►**B**

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

(DO L 129I de 17.5.2019, p. 1)

Modificado por:

		Diario Oficial		
		nº	página	fecha
►**M1**	Reglamento de Ejecución (UE) 2020/1125 del Consejo de 30 de julio de 2020	L 246	4	30.7.2020
►**M2**	Reglamento de Ejecución (UE) 2020/1536 del Consejo de 22 de octubre de 2020	L 351 I	1	22.10.2020
►**M3**	Reglamento de Ejecución (UE) 2020/1744 del Consejo de 20 de noviembre de 2020	L 393	1	23.11.2020
►**M4**	Reglamento de Ejecución (UE) 2022/595 de la Comisión de 11 de abril de 2022	L 114	60	12.4.2022

Rectificado por:

►**C1** Rectificación, DO L 230 de 17.7.2020, p. 37 (2019/796)

▼B

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

Artículo 1

1. El presente Reglamento se aplica a los ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, que constituyan una amenaza externa para la Unión o para sus Estados miembros.

2. Entre los ciberataques que constituyen una amenaza externa se incluyen aquellos que:

a) se originen, o se cometan, desde el exterior de la Unión;

b) utilicen infraestructura fuera de la Unión;

c) hayan sido cometidos por una persona física o jurídica, una entidad o un organismo establecidos o que tengan actividad fuera de la Unión; o

d) hayan sido cometidos con el apoyo, bajo la dirección o bajo el control de una persona física o jurídica que tenga actividad fuera de la Unión.

3. A tal fin, los ciberataques son acciones que implican cualesquiera de los siguientes elementos:

a) acceso a sistemas de información;

b) intromisión en sistemas de información;

c) intromisión en datos; o

d) interceptación de datos,

cuando dichas acciones no estén debidamente autorizadas por el propietario o por otro titular de derechos del sistema o de los datos, o de parte de los mismos, o no estén permitidas por el Derecho de la Unión o de un Estado miembro.

4. Entre los ciberataques que constituyen una amenaza para los Estados miembros se incluyen los que afecten a los sistemas de información relacionados, entre otras aspectos, con:

a) las infraestructuras críticas, incluidos los cables submarinos y los objetos lanzados al espacio ultraterrestre, que resulten esenciales para el mantenimiento de funciones vitales de la sociedad, o para la salud, la seguridad, la protección y el bienestar económico o social de las personas;

b) los servicios necesarios para el mantenimiento de actividades sociales o económicas esenciales, en particular en los sectores de la energía (electricidad, petróleo y gas); el transporte (aéreo, ferroviario, fluvial o marítimo y por carretera); la actividad bancaria; las infraestructuras de los mercados financieros; el sector sanitario (proveedores de asistencia sanitaria, hospitales y clínicas privadas); el suministro y la distribución de agua potable; las infraestructuras digitales; y cualquier otro sector que resulte esencial para el Estado miembro de que se trate;

▼B

c) las funciones vitales del Estado, en particular en los ámbitos de la Defensa, la gobernanza y el funcionamiento de las instituciones, incluido en el caso de las elecciones públicas o los procesos electorales, el funcionamiento de las infraestructuras económicas y civiles, la seguridad interior, y las relaciones exteriores, también a través de las misiones diplomáticas;

d) el almacenamiento o el tratamiento de información clasificada; o

e) los equipos de respuesta de emergencia del Estado.

5. Los ciberataques que constituyen una amenaza para la Unión incluirán los cometidos contra sus instituciones, órganos y organismos, sus delegaciones en terceros países o ante organizaciones internacionales, sus operaciones y misiones de la política común de seguridad y defensa (PCSD) y sus representantes especiales.

6. Cuando se estimen necesarias para el cumplimiento de los objetivos de la política exterior y de seguridad común (PESC) en las disposiciones pertinentes del artículo 21 del Tratado de la Unión Europea, también podrán aplicarse medidas restrictivas con arreglo al presente Reglamento en respuesta a ciberataques que tengan un efecto significativo contra terceros Estados u organizaciones internacionales.

7. A efectos del presente Reglamento, se entenderá por:

a) «Sistemas de información»: todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos digitales, así como los datos digitales almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.

b) «Intromisión en sistemas de información»: obstaculización o interrupción del funcionamiento de un sistema de información introduciendo datos digitales, transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo tales datos, o haciéndolos inaccesibles.

c) «Intromisión en datos»: borrado, dañado, deterioro, alteración o supresión de los datos digitales en un sistema de información, o inutilización del acceso a estos datos. También incluirá el robo de datos, fondos, recursos económicos o derechos de propiedad intelectual.

d) «Interceptación de datos»: interceptación, por medios técnicos, de transmisiones no públicas de datos digitales hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos digitales.

