CSIC
Consejo Superior de Investigaciones Científicas

Nota de prensa

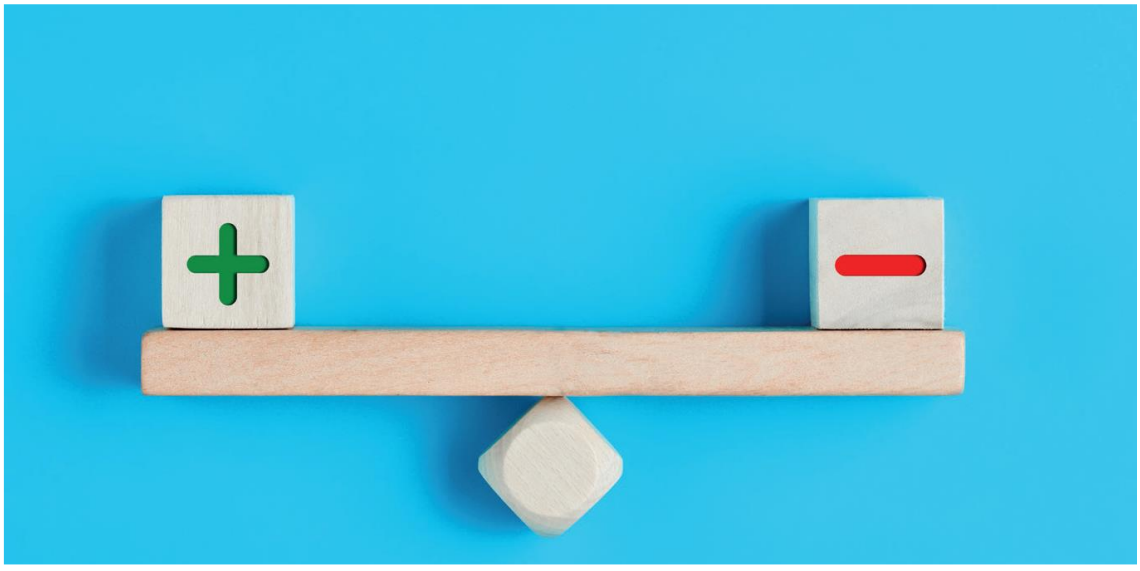
CSIC comunicación
Tel.: +34 91 568 14 77 / 618 40 95 65
comunicacion@csic.es
www.csic.es

Madrid, 23 de mayo de 2022

Riadas, robos o ciberataques: investigadores del CSIC explican cómo gestionar el riesgo

- **Los científicos David Ríos y Roi Naveiro son autores de 'Análisis de riesgos', un nuevo título de la colección ¿Qué sabemos de? (CSIC-Catarata)**

- **El texto describe las herramientas y metodologías que se utilizan para cuantificar y gestionar el riesgo, algo fundamental en la sociedad moderna**



Hay un enorme potencial del análisis de riesgo aplicado al ámbito social para beneficio de administraciones y organizaciones no gubernamentales. / CSIC-Catarata

Los riesgos son parte de nuestra vida. Una epidemia, un robo en nuestro domicilio, un incendio forestal o un ciberataque representan algunas de las amenazas a las que las sociedades modernas deben hacer frente. Los investigadores del CSIC **David Ríos** y **Roi Naveiro** presentan, en el último número de la colección ¿Qué sabemos de? (CSIC-Catarata), distintas metodologías para **abordar el análisis y la gestión de los riesgos.** El libro ***Análisis de riesgos*** expone una disciplina poco conocida, pero imprescindible en

CSIC comunicación
Tel.: 91 568 14 77
comunicacion@csic.es
www.csic.es/prensa

la actualidad. “Existe una **inadecuada gestión de riesgos tanto a nivel individual como social**, lo que se agrava por la falta de formación sólida en probabilidad y estadística en la mayoría de la población. Nuestro texto explica de forma sencilla los ingredientes fundamentales de este ámbito de estudio y las herramientas básicas que existen para desarrollarlo”, comentan los autores.

Para los científicos del Instituto de Ciencias Matemáticas (ICMAT) el riesgo es “una condición en la que existe una posibilidad incierta de desviación adversa frente al resultado que se espera o desea”. A partir de aquí, los autores exponen las tres fases principales del análisis de riesgos: la **evaluación de las amenazas bajo estudio**, que aborda la estimación de la probabilidad de que estas se materialicen así como la evaluación de su impacto en caso de que lo hagan; la **gestión**, que comprende las actividades realizadas para reducir la probabilidad de que se materialicen las amenazas o minimizar su impacto; y la **comunicación**, que se refiere al intercambio de opiniones e información relativa a los riesgos, ya sea entre evaluadores, gestores o cualquier otra parte involucrada en el problema.

Este último punto es básico. “En estos tiempos protagonizados por la pandemia por COVID-19 hemos oído disertaciones sobre los riesgos de vacunarse, nos han presentado esquemas de colores para explicarnos la incidencia de casos en diferentes regiones, hemos hablado del riesgo de contraer el virus si viajamos en transporte público, etc. No cabe duda de que una de las palabras más repetidas ha sido riesgo, pero, siendo honestos, debemos admitir que una mala gestión de los riesgos y una peor comunicación de los mismos pueden haber estado detrás de unos resultados manifiestamente mejorables en el control de la pandemia”, afirman los investigadores.

