2026/589

16.3.2026

REGLAMENTO DE EJECUCIÓN (UE) 2026/589 DEL CONSEJO

de 16 de marzo de 2026

por el que se aplica el Reglamento (UE) 2019/796 relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2019/796 del Consejo, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros [1], y en particular su artículo 13, apartado 1,

Vista la propuesta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad,

Considerando lo siguiente:

(1) El 17 de mayo de 2019, el Consejo adoptó el Reglamento (UE) 2019/796.

(2) Como parte de la actuación continua, específica y coordinada de la Unión frente a los agentes de ciberamenazas persistentes, procede incluir a dos personas físicas y tres entidades en la lista de personas físicas o jurídicas, entidades y organismos sujetos a medidas restrictivas que figura en el anexo I del Reglamento (UE) 2019/796. Dichas personas físicas y entidades son responsables de ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión o sus Estados miembros, o están implicadas en ellos.

(3) Por lo tanto, procede modificar el anexo I del Reglamento (UE) 2019/796 en consecuencia.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

El anexo I del Reglamento (UE) 2019/796 se modifica de conformidad con el anexo del presente Reglamento.

Artículo 2

El presente Reglamento entrará en vigor el día de su publicación en el *Diario Oficial de la Unión Europea*.

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

Hecho en Bruselas, el 16 de marzo de 2026.

Por el Consejo

La Presidenta

K. KALLAS

[1] DO L 129 I de 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ANEXO

El anexo I del Reglamento (UE) 2019/796 se modifica como sigue:

1) Bajo el epígrafe «A. Personas físicas», se añaden las entradas siguientes:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«18.	CHEN Cheng	陈诚 (ortografía china) Alias: Jesse Chen lengmo l3n6m0 Fecha de nacimiento: 20.10.1984 Lugar de nacimiento: Yancheng, Jiangsu, China Nacionalidad: china Sexo: masculino	Chen Cheng es un empresario chino, cofundador y uno de los directores generales (director de operaciones) de Anxun Information Technology Co. Ltd. También es representante legal de la sucursal de Sichuan de dicha empresa. Anxun Information Technology Co. Ltd., también conocida como i-Soon, es una empresa con sede en la República Popular China (RPC) que ofrece servicios de "alquiler de piratería informática". Anxun Information Technology Co. Ltd. ha atacado infraestructuras críticas y funciones estatales vitales de Estados miembros, y ha accedido a información clasificada y la ha vendido. Además, Anxun Information Technology Co. Ltd. ha atacado a Gobiernos de varios terceros Estados, constituyendo así una amenaza para los objetivos de la política exterior y de seguridad común (PESC) de la Unión establecidos en el artículo 21, apartado 2, letras a) a c), del Tratado de la Unión Europea. Anxun Information Technology Co. Ltd. obtiene un importante beneficio económico por los servicios prestados. Por lo tanto, Anxun Information Technology Co. Ltd. es responsable de ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión y sus Estados miembros, así como de ataques contra terceros Estados. Como tal, Chen Cheng es responsable de ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros, así como de ciberataques con un efecto significativo contra terceros Estados, y está implicado en ellos.	16.3.2026

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
19.	WU Haibo	吴海波 (ortografía china) Alias: shutdown shutd0wn Lugar de nacimiento: China Nacionalidad: china Sexo: masculino	Wu Haibo es un empresario chino, cofundador y uno de los directores generales (consejero delegado) de Anxun Information Technology Co. Ltd. También es el representante legal, presidente y director general de la sucursal de Shanghái ("central") de Anxun Information Technology Co. Ltd. Además, actúa como representante legal de la sucursal de Sichuan de dicha empresa. Anxun Information Technology Co. Ltd., también conocida como i-Soon, es una empresa con sede en la República Popular China (RPC) que ofrece servicios de "alquiler de piratería informática". Anxun Information Technology Co. Ltd. ha atacado infraestructuras críticas y funciones estatales vitales de Estados miembros, y ha accedido a información clasificada y la ha vendido. Además, Anxun Information Technology Co. Ltd. ha atacado a Gobiernos de varios terceros Estados, constituyendo así una amenaza para los objetivos de la política exterior y de seguridad común (PESC) de la Unión establecidos en el artículo 21, apartado 2, letras a) a c), del Tratado de la Unión Europea. Anxun Information Technology Co. Ltd. obtiene un importante beneficio económico por los servicios prestados. Por lo tanto, Anxun Information Technology Co. Ltd. es responsable de ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros, así como de ataques contra terceros Estados. Wu Haibo ha estado implicado en la dirección y el fomento de intentos de ciberataques con un efecto significativo contra Estados miembros. Como tal, es responsable de ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros, así como de ciberataques con un efecto significativo contra terceros Estados, y está implicado en ellos.	16.3.2026».