8. A efectos del presente Reglamento, se aplicarán las siguientes definiciones suplementarias:

a) «Demanda»: toda reclamación, con independencia de que se haya realizado por la vía judicial, antes o después de la fecha de entrada en vigor del presente Reglamento, formulada en virtud de un contrato o transacción o en relación con estos, y que incluirá en particular:

   i) toda demanda de cumplimiento de una obligación derivada de un contrato o transacción o en relación con estos;

   ii) toda demanda de prórroga o pago de una fianza, una garantía financiera o una indemnización, independientemente de la forma que adopte;

   iii) toda demanda de compensación en relación con un contrato o transacción;

   iv) toda demanda de reconvención;

▼B

v) toda reclamación de reconocimiento o ejecución, incluso mediante procedimiento de *exequatur*, de una sentencia, un laudo arbitral o una decisión equivalente, dondequiera que se adopte o se dicte.

b) «Contrato o transacción»: cualquier transacción con independencia de la forma que adopte y de la legislación aplicable, comprenda uno o más contratos u obligaciones similares entre partes idénticas o entre partes diferentes; a tal efecto, el término «contrato» incluirá cualquier fianza, garantía o indemnización, en particular garantías financieras o indemnizaciones financieras, y crédito, jurídicamente independientes o no, así como cualquier disposición conexa derivada de la transacción o en relación con ella.

c) «Autoridades competentes»: las autoridades competentes de los Estados miembros tal como se mencionan en los sitios web enumerados en el anexo II.

d) «Recursos económicos»: los activos de todo tipo, tangibles o intangibles, mobiliarios o inmobiliarios, que no sean fondos, pero que puedan utilizarse para obtener fondos, bienes o servicios.

e) «Inmovilización de recursos económicos»: toda actuación con la que se pretenda impedir el uso de recursos económicos para obtener fondos, bienes o servicios de cualquier manera, incluidos la venta, el alquiler o la constitución de una hipoteca.

f) «Inmovilización de fondos»: el hecho de impedir cualquier movimiento, transferencia, alteración, utilización, negociación de fondos o acceso a estos, cuyo resultado sea un cambio de volumen, importe, localización, titularidad, posesión, naturaleza o destino de esos fondos, o cualquier otro cambio que permita la utilización de dichos fondos, incluida la gestión de cartera.

g) «Fondos»: los activos y beneficios financieros de cualquier naturaleza incluidos en la siguiente relación no exhaustiva:

i) efectivo, cheques, derechos dinerarios, efectos, giros y otros instrumentos de pago;

ii) depósitos en entidades financieras u otros entes, saldos en cuentas, deudas y obligaciones de deuda;

iii) valores negociables e instrumentos de deuda públicos y privados, tales como acciones y participaciones, certificados de valores, bonos, pagarés, warrants, obligaciones y contratos relacionados con productos financieros derivados;

iv) intereses, dividendos u otros ingresos devengados o generados por activos;

v) créditos, derechos de compensación, garantías, garantías de buena ejecución u otros compromisos financieros;

vi) cartas de crédito, conocimientos de embarque y comprobantes de venta; y

vii) documentos que atestigüen un interés en fondos o recursos financieros.

▼B

h) «Territorio de la Unión»: los territorios de los Estados miembros en los que es aplicable el Tratado, y en las condiciones establecidas en el mismo, incluido su espacio aéreo,.

Artículo 2

Los factores que determinen si un ciberataque tiene un efecto significativo a que se refiere el artículo 1, apartado 1, incluirán cualesquiera de los siguientes elementos:

a) el alcance, la escala, la repercusión o la gravedad de la perturbación ocasionada; incluido en las actividades económicas y sociales, los servicios esenciales, las funciones fundamentales del Estado, el orden público o la seguridad pública;

b) el número de personas físicas o jurídicas, entidades u organismos afectados;

c) el número de Estados miembros afectados;

d) el importe de las pérdidas económicas ocasionadas, por ejemplo mediante un robo a gran escala de fondos, de recursos económicos o de propiedad intelectual;

e) los beneficios económicos obtenidos por el infractor, para sí o para otros;

f) la cantidad o la naturaleza de los datos sustraídos o la magnitud de las violaciones de datos; o

g) la naturaleza de los datos comercialmente sensibles a los que se haya tenido acceso.

