BASE DE DATOS DE Norma CEF.-
Referencia: NCL012467

**REGLAMENTO DE EJECUCIÓN (UE) 2019/1583, DE LA COMISIÓN, de 25 de septiembre, por el que se modifica el Reglamento de Ejecución (UE) 2015/1998 por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea, en lo que se refiere a las medidas de ciberseguridad.**

*(DOUE L 246, de 26 de septiembre de 2019)*

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) n.º 2320/2002, y en particular su artículo 1 y su artículo 4, apartado 3,

Considerando lo siguiente:

(1) Uno de los principales objetivos del Reglamento (CE) n.º 300/2008 es sentar las bases para una interpretación común del anexo 17 (anexo sobre seguridad) del Convenio sobre Aviación Civil Internacional, de 7 de diciembre de 1944, en su décima edición, de 2017, del que todos los Estados miembros de la Unión son signatarios.

(2) Dicho objetivo ha de alcanzarse mediante: a) el establecimiento de reglas comunes y normas básicas comunes de seguridad aérea, y b) mecanismos para supervisar su cumplimiento.

(3) Al modificar la legislación aplicable, el propósito consiste en ayudar a los Estados miembros a garantizar el pleno cumplimiento de la última enmienda (enmienda 16) al anexo 17 del Convenio sobre Aviación Civil Internacional, que introdujo nuevas normas en materia de organización nacional y de la autoridad competente (punto 3.1.4) y en materia de medidas preventivas relativas a la ciberseguridad (punto 4.9.1).

(4) Al transponer estas normas a la legislación de la Unión aplicable en materia de seguridad de la aviación, se garantizará que las autoridades pertinentes establezcan y apliquen procedimientos para compartir con otras autoridades y agencias nacionales, gestores aeroportuarios, compañías aéreas y otras entidades interesadas, según corresponda y de manera práctica y oportuna, la información pertinente que les ayude a efectuar evaluaciones eficaces del riesgo de sus operaciones en materia de, entre otros ámbitos, la ciberseguridad y las medidas aplicables para combatir las ciberamenazas.

(5) La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo establece medidas destinadas a lograr un elevado nivel común de seguridad de las redes y sistemas de información en la Unión a fin de mejorar el funcionamiento del mercado interior. A nivel nacional, las medidas derivadas de la Directiva SRI y del presente Reglamento deben coordinarse para evitar lagunas y duplicaciones de obligaciones.

(6) Procede, por tanto, modificar el Reglamento de Ejecución (UE) 2015/1998 de la Comisión en consecuencia.

(7) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité de Seguridad de la Aviación Civil previsto en el artículo 19, apartado 1, del Reglamento (CE) n.º 300/2008.

HA ADOPTADO EL PRESENTE REGLAMENTO:

**Artículo 1.**

El anexo del Reglamento de Ejecución (UE) 2015/1998 se modifica de conformidad con el anexo del presente Reglamento.

**Artículo 2.**

El presente Reglamento entrará en vigor el 31 de diciembre de 2020.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 25 de septiembre de 2019.

*Por la Comisión*
*El Presidente*
Jean-Claude JUNCKER

**ANEXO**

El anexo del Reglamento de Ejecución (UE) 2015/1998 se modifica como sigue:

1) Se añade el punto 1.0.6 siguiente:

«1.0.6. La autoridad competente establecerá y pondrá en práctica procedimientos para compartir con otras autoridades y organismos nacionales, gestores aeroportuarios, compañías aéreas y otras entidades interesadas, según corresponda y de manera práctica y oportuna, la información pertinente que les permita efectuar evaluaciones eficaces del riesgo de sus operaciones.»

2) Se añade el punto 1.7 siguiente:

«1.7. DEFINICIÓN DE LOS SISTEMAS CRÍTICOS DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES Y DE LOS DATOS CRÍTICOS EMPLEADOS PARA LOS FINES DE LA AVIACIÓN CIVIL Y PROTECCIÓN DE ESTOS FRENTE A LAS CIBERAMENAZAS

1.7.1. La autoridad competente velará por que los gestores aeroportuarios, las compañías aéreas y las entidades definidas en el programa nacional de seguridad de la aviación civil definan y protejan sus sistemas críticos de tecnología de la información y las comunicaciones y los datos críticos frente a ciberataques que pudieran afectar a la seguridad de la aviación civil.

