PRÓLOGO

La información que las instituciones públicas tratan es para ellas un elemento fundamental para cumplir con la misión, valores y principios que las inspiran. En este sentido, protegerla de los riesgos a los que está sometida y aplicar medidas y salvaguardas que minimicen los ataques internos y externos que pueden provocar que sea accedida, modificada o eliminada de forma no autorizada es fundamental. Si en un principio las medidas para minimizar los riesgos estaban dirigidas a protegerla físicamente, evitar su robo o que se perdiese por causa de un incendio, una inundación o de una acción humana intencionada o accidental, hoy los riesgos se han multiplicado y existen muchos y variados agentes que la amenazan.

Así, la información y los sistemas informáticos que la tratan deben estar protegidos contra amenazas de rápida evolución que pueden incidir en la confidencialidad, integridad, disponibilidad y en el valor que esta tiene para las instituciones. Para defenderse de estas amenazas, se requiere de una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar su protección, analizar y corregir las vulnerabilidades que los sistemas informáticos puedan sufrir en cada momento, y dar una respuesta efectiva a los incidentes de seguridad que materializan estas amenazas sobre la información y los sistemas.

Esta estrategia de seguridad debería estar basada en estándares o marcos de referencia como el conjunto de normas de la serie ISO 27000 o el Esquema Nacional de Seguridad (ENS), que es de obligado cumplimiento para las Administraciones Públicas e instituciones del sector público como las universidades, así como para sus proveedores de servicios. El ENS, que hace unos días se ha actualizado con la publicación del Real Decreto 311/2022, de 3 de mayo, establece entre sus principios básicos y requisitos mínimos, que la seguridad de los sistemas de información debe comprometer a todos los miembros de la organización, que debe existir una gobernanza de la seguridad, que se debe concienciar y formar en seguridad a las personas que las componen, y que debe existir un proceso continuo de revisión y mejora en su aplicación.

Este nuevo ENS ve la luz en un momento en que las amenazas y los vectores de ataque han evolucionado enormemente y que en su mayoría son consecuencia del mundo hiperconectado en el que vivimos, por lo que frente a estas nuevas ciberamenazas las instituciones deben fortalecer la ciberseguridad y dotarse de los recursos materiales y humanos necesarios y proporcionales al riesgo al que estén expuetas, contando con una adecuada organización y planificación.

Por otro lado, los ciberatacantes utilizan cada vez más tecnologías de última generación con herramientas más sofisticadas para alcanzar los objetivos de sus ataques, robo de información, extorsión, etc., que en muchos casos adquieren a muy bajo precio o como un servicio para perpetrar su ataque. Por ello, las instituciones deben recurrir también para su defensa a estas nuevas tecnologías, Inteligencia Artificial, *Machine Learning*, *Big Data*, etc., y aún más importante actuar de forma conjunta y colaborar en su ciberdefensa compartiendo información y esfuerzos.

En definitiva, los nuevos riesgos exigen que adoptemos nuevas medidas que nos permitan garantizar la confidencialidad, integridad y disponibilidad de la información y la privacidad de las personas. Este nuevo número de la revista RUIDERAe incluye artículos sobre las medidas de seguridad que las universidades pueden y deben implementar para garantizar la privacidad y seguridad de la información personal, para cumplir con el ENS y la mejora continua de la seguridad, sobre cómo la Inteligencia Artificial puede ayudar en la ciberseguridad, cómo debe ser la respuesta a incidentes de seguridad en un escenario global o la importancia de la colaboración entre las instituciones públicas y entre estas y el sector privado. Asimismo, una vez producido el ataque, sobre la importancia de compartir información o implementar planes de continuidad de negocio.

Por último, queremos dar la enhorabuena a todos los autores de los artículos publicados en este número por la rigurosidad, calidad y actualidad de sus aportaciones y que ponen de manifiesto la importancia que la seguridad de la información tiene hoy en día para el desarrollo y bienestar de nuestra sociedad.

José Julián Garde López-Brea
Rector de la Universidad de Castilla-La Mancha