Artículo 3

1. Se inmovilizarán todos los fondos y recursos económicos que pertenezcan a cualquier persona física o jurídica, entidad u organismo que figure en el anexo I, al igual que todos los fondos y recursos económicos que esas personas físicas o jurídicas, entidades u organismos posean, detengan o controlen.

2. No se pondrá a disposición directa ni indirecta de las personas físicas o jurídicas, entidades u organismos que figuren en el anexo I ni se utilizará en su beneficio ningún tipo de fondos o recursos económicos.

3. El anexo I incluirá, tal y como estén definidas por el Consejo de conformidad con el artículo 5, apartado 1, de la Decisión (PESC) 2019/797, a:

a) las personas físicas o jurídicas, entidades u organismos que sean responsables de los ciberataques o intentos de ciberataques;

b) las personas físicas o jurídicas, entidades u organismos que presten ayuda financiera, técnica o material o que estén implicadas de alguna otra forma en ciberataques o tentativas de ciberataque, en particular mediante la planificación, preparación, dirección o fomento de dichos ataques, así como la participación en ellos o la ayuda a su comisión, o la facilitación de su comisión por acción u omisión;

c) las personas físicas o jurídicas, entidades u organismos asociados con las personas físicas o jurídicas, entidades u organismos a que se refieren las letras a) y b) del presente apartado.

▼B

Artículo 4

1. No obstante lo dispuesto en el artículo 3, las autoridades competentes de los Estados miembros podrán autorizar la liberación de determinados fondos o recursos económicos inmovilizados o la puesta a disposición de determinados fondos o recursos económicos, en las condiciones que consideren oportunas, tras haberse cerciorado de que dichos fondos o recursos económicos:

a) ►C1 son necesarios para satisfacer las necesidades básicas de las personas físicas o jurídicas, entidades u organismos enumerados en el anexo I ◄ y de los miembros de la familia que dependan de dichas personas físicas, como el pago de alimentos, alquileres o hipotecas, medicamentos y tratamientos médicos, impuestos, primas de seguros y tasas de servicios públicos;

b) se destinan exclusivamente al pago de honorarios profesionales razonables o al reembolso de gastos correspondientes a la prestación de servicios jurídicos;

c) se destinan exclusivamente al pago de tasas o gastos ocasionados por servicios ordinarios de custodia o mantenimiento de los fondos o recursos económicos inmovilizados;

d) son necesarios para gastos extraordinarios, siempre y cuando la autoridad competente que corresponda haya notificado a las autoridades competentes de los demás Estados miembros y a la Comisión, al menos dos semanas antes de la autorización, los motivos por los cuales considera que debe concederse una autorización específica; o

e) se ingresan en la cuenta o se pagan con cargo a la cuenta de una misión diplomática o consular o de una organización internacional que goce de inmunidad con arreglo al Derecho internacional, en la medida en que dichos pagos estén destinados a ser utilizados para los fines oficiales de la misión diplomática o consular o de la organización internacional.

2. El Estado miembro de que se trate informará a los demás Estados miembros y a la Comisión de cualquier autorización concedida en virtud del apartado 1 en el plazo de dos semanas tras la autorización.

Artículo 5

1. Como excepción a lo dispuesto en el artículo 3, apartado 1, las autoridades competentes de los Estados miembros podrán autorizar la liberación de determinados fondos o recursos económicos inmovilizados siempre que concurran las siguientes condiciones:

a) que los fondos o recursos económicos sean objeto de una resolución arbitral pronunciada antes de la fecha en que la persona física o jurídica, entidad u organismo a que se refiere el artículo 3 haya sido incluido en la lista del anexo I, o de una resolución judicial o administrativa adoptada en la Unión, o de una resolución judicial con fuerza ejecutiva en el Estado miembro de que se trate, dictada antes o después de esa fecha;

b) que los fondos o recursos económicos vayan a utilizarse exclusivamente para satisfacer las obligaciones impuestas por tales resoluciones o reconocerse como válidas en tales resoluciones, dentro de los límites establecidos por la legislación y la reglamentación aplicable a los derechos de los acreedores;

c) que la resolución no beneficie a una persona física o jurídica, entidad u organismo enumerado en el anexo I; y

d) que el reconocimiento de la resolución no sea contrario al orden público del Estado miembro de que se trate.