1.7.2. Los gestores aeroportuarios, las compañías aéreas y las entidades definirán en su programa de seguridad, o en cualquier documento pertinente a que este haga referencia, los sistemas críticos de tecnología de la información y las comunicaciones y los datos críticos descritos en el punto 1.7.1.

El programa de seguridad, o cualquier documento pertinente a que este haga referencia, detallará las medidas para garantizar la protección frente a los ciberataques mencionados en el punto 1.7.1, así como para garantizar que estos son detectados, que se responde a ellos y que se subsanan sus efectos.

1.7.3. Las medidas detalladas para proteger dichos sistemas y datos frente a actos de interferencia ilícita se definirán, desarrollarán y aplicarán de conformidad con una evaluación del riesgo efectuada por el gestor aeroportuario, la compañía aérea o la entidad, según corresponda.

1.7.4. Cuando una autoridad o un organismo específico sea competente para adoptar medidas relacionadas con las ciberamenazas en un Estado miembro, podrá ser designado como competente para la coordinación o el seguimiento de las disposiciones en materia de ciberseguridad que figuran en el presente Reglamento.

1.7.5. Cuando los gestores aeroportuarios, las compañías aéreas y las entidades definidas en el programa nacional de seguridad de la aviación civil se sometan a requisitos de ciberseguridad independientes derivados de otra legislación nacional o de la legislación de la Unión, la autoridad competente podrá sustituir el cumplimiento de los requisitos del presente Reglamento por el cumplimiento de los elementos incluidos en dichas legislaciones. La autoridad competente deberá coordinarse con las demás autoridades competentes pertinentes para garantizar que los regímenes de supervisión estén coordinados o sean compatibles.».

3) El punto 11.1.2 se sustituye por el texto siguiente:

«11.1.2. El personal especificado a continuación deberá haber superado una verificación de antecedentes reforzada o normal:

a) las personas seleccionadas para efectuar inspecciones, controles de acceso o cualquier otro control de seguridad, o para asumir la responsabilidad de ellos, en cualquier zona que no constituya una zona restringida de seguridad;

b) las personas que tengan acceso no acompañado a la carga y el correo aéreos, el correo y el material de la compañía aérea, las provisiones de a bordo y los suministros de aeropuerto que hayan sido objeto de los controles de seguridad exigidos;

c) las personas con derechos de administrador o con acceso sin supervisión e ilimitado a los sistemas críticos de tecnología de la información y las comunicaciones y los datos críticos descritos en el punto 1.7.1 que se emplean para los fines de la seguridad de la aviación civil de conformidad con el programa nacional de seguridad de la aviación, o aquellas personas que hayan sido calificadas como tales en la evaluación del riesgo mencionada en el punto 1.7.3.

Salvo que el presente Reglamento especifique lo contrario, la autoridad competente determinará, con arreglo a las normas nacionales aplicables, si es necesario superar una verificación de antecedentes reforzada o normal.»

4) Se añade el punto 11.2.8 siguiente:

«11.2.8. Formación de personas con funciones y responsabilidades relacionados con las ciberamenazas

11.2.8.1. Las personas que apliquen las medidas establecidas en el punto 1.7.2 tendrán las capacidades y aptitudes necesarias para llevar a cabo sus tareas de manera efectiva. Deberán ser conscientes de los ciberriesgos pertinentes, en la medida en que sea necesario.

11.2.8.2. Las personas que tengan acceso a los datos o los sistemas recibirán una formación laboral adecuada y específica, acorde con sus funciones y sus responsabilidades, que incluirá la toma de conciencia de los riesgos pertinentes cuando su función laboral así lo requiera. La autoridad competente, o la autoridad u organismo establecido en el punto 1.7.4, deberá definir o aprobar el contenido del curso.»