El análisis de riesgos en la ciberseguridad

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano.

La calidad de las grandes decisiones sobre la ciberseguridad que tienen que ver con las medidas que se toman frente a los riesgos y amenazas que padecen las infraestructuras críticas, los sistemas y tecnologías de la información o los servicios públicos y privados que se prestan sobre ellas depende de la calidad de los análisis de riesgos utilizados. El sentido común no basta para decidir qué riesgos se afrontan y cuáles no, las prioridades de inversión o los riesgos que se desplazan hacia terceros. Los análisis de riesgos orientan a quienes tienen que aconsejar o tomar esas decisiones.

Las metodologías de análisis en España se han desarrollado rápida y eficazmente, como se verá a continuación con algunos ejemplos, pero el objeto de análisis, la ciberseguridad, se ha ido complicando progresivamente debido al incremento de la complejidad de los factores tecnológicos, empresariales y regulatorios implicados. Cada sector empresarial o de la Administración ha respondido a la complejidad enriqueciendo los análisis cualitativos tradicionales con nuevos tipos de análisis cuantitativos que han aumentado el rigor y la objetividad de los resultados. Sin embargo, y a pesar del progreso analítico en cada sector individual –infraestructuras críticas, banca, seguros, operadores…–, el reto ahora es el de interconectar las distintas metodologías y disciplinas de análisis para potenciar análisis transversales y transdisciplinares.

“el reto ahora es el de interconectar las distintas metodologías y disciplinas de análisis [de riesgos] para potenciar análisis transversales y transdisciplinares”.

Esta necesidad es más evidente en las grandes empresas y organizaciones, donde interactúan varios tipos de riesgos, que en las pymes donde se reduce el ámbito de análisis. La complejidad no dispone de modelos de análisis adecuados porque la diversidad de riesgos, indicadores y metodologías ha impedido elaborar estándares y métricas de propósito general que facilitaran el desarrollo posterior de modelos de análisis sectoriales. Un reciente estudio de *Science* pone de relieve el daño que producen las barreras disciplinares en el análisis de ciberriesgos y las ventajas que generaría, por ejemplo, una colaboración entre los expertos en riesgos regulatorios y los expertos en computación o entre expertos en economía que evalúen los incentivos para reducir ciberriesgos y expertos en ciencias de la conducta humana[1]. A falta de esa colaboración transversal (entre sectores) y transdisciplinar (entre áreas de conocimiento), las decisiones importantes, como mudarse a la nube, el desarrollo de aplicaciones o la organización de la cadena de suministro, se adoptan sobre una débil base metodológica. Además, la falta de métricas relevantes –las que transmiten una

[1] Gregory Falco et al. (2019), “Cyber risk research impeded by disciplinary research”, *Science Policy Forum*, vol. 366, nº 6464, 29/XI/2019.

idea de riesgo a los decisores no iniciados– dificulta el proceso de decisiones de los directivos y consejos de administración.

El Incibe ha desarrollado un análisis de riesgos básico a disposición de los empresarios para que elaboren su plan director de seguridad. El riesgo se determina combinando en una matriz la probabilidad de ocurrencia con el impacto potencial, proporcionando a los que tienen que adoptar decisiones un mapa de riesgos. Se apoya en la metodología Magerit de análisis y gestión de riesgos en los sistemas de información, desarrollada por el Centro Criptológico Nacional (CCN-CERT). Estas herramientas permiten a los responsables analizar el entorno del análisis de riesgo (EAR) para identificar los activos que proteger y las medidas más adecuadas para hacerlo. También aquí el CCN-CERT pone a disposición de los analistas algunas herramientas de análisis en diferentes versiones: íntegra (PILAR), simplificada para pymes y Administraciones locales (PILAR Basic), exprés (μPILAR) o personalizada (RMAT).

