2025/886

13.5.2025

# REGLAMENTO DE EJECUCIÓN (UE) 2025/886 DEL CONSEJO

## de 12 de mayo de 2025

## 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,

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) El Consejo ha revisado la lista de personas físicas y jurídicas, entidades y organismos del anexo I del Reglamento (UE) 2019/796. Atendiendo a dicha revisión, deben actualizarse los motivos de la inclusión de seis personas en la lista de personas físicas y jurídicas, entidades y organismos sujetos a medidas restrictivas.

(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 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.

Hecho en Bruselas, el 12 de mayo de 2025.

*Por el Consejo*

*La Presidenta*

B. NOWACKA

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

*ANEXO*

En el anexo I del Reglamento (UE) 2019/796, bajo el epígrafe «A. Personas físicas», las entradas 3 a 8 se sustituyen por el texto siguiente:

| | Nombre | Información identificativa | Motivos | Fecha de inclusión en la lista |
|---|---|---|---|---|
| «3. | Alexey Valeryevich MININ | Алексей Валерьевич МИНИН<br>Fecha de nacimiento: 27.5.1972<br>Lugar de nacimiento: provincia de Perm, República Socialista Federativa Soviética de Rusia, actualmente Federación de Rusia<br>Número de pasaporte: 120017582<br>Expedido por: Ministry of Foreign Affairs of the Russian Federation<br>Validez: del 17.4.2017 al 17.4.2022<br>Lugar: Moscú, Federación de Rusia<br>Nacionalidad: rusa<br>Sexo: masculino | Alexey Minin participó en una tentativa de ciberataque con un efecto significativo potencial contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos, así como en ciberataques con un efecto significativo contra terceros Estados.<br>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) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.<br>Un jurado de acusación del Distrito Oeste de Pensilvania (Estados Unidos de América) ha acusado a Alexey Minin, como agente del GRU, de piratería informática, fraude electrónico, usurpación de identidad agravada y blanqueo de capitales.<br>El GRU sigue perpetrando ciberataques contra la Unión o sus Estados miembros. Por consiguiente, Alexey Minin, como miembro del GRU, está implicado en ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, constitutivos de una amenaza externa para la Unión o para sus Estados miembros. | 30.7.2020 |

| | Nombre | Información identificativa | Motivos | Fecha de inclusión en la lista |
|---|---|---|---|---|
| 4. | Aleksei Sergeyvich MORENETS | Алексей Сергеевич МОРЕНЕЦ<br>Fecha de nacimiento: 31.7.1977<br>Lugar de nacimiento: provincia de Murmanskaya, República Socialista Federativa Soviética de Rusia, actualmente Federación de Rusia<br>Número de pasaporte: 100135556<br>Expedido por: Ministry of Foreign Affairs of the Russian Federation<br>Validez: del 17.4.2017 al 17.4.2022<br>Lugar: Moscú, Federación de Rusia<br>Nacionalidad: rusa<br>Sexo: masculino | Aleksei Morenets participó en una tentativa de ciberataque con un efecto significativo potencial contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos, así como en ciberataques con un efecto significativo contra terceros Estados.<br>Como operador informático 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) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.<br>Un jurado de acusación del Distrito Oeste de Pensilvania (Estados Unidos de América) ha acusado a Aleksei Morenets, como miembro de la unidad militar 26165, de piratería informática, fraude electrónico, usurpación de identidad agravada y blanqueo de capitales.<br>El GRU sigue perpetrando ciberataques contra la Unión o sus Estados miembros. Por consiguiente, Aleksei Morenets, como miembro del GRU, está implicado en ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, constitutivos de una amenaza externa para la Unión o para sus Estados miembros. | 30.7.2020 |

| | Nombre | Información identificativa | Motivos | Fecha de inclusión en la lista |
|---|---|---|---|---|
| 5. | Evgenii Mikhaylovich SEREBRIAKOV | Евгений Михайлович СЕРЕБРЯКОВ<br>Fecha de nacimiento: 26.7.1981<br>Lugar de nacimiento: Kursk, República Socialista Federativa Soviética de Rusia, actualmente Federación de Rusia<br>Número de pasaporte: 100135555<br>Expedido por: Ministry of Foreign Affairs of the Russian Federation<br>Validez: del 17.4.2017 al 17.4.2022<br>Lugar: Moscú, Federación de Rusia<br>Nacionalidad: rusa<br>Sexo: masculino | Evgenii Serebriakov participó en una tentativa de ciberataque con un efecto significativo potencial contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos, así como en ciberataques con un efecto significativo contra terceros Estados.<br>Como operador informático 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) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.<br>Desde la primavera de 2022, Evgenii Serebriakov dirige “Sandworm” (alias “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” y “Telebots”), agente y grupo de piratas informáticos vinculado a la unidad 74455 de la Dirección Central de Inteligencia de Rusia. “Sandworm” ha llevado a cabo ciberataques contra Ucrania, incluidos organismos gubernamentales ucranianos, tras la guerra de agresión de Rusia contra Ucrania.<br>El GRU sigue perpetrando ciberataques contra la Unión o sus Estados miembros. Por consiguiente, Evgenii Serebriakov, como miembro del GRU, está implicado en ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, constitutivos de una amenaza externa para la Unión o para sus Estados miembros. | 30.7.2020 |