Metodologías diversas para distintas amenazas

Ríos y Naveiro explican que existen metodologías muy extendidas para el análisis de riesgos, como las **matrices de riesgos** y los **análisis de escenarios**. Para ambas, la estimación de la probabilidad de que las potenciales amenazas bajo estudio sucedan y del impacto que conllevan es central. No obstante, a menudo estas estimaciones se realizan de manera pseudocuantitativa, presentan una notable imprecisión y conducen a asignaciones de recursos de gestión mejorables. En aplicaciones sensibles e importantes del análisis de riesgos, es necesario afinar al máximo las estimaciones de probabilidades e impactos que se realicen. “Por ejemplo, en lugar de utilizar frases como *La probabilidad de que Pedro Sánchez no culmine esta legislatura es media*, con una metodología más sofisticada podríamos llegar a expresiones más precisas y útiles como *La probabilidad de que Pedro Sánchez no culmine esta legislatura es 0,35*”, señalan los científicos. “Necesitamos procedimientos y herramientas para **modelizar cuantitativamente la incertidumbre y los impactos, y ser así más certeros en nuestra previsión y toma de decisiones**. En todo caso, hay que tener en cuenta los recursos de los que se dispone para analizar una situación concreta y, a partir de ahí, decidir el tipo de aproximación que se realiza”, añaden.

No todas las amenazas tienen la misma naturaleza, por eso la forma de afrontarlas dependerá de su tipología. A juicio de los investigadores, una distinción fundamental ha

de hacerse **entre riesgos naturales**, como los asociados a fenómenos meteorológicos extremos como un huracán o las lluvias torrenciales, **y riesgos adversarios, que son consecuencia de las acciones de agentes inteligentes**, como puede ser un ataque terrorista. Las herramientas tradicionales no son adecuadas para este segundo tipo, porque los adversarios inteligentes pueden responder a las contramedidas que implementemos. "Por ejemplo, si queremos proteger una planta nuclear contra ataques terroristas podemos distribuir patrullas en las entradas por carretera, pero entonces los atacantes pueden responder utilizando el alcantarillado para acceder a la planta. Esta adaptabilidad, que no se observa en los riesgos naturales, requiere un marco matemático para predecir cómo los adversarios reaccionan frente a nuestras acciones", explican los autores.

En la frontera de los riesgos

Más allá de la seguridad en el hogar o en la aviación, que se refieren a riesgos que podríamos denominar 'clásicos', **en la última década ha aparecido una nueva fuente de amenazas derivadas de la aplicación masiva y creciente de sistemas de inteligencia artificia**l en la automatización de múltiples tareas. Estos riesgos son adversarios en su mayoría y tienen relevancia, por ejemplo, en la detección automática de transacciones fraudulentas en los pagos *online*. "Este tipo de fraude requiere nuevos métodos de prevención y detección basados en herramientas de aprendizaje automático (*machine learning,* ML), que analizan millones de transacciones pasadas, tanto legítimas como fraudulentas. A partir de este conocimiento, en los pocos segundos que pasan desde que ejecutamos una compra *online* hasta que esta resulta aceptada, un algoritmo de ML estudia si esta compra sugiere un patrón fraudulento. Si esto fuera así, la compra se detendría y pasaría a estudio. Recientemente, se ha observado que los defraudadores modifican intencionalmente sus patrones de fraude para evitar ser detectados por los sistemas de ML y generan enormes costes a las entidades bancarias", aclaran los científicos del ICMAT.

Otra de las aplicaciones de estas nuevas herramientas se centra en evaluar y controlar las **brechas de seguridad de los vehículos autónomos**. Es posible engañar a los equipos de visión computacional de los sistemas de conducción automatizada contaminando las imágenes que estos reciben, haciendo posible, por ejemplo, que un vehículo autónomo confunda una señal de stop con una de ceda el paso, y provocando una toma de decisiones errónea con consecuencias potencialmente catastróficas. Del estudio de la seguridad de los algoritmos de ML subyacentes a sistemas como los vehículos autónomos se encarga el **aprendizaje automático adversario,** un campo activo de investigación que los expertos consideran fundamental en el corto y medio plazo.

Por otro lado, los autores destacan que el análisis de riesgos posee un enorme potencial en el ámbito social para beneficio de las administraciones y las organizaciones no gubernamentales. "Comparando con los usos industriales del análisis de riesgos, no es difícil vislumbrar las enormes aplicaciones potenciales que esta disciplina tendría en problemas relativos al desarrollo racional de planes para infraestructuras, el empleo del conocimiento sobre el comportamiento de los individuos para promover la eficiencia

energética o la identificación de barrios con servicios sociales inadecuados, entre otros muchos", concluyen.

Análisis de riesgos es el número 134 de la colección de divulgación '¿Qué sabemos de?' (CSIC-Catarata). El libro puede adquirirse tanto en librerías como en las páginas web de Editorial CSIC y Los Libros de la Catarata. Para solicitar entrevistas con los autores o más información, contactar con: comunicacion@csic.es (91 568 14 77).

Sobre los autores

David Ríos Insua es AXA-ICMAT Chair en Análisis de Riesgos Adversarios y profesor de investigación en análisis de riesgos y ciencia de datos del CSIC en el ICMAT. Académico numerario en la Real Academia de Ciencias Exactas, Físicas y Naturales de España, ha recibido el premio DeGroot de ISBA y el premio de la Society for Risk Analysis por sus trabajos sobre análisis de riesgos en la lucha contra el terrorismo.

Roi Naveiro Flores es investigador posdoctoral del CSIC en el ICMAT. Graduado en Física por la Universidad de Salamanca, máster en Física Teórica y doctorado en Estadística e Investigación Operativa por la UCM. Actualmente trabaja en proyectos tanto metodológicos como aplicados, en los que trata de aplicar técnicas avanzadas de *machine learning*, estadística bayesiana y teoría de la decisión a problemas relacionados con el descubrimiento de fármacos, el diseño de materiales o la conducción autónoma, entre otros.

CSIC Cultura Científica