▼B

2. El Estado miembro de que se trate informará a los demás Estados miembros y a la Comisión de cualquier autorización concedida en virtud del apartado 1 en el plazo de dos semanas tras la autorización.

Artículo 6

1. Como excepción a lo dispuesto en el artículo 3, apartado 1, y siempre que un pago sea debido por una persona física o jurídica, entidad u organismo que figure en el anexo I en virtud de un contrato o acuerdo celebrado por la persona física o jurídica, entidad u organismo en cuestión, o de una obligación que le fuera aplicable, antes de la fecha en que se haya incluido en el anexo I a dicha persona física o jurídica, entidad u organismo, las autoridades competentes de los Estados miembros podrán autorizar, en las condiciones que consideren oportunas, la liberación de determinados fondos o recursos económicos inmovilizados, siempre que la autoridad competente en cuestión haya considerado que:

a) los fondos o los recursos económicos serán utilizados para efectuar un pago por una persona física o jurídica, una entidad o un organismo contemplados en el anexo I; y

b) el pago no infringe el artículo 3, apartado 2.

2. El Estado miembro de que se trate informará a los demás Estados miembros y a la Comisión de cualquier autorización concedida en virtud del apartado 1 en el plazo de dos semanas tras la autorización.

Artículo 7

1. El artículo 3, apartado 2, no impedirá el abono en las cuentas inmovilizadas por instituciones financieras o crediticias que reciban fondos transferidos por terceros a la cuenta de una persona física o jurídica, entidad u organismo que figure en la lista, siempre que los abonos a dichas cuentas también se inmovilicen. Las entidades financieras o de crédito informarán sin demora a la autoridad competente pertinente sobre cualquier operación de ese tipo.

2. El artículo 3, apartado 2, no se aplicará al abono en cuentas inmovilizadas de:

a) intereses u otros beneficios correspondientes a dichas cuentas;

b) pagos en virtud de contratos o acuerdos celebrados u obligaciones contraídas antes de la fecha en que la persona física o jurídica, entidad u organismo a que se refiere el artículo 3, apartado 1, se haya incluido en el anexo I; o

c) pagos adeudados en virtud de una resolución judicial, administrativa o arbitral adoptada en un Estado miembro o ejecutiva en el Estado miembro de que se trate;

siempre que dichos intereses, otros beneficios y pagos permanezcan sujetos a las medidas establecidas en el artículo 3, apartado 1.

Artículo 8

1. Sin perjuicio de las normas aplicables en materia de comunicación de información, confidencialidad y secreto profesional, las personas físicas y jurídicas, entidades y organismos:

▼B

a) transmitirán inmediatamente cualquier información que facilite el cumplimiento del presente Reglamento, como información sobre las cuentas y los importes inmovilizados de conformidad con el artículo 3, apartado 1, a la autoridad competente del Estado miembro de residencia o establecimiento, y remitirán esa información a la Comisión, directamente o a través de los Estados miembros; y

b) cooperarán con las autoridades competentes en toda verificación de la información a que se refiere la letra a).

2. Toda información adicional recibida directamente por la Comisión se pondrá a disposición de los Estados miembros.

3. Toda información facilitada o recibida de conformidad con el presente artículo se utilizará exclusivamente para los fines para los cuales se haya facilitado o recibido.

Artículo 9

Queda prohibido participar de manera consciente y deliberada en acciones cuyo objeto o efecto sea eludir las medidas a que se refiere el artículo 3.

Artículo 10

1. La inmovilización de fondos y recursos económicos o la negativa a facilitarlos, llevadas a cabo de buena fe con la convicción de que dicha acción se atiene al presente Reglamento, no dará origen a ningún tipo de responsabilidad por parte de la persona física o jurídica, entidad u organismo que la ejecute, ni de sus directores o empleados, a menos que se pruebe que los fondos o recursos económicos han sido inmovilizados o retenidos por motivo de negligencia.

2. Las acciones emprendidas por personas físicas o jurídicas, entidades u organismos no generarán responsabilidad de ninguna clase por su parte si no sabían, y no tenían ningún motivo razonable para sospechar, que sus acciones infringirían las medidas establecidas en el presente Reglamento.