Las metodologías siguen los principios y directrices genéricas adoptados en la norma internacional ISO 31000 –actualizada por la ISO 31010–de la Organización Internacional de Normalización (International Standards Organization) para gestionar los riesgos genéricos de las organizaciones, que luego cada una tiene que adaptar a sus peculiaridades cibernéticas. Las directrices de la ISO 31000 también se aplican al Mapa de Ciberriesgos que acaban de publicar ISMS Forum y la Agencia Española de Gerencia de Riesgos y Seguros (AGER). El grupo de trabajo que ha estado detrás de su elaboración describe la metodología del mapa de riesgos y cómo se integran en una matriz las valoraciones de probabilidad e impacto para ayudar a tomar decisiones sobre la eliminación, transferencia, mitigación, explotación o aceptación de los riesgos –se incluyen dos casos prácticos para una mejor comprensión–.

Los ejemplos de metodologías sectoriales se multiplican y actualizan, constatando la consolidación de la función de análisis y de los perfiles profesionales de los analistas. Entre otras, se pueden mencionar las dedicadas a la seguridad industrial. Destaca el Modelo de Análisis de Riesgos Ligeros de Seguridad Integral de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB), a iniciativa del Esquema Nacional de Seguridad Industrial (ENSI), que aparece en la Figura 1.

Figura 1. Marco conceptual del modelo de análisis de riesgo sobre ciberseguridad en sistemas de control industrial

Fuente: ARLI-SI: Análisis de Riesgos Ligero de Seguridad Integral, Incibe-CERT.

La Autoridad Bancaria Europea (EBA, en sus siglas en inglés) también ha elaborado sus propias directrices para la evaluación de los riesgos de ciberseguridad en el marco del proceso de revisión y evaluación supervisora (PRES). Esta evaluación forma parte de un proceso de supervisión que tiene en cuenta diversas prioridades. Para 2020, las Prioridades de Supervisión Bancaria incluyen, entre otras, revisión de los modelos internos de capital, riesgos de mercado, criterios de suscripción, capital interno y adecuación de liquidez, modelos de negocio, gobernanza, prueba de estrés y, desde luego, la ciberseguridad. Este modelo de análisis compuesto sirve para reiterar la importancia de combinar los análisis verticales (prioridades) con los horizontales (interacciones), de forma que la supervisión final sea algo más que la yuxtaposición de análisis sectoriales, tal y como defendían los analistas en *Science*. Para abundar en su argumentación, mencionan el caso del riesgo residual en las grandes organizaciones, un riesgo que escapa al control de los análisis verticales y que planea sobre los directores de seguridad de la información (CISO o *chief information security officer*) y los directores de sistemas de información (CIO o *chief information officer*) sin que cuenten con un sistema de análisis que los respalde.

Otro caso de estudio que muestra la necesidad de articular sistemas de análisis transversales y transdisciplinares se encuentra en la Unión Europea. ENISA, la Agencia Europea de Seguridad de las Redes y de la Información, está tratando de articular modelos de análisis de ciberriesgos sectoriales a nivel europeo. Por ejemplo, y paralelamente a la implantación del Reglamento General de Protección de Datos (RGPD) y la Directiva NIS, ENISA comenzó a interesarse por la adaptación del sector de los seguros a la nueva realidad digital. Como resultado, elaboró en 2016 el estudio "Cyber Insurance: Recent Advances, Good Practices and Challenges" consultando al sector sobre sus métodos de análisis, un sector de difícil armonización, incluida la terminología de riesgos[2] –aseguradoras como Lloyd's han esperado hasta el 1 de enero de 2020 para declarar obligatoria en sus pólizas la cláusula de cobertura o exclusión de ciberriesgos–. Al igual que las instituciones oficiales mencionadas en España, ENISA colabora con los actores principales, los centros de investigación y los Estados miembros para desarrollar modelos de análisis o, como ha ocurrido con la controversia sobre las redes de quinta generación (5G), coordinar los análisis nacionales de riesgo. También analiza las limitaciones de los modelos, como las detectadas en la capacidad de usar inteligencia en el análisis de riesgos ("Exploring the opportunities and limitations of current Threat Intelligence Platforms"). Al hacerlo, se incrementa el acervo metodológico europeo para –algún día– disponer de los modelos transversales y transdisciplinares de análisis de riesgo que se proponían al principio de este comentario.

[2] ENISA ha complementado el informe anterior con otro sobre "Commonality of risk assessment language in cyber insurance" en 2017, https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance.