
Europa insiste en medidas de protección, mientras se recupera de un ciberataque

Por: Dayán González Ramírez
23/09/2025



Han transcurrido cerca de 72 horas desde el ciberataque que afectó a varios aeropuertos europeos, y algunos de ellos aún no han logrado recuperar la normalidad. Esto ocurre a pesar de las acciones implementadas y las recomendaciones emitidas por la Unión Europea.

Entre los aeropuertos afectados se encuentran Heathrow, en Londres —el de mayor tráfico aéreo del continente—, así como las terminales de Dublín y Bruselas. Este último continúa en proceso de recuperación y se ha visto obligado a cancelar uno de cada diez vuelos programados para este martes.

Durante la noche del viernes, diversos medios regionales informaron sobre un ataque digital dirigido al software MUSE, gestionado por Collins Aerospace, filial del grupo estadounidense RTX. El incidente inutilizó los sistemas electrónicos de facturación y etiquetado de equipaje, provocando un caos que aún persiste. Durante el sábado y el domingo, varios de los servicios comprometidos debieron realizarse de manera manual, lo que generó decenas de cancelaciones, filas kilométricas y desvíos de vuelos.

Hasta este lunes, se calcula que más de 100.000 personas han sufrido las consecuencias. Aunque no se han publicado datos oficiales, expertos estiman que las pérdidas económicas son millonarias.

Hasta el momento de redactar esta información, se desconoce la autoría del incidente cibernético, que ha evidenciado la fragilidad de los sistemas tecnológicos en el sector aeroportuario. Las autoridades insisten en que el ataque compromete únicamente los procesos logísticos, sin afectar la seguridad aérea ni el control del tráfico.

Sin embargo, cabe señalar que los servicios atacados contienen información sensible, como datos de pasajeros, y han demostrado su capacidad para influir en la movilidad y las cadenas de suministro que dependen de los aeropuertos.

Bruselas responde con medidas urgentes

Con una situación más controlada, las autoridades del bloque comunitario han reiterado la necesidad de implementar con urgencia la normativa NIS2, que corresponde al Reglamento de Ejecución de la Comisión sobre entidades y redes críticas. Según el sitio web oficial de la Comisión Europea, esta normativa establece requisitos técnicos y metodológicos para proveedores de servicios, que son imprescindibles para la ciberseguridad.

Hasta el momento, solo 12 países de la Unión Europea han completado el proceso de transposición de la directiva, mientras que otros 19 la incumplen, lo que ha generado procedimientos de infracción contra algunos de ellos.

La directiva NIS2 obliga a cada Estado miembro a contar con una estrategia nacional de ciberseguridad. Además, amplía el alcance de los sectores obligados a protegerse, incluyendo energía, transporte, salud, banca, agua e infraestructura digital.

Sobre este tema, la comisaria europea de Emergencias y Preparación de Crisis, Hadja Lahbib, expresó a través de sus redes sociales:

“El ciberataque, que ha paralizado los aeropuertos de toda Europa, demuestra lo reales y complejas que son las amenazas actuales... Debemos invertir en preparación para garantizar que estamos listos ante cualquier eventualidad.”