Artículo 11

1. No se satisfará demanda alguna relacionada con un contrato o transacción cuya ejecución se haya visto afectada, directa o indirectamente, total o parcialmente, por las medidas impuestas por el presente Reglamento, incluidas las demandas de indemnización o cualquier otra demanda de este tipo, tales como una demanda de compensación o una demanda a título de garantía, en particular cualquier demanda que tenga por objeto la prórroga o el pago de una fianza, una garantía o una indemnización, especialmente garantías o indemnizaciones financieras, con independencia de la forma que adopte, si la presentan:

a) personas físicas o jurídicas, entidades u organismos designados que figuren en la lista del anexo I;

b) cualquier persona física o jurídica, entidad u organismo que actúe a través o en nombre de una de las personas físicas o jurídicas, entidades u organismos a que se refiere la letra a).

2. En cualquier procedimiento de demanda, la carga de la prueba de que el apartado 1 no prohíbe estimar la demanda recaerá en la persona física o jurídica, entidad u organismo que la formula.

3. El presente artículo se entenderá sin perjuicio del derecho de las personas físicas o jurídicas, entidades y organismos mencionados en el apartado 1 a recurrir por la vía judicial la legalidad del incumplimiento de obligaciones contractuales de conformidad con el presente Reglamento.

▼B

Artículo 12

1. La Comisión y los Estados miembros se comunicarán mutuamente las medidas adoptadas en aplicación del presente Reglamento y compartirán toda la información pertinente de que dispongan relacionada con el presente Reglamento, en particular la información con respecto a:

a) los fondos inmovilizados con arreglo al artículo 3 y las autorizaciones concedidas en virtud de los artículos 4, 5 y 6;

b) los problemas de violación del presente Rglamento y de su ejecución, y las sentencias dictadas por los tribunales nacionales.

2. Los Estados miembros se comunicarán mutua e inmediatamente y comunicarán a la Comisión cualquier otra información pertinente de que tengan conocimiento y que pueda afectar a la aplicación efectiva del presente Reglamento.

Artículo 13

1. Cuando el Consejo decida someter a una persona física o jurídica, entidad u organismo a las medidas a las que se refiere el artículo 3, modificará el anexo I en consecuencia.

2. El Consejo comunicará la decisión a que se refiere el apartado 1, junto con los motivos de inclusión en la lista, a la persona física o jurídica, entidad u organismo de que se trate, bien directamente si se conoce su dirección, o mediante la publicación de un anuncio, ofreciendo a dicha persona física o jurídica, entidad u organismo la oportunidad de presentar observaciones.

3. En caso de que se formulen observaciones o se presenten nuevas pruebas sustanciales, el Consejo reconsiderará la decisión a que se refiere el apartado 1 e informará a la persona física o jurídica, entidad u organismo de que se trate en consecuencia.

4. La lista del anexo I se revisará periódicamente y como mínimo cada doce meses.

5. La Comisión estará facultada para modificar el anexo II, atendiendo a la información facilitada por los Estados miembros.

Artículo 14

1. En el anexo I se expondrán los motivos de la inclusión en la lista de las personas físicas o jurídicas, entidades u organismos afectados.

2. El anexo I contendrá, cuando esté disponible, la información necesaria para identificar a las personas físicas o jurídicas, entidades u organismos de que se trate. Por lo que respecta a las personas físicas, esa información podrá incluir el nombre, los apellidos y los alias, el lugar y fecha de nacimiento, la nacionalidad, el número de pasaporte o de documento de identidad, el sexo, la dirección postal, si se conoce, y el cargo o la profesión. Respecto de las personas jurídicas, entidades u organismos, dicha información podrá incluir el nombre, la fecha y el lugar de registro, el número de registro y el domicilio social.

Artículo 15

1. Los Estados miembros establecerán las normas sobre las sanciones aplicables a las infracciones de las disposiciones del presente Reglamento y adoptarán todas las medidas necesarias para garantizar su aplicación. Las sanciones establecidas deberán ser efectivas, proporcionadas y disuasorias.

▼B

2. Los Estados miembros notificarán a la Comisión las normas mencionadas en el apartado 1 sin demora tras la entrada en vigor del presente Reglamento, así como cualquier modificación posterior.

Artículo 16

1. La Comisión llevará a cabo el tratamiento de datos personales en el ejercicio de sus funciones conforme al presente Reglamento. Dichas funciones incluyen:

a) añadir el contenido del anexo I en la lista electrónica consolidada de personas, grupos y entidades sujetos a sanciones financieras de la Unión y en el mapa interactivo de sanciones, ambos de acceso público;

b) tratar la información sobre las repercusiones de las medidas del presente Reglamento, tales como el valor de los fondos inmovilizados y la información sobre las autorizaciones concedidas por las autoridades competentes.