2) Bajo el epígrafe «B. Personas jurídicas, entidades y organismos», se añaden las entradas siguientes:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (ortografía china) Alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Dirección: Fenghao East Road, Room 103, Building 6, N.º 9, distrito de Haidian de Pekín, China Lugar de registro: Pekín, China Fecha de registro: 2.9.2010 Código de Crédito Social Unificado: 91110108562135265P	Integrity Technology Group es una empresa de ciberseguridad, con sede en la República Popular China (RPC), que facilitó ciberataques vinculados a Advanced Persistent Threat (APT) Flax Typhoon. Tal APT utilizó los productos y la tecnología de Integrity Technology Group para desplegar sus actividades de explotación de redes informáticas. Desde entonces, los productos de Integrity Technology Group se han utilizado para poner en peligro dispositivos del internet de las cosas y acceder a ellos en los Estados miembros, así como en países de toda Europa y a nivel mundial. Entre 2022 y 2023, Flax Typhoon accedió al menos a 65 600 dispositivos de la internet de las cosas en seis Estados miembros utilizando los productos de Integrity Technology Group. Por lo tanto, los productos e infraestructuras comerciales de Integrity Technology Group se utilizaron de forma rutinaria en ciberataques contra Estados miembros y terceros Estados. Por consiguiente, al afectar a sistemas de información relacionados con la infraestructura digital, Integrity Technology Group presta apoyo técnico y material para ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros y terceros Estados.	16.3.2026

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
6.	Emennet Pasargad	Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Lugar de registro: Teherán, Irán Número de registro: 554267 Lugar principal de actividad: Teherán, Irán	Emennet Pasargad es un ciberagente iraní (empresa) que ha atacado numerosas entidades, en particular en Estados miembros y en los Estados Unidos (EE. UU.). Emennet Pasargad, actuando bajo el alias "Anzu Team", atacó la infraestructura digital de Suecia y comprometió un servicio de SMS sueco, lo que afectó a un gran número de personas. Además, actuando bajo el alias "Holy Souls", la entidad comprometió la base de datos de suscriptores de la revista satírica francesa *Charlie Hebdo* y la publicitó para su venta en la red oscura. Emennet Pasargard comprometió vallas publicitarias durante los Juegos Olímpicos de París y difundió campañas de desinformación a través de ellas. Emennet Pasargad también intentó interferir en las elecciones presidenciales estadounidenses de 2020, poniendo en riesgo la democracia y el Estado de Derecho, al obtener información confidencial sobre los votantes estadounidenses y conseguir acceso no autorizado a la red informática de una empresa de medios de comunicación estadounidense. Por consiguiente, Emennet Pasargad es responsable de ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros, así como de ciberataques con un efecto significativo contra un tercer Estado.	16.3.2026

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (ortografía china) Alias: i-Soon Dirección: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, distrito de Minhang, Shanghái Código de Crédito Social Unificado: 91510105332025597A (sucursal de Sichuan) Código de Crédito Social Unificado: 9131011656190613 6G (sucursal de Shanghái) Sitio web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Números de teléfono: +862161119992, +8605645893417, +8613761671735, +864000665915 Correo electrónico: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. es una empresa con sede en la República Popular China que ofrece servicios de “alquiler de piratería informática”. Ha atacado infraestructuras críticas y funciones estatales vitales de Estados miembros, y ha accedido a información clasificada y la ha vendido. Además, Anxun Information Technology Co. Ltd. ha atacado a Gobiernos de varios terceros Estados, constituyendo así una amenaza para los objetivos de la política exterior y de seguridad común (PESC) de la Unión, establecidos en el artículo 21, apartado 2, letras a) a c), del Tratado de la Unión Europea.. Anxun Information Technology Co. Ltd. obtiene un importante beneficio económico por los servicios prestados. Por consiguiente, Anxun Information Technology Co. Ltd. es responsable de ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros, así como de ciberataques con un efecto significativo contra terceros Estados.	16.3.2026».