2025/173

27.1.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/173 DEL CONSEJO

de 27 de enero 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, 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) Las medidas restrictivas selectivas contra los ciberataques con un efecto significativo, que constituyan una amenaza externa para la Unión o sus Estados miembros, forman parte de las medidas previstas en el marco de la Unión para una respuesta diplomática conjunta a las actividades informáticas malintencionadas, a saber, el conjunto de instrumentos de ciberdiplomacia, y son un instrumento crucial de prevención y disuasión y de respuesta a tales actividades.

(3) Las actividades informáticas malintencionadas contra infraestructuras críticas o servicios esenciales, en particular mediante el uso de programas de secuestro y de borrado de archivos, el ataque a las cadenas de suministro y el ciberespionaje, incluidas las actividades de robo de propiedad intelectual, están aumentando en número, frecuencia y sofisticación. Debido a sus consecuencias disruptivas y destructivas, dichas actividades suponen una amenaza sistémica para la seguridad, la economía y la democracia, y para la sociedad de la Unión en general.

(4) En 2020, se perpetraron ciberataques con efectos significativos contra Estonia. Se llevaron a cabo ciberataques dirigidos contra los sistemas informáticos de múltiples instituciones, con el fin de utilizar los datos para amenazar la seguridad de Estonia. Dichos ciberataques afectaron al almacenamiento de información clasificada.

(5) Como parte de la actuación continua, específica y coordinada de la Unión frente a los agentes de ciberamenazas persistentes, procede incluir a tres personas físicas en la lista de personas físicas y jurídicas, entidades y organismos sujetos a medidas restrictivas que figura en el anexo I del Reglamento (UE) 2019/796. Dichas personas 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.

(6) 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 con arreglo a lo dispuesto en 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 27 de enero de 2025.

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

En el anexo I del Reglamento (UE) 2019/796, se añaden las entradas siguientes en la sección A, «Personas físicas»:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Fecha de nacimiento: 16.9.1997 Nacionalidad: rusa Sexo: masculino Entidad asociada: Main Directorate of the General Staff of the Armed Forces of the Russian Federation	Nikolay Korchagin participa en ciberataques con efectos significativos, y es responsable de ellos, mediante la realización de actividades de inteligencia contra Estonia y la obtención ilegal de acceso a un sistema informático. Nikolay Korchagin es oficial de la unidad militar 29155 de la Dirección Principal del Alto Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (military unit 29155 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation) (GRU). En el ejercicio de dicho cargo, participa en ciberataques contra sistemas informáticos, y es responsable de ellos, con el fin de recopilar datos de los sistemas de datos de múltiples instituciones que ofrecen de forma independiente o combinada una visión general de la política de ciberseguridad de Estonia y de las cibercapacidades del Estado, así como datos personales sensibles y otros datos sensibles, con el fin de utilizarlos para amenazar la seguridad de Estonia. Los ataques afectan al almacenamiento de información clasificada. Los ataques afectaron a aliados y socios de Estonia. Por lo tanto, Nikolay Korchagin está implicado en ciberataques con efectos significativos que constituyen una amenaza externa para un Estado miembro y es responsable de ellos.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Fecha de nacimiento: 1.9.1997 Nacionalidad: rusa Sexo: masculino Entidad asociada: Main Directorate of the General Staff of the Armed Forces of the Russian Federation	Vitaly Shevchenko participa en ciberataques con efectos significativos, y es responsable de ellos, mediante la realización de actividades de inteligencia contra Estonia y la obtención ilegal de acceso a un sistema informático. Vitaly Shevchenko es oficial de la unidad militar 29155 de la Dirección Principal del Alto Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (military unit 29155 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation) (GRU). En el ejercicio de este cargo, participa en ciberataques contra sistemas informáticos, y es responsable de ellos, con el fin de recopilar datos de los sistemas de datos de múltiples instituciones, que ofrecen de forma independiente o combinada una visión general de la política de ciberseguridad de Estonia y de las cibercapacidades del Estado, así como datos personales sensibles y otros datos sensibles, con el fin de utilizarlos para amenazar la seguridad de Estonia. Los ataques afectan al almacenamiento de información clasificada. Los ataques afectaron a aliados y socios de Estonia. Por lo tanto, Vitaly Shevchenko está implicado en ciberataques con efectos significativos que constituyen una amenaza externa para un Estado miembro y es responsable de ellos.	27.1.2025

ELI: http://data.europa.eu/eli/reg_impl/2025/173/oj

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Fecha de nacimiento: 17.6.1980 Nacionalidad: rusa Sexo: masculino Entidad asociada: Main Directorate of the General Staff of the Armed Forces of the Russian Federation	Yuriy Denisov participa en ciberataques con efectos significativos, y es responsable de ellos, mediante la realización de actividades de inteligencia contra Estonia y la obtención ilegal de acceso a un sistema informático. Yuriy Denisov es oficial de la unidad militar 29155 de la Dirección Principal del Alto Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (military unit 29155 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation) (GRU). En el ejercicio de este cargo, participa en ciberataques contra sistemas informáticos, y es responsable de ellos, con el fin de recopilar datos de los sistemas de datos de múltiples instituciones, que ofrecen de forma independiente o combinada una visión general de la política de ciberseguridad de Estonia y de las cibercapacidades del Estado, así como datos personales sensibles y otros datos sensibles, con el fin de utilizarlos para amenazar la seguridad de Estonia. Los ataques afectan al almacenamiento de información clasificada. Los ataques afectaron a aliados y socios de Estonia. Por lo tanto, Yuriy Denisov está implicado en ciberataques con efectos significativos que constituyen una amenaza externa para un Estado miembro y es responsable de ellos.	27.1.2025».