2. A efectos del presente Reglamento, queda designado el servicio de la Comisión citado en el anexo II como «responsable del tratamiento» en la Comisión a efectos del artículo 3, apartado 8, del Reglamento (UE) n.º 2018/1725, para garantizar que las personas físicas afectadas puedan ejercer sus derechos conforme a dicho Reglamento.

Artículo 17

1. Los Estados miembros designarán a las autoridades competentes a que se refiere el presente Reglamento y las mencionarán en los sitios web que figuran en el anexo II. Los Estados miembros notificarán a la Comisión todo cambio de las direcciones de sus sitios web enumerados en el anexo II.

2. Los Estados miembros notificarán a la Comisión, inmediatamente después de la entrada en vigor del presente Reglamento, cuáles son sus respectivas autoridades competentes, incluidos los datos de contacto de dichas autoridades, así como toda modificación posterior.

3. Cuando el presente Reglamento requiera notificar, informar o establecer cualquier otra forma de comunicación con la Comisión, la dirección y otros datos de contacto que se utilizarán para dicha comunicación serán los indicados en el anexo II.

Artículo 18

El presente Reglamento se aplicará:

a) en el territorio de la Unión, incluido su espacio aéreo;

b) a bordo de toda aeronave o buque que esté bajo la jurisdicción de un Estado miembro;

c) a toda persona física, ya se encuentre dentro o fuera del territorio de la Unión, que sea nacional de un Estado miembro;

d) a toda persona jurídica, entidad u organismo, ya se encuentre dentro o fuera del territorio de la Unión, registrado o constituido con arreglo al Derecho de un Estado miembro;

e) a toda persona jurídica, entidad u organismo en relación con cualquier actividad comercial efectuada, en su totalidad o en parte, en la Unión.

▼B

Artículo 19

El presente Reglamento entrará en vigor el día siguiente al 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.

▼B

ANEXO I

Lista de personas físicas y jurídicas, entidades y organismos a que se refiere el artículo 3

▼M1

A. Personas físicas

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
▼M3				
1.	GAO Qiang	Fecha de nacimiento: 4 de octubre de 1983 Lugar de nacimiento: provincia de Shandong (China) Dirección: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nacionalidad: china Sexo: masculino	Gao Qiang está implicado en la operación «Cloud Hopper», una serie de ciberataques con un efecto significativo realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados. La operación «Cloud Hopper» se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas. El grupo conocido como «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» y «Potassium») llevó a cabo la operación «Cloud Hopper». Puede relacionarse a Gao Qiang con el APT10, entre otras cosas por su relación con la infraestructura de mando y control del grupo. Además, Gao Qiang estuvo empleado en Huaying Haitai, entidad incluida en la lista por facilitar y prestar apoyo a la operación «Cloud Hopper». Gao Qiang tiene vínculos con Zhang Shilong, que también ha sido incluido en la lista en relación con la operación «Cloud Hopper». Por lo tanto, Gao Qiang está relacionado tanto con Huaying Haitai como con Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Fecha de nacimiento: 10 de septiembre de 1981 Lugar de nacimiento: China Dirección: Hedong, Yuyang Road No 121, Tianjin, China Nacionalidad: china Sexo: masculino	Zhang Shilong está implicado en la operación «Cloud Hopper», una serie de ciberataques con un efecto significativo, realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados. La operación «Cloud Hopper» se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas.	30.7.2020

▼M3

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			El grupo conocido como «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» y «Potassium») llevó a cabo la operación «Cloud Hopper». Puede relacionarse a Zhang Shilong con APT10, entre otras cosas por el software malicioso que desarrolló y probó en relación con los ciberataques llevados a cabo por APT10. Además, Zhang Shilong estuvo empleado en Huaying Haitai, entidad incluida en la lista por facilitar y prestar apoyo a la operación «Cloud Hopper». Zhang Shilong tiene vínculos con Gao Qiang, que también ha sido incluido en la lista en relación con la operación «Cloud Hopper». Por lo tanto, Zhang Shilong está relacionado tanto con Huaying Haitai como con Gao Qiang.	

▼M1

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Fecha de nacimiento: 27 de mayo de 1972 Lugar de nacimiento: Oblast Perm, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 120017582, Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Alexey Minin participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como agente auxiliar de inteligencia humana del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Alexey Minin formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Fecha de nacimiento: 31 de julio de 1977 Lugar de nacimiento: Oblast Murmanskaya, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 100135556 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Aleksei Morenets participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como informático especializado en ciberseguridad del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Aleksei Morenets formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020

▼M1

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Fecha de nacimiento: 26 de julio de 1981 Lugar de nacimiento: Kursk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 100135555 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Evgenii Serebriakov participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como informático especializado en ciberseguridad del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Evgenii Serebriakov formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Fecha de nacimiento: 24 de agosto de 1972 Lugar de nacimiento: Ulyanovsk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 120018866 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Oleg Sotnikov participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como agente auxiliar de inteligencia humana del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Oleg Sotnikov formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020

▼M1

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
▼M2				
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Fecha de nacimiento: 15 de noviembre de 1990 Lugar de nacimiento: Kursk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Nacionalidad: rusa Sexo: masculino	Dmitry Badin participó en un ciberataque con un efecto significativo contra el Parlamento federal alemán (Bundestag). Como agente de inteligencia militar del 85.° Centro Principal de Servicios Especiales (GTsSS) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Dmitry Badin formó parte de un equipo de agentes rusos de inteligencia militar que dirigieron un ciberataque contra el Parlamento federal alemán (Bundestag) en abril y mayo de 2015. Este ciberataque iba dirigido contra el sistema de información del Parlamento y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como de la canciller Angela Merkel.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Fecha de nacimiento: 21 de febrero de 1961 Nacionalidad: rusa Sexo: masculino	Igor Kostyukov es el actual jefe del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), después de haber sido primer jefe adjunto del mismo. Una de las unidades bajo su mando es el 85.° Centro Principal de Servicios Especiales (GTsSS), conocido también como «unidad militar 26165» (sobrenombres en el sector: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» y «Strontium»). Como tal, Igor Kostyukov es responsable de los ciberataques perpetrados por el GTsSS, entre ellos los ciberataques con un efecto significativo constitutivos de amenaza externa para la Unión o sus Estados miembros. En particular, agentes de inteligencia militar del GTsSS participaron en el ciberataque contra el Parlamento federal alemán (Bundestag) ocurrido en abril y mayo de 2015 y la tentativa de ciberataque dirigido a piratear la red wifi de la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos en abril de 2018. El ciberataque contra el Parlamento federal alemán iba dirigido contra su sistema de información y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como de la canciller Angela Merkel.	22.10.2020

▼M1

B. Personas jurídicas, entidades y organismos

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Lugar: Tianjin, China	Huaying Haitai prestó apoyo financiero, técnico o material para la operación «Cloud Hopper», una serie de ciberataques con un efecto significativo, realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados, y facilitó dicha operación. La operación «Cloud Hopper» se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas. El grupo conocido como «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» y «Potassium») llevó a cabo la operación «Cloud Hopper». Puede relacionarse a Huaying Haitai con APT10. Además, Huaying Haitai tuvo en su nómina a Gao Qiang y a Zhang Shilong, ambos incluidos en la lista en relación con la operación «Cloud Hopper». Por ello se relaciona a Huaying Haitai con Gao Qiang y Zhang Shilong.	30.7.2020
2.	Chosun Expo	Alias: Chosen Expo; Korea Export Joint Venture Lugar: RPDC	Chosun Expo prestó apoyo financiero, técnico o material para una serie de ciberataques con un efecto significativo realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados, y facilitó su realización; entre ellos se incluye el ciberataque conocido como «WannaCry» y varios ciberataques contra la Autoridad de Supervisión Financiera de Polonia y Sony Pictures Entertainment, así como el ciberrobo al Banco de Bangladesh y la tentativa de ciberrobo al Banco Tien Phong de Vietnam. «WannaCry» perturbó sistemas de información de todo el mundo mediante ataques con programas de secuestro y el bloqueo del acceso a los datos. Afectó a los sistemas de información de empresas de la Unión, entre ellos diversos sistemas de información relativos a servicios necesarios para el mantenimiento de servicios y actividades económicas esenciales en los Estados miembros.	30.7.2020

