z is medium.
- If X is low AND Y is low, then Z is low.

Fuzzy Inference:

Using the defined fuzzy rules, we can apply fuzzy inference to obtain fuzzy output based on the valuations of linguistic variables. For example, if we have values of X = 25 and Y = 0.5, we can calculate the fuzzy output Z using the defined fuzzy rules and membership functions.

Defuzzyification:

To obtain a numerical value representing the level of risk, we can apply defuzzyfication to the fuzzy output obtained. This involves transforming the fuzzy output into a numerical value representing the overall risk level.

This example illustrates how fuzzy formulae can be used to assess risk in cybersecurity economics. However, it is important to note that the specific membership functions, fuzzy rules and inference algorithms may vary depending on the context and needs of the application.

Defuzzification is the process by which a fuzzy output is converted into a numeric value defined within the variability domain of the output. There are several methods of defuzzification, but one of the most common is the center of gravity or centroid method.

In the center-of-gravity method, the fuzzy output is represented as an aggregate membership function indicating the membership distribution within the variability domain. Defuzzification is done by calculating the centroid or center of gravity of this aggregate membership function.

Here is a step-by-step explanation of the center of gravity method for defuzzification:

i. Aggregation of fuzzy output: The fuzzy output is aggregated using the defined fuzzy rules and appropriate fuzzy operators (such as minimum, maximum or other aggregation operators). The aggregated output represents an aggregated membership function that describes the membership distribution within the variability domain of the output.

ii. Calculation of the centroid: The centroid or center of gravity of the aggregate membership function is calculated using the concept of a weighted average.

iii. Calculation of area under the curve: The area under the curve of the aggregate membership function is calculated using the definite integral. This value represents the sum of the areas of the trapezoids formed by the points of intersection of the curve with the x-axis.
Area = ∫[z_min, z_max] A(z) dz
Where z_min and z_max represent the minimum and maximum x-axis values of the aggregate membership function, respectively.

iv. Calculation of the centroid: The centroid or centre of gravity is calculated as the weighted average of the x-axis points, taking the area under the curve as the relative weight. The formula for calculating the centroid is as follows:
Centroid = (1 / Area) * ∫[z_min, z_max] z * A(z) dz

The value of the centroid represents the numerical result of the defuzzification and indicates the overall risk level.

Note that these formulae are specific to the center of gravity method, which is one of the common defuzzification methods. There are also other defuzzification methods, such as the maximum value method or the maximum center method, which can be used according to the specific needs of the cybersecurity economics problem.

Concluding remarks

In the light of what has been stated in this paper, the economics aspect of cybersecurity is certainly an area of great interest and booming. In the years to come, we will certainly see an increase in this area of cybersecurity. That will go hand in hand with cybersecurity in general, because as everyone knows, the digital sector will be increasingly used by all of us, be it individuals, the public sector, or private companies of any size. It follows that necessarily an impressive amount of data and information will be produced, developed and exchanged all over the world and will have to be protected and safeguarded, such protection has an investment cost, just as potential damages have a cost to be addressed and protected also through dedicated and specific insurance products. The hope is that systemic events can be avoided and that such investment costs are increasingly considered a structural investment by all those affected by such events, who also through adequate information and specific training can avoid frequent incidents by reducing damage and costs.

References

1.- Cat, J. L'unità della scienza. Nella Stanford Encyclopedia of Philosophy; Zalta, EN, ed.; Laboratorio di ricerca sulla metafisica, Stanford University: Stanford, CA, USA, 2017.

2.- Von Solms, R.; Van Niekerk, J. Dalla sicurezza delle informazioni alla sicurezza informatica. Calcola. Sicuro. 2013, 38, 97–102.

3.- ISO/IEC27002. Information Technology–Security Techniques–Code of Practice for Information Security Controls, (AS ISO/IEC 27002: 2015); Organizzazione internazionale per la standardizzazione: Ginevra, Svizzera, 2015.

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

ULTIMOS ACTOS INTERNACIONALES DE LA REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

VII ACTO INTERNACIONAL (24/11/2011)
"Decidir hoy para crear el futuro del Mediterráneo"

VIII ACTO INTERNACIONAL (5/11/2013)
"Ciencia, cultura y deporte en el Siglo XXI"

IX ACTO INTERNACIONAL (11/11/2014)
"Revolución, evolución e involución en el futuro de los sistemas sociales"

X ACTO INTERNACIONAL (18/11/2015)
"Ciencia y realidades económicas: reto del mundo
post-crisis a la actividad investigadora"

XI ACTO INTERNACIONAL (10/11/2016)
"El comportamiento de los actores económicos ante el reto del futuro"

XII ACTO INTERNACIONAL (16/11/2017)
"Las nuevas áreas del poder económico mundial"

XIII ACTO INTERNACIONAL (15-16/11/2018)
"Desafíos de la nueva sociedad sobrecompleja:
humanismo, transhumanismo, dataísmo i otros ismos"

XIV ACTO INTERNACIONAL (14-15/11/2019)
"Migraciones"

XV ACTO INTERNACIONAL (19-20/11/2020)
"La vejez: conocimiento, vivencia y experiencia"

XVI ACTO INTERNACIONAL (18-19/11/2021)
"La nueva economía después del Sars-Cov-2.
Realidades y revolución tecnológica"

XVII ACTO INTERNACIONAL (16-17/11/2022)
"¿Por Qué no un mundo sostenible?
La ciencia económica va a su encuentro."

II SEMINARIO INTERNACIONAL (24-25/5/2023)
"La Ciberseguridad en la Ciencia y en las Actividades Económicas"

Real Academia de Ciencias Económicas y Financieras

SEMINARIO INTERNACIONAL DE PRIMAVERA DE BARCELONA

MS-85/24

LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONÓMICAS

II Seminario Internacional de Primavera de Barcelona

La Real Academia de Ciencias Económicas y Financieras organiza cada año una serie de actos académicos internacionales en su sede de Barcelona con la participación de científicos, expertos y académicos de diferentes continentes. Este año 2023 se ha desarrollado el II Seminario Internacional de Primavera con plena normalidad. La presencia de participantes ha sido de las más elevadas, añadiéndose además numerosas participaciones virtuales.

Las aportaciones científicas realizadas por los ponentes se han centrado en torno a la cuestión que plantea la ciberseguridad en la ciencia y las actividades económicas haciendo especial hincapié en los profundos cambios estructurales, en ocasiones disruptivos, que ya se están produciendo y seguirán produciéndose en el futuro: nos referimos a los efectos económicos, por una parte; y a la revolución tecnológica como nuevo paradigma social, por otra.

El contenido de los trabajos aportados a esta conferencia internacional ha quedado recogido y publicado en una obra en forma de libro, así como en los distintos formatos digitales de los canales habituales.

La actividad científica y académica de la Real Academia de Ciencias Económicas y Financieras sigue su andadura siempre adaptándose a las vicisitudes del entorno y fiel al mandato que tiene encomendado en su tarea de investigar y difundir el conocimiento.

INSTITUTO DE ESPAÑA

Real Academia
de Ciencias Económicas y Financieras

Barcelona Economics Network