| | Nombre | Información identificativa | Motivos | Fecha de inclusión en la lista |
|---|---|---|---|---|
| 6. | Oleg Mikhaylovich SOTNIKOV | Олег Михайлович СОТНИКОВ<br>Fecha de nacimiento: 24.8.1972<br>Lugar de nacimiento: Ulyanovsk, República Socialista Federativa Soviética de Rusia, actualmente Federación de Rusia<br>Número de pasaporte: 120018866<br>Expedido por: Ministry of Foreign Affairs of the Russian Federation<br>Validez: del 17.4.2017 al 17.4.2022<br>Lugar: Moscú, Federación de Rusia<br>Nacionalidad: rusa<br>Sexo: masculino | Oleg Sotnikov participó en una tentativa de ciberataque con un efecto significativo potencial contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos, así como en ciberataques con un efecto significativo contra terceros Estados.<br>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) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.<br>Un jurado de acusación del Distrito Oeste de Pensilvania (Estados Unidos de América) ha acusado a Oleg Sotnikov, como agente del GRU, de piratería informática, fraude electrónico, usurpación de identidad agravada y blanqueo de capitales.<br>El GRU sigue perpetrando ciberataques contra la Unión o sus Estados miembros. Por consiguiente, Oleg Sotnikov, como miembro del GRU, está implicado en ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, constitutivos de una amenaza externa para la Unión o para sus Estados miembros. | 30.7.2020 |

| | Nombre | Información identificativa | Motivos | Fecha de inclusión en la lista |
|---|---|---|---|---|
| 7. | Dmitry Sergeyevich BADIN | Дмитрий Сергеевич БАДИН<br>Fecha de nacimiento: 15.11.1990<br>Lugar de nacimiento: Kursk, República Socialista Federativa Soviética de Rusia, actualmente Federación de Rusia<br>Nacionalidad: rusa<br>Sexo: masculino | Dmitry Badin participó en un ciberataque con un efecto significativo contra el Parlamento federal alemán (Deutscher Bundestag) y en ciberataques con un efecto significativo contra terceros Estados.<br>Como agente de inteligencia militar del 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), Dmitry Badin formó parte de un equipo de agentes rusos de inteligencia militar que perpetró un ciberataque contra el Parlamento federal alemán en abril y mayo de 2015. Ese 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 la de la excanciller Angela Merkel.<br>Un jurado de acusación del Distrito Oeste de Pensilvania (Estados Unidos de América) ha acusado a Dmitry Badin, como miembro de la unidad militar 26165, de piratería informática, fraude electrónico, usurpación de identidad agravada y blanqueo de capitales.<br>El GRU sigue perpetrando ciberataques contra la Unión o sus Estados miembros. Por consiguiente, Dmitry Badin, como miembro del GRU, está implicado en ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, constitutivos de una amenaza externa para la Unión o para sus Estados miembros. | 22.10.2020 |

| | Nombre | Información identificativa | Motivos | Fecha de inclusión en la lista |
|---|---|---|---|---|
| 8. | Igor Olegovich KOSTYUKOV | Игорь Олегович КОСТЮКОВ<br>Fecha de nacimiento: 21.2.1961<br>Nacionalidad: rusa<br>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.º Centro Principal de Servicios Especiales (GTsSS) (alias "unidad militar 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" y "Strontium").<br>Como tal, Igor Kostyukov es responsable de los ciberataques perpetrados por el GTsSS, entre ellos los ciberataques con un efecto significativo constitutivos de una amenaza externa para la Unión o sus Estados miembros.<br>En particular, agentes de inteligencia militar del GTsSS participaron en el ciberataque contra el Parlamento federal alemán (Deutscher Bundestag) 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.<br>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 la de la excanciller Angela Merkel.<br>El GRU sigue perpetrando ciberataques contra la Unión o sus Estados miembros. Por consiguiente, Igor Kostyukov, como miembro del GRU, está implicado en ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, constitutivos de una amenaza externa para la Unión o para sus Estados miembros. | 22.10.2020». |