▼M1

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			El ciberataque «WannaCry» fue llevado a cabo por el grupo conocido como «APT38» («Advanced Persistent Threat 38») o el «Grupo Lazarus». Puede relacionarse a Chosun Expo con APT38/Grupo Lazarus, entre otras cosas a través de las cuentas utilizadas para los ciberataques.	
3.	Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU)	Dirección: 22 Kirova Street, Moscú, Federación de Rusia	El Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), también conocido por el código 74455, es responsable de diversos ciberataques con un efecto significativo llevados a cabo desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados; entre ellos se incluyen los ciberataques conocidos como «NotPetya» o «EternalPetya» en junio de 2017 y los ciberataques dirigidos contra una red eléctrica ucraniana en el invierno de 2015 y 2016. El ciberataque «NotPetya» o «EternalPetya» impidió el acceso a los datos en una serie de empresas de la Unión, de Europa en general y de todo el mundo, mediante ataques a ordenadores con programas de secuestro y el bloqueo del acceso a los datos, lo que causó, entre otros efectos, importantes pérdidas económicas. El ciberataque contra una red eléctrica ucraniana provocó el apagado de partes de dicha red durante el invierno.	30.7.2020
			El ciberataque «NotPetya» o «EternalPetya» fue llevado a cabo por el grupo conocido como«Sandworm» (alias «Sandworm Team», «BlackEnergy Group», «Vodoo Bear», «Quedagh», «Olympic Destroyer» y «Telebots»), que también está detrás del ataque contra la red eléctrica ucraniana. El Centro Principal de Tecnologías Especiales del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia desempeña un papel activo en las actividades informáticas llevadas a cabo por Sandworm, por lo que es posible relacionarlo con dicho grupo.	

▼M1

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
▼M2				
4.	85.º Centro Principal de Servicios Especiales (GTsSS) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU)	Dirección: Komsomol'skiy Prospekt, 20, Moscú, 119146, Federación de Rusia	El 85.° Centro Principal de Servicios Especiales (GTsSS) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), conocido también como «unidad militar 26165» (sobrenombres en el sector: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» y «Strontium»), es responsable de ciberataques con un efecto significativo constitutivos de amenaza externa para la Unión o sus Estados miembros. En particular, agentes de inteligencia militar del GTsSS participaron en el ciberataque contra el Parlamento federal alemán (Bundestag) ocurrido en abril y mayo de 2015 y en la tentativa de ciberataque dirigido a piratear la red wifi de la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos en abril de 2018. El ciberataque contra el Parlamento federal alemán iba dirigido contra su sistema de información y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como de la canciller Angela Merkel.	22.10.2020

▼B

ANEXO II

Sitios web de información sobre las autoridades competentes y dirección para las notificaciones a la Comisión

▼M4

BÉLGICA

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGARIA

https://www.mfa.bg/en/EU-sanctions

CHEQUIA

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DINAMARCA

http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/

ALEMANIA

https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html

ESTONIA

https://vm.ee/et/rahvusvahelised-sanktsioonid

IRLANDA

https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/

GRECIA

http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html

ESPAÑA

https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/SancionesInternacionales.aspx

FRANCIA

http://www.diplomatie.gouv.fr/fr/autorites-sanctions/

CROACIA

https://mvep.gov.hr/vanjska-politika/medjunarodne-mjere-ogranicavanja/22955

ITALIA

https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

CHIPRE

https://mfa.gov.cy/themes/

LETONIA

http://www.mfa.gov.lv/en/security/4539

LITUANIA

http://www.urm.lt/sanctions

LUXEMBURGO

https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html

HUNGRÍA

https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szankcios-tajekoztato

▼**M4**

MALTA

https://foreignandeu.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx

PAÍSES BAJOS

https://www.rijksoverheid.nl/onderwerpen/internationale-sancties

AUSTRIA

https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/

POLONIA

https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe

https://www.gov.pl/web/diplomacy/international-sanctions

PORTUGAL

https://www.portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas

RUMANÍA

http://www.mae.ro/node/1548

ESLOVENIA

http://www.mzz.gov.si/si/omejevalni_ukrepi

ESLOVAQUIA

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINLANDIA

https://um.fi/pakotteet

SUECIA

https://www.regeringen.se/sanktioner

Dirección para las notificaciones a la Comisión Europea:

Comisión Europea

Dirección General de Estabilidad Financiera, Servicios Financieros y Unión de los Mercados de Capitales – DG FISMA

Rue de Spa 2

B-1049 Bruselas, Bélgica

Correo electrónico: relex-sanctions@ec.